ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Συγκριτική μελέτη της εγχώριας αγοράς πλατφορμών ηλεκτρονικού εμπορίου»

Του φοιτητή
Μανωλέσκου Εμμανουήλ
Αρ. Μητρώου: 06/3002

Επιβλέπων
Γουλιάνας Κωνσταντίνος
Βαθμίδα: Καθηγητής

Ημερομηνία 31/01/2024

Τίτλος: Συγκριτική μελέτη της εγχώριας αγοράς πλατφορμών ηλεκτρονικού εμπορίου

Κωδικός Δ.Ε: 22197

Ονοματεπώνυμο φοιτητή: Μανωλέσκος Εμμανουήλ

Ονοματεπώνυμο εισηγητή: Γουλιάνας Κωνσταντίνος

Ημερομηνία ανάληψης: 30-03-2022

Ημερομηνία περάτωσης: 31-01-2024

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως πτυχιακή εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

ΠΡΟΛΟΓΟΣ

Η παρούσα εργασία μελετάει κυρίως το θέμα της ασφάλειας που παρέχουν τα έτοιμα συστήματα διαχείρισης περιεχομένου (CMS) όπως το Joomla και το Wordpress όσον αφορά σε ιστοσελίδες ηλεκτρονικών καταστημάτων (ecommerce). Η μελέτη πραγματοποιείται στα πλαίσια πτυχιακής εργασίας και έχει χωριστεί σε δύο βασικά μέρη, το θεωρητικό πλαίσιο και το πρακτικό μέρος.

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία πραγματοποιήθηκε στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος (μέρος του πρώην Τ.Ε.Ι Θεσσαλονίκης, σχολή Τεχνολόγων Εφαρμογών, τμήμα Πληροφορικής) κατά το έτος 2023. Η εργασία αυτή δεν θα μπορούσε να είχε ολοκληρωθεί χωρίς την καταλυτική συνδρομή του κ. Κωνσταντίνου Γουλιάνα τον οποίο ευχαριστώ βαθυά για την υπομονή και την στήριξη που μου προσέφερε, τόσο σε φοιτιτικό όσο και σε προσωπικό επίπεδο. Θα ήθελα ακόμα να ευχαριστήσω τον κ. Βασίλειο Κώστογλου για τις κατευθύνσεις και τις επιλογές που μου προσέφερε, ειδικά στα τελευταία χρόνια φοίτησης μου στο τμήμα. Επίσης θέλω να ευχαριστήσω τους πρώην συμφοιτητές μου Στυλιανό Μόσχο και Ιωάννη Βαρσάμη, τους πρώην συνεργάτες μου Κωνσταντίνο και Μιχάλη Λαζαρίδη και φυσικά τους τόσους ανθρώπους στο στενό φιλικό και συντροφικό μου περιβάλλον για την επίμονη στήριξη τους στην επιλογή μου να ολοκληρώσω τις σπουδές μετά απο χρόνια, παρά την απογοήτευση και τις τόσες δυσκολίες που προέκυπταν κατα καιρούς και καθιστούσαν τη περάτωση της αβέβαιη. Τέλος, θα ήθελα να ευχαριστήσω ολα τα μέλη της οικογένειας μου και ιδιαίτερα τον εκλιπών πατέρα μου Φιλήμων Μανωλέσκο, την μητέρα μου Σμαράγδα Μπαρμπή, τον αγαπημένο μου αδελφο Γεώργιο-Βίκτωρα Αλεξόπουλο και τον θετό μου πατέρα Σταύρο Αλεξόπουλο, οι οποίοι υπήρξαν πάντα ένα ανεκτίμητο στήριγμα για μένα και στους οποίους οφείλω μεγάλο μέρος για όλη τη διαδρομή της ζωής και των σπουδών μου, μέχρι σήμερα.

ΠΕΡΙΛΗΨΗ

Τα συστήματα διαχείρισης περιεχομένου (Content Management System) κερδίζουν ολοένα και περισσότερο έδαφος στη δημιουργία ιστοσελίδων και ειδικότερα ηλεκτρονικών καταστημάτων για την ευκολία που παρέχουν στους χρήστες.

Στόχος της παρούσας εργασίας είναι η ανάλυση της ασφάλειας για τα ηλεκτρονικά καταστήματα τα οποία έχουν δημιουργηθεί με λογισμικό CMS (Content Management System) όπως είναι το Joomla και το Wordpress. Τα περισσότερα πλέον ηλεκτρονικά καταστήματα έχουν κατασκευαστεί με κάποιο CMS καθώς παρέχουν πληθώρα δυνατοτήτων μέσα από τα εργαλεία (plugins) που παρέχουν, είτε δωρεάν είτε όχι.

Στο πρώτο μέρος της εργασίας γίνεται μια βιβλιογραφική ανασκόπηση για τους κινδύνους των ιστοσελίδων, τι ακριβώς είναι, πως προκαλούνται και που εντοπίζονται. Αναλύονται οι πλατφόρμες CMS που θα χρησιμοποιηθούν στο πρακτικό μέρος.

Στο κυρίως μέρος το οποίο αποτελεί και το πρακτικό κομμάτι της εργασίας αναλύονται όλα τα εργαλεία καθώς και οι αναλύσεις (τεστ) τα οποία θα γίνουν στα ενδεικτικά ηλεκτρονικά καταστήματα που θα στηθούν ειδικά για το σκοπό αυτό.

Τέλος, γίνεται μια προσπάθεια να συγκεντρωθούν όλες οι ευπάθειες που θα εντποπιστούν καθώς και προτάσεις για την αντιμετώπισή τους.

ABSTRACT

Content Management Systems (CMS) are increasingly gaining ground in website creation and particularly in the development of online commercial stores due to the convenience of creation they offer, both to developers and users. The aim of this study is to analyze the security of online stores that have been created using CMS software such as Joomla and WordPress. Nowadays, most online stores are built using some CMS because they offer a plethora of capabilities through tools (plugins) that are entirely free, or not.

In the first part of the study, a literature review is conducted on the risks of websites—what they are exactly, how they are caused and where they are located. The CMS platforms that will be used in the practical part of the study are analyzed.

In the main part, which also constitutes the practical segment of the study, all tools and analyses (tests) that will be performed on representative online stores specifically set up for this purpose are examined.

Finally, a try-of-effort is made to compile all the vulnerabilities that were located as well as recommendations for addressing them.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια, η τεχνολογία έχει διεισδύσει βαθύτατα στην καθημερινότητα των πωλητών και των καταναλωτών, οπού αποτέλεσμα αυτού είναι και η ανάγκη δημιουργίας ηλεκτρονικών καταστημάτων στο τομέα των επιχειρήσεων. Ωστόσο, μαζί με τις ευκαιρίες που προσφέρει η ευκολία δημιουργίας ενός ηλεκτρονικού καταστήματος, εμφανίζονται και πολλοί κίνδυνοι σχετικά με την ασφάλεια των πληροφοριών. Η κυβερνοασφάλεια είναι ένας τομέας που έχει λάβει ιδιαίτερη προσοχή λόγω των αυξανόμενων κυβερνοεπιθέσεων και της ανάγκης για προστασία των δεδομένων. Η ασφάλεια των δικτυακών συστημάτων έχει μετατραπεί σε πρωταρχικό μέλημα για οργανώσεις και ιδρύματα. Τα δεδομένα αποτελούν το μεγαλύτερο περιουσιακό στοιχείο των περισσότερων και η προστασία τους από κυβερνοεπιθέσεις, διαρροές και παραβιάσεις αποτελεί θεμελιώδη προτεραιότητα. Σε ένα τέτοιο περιβάλλον η ασφάλεια δεν αποτελεί πολυτέλεια, αλλά ανάγκη.

Κάθε ιστοσελίδα και ηλεκτρονικό κατάστημα, ανεξάρτητα από το μέγεθος ή τον σκοπό της, φέρει την ευθύνη να προστατεύει τα δεδομένα των χρηστών της. Η εμπιστοσύνη των χρηστών είναι ευαίσθητη, και μια μόνο παραβίαση μπορεί να οδηγήσει σε απώλεια της εμπιστοσύνης, με συνέπειες πολύ πέραν της απώλειας δεδομένων.

Το περιβάλλον του Διαδικτύου είναι δυναμικό και συνεχώς μεταβαλλόμενο. Οι τεχνικές επίθεσης και εκμετάλλευσης των ευπαθειών στο λογισμικό και το υλικό, συνεχώς εξελίσονται. Γι' αυτό το λόγο, η ανάπτυξη μιας ιστοσελίδας δεν πρέπει να σταματά στον σχεδιασμό και την υλοποίησή της, αλλά να συνεχίζεται με τη διαρκή ενημέρωση και αναβάθμιση των μέτρων ασφαλείας.

Πέραν των βασικών τεχνικών μέτρων, όπως η εγκατάσταση προστατευτικών τειχών και τα συστήματα ανίχνευσης εισβολών, η εκπαίδευση και η ευαισθητοποίηση του ανθρώπινου παράγοντα είναι εξίσου σημαντικές. Πολλές φορές, οι κυβερνοεπιθέσεις έχουν επιτυχία λόγω των πιο προφανών ανθρώπινων λαθών.

Η ασφάλεια στα ηλεκτρονικά καταστήματα (e-shops) είναι από τα πλέον κρίσιμα ζητήματα της ψηφιακής εποχής. Στα e-shops υπάρχει διαχείριση ευαίσθητων δεδομένα των χρηστών, από προσωπικές πληροφορίες όπως διευθύνσεις και τηλέφωνα, μέχρι στοιχεία πιστωτικών καρτών

και άλλες πληροφορίες πληρωμής. Μια παραβίαση της ασφάλειας σε ένα e-shop μπορεί να έχει καταστροφικές συνέπειες, τόσο για τους πελάτες όσο και για την εταιρεία. Πέραν της απώλειας της εμπιστοσύνης των πελατών, υπάρχει και ο κίνδυνος νομικών επακόλουθων και σημαντικών οικονομικών απωλειών. Επομένως, η επένδυση σε αδιάσειστα συστήματα ασφαλείας, προστασίας από επιθέσεις και η συνεχής ενημέρωση στις καλύτερες και νεότερες πρακτικές κυβερνοασφάλειας είναι αναγκαία για κάθε εταιρία και κατάστημα που επιδιώκει τη διατήρηση της αξιοπιστίας τής.

ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

Η ασφάλεια των ιστοσελίδων είναι μια από τις πιο κρίσιμες διαστάσεις της κυβερνοασφάλειας στην εποχή του Διαδικτύου. Με την επέκταση της ψηφιακής αγοράς, οι ιστοσελίδες υπηρετούν ως πρωτεύουσες πύλες για την αλληλεπίδραση μεταξύ των επιχειρήσεων και των καταναλωτών [1].

Πρακτικά, η ασφάλεια των ιστοσελίδων συνίσταται σε πολλαπλά επίπεδα προστασίας. Η κρυπτογράφηση με τη χρήση πρωτοκόλλων όπως το SSL/TLS είναι απαραίτητη για την ασφαλή μεταφορά δεδομένων μεταξύ του διακομιστή και του πελάτη [2]. Εκτός από αυτό, είναι κρίσιμη η προφύλαξη από επιθέσεις όπως SQL Injection, όπου οι εισβολείς προσπαθούν να εκτελέσουν κακόβουλες εντολές SQL για να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες όπως και επιθέσεις Cross-Site Scripting (XSS), που επιτρέπουν στους εισβολείς να εκτελέσουν ενέργειες εκ μέρους των χρηστών [3].

Οι κίνδυνοι που αντιμετωπίζουν οι ιστοσελίδες είναι ποικίλοι και συχνά εξελίσσονται. Εκτός από τις επιθέσεις SQL Injection και XSS, υπάρχει ο κίνδυνος των DDoS επιθέσεων, που αποσκοπούν στην πλήρη αδράνεια της ιστοσελίδας δημιουργώντας μεγάλη εικονική κίνηση «flood» στο δίκτυο [4]. Άλλοι κίνδυνοι περιλαμβάνουν την κλοπή δεδομένων, την αποκάλυψη ευπαθειών και την κακή χρήση των εργαλείων διαχείρισης περιεχομένου.

Στο πλαίσιο αυτό, είναι απαραίτητο για τις επιχειρήσεις τους οργανισμούς και τι εταιριές να εφαρμόσουν συστηματικά πρωτόκολλα ασφάλειας και να παρακολουθούν συνεχώς για πιθανές

απειλές. Η ασφάλεια των ιστοσελίδων δεν είναι πλέον προαιρετική, αλλά ουσιαστική για την προστασία των πληροφοριών και της διατήρηση της εμπιστοσύνης των χρηστών.

Δοκιμές διείσδυσης (Penetration Testing)

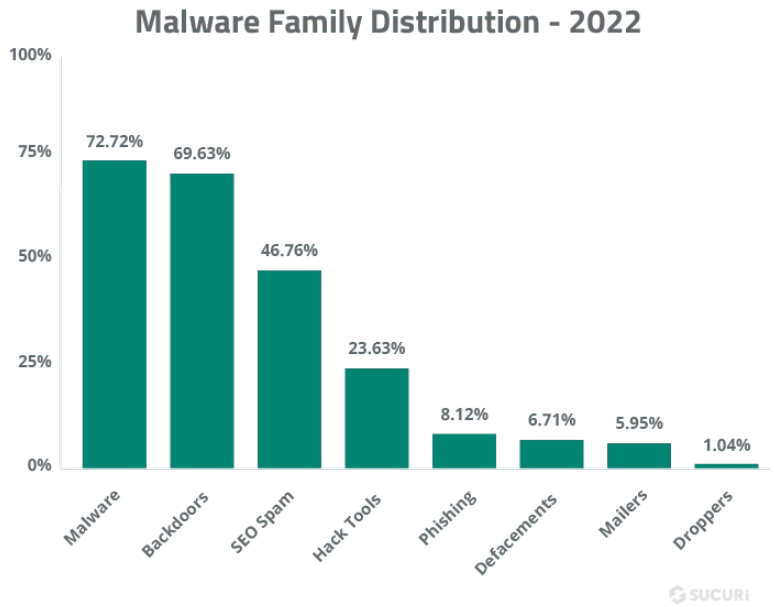
Η δοκιμή διείσδυσης, γνωστή και ως Penetration test, αποτελεί μια εξειδικευμένη τεχνική αξιολόγησης της ασφάλειας ιστοσελίδων, δικτύων και άλλων υποδομών πληροφορικής. Στο πλαίσιο αυτής της διαδικασίας, προσομοιώνονται επιθέσεις από μη εξουσιοδοτημένους χρήστες ή συστήματα, είτε εσωτερικά είτε εξωτερικά, με σκοπό την απόκτηση πρόσβασης σε ευαίσθητα δεδομένα, όπως και την πρόκληση βλαβών στη λειτουργία.

Ο κύριος στόχος της δοκιμής διείσδυσης είναι η αξιολόγηση της ασφάλειας των συστημάτων, κατά πόσο είναι εφικτή η παραβίαση αυτών και η ανάλυση των πιθανών συνεπειών που μπορεί να έχουν τέτοιες παραβιάσεις στους σχετικούς πόρους ή λειτουργίες.

Η δοκιμή διείσδυσης συμβάλλει στην αντιμετώπιση των γενικών πτυχών ελέγχου και συμμόρφωσης των κανονισμών και των βέλτιστων πρακτικών του κλάδου. Μέσω της εκμετάλλευσης της υποδομής μιας οργάνωσης, η δοκιμή διείσδυσης μπορεί να αποδείξει ακριβώς πώς ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα.

Η διαδικασία της δοκιμής διείσδυσης αποτελείται από διάφορα στάδια, όπως η συλλογή πληροφοριών, η έρευνα και εκμετάλλευση, η σύνταξη αναφοράς και συστάσεων, καθώς και η αντιμετώπιση με συνεχή υποστήριξη. Οι δοκιμές πραγματοποιούνται κυρίως με σκοπό τη διατήρηση της ασφάλειας της ανάπτυξης ασφαλούς λογισμικού κατά τη διάρκεια του κύκλου ζωής του.

Σε έρευνα που διεξήχθη το 2022 από την εταιρία Sucuri, εντοπίσθηκε πως 14.51% των ευπαθειών είχαν προκληθεί σε ιστοσελίδες με λογισμικό Wordpress που λειτουργούσαν με παλαιότερες εκδόσεις του Woocoomerce, εργαλείο (plugin) το οποίο βοηθάει στη δημιουργία ηλεκτρικού καταστήματος [1]. Στην ίδια έρευνα αξιολογήθηκαν και άλλες επιθέσεις και ευπάθειες ώστε να εντοπιστούν οι συχνότερες εξ αυτών με σκοπό την αντιμετώπισή τους.



Εικόνα 1: Η συχνότητα με την οποία εντοπίζονται οι ευπάθειες (πηγή: https://sucuri.net/)

Το παραπάνω διάγραμμα εμφανίζει τα ευρήματα κατά την εκκαθάριση των υπολογιστών. Αυτό πρακτικά σημαίνει πως μια ιστοσελίδα ενδεχομένως να έχει προσβληθεί από δύο ή περισσότερες ευπάθειες.

Στην ίδια έρευνα εντοπίστηκαν πολλές περιπτώσεις υποκλοπής στοιχείων πιστωτικής κάρτας. Στο 90% των περιπτώσεων, οι ιστότοποι βρέθηκαν να περιέχουν σύστημα υποκλοπής από την πλευρά του διακομιστή με τη μορφή κακόβουλου κώδικα PHP που δεν είναι εξωτερικά ορατος και μπορούν να εντοπιστούν μόνο σε επίπεδο διακομιστή. Ένα άλλο 14% των ιστότοπων είχαν σύστημα υποκλοπής από την πλευρά του πελάτη που βρέθηκαν με τη μορφή κακόβουλων εκτελέσεων κώδικα (injections) JavaScript. Οι πιο συνηθισμένες τοποθεσίες όπου βρέθηκαν αυτά τα τμήματα κώδικα για υποκλοπές πιστωτικών καρτών εμφανίζονται στην επόμενη εικόνα όπου φαίνεται το αρχείο και η συχνότητα με την οποία είχε μολυνθεί.

Credit Card Skimmer File Locations - 2022

File name	Percentage
./wp-content/plugins/woocommerce/templates/checkout/form-checkout.php	29.37%
./wp-includes/vars.php	25.99%
./wp-content/plugins/wpyii2/wpyii2.php	20.68%
./wp-content/plugins/wpzip/wpzip.php	13.72%
./app/Mage.php	5.02%
./wp-content/plugins/wpputty/wpputty.php	5.02%
./app/code/core/Mage/Core/Helper/Cookie.php	4.73%
./app/code/core/Mage/Core/Model/Config/Base.php	4.44%
./app/code/core/Mage/Core/Model/Abstract.php	4.25%
./app/code/core/Mage/Core/Model/Session/Abstract/Varien.php	4.25%

Εικόνα 2: Συγκεντρωτική Ανάλυση Συχνότητας Ευπαθών Αρχείων για Skimmers σε Συστήματα WordPress – 2022 (πηγή: https://sucuri.net/)

Από την παραπάνω εικόνα είναι εμφανές πως τον μεγαλύτερο κίνδυνο διατρέχει το αρχείο "form-checkout.php" το οποίο είναι υπεύθυνο για την ολοκλήρωση μιας αγοράς μέσω του Woocoomerce, του δημοφιλέστερου δηλαδή εργαλείου δημιουργίας ηλεκτρονικού καταστήματος.

ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ

Στόχος της παρούσας μελέτης είναι η ανάλυση της ασφάλειας για τα ηλεκτρονικά καταστήματα τα οποία έχουν δημιουργηθεί με λογισμικό CMS (Content Management System) όπως είναι το Joomla και το Wordpress. Η επιλογή των παραπάνω λογισμικών έγινε με βασικό κριτήριο τη χρήση τους, δηλαδή το μερίδιο αγοράς που έχει το καθένα στη δημιουργία ιστοσελίδων. Σε έρευνα που διεξήχθη το 2023, περίπου 810 εκατομμύρια ιστοσελίδες έχουν δημιουργηθεί με την πλατφόρμα Wordpress. Αυτό αντιστοιχεί στο 43% όλων των ιστοσελίδων που υπάρχουν στο

διαδίκτυο, καθιστώντας το Wordpress στην πιο δημοφιλή πλατφόρμα CMS με μεγάλη διαφορά από τις άλλες πλατφόρμες. Για το λόγο αυτό στην παρούσα εργασία επιλέχθηκαν δύο πλατφόρμες CMS για τις δοκιμές καθώς επίσης δίνεται μεγάλη έμφαση στο Wordpress. Η δεύτερη πλατφόρμα που έχει επιλεχθεί είναι το Joomla, μια πλατφόρμα με 30 εκατομμύρια ιστοσελίδες παγκοσμίως (περίπου το 1.8% της παγκόσμιας αγοράς) [1]. Τα δύο αυτά συστήματα όμως είναι στην πρώτη πεντάδα όσον αφορά τα CMS και ειδικότερα στην Ελλάδα είναι τα δύο πιο δημοφιλή. Πιο συγκεκριμένα, το μερίδιο της αγοράς μόνο στα CMS διαμορφώνεται ως εξής [1]:

1. WordPress – 64.2%
2. Shopify – 6.2%
3. Wix – 3.4%
4. Squarespace – 3%
5. Joomla – 2.5%

Με δεδομένο πως τα Shopify, Wix και Squarespace διαθέτουν τις υπηρεσίες τους επι πληρωμή, επιλέχθηκαν το Wordpress και το Joomla για τις δοκιμές.

Μεθοδολογία

Στο πλαίσιο της παρούσας εργασίας, υλοποιήθηκε μια προσεκτικά σχεδιασμένη μεθοδολογία για την εκτέλεση δοκιμών διείσδυσης (penetration tests) και την ανίχνευση ευπαθειών σε διάφορες διαδυκτιακές εφαρμογές οι οποίες δημιουργήθηκαν με αποκλειστικό σκοπό να ελεγχθούν για ευπάθειες. Ενδεχομένως σε πραγματικές συνθήκες, δηλαδή σε ιστοσελίδες οι οποίες θα φιλοξενούνται σε πραγματικούς servers κάποια αποτελέσματα να ήταν διαφορετικά αλλά λόγω της επικινδυνότητας που έχουν πολλές μέθοδοι από αυτές που χρησιμοποιήθηκαν, όλες οι δοκιμές έγιναν σε ελεγχόμενο περιβάλλον (localhost) καθώς και σε εικονικούς υπολογιστές (virtual machines). Η μεθοδολογία που ακολουθήθηκε περιγράφεται αναλυτικά στα παρακάτω βήματα:

Δημιουργία Εικονικών Μηχανών: Αρχικά, δημιουργήθηκαν τρεις διαφορετικές εικονικές μηχανές στο Amazon Web Services (AWS), οι οποίες είχαν εγκατεστημένα τα λειτουργικά συστήματα Windows 11, Windows 10 και Kali Linux αντίστοιχα.

Εγκατάσταση Java JDK: Σε όλες τις εικονικές μηχανές εγκαταστάθηκε το Java JDK, προκειμένου να εξασφαλιστεί η συμβατότητα με τις εφαρμογές που θα χρησιμοποιηθούν για τις δοκιμές διείσδυσης.

Εγκατάσταση XAMPP, WordPress και Joomla στα Windows: Στις εικονικές μηχανές με λειτουργικό σύστημα Windows, εγκαταστάθηκε το XAMPP, το οποίο είναι ένα λογισμικό που παρέχει περιβάλλον Apache, MariaDB, PHP και Perl. Στη συνέχεια, δημιουργήθηκαν δύο ιστοσελίδες e-shop, μία με την χρήση του CMS WordPress και μία με την χρήση του CMS Joomla. Κάθε ιστοσελίδα αναπτύχθηκε και ρυθμίστηκε με σκοπό την προσομοίωση ενός πραγματικού περιβάλλοντος e-shop.

Εγκατάσταση Kali Linux και XAMPP: Στην τρίτη εικονική μηχανή, εγκαταστάθηκε το Kali Linux και το XAMPP. Το Kali Linux είναι ένα λειτουργικό σύστημα που έχει σχεδιαστεί ειδικά για την πραγματοποίηση δοκιμών διείσδυσης και ανάλυσης ευπαθειών.

Δοκιμές Διείσδυσης στα Windows: Χρησιμοποιώντας τα εργαλεία OWASP ZAP, Nessus, Zenmap και Wireshark, πραγματοποιήθηκαν δοκιμές διείσδυσης στις ιστοσελίδες e-shop που δημιουργήθηκαν στα Windows. Κάθε εργαλείο χρησιμοποιήθηκε για διαφορετικούς σκοπούς, όπως η ανίχνευση ευπαθειών, η ανάλυση της κίνησης δικτύου και η εξερεύνηση των δικτυακών υπηρεσιών.

Δοκιμές Διείσδυσης στο Kali Linux: Στην εικονικό περιβάλλον Kali Linux, εισήχθησαν οι ιστοσελίδες e-shop και πραγματοποιήθηκαν δοκιμές διείσδυσης χρησιμοποιώντας τα εργαλεία WPScan και SQLMap. Το WPScan χρησιμοποιήθηκε για την ανίχνευση ευπαθειών στο WordPress, ενώ το SQLMap για την ανίχνευση ευπαθειών SQL Injection.

Ανάλυση Αποτελεσμάτων: Τα αποτελέσματα και οι αναφορές που παρήχθησαν από κάθε εργαλείο κατά τη διάρκεια των δοκιμών διείσδυσης θα αναλυθούν λεπτομερώς σε μεταγενέστερο στάδιο. Η ανάλυση αυτή θα περιλαμβάνει την εξέταση κάθε ευπάθειας που ανιχνεύθηκε, την αξιολόγηση της σοβαρότητάς της και την αναζήτηση πιθανών λύσεων και προληπτικών μέτρων.

Οι λειτουργίες που θα υποβληθούν σε εξέταση και θα τεθούν υπό έλεγχο είναι οι εξής:

1. Έλεγχος Ταυτότητας και Εξουσιοδότησης (Authentication and Authorization): Η ιστοσελίδα του ηλεκτρονικού καταστήματος θα πρέπει να διαθέτει ένα ασφαλές σύστημα σύνδεσης που απαιτεί ισχυρούς κωδικούς πρόσβασης και έχει λάβει μέτρα για την αποτροπή επιθέσεων. Θα πρέπει επίσης να διαθέτει κατάλληλους ελέγχους εξουσιοδότησης για να διασφαλίσει ότι οι χρήστες μπορούν να έχουν πρόσβαση μόνο στις σελίδες και τις λειτουργίες στις οποίες είναι εξουσιοδοτημένοι να έχουν πρόσβαση.
2. Επικύρωση Εισόδου (Input Validation): Η ιστοσελίδα του ηλεκτρονικού καταστήματος θα πρέπει να επικυρώνει όλα τα στοιχεία εισόδου του χρήστη για να αποτρέψει την SQL injection, τη δημιουργία cross-site scripting (XSS) και άλλες επιθέσεις.
3. Ασφαλείς Επικοινωνίες (Secure Communications): Η ιστοσελίδα του ηλεκτρονικού καταστήματος θα πρέπει να χρησιμοποιεί ασφαλή πρωτόκολλα επικοινωνίας όπως το HTTPS για την προστασία των ευαίσθητων δεδομένων κατά τη μεταφορά.
4. Επεξεργασία Πληρωμών (Payment Processing): Η ιστοσελίδα του ηλεκτρονικού καταστήματος θα πρέπει να διαθέτει ασφαλές σύστημα επεξεργασίας πληρωμών που να συμμορφώνεται με πρότυπα όπως το PCI DSS.
5. Διαμόρφωση Διακομιστή (Server Configuration): Η ιστοσελίδα του ηλεκτρονικού καταστήματος θα πρέπει να έχει μια ασφαλή διαμόρφωση διακομιστή που περιλαμβάνει κατάλληλες άδειες αρχείων, ασφαλείς κωδικούς πρόσβασης και τακτικές ενημερώσεις ασφαλείας.
6. Ενσωματώσεις Τρίτων (Third-party Integrations): Η ιστοσελίδα του ηλεκτρονικού καταστήματος θα πρέπει να ελεγχθεί για τρωτά σημεία σε οποιεσδήποτε ενσωματώσεις τρίτων, όπως πύλες πληρωμών, πάροχοι αποστολής και άλλες υπηρεσίες.

Διεξάγοντας αυτές τις δοκιμές για την εντοπισμό τρωτών σημείων, μπορεί να διασφαλιστεί ότι η ιστοσελίδα του ηλεκτρονικού καταστήματος είναι ασφαλής και προστατευμένη από πιθανές επιθέσεις.

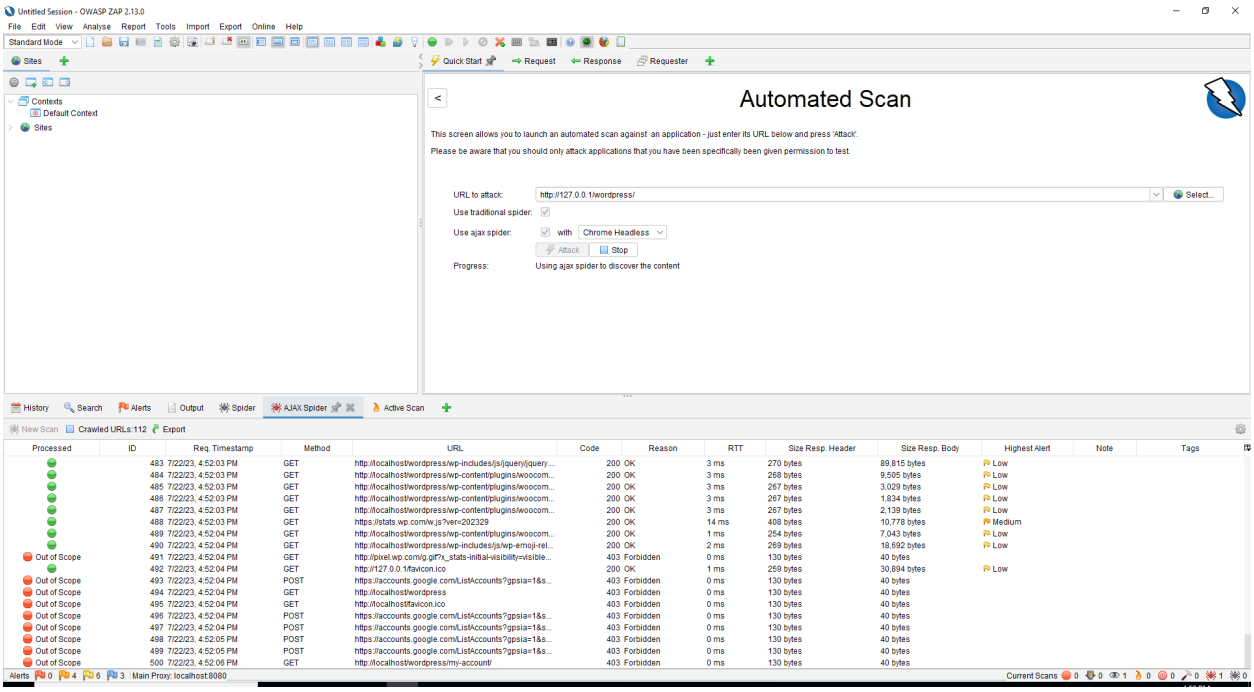
Penetration testing στο WordPress (Woocommerce)

OWASP ZAP (WordPress Pen Tests)

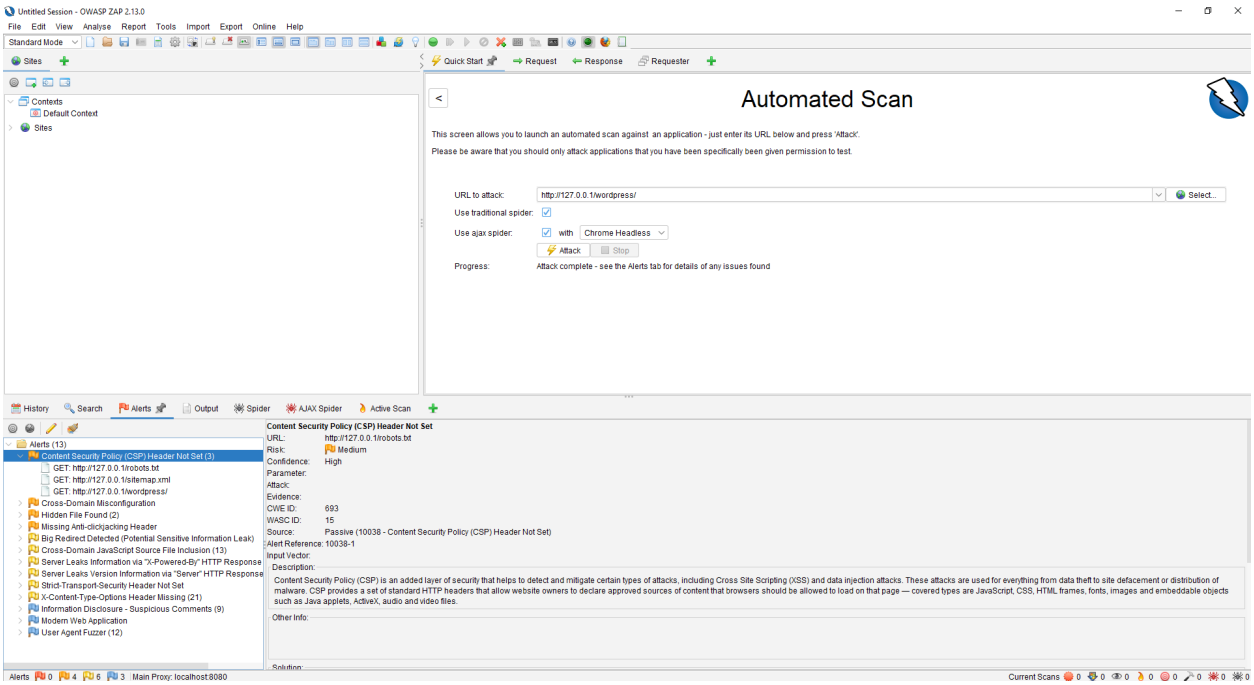
Το OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) είναι ένα ανοιχτού κώδικα εργαλείο για τη δοκιμή της ασφάλειας ιστοσελίδων. Αποτελεί μια πολύ χρήσιμη πλατφόρμα για τους επαγγελματίες ασφαλείας που εργάζονται με δοκιμές διείσδυσης (penetration tests). Το OWASP ZAP παρέχει δυνατότητες όπως ο αυτόματος σαρωτής, ο οποίος μπορεί να ανακαλύψει πολλές ευπάθειες σε μια ιστοσελίδα, συμπεριλαμβανομένων των παραβιάσεων της πολιτικής ίδιας προέλευσης (Same Origin Policy), των επιθέσεων SQL Injection και των επιθέσεων Cross-Site Scripting (XSS).Σε γενικές γραμμές, το OWASP ZAP είναι ένα ισχυρό εργαλείο για την εξασφάλιση της ασφάλειας των ιστοσελίδων, παρέχοντας εκτενείς δυνατότητες δοκιμής διείσδυσης.

Εγκατάσταση και ρύθμιση του OWASP ZAP

Για την εκτέλεση του εργαλείου δοκιμής διείσδυσης OWASP ZAP στην εικονική μηχανή, ήταν απαραίτητη η λήψη και η εγκατάσταση της πλατφόρμας ανάπτυξης Java (Java JDK 20). Κατά την αρχικοποίηση της εφαρμογής, ζητήθηκε από τον χρήστη να επιλέξει εάν επιθυμεί να αποθηκευτεί το προγραμματισμένο τεστ διείσδυσης. Με την επιλογή των προεπιλεγμένων ρυθμίσεων, ξεκίνησε η διαδικασία του τεστ, ενώ στο πεδίο URL εισήχθη η διεύθυνση 'http://localhost/wordpress'. Οι μέθοδοι “crawling” που χρησιμοποιήθηκαν για την ανίχνευση των συνδέσμων της ιστοσελίδας ήταν οι προεπιλεγμένες “Ajax Spider” και “Traditional Spider”.



Εικόνα 3: Αυτοματοποιημένη Σάρωση OWASP ZAP για Ανίχνευση Ευπαθειών



Εικόνα 4: Κατηγοριοποίηση Αποτελεσμάτων OWASP ZAP για Αναλυτική Διάγνωση

Κατά την ολοκλήρωση της σάρωσης, θα πρέπει να σημειωθεί πως η βάση δεδομένων είχε καταστραφεί. Στην επόμενη λίστα που ακολουθεί είναι οι λεπτομέρειες σχετικά με τυχόν προβλήματα που εντοπίστηκαν.

- Λανθασμένη διαμόρφωση διαφορετικού τομέα.
- Εντοπίστηκε κρυφό αρχείο (2 περιπτώσεις).
- Απουσία κεφαλίδας Anti-clickjacking.
- Εντοπίστηκε μεγάλη ανακατεύθυνση (Πιθανή διαρροή ευαίσθητων πληροφοριών).
- Συμπερίληψη αρχείου πηγαίου κώδικα JavaScript από διαφορετικό τομέα (13 περιπτώσεις).
- Ο διακομιστής διαρρέει πληροφορίες μέσω της απάντησης HTTP "X-Powered-By".
- Ο διακομιστής διαρρέει πληροφορίες μέσω της απάντησης HTTP "Server".
- Η κεφαλίδα Strict Transport-Security δεν έχει οριστεί.
- Λείπει η κεφαλίδα X-Content-Type-Options (21 περιπτώσεις).
- Αποκάλυψη πληροφοριών - Ύποπτα σχόλια (9 περιπτώσεις).
- Σύγχρονη εφαρμογή ιστού.
- User Agent Fuzzer (12 περιπτώσεις).

Υπάρχει μια λεπτομερής ειδοποίηση σχετικά με την "Κεφαλίδα Πολιτικής Ασφάλειας Περιεχομένου (CSP) που δεν έχει οριστεί" με επίπεδο κινδύνου μεσαίο και υψηλή εμπιστοσύνη. Η περιγραφή εξηγεί τι είναι το CSP και τη σημασία του στην αντιμετώπιση ορισμένων τύπων επιθέσεων, συμπεριλαμβανομένων των επιθέσεων Cross-Site Scripting (XSS) και επιθέσεων εισαγωγής δεδομένων.

Αναλυτικότερα :

Το αρχείο αναφοράς σάρωσης ZAP περιέχει τις ακόλουθες ειδοποιήσεις μέσου κινδύνου (medium risk):

- Δεν έχει οριστεί η κεφαλίδα Πολιτικής Ασφάλειας Περιεχομένου (CSP) για τον ιστότοπο http://127.0.0.1/wordpress . Αυτή η ειδοποίηση εμφανίζεται όταν ένας ιστότοπος δεν

ορίζει μια κεφαλίδα Πολιτικής Ασφάλειας Περιεχομένου (CSP), η οποία μπορεί να βοηθήσει στην πρόληψη μιας σειράς επιθέσεων, συμπεριλαμβανομένης της XSS. Η ειδοποίηση εμφανίστηκε με υψηλή εμπιστοσύνη.

- Βρέθηκε Κρυμμένο Αρχείο στο http://127.0.0.1/server-status . Αυτή η ειδοποίηση εμφανίζεται όταν ανακαλύπτεται ένα κρυμμένο αρχείο ή κατάλογος στον διακομιστή. Η ειδοποίηση εμφανίστηκε με υψηλή εμπιστοσύνη.
- Λανθασμένη Διαμόρφωση Διατομειακής Επικοινωνίας για τον ιστότοπο https://stats.wp.com/w.js?ver=202329. Αυτή η ειδοποίηση εμφανίζεται όταν ένας ιστότοπος είναι διαμορφωμένος ώστε να επιτρέπει την πρόσβαση στους πόρους του από άλλους ιστότοπους, πράγμα που μπορεί να οδηγήσει σε αποκάλυψη πληροφοριών ή άλλες ευπάθειες. Η ειδοποίηση εμφανίστηκε με μέση εμπιστοσύνη.
- Απουσία Κεφαλίδας Αντι-Clickjacking για τον ιστότοπο http://127.0.0.1/wordpress. Αυτή η ειδοποίηση εμφανίζεται όταν ένας ιστότοπος δεν ορίζει μια κεφαλίδα για την πρόληψη των επιθέσεων clickjacking, όπου ένας επιτιθέμενος ξεγελά έναν χρήστη να κάνει κλικ σε ένα κρυμμένο στοιχείο μιας ιστοσελίδας. Η ειδοποίηση εμφανίστηκε με μέση εμπιστοσύνη.

<u>Ακολουθούν κάποιες γενικές λύσεις για τις ειδοποιήσεις μέσου κινδύνου που προσδιορίστηκαν στην Έκθεση Σάρωσης ZAP:</u>

- Δεν έχει οριστεί η κεφαλίδα Πολιτικής Ασφάλειας Περιεχομένου (CSP): Η Πολιτική Ασφάλειας Περιεχομένου (CSP) είναι μια λειτουργία ασφάλειας που μπορεί να βοηθήσει στην πρόληψη μιας σειράς επιθέσεων, συμπεριλαμβανομένης της XSS. Για να επιλυθεί αυτήν την ειδοποίηση, θα πρέπει να οριστεί μια κεφαλίδα CSP για τον ιστότοπο. Η συγκεκριμένη πολιτική που θα οριστεί θα εξαρτηθεί από τις ανάγκες του ιστότοπου αλλά μια τυπική πολιτική θα μπορούσε να φαίνεται κάπως έτσι: `Content-Security-Policy: default-src 'self'`. Αυτή η πολιτική θα επιτρέπει μόνο τη φόρτωση πόρων από την ίδια προέλευση.
- Βρέθηκε Κρυμμένο Αρχείο: Αυτή η ειδοποίηση εμφανίζεται όταν ανακαλύπτεται ένα κρυμμένο αρχείο ή κατάλογος στον διακομιστή. Για να επιλυθεί αυτή η ειδοποίηση, θα πρέπει να αφαιρεθούν οποιαδήποτε περιττά αρχεία από τον διακομιστή και να διασφαλισθεί ότι τα απαραίτητα αρχεία είναι κατάλληλα προστατευμένα. Εάν το αρχείο

είναι απαραίτητο και θα πρέπει να είναι προσβάσιμο, πρέπει να επιβεβαιωθεί ότι δεν περιέχει ευαίσθητες πληροφορίες. Εάν το αρχείο δεν είναι απαραίτητο ή δεν θα πρέπει να είναι προσβάσιμο, να αφαιρεθεί ή περιοριστεί η πρόσβαση σε αυτό.

- Λανθασμένη Διαμόρφωση Διατομειακής Επικοινωνίας: Αυτή η ειδοποίηση εμφανίζεται όταν ένας ιστότοπος είναι διαμορφωμένος ώστε να επιτρέπει την πρόσβαση στους πόρους του από άλλους ιστότοπους, πράγμα που μπορεί να οδηγήσει σε αποκάλυψη πληροφοριών ή άλλες ευπάθειες. Για να επιλυθεί αυτή η ειδοποίηση, θα πρέπει να εξεταστεί η πολιτική Διατομειακής Κοινής Χρήσης Πόρων (CORS) του ιστότοπού και να διασφαλιστεί ότι επιτρέπει την πρόσβαση μόνο από έμπιστους τομείς.
- Απουσία Κεφαλίδας Αντι-Clickjacking: Αυτή η ειδοποίηση εμφανίζεται όταν ένας ιστότοπος δεν ορίζει μια κεφαλίδα για την πρόληψη των επιθέσεων clickjacking. Για να επιλυθεί αυτή η ειδοποίηση, θα πρέπει να οριστεί η κεφαλίδα 'X-Frame-Options' για τον ιστότοπό σε 'DENY' ή 'SAMEORIGIN'. Αυτό θα αποτρέψει την εμφάνιση του ιστότοπού σε ένα πλαίσιο, το οποίο είναι ο τρόπος με τον οποίο συνήθως εκτελούνται οι επιθέσεις clickjacking.

Nessus Essentials

Το Nessus Essentials, γνωστό και ως Nessus, είναι ένα εργαλείο αυτοματοποιημένης εξέτασης ευπαθειών που χρησιμοποιείται ευρέως στην κοινότητα ασφάλειας πληροφοριακών συστημάτων. Αναπτύχθηκε αρχικά από την Tenable Network Security, ενώ η έκδοση "Essentials" είναι διαθέσιμη δωρεάν για χρήση σε μικρότερες κλίμακες.

Το Nessus χρησιμοποιείται για την ανακάλυψη ευπαθειών σε δίκτυα, συστήματα και εφαρμογές ιστού. Αυτό γίνεται μέσω της σάρωσης διαφόρων πρωτοκόλλων και υπηρεσιών για να εντοπίσει πιθανές ευπάθειες, όπως απαρχαιωμένο λογισμικό, λάθη στην παραμετροποίηση, και άλλα προβλήματα που θα μπορούσαν να εκμεταλλευτούν.

Στο πλαίσιο του Penetration Testing σε ένα Web app, το Nessus μπορεί να χρησιμοποιηθεί για να εντοπίσει και να αξιολογήσει ευπάθειες που θα μπορούσαν να εκμεταλλευτούν κατά τη διάρκεια μιας επίθεσης. Αυτό μπορεί να περιλαμβάνει ευπάθειες σε επίπεδο εφαρμογής, όπως Cross-Site Scripting (XSS), SQL Injection, και Cross-Site Request Forgery (CSRF), καθώς και ευπάθειες

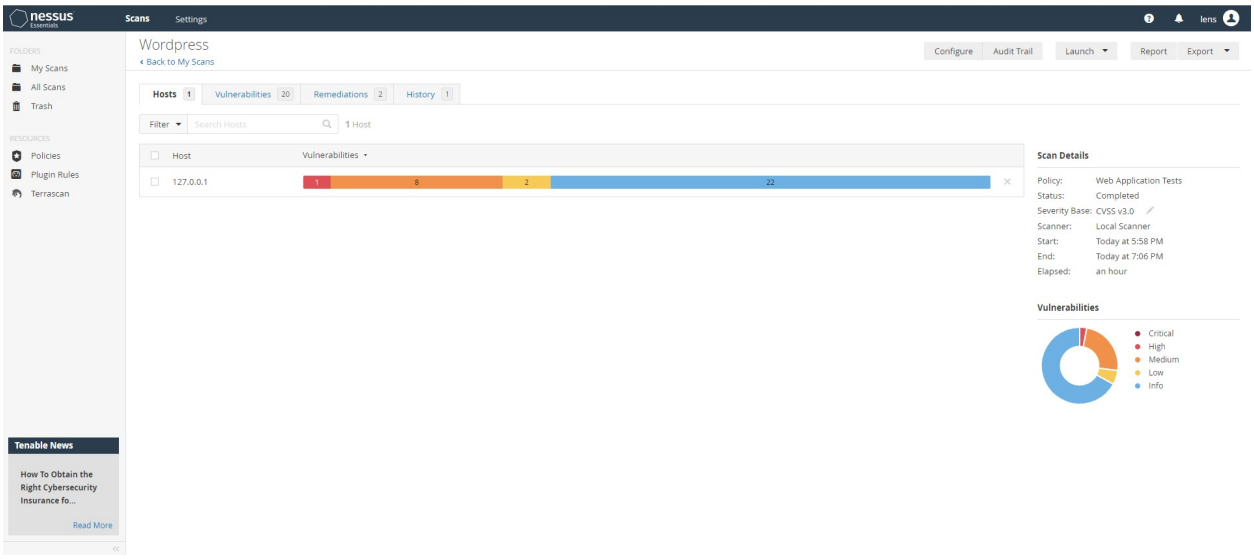
σε επίπεδο δικτύου ή λειτουργικού συστήματος που μπορεί να επηρεάσουν την ασφάλεια της εφαρμογής. Η χρήση του Nessus σε αυτό το πλαίσιο μπορεί να βοηθήσει τους επαγγελματίες ασφάλειας πληροφορικής να κατανοήσουν καλύτερα τις ευπάθειες της εφαρμογής τους και να λάβουν τα κατάλληλα μέτρα για την προστασία της.

Εγκατάσταση και ρύθμιση του Nessus Essentials

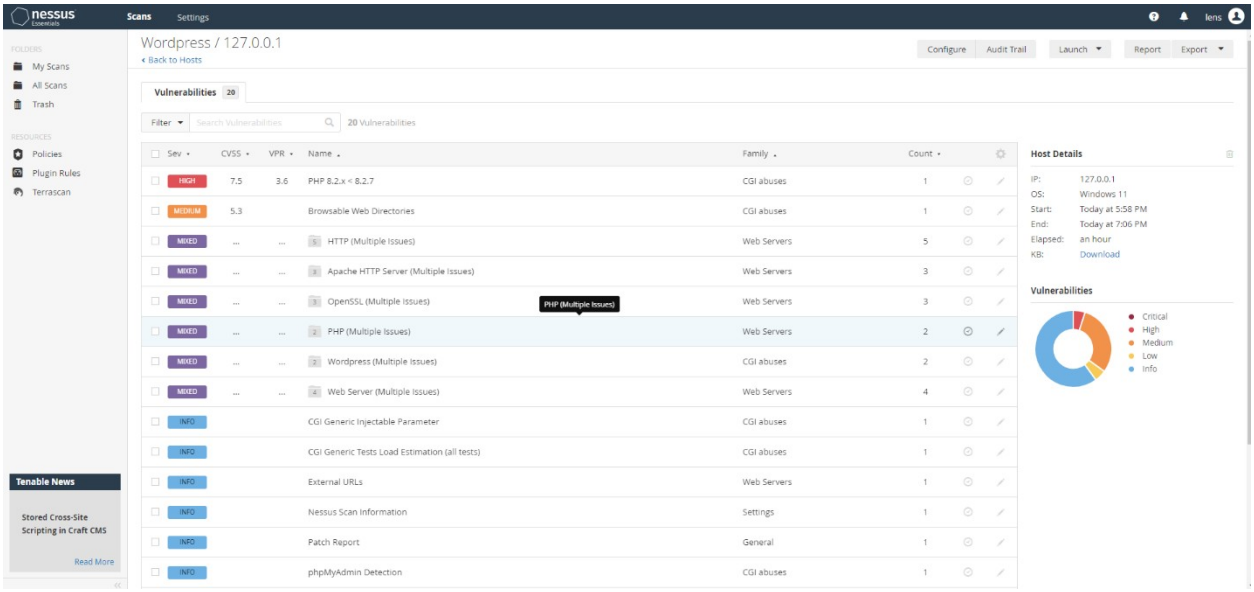
Για την εγκατάσταση του Nessus Essentials, ήταν απαραίτητη η δημιουργία λογαριασμού στην επίσημη ιστοσελίδα της εφαρμογής (https://www.tenable.com/products/nessus/nessus-essentials), παρέχοντας ένα επαγγελματικό email. Ο κωδικός για τη χρήση του λογισμικού αποστάλθηκε από την εταιρεία στο παρεχόμενο email. Μετά την εγκατάσταση του Nessus Essentials, άνοιξε μια νέα καρτέλα στον προεπιλεγμένο περιηγητή του υπολογιστή, ζητώντας την ενεργοποίηση του λογισμικού με τον κωδικό άδειας χρήσης που παρασχέθηκε και τον ορισμό ενός admin username και password.

Η τοπική διεύθυνση από την οποία θα χρησιμοποιηθεί το Nessus Essentials είναι η https://localhost:8834/#/. Από τον πίνακα ελέγχου του λογισμικού, επιλέχθηκε το Web Application Test από την ομάδα Vulnerabilities. Επιλέχθηκαν οι προεπιλεγμένες επιλογές και ένα όνομα για τη διαδικασία σάρωσης στο μενού ρυθμίσεων, ενώ στην καρτέλα Credential απενεργοποιήθηκε οποιαδήποτε πιστοποίηση σχετικά με την πρόσβαση στη σελίδα όπου θα πραγματοποιηθεί το τεστ διείσδυσης. Ως στόχος επιλέχθηκε το 127.0.0.1 και ως εύρος θυρών τα 80,443,3306,8080. Επιλέχθηκε κάθε οικογένεια προσθέτων, ώστε να πραγματοποιηθεί μια ολοκληρωμένη διαδικασία δοκιμής διείσδυσης. Μετά από όλα αυτά, έγινε η αποθήκευση των ρυθμίσεων και η εκτέλεση των τεστ, οι οποίες διήρκησαν αρκετή ώρα μέχρι να παρουσιαστούν τα αντίστοιχα αποτελέσματα.

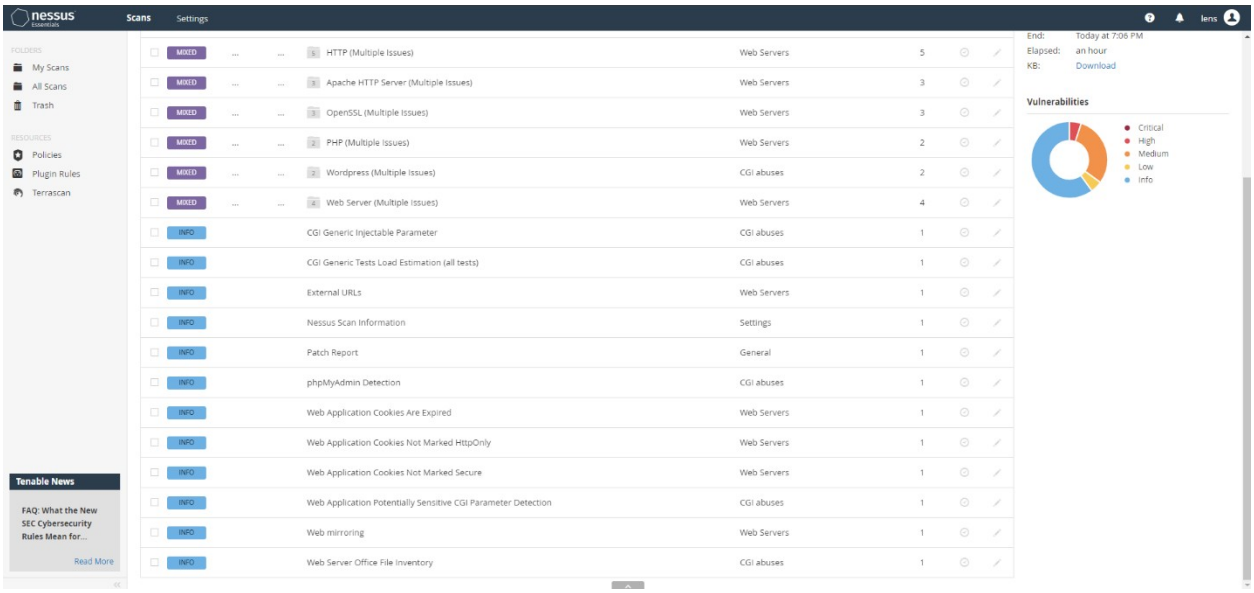
Nessus Essentials (WordPress Pen Tests)



Εικόνα 5:Κατηγορίες Ευπαθειών σε Σάρωση WordPress με Nessus



Εικόνα 6: Λεπτομερής Αναφορά Ευπαθειών WordPress από Nessus



Εικόνα 7:Λεπτομερής Αναφορά Ευπαθειών WordPress από Nessus

CGI abuses : Αυτή η οικογένεια πρόσθετων περιλαμβάνει δοκιμές για διάφορες ευπάθειες και λανθασμένες ρυθμίσεις που σχετίζονται ειδικά με τα σενάρια CGI (Common Gateway Interface). Αυτά μπορεί να περιλαμβάνουν ζητήματα όπως ευπάθειες injection εντολών, ευπάθειες αποκάλυψης πληροφοριών κα.

CGI abuses : XSS: Αυτή η οικογένεια πρόσθετων επικεντρώνεται ειδικά στις ευπάθειες Cross-Site Scripting (XSS) εντός των σεναρίων CGI. Οι ευπάθειες XSS προκύπτουν όταν μια εφαρμογή συμπεριλαμβάνει μη έμπιστα δεδομένα σε μια νέα ιστοσελίδα χωρίς κατάλληλη επικύρωση ή διαφυγή ή ενημερώνει μια υπάρχουσα ιστοσελίδα με δεδομένα που παρέχει ο χρήστης.

Web servers : Αυτή η οικογένεια πρόσθετων περιλαμβάνει ελέγχους για ευπάθειες και λανθασμένες ρυθμίσεις που σχετίζονται ειδικά με το λογισμικό του διακομιστή ιστού (όπως Apache, Nginx, IIS κλπ.). Αυτά θα μπορούσαν να περιλαμβάνουν ελέγχους για γνωστές ευπάθειες στο λογισμικό του διακομιστή ιστού, μη ασφαλή διαμόρφωση διακομιστή κα.

Settings : Αυτή η οικογένεια πρόσθετων περιλαμβάνει ελέγχους για μη ασφαλείς ρυθμίσεις διαμόρφωσης στον διακομιστή. Αυτά θα μπορούσαν να περιλαμβάνουν ελέγχους για προεπιλεγμένα διαπιστευτήρια, μη ασφαλείς ρυθμίσεις SSL/TLS κα.

Περιληπτική Ανάλυση του Wordpress_Complete list of vulnerabilities by host :

Το pdf αρχείο με όνομα “Wordpress_Complete list of vulnerabilities by host” είναι μια αναφορά που δημιουργήθηκε από το Nessus, περιγράφοντας μια λίστα ευπαθειών που βρέθηκαν στον localhost WordPress. Η αναφορά έχει την εξής δομή:

Η πρώτη σελίδα είναι μια σελίδα εξωφύλλου με τον τίτλο και την ημερομηνία δημιουργίας της αναφοράς (Σελίδα 1).

Η δεύτερη σελίδα περιέχει έναν πίνακα περιεχομένων, υποδεικνύοντας ότι οι ευπάθειες για τον οικοδεσπότη 127.0.0.1 θα περιγραφούν από τη σελίδα 4 και μετά (Σελίδα 2).

Η τέταρτη και πέμπτη σελίδα παραθέτουν τις ευπάθειες που βρέθηκαν για τον οικοδεσπότη 127.0.0.1. Αυτές οι ευπάθειες κατηγοριοποιούνται ανάλογα με τη σοβαρότητα (Κρίσιμο, Υψηλό, Μέσο, Χαμηλό, Πληροφορίες) και περιλαμβάνουν λεπτομέρειες όπως η βαθμολογία CVSS V3.0, η βαθμολογία VPR, το plugin και το όνομα της ευπάθειας. Ορισμένα παραδείγματα ευπαθειών που αναφέρονται περιλαμβάνουν το "PHP 8.2.x < 8.2.7", το "OpenSSL 1.1.1 < 1.1.1v Vulnerability", το "Apache mod_info /server-info Information Disclosure" και το "WordPress User Enumeration" μεταξύ άλλων (Σελίδες 4-5). Η ολοκληρωμένη λίστα με τις ευπάθειες που βρέθηκαν έχουν καταγραφεί στο Παράρτημα 1.

Η αναφορά έχει την εξής δομή:

Το έγγραφο ξεκινά παρουσιάζοντας μια επισκόπηση των ευπαθειών που βρέθηκαν στον οικοδεσπότη 127.0.0.1. Καταγράφει συνολικά 33 ευπάθειες, κατηγοριοποιημένες ανά επίπεδα σοβαρότητας: Κρίσιμο, Υψηλό, Μεσαίο, Χαμηλό και Πληροφορίες. Το έγγραφο παρέχει επίσης πληροφορίες για την ώρα έναρξης και λήξης της σάρωσης και το λειτουργικό σύστημα του οικοδεσπότη.

Από τη σελίδα 5 και μετά, το έγγραφο παρέχει μια λεπτομερή ανάλυση κάθε ευπάθειας. Για παράδειγμα, στη σελίδα 5, συζητά μια ευπάθεια στο PHP 8.2.x < 8.2.7, η οποία θεωρείται υψηλής σοβαρότητας. Το έγγραφο παρέχει μια σύνοψη της ευπάθειας, μια λεπτομερή περιγραφή, μια λύση και τον παράγοντα κινδύνου. Παρέχει επίσης συνδέσμους για περαιτέρω

ανάγνωση και τις βαθμολογίες CVSS (Common Vulnerability Scoring System), που είναι ο κλάδος για την αξιολόγηση της σοβαρότητας των ευπαθειών ασφάλειας των υπολογιστικών συστημάτων.

Το έγγραφο συνεχίζει με αυτόν τον τρόπο, αναλύοντας ευπάθειες όπως Apache mod_info /server-info Information Disclosure, Apache mod_status /server-status Information Disclosure, Browsable Web Directories, HTTP TRACE / TRACK Methods Allowed, OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities, PHP expose_php Information Disclosure, και WordPress User Enumeration, μεταξύ άλλων. Για κάθε ευπάθεια, το έγγραφο παρέχει παρόμοιο επίπεδο λεπτομέρειας, συμπεριλαμβανομένης μιας σύνοψης, περιγραφής, λύσης, παράγοντα κινδύνου και βαθμολογιών CVSS.

Ανάλυση των κυριότερων ευπαθειών και προτεινόμενες λύσεις :

1. Ευπάθεια: PHP 8.2.x < 8.2.7

   Περιγραφή:
   Η ευπάθεια "PHP 8.2.x < 8.2.7" που εντοπίστηκε στον απομακρυσμένο διακομιστή ιστού αναφέρεται στην έκδοση της PHP που είναι εγκατεστημένη και είναι προγενέστερη της 8.2.7. Ως εκ τούτου, επηρεάζεται από μια ευπάθεια όπως αναφέρεται στη συμβουλευτική έκδοση 8.2.7 . Η ευπάθεια αυτή έχει ως αποτέλεσμα τη δυνατότητα εκμετάλλευσης από απομακρυσμένους επιτιθέμενους, που μπορεί να οδηγήσει σε απώλεια ευαίσθητων δεδομένων ή σε παραβιάσεις ασφαλείας. Η ευπάθεια αυτή έχει καταγραφεί ως CVE-2023-3247.

   Προτεινόμενη λύση :
   Η προτεινόμενη λύση για την αντιμετώπιση αυτής της ευπάθειας είναι η αναβάθμιση στην έκδοση PHP 8.2.7 ή νεότερη. Η αναβάθμιση σε μια νεότερη έκδοση της PHP θα διορθώσει την ευπάθεια και θα βελτιώσει την ασφάλεια του διακομιστή ιστού.

2. Ευπάθεια: 10678 - Apache mod_info /server-info Information Disclosure

   Περιγραφή:

   Ο απομακρυσμένος διακομιστής ιστού αποκαλύπτει πληροφορίες διαμόρφωσης. Ένας απομακρυσμένος επιτιθέμενος χωρίς πιστοποίηση μπορεί να λάβει μια επισκόπηση της διαμόρφωσης του απομακρυσμένου διακομιστή Apache αιτώντας το URL '/server-info'. Αυτή η επισκόπηση περιλαμβάνει πληροφορίες όπως εγκατεστημένα modules, τη διαμόρφωσή τους και διάφορες ρυθμίσεις εκτέλεσης.

   Προτεινόμενη λύση:

   Ενημερώστε τα αρχεία διαμόρφωσης του Apache για να απενεργοποιήσετε το mod_status ή να περιορίσετε την πρόσβαση σε συγκεκριμένους οικοδεσπότες.

3. Ευπάθεια "10677 - Apache mod_status /server-status Information Disclosure"

   Περιγραφή:

   Αναφέρεται στην πληροφορία που αποκαλύπτεται από τον απομακρυσμένο διακομιστή ιστού μέσω του mod_status του Apache. Ένας απομακρυσμένος επιτιθέμενος χωρίς πιστοποίηση μπορεί να λάβει μια επισκόπηση της δραστηριότητας και της απόδοσης του απομακρυσμένου διακομιστή Apache ιστού αιτώντας το URL '/server-status'. Αυτή η επισκόπηση περιλαμβάνει πληροφορίες όπως τρέχοντες οικοδεσπότες και αιτήσεις που επεξεργάζονται, τον αριθμό των εργατών που είναι αδρανείς και των αιτήσεων εξυπηρέτησης, καθώς και την χρήση της CPU .

   Προτεινόμενη λύση:

   Αντιμετώπιση αυτής της ευπάθειας είναι η ενημέρωση των αρχείων διαμόρφωσης του Apache για να απενεργοποιήσετε το mod_status ή να περιορίσετε την πρόσβαση σε συγκεκριμένους οικοδεσπότες.

4. Ευπάθεια "40984 - Browsable Web Directories" .

Περιγραφή:

Αναφέρεται στην δυνατότητα περιήγησης σε καταλόγους του απομακρυσμένου διακομιστή ιστού. Αυτό σημαίνει ότι οι επισκέπτες μπορούν να δουν τα περιεχόμενα των καταλόγων που δεν περιέχουν αρχείο index, το οποίο μπορεί να οδηγήσει στην αποκάλυψη ευαίσθητων πληροφοριών ή στην παροχή πρόσβασης σε ευαίσθητους πόρους.

Προτεινόμενη λύση:

Αντιμετώπιση αυτής της ευπάθειας είναι να βεβαιωθείτε ότι οι περιηγήσιμοι κατάλογοι δεν αποκαλύπτουν εμπιστευτικές πληροφορίες ή δεν παρέχουν πρόσβαση σε ευαίσθητους πόρους. Επιπλέον, χρησιμοποιήστε περιορισμούς πρόσβασης ή απενεργοποιήστε την ευρετηρίαση καταλόγων για οποιονδήποτε το κάνει .

5. Ευπάθεια "11213 - HTTP TRACE / TRACK Methods Allowed"

Περιγραφή:

Αναφέρεται στην ενεργοποίηση των μεθόδων ‘TRACE’ και ‘TRACK’ του ‘HTTP’ στον απομακρυσμένο διακομιστή ιστού. Αυτές οι μέθοδοι χρησιμοποιούνται για την αποσφαλμάτωση των συνδέσεων του διακομιστή ιστού .

Προτεινόμενη λύση:

Αντιμετώπιση αυτής της ευπάθειας είναι η απενεργοποίηση αυτών των μεθόδων HTTP. Μπορείτε να προσθέσετε τις παρακάτω γραμμές για κάθε εικονικό οικοδεσπότη στο αρχείο διαμόρφωσής σας: Εναλλακτικά, σημειώστε ότι οι εκδόσεις του Apache 1.3.34, 2.0.55, και 2.2 υποστηρίζουν την απενεργοποίηση της μεθόδου ‘TRACE’ μέσω της οδηγίας 'TraceEnable'

6. Ευπάθεια "173260 - OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities"

Περιγραφή:
Αναφέρεται στην έκδοση του OpenSSL που είναι εγκατεστημένη στον απομακρυσμένο διακομιστή ιστού και είναι προηγούμενη της 1.1.1u. Κατά συνέπεια, επηρεάζεται από πολλαπλές ευπάθειες όπως αναφέρονται στην συμβουλευτική 1.1.1u .

Προτεινόμενη λύση:
Η προτεινόμενη λύση για την αντιμετώπιση αυτής της ευπάθειας είναι η αναβάθμιση στην έκδοση 1.1.1u του OpenSSL ή σε μεταγενέστερη .

7. Ευπάθεια "178475 - OpenSSL 1.1.1 < 1.1.1v Vulnerability"

Περιγραφή :
Αναφέρεται στην έκδοση του OpenSSL που είναι εγκατεστημένη στον απομακρυσμένο διακομιστή ιστού και είναι προηγούμενη της 1.1.1v. Κατά συνέπεια, επηρεάζεται από μια ευπάθεια όπως αναφέρεται στην συμβουλευτική 1.1.1v .

Προτεινόμενη λύση:
Η προτεινόμενη λύση για την αντιμετώπιση αυτής της ευπάθειας είναι η αναβάθμιση στην έκδοση 1.1.1v του OpenSSL ή σε μεταγενέστερη .

8. Ευπάθεια "46803 - PHP expose_php Information Disclosure"

Περιγραφή :
Αναφέρεται στην διαμόρφωση της PHP στον απομακρυσμένο διακομιστή ιστού, η οποία επιτρέπει την αποκάλυψη ευαίσθητων πληροφοριών. Συγκεκριμένα, η εγκατάσταση της PHP είναι διαμορφωμένη με τέτοιο τρόπο ώστε να επιτρέπει την αποκάλυψη πιθανώς ευαίσθητων πληροφοριών σε έναν επιτιθέμενο μέσω ενός ειδικού URL. Τέτοιο URL ενεργοποιεί ένα "Easter egg" που είναι ενσωματωμένο στην ίδια την PHP.

Προτεινόμενη λύση:

Η προτεινόμενη λύση για την αντιμετώπιση αυτής της ευπάθειας είναι να αλλάξετε την τιμή της 'expose_php' σε 'Off' στο αρχείο διαμόρφωσης της PHP, το php.ini, για να απενεργοποιήσετε αυτή τη συμπεριφορά. Στη συνέχεια, πρέπει να επανεκκινήσετε τον δαίμονα του διακομιστή ιστού για να τεθεί σε ισχύ αυτή η αλλαγή .

9. Ευπάθεια "90067 - WordPress User Enumeration"

Περιγραφή :

Αναφέρεται στην δυνατότητα ενός μη εξουσιοδοτημένου, απομακρυσμένου επιτιθέμενου να εκμεταλλευτεί αυτή την ευπάθεια για να μάθει τα ονόματα των έγκυρων χρηστών του WordPress. Αυτές οι πληροφορίες θα μπορούσαν να χρησιμοποιηθούν για περαιτέρω επιθέσεις.

Προτεινόμενη λύση:

Στο έγγραφο δεν παρέχεται συγκεκριμένη λύση για την αντιμετώπιση αυτής της ευπάθειας. Ωστόσο, γενικά, η προστασία από την εξαγωγή χρηστών στο ‘WordPress’ μπορεί να επιτευχθεί με τη χρήση ενός ‘plugin’ ασφαλείας ή με την προσθήκη κώδικα στο αρχείο ‘functions.php’ του θέματος του ‘WordPress’ που εμποδίζει την εξαγωγή χρηστών.

10. Ευπάθεια "42057 - Web Server Allows Password Auto-Completion"

Περιγραφή :

Αναφέρεται στο γεγονός ότι ο απομακρυσμένος διακομιστής ιστού περιέχει τουλάχιστον ένα πεδίο φόρμας ‘HTML’ που έχει είσοδο τύπου 'password' όπου το 'autocomplete' δεν έχει οριστεί σε 'off'. Αυτό σημαίνει ότι οι χρήστες που χρησιμοποιούν τις επηρεαζόμενες φόρμες μπορεί να έχουν τα διαπιστευτήριά τους αποθηκευμένα στους browsers τους, το οποίο μπορεί να οδηγήσει σε απώλεια εμπιστευτικότητας εάν κάποιος από αυτούς χρησιμοποιεί έναν κοινόχρηστο υπολογιστή ή εάν παραβιαστεί ο λογαριασμός του.

Προτεινόμενη λύση:

Η προτεινόμενη λύση για την αντιμετώπιση αυτής της ευπάθειας είναι να προσθέσετε το χαρακτηριστικό 'autocomplete=off' σε αυτά τα πεδία για να αποτρέψετε τους browsers από την αποθήκευση διαπιστευτηρίων .

11. Ευπάθεια "26194 - Web Server Transmits Cleartext Credentials"

Περιγραφή :

Αναφέρεται στην περίπτωση όπου ο απομακρυσμένος διακομιστής ιστού περιέχει αρκετά πεδία φόρμας HTML που περιέχουν μια είσοδο τύπου 'password', τα οποία μεταδίδουν τις πληροφορίες τους σε έναν απομακρυσμένο διακομιστή ιστού σε απλό κείμενο. Ένας επιτιθέμενος που παρακολουθεί την κίνηση μεταξύ του προγράμματος περιήγησης ιστού και του διακομιστή μπορεί να λάβει τα ονόματα χρήστη και τους κωδικούς πρόσβασης των έγκυρων χρηστών .

Προτεινόμενη λύση:

Η προτεινόμενη λύση για την αντιμετώπιση αυτής της ευπάθειας είναι να διασφαλίσετε ότι κάθε ευαίσθητη φόρμα μεταδίδει περιεχόμενο μέσω HTTPS. Αυτό θα αποτρέψει την μετάδοση των διαπιστευτηρίων σε απλό κείμενο και θα προστατεύσει τις πληροφορίες των χρηστών από την παρακολούθηση από επιτιθέμενους .

Wireshark (WordPress Pen Tests)

Το Wireshark είναι ένα εργαλείο ανάλυσης πακέτων δικτύου που χρησιμοποιείται ευρέως στην κοινότητα της ασφάλειας πληροφορικής. Παρέχει τη δυνατότητα στους χρήστες να επιθεωρούν τα δεδομένα που περνούν μέσα από ένα δίκτυο σε μικροεπίπεδο, πράγμα που το καθιστά ιδιαίτερα χρήσιμο για την ανάλυση και την επίλυση προβλημάτων δικτύου, την ανάλυση πρωτοκόλλων και την πληροφόρηση της δικτυακής επικοινωνίας.

Στο πλαίσιο της δοκιμής διείσδυσης σε μια εφαρμογή ιστού, το Wireshark μπορεί να χρησιμοποιηθεί για την παρακολούθηση και την ανάλυση της δικτυακής επικοινωνίας που

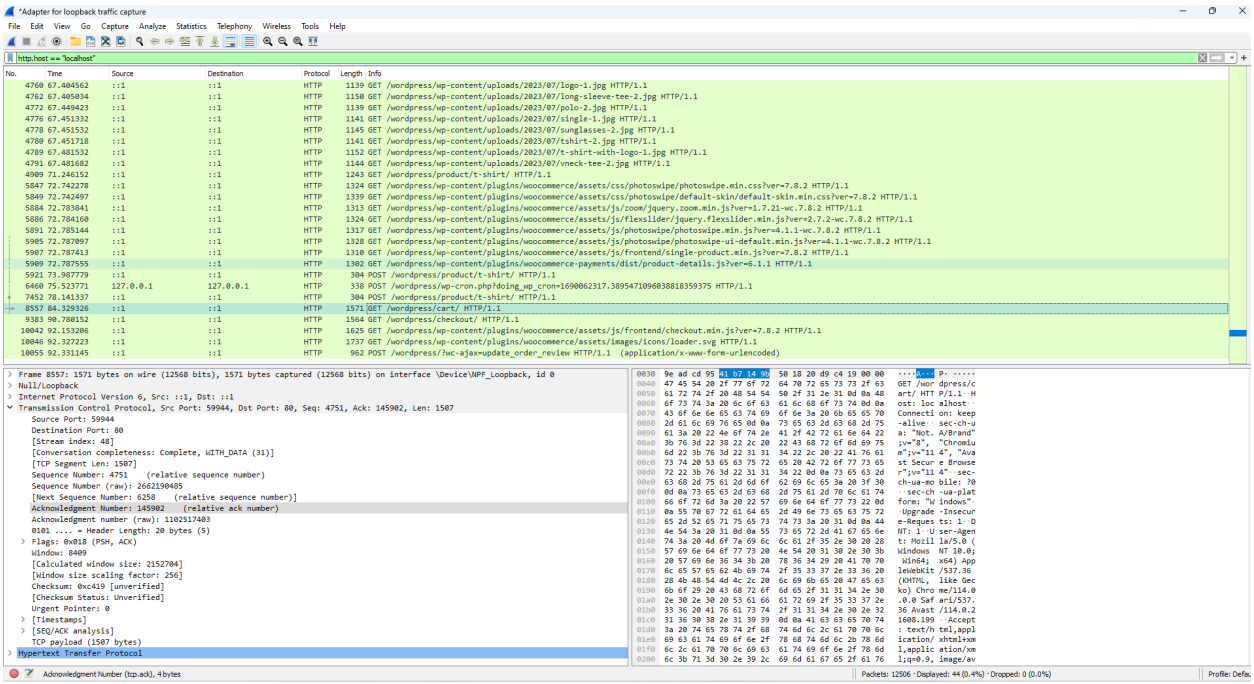
σχετίζεται με την εφαρμογή. Αυτό μπορεί να περιλαμβάνει την παρακολούθηση των ‘HTTP’ ή ‘HTTPS’ αιτήσεων και αποκρίσεων, την ανάλυση των δεδομένων που μεταδίδονται μεταξύ του πελάτη και του διακομιστή, και των εντοπισμό πιθανών ευπαθειών ή αδυναμιών στην επικοινωνία.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι το Wireshark είναι ένα εργαλείο ανάλυσης δικτύου και δεν παρέχει τη δυνατότητα εκτέλεσης επιθέσεων ή εκμετάλλευσης ευπαθειών. Ως εκ τούτου, ενώ μπορεί να είναι χρήσιμο για την κατανόηση της δικτυακής επικοινωνίας και των εντοπισμό πιθανών ευπαθειών, θα πρέπει να χρησιμοποιηθεί σε συνδυασμό με άλλα εργαλεία δοκιμής διείσδυσης για πιο ολοκληρωμένα αποτελέσματα.

Εγκατάσταση και ρύθμιση του Wireshark

Από την σελίδα της εφαρμογής “https://www.wireshark.org/download.html” επιλέχθηκε προς download η σχετική έκδοση για ‘Windows x64’. Μετά την εγκατάσταση, στην αρχική οθόνη του ‘Wireshark’ επιλέχθηκε το ‘Adapter for loopback traffic capture’ και στο πάνω μέρος της εφαρμογής ‘*http and tcp.port == 80’* ως ‘display filter’. Έτσι επιτυγχάνεται το ‘network monitoring’ της σελίδας wordpress στον localhost . Τα reports εμφανίζονται συνεχώς όσο μέσα στην σελίδα υπάρχει κάποια κινητικότητα.

Η εικόνα περιέχει μια ανάλυση καταγραφής πακέτων Wireshark.



Εικόνα 8:Ανίχνευση Δικτυακών Πακέτων σε Πραγματικό Χρόνο με το Εργαλείο Ανάλυσης Wireshark

<u>Ακολουθεί μια ανάλυση των πληροφοριών που εξήχθησαν:</u>

- Η καταγραφή έγινε στη διεπαφή loopback, η οποία χρησιμοποιείται για την τοπική κίνηση στη μηχανή.

- Το εφαρμοσμένο φίλτρο ήταν για επίβλεψη του στόχου ο οποίος είναι ο localhost.

- Η καταγραφή δείχνει αιτήσεις HTTP που έγιναν στον ιστότοπο “WordPress”. Οι αιτήσεις είναι για διάφορους πόρους όπως εικόνες (π.χ., `logo-1.jpg`, `long-sleeve-tee-2.jpg`, `polo-2.jpg`, κλπ.), σελίδες προϊόντων (π.χ. `/wordpress/product/t-shirt/`), και διάφορα αρχεία CSS, JS σχετικά με το πρόσθετο WooCommerce (π.χ., `photoswipe.min.css`, `jquery.zoom.min.js`, `photoswipe-ui-default.min.js`, κλπ.).

- Υπάρχουν επίσης αιτήσεις POST προς το `/wordpress/product/t-shirt/` και το `/wordpress/wp-cron.php`.

- Η συμβολοσειρά του χρήστη στις κεφαλίδες HTTP υποδηλώνει ότι οι αιτήσεις έγιναν από ένα σύστημα Windows 10 χρησιμοποιώντας Chrome/114.0.608.199 και Avast/114.0.608.199.

- Η καταγραφή δείχνει επίσης λεπτομέρειες TCP όπως τις πηγαίες και προοριστικές θύρες, τους αριθμούς ακολουθίας, τους αριθμούς επιβεβαίωσης και flags.

Αναλυτικότερα :

Τα δεδομένα που παρείχε το WordPress είναι καταγραφές πακέτων HTTP που εξήχθησαν από το Wireshark. Ακολουθεί μια απλοποιημένη ερμηνεία του τι αντιπροσωπεύουν αυτά τα δεδομένα:

Frame 641 - Έγινε ένα αίτημα HTTP GET IPv6 στο endpoint `/wordpress/my-account/` στην ίδια μηχανή (Πηγή και Προορισμός είναι ::1, που είναι η διεύθυνση IPv6 για το localhost). Το αίτημα στάλθηκε από τη θύρα 59908 στη θύρα 80.

Frame 1084 - Έγινε ένα αίτημα HTTP POST IPv4 στο `/wordpress/wp-cron.php` στην ίδια μηχανή (Πηγή και Προορισμός είναι 127.0.0.1, που είναι η διεύθυνση IPv4 για το localhost). Το αίτημα στάλθηκε από τη θύρα 59911 στη θύρα 80.

Frame 2122 - Έγινε άλλο ένα αίτημα HTTP GET IPv6 στο endpoint `/wordpress/my-account/` στην ίδια μηχανή, παρόμοιο με το Καρέ 641 αλλά σε μεταγενέστερη χρονική στιγμή.

Frame 2736 - Έγινε ένα αίτημα HTTP GET IPv6 στο endpoint `/wordpress/checkout/` στην ίδια μηχανή.

Frame 3177 - Έγινε ένα αίτημα HTTP GET IPv6 στο endpoint `/wordpress/cart/` στην ίδια μηχανή.

Τα πακέτα είναι μέρος μιας αλληλεπίδρασης με τον ιστότοπο WordPress που λειτουργεί τοπικά στη μηχανή όπου πραγματοποιήθηκε η καταγραφή. Είναι η δραστηριότητα ενός διαχειριστή που πλοηγείται σε διάφορες περιοχές του ιστότοπου (Ο Λογαριασμός Μου, Αγορά, Καλάθι) και το WordPress εκτελεί κάποιες εργασίες στο παρασκήνιο (wp-cron.php).

Όλα αυτά τα πακέτα είναι πακέτα loopback (όπως υποδεικνύεται από το πρωτόκολλο "Null/Loopback"), που σημαίνει ότι στάλθηκαν από την τοπική μηχανή στον εαυτό της. Αυτό

είναι σύνηθες όταν δοκιμάζονται εφαρμογές τοπικά ή τρέχουν εφαρμογές διακομιστή που επικοινωνούν εσωτερικά.

Η θύρα 80 είναι η προεπιλεγμένη θύρα για την επικοινωνία HTTP. Η "Πηγαία Θύρα" είναι μια τυχαία εκχωρημένη θύρα που χρησιμοποιείται από την εφαρμογή-πελάτη για να λαμβάνει δεδομένα από τον διακομιστή.

Frame 3802 - Έγινε ένα αίτημα HTTP GET IPv6 για να ανακτηθεί το αρχείο JavaScript `country-select.min.js` από το πρόσθετο WooCommerce του ιστοτόπου WordPress. Το αίτημα στάλθηκε από τη θύρα 59908 στη θύρα 80.

Frame 3812 - Έγινε ένα αίτημα HTTP GET IPv6 για να ανακτηθεί άλλο ένα αρχείο JavaScript `address-i18n.min.js` από το πρόσθετο WooCommerce. Αυτό το αίτημα στάλθηκε από μια διαφορετική πηγαία θύρα (59927) αλλά κατευθυνόταν πάντα στη θύρα 80.

Frame 3814 - Έγινε ένα αίτημα HTTP GET IPv6 για να ανακτηθεί το αρχείο JavaScript `cart.min.js` από το πρόσθετο WooCommerce. Αυτό το αίτημα στάλθηκε από μια άλλη μοναδική πηγαία θύρα (59928) στη θύρα 80.

Frame 3824 - Έγινε ένα αίτημα HTTP GET IPv6 στο endpoint `/wordpress/shop/` του τοπικού ιστοτόπου WordPress. Αυτό το αίτημα στάλθηκε από την προηγούμενη πηγαία θύρα (59908) στη θύρα 80.

Frame 4675 - Έγινε ένα αίτημα HTTP GET IPv6 για να ανακτηθεί ένα αρχείο CSS `wc-blocks-vendors-style.css` από το πρόσθετο WooCommerce. Αυτό το αίτημα στάλθηκε από την πηγαία θύρα 59928 στη θύρα 80.

Όλα αυτά τα πακέτα είναι και πάλι πακέτα loopback (η πηγή και ο προορισμός είναι οι ίδιοι, δηλαδή ::1 που είναι το localhost για το IPv6). Αυτά τα πακέτα αντιπροσωπεύουν τον περιηγητή ιστού που κάνει αιτήσεις στον τοπικό διακομιστή που φιλοξενεί τον ιστότοπο WordPress. Οι διάφορες θύρες (59908, 59927, 59928) από τις οποίες στέλνονται τα αιτήματα αντιπροσωπεύουν συνήθως διάφορα νήματα ή διεργασίες στον περιηγητή ιστού. Επιτρέπουν στον περιηγητή να κάνει και να διαχειρίζεται πολλαπλά ταυτόχρονα αιτήματα στον διακομιστή.

Το WooCommerce όπως αναφέρθηκε είναι ένα δημοφιλές πρόσθετο για το WordPress που προσθέτει λειτουργίες ηλεκτρονικού εμπορίου στον ιστότοπο, επιτρέποντας στον ιστότοπο να

λειτουργεί ως ένα ηλεκτρονικό κατάστημα. Τα αιτήματα προς τα σενάρια WooCommerce υποδηλώνουν ότι ο χρήστης αλληλεπιδρά με το μέρος του ιστοτόπου που είναι το ηλεκτρονικό κατάστημα, είτε στο πλαίσιο της ρύθμισής του είτε κάνοντας συναλλαγές.

Περισσότερα αιτήματα HTTP GET για πόρους από έναν τοπικό διακομιστή WordPress, όλα μέσω Ipv6:

Frame 4677 - Ένα αίτημα GET στέλνεται για το αρχείο `wc-blocks-style.css` από το πρόσθετο WooCommerce, που χρησιμοποιείται για το στυλιστικό μέρος των λειτουργιών ηλεκτρονικού εμπορίου του ιστοτόπου WordPress. Η πηγαία θύρα είναι 59927 και η θύρα προορισμού είναι 80.

Frame 4718 - Ένα αίτημα GET στέλνεται για ένα αρχείο εικόνας `album-1.jpg` από τον κατάλογο `uploads` του διακομιστή WordPress. Αυτό υποδηλώνει ότι ο διακομιστής παρέχει μια ιστοσελίδα που περιλαμβάνει αυτήν την εικόνα. Η πηγαία θύρα είναι 59908 και η θύρα προορισμού είναι 80.

Frame 4720 - Ένα αίτημα GET στέλνεται για άλλη μια εικόνα `beanie-2.jpg` από τον ίδιο κατάλογο `uploads`. Αυτό υποδηλώνει ότι ο διακομιστής παρέχει μια άλλη ιστοσελίδα που περιλαμβάνει αυτήν την εικόνα ή την ίδια σελίδα με πολλαπλές εικόνες. Η πηγαία θύρα είναι 59927 και η θύρα προορισμού είναι 80.

Frame 4722 - Ένα αίτημα GET στέλνεται για μια τρίτη εικόνα `beanie-with-logo-1.jpg` από τον κατάλογο `uploads`. Αυτό θα μπορούσε να είναι η ίδια ιστοσελίδα ή μια διαφορετική που περιλαμβάνει αυτήν την εικόνα. Η πηγαία θύρα είναι 59928 και η θύρα προορισμού είναι 80.

Τα διάφορα αιτήματα για εικόνες υποδηλώνουν ότι ο χρήστης αλληλεπιδρά με ένα μέρος του ιστοτόπου που εμφανίζει εικόνες, σελίδες προϊόντων και μια γκαλερί. Οι διάφορες πηγαίες θύρες θα μπορούσαν να αντιπροσωπεύουν διάφορα νήματα ή διεργασίες από τον περιηγητή ιστού ή τον διακομιστή, επιτρέποντας πολλαπλά ταυτόχρονα αιτήματα.

Επιπλέον αιτήματα HTTP GET για πόρους από έναν τοπικό διακομιστή WordPress, όλα μέσω Ipv6:

Frame 4728 - Έγινε ένα αίτημα GET για ένα αρχείο εικόνας `belt-2.jpg` από τον κατάλογο `uploads` του διακομιστή WordPress. Αυτό υποδηλώνει ότι ο διακομιστής παρέχει μια

ιστοσελίδα που περιλαμβάνει αυτήν την εικόνα. Η πηγαία θύρα είναι 59934 και η θύρα προορισμού είναι 80.

Frame 4739 - Έγινε ένα αίτημα GET για άλλη μια εικόνα `cap-2.jpg` από τον ίδιο κατάλογο `uploads`. Αυτό υποδηλώνει ότι ο διακομιστής παρέχει μια ιστοσελίδα που περιλαμβάνει αυτήν την εικόνα. Η πηγαία θύρα είναι 59935 και η θύρα προορισμού είναι 80.

Frame 4746 - Έγινε ένα αίτημα GET για μια τρίτη εικόνα `hoodie-2.jpg` από τον κατάλογο `uploads`. Αυτό είναι η ίδια ιστοσελίδα ή μια διαφορετική που περιλαμβάνει αυτήν την εικόνα. Η πηγαία θύρα είναι 59936 και η θύρα προορισμού είναι 80.

Frame 4752 - Έγινε ένα αίτημα GET για μια εικόνα `hoodie-with-logo-2.jpg` από τον κατάλογο `uploads`. Πάλι, αυτό είναι πιθανότατα μια εικόνα προϊόντος σε μια ιστοσελίδα. Η πηγαία θύρα είναι 59935 και η θύρα προορισμού είναι 80.

Frame 4754 - Έγινε ένα αίτημα GET για άλλη μια εικόνα `hoodie-with-zipper-2.jpg` από τον κατάλογο `uploads`. Αυτό υποδηλώνει ότι ο διακομιστής παρέχει μια ιστοσελίδα που περιλαμβάνει αυτήν την εικόνα. Η πηγαία θύρα είναι 59934 και η θύρα προορισμού είναι 80.

Από την ανάλυση των παρεχόμενων πληροφοριών, μπορούμε να καταλήξουμε στα εξής συμπεράσματα:

1. Οι πληροφορίες προέρχονται από την καταγραφή της δικτυακής κίνησης μιας τοπικής εγκατάστασης του WordPress, χρησιμοποιώντας το πρόγραμμα ανάλυσης πακέτων δικτύου Wireshark.

2. Η κίνηση που καταγράφηκε είναι αποκλειστικά τοπική (loopback), πράγμα που σημαίνει ότι οι αιτήσεις HTTP προέρχονται από και προορίζονται για την ίδια μηχανή.

3. Οι αιτήσεις HTTP που καταγράφηκαν περιλαμβάνουν αιτήσεις για διάφορους πόρους, όπως εικόνες, σελίδες προϊόντων, και αρχεία CSS και JavaScript, που σχετίζονται με το WordPress και το πρόσθετο WooCommerce.

4. Υπάρχουν επίσης αιτήσεις POST προς το `/wordpress/product/t-shirt/` και το `/wordpress/wp-cron.php`, που υποδηλώνουν δραστηριότητα του διαχειριστή και εργασίες στο παρασκήνιο αντίστοιχα.

5. Η συμβολοσειρά του χρήστη στις κεφαλίδες HTTP υποδηλώνει ότι οι αιτήσεις έγιναν από ένα σύστημα Windows 10 χρησιμοποιώντας Chrome/114.0.608.199 και Avast/114.0.608.199.

6. Η καταγραφή παρέχει επίσης λεπτομέρειες TCP, όπως τις πηγαίες και προοριστικές θύρες, τους αριθμούς ακολουθίας, τους αριθμούς επιβεβαίωσης και flags.

7. Η κίνηση που καταγράφηκε αντιπροσωπεύει την αλληλεπίδραση ενός διαχειριστή με τον ιστότοπο WordPress, περιλαμβάνοντας την πλοήγηση σε διάφορες περιοχές του ιστοτόπου και την εκτέλεση εργασιών στο παρασκήνιο.

8. Τα αιτήματα προς τα σενάρια WooCommerce υποδηλώνουν ότι ο χρήστης αλληλεπιδρά με το μέρος του ιστοτόπου που είναι το ηλεκτρονικό κατάστημα, είτε στο πλαίσιο της ρύθμισής του είτε κάνοντας συναλλαγές.

9. Τα αιτήματα για εικόνες υποδηλώνουν ότι ο χρήστης αλληλεπιδρά με ένα μέρος του ιστοτόπου που εμφανίζει εικόνες, σελίδες προϊόντων και μια γκαλερί.

Nmap / Zenmap

Το Zenmap είναι ένα γραφικό περιβάλλον χρήστη (GUI) για το Nmap, ένα δωρεάν και ανοιχτού κώδικα πρόγραμμα σάρωσης δικτύου σχεδιασμένο για την ανακάλυψη hosts και υπηρεσιών σε ένα δίκτυο. Χρησιμοποιείται για την ανακάλυψη συσκευών που λειτουργούν σε ένα δίκτυο και για την ανίχνευση των ανοιχτών θυρών σε συγκεκριμένες συσκευές. Με αυτό τον τρόπο, το Nmap παρέχει πληροφορίες για τις υπηρεσίες που τρέχουν σε ένα δίκτυο, τις θύρες που είναι ανοιχτές και άλλες χρήσιμες πληροφορίες ασφάλειας.

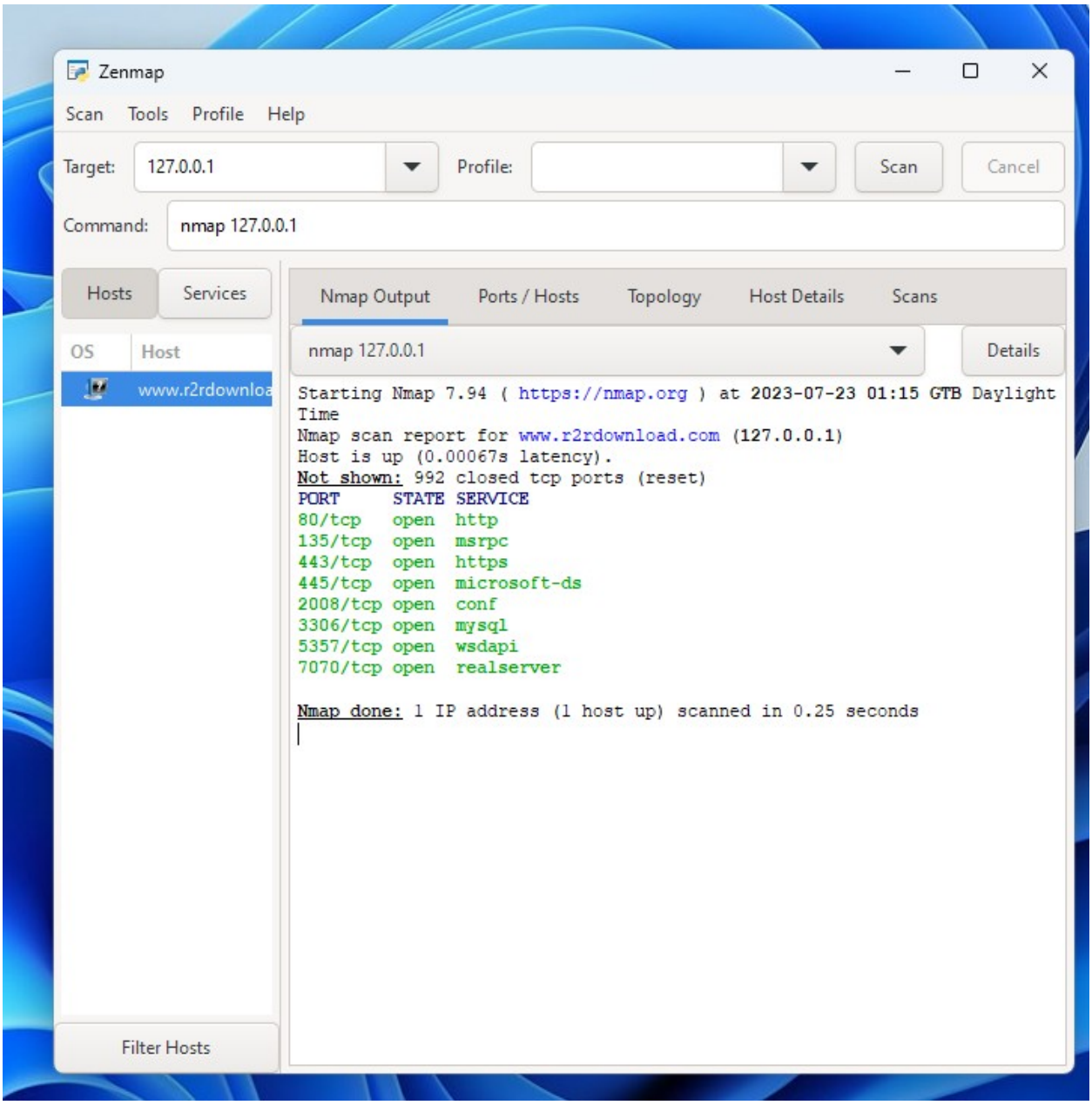
Εγκατάσταση και ρύθμιση του Zenmap

Το download της εφαρμογής έγινε από τον ιστότοπο της εφαρμογής https://nmap.org/zenmap/

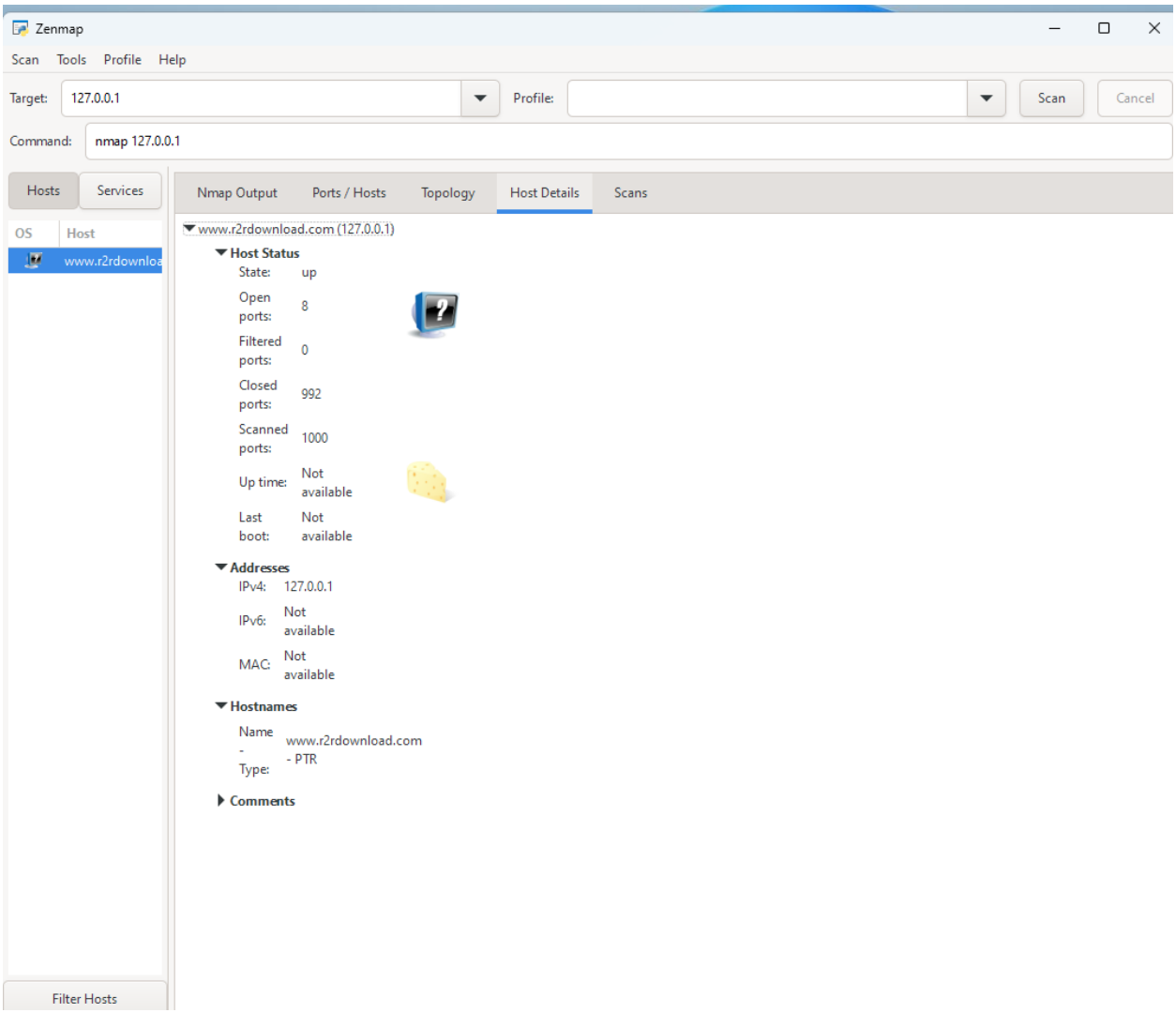
Στην συνέχεια μετά το άνοιγμα της εφαρμογής ως target τέθηκε το 127.0.0.1 .

Basic port scanning εντολή

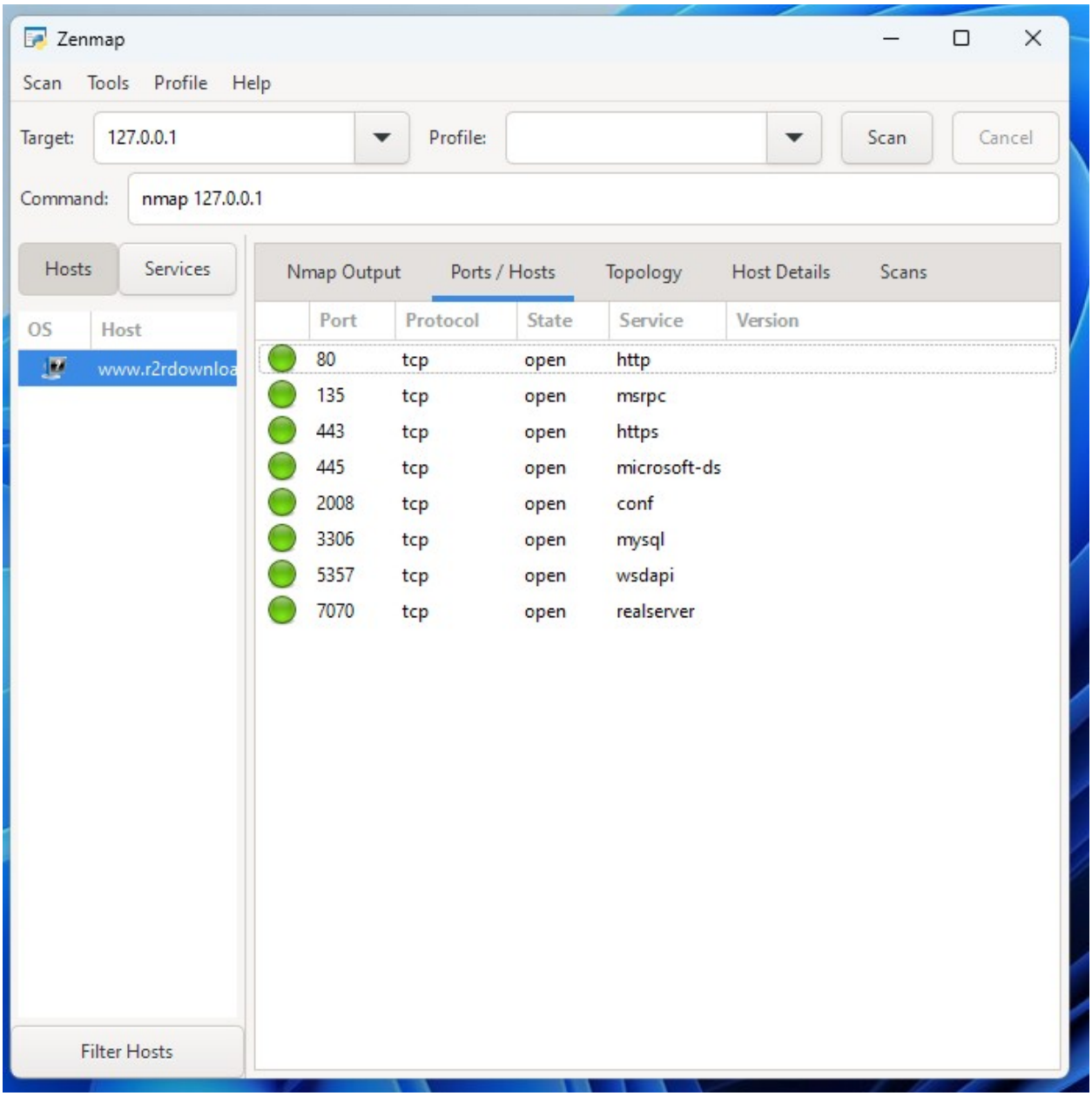
Nmap 127.0.0.1



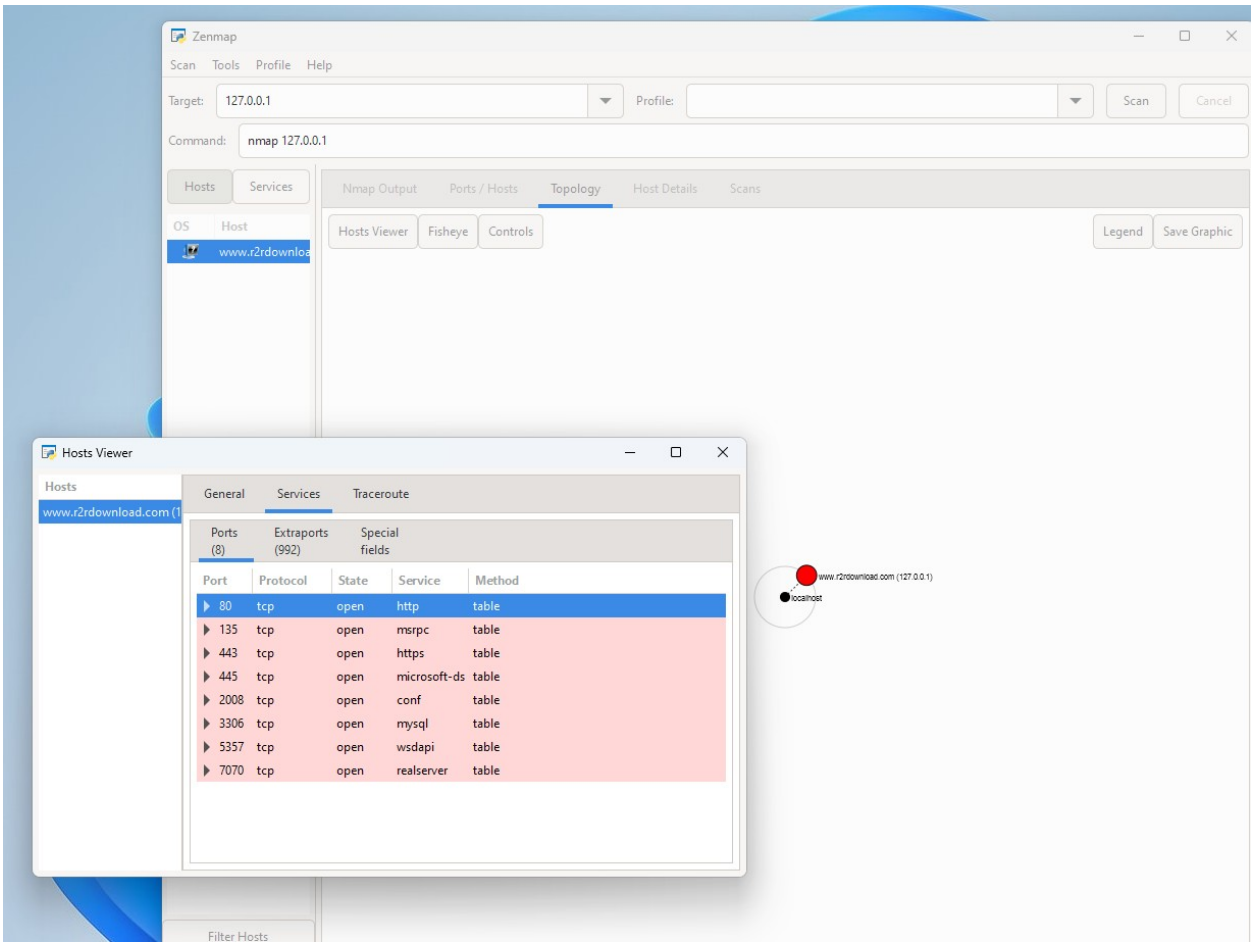
Εικόνα 9: Διαγνωστική Σάρωση Πρωτοκόλλων και Εντοπισμός Ανοικτών Θυρών Στο Δίκτυο με Χρήση Zenmap



Εικόνα 10:Αποτελέσματα Ανάλυσης Δικτύου σε localhost Με Zenmap



Εικόνα 11: Συνοπτική Επισκόπηση Πρωτοκόλλων Και Θυρών σε Χρήση με Zenmap



Εικόνα 12:Καταγραφή Θυρών και Πρωτοκόλλων σε Λειτουργία - Σάρωση Zenmap

Το scan έδειξε τις παρακάτω θύρες ανοιχτές, γεγονός το οποίο ενδεχομένως να αποτελεί κίνδυνο.

- Port 80/tcp

- Port 445/tcp

- Port 135/tcp

- Port 443/tcp

- Port 3306/tcp

- Port 2008/tcp

- Port 5357/tcp

- Port 7070/tcp

Τα services που σχετίζονται με αυτές τις θύρες ειναι:

- Port 80: HTTP (Web server)

- Port 445: Microsoft-DS (Windows shares)

- Port 135: RPC (Remote Procedure Call)

- Port 443: HTTPS (Secure Web server)

- Port 3306: MySQL (Database server)

- Port 2008: Unknown

- Port 5357: WSDAPI (Web Services on Devices)

- Port 7070: Unknown

The report επίσης αναφέρει ότι το scan πραγματοποιήθηκε σε 0.49 δευτερόλεπτα , με 1000 raw packets σταλμένα (44.000KB) and 2008 ληφθέντα (84.352KB).

1. Θύρα 80/tcp (HTTP): Αυτή η θύρα χρησιμοποιείται συνήθως για μη κρυπτογραφημένη επικοινωνία ιστού. Εάν ένας διακομιστής ιστού λειτουργεί σε αυτή τη θύρα, θα μπορούσε να είναι ευάλωτος σε διάφορες επιθέσεις, όπως SQL Injection, Cross-Site Scripting (XSS), ή Cross-Site Request Forgery (CSRF), μεταξύ άλλων. Οι συγκεκριμένες ευπάθειες θα εξαρτώνταν από την εφαρμογή ιστού που λειτουργεί σε αυτή τη θύρα.

2. Θύρα 445/tcp (Microsoft-DS): Αυτή η θύρα χρησιμοποιείται για τις κοινές προσβάσεις Windows. Είναι γνωστό ότι είναι ευάλωτη σε διάφορες επιθέσεις εάν δεν έχει ασφαλιστεί σωστά, όπως η διάσημη επίθεση ransomware WannaCry που εκμεταλλεύτηκε το πρωτόκολλο SMB σε αυτή τη θύρα.

3. Θύρα 135/tcp (RPC): Αυτή η θύρα χρησιμοποιείται από τη Microsoft για το πρωτόκολλο Remote Procedure Call (RPC), το οποίο μπορεί να εκμεταλλευτεί εάν δεν έχει ασφαλιστεί σωστά. Για παράδειγμα, θα μπορούσε να είναι ευάλωτο στην ευπάθεια "Unquoted Service Path".

4. Θύρα 443/tcp (HTTPS): Αυτή η θύρα χρησιμοποιείται για κρυπτογραφημένη επικοινωνία ιστού. Όπως και στη θύρα 80, οι συγκεκριμένες ευπάθειες θα εξαρτώνταν από την εφαρμογή ιστού που λειτουργεί σε αυτή τη θύρα. Επιπλέον, εάν η διαμόρφωση SSL/TLS δεν είναι ασφαλής, θα μπορούσε να είναι ευάλωτη σε επιθέσεις όπως το POODLE ή το Heartbleed.

5. Θύρα 3306/tcp (MySQL): Αυτή η θύρα χρησιμοποιείται για τις βάσεις δεδομένων MySQL. Εάν η βάση δεδομένων δεν έχει ασφαλιστεί σωστά, θα μπορούσε να είναι ευάλωτη σε επιθέσεις όπως SQL Injection ή ανεπιθύμητη πρόσβαση.

6. Θύρα 2008/tcp: Αυτή η θύρα δεν σχετίζεται με μια γνωστή υπηρεσία και θα μπορούσε να χρησιμοποιηθεί για διάφορους σκοπούς. Θα χρειαζόταν να εντοπιστεί η συγκεκριμένη υπηρεσία που λειτουργεί σε αυτή τη θύρα για να αξιολογηθούν οι ευπάθειές της.

7. Θύρα 5357/tcp (WSDAPI): Αυτή η θύρα χρησιμοποιείται από τα Windows για τις Υπηρεσίες στις Συσκευές μέσω Ιστού. Εάν δεν έχει ασφαλιστεί σωστά, θα μπορούσε να εκμεταλλευτεί.

8. Θύρα 7070/tcp: Όπως και η θύρα 2008, αυτή η θύρα δεν σχετίζεται με μια γνωστή υπηρεσία. Θα χρειαζόταν να εντοπιστεί η συγκεκριμένη υπηρεσία που λειτουργεί σε αυτή τη θύρα για να αξιολογηθούν οι ευπάθειές της.

WPScan (WordPress Pen Tests)

Το WPScan είναι ένα ελεύθερο και ανοιχτού κώδικα εργαλείο που χρησιμοποιείται για την ανίχνευση ευπαθειών σε ιστοσελίδες που χρησιμοποιούν το WordPress. Αναπτύχθηκε με την πρόθεση να βοηθήσει τους επαγγελματίες της ασφάλειας των πληροφοριακών συστημάτων και τους διαχειριστές ιστοσελίδων να εντοπίζουν και να διορθώνουν ευπάθειες στις ιστοσελίδες τους.

Το WPScan είναι ιδιαίτερα χρήσιμο για το penetration testing, καθώς παρέχει μια ευρεία γκάμα λειτουργιών που μπορούν να βοηθήσουν στην ανίχνευση και την εκμετάλλευση ευπαθειών. Μερικές από αυτές τις λειτουργίες περιλαμβάνουν την ανίχνευση αδύναμων κωδικών

πρόσβασης, την αναζήτηση για ενημερώσεις που δεν έχουν εφαρμοστεί, την αναγνώριση εγκατεστημένων πρόσθετων και θεμάτων που μπορεί να περιέχουν ευπάθειες, και την αναζήτηση για διάφορες ευπάθειες που είναι γνωστές στην κοινότητα της ασφάλειας.

Επιπλέον, το WPScan μπορεί να αυτοματοποιήσει τη διαδικασία της ανίχνευσης ευπαθειών, επιτρέποντας στους επαγγελματίες της ασφάλειας να εξοικονομήσουν χρόνο και πόρους. Αυτό το καθιστά ένα πολύτιμο εργαλείο για την προετοιμασία και την εκτέλεση penetration testing, καθώς μπορεί να βοηθήσει στην ανακάλυψη και την εκμετάλλευση ευπαθειών πριν αυτές εκμεταλλευτούν από κακόβουλους χρήστες.

Εγκατάσταση WPScan σε λειτουργικό σύστημα Kali Linux

Για να χρησιμοποιήσετε το WPScan στο Kali Linux, θα πρέπει πρώτα να το εγκαταστήσετε, εάν δεν έχει ήδη εγκατασταθεί. Το Kali Linux συνήθως περιλαμβάνει το WPScan στην προεπιλεγμένη εγκατάσταση, αλλά εάν χρειάζεται να το εγκαταστήσετε, μπορείτε να το κάνετε με την εντολή `sudo apt-get install wpscan` σε χρήση γραμμή εντολής τερματικού, σε linux περιβάλλον.

Αφού εγκαταστήσετε το WPScan, μπορείτε να το χρησιμοποιήσετε για να σαρώσετε μια ιστοσελίδα για ευπάθειες. Ακολουθούν παραδείγματα χρήσης:

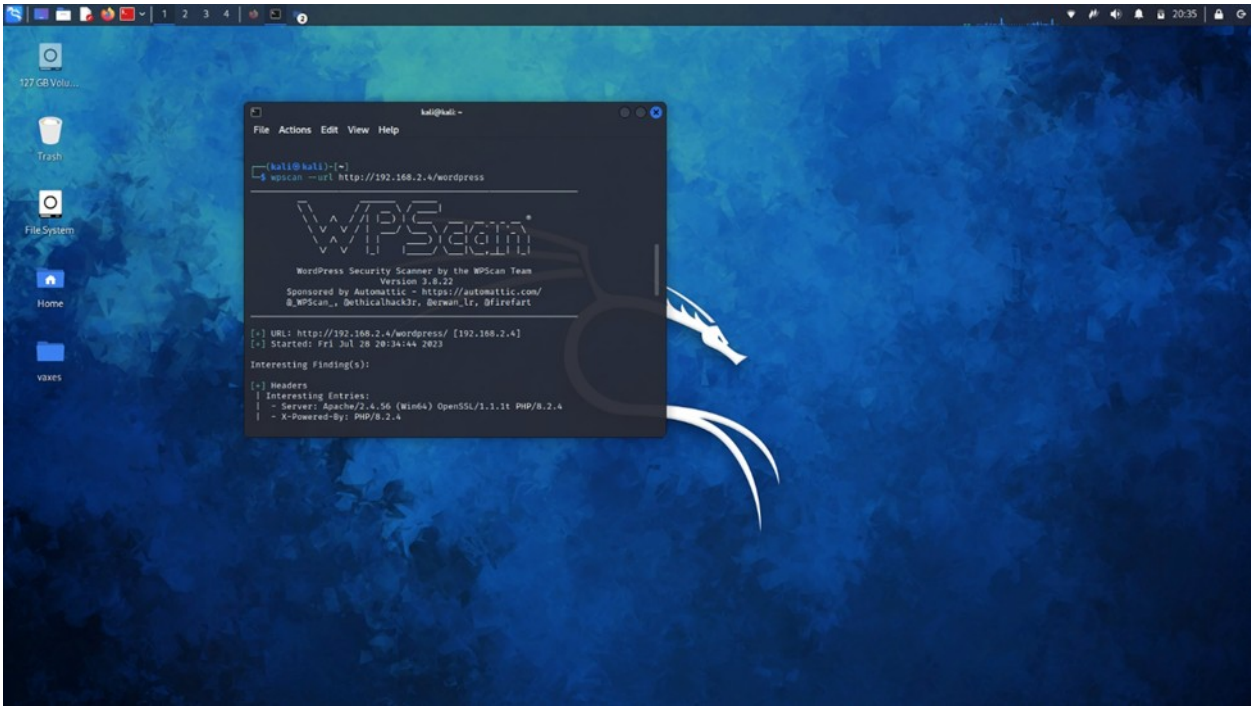
1. Ανοίξτε ένα τερματικό και πληκτρολογήστε την εντολή `wpscan --url yourwebsite.com`, αντικαθιστώντας το "yourwebsite.com" με τη διεύθυνση της ιστοσελίδας που θέλετε να σαρώσετε.

2. Αν θέλετε να σαρώσετε για ευπάθειες σε πρόσθετα, μπορείτε να προσθέσετε την επιλογή `--enumerate vp`.

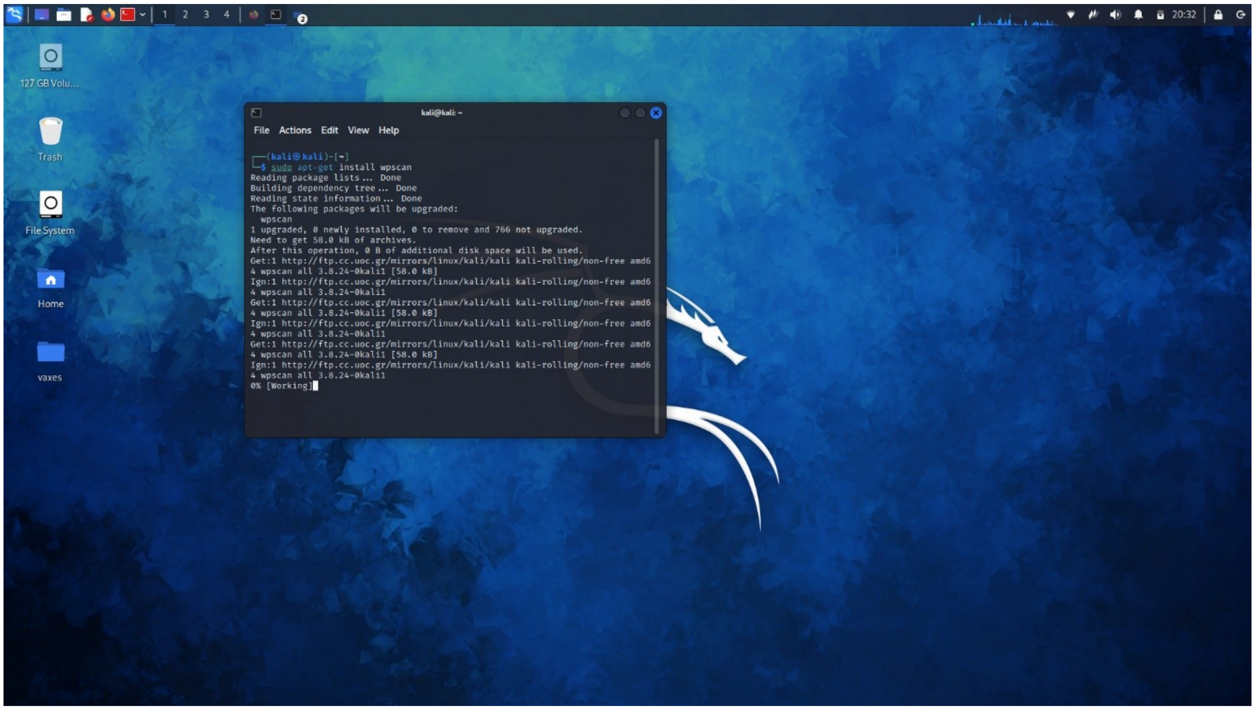
3. Αν θέλετε να σαρώσετε για ευπαθειές σε θέματα, μπορείτε να προσθέσετε την επιλογή `--enumerate vt`.

4. Αν θέλετε να σαρώσετε για αδύναμους κωδικούς πρόσβασης, μπορείτε να προσθέσετε την επιλογή `--passwords wordlist.txt`, αντικαθιστώντας το "wordlist.txt" με τη διαδρομή προς τη λίστα κωδικών πρόσβασης που θέλετε να χρησιμοποιήσετε.

Στην συνέχεια παρουσιάζεται η εγκατάσταση του WPScan μέσω του terminal στο Kali Linux.



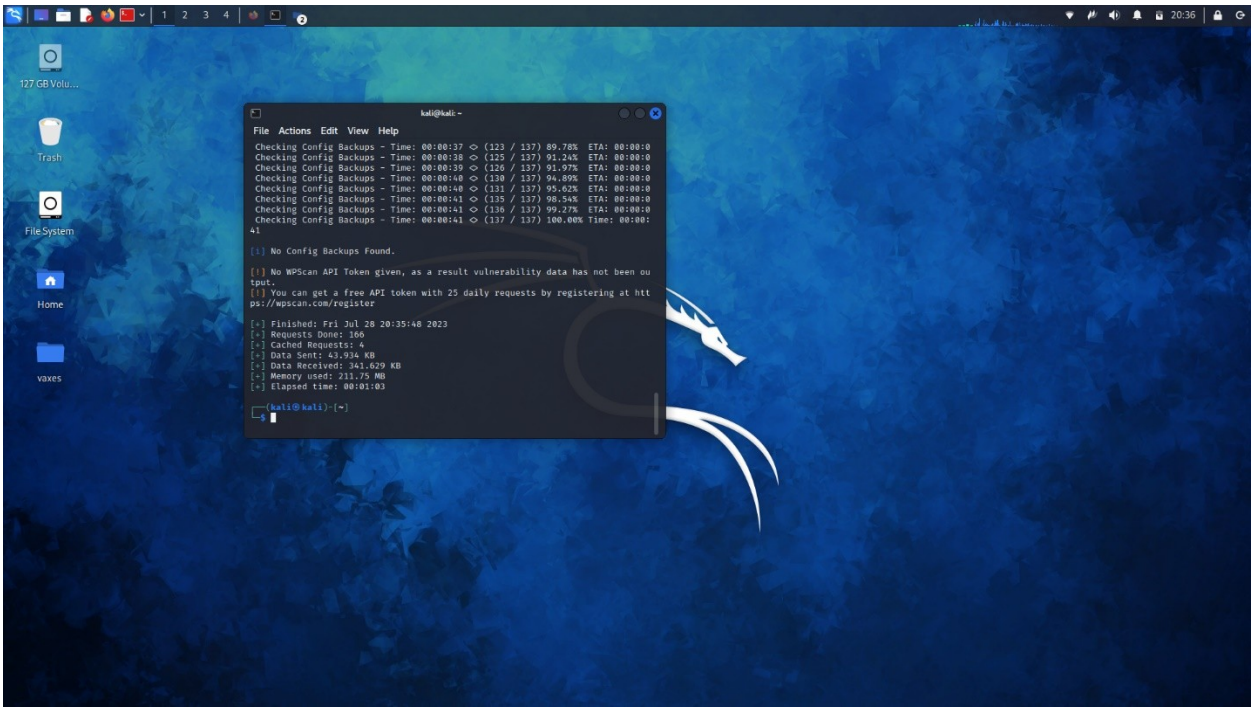
Εικόνα 13:Εκκίνηση WPScan για Ελέγχους Ασφάλειας σε WordPress



Εικόνα 14:Σάρωση Ιστοσελίδας WordPress με WPScan για Εντοπισμό Ευπαθειών

Ακολουθεί η εκτέλεση της βασικής σάρωσης του Wordpress προς εύρεση πιθανών ευπαθειών με την εντολη ‘wpscan --url http://192.168.2.4/wordpress’

Εικόνα 15:Σάρωση Ιστοσελίδας WordPress με WPScan για Εντοπισμό Ευπαθειών



Εικόνα 16:Αποτελέσματα WPScan-Καταγραφή Δικτυακής Δραστηριότητας WordPress

<u>Ανάλυση και επεξήγηση των πιο κρίσιμων σημείων της αναφοράς του WPScan :</u>

1. Επικεφαλίδες (Headers): Πρόκειται για τις επικεφαλίδες HTTP που ο διακομιστής στέλνει πίσω με τις απαντήσεις του. Μπορούν να παρέχουν πληροφορίες σχετικά με το λογισμικό και τη διαμόρφωση του διακομιστή. Σε αυτήν την περίπτωση, ο διακομιστής εκτελεί την έκδοση Apache 2.4.56 σε ένα σύστημα Windows 64-bit, με την έκδοση OpenSSL 1.1.1t για υποστήριξη SSL/TLS και την έκδοση PHP 8.2.4 για την επεξεργασία σεναρίων PHP.

2. XML-RPC: Το XML-RPC είναι ένα πρωτόκολλο που επιτρέπει τις απομακρυσμένες κλήσεις διαδικασιών μέσω HTTP. Χρησιμοποιείται από ορισμένες λειτουργίες του WordPress, όπως τα pingbacks και τα trackbacks, αλλά μπορεί επίσης να εκμεταλλευτεί για επιθέσεις όπως η εκτίμηση κωδικών πρόσβασης με μέθοδο brute force ή η ενίσχυση DDoS. Το γεγονός ότι είναι ενεργοποιημένο σε αυτόν τον διακομιστή θα μπορούσε να αποτελέσει πιθανό κίνδυνο ασφαλείας.

3. Έκδοση WordPress: Ο ιστότοπος εκτελεί την έκδοση 6.2.2 του WordPress. Η ενημέρωση του WordPress είναι σημαντική για την ασφάλεια, καθώς οι νέες εκδόσεις συχνά περιλαμβάνουν

διορθώσεις για γνωστές ευπαθειές. Το γεγονός ότι αυτός ο ιστότοπος εκτελεί την τελευταία έκδοση είναι θετικό σημάδι.

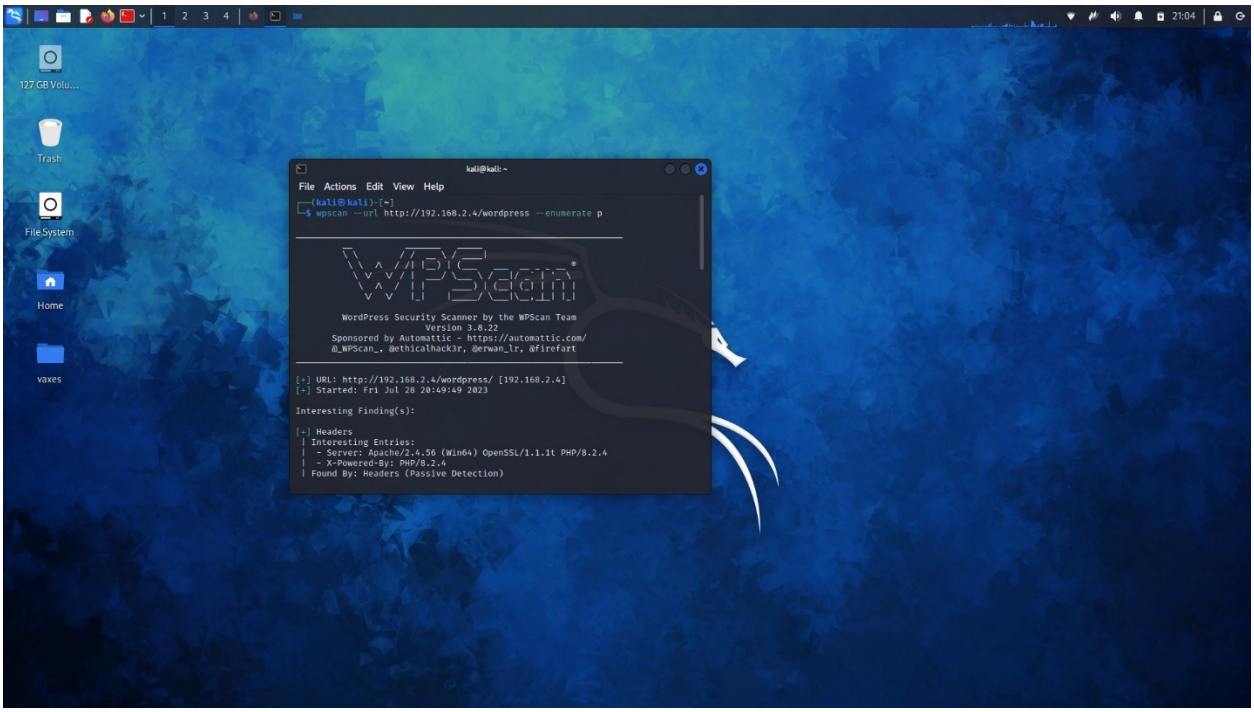
4. Πρόσθετα (Plugins): Το πρόσθετο WooCommerce είναι εγκατεστημένο στον ιστότοπο, αλλά δεν είναι η τελευταία έκδοση. Τα πρόσθετα μπορούν να εισάγουν τις δικές τους ευπαθειές ασφαλείας, επομένως είναι σημαντικό να τα διατηρούμε ενημερωμένα. Το γεγονός ότι αυτό το πρόσθετο είναι εκπρόθεσμο θα μπορούσε να αποτελέσει πιθανό κίνδυνο ασφαλείας.

5. Αντίγραφα ασφαλείας διαμόρφωσης (Config Backups): Τα αντίγραφα ασφαλείας διαμόρφωσης μπορεί μερικές φορές να περιλαμβάνουν ευαίσθητες πληροφορίες, όπως κωδικοί πρόσβασης βάσεων δεδομένων. Το γεγονός ότι το WPScan δεν βρήκε κανένα αντίγραφο ασφαλείας διαμόρφωσης είναι θετικό σημάδι από την οπτική γωνία της ασφάλειας.

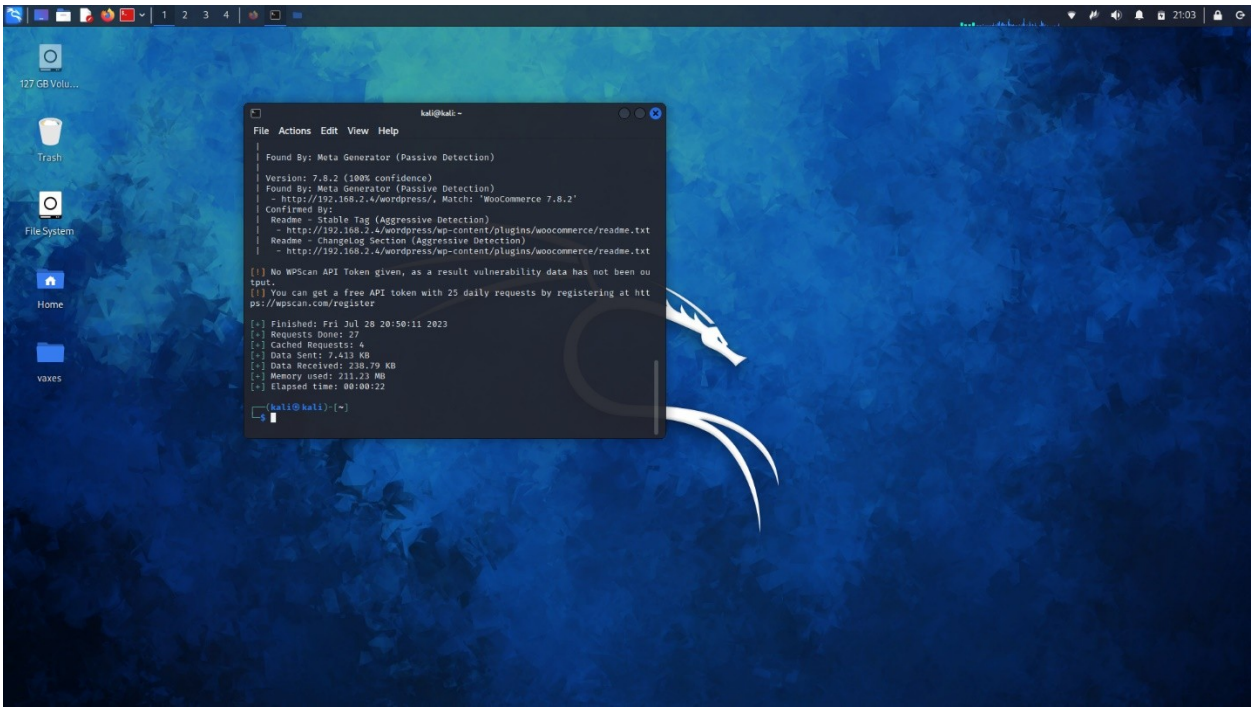
6. Διακριτικό API WPScan (WPScan API Token): Το WPScan μπορεί να χρησιμοποιήσει ένα διακριτικό API για να λάβει δεδομένα ευπαθειών από τη ‘βάση δεδομένων ευπαθειών’ WPScan. Αυτό μπορεί να παρέχει πιο λεπτομερείς πληροφορίες σχετικά με γνωστές ευπάθειες στον πυρήνα του WordPress, τα πρόσθετα και τα θέματα. Ωστόσο, δεν παρασχέθηκε διακριτικό API σε αυτήν την περίπτωση, επομένως αυτά τα δεδομένα δεν περιλήφθηκαν στην έξοδο.

Ακολουθεί η εκτέλεση της εντολής για την απαρίθμηση των πρόσθετων (plugins) στο WPScan 'wpscan --url http://192.168.2.4/wordpress --enumerate p'

Η εντολή είναι `--enumerate p` ή `--enumerate vp`. Αυτή η εντολή καλεί το WPScan να σαρώσει τον ιστότοπο WordPress και να παραθέσει όλα τα εγκατεστημένα πρόσθετα. Αυτό μπορεί να είναι χρήσιμο για την εντοπισμός πρόσθετων που μπορεί να περιέχουν γνωστές ευπάθειες ή που μπορεί να μην έχουν ενημερωθεί στην τελευταία τους έκδοση. Για παράδειγμα, αν θέλετε να σαρώσετε τον ιστότοπο example.com και να απαριθμήσετε όλα τα εγκατεστημένα πρόσθετα, θα χρησιμοποιούσατε την εντολή: `wpscan --url example.com --enumerate p`



Εικόνα 17: Εκτέλεση Σάρωσης στο WPScan με Εντολή 'enumerate ' στο WordPress Site



Εικόνα 18:Ανίχνευση Πιθανών Ευπαθειών σε WordPress με WPScan

<u>Ανάλυση και επεξήγηση των πιο κρίσιμων σημείων της αναφοράς του WPScan (Αναλυτικά όλη η αναφορά στο ΠΑΡΑΡΤΗΜΑ 4):</u>

1. Επικεφαλίδες: Ο διακομιστής τρέχει Apache έκδοση 2.4.56 σε ένα σύστημα Windows 64-bit. Αυτό είναι σημαντικό γιατί οι εκδόσεις του λογισμικού του διακομιστή μπορεί να περιέχουν ευπάθειες που μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Επιπλέον, ο διακομιστής χρησιμοποιεί OpenSSL έκδοση 1.1.1t για την υποστήριξη SSL/TLS, το οποίο είναι ζωτικής σημασίας για την ασφάλεια των συνδέσεων και PHP έκδοση 8.2.4 για την επεξεργασία σεναρίων PHP.

2. XML-RPC: Το XML-RPC φαίνεται να είναι ενεργοποιημένο. Αυτό είναι σημαντικό γιατί το XML-RPC μπορεί να χρησιμοποιηθεί για επιθέσεις από απόσταση, όπως η εκτέλεση απομακρυσμένων διαδικασιών ή η εκτέλεση επιθέσεων brute force.

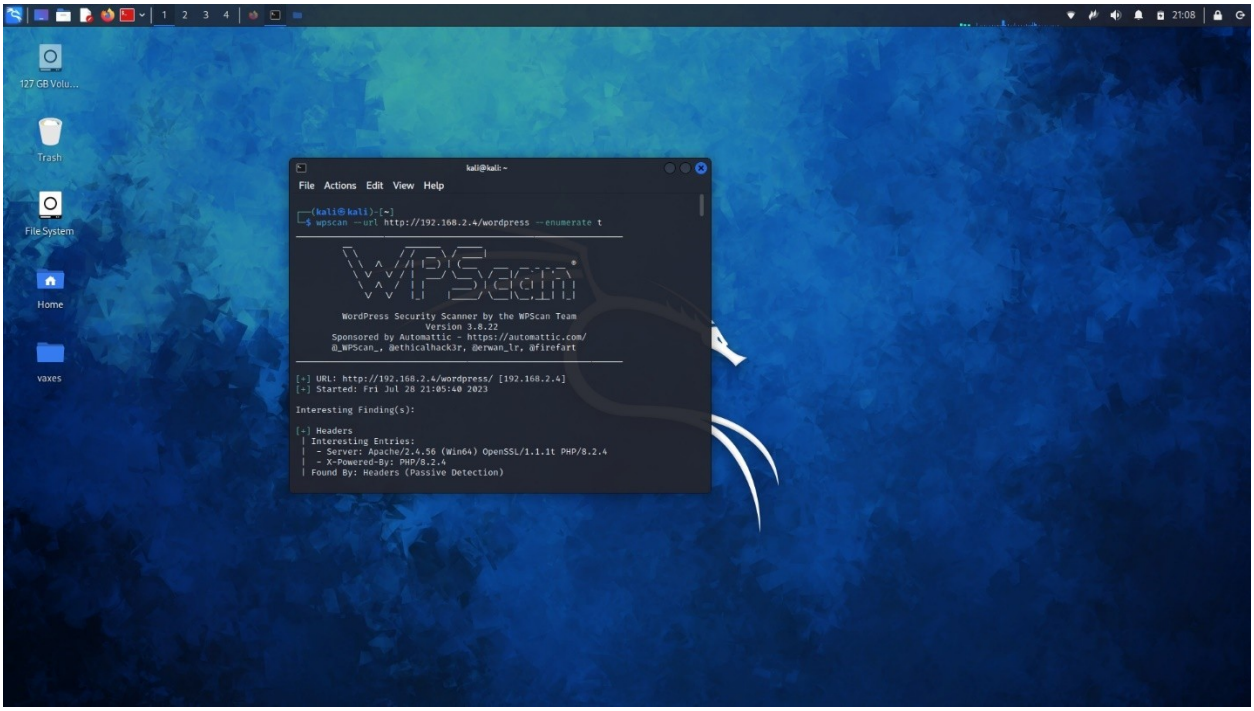
3. Έκδοση WordPress: Ο ιστότοπος τρέχει την έκδοση 6.2.2 του WordPress, η οποία είναι η τελευταία και κυκλοφόρησε στις 20 Μαΐου 2023. Η ενημέρωση του WordPress είναι ζωτικής

σημασίας για την ασφάλεια, καθώς οι νεότερες εκδόσεις συχνά περιλαμβάνουν διορθώσεις για γνωστές ευπάθειες.

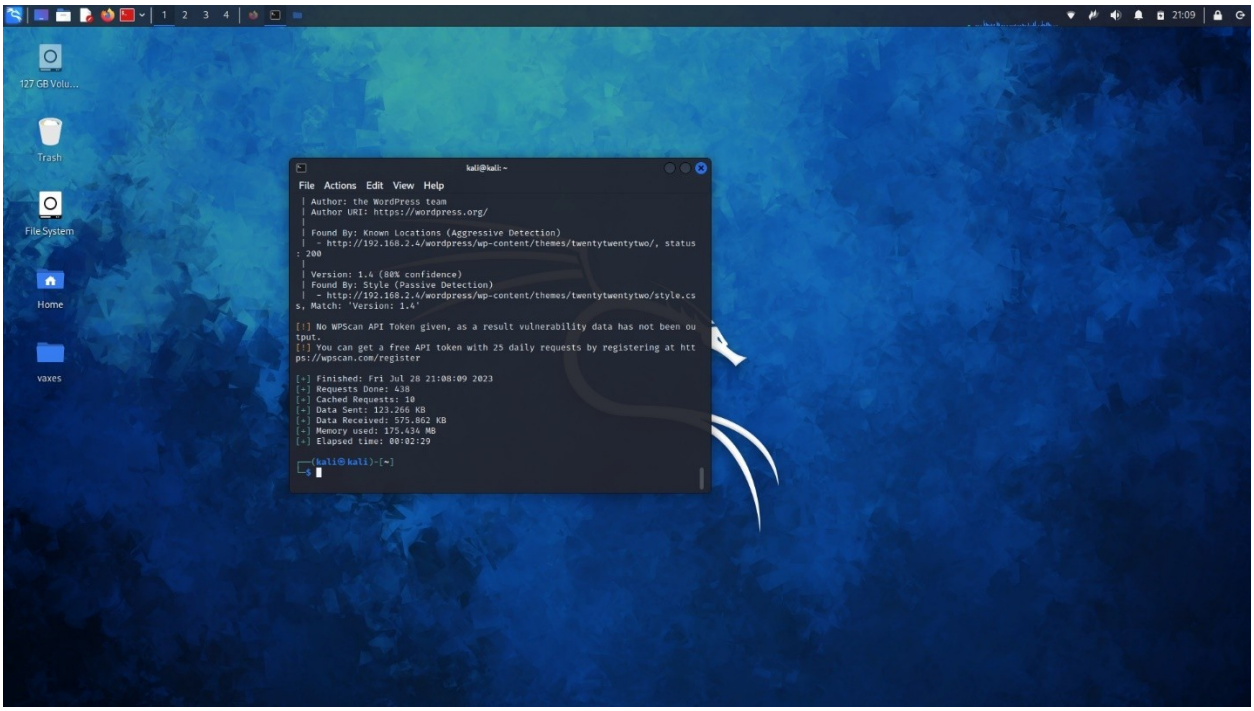
4. Πρόσθετα: Το πρόσθετο WooCommerce είναι εγκατεστημένο στον ιστότοπο, αλλά δεν είναι η τελευταία έκδοση. Η τρέχουσα έκδοση είναι 7.8.2, ενώ η τελευταία είναι η 7.9.0. Τα παλαιότερα πρόσθετα πινανόν να αποτελούν κίνδυνο ασφάλειας, καθώς πιθανόν να έχουν γνωστές ευπάθειες που έχουν διορθωθεί σε νεότερες εκδόσεις. Επιπλέον, το WPScan δεν μπόρεσε να εξάγει δεδομένα ευπάθειας λόγω της έλλειψης ενός διακριτικού API του WPScan.

Ακολουθεί η εκτέλεση της εντολής 'wpscan --url http://192.168.2.4/wordpress --enumerate t'.

Η επιλογή --enumerate t οδηγεί το WPScan να εντοπίσει και να παραθέσει όλα τα εγκατεστημένα θέματα (themes) της εγκατάστασης.



Εικόνα 19:Σάρωση Ασφάλειας με WPScan Χρησιμοποιώντας Εντολή Εντοπισμού Θεμάτων



Εικόνα 20:Λεπτομερής Έλεγχος Θεμάτων WordPress με 'wpscan --enumerate t'

<u>Ανάλυση και επεξήγηση των πιο κρίσιμων σημείων της αναφοράς του WPScan :</u>

1. Έκδοση Διακομιστή και PHP: Ο ιστότοπος χρησιμοποιεί τον διακομιστή Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4. Αυτό υποδηλώνει ότι ο διακομιστής λειτουργεί σε λειτουργικό σύστημα Windows 64-bit με OpenSSL για ασφαλείς συνδέσεις. Η έκδοση PHP είναι 8.2.4, η οποία είναι σχετικά πρόσφατη, αλλά είναι σημαντικό να διατηρείται ενημερωμένη στην τελευταία έκδοση για να αποφεύγονται πιθανές ευπάθειες ασφαλείας.

2. Ενεργοποίηση XML-RPC: Το XML-RPC είναι ενεργοποιημένο στον ιστότοπο. Το XML-RPC είναι ένα πρωτόκολλο που επιτρέπει τις απομακρυσμένες κλήσεις διαδικασιών μέσω HTTP. Μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, όπως η διαχείριση αναρτήσεων, σχολίων και πολυμέσων, ή η λήψη δεδομένων. Ωστόσο, μπορεί επίσης να αποτελέσει πιθανό κίνδυνο ασφαλείας εάν δεν είναι κατάλληλα ασφαλισμένο, καθώς μπορεί να χρησιμοποιηθεί για επιθέσεις brute force.

3. Ενεργοποίηση “Καταλόγου Ανεβάσματος”: Ο κατάλογος ανεβάσματος στον ιστότοπο έχει ενεργοποιημένη τη λίστα καταλόγου. Αυτό σημαίνει ότι οποιοσδήποτε μπορεί να δει τα

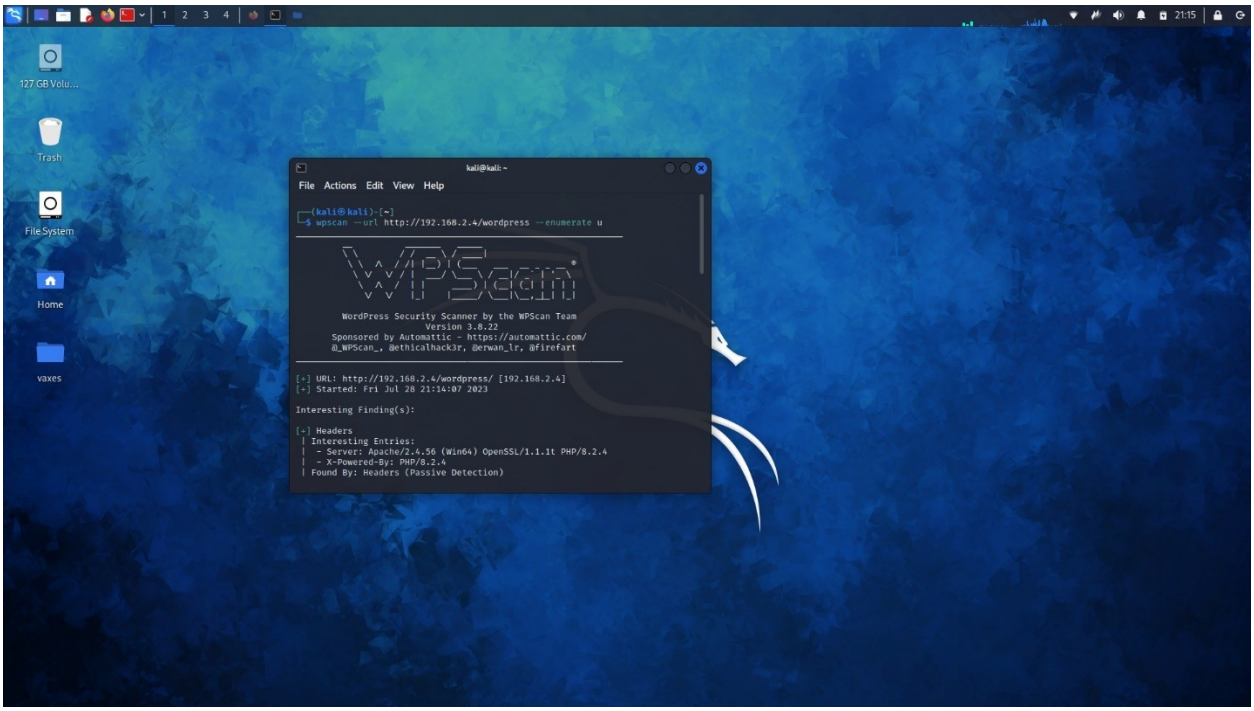
περιεχόμενα του καταλόγου ανεβάσματος, το οποίο θα μπορούσε ενδεχομένως να εκθέσει ευαίσθητα δεδομένα. Γενικά, συνιστάται να απενεργοποιηθεί η λίστα καταλόγου για να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση στα αρχεία.

4. Ενεργοποίηση Εξωτερικού WP-Cron: Το εξωτερικό WP-Cron είναι ενεργοποιημένο. Το WP-Cron είναι ένας προγραμματιστής εργασιών που χρησιμοποιεί το WordPress για να αυτοματοποιεί εργασίες όπως η δημοσίευση προγραμματισμένων αναρτήσεων, ο έλεγχος για ενημερώσεις θεμάτων ή πρόσθετων και η αποστολή ειδοποιήσεων μέσω email. Παρόλο που είναι μια απαραίτητη λειτουργία για πολλούς ιστότοπους WordPress, μπορεί ενδεχομένως να γίνει εκμεταλεύσιμο εάν δεν είναι κατάλληλα ασφαλισμένο.

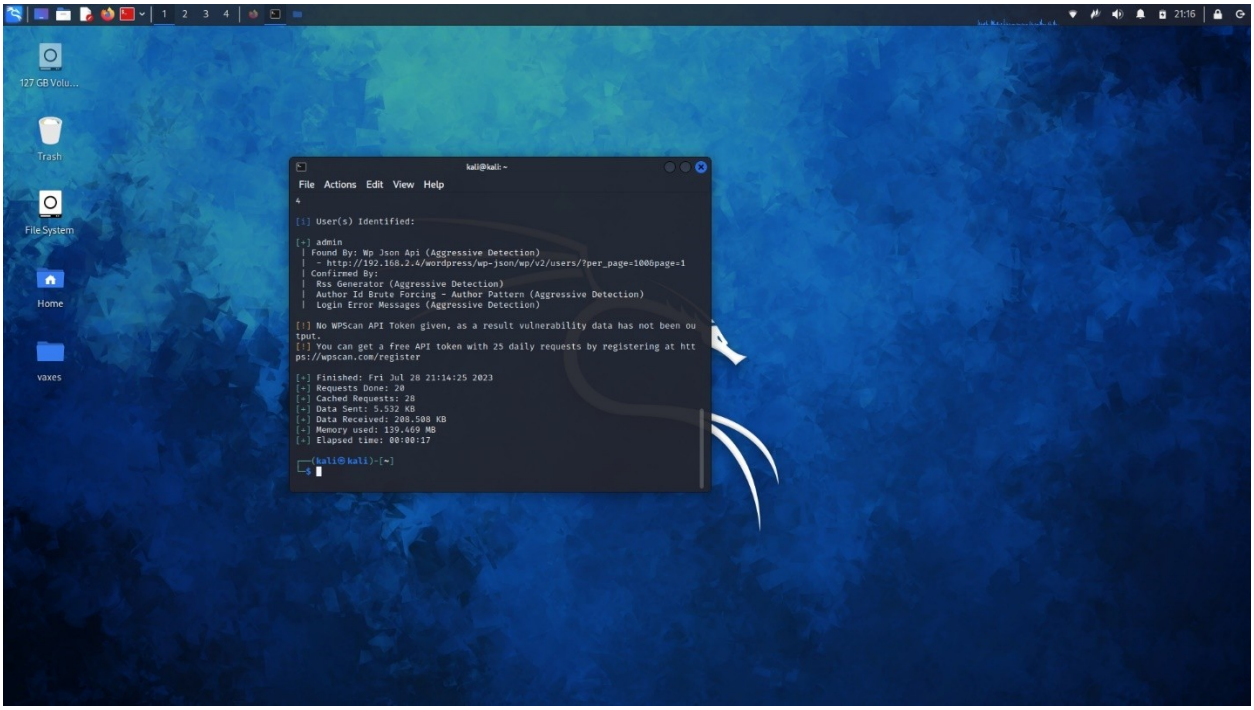
5. Έκδοση WordPress και Προσβασιμότητα Αρχείου Readme: Ο ιστότοπος λειτουργεί με την έκδοση 6.2.2 του WordPress και το αρχείο readme είναι προσβάσιμο. Το αρχείο readme μπορεί να παρέχει χρήσιμες πληροφορίες για τον ιστότοπο αλλά μπορεί επίσης να εκθέσει πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν από επιτιθέμενους, επομένως συχνά συνιστάται να αποκλείεται η πρόσβαση σε αυτό. Το γεγονός ότι η έκδοση του WordPress είναι ενημερωμένη είναι θετικό, καθώς σημαίνει ότι ο ιστότοπος πιθανότατα προστατεύεται από γνωστές ευπάθειες παλαιότερων εκδόσεων.

6.Θέματα WordPress: Ο ιστότοπος χρησιμοποιεί τα θέματα twentytwentyone, twentytwentythree, και twentytwentytwo. Όλα αυτά τα θέματα είναι ενημερωμένα. Η διατήρηση των θεμάτων ενημερωμένων είναι σημαντική για την ασφάλεια και τη λειτουργικότητα. Ωστόσο, είναι επίσης σημαντικό να ελέγχεται για οποιαδήποτε αχρησιμοποίητα θέματα και να αφαιρούνται, καθώς μπορούν επίσης να αποτελέσουν κίνδυνο ασφαλείας.

Ακολουθεί η εκτέλεση της εντολής 'wpscan --url http://192.168.2.4/wordpress --enumerate u' ώστε να ξεκινήσει η σάρωση του καθορισμένου URL και να απαριθμήσει (να αναγνωρίσει και να καταγράψει) τους χρήστες του ιστότοπου WordPress.



Εικόνα 21:Σάρωση Ιστοσελίδας WordPress για Χρήστες με Χρήση WPScan και Παραμέτρου 'enumerate u'



Εικόνα 22:"Αποτελέσματα Σάρωσης Χρηστών στο WordPress με 'wpscan --enumerate u'

Ανάλυση και επεξήγηση των πιο κρίσιμων σημείων της αναφοράς του WPScan :

1. Επικεφαλίδες: Ο διακομιστής που χρησιμοποιείται είναι ο Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4. Αυτό υποδηλώνει ότι ο διακομιστής λειτουργεί σε λειτουργικό σύστημα Windows 64-bit με OpenSSL για ασφαλείς συνδέσεις. Η έκδοση PHP είναι 8.2.4 η οποία είναι σχετικά πρόσφατη αλλά είναι σημαντικό να διατηρείται ενημερωμένη στην τελευταία έκδοση για να αποφεύγονται πιθανές ευπάθειες ασφαλείας.

2. XML-RPC: Το XML-RPC φαίνεται να είναι ενεργοποιημένο στον ιστότοπο. Το XML-RPC είναι ένα πρωτόκολλο που επιτρέπει τις απομακρυσμένες κλήσεις διαδικασιών μέσω HTTP. Μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, όπως η διαχείριση αναρτήσεων, σχολίων και πολυμέσων, ή η λήψη δεδομένων. Ωστόσο, μπορεί επίσης να αποτελέσει πιθανό κίνδυνο ασφαλείας εάν δεν είναι κατάλληλα ασφαλισμένο καθώς μπορεί να χρησιμοποιηθεί για επιθέσεις brute force.

3. Αρχείο readme του WordPress: Το αρχείο readme του WordPress βρέθηκε στον ιστότοπο. Αυτό το αρχείο περιέχει πληροφορίες σχετικά με την εγκατάσταση και τη χρήση του WordPress, αλλά μπορεί επίσης να παρέχει πληροφορίες σε κακόβουλους χρήστες σχετικά με την έκδοση του WordPress που χρησιμοποιείται.

4. Κατάλογος Ανεβάσματος: Ο κατάλογος ανεβάσματος στον ιστότοπο έχει ενεργοποιημένη τη λίστα καταλόγου. Αυτό σημαίνει ότι οποιοσδήποτε μπορεί να δει τα περιεχόμενα του καταλόγου ανεβάσματος, το οποίο θα μπορούσε ενδεχομένως να εκθέσει ευαίσθητα δεδομένα. Γενικά, συνιστάται να απενεργοποιηθεί η λίστα καταλόγου για να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση στα αρχεία.

5. Εξωτερικό WP-Cron: Το εξωτερικό WP-Cron φαίνεται να είναι ενεργοποιημένο. Το WP-Cron είναι ένας προγραμματιστής εργασιών που χρησιμοποιεί το WordPress για να αυτοματοποιεί εργασίες όπως η δημοσίευση προγραμματισμένων αναρτήσεων, ο έλεγχος για ενημερώσεις θεμάτων ή πρόσθετων κ.λπ. Ωστόσο, εάν δεν είναι κατάλληλα ασφαλισμένο, μπορεί να χρησιμοποιηθεί για DDoS επιθέσεις.

6. Έκδοση WordPress: Η έκδοση του WordPress που χρησιμοποιείται είναι η 6.2.2, η οποία είναι η τελευταία έκδοση που κυκλοφόρησε στις 20 Μαΐου 2023. Αυτό είναι θετικό, καθώς σημαίνει ότι ο ιστότοπος είναι πιθανότατα προστατευμένος από γνωστές ευπάθειες που επηρεάζουν παλαιότερες εκδόσεις του WordPress.

7. Χρήστες WordPress: Έχει αναγνωριστεί ένας χρήστης με το όνομα "admin". Αυτός ο χρήστης εντοπίστηκε μέσω του Wp Json Api, του Rss Generator, της διαδικασίας Brute Forcing Author IDs και των μηνυμάτων σφάλματος σύνδεσης. Η χρήση του "admin" ως όνομα χρήστη μπορεί να αυξήσει τον κίνδυνο επιθέσεων brute force, καθώς είναι ένα πολύ συνηθισμένο όνομα χρήστη που χρησιμοποιείται σε πολλές προσπάθειες επίθεσης. Συνίσταται να είναι διαφορετικό απο το προεπιλεγμένο.

SQLMap (WordPress Pen Tests)

Το SQLMap είναι ένα ανοιχτού κώδικα εργαλείο διύσδυσης που αυτοματοποιεί τη διαδικασία εντοπισμού και εκμετάλλευσης ευπαθειών SQL Injection σε μια εφαρμογή ιστού. Το SQL Injection είναι μια τεχνική που επιτρέπει σε χρήστες να εκτελέσουν επιβλαβείς SQL εντολές στη βάση δεδομένων μιας εφαρμογής.

Το Sqlmap είναι ιδιαίτερα χρήσιμο για τη δοκιμή διείσδυσης (penetration testing) για τους παρακάτω λόγους:

1. Αυτοματοποίηση: Το Sqlmap αυτοματοποιεί τη διαδικασία εντοπισμού ευπαθειών SQL Injection, κάτι που μπορεί να είναι χρονοβόρο και περίπλοκο αν γίνει χειροκίνητα.

2. Πληρότητα: Το Sqlmap μπορεί να εντοπίσει μια μεγάλη ποικιλία τύπων SQL Injection, συμπεριλαμβανομένων των UNION-based, Blind, Boolean-based, Time-based και Out-of-band.

3. Ευελιξία: Το Sqlmap υποστηρίζει αρκετές βάσεις δεδομένων, συμπεριλαμβανομένων των MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, HSQLDB και Informix.

4. Εκτεταμένες δυνατότητες: Πέρα από την ανίχνευση ευπαθειών, το Sqlmap μπορεί επίσης να εκμεταλλευτεί τις εντοπισμένες ευπάθειες για να ανακτήσει δεδομένα, να εκτελέσει εντολές στον εξυπηρετητή ή να ανεβάσει αρχεία.

Για τους παραπάνω λόγους, το Sqlmap είναι ένα πολύτιμο εργαλείο στο χώρο της ασφάλειας πληροφοριακών συστημάτων και τους ερεύνα σχετικά με τις ευπάθειες.

Εγκατάσταση SQLMap σε λειτουργικό σύστημα Kali Linux

Για να εγκαταστήσετε το Sqlmap στο Kali Linux, μπορείτε να χρησιμοποιήσετε τον διαχειριστή πακέτων του συστήματος. Ακολουθήστε τα παρακάτω βήματα:

1. Ανοίξτε ένα τερματικό.

2. Ενημερώστε τη λίστα των πακέτων του συστήματος εκτελώντας την εντολή:

sudo apt-get update

3. Εγκαταστήστε το sqlmap εκτελώντας την εντολή:

sudo apt-get install sqlmap

Αυτό θα εγκαταστήσει το Sqlmap στο σύστημά σας. Μπορείτε να επιβεβαιώσετε ότι η εγκατάσταση ήταν επιτυχής εκτελώντας την εντολή `sqlmap -h`, η οποία θα εμφανίσει τη βοήθεια και τις επιλογές του Sqlmap.

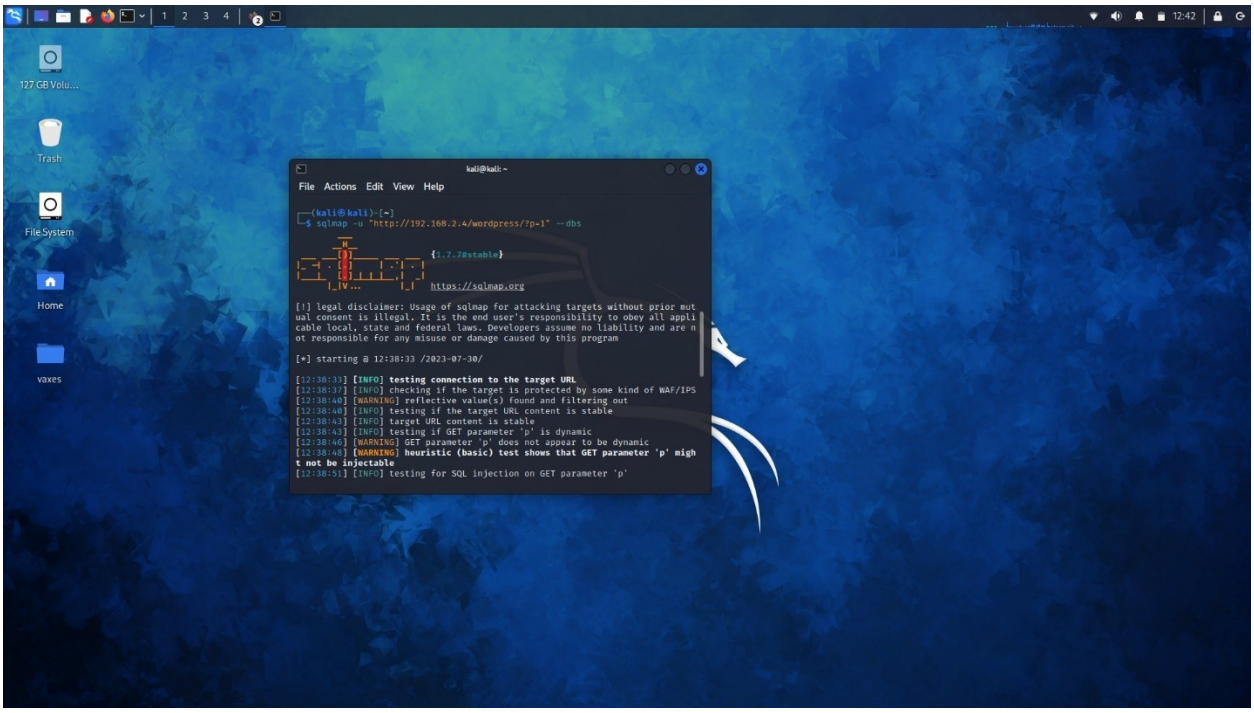
Ακολουθεί η εκτέλεση της βασικής σάρωσης της SQL db του Wordpress προς εύρεση πιθανών ευπαθειών με την εντολη ‘sqlmap -u "http://192.168.2.4/wordpress/?p=1" –dbs’

Αυτή η εντολή χρησιμοποιεί το εργαλείο sqlmap για να δοκιμάσει την ευπάθεια SQL Injection σε μια συγκεκριμένη διεύθυνση URL και να ανακτήσει τα ονόματα όλων των βάσεων δεδομένων, εάν βρεθεί κάποια ευπάθεια. Ας δούμε την εντολή λεπτομερώς:

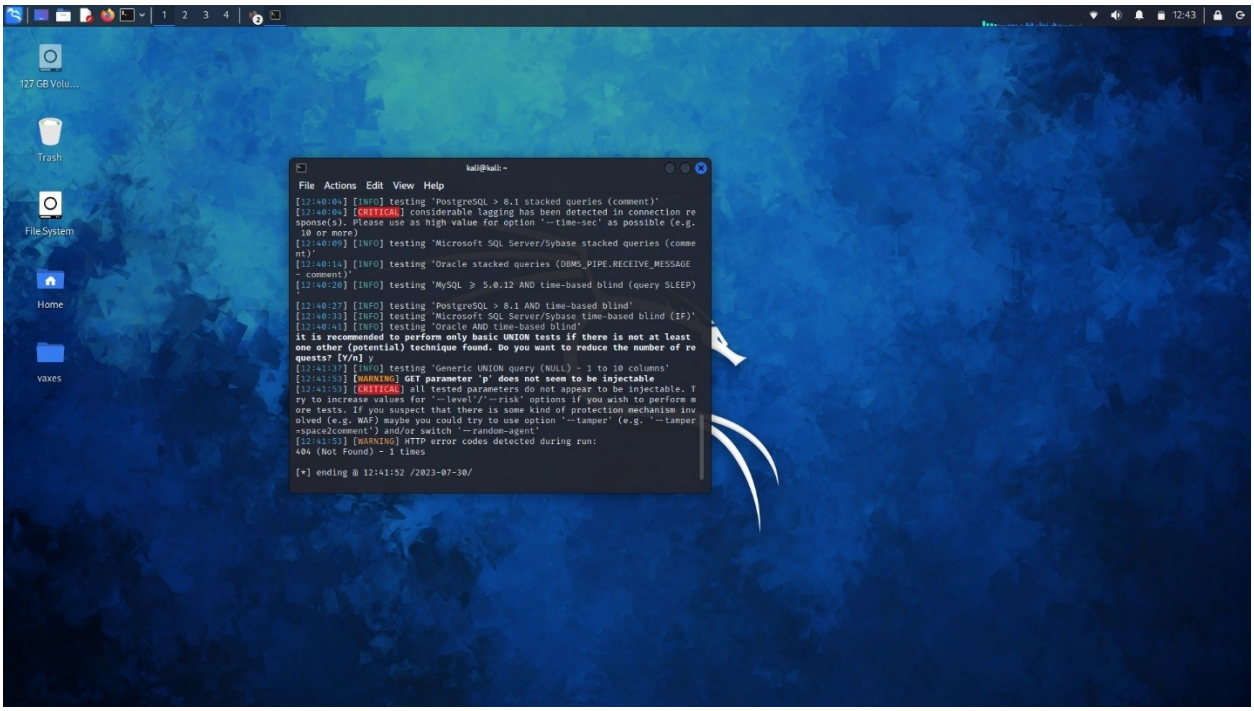
- `-u "http://192.168.2.4/wordpress/?p=1"`: Η επιλογή `-u` χρησιμοποιείται για να καθορίσει τη διεύθυνση URL που θέλουμε να δοκιμάσουμε. Σε αυτήν την περίπτωση, δοκιμάζουμε τη διεύθυνση URL "http://192.168.2.4/wordpress/?p=1".

- `--dbs`: Αυτή η επιλογή λέει στο sqlmap να ανακτήσει τα ονόματα όλων των βάσεων δεδομένων αν βρεθεί ευπάθεια SQL Injection.

Συνοψίζοντας, αυτή η εντολή λέει στο sqlmap να δοκιμάσει τη διεύθυνση URL "http://192.168.2.4/wordpress/?p=1" για ευπαθείες SQL Injection και, εάν βρεθεί κάποια ευπάθεια, να ανακτήσει τα ονόματα όλων των βάσεων δεδομένων.



Εικόνα 23:Έναρξη Εκτέλεσης SQLMap με Εστίαση στην Ανακάλυψη Βάσεων Δεδομένων



Εικόνα 24 :Ανίχνευση Ευπαθειών με Δοκιμές SQLMap σε WordPress

Με το πέρας της σάρωσης του SQLMap εμφάνισε τα εξης

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.2.4/wordpress/?p=1" --dbs
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:38:33 /2023-07-30/

[12:38:33] [INFO] testing connection to the target URL

[12:38:37] [INFO] checking if the target is protected by some kind of WAF/IPS

[12:38:40] [WARNING] reflective value(s) found and filtering out

[12:38:40] [INFO] testing if the target URL content is stable

[12:38:43] [INFO] target URL content is stable

[12:38:43] [INFO] testing if GET parameter 'p' is dynamic

[12:38:46] [WARNING] GET parameter 'p' does not appear to be dynamic

[12:38:48] [WARNING] heuristic (basic) test shows that GET parameter 'p' might not be injectable

[12:38:51] [INFO] testing for SQL injection on GET parameter 'p'

[12:38:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[12:39:09] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

got a 301 redirect to 'http://192.168.2.4/wordpress/?p=%28SELECT%20%28CASE%20WHEN%20%286375%3D5528%29%20THEN%201%20ELSE%20%28SELECT%205528%20UNION%20SELECT%205590%29%20END'. Do you want to follow? [Y/n] y

[12:39:30] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[12:39:37] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[12:39:44] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[12:39:53] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[12:40:00] [INFO] testing 'Generic inline queries'

[12:40:04] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[12:40:04] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)

[12:40:09] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[12:40:14] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[12:40:20] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[12:40:27] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[12:40:33] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[12:40:41] [INFO] testing 'Oracle AND time-based blind'

it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y

[12:41:37] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[12:41:53] [WARNING] GET parameter 'p' does not seem to be injectable

[12:41:53] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[12:41:53] [WARNING] HTTP error codes detected during run:

404 (Not Found) - 1 times

[*] ending @ 12:41:52 /2023-07-30/

Ανάλυση και επεξήγηση των πιο κρίσιμων σημείων της αναφοράς της εντολής :

Στην παρούσα ανάλυση παρέχονται επίσης λύσεις για τη βελτίωση της ασφάλειας:

1. Κλήση sqlmap: `sqlmap -u "http://192.168.2.4/wordpress/?p=1" --dbs`. Το URL ελέγχεται για ευπάθειες SQL Injection με τη χρήση της επιλογής `--dbs` για την ανακάλυψη των βάσεων δεδομένων του στόχου.

Λύση: Εάν εντοπιστεί ευπάθεια SQL Injection, θα πρέπει να διορθωθεί με την εφαρμογή παραμέτρων προστασίας στις εισόδους του χρήστη, τη χρήση prepared statements ή ORM frameworks, και την ενεργοποίηση WAF.

2. Το σύστημα ελέγχει για πιθανή προστασία WAF/IPS.

Λύση: Εάν δεν υπάρχει προστασία WAF ή IPS θα πρέπει να προστεθεί.

3. Το περιεχόμενο του URL και η παράμετρος GET 'p' ελέγχονται για σταθερότητα και δυναμικότητα αντίστοιχα.

Λύση: Εάν οι παράμετροι είναι δυναμικές, θα πρέπει να περιοριστούν οι δυνατότητες των χρηστών για εισαγωγή δυναμικού περιεχομένου ή να ελεγχθεί προσεκτικά για επιθέσεις SQL Injection.

4. Εφαρμόζονται διάφορες τεχνικές για την εξέταση της ευπάθειας SQL Injection.

Λύση: Η εφαρμογή πρέπει να ελεγχθεί για αυτές τις ευπάθειες και να διορθωθεί ανάλογα.

5. Καθυστερήσεις στην απόκριση της σύνδεσης που μπορεί να υποδηλώνουν ύπαρξη προστασίας.

Λύση: Η επιλογή `--time-sec` μπορεί να αυξηθεί για να παρακάμψει αυτό το πρόβλημα. Εάν υπάρχει WAF, η επιλογή `--tamper` μπορεί να χρησιμοποιηθεί για να παρακάμψει την ανίχνευση.

6. Η παράμετρος GET 'p' δεν φαίνεται να είναι επιρρεπής σε εισαγωγές.

Λύση: Η επιλογή `--level` ή `--risk` θα μπορούσε να αυξηθεί για περισσότερες δοκιμές. Επίσης, το `--tamper` και το `--random-agent` μπορεί να χρησιμοποιηθούν για να παρακάμψουν τυχόν μηχανισμούς προστασίας.

7. Εντοπίζεται ένας κωδικός λάθους HTTP 404.

Λύση: Η πρόσβαση σε ένα μη υπάρχον URL θα πρέπει να αποφεύγεται, καθώς η προσπάθεια μπορεί να οδηγήσει σε λάθη και αστάθεια.

Ακολουθεί η εκτέλεση της εξειδικευμένης σάρωσης της SQL db του Wordpress προς εύρεση πιθανών ευπαθειών με την εντολη: ‘sqlmap -u "http://192.168.2.4/wordpress/?p=1" --dump-all --level=5 --risk=2 --tamper=space2comment‘

Ας εξετάσουμε τα επιμέρους στοιχεία της εντολής:

- `-u "http://192.168.2.4/wordpress/?p=1"`: Η παράμετρος `-u` ακολουθείται από την διεύθυνση URL της σελίδας που θέλουμε να ελέγξουμε για ευπάθειες SQL Injection.

- `--dump-all`: Η επιλογή αυτή προκαλεί την αναζήτηση και την εξαγωγή όλων των βάσεων δεδομένων DBMS, των πινάκων, των στηλών και των δεδομένων.

- `--level=5`: Η παράμετρος `--level` καθορίζει το επίπεδο των δοκιμών που θα πραγματοποιηθούν. Το `5` είναι το μέγιστο επίπεδο και πραγματοποιεί τις πιο λεπτομερείς δοκιμές.

- `--risk=2`: Η παράμετρος `--risk` καθορίζει το επίπεδο του κινδύνου των δοκιμών που θα πραγματοποιηθούν. Το `2` είναι ένα μέτριο επίπεδο κινδύνου, που παρέχει μια ισορροπία μεταξύ της αποφυγής υπερβολικά επιθετικών δοκιμών και της εξασφάλισης αποτελεσματικής εύρεσης ευπαθειών.

- `--tamper=space2comment`: Η επιλογή `--tamper` ακολουθείται από ένα script που αλλοιώνει το payload. Το `space2comment` αλλοιώνει το payload μετατρέποντας τα κενά σε σχόλια, το οποίο μπορεί να αποφύγει ορισμένους τύπους ανίχνευσης.

Η εντολή αυτή αναλαμβάνει τη διενέργεια μιας ολοκληρωμένης δοκιμής για την εύρεση ευπαθειών SQL Injection στον συγκεκριμένο ιστότοπο.

Ακολουθεί η εκτέλεση της βασικής σάρωσης της SQL db του Wordpress προς εύρεση πιθανών ευπαθειών με την εντολη: 'sqlmap -u "http://192.168.2.4/wordpress/?p=1" --dump --level=3 --risk=1 --tamper=space2comment

Η συγκεκριμένη εντολή αναλύεται ως εξής:

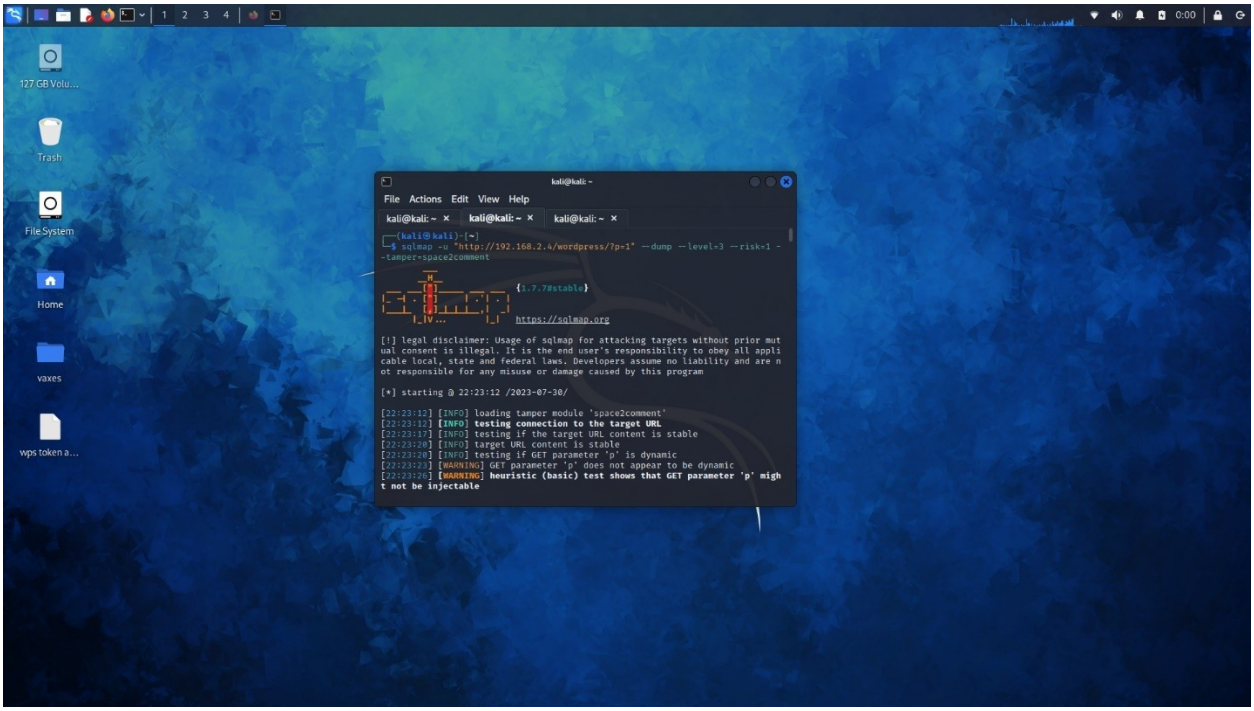
- `-u "http://192.168.2.4/wordpress/?p=1"`: Ορίζει τη διεύθυνση URL προς την οποία θα γίνει η ανάλυση. Σε αυτήν την περίπτωση, η εντολή θα εξετάσει τη σελίδα WordPress στη διεύθυνση 192.168.2.4 με την παράμετρο p ίση με 1.

- `--dump`: Αυτός ο διακόπτης οδηγεί το sqlmap να αποκτήσει (ή "να εκχωρήσει") όλα τα δεδομένα από τη βάση δεδομένων που είναι ευάλωτη σε SQL Injection.

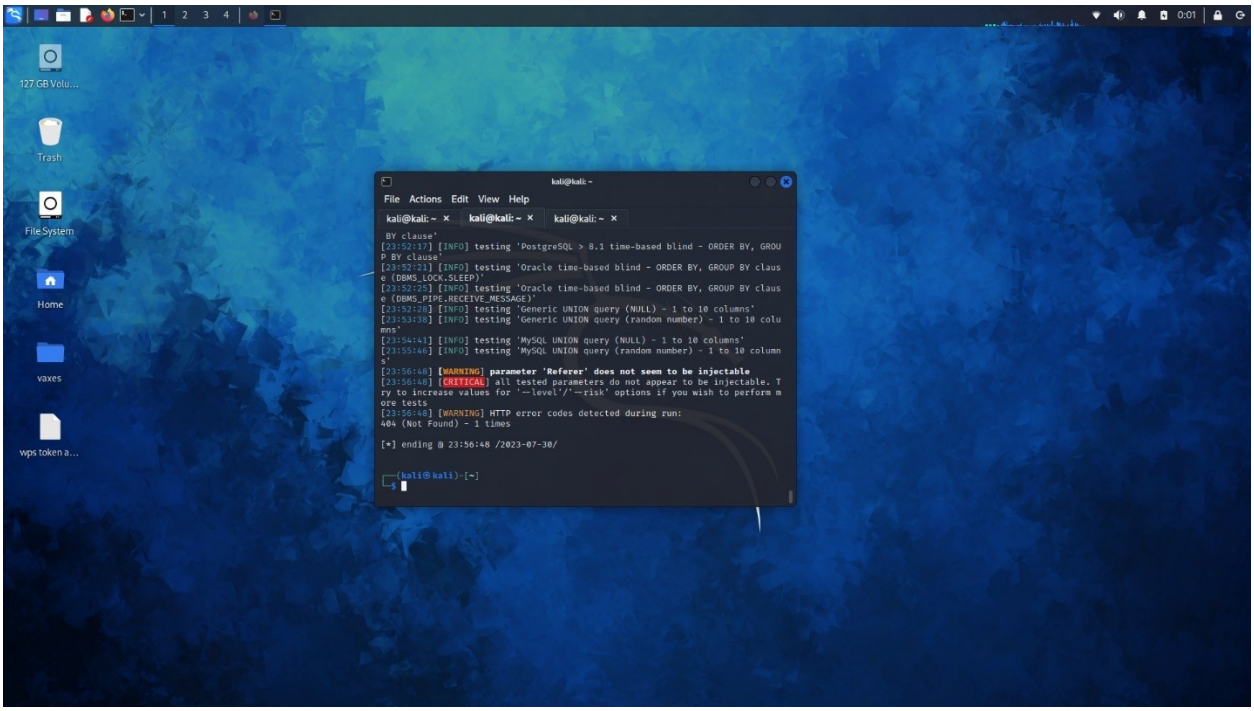
- `--level=3`: Ορίζει το επίπεδο των δοκιμών που θα εκτελέσει το sqlmap. Όσο μεγαλύτερο είναι το επίπεδο, τόσο περισσότερες δοκιμές γίνονται. Στο επίπεδο 3, το sqlmap θα δοκιμάσει μια ευρεία γκάμα σημείων εισόδου.

- `--risk=1`: Καθορίζει τον κίνδυνο των δοκιμών SQL Injection που πρόκειται να εκτελέσει το sqlmap. Στον κίνδυνο 1, το sqlmap θα εκτελέσει τις πλέον ασφαλείς δοκιμές, αυτές που είναι πιο πιθανό να μην προκαλέσουν αλλαγές στη βάση δεδομένων.

- `--tamper=space2comment`: Αυτός ο διακόπτης οδηγεί το sqlmap να τροποποιεί τις SQL εντολές που χρησιμοποιεί για τις δοκιμές του, αντικαθιστώντας τα κενά με σχόλια. Αυτό μπορεί να βοηθήσει στην παράκαμψη ορισμένων απλών φίλτρων ασφαλείας που προσπαθούν να εμποδίσουν τις επιθέσεις SQL Injection.



Εικόνα 25Αποτελέσματα SQLMap με '--dump'- Εξαγωγή Πληροφοριών Βάσης Δεδομένων



Εικόνα 26:Διερεύνηση SQL Injections μέσω SQLMap στο WordPress

<u>Με το πέρας της σάρωσης του SQLMap εμφάνισε τα εξής</u>

┌──(kali㉿kali)-[~]

└─$ sqlmap -u "http://192.168.2.4/wordpress/?p=1" --dump --level=3 --risk=1 --tamper=space2comment

___

__H__

___ ___["]_____ ___ ___ {1.7.7#stable}

|_ -| . ["] | .'| . |

|___|_ [,]_|_|_|__,| _|

|_|V... |_| https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:23:12 /2023-07-30/

[22:23:12] [INFO] loading tamper module 'space2comment'

[22:23:12] [INFO] testing connection to the target URL

[22:23:17] [INFO] testing if the target URL content is stable

[22:23:20] [INFO] target URL content is stable

[22:23:20] [INFO] testing if GET parameter 'p' is dynamic

[22:23:23] [WARNING] GET parameter 'p' does not appear to be dynamic

[22:23:26] [WARNING] heuristic (basic) test shows that GET parameter 'p' might not be injectable

[22:23:28] [INFO] testing for SQL injection on GET parameter 'p'

[22:23:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[22:23:33] [WARNING] reflective value(s) found and filtering out

[22:24:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'

[22:25:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'

[22:25:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'

[22:26:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'

[22:27:12] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'

[22:28:23] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'

[22:29:32] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'

[22:30:42] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[22:31:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

got a 301 redirect to 'http://192.168.2.4/wordpress/?p=%28SELECT%2F%2A%2A%2F%28CASE%2F%2A%2A%2FWHEN%2F%2A%2A%2F%283742%3D7013%29%2F%2A%2A%2FTHEN%2F%2A%2A%2F1%2F%2A%2A%2FELSE%2F%2A%2A%2F%28SELECT%2F%2A%2A%2F7013%2F%2A%2A%2FUNION%2F%2A%2A%2FSELECT%2F%2A%2A%2F5131%29%2F%2A%2A%2FEND'. Do you want to follow? [Y/n] y

[22:33:46] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'

[22:33:53] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'

[22:33:58] [INFO] testing 'Oracle boolean-based blind - Parameter replace'

[22:34:04] [INFO] testing 'Informix boolean-based blind - Parameter replace'

[22:34:09] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'

[22:34:15] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'

[22:34:20] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'

[22:34:20] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'

[22:34:25] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'

[22:34:25] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[22:34:31] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'

[22:34:31] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[22:34:31] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'

[22:34:39] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'

[22:34:45] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'

[22:34:51] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'

[22:35:59] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'

[22:36:35] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'

[22:37:12] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[22:37:44] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[22:38:17] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

[22:38:49] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[22:39:22] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[22:40:00] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[22:40:33] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'

[22:41:07] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'

[22:41:41] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[22:42:15] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)'

[22:42:48] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[22:43:22] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'

[22:43:56] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'

[22:44:29] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'

[22:45:02] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'

[22:45:35] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'

[22:46:10] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'

[22:46:43] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'

[22:46:46] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'

[22:46:49] [INFO] testing 'PostgreSQL error-based - Parameter replace'

[22:46:52] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'

[22:46:54] [INFO] testing 'Oracle error-based - Parameter replace'

[22:46:57] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'

[22:47:00] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'

[22:47:03] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'

[22:47:06] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'

[22:47:24] [INFO] testing 'Generic inline queries'

[22:47:27] [INFO] testing 'MySQL inline queries'

[22:47:30] [INFO] testing 'PostgreSQL inline queries'

[22:47:33] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'

[22:47:36] [INFO] testing 'Oracle inline queries'

[22:47:39] [INFO] testing 'SQLite inline queries'

[22:47:42] [INFO] testing 'Firebird inline queries'

[22:47:44] [INFO] testing 'ClickHouse inline queries'

[22:47:46] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'

[22:48:05] [INFO] testing 'MySQL >= 5.0.12 stacked queries'

[22:48:39] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'

[22:48:56] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[22:49:14] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'

[22:49:31] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[22:49:50] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'

[22:50:09] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[22:50:26] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[22:50:59] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'

[22:51:32] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'

[22:51:51] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'

[22:52:10] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'

[22:52:43] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'

[22:53:17] [INFO] testing 'MySQL AND time-based blind (ELT)'

[22:53:51] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[22:54:24] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[22:54:56] [INFO] testing 'Oracle AND time-based blind'

[22:55:29] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'

[22:55:32] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)'

[22:55:34] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'

[22:55:38] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'

[22:55:41] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'

[22:55:45] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'

[22:55:47] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'

[22:55:50] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'

[22:55:53] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'

it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y

[22:56:13] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[22:57:21] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'

[22:57:55] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[22:59:04] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'

[22:59:34] [WARNING] GET parameter 'p' does not seem to be injectable

[22:59:34] [WARNING] parameter 'User-Agent' does not appear to be dynamic

[22:59:36] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable

[22:59:39] [INFO] testing for SQL injection on parameter 'User-Agent'

[22:59:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[23:00:14] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'

[23:00:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'

[23:00:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'

[23:01:09] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'

[23:01:30] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'

[23:02:17] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'

[23:03:04] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'

[23:03:54] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[23:04:33] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[23:04:35] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'

[23:04:39] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'

[23:04:41] [INFO] testing 'Oracle boolean-based blind - Parameter replace'

[23:04:44] [INFO] testing 'Informix boolean-based blind - Parameter replace'

[23:04:45] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'

[23:04:47] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'

[23:04:49] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'

[23:04:50] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'

[23:04:52] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'

[23:04:53] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[23:04:56] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'

[23:04:59] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[23:04:59] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'

[23:05:02] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'

[23:05:06] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'

[23:05:09] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'

[23:05:42] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'

[23:06:01] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'

[23:06:19] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[23:06:54] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[23:07:33] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

[23:08:07] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[23:08:39] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[23:09:11] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[23:09:43] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'

[23:10:13] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'

[23:10:46] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[23:11:17] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)'

[23:11:51] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[23:12:23] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'

[23:12:56] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'

[23:13:28] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'

[23:14:02] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'

[23:14:32] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'

[23:15:03] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'

[23:15:33] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'

[23:15:35] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'

[23:15:38] [INFO] testing 'PostgreSQL error-based - Parameter replace'

[23:15:39] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'

[23:15:41] [INFO] testing 'Oracle error-based - Parameter replace'

[23:15:42] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'

[23:15:45] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'

[23:15:49] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'

[23:15:52] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'

[23:16:09] [INFO] testing 'Generic inline queries'

[23:16:11] [INFO] testing 'MySQL inline queries'

[23:16:12] [INFO] testing 'PostgreSQL inline queries'

[23:16:13] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'

[23:16:15] [INFO] testing 'Oracle inline queries'

[23:16:16] [INFO] testing 'SQLite inline queries'

[23:16:18] [INFO] testing 'Firebird inline queries'

[23:16:19] [INFO] testing 'ClickHouse inline queries'

[23:16:21] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'

[23:16:40] [INFO] testing 'MySQL >= 5.0.12 stacked queries'

[23:17:11] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'

[23:17:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[23:17:46] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'

[23:18:03] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[23:18:19] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'

[23:18:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[23:18:53] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[23:19:23] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'

[23:19:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'

[23:20:12] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'

[23:20:29] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'

[23:21:02] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'

[23:21:34] [INFO] testing 'MySQL AND time-based blind (ELT)'

[23:22:06] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[23:22:39] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[23:23:12] [INFO] testing 'Oracle AND time-based blind'

[23:23:44] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'

[23:23:46] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)'

[23:23:47] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'

[23:23:49] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'

[23:23:50] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'

[23:23:51] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'

[23:23:54] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'

[23:23:57] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'

[23:23:59] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'

[23:24:02] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[23:25:07] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'

[23:26:13] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[23:27:15] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'

[23:28:18] [WARNING] parameter 'User-Agent' does not seem to be injectable

[23:28:18] [WARNING] parameter 'Referer' does not appear to be dynamic

[23:28:19] [WARNING] heuristic (basic) test shows that parameter 'Referer' might not be injectable

[23:28:20] [INFO] testing for SQL injection on parameter 'Referer'

[23:28:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[23:28:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'

[23:29:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'

[23:29:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'

[23:29:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'

[23:30:03] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'

[23:30:34] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'

[23:31:08] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'

[23:31:40] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[23:32:12] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[23:32:13] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'

[23:32:14] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'

[23:32:16] [INFO] testing 'Oracle boolean-based blind - Parameter replace'

[23:32:18] [INFO] testing 'Informix boolean-based blind - Parameter replace'

[23:32:19] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'

[23:32:21] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'

[23:32:22] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'

[23:32:24] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'

[23:32:25] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'

[23:32:27] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[23:32:30] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'

[23:32:33] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[23:32:33] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'

[23:32:37] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'

[23:32:41] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'

[23:32:44] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'

[23:33:16] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'

[23:33:33] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'

[23:33:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[23:34:22] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[23:34:54] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

[23:35:27] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[23:36:03] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[23:36:39] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[23:37:11] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'

[23:37:45] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'

[23:38:20] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[23:38:52] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)'

[23:39:23] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[23:39:58] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'

[23:40:31] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'

[23:41:05] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'

[23:41:41] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'

[23:42:12] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'

[23:42:46] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'

[23:43:20] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'

[23:43:21] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'

[23:43:23] [INFO] testing 'PostgreSQL error-based - Parameter replace'

[23:43:24] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'

[23:43:26] [INFO] testing 'Oracle error-based - Parameter replace'

[23:43:27] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'

[23:43:30] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'

[23:43:32] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'

[23:43:36] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'

[23:43:54] [INFO] testing 'Generic inline queries'

[23:43:56] [INFO] testing 'MySQL inline queries'

[23:43:57] [INFO] testing 'PostgreSQL inline queries'

[23:43:58] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'

[23:44:00] [INFO] testing 'Oracle inline queries'

[23:44:01] [INFO] testing 'SQLite inline queries'

[23:44:03] [INFO] testing 'Firebird inline queries'

[23:44:04] [INFO] testing 'ClickHouse inline queries'

[23:44:06] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'

[23:44:25] [INFO] testing 'MySQL >= 5.0.12 stacked queries'

[23:44:58] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'

[23:45:14] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[23:45:30] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'

[23:45:49] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[23:46:06] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'

[23:46:23] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[23:46:43] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[23:47:16] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'

[23:47:53] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'

[23:48:10] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'

[23:48:28] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'

[23:49:02] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'

[23:49:38] [INFO] testing 'MySQL AND time-based blind (ELT)'

[23:50:11] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[23:50:48] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[23:51:26] [INFO] testing 'Oracle AND time-based blind'

[23:52:05] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'

[23:52:07] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)'

[23:52:09] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'

[23:52:11] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'

[23:52:12] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'

[23:52:14] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'

[23:52:17] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'

[23:52:21] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'

[23:52:25] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'

[23:52:28] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[23:53:38] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'

[23:54:41] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[23:55:46] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'

[23:56:48] [WARNING] parameter 'Referer' does not seem to be injectable

[23:56:48] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests

[23:56:48] [WARNING] HTTP error codes detected during run:

404 (Not Found) - 1 times

[*] ending @ 23:56:48 /2023-07-30/

Ανάλυση και επεξήγηση των πιο κρίσιμων σημείων της αναφοράς της εντολής:

1. Δοκιμή: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY ή GROUP BY clause (EXTRACTVALUE)

- Λύση: Βεβαιωθείτε ότι η εφαρμογή καθαρίζει σωστά την είσοδο του χρήστη για να αποτρέψει επιθέσεις SQL injection. Χρησιμοποιήστε παραμετροποιημένα ερωτήματα ή προετοιμασμένες δηλώσεις για να αποτρέψετε την εισαγωγή κακόβουλου κώδικα SQL.

2. Δοκιμή: PostgreSQL AND error-based - WHERE ή HAVING clause

- Λύση: Όπως και παραπάνω, καθαρίστε την είσοδο του χρήστη και χρησιμοποιήστε παραμετροποιημένα ερωτήματα ή προετοιμασμένες δηλώσεις για να αποτρέψετε την SQL injection.

3. Δοκιμή: Microsoft SQL Server/Sybase AND error-based - WHERE ή HAVING clause (CONVERT)

- Λύση: Εφαρμόστε σωστή επικύρωση εισόδου και χρησιμοποιήστε παραμετροποιημένα ερωτήματα ή αποθηκευμένες διαδικασίες για να αποτρέψετε επιθέσεις SQL injection.

4. Δοκιμή: Oracle AND error-based - WHERE ή HAVING clause (XMLType)

- Λύση: Χρησιμοποιήστε μεταβλητές δέσμευσης, παραμετροποιημένα ερωτήματα ή αποθηκευμένες διαδικασίες για να αποτρέψετε την SQL injection. Αποφύγετε τη δημιουργία δυναμικών ερωτημάτων SQL μέσω συγχώνευσης συμβολοσειρών.

5. Δοκιμή: Firebird AND error-based - WHERE ή HAVING clause

- Λύση: Εφαρμόστε σωστή επικύρωση εισόδου και χρησιμοποιήστε παραμετροποιημένα ερωτήματα ή αποθηκευμένες διαδικασίες για να αποτρέψετε επιθέσεις SQL injection.

6. Δοκιμή: MonetDB AND error-based - WHERE ή HAVING clause

- Λύση: Χρησιμοποιήστε παραμετροποιημένα ερωτήματα ή προετοιμασμένες δηλώσεις για να αποτρέψετε την SQL injection. Αποφύγετε τη δημιουργία δυναμικών ερωτημάτων SQL μέσω συγχώνευσης συμβολοσειρών.

7. Δοκιμή: Vertica AND error-based - WHERE ή HAVING clause

- Λύση: Εφαρμόστε σωστή επικύρωση εισόδου και χρησιμοποιήστε παραμετροποιημένα ερωτήματα ή αποθηκευμένες διαδικασίες για να αποτρέψετε επιθέσεις SQL injection

8. Δοκιμή: IBM DB2 AND error-based - WHERE ή HAVING clause

- Λύση: Χρησιμοποιήστε μεταβλητές δέσμευσης, παραμετροποιημένα ερωτήματα ή αποθηκευμένες διαδικασίες για να αποτρέψετε την SQL injection. Αποφύγετε τη δημιουργία δυναμικών ερωτημάτων SQL μέσω συγχώνευσης συμβολοσειρών.

9. Δοκιμή: ClickHouse AND error-based - WHERE, HAVING, ORDER BY ή GROUP BY clause

- Λύση: Εφαρμόστε σωστή επικύρωση εισόδου και χρησιμοποιήστε παραμετροποιημένα ερωτήματα ή αποθηκευμένες διαδικασίες για να αποτρέψετε επιθέσεις SQL injection

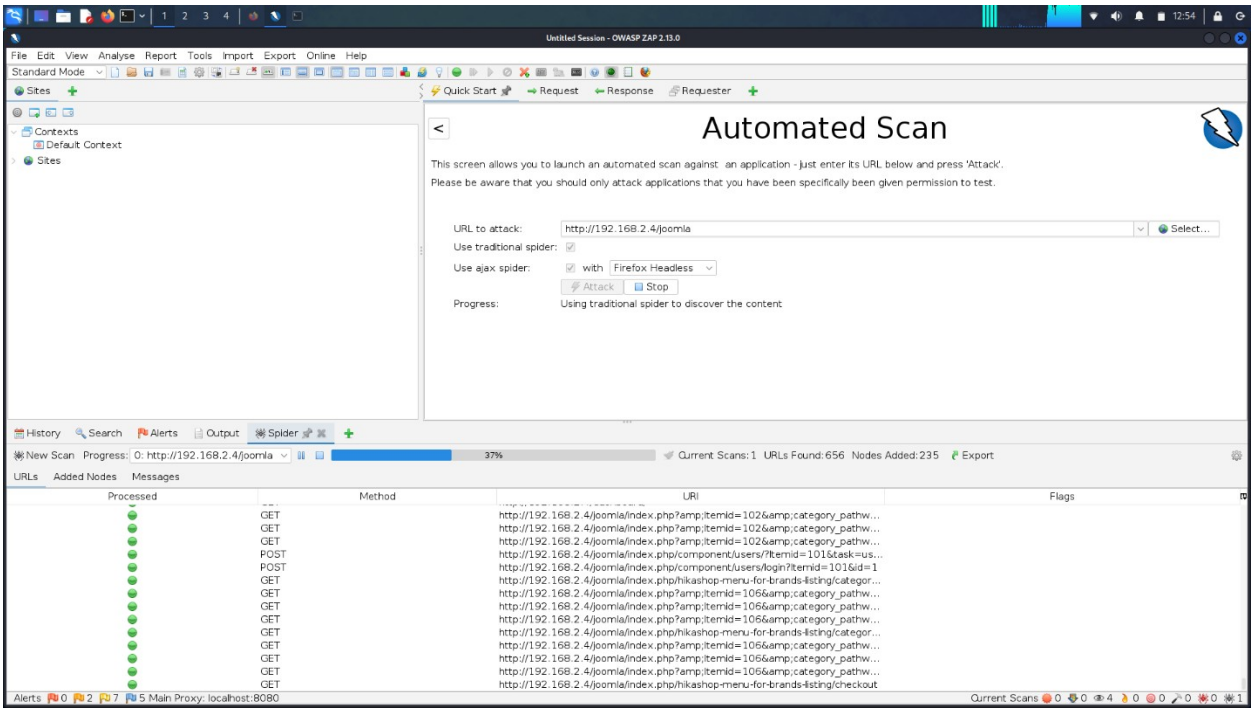
10. Δοκιμή: MySQL >= 5.0 error-based - Parameter replace (FLOOR)

- Λύση: Βεβαιωθείτε ότι η εφαρμογή καθαρίζει σωστά την είσοδο του χρήστη για να αποτρέψει επιθέσεις SQL injection. Χρησιμοποιήστε παραμετροποιημένα ερωτήματα ή προετοιμασμένες δηλώσεις για να αποτρέψετε την εισαγωγή κακόβουλου κώδικα SQL

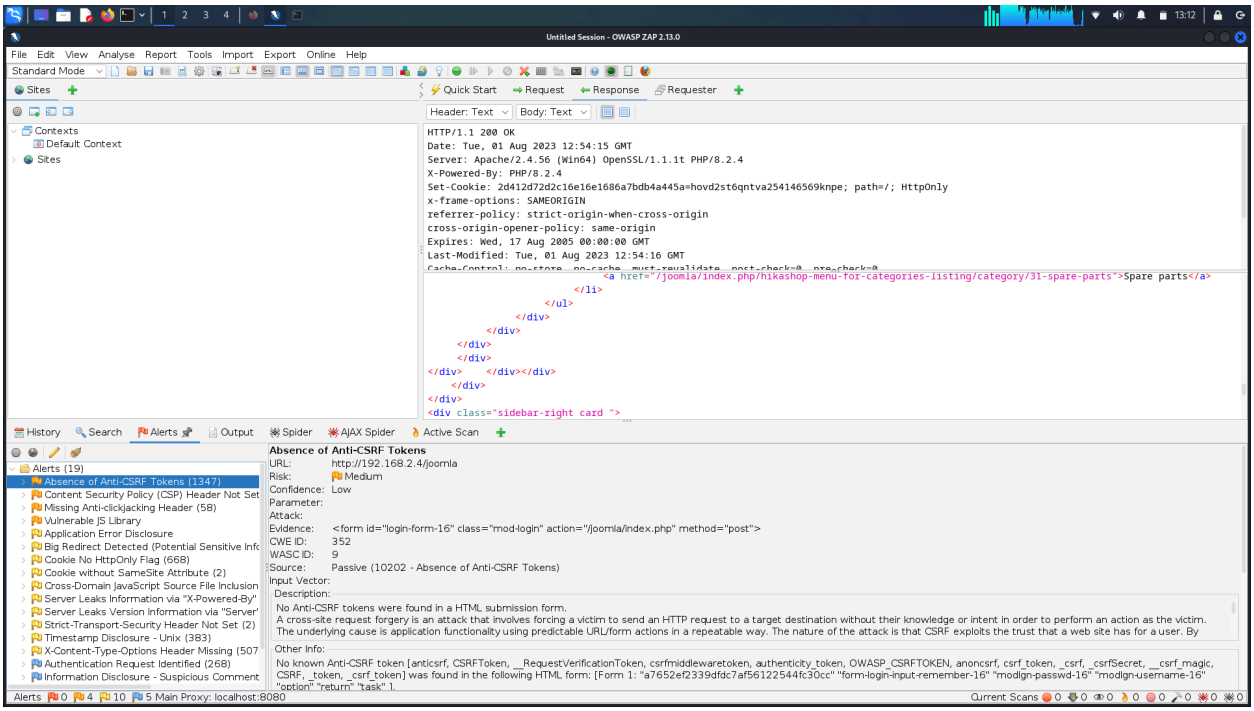
Penetration Testing στο Joomla (VirtueMart)

OWASP ZAP (Joomla Pen Tests)

- Η σάρωση πραγματοποιήθηκε σε μια τοπική εφαρμογή (http://127.0.0.1/joomla/) μέσα από λειτουργικό σύστημα Kali Linux και ο λόγος ήταν διότι μέσα από τα Windows το Zap κατέστρεφε το Web Application και την βάση δεδομένων.



Εικόνα 27:Προετοιμασία OWASP ZAP για Penetration Testing στο Joomla e-shop - VirtueMart



Εικόνα 28:Λεπτομερής Προβολή Αποτελεσμάτων OWASP ZAP σε Joomla e-shop

Αυτή η αναφορά παρουσιάζει τα αποτελέσματα της σάρωσης που πραγματοποιήθηκε από το OWASP ZAP στην ιστοσελίδα Joomla. Η σάρωση αναγνώρισε μια σειρά από πιθανά θέματα ασφαλείας, τα οποία κατηγοριοποιούνται ανάλογα με το επίπεδο κινδύνου (Υψηλό, Μέσο, Χαμηλό, Ενημερωτικό) και το επίπεδο εμπιστοσύνης (Υψηλό, Μέσο, Χαμηλό).

Ακολουθεί μια επισκόπηση ορισμένων από τα ευρήματα:

1. Έλλειψη Αντι-CSRF Tokens (Μέσος Κίνδυνος): Αυτό υποδηλώνει ότι η εφαρμογή σας μπορεί να είναι ευάλωτη σε επιθέσεις Cross-Site Request Forgery (CSRF). Τα CSRF tokens χρησιμοποιούνται για την πρόληψη των επιθέσεων CSRF, διασφαλίζοντας ότι κάθε υποβολή φόρμας είναι μοναδική και δεν μπορεί να αντιγραφεί από επιτιθέμενο.

2. Content Security Policy (CSP) Header Δεν Έχει Οριστεί (Μέσος Κίνδυνος): Η CSP είναι μια λειτουργία ασφαλείας που βοηθά στην πρόληψη μιας ποικιλίας επιθέσεων, συμπεριλαμβανομένων των επιθέσεων Cross-Site Scripting (XSS) και επιθέσεων εισαγωγής δεδομένων. Εάν δεν έχει οριστεί, η εφαρμογή σας μπορεί να είναι πιο ευάλωτη σε αυτούς τους τύπους επιθέσεων.

3. Λείπει η Επικεφαλίδα Anti-clickjacking (Μέσος Κίνδυνος): Το clickjacking είναι μια τεχνική όπου ένας επιτιθέμενος ξεγελά έναν χρήστη να κάνει κλικ σε κάτι διαφορετικό από αυτό που ο χρήστης αντιλαμβάνεται ότι κάνει κλικ. Οι επικεφαλίδες anti-clickjacking μπορούν να βοηθήσουν στην πρόληψη αυτού του τύπου επίθεσης.

4. Ευάλωτη Βιβλιοθήκη JS (Μέσος Κίνδυνος): Αυτό υποδηλώνει ότι η εφαρμογή σας χρησιμοποιεί μια βιβλιοθήκη JavaScript που έχει γνωστές ευπάθειες. Θα πρέπει να ενημερώσετε αυτήν τη βιβλιοθήκη σε μια ασφαλή έκδοση.

5. Ο Διακομιστής Διαρρέει Πληροφορίες μέσω των Πεδίων Επικεφαλίδας HTTP Απάντησης "X-Powered-By" (Χαμηλός Κίνδυνος): Αυτό υποδηλώνει ότι ο διακομιστής σας αποκαλύπτει πιθανές ευαίσθητες πληροφορίες στις επικεφαλίδες HTTP, οι οποίες θα μπορούσαν να βοηθήσουν έναν επιτιθέμενο να συλλέξει πληροφορίες για το σύστημά σας.

6. Λείπει η Επικεφαλίδα X-Content-Type-Options (Χαμηλός Κίνδυνος): Αυτή η επικεφαλίδα χρησιμοποιείται για την προστασία από επιθέσεις σύγχυσης τύπου MIME. Εάν δεν έχει οριστεί, η εφαρμογή σας μπορεί να είναι πιο ευάλωτη σε αυτούς τους τύπους επιθέσεων.

7. Αποκάλυψη Πληροφοριών - Υποψίες Σχόλια (Ενημέρωση): Αυτό υποδηλώνει ότι η εφαρμογή σας μπορεί να αποκαλύπτει πιθανές ευαίσθητες πληροφορίες σε σχόλια στον πηγαίο κώδικα.

8. Σύγχρονη Ιστοεφαρμογή (Ενημέρωση): Αυτό δεν είναι μια ευπάθεια αλλά μια ένδειξη ότι η εφαρμογή σας χρησιμοποιεί σύγχρονες τεχνολογίες web.

Τρόποι αντιμετώπισης ευπαθειών

1. Έλλειψη Αντι-CSRF Tokens: Θα πρέπει να εφαρμόσετε τη χρήση tokens CSRF στην εφαρμογή σας. Αυτά τα tokens διασφαλίζουν ότι κάθε υποβολή φόρμας είναι μοναδική και δεν μπορεί να αντιγραφεί από επιτιθέμενο.

2. Content Security Policy (CSP) Header Δεν Έχει Οριστεί: Θα πρέπει να ορίσετε μια πολιτική ασφαλείας περιεχομένου (CSP) για την εφαρμογή σας. Αυτό μπορεί να γίνει προσθέτοντας την επικεφαλίδα 'Content-Security-Policy' στις απαντήσεις HTTP της εφαρμογής σας.

3. Λείπει η Επικεφαλίδα Anti-clickjacking: Θα πρέπει να προσθέσετε την επικεφαλίδα 'X-Frame-Options' στις απαντήσεις HTTP της εφαρμογής σας. Αυτό θα αποτρέψει την εφαρμογή σας από το να εμφανίζεται μέσα σε ένα frame, το οποίο μπορεί να βοηθήσει στην πρόληψη επιθέσεων clickjacking.

4. Ευάλωτη Βιβλιοθήκη JS: Θα πρέπει να ενημερώσετε την ευάλωτη βιβλιοθήκη JavaScript σε μια ασφαλή έκδοση. Αν δεν είναι δυνατή η ενημέρωση, θα πρέπει να εξετάσετε την αντικατάσταση της βιβλιοθήκης με μια άλλη που δεν είναι ευάλωτη.

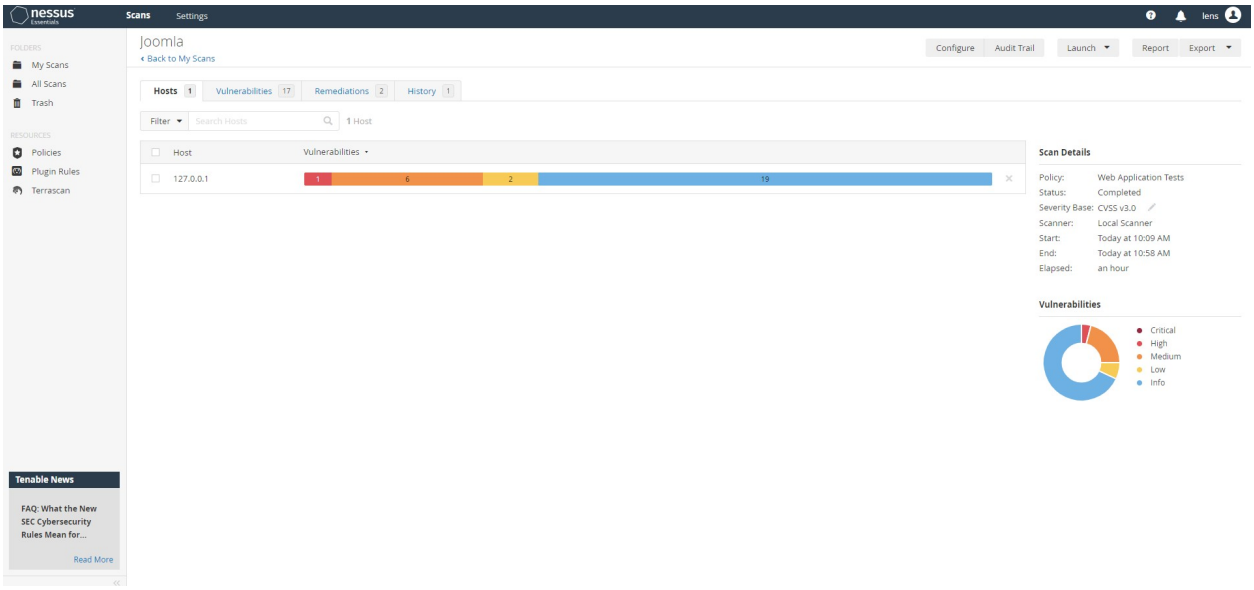
5. Ο Διακομιστής Διαρρέει Πληροφορίες μέσω των Πεδίων Επικεφαλίδας HTTP Απάντησης "X-Powered-By": Θα πρέπει να ρυθμίσετε τον διακομιστή σας να μην στέλνει αυτήν την επικεφαλίδα. Αυτό μπορεί να γίνει συνήθως μέσω του αρχείου ρυθμίσεων του διακομιστή σας.

6. Λείπει η Επικεφαλίδα X-Content-Type-Options: Θα πρέπει να προσθέσετε την επικεφαλίδα 'X-Content-Type-Options' με την τιμή 'nosniff' στις απαντήσεις HTTP της εφαρμογής σας. Αυτό θα αποτρέψει τους πελάτες από το να προσπαθήσουν να μαντέψουν τον τύπο MIME του περιεχομένου.

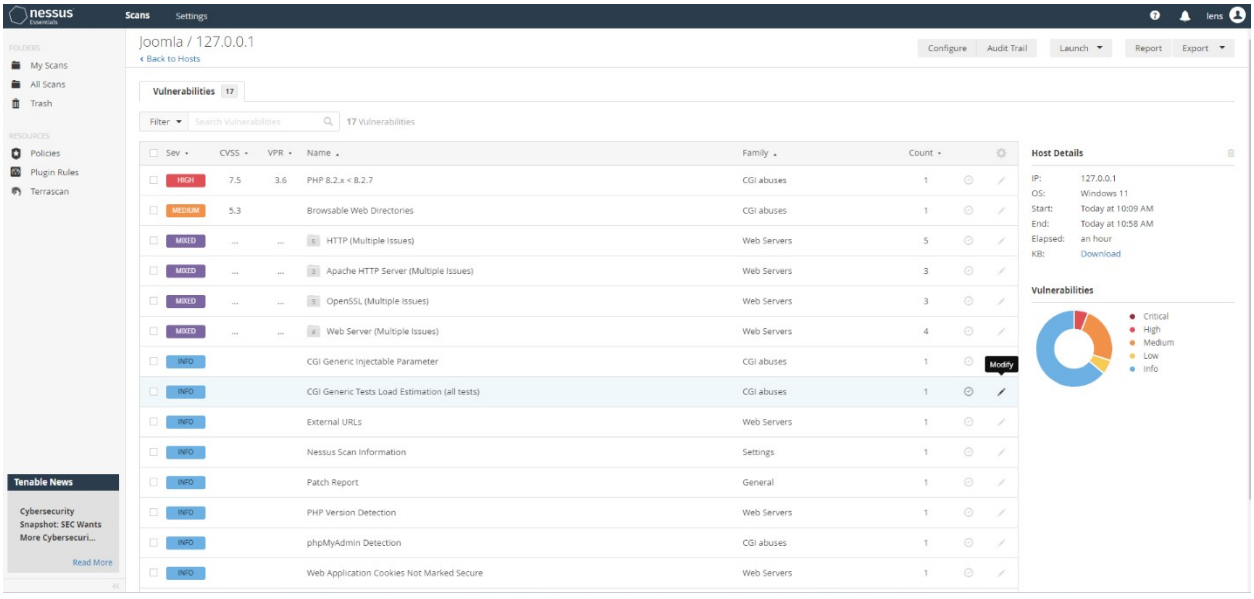
7. Αποκάλυψη Πληροφοριών - Υποψίες Σχόλια: Θα πρέπει να εξετάσετε τα σχόλια που αναφέρονται στην αναφορά και να αφαιρέσετε όσα περιέχουν ευαίσθητες πληροφορίες.

8. Σύγχρονη εφαρμογή ιστού : Αυτό δεν είναι μια ευπάθεια, αλλά μια ένδειξη ότι η εφαρμογή σας χρησιμοποιεί σύγχρονες τεχνολογίες web. Δεν χρειάζεται να ληφθεί καμία δράση γι' αυτό.

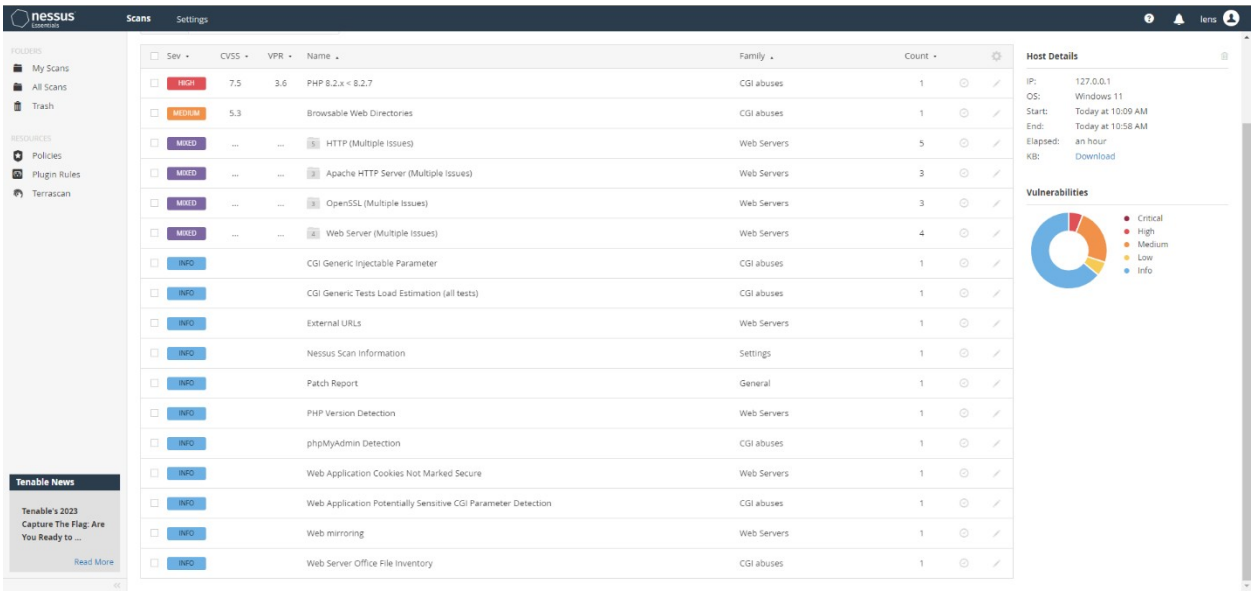
Nessus Essentials (Joomla Pen Tests) :



Εικόνα 29:Επισκόπηση Σάρωσης Ευπαθειών Joomla με Nessus Essentials



Εικόνα 30:Λεπτομερής Αναφορά Ευπαθειών Joomla από Nessus Essentials



Εικόνα 31:Συνέχεια Εκτεταμένης Αποτίμησης Ευπαθειών Joomla με Nessus Essentials

Η ολοκληρωμένη λίστα με τις ευπάθειες που βρέθηκαν και αναφέρονται στο εξαγόμενο αρχείο pdf είναι οι εξής :

1. PHP 8.2.x < 8.2.7 (Severity: High, CVSS V3.0: 7.5, VPR Score: 3.6, Plugin: 177511)
2. OpenSSL 1.1.1 < 1.1.1v Vulnerability (Severity: Medium, CVSS V3.0: 5.9, VPR Score: 4.4, Plugin: 178475)
3. Apache mod_info /server-info Information Disclosure (Severity: Medium, CVSS V3.0: 5.3, Plugin: 10678)
4. Apache mod_status /server-status Information Disclosure (Severity: Medium, CVSS V3.0: 5.3, Plugin: 10677
5. Browsable Web Directories (Severity: Medium, CVSS V3.0: 5.3, Plugin: 40984
6. HTTP TRACE / TRACK Methods Allowed (Severity: Medium, CVSS V3.0: 5.3, VPR Score: 4.0, Plugin: 11213)
7. OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities (Severity: Medium, CVSS V3.0: 5.3, VPR Score: 4.4, Plugin: 173260)
8. Web Server Allows Password Auto-Completion (Severity: Low, CVSS: N/A, Plugin: 42057)

9. Web Server Transmits Cleartext Credentials (Severity: Low, CVSS V3.0: 2.6, Plugin: 26194)

12. Apache HTTP Server Version (Plugin: 48204)
13. CGI Generic Injectable Parameter (Plugin: 47830)
14. CGI Generic Tests Load Estimation (all tests) (Plugin: 33817)
15. External URLs (Plugin: 49704)
16. HTTP Methods Allowed (per directory) (Plugin: 43111)
17. HTTP Server Type and Version (Plugin: 10107)
18. HyperText Transfer Protocol (HTTP) Information (Plugin: 24260)
19. HyperText Transfer Protocol (HTTP) Redirect Information (Plugin: 91634)
20. Nessus Scan Information (Plugin: 19506)
21. OpenSSL Version Detection (Plugin: 57323)
22. PHP Version Detection (Plugin: 48243)
23. Patch Report (Plugin: 66334)
24. Web Application Cookies Not Marked Secure (Plugin: 85602)
25. Web Application Potentially Sensitive CGI Parameter Detection (Plugin: 40773)
26. Web Server Directory Enumeration (Plugin: 11032)
27. Web Server Harvested Email Addresses (Plugin: 49705)
28. Web Server Office File Inventory (Plugin: 11419
29. Web mirroring (Plugin: 10662)
30. phpMyAdmin Detection (Plugin: 17219)

<u>Ανάλυση των ευπαθειών και προτεινόμενες λύσεις :</u>

Ακολουθεί η ανάλυση των ευπαθειών και άλλων θεμάτων που αναφέρονται στο PDF:

1. PHP 8.2.x < 8.2.7: Η έκδοση PHP που τρέχει στον απομακρυσμένο διακομιστή ιστού επηρεάζεται από μια ευπάθεια. Η λύση είναι να αναβαθμίσετε στην έκδοση PHP 8.2.7 ή νεότερη.

2. OpenSSL 1.1.1 < 1.1.1v Vulnerability: Η έκδοση OpenSSL που εντοπίστηκε στον διακομιστή είναι 1.1.1t. Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτήν την ευπάθεια . Συνιστάται η αναβάθμιση στην τελευταία έκδοση του OpenSSL για να διορθωθούν τυχόν ευπάθειες.

3. Apache mod_info /server-info Information Disclosure: Το έγγραφο προτείνει την ενημέρωση των αρχείων διαμόρφωσης του Apache για να απενεργοποιήσει το mod_info ή να περιορίσει την πρόσβαση σε συγκεκριμένους οικοδεσπότες.

4. Apache mod_status /server-status Information Disclosure: Όπως και με το mod_info, το έγγραφο προτείνει την ενημέρωση των αρχείων διαμόρφωσης του Apache για να απενεργοποιήσει το mod_status ή να περιορίσει την πρόσβαση σε συγκεκριμένους οικοδεσπότες.

5. **Browsable Web Directories**: Ορισμένοι κατάλογοι στον απομακρυσμένο διακομιστή ιστού είναι περιηγήσιμοι. Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα (Σελίδα 9). Συνιστάται η απενεργοποίηση της περιήγησης καταλόγων στον διακομιστή ιστού για να αποτραπεί η πρόσβαση σε ευαίσθητα αρχεία.

6. **HTTP TRACE / TRACK Methods Allowed**: Ο απομακρυσμένος διακομιστής ιστού υποστηρίζει τις μεθόδους TRACE και/ή TRACK. Το έγγραφο προτείνει την απενεργοποίηση αυτών των μεθόδων HTTP (Σελίδες 9-10).

7. OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτήν την ευπάθεια . Συνιστάται η αναβάθμιση στην τελευταία έκδοση του OpenSSL για να διορθωθούν τυχόν ευπάθειες.

8. Web Server Allows Password Auto-Completion: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα . Συνιστάται η απενεργοποίηση της αυτόματης συμπλήρωσης κωδικού πρόσβασης στον διακομιστή ιστού για να αυξηθεί η ασφάλεια.

9. Web Server Transmits Cleartext Credentials*: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα . Συνιστάται η χρήση κρυπτογραφημένων συνδέσεων (π.χ. HTTPS) για τη μετάδοση διαπιστευτηρίων, προκειμένου να αποτραπεί η παρακολούθηση των διαπιστευτηρίων από επιθέσεις.

10. Apache HTTP Server Version: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η αναβάθμιση στην τελευταία έκδοση του Apache HTTP Server για να διορθωθούν τυχόν ευπάθειες.

11. CGI Generic Injectable Parameter: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η χρήση τεχνικών ελέγχου εισόδου για να αποτραπεί η εισαγωγή επιβλαβών δεδομένων.

12. CGI Generic Tests Load Estimation: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η χρήση τεχνικών βελτιστοποίησης φόρτου για να διασφαλιστεί η αποδοτική λειτουργία του διακομιστή.

13. External URLs: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα . Συνιστάται η προσεκτική διαχείριση των εξωτερικών URL, προκειμένου να αποτραπεί η πρόσβαση σε επιβλαβείς ιστοσελίδες.

14. HTTP Methods Allowed (per directory): Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα . Συνιστάται η περιορισμένη χρήση των μεθόδων HTTP, προκειμένου να αποτραπεί η παραβίαση της ασφάλειας.

15. HTTP Server Type and Version: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα . Συνιστάται η αναβάθμιση στην τελευταία έκδοση του διακομιστή HTTP για να διορθωθούν τυχόν ευπάθειες.

16. HyperText Transfer Protocol (HTTP) Information: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα . Συνιστάται η προσεκτική διαχείριση των πληροφοριών HTTP, προκειμένου να αποτραπεί η παραβίαση της ασφάλειας.

17. HyperText Transfer Protocol (HTTP) Redirect Information: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα . Συνιστάται η προσεκτική διαχείριση των πληροφοριών ανακατεύθυνσης HTTP

18. HyperText Transfer Protocol (HTTP) Redirect Information: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η προσεκτική διαχείριση των πληροφοριών ανακατεύθυνσης HTTP προκειμένου να αποτραπεί η παραβίαση της ασφάλειας.

19. Nessus Scan Information: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η τακτική χρήση εργαλείων σάρωσης όπως το Nessus για τον εντοπισμό και την αντιμετώπιση τυχόν ευπαθειών.

20. OpenSSL Version Detection: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η αναβάθμιση στην τελευταία έκδοση του OpenSSL για να διορθωθούν τυχόν ευπάθειες.

21. PHP Version Detection: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η αναβάθμιση στην τελευταία έκδοση της PHP για να διορθωθούν τυχόν ευπάθειες.

22. Patch Report: Το έγγραφο προτείνει την εγκατάσταση των ενημερώσεων που αναφέρονται.

23. Web Application Cookies Not Marked Secure: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η χρήση ασφαλών cookies στην εφαρμογή ιστού, προκειμένου να αποτραπεί η παραβίαση της ασφάλειας.

24. Web Application Potentially Sensitive CGI Parameter Detection: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η προσεκτική διαχείριση των παραμέτρων CGI, προκειμένου να αποτραπεί η παραβίαση της ασφάλειας.

25. Web Server Directory Enumeration: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η απενεργοποίηση της απαρίθμησης καταλόγων στον διακομιστή ιστού για να αποτραπεί η πρόσβαση σε ευαίσθητα αρχεία.

26. Web Server Harvested Email Addresses: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η προσεκτική διαχείριση των διευθύνσεων email, προκειμένου να αποτραπεί η συλλογή τους από επιθετικούς.

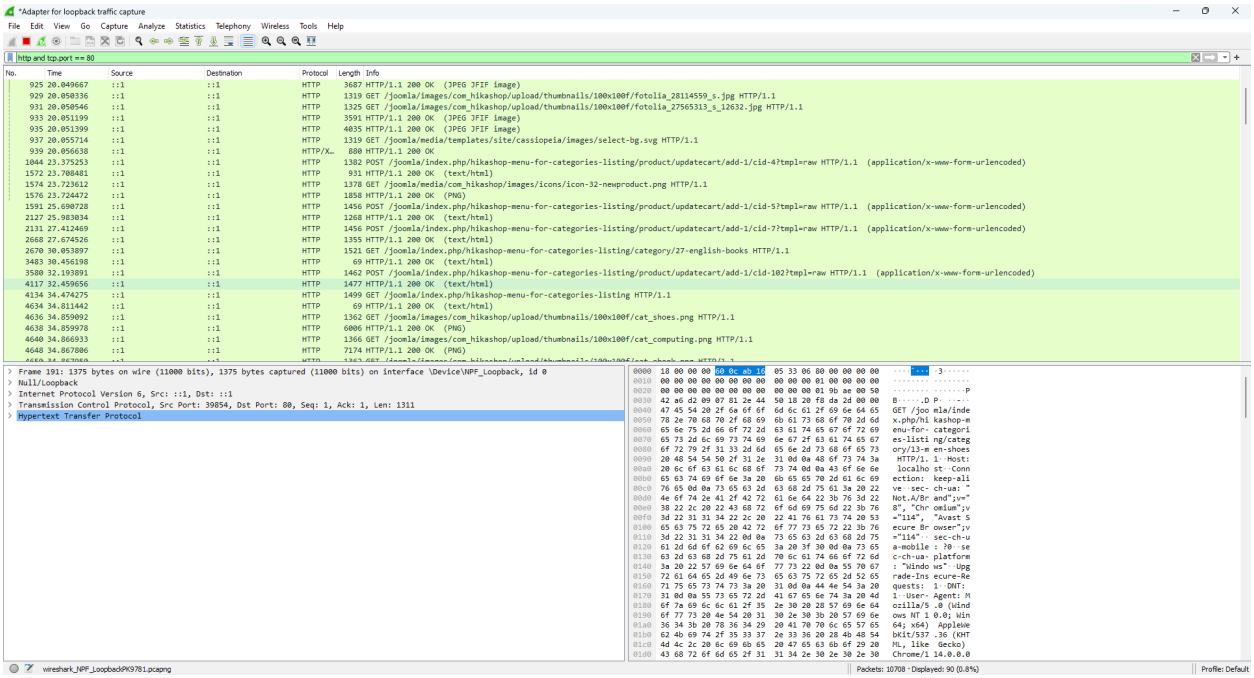
27. Web Server Office File Inventory: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η διασφάλιση ότι τα αρχεία Office που φιλοξενούνται στον διακομιστή ιστού δεν περιέχουν ευαίσθητες πληροφορίες και ότι είναι προσβάσιμα μόνο από χρήστες με έγκυρα διαπιστευτήρια.

28. Web mirroring: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η προσεκτική διαχείριση της διαδικασίας αντικατοπτρισμού του ιστότοπου, προκειμένου να αποτραπεί η παραβίαση της ασφάλειας.

29. Web Server Office File Inventory: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα. Συνιστάται η προσεκτική διαχείριση των αρχείων Office που αποθηκεύονται στον διακομιστή ιστού, προκειμένου να αποτραπεί η πρόσβαση σε ευαίσθητα αρχεία.

30. phpMyAdmin Detection: Το έγγραφο δεν παρέχει μια συγκεκριμένη λύση για αυτό το θέμα . Συνιστάται η αναβάθμιση στην τελευταία έκδοση του phpMyAdmin και η εφαρμογή των κατάλληλων μέτρων ασφαλείας για να αποτραπεί η παραβίαση της ασφάλειας.

Wireshark (Joomla Pen Tests)



Εικόνα 32:Παρακολούθηση Δικτύου Joomla e-shop με Wireshark - Εντοπισμός Πακέτων

Ακολουθεί μια ανάλυση των πληροφοριών που εξήχθησαν:

1. Το πρώτο πακέτο είναι ένα IGMPv2 Membership Report πακέτο που στέλνεται από την IP 192.168.2.4 στην IP 224.0.0.251. Το IGMPv2 χρησιμοποιείται για την διαχείριση ομαδικών μελών σε ένα δίκτυο.

2-5. Τα πακέτα 2 έως 5 είναι TCP πακέτα που στέλνονται μεταξύ των πορτών 17656 και 17657 στην localhost (127.0.0.1). Τα πακέτα PSH, ACK μεταφέρουν δεδομένα (ένα byte με την τιμή 31), ενώ τα πακέτα ACK επιβεβαιώνουν την παραλαβή των δεδομένων.

6-9. Τα πακέτα 6 έως 9 είναι παρόμοια με τα πακέτα 2 έως 5 αλλά η ακολουθία των αριθμών έχει αυξηθεί κατά ένα.

10-12. Τα πακέτα 10 έως 12 είναι TCP πακέτα που στέλνονται μεταξύ των πορτών 39852 και 8834 στην IPv6 localhost (::1). Το πακέτο SYN αρχίζει μια νέα TCP σύνδεση, το πακέτο SYN, ACK απαντά στο αρχικό SYN, και το πακέτο ACK επιβεβαιώνει την επιτυχή εγκατάσταση της σύνδεσης.

13. Το δέκατο τρίτο πακέτο είναι ένα IGMPv2 Membership Report πακέτο που στέλνεται από την IP 192.168.2.4 στην IP 239.192.152.143. Αυτό είναι παρόμοιο με το πρώτο πακέτο, αλλά για μια διαφορετική ομάδα.

14-15. Τα πακέτα 14 και 15 είναι παρόμοια με τα πακέτα 2 έως 5, αλλά η ακολουθία των αριθμών έχει αυξηθεί κατά ένα.

16-19. Τα πακέτα 16 έως 19 είναι TLSv1.3 πακέτα που στέλνονται μεταξύ των πορτών 39852 και 8834 στην IPv6 localhost. Τα πακέτα Client Hello και Server Hello αρχίζουν την διαδικασία χειραψίας του TLS, ενώ τα πακέτα ACK επιβεβαιώνουν την παραλαβή των πακέτων.

20-21. Τα πακέτα 20 και 21 είναι παρόμοια με τα πακέτα 16 έως 19, αλλά για την αλλαγή της κρυπτογραφικής συμφωνίας (Change Cipher Spec).

22. Το εικοστό δεύτερο πακέτο είναι ένα TCP FIN, ACK πακέτο που στέλνεται από την πόρτα 39852 στην πόρτα 8834 στην IPv6 localhost. Αυτό το πακέτο χρησιμοποιείται για να κλείσει μια TCP σύνδεση.

23-25. Τα πακέτα 23 και 25 είναι παρόμοια με τα προηγούμενα TCP πακέτα που στέλνονται μεταξύ των πορτών 17656 και 17657 στην localhost, αλλά η ακολουθία των αριθμών έχει αυξηθεί κατά ένα.

26-27. Τα πακέτα 26 και 27 είναι TCP πακέτα που στέλνονται μεταξύ των πορτών 8834 και 39852 στην IPv6 localhost. Το πακέτο PSH, ACK μεταφέρει δεδομένα, ενώ το πακέτο RST, ACK τερματίζει αμέσως την TCP σύνδεση.

28-29. Τα πακέτα 28 και 29 είναι TCP πακέτα που στέλνονται μεταξύ των πορτών 39853 και 8834 στην IPv6 localhost. Το πακέτο SYN αρχίζει μια νέα TCP σύνδεση, ενώ το πακέτο SYN, ACK απαντά στο αρχικό SYN.

Από την ανάλυση των πακέτων τα κυριότερα συμπεράσματα τα οποία εξάγονται είναι τα εξής:

1. Υπάρχει ενεργή επικοινωνία στο δίκτυο, τόσο σε IPv4 όσο και σε IPv6. Η επικοινωνία περιλαμβάνει τόσο την εσωτερική επικοινωνία (localhost) όσο και την επικοινωνία με άλλες συσκευές στο δίκτυο (192.168.2.4).

2. Υπάρχει ενεργή χρήση των πρωτοκόλλων TCP και IGMPv2. Το TCP χρησιμοποιείται για την αξιόπιστη μεταφορά δεδομένων, ενώ το IGMPv2 χρησιμοποιείται για την διαχείριση ομαδικών μελών στο δίκτυο.

3. Υπάρχει επίσης χρήση του πρωτοκόλλου TLSv1.3, το οποίο είναι ένα πρωτόκολλο ασφαλείας που χρησιμοποιείται για την προστασία της επικοινωνίας από επιθέσεις παρενόχλησης και παρακολούθησης.

4. Οι πόρτες που χρησιμοποιούνται για την TCP επικοινωνία είναι οι 17656, 17657, 39852, 39853 και 8834. Αυτές οι πόρτες μπορεί να αντιστοιχούν σε συγκεκριμένες εφαρμογές ή υπηρεσίες που τρέχουν στην συσκευή.

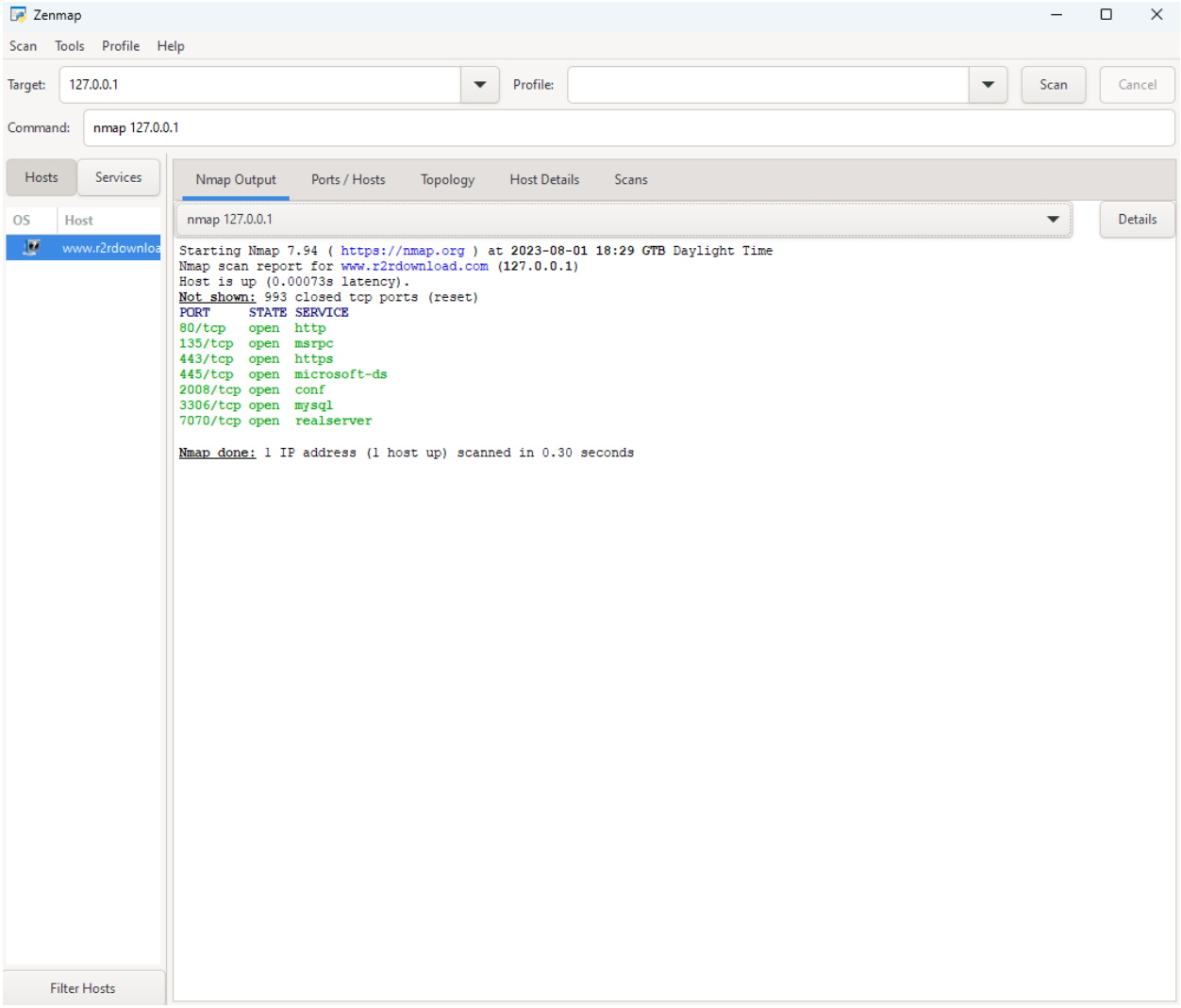
5. Οι διευθύνσεις IP που χρησιμοποιούνται για την IGMPv2 επικοινωνία είναι οι 224.0.0.251 και 239.192.152.143. Αυτές οι διευθύνσεις αντιστοιχούν σε ομάδες πολυδιανομής, που μπορεί να χρησιμοποιούνται για διάφορες υπηρεσίες, όπως η μετάδοση πολυμέσων.

Zenmap/Nmap (Joomla Pen Tests)

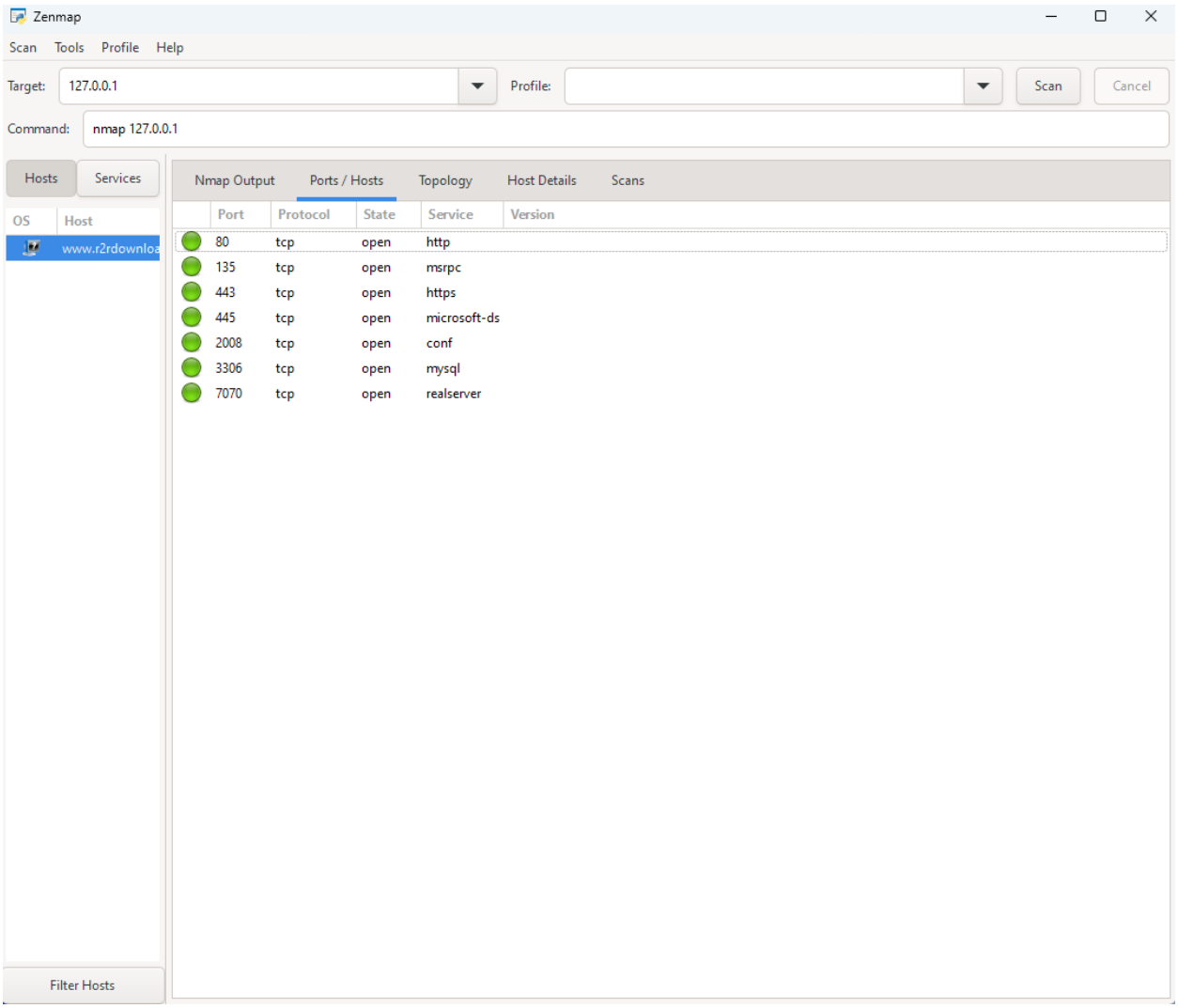
Το Nmap όπως προαναφέρθηκε χρησιμοποιείται για την ανακάλυψη συσκευών που λειτουργούν σε ένα δίκτυο και για την ανίχνευση των ανοιχτών θυρών σε συγκεκριμένες συσκευές. Με αυτό τον τρόπο, το Nmap παρέχει πληροφορίες για τις υπηρεσίες που τρέχουν σε ένα δίκτυο, τις θύρες που είναι ανοιχτές και πολλές άλλες χρήσιμες πληροφορίες ασφάλειας.

Βασική port scanning εντολή :

Nmap 127.0.0.1



Εικόνα 33Εκτέλεση Zenmap για Εύρεση Ανοιχτών Θυρών με Εγκατεστημένο το Joomla e-shop



Εικόνα 34:Zenmap - Αναλύει το Δίκτυο με με Εγκατεστημένο το Joomla e-shop - Αποτελέσματα Σάρωσης

<u>Το scan έδειξε τις παρακάτω θύρες ανοιχτές.</u>

<u>- Port 80/tcp</u>

<u>- Port 445/tcp</u>

<u>- Port 135/tcp</u>

<u>- Port 443/tcp</u>

<u>- Port 3306/tcp</u>

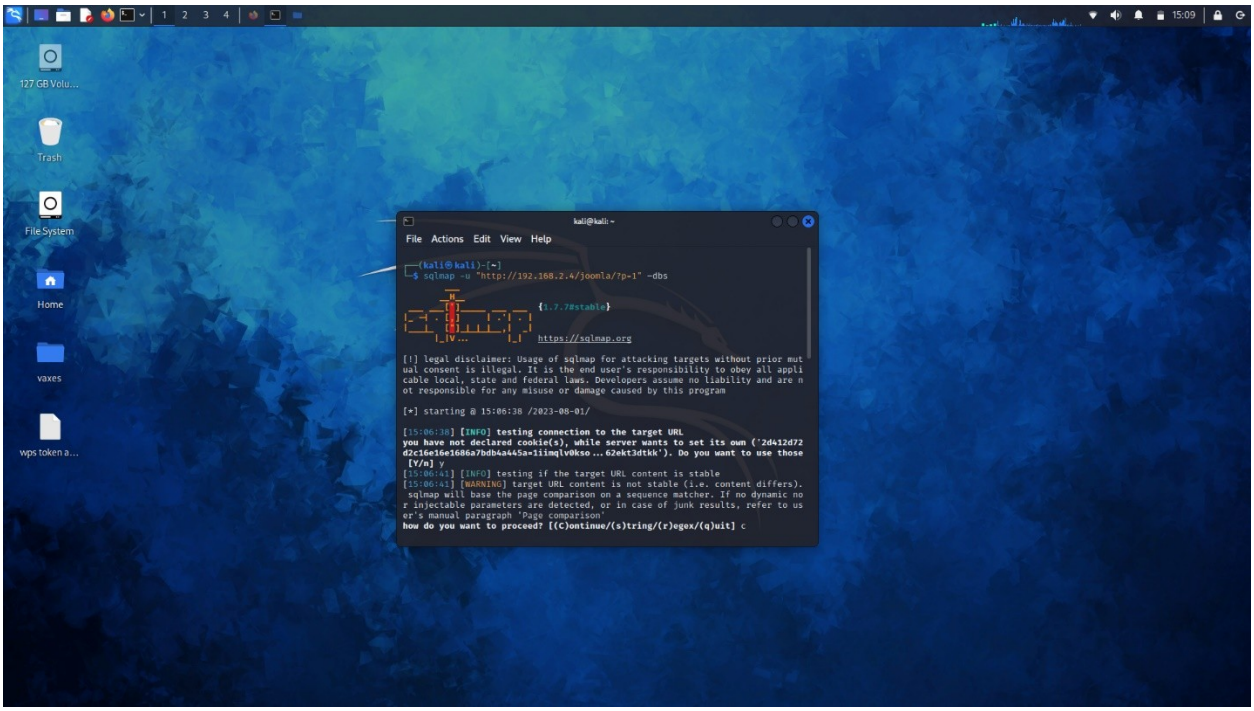
- Port 2008/tcp

- Port 7070/tcp

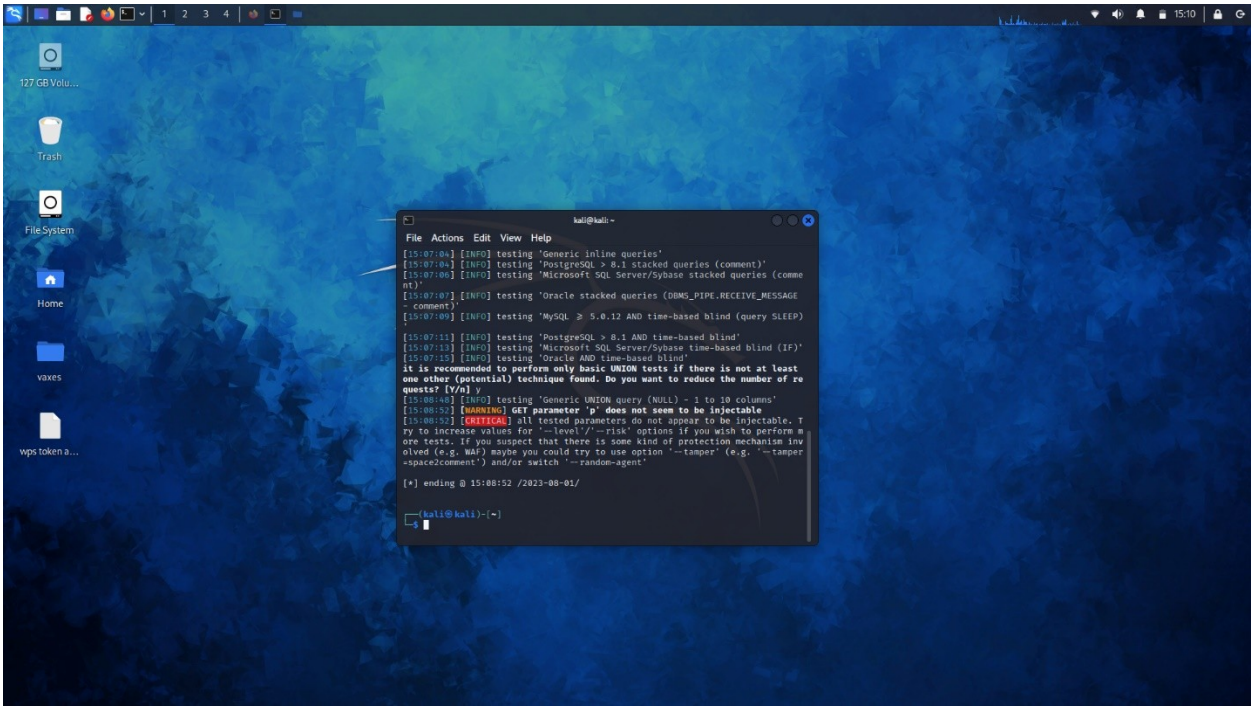
SQLMap (Joomla Pen Tests)

Το SQLMap είναι ένα ανοιχτού κώδικα εργαλείο που ανιχνεύει και εκμεταλλεύεται τις αδυναμίες SQL Injection σε εφαρμογές βάσεων δεδομένων. Οι επιθέσεις SQL Injection είναι μεταξύ των πιο διαδεδομένων και επικίνδυνων επιθέσεων στον κυβερνοχώρο, καθώς επιτρέπουν στους επιτιθέμενους να εκτελέσουν αυθαίρετες εντολές SQL μέσω μιας εφαρμογής web, προσβάλλοντας τη βάση δεδομένων. Το SQLMap αυτοματοποιεί τη διαδικασία ανακάλυψης, εκμετάλλευσης και λήψης των δεδομένων από τη βάση δεδομένων.

Με το SQLMap, οι χρήστες μπορούν να εντοπίζουν αδυναμίες στις εφαρμογές τους, να αναλύουν την κατασκευή της βάσης δεδομένων, να αποκτούν πρόσβαση σε ευαίσθητα δεδομένα ή ακόμη και να εκτελούν διαχειριστικές λειτουργίες. Παρότι είναι ένα ισχυρό εργαλείο στο χώρο της ασφάλειας της πληροφορικής προς το σκοπό της εκτίμησης κινδύνου και του ελέγχου εφαρμογών, θα πρέπει για λόγους ασφαλείας να χρησιμοποιείται με προσοχή και μόνο σε συστήματα όπου ο χρήστης έχει την κατάλληλη εξουσιοδότηση, προς αποφυγή πρόκλησης προβλημάτων.



Εικόνα 35:Χρήση SQLMap για Αναζήτηση SQL Ευπαθειών στο Joomla e-shop



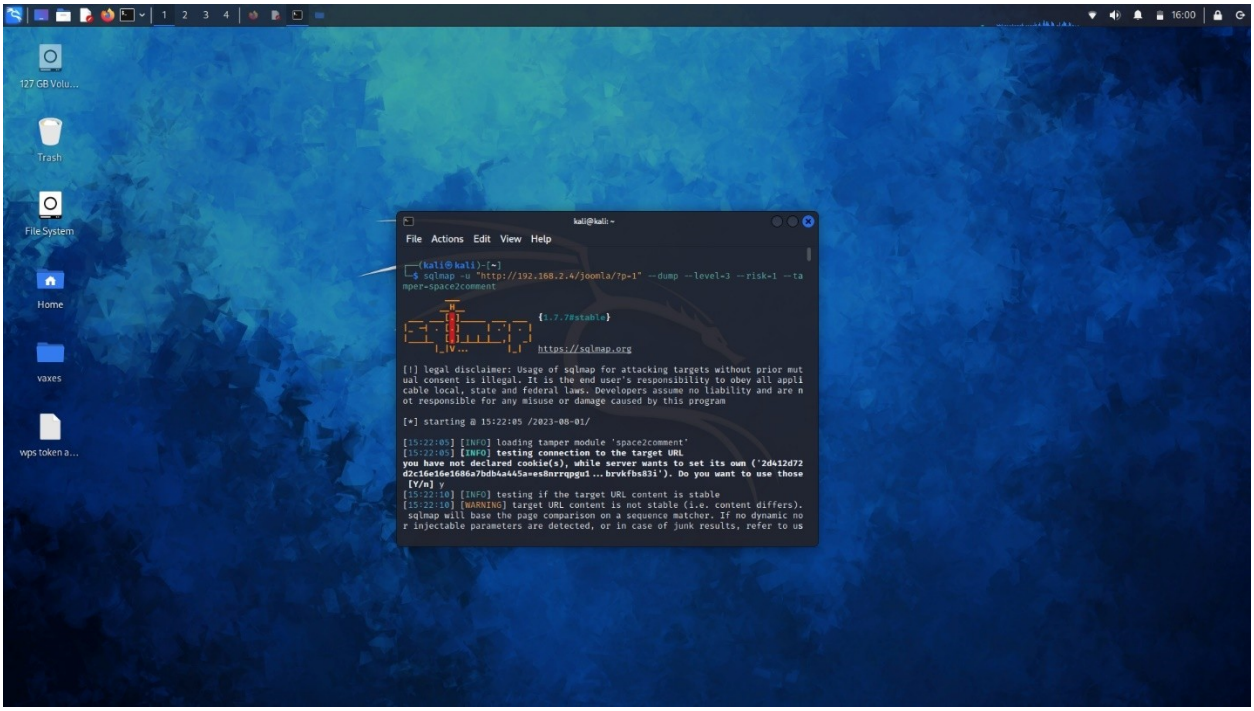
Εικόνα 36:Εκτέλεση SQLMap στο Joomla e-shop - Αναφορά Ευπαθειών SQL

Από την έξοδο της εντολής sqlmap, παρατηρούμε ότι η δοκιμαζόμενη σελίδα Joomla δεν φαίνεται να είναι ευάλωτη σε επιθέσεις SQL Injection. Το εργαλείο sqlmap διεξήγαγε μια σειρά

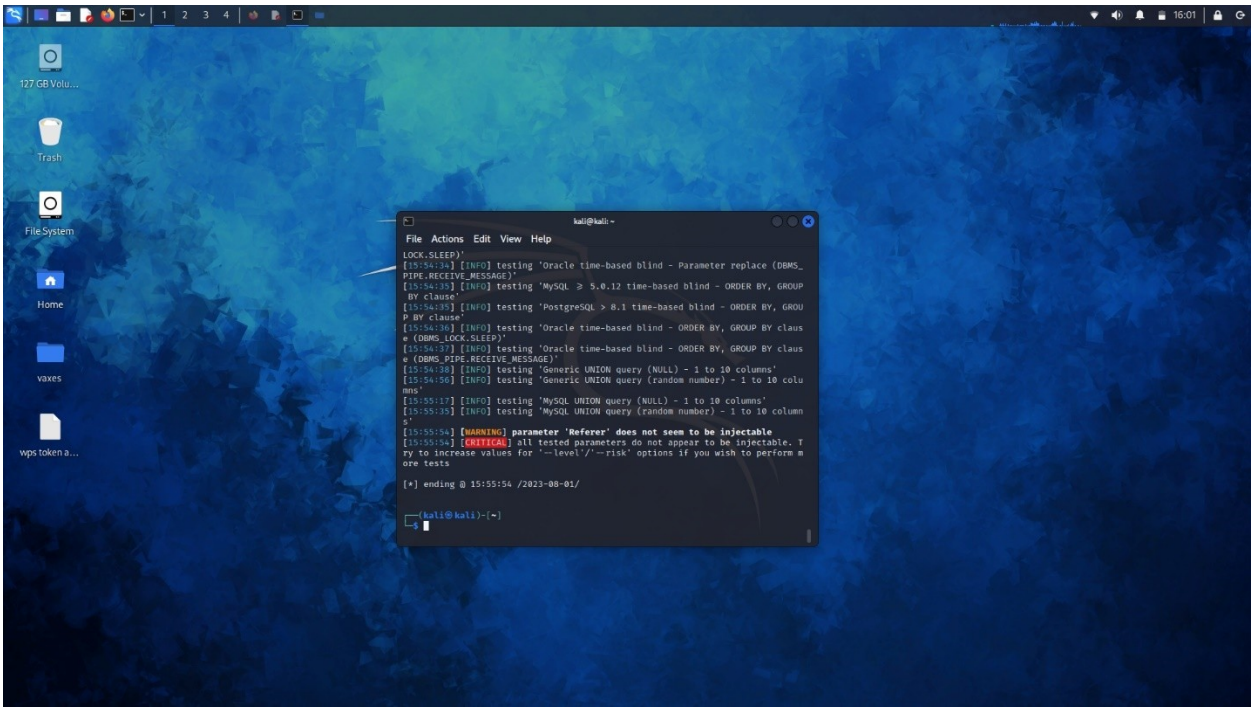
από δοκιμές χρησιμοποιώντας διάφορες τεχνικές επίθεσης SQL Injection, ωστόσο δεν ανακάλυψε καμία ευπάθεια (ΠΑΡΑΡΤΗΜΑ 2).

Αυτό μπορεί να υποδηλώνει ότι η σελίδα είναι καλά προστατευμένη ή ότι η παράμετρος 'p' που δοκιμάστηκε δεν είναι ευάλωτη σε επιθέσεις SQL Injection. Εναλλακτικά, μπορεί να υπάρχει κάποιος μηχανισμός προστασίας, όπως ένα Web Application Firewall (WAF), που αποτρέπει την επιτυχή εκτέλεση της επίθεσης.

Ακολουθεί η εκτέλεση της βασικής σάρωσης της SQL db του JOOMLA προς εύρεση πιθανών ευπαθειών με την εντολη ‘sqlmap -u "http://192.168.2.4/joomla/?p=1" --dump --level=3 --risk=1 --tamper=space2comment ‘



Εικόνα 37:Εκτέλεση SQLMap με Παράμετρο '--dump' για Αναζήτηση Ευπαθειών στην SQL db του Joomla



Εικόνα 38:Σάρωση Joomla db με SQLMap: Εκτεταμένη Εντολή για Αποτελεσματική Ανίχνευση

<u>Ανάλυση και επεξήγηση των πιο κρίσιμων σημείων της αναφοράς της εντολής</u>

Το εργαλείο δοκιμάζει διάφορες τεχνικές επίθεσης, όπως Boolean-based blind, Time-based blind, Error-based, UNION query και Stacked queries, σε διάφορες παραμέτρους, όπως 'p', 'User-Agent' και 'Referer'.

1. Χρήση Παραμετροποιημένων Ερωτημάτων: Αυτή είναι η πιο αποτελεσματική μέθοδος για την πρόληψη των επιθέσεων SQL Injection. Αντί να ενσωματώνετε τις τιμές των χρηστών απευθείας στα ερωτήματα, θα πρέπει να χρησιμοποιείτε παραμετροποιημένα ερωτήματα που σας επιτρέπουν να ορίσετε πού θα πρέπει να εμφανιστούν οι τιμές των χρηστών.

2. Χρήση ORM Πλαισίων: Τα Object-Relational Mapping (ORM) frameworks, όπως το Hibernate στην Java ή το Entity Framework στην .NET, μπορούν να προσφέρουν προστασία από

τις επιθέσεις SQL Injection, καθώς αυτά δημιουργούν ερωτήματα SQL δυναμικά με τη χρήση παραμετροποιημένων ερωτημάτων.

3. Επαλήθευση και Καθαρισμός Εισόδου: Πρέπει να επαληθεύετε πάντα τα δεδομένα εισόδου από τους χρήστες. Αυτό μπορεί να περιλαμβάνει την επαλήθευση του τύπου, του μήκους, της μορφής και του εύρους των δεδομένων.

4. Χρήση WAF: Ένα Web Application Firewall (WAF) μπορεί να βοηθήσει στην ανίχνευση και την πρόληψη των επιθέσεων SQL Injection.

5. Περιορισμός Δικαιωμάτων: Πρέπει να περιορίζετε τα δικαιώματα των χρηστών στη βάση δεδομένων στο ελάχιστο απαραίτητο. Αυτό μπορεί να μειώσει τις πιθανές ζημιές από μια επίθεση SQL Injection.

ΣΥΓΚΡΙΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Στόχος της παρούσας εργασίας, όπως προαναφέρθηκε, είναι η συγκέντρωση όλων των ευπαθειών που εντοπίστηκαν κατά τις δοκιμές και η παρουσίασή τους σε έναν συγκεντρωτικό πίνακα. Στην αριστερή στήλη έχουν καταχωρηθεί όλες οι δοκιμές που έγιναν και έχουν κατηγοριοποιηθεί βάσει των εργαλείων. Η δεύτερη στήλη αναφέρεται στην ανταπόκριση που είχε το ηλεκτρονικό κατάστημα σε Joomla και στην τρίτη στήλη το ηλεκτρονικό κατάστημα σε Wordpress.

Safety Features/Tools Used (Εργαλεία/Χαρακτηριστικά Ασφαλείας)	Joomla E-commerce VirtueMart Reaction	WordPress E-commerce WoocomerceReaction
OWASP ZAP Tests (Δοκιμές OWASP ZAP)		
Misconfiguration of different domains (Λανθασμένη Διαμόρφωση Διαφορετικών Domains)	Κανένα Πρόβλημα	Ναι
Hidden file detected (Ανιχνευμένο Κρυμμένο Αρχείο)	Κανένα Πρόβλημα	Ναι (2 περιπτώσεις)
Anti-clickjacking header (Κεφαλίδα Κατά του Clickjacking)	Λείπει (Μέσος Κίνδυνος)	Λείπει (Μέσος Κίνδυνος)
Large redirection detected (Μεγάλη Ανίχνευση Ανακατεύθυνσης)	Κανένα Πρόβλημα	Ναι
Inclusion of JS from different domain (Συμπερίληψη JS από Διαφορετικό Domain)	Κανένα Πρόβλημα	Ναι (13 περιπτώσεις)
HTTP X-Powered-By" response (Απάντηση HTTP "X-Powered-By")"	Διαρροή πληροφοριών (Χαμηλός Κίνδυνος)	Διαρροή πληροφοριών
HTTP Server" response (Απάντηση HTTP "Server")"	Κανένα Πρόβλημα	Διαρροή πληροφοριών
Strict Transport-Security header (Κεφαλίδα Αυστηρής Ασφάλειας Μεταφοράς)	Κανένα Πρόβλημα	Δεν έχει οριστεί
X-Content-Type-Options header (Κεφαλίδα X-Content-Type-Options)	Λείπει (Χαμηλός Κίνδυνος)	Λείπει (21 περιπτώσεις)
Information Disclosure - Comments (Διαρροή Πληροφοριών - Σχόλια)	Υποψίες Σχόλια (Ενημέρωση)	Ναι (9 περιπτώσεις)
Modern web application (Σύγχρονη Εφαρμογή Ιστού)	Ναι (Ενημέρωση)	Ναι
User Agent Fuzzer (Ανιχνευτής User Agent)	Κανένα Πρόβλημα	Ναι (12 περιπτώσεις)
Content Security Policy (CSP) header (Κεφαλίδα Πολιτικής Ασφάλειας Περιεχομένου)	Λείπει (Μέσος Κίνδυνος)	Λείπει (Μέσος Κίνδυνος)
Cross-Domain Communication (Επικοινωνία Διαφορετικών Domains)	Κανένα Πρόβλημα	Λανθασμένη διαμόρφωση
Vulnerable JS Library (Ευάλωτη Βιβλιοθήκη JS)	Ναι (Μέσος	Κανένα

	Κίνδυνος)	Πρόβλημα
CSRF Tokens (Διακριτικά CSRF)	Λείπει (Μέσος Κίνδυνος	Κανένα Πρόβλημα
Nessus Essentials (Βασικά Nessus)		
PHP 8.2.x < 8.2.7	ΥΨΗΛΟΣ	ΥΨΗΛΟΣ
OpenSSL 1.1.1 < 1.1.1v Vulnerability (Ευπάθεια OpenSSL 1.1.1 < 1.1.1v)	ΜΕΣΑΙΟΣ	ΜΕΣΑΙΟΣ
Apache mod_info /server-info Information Disclosure (Διαρροή Πληροφοριών Apache mod_info /server-info)	ΜΕΣΑΙΟΣ	ΜΕΣΑΙΟΣ
Apache mod_status /server-status Information Disclosure (Διαρροή Πληροφοριών Apache mod_status /server-status)	ΜΕΣΑΙΟΣ	ΜΕΣΑΙΟΣ
Browsable Web Directories (Περιηγήσιμοι Κατάλογοι Ιστού)	ΜΕΣΑΙΟΣ	ΜΕΣΑΙΟΣ
HTTP TRACE / TRACK Methods Allowed (Επιτρεπόμενες Μέθοδοι HTTP TRACE / TRACK)	ΜΕΣΑΙΟΣ	ΜΕΣΑΙΟΣ
OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities (Πολλαπλές Ευπάθειες OpenSSL 1.1.1 < 1.1.1u)	ΜΕΣΑΙΟΣ	ΜΕΣΑΙΟΣ
PHP expose_php Information Disclosure (Διαρροή Πληροφοριών PHP expose_php)		ΜΕΣΑΙΟΣ
WordPress User Enumeration (Απαρίθμηση Χρηστών WordPress)		ΜΕΣΑΙΟΣ
Web Server Allows Password Auto-Completion (Ο Διακομιστής Ιστού Επιτρέπει Αυτόματη Συμπλήρωση Κωδικού)	ΧΑΜΗΛΟΣ	ΧΑΜΗΛΟΣ
Web Server Transmits Cleartext Credentials (Ο Διακομιστής Ιστού Μεταδίδει Διακριτικά σε Απλό Κείμενο)	ΧΑΜΗΛΟΣ	ΧΑΜΗΛΟΣ
SQLmap (Δοκιμές SQLmap)		
Tested with sqlmap (Δοκιμασμένο με sqlmap)	Δοκιμασμένο	Δοκιμασμένο
Vulnerabilities Detected (Εντοπισμένες Ευπάθειες)	Δεν έχει καθοριστεί	Βρέθηκε
Protection parameters in user inputs (Παράμετροι προστασίας στις εισόδους χρηστών)	Κανένα Πρόβλημα	Συνιστάται
Use of prepared statements or ORM frameworks (Χρήση προετοιμασμένων δηλώσεων ή πλαισίων ORM)	Συνιστάται	Συνιστάται
Enabling Web Application Firewall (WAF) (Ενεργοποίηση Τείχους Προστασίας Εφαρμογής Ιστού)	Συνιστάται	Συνιστάται
Increasing --level or --risk for more tests (Αύξηση του --level ή --risk για περισσότερες δοκιμές)	Κανένα Πρόβλημα	Συνιστάται
Using --tamper and --random-agent (Χρήση --tamper και --random-agent)	Κανένα Πρόβλημα	Συνιστάται
Avoiding accessing non-existent URLs (Αποφυγή πρόσβασης σε μη υπάρχουσες διευθύνσεις URL)	Κανένα Πρόβλημα	Συνιστάται
Properly sanitizing user input (Σωστός καθαρισμός της εισόδου του χρήστη)	Κανένα Πρόβλημα	Συνιστάται

Using parameterized queries (Χρήση παραμετροποιημένων ερωτημάτων)	Πολύ Συνιστάται	Πολύ Συνιστάται
Cleaning user input (Καθαρισμός της εισόδου του χρήστη)	Συνιστάται	Συνιστάται
Input validation and sanitization (Επικύρωση και καθαρισμός εισόδου)	Πολύ Συνιστάται	Δεν αναφέρεται
Limiting database user rights (Περιορισμός δικαιωμάτων χρήστη βάσης δεδομένων)	Συνιστάται	Δεν αναφέρεται

Πίνακας 1: Συγκεντρωτικός πίνακας ευπαθειών Joomla και Wordpress

Ακολουθεί ένα υπόμνημα για την καλύτερη κατανόηση των απαντήσεων:

Όταν αναφερόμαστε στην απάντηση "Ναι", σημαίνει ότι έχει εντοπιστεί μια συγκεκριμένη ευπάθεια ή πρόβλημα στην εφαρμογή. Εάν η απάντηση εμφανίζεται ως "Ναι (Χ περιπτώσεις)", τότε το ζήτημα έχει παρατηρηθεί Χ φορές. Η έκφραση "Κανένα Πρόβλημα" χρησιμοποιείται όταν δεν εντοπίζεται κάποιο ζήτημα ή ευπάθεια. Η ένδειξη "Λείπει (Μέσος/Χαμηλός Κίνδυνος)" δηλώνει την απουσία ενός χαρακτηριστικού ασφάλειας που ενδέχεται να οδηγήσει σε κάποιον κίνδυνο. Με τον όρο "Διαρροή πληροφοριών" καταδεικνύεται ότι πληροφορίες οι οποίες θα έπρεπε να παραμείνουν κρυφές διέρρευσαν. "Δεν έχει οριστεί" σημαίνει πως δεν υπάρχει κάποια συγκεκριμένη απάντηση για το αποτέλεσμα του ελέγχου. Σχόλια που χαρακτηρίζονται ως "Υποψίες Σχόλια (Ενημέρωση)" υποδεικνύουν την ανάγκη για περαιτέρω εξέταση. Όταν κάτι έχει "Δοκιμαστεί", αυτό σημαίνει ότι το εργαλείο ή η δοκιμή έχει εφαρμοστεί. Ο όρος "Βρέθηκε" χρησιμοποιείται όταν έχουν ανιχνευτεί μία ή περισσότερες ευπάθειες. Τέλος, "Συνιστάται" και "Πολύ Συνιστάται" χρησιμοποιούνται για να δηλώσουν τη συνιστάμενη εφαρμογή μιας λύσης ή πρακτικής, με τον τελευταίο όρο να δηλώνει υψηλότερο βαθμό επείγουσας δράσης. Οι όροι "ΥΨΗΛΟΣ", "ΜΕΣΑΙΟΣ", και "ΧΑΜΗΛΟΣ" χρησιμοποιούνται για να καταδείξουν το επίπεδο κινδύνου μιας εντοπισμένης ευπάθειας.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία, πραγματοποιήθηκε μια εκτενής ανάλυση των πιθανών ευπαθειών που μπορεί να παρουσιάζουν οι ιστοσελίδες ενός ηλεκτρονικού καταστήματος με βάση τα δύο επικρατέστερα συστήματα διαχείρισης περιεχομένου ανοιχτού κώδικα (CMS), το WordPress και το Joomla. Η ανάλυση αυτή επέτρεψε την αναγνώριση των κοινών και των διαφορετικών ευπαθειών που παρουσιάζουν τα δύο αυτά συστήματα καθώς και την ανάπτυξη στρατηγικών για την αντιμετώπιση και την πρόληψη των επιθέσεων. Επιπρόσθετα, η ανάλυση που έγινε ανέδειξε τη σημασία που έχει σε έτοιμες πλατφόρμες CMS να είναι όλα τα πρόσθετα ενημερωμένα στην τελευταία τους έκδοση καθώς όσο πιο παλιά είναι η έκδοση κάποιου πρόσθετου, θέματος ή και της ίδιας της πλατφόρμας, τόσο μεγαλύτερος είναι ο κίνδυνος να υπάρχουν ευπάθειες λόγω της εξέλιξης των τρόπων επίθεσης καθώς και λόγω της πολυπλοκότητας των πληροφοριακών συστημάτων και των εφαρμογών. Σημαντική ωστόσο είναι και η παραμετροποίηση αρχείων και εφαρμογών, τουλάχιστον σε βασικό βαθμό, βάση των πιο γνωστών ευπαθειών και προτάσεων αντιμετώπισης τους, ώστε να διασφαλίζεται από ένα επίπεδο και πάνω η εύρυθμη λειτουργία των συστημάτων, των στοιχείων και των πληροφοριών τους.

Επιπλέον, η εργασία αυτή προσέφερε σημαντικές πληροφορίες για την ανάπτυξη και την εφαρμογή αποτελεσματικών στρατηγικών ασφαλείας σε περιβάλλοντα ηλεκτρονικού εμπορίου καθώς έγιναν προτάσεις αντιμετώπισης για την κάθε ευπάθεια που εντοπίστηκε. Η ανάλυση των αποτελεσμάτων και η αξιολόγηση των ευπαθειών που εντοπίστηκαν, επέτρεψαν την κατανόηση των κρίσιμων περιοχών που απαιτούν βελτίωση, ενώ παρείχαν επίσης σημαντικές πληροφορίες για την ανάπτυξη πιο ασφαλών και ανθεκτικών συστημάτων στο μέλλον. Σε κάθε κατηγορία δοκιμών υπάρχει μια ενότητα με προτεινόμενη λύση για την αντιμετώπιση τυχόν ευπαθειών.

Τέλος, η αξιολόγηση των εργαλείων δοκιμών διείσδυσης, όπως τα OWASP ZAP, Nessus, Zenmap, Wireshark, WPScan και SQLMap, κατέδειξε την σημαντικότητα υπάρξης τέτοιων εργαλείων, την αποτελεσματικότητα και την ευελιξία τους στην ανίχνευση και την ανάλυση ευπαθειών. Η εφαρμογή των εργαλείων αυτών σε πραγματικές συνθήκες, επέτρεψε την κατανόηση των δυνατοτήτων και των περιορισμών τους, ενώ συνέβαλε στην εξέταση των τρόπων με τους οποίους μπορούν να χρησιμοποιηθούν για την ενίσχυση της ασφάλειας των ιστοσελίδων και των εφαρμογών ηλεκτρονικών καταστημάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Silkalns, “WordPress statistics: How many websites use WordPress in 2023?,” *Colorlib*, Aug. 2023, [Online]. Available: https://colorlib.com/wp/wordpress-statistics/

[2] “2022 Website Threat Research Report,” *Sucuri*, Aug. 02, 2023. https://sucuri.net/reports/2022-hacked-website-report/

[3] OWASP (2020). OWASP Top Ten Web Application Security Risks. *OWASP.* [online] Available at: **https://owasp.org/www-project-top-ten/** (Accessed: 1 November 2020)

[4] J. Nazario, "Defense and Detection Strategies against Internet Worms," Norwood, MA, USA: Artech House, 2004.

[5] E. Rescorla, "SSL and TLS: Designing and Building Secure Systems," Boston, MA, USA: Addison-Wesley, 2001.

[6] R. Barnes, "Web Application Security: A Beginner’s Guide," New York, NY, USA: McGraw-Hill, 2011.

[7] D. Dittrich και S. Dietrich, "DDoS: Attacks and Defense," Norwood, MA, USA: Artech House, 2004

[8] PortSwigger (2020). Burp Suite - Application Security Testing Software. [online] Available at: **https://portswigger.net/burp** (Accessed: 1 November 2020)

[9] Πάγκαλος, Γ., Μαυρίδης Ι. (2002). *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων.* Θεσσαλονίκη: Εκδόσεις Ανικούλα.

[10] Gross, M. L., Canetti, D., & Vashdi, D. R. (Gross). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

[11] Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. *International Research Journal of Engineering and Technology*.

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ 1

1. **PHP 8.2.x < 8.2.7 (Σοβαρότητα: Υψηλή, CVSS V3.0: 7.5, Βαθμολογία VPR: 3.6, Plugin: 177511)**
2. **Ευπάθεια OpenSSL 1.1.1 < 1.1.1v (Σοβαρότητα: Μεσαία, CVSS V3.0: 5.9, Βαθμολογία VPR: 4.4, Plugin: 178475)**
3. **Apache mod_info /server-info Αποκάλυψη Πληροφοριών (Σοβαρότητα: Μεσαία, CVSS V3.0: 5.3, Plugin: 10678)**
4. **Apache mod_status /server-status Αποκάλυψη Πληροφοριών (Σοβαρότητα: Μεσαία, CVSS V3.0: 5.3, Plugin: 10677)**
5. **Περιηγήσιμοι Κατάλογοι Web (Σοβαρότητα: Μεσαία, CVSS V3.0: 5.3, Plugin: 40984)**
6. **Επιτρέπονται οι Μέθοδοι HTTP TRACE / TRACK (Σοβαρότητα: Μεσαία, CVSS V3.0: 5.3, Βαθμολογία VPR: 4.0, Plugin: 11213)**
7. **OpenSSL 1.1.1 < 1.1.1u Πολλαπλές Ευπάθειες (Σοβαρότητα: Μεσαία, CVSS V3.0: 5.3, Βαθμολογία VPR: 4.4, Plugin: 173260)**
8. **PHP expose_php Αποκάλυψη Πληροφοριών (Σοβαρότητα: Μεσαία, CVSS V3.0: 5.0, Plugin: 46803)**
9. **Απαρίθμηση Χρηστών WordPress (Σοβαρότητα: Μεσαία, CVSS V3.0: 5.0, Plugin: 90067)**
10. **Ο Διακομιστής Web Επιτρέπει την Αυτόματη Συμπλήρωση Κωδικού Πρόσβασης (Σοβαρότητα: Χαμηλή, CVSS: N/A, Plugin: 42057)**
11. **Ο Διακομιστής Web Μεταδίδει Διαφανείς Διαπιστευτήρια (Σοβαρότητα: Χαμηλή, CVSS V3.0: 2.6, Plugin: 26194)**
12. **Έκδοση Διακομιστή Apache HTTP (Plugin: 48204)**
13. **Γενική Ενέσιμη Παράμετρος CGI (Plugin: 47830)**

14. **Γενικές Δοκιμές Φόρτωσης CGI (όλες οι δοκιμές) (Plugin: 33817)**
15. **Εξωτερικές Διευθύνσεις URL (Plugin: 49704)**
16. **Επιτρεπόμενες Μέθοδοι HTTP (ανά κατάλογο) (Plugin: 43111)**
17. **Τύπος και Έκδοση Διακομιστή HTTP (Plugin: 10107)**
18. **Πληροφορίες Πρωτοκόλλου Μεταφοράς HyperText (HTTP) (Plugin: 24260)**
19. **Πληροφορίες Ανακατεύθυνσης Πρωτοκόλλου Μεταφοράς HyperText (HTTP) (Plugin: 91634)**
20. **Πληροφορίες Σάρωσης Nessus (Plugin: 19506)**
21. **Ανίχνευση Έκδοσης OpenSSL (Plugin: 57323)**
22. **Ανίχνευση Έκδοσης PHP (Plugin: 48243)**
23. **Έκθεση Επιδιορθώσεων (Plugin: 66334)**
24. **Τα Cookies της Εφαρμογής Web Έχουν Λήξει (Plugin: 100669)**
25. **Τα Cookies της Εφαρμογής Web Δεν Είναι Σημειωμένα ως HttpOnly (Plugin: 85601)**
26. **Τα Cookies της Εφαρμογής Web Δεν Είναι Σημειωμένα ως Ασφαλή (Plugin: 85602)**
27. **Ανίχνευση Πιθανώς Ευαίσθητης Παραμέτρου CGI της Εφαρμογής Web (Plugin: 40773)**
28. **Απαρίθμηση Καταλόγου Διακομιστή Web (Plugin: 11032)**
29. **Συγκεντρωμένες Διευθύνσεις Email Διακομιστή Web (Plugin: 49705)**
30. **Κατάλογος Αρχείων Office Διακομιστή Web (Plugin: 11419)**
31. **Αντιγραφή Ιστοσελίδας (Plugin: 10662)**
32. **Ανίχνευση WordPress (Plugin: 18297)**
33. **Ανίχνευση phpMyAdmin (Plugin: 17219)**

ΠΑΡΑΡΤΗΜΑ 2 – SQLMap

└─$ sqlmap -u "http://192.168.2.4/joomla/?p=1" --dump --level=3 --risk=1 --tamper=space2comment

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:22:05 /2023-08-01/

[15:22:05] [INFO] loading tamper module 'space2comment'

[15:22:05] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('2d412d72d2c16e16e1686a7bdb4a445a=es8nrrqpgu1...brvkfbs83i'). Do you want to use those [Y/n] y

[15:22:10] [INFO] testing if the target URL content is stable

[15:22:10] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'

how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c

[15:22:14] [INFO] testing if GET parameter 'p' is dynamic

[15:22:14] [WARNING] GET parameter 'p' does not appear to be dynamic

[15:22:15] [WARNING] heuristic (basic) test shows that GET parameter 'p' might not be injectable

[15:22:16] [INFO] testing for SQL injection on GET parameter 'p'

[15:22:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[15:22:17] [WARNING] reflective value(s) found and filtering out

[15:22:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'

[15:23:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'

[15:23:11] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'

[15:23:27] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'

[15:23:42] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'

[15:24:10] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'

[15:24:37] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'

[15:25:05] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[15:25:33] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[15:25:35] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'

[15:25:36] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'

[15:25:37] [INFO] testing 'Oracle boolean-based blind - Parameter replace'

[15:25:38] [INFO] testing 'Informix boolean-based blind - Parameter replace'

[15:25:40] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'

[15:25:41] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'

[15:25:43] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'

[15:25:43] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'

[15:25:44] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'

[15:25:44] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[15:25:46] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'

[15:25:46] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[15:25:46] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'

[15:25:49] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'

[15:25:51] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'

[15:25:54] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'

[15:26:19] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'

[15:26:34] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'

[15:26:49] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[15:26:59] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[15:27:08] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

[15:27:17] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[15:27:26] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[15:27:35] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[15:27:44] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'

[15:27:53] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'

[15:28:02] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[15:28:11] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)'

[15:28:20] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[15:28:29] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'

[15:28:38] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'

[15:28:47] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'

[15:28:56] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'

[15:29:05] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'

[15:29:14] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'

[15:29:23] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'

[15:29:24] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'

[15:29:24] [INFO] testing 'PostgreSQL error-based - Parameter replace'

[15:29:24] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'

[15:29:25] [INFO] testing 'Oracle error-based - Parameter replace'

[15:29:25] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'

[15:29:26] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'

[15:29:27] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'

[15:29:28] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'

[15:29:33] [INFO] testing 'Generic inline queries'

[15:29:33] [INFO] testing 'MySQL inline queries'

[15:29:34] [INFO] testing 'PostgreSQL inline queries'

[15:29:34] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'

[15:29:34] [INFO] testing 'Oracle inline queries'

[15:29:35] [INFO] testing 'SQLite inline queries'

[15:29:35] [INFO] testing 'Firebird inline queries'

[15:29:35] [INFO] testing 'ClickHouse inline queries'

[15:29:36] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'

[15:29:41] [INFO] testing 'MySQL >= 5.0.12 stacked queries'

[15:29:50] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'

[15:29:55] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[15:30:00] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'

[15:30:05] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[15:30:09] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'

[15:30:15] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[15:30:19] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[15:30:28] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'

[15:30:37] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'

[15:30:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'

[15:30:47] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'

[15:30:56] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'

[15:31:06] [INFO] testing 'MySQL AND time-based blind (ELT)'

[15:31:15] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[15:31:24] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[15:31:33] [INFO] testing 'Oracle AND time-based blind'

[15:31:42] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'

[15:31:42] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)'

[15:31:43] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'

[15:31:43] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'

[15:31:43] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'

[15:31:44] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'

[15:31:45] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'

[15:31:45] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'

[15:31:46] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'

it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y

[15:33:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[15:33:19] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'

[15:33:37] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[15:33:55] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'

[15:34:14] [WARNING] GET parameter 'p' does not seem to be injectable

[15:34:14] [INFO] testing if parameter 'User-Agent' is dynamic

[15:34:14] [WARNING] parameter 'User-Agent' does not appear to be dynamic

[15:34:14] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable

[15:34:15] [INFO] testing for SQL injection on parameter 'User-Agent'

[15:34:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[15:34:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'

[15:34:58] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'

[15:35:09] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'

[15:35:24] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'

[15:35:39] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'

[15:36:07] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'

[15:36:34] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'

[15:37:02] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[15:37:30] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[15:37:31] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'

[15:37:32] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'

[15:37:34] [INFO] testing 'Oracle boolean-based blind - Parameter replace'

[15:37:35] [INFO] testing 'Informix boolean-based blind - Parameter replace'

[15:37:36] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'

[15:37:37] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'

[15:37:39] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'

[15:37:40] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'

[15:37:41] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'

[15:37:42] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[15:37:45] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'

[15:37:47] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[15:37:47] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'

[15:37:50] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'

[15:37:52] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'

[15:37:55] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'

[15:38:22] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'

[15:38:37] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'

[15:38:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[15:39:02] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[15:39:11] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

[15:39:20] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[15:39:29] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[15:39:38] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[15:39:47] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'

[15:39:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'

[15:40:05] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[15:40:14] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)'

[15:40:23] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[15:40:32] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'

[15:40:41] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'

[15:40:50] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'

[15:40:59] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'

[15:41:09] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'

[15:41:18] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'

[15:41:27] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'

[15:41:28] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'

[15:41:28] [INFO] testing 'PostgreSQL error-based - Parameter replace'

[15:41:28] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'

[15:41:29] [INFO] testing 'Oracle error-based - Parameter replace'

[15:41:29] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'

[15:41:30] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'

[15:41:31] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'

[15:41:32] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'

[15:41:37] [INFO] testing 'Generic inline queries'

[15:41:37] [INFO] testing 'MySQL inline queries'

[15:41:38] [INFO] testing 'PostgreSQL inline queries'

[15:41:38] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'

[15:41:38] [INFO] testing 'Oracle inline queries'

[15:41:39] [INFO] testing 'SQLite inline queries'

[15:41:39] [INFO] testing 'Firebird inline queries'

[15:41:40] [INFO] testing 'ClickHouse inline queries'

[15:41:40] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'

[15:41:45] [INFO] testing 'MySQL >= 5.0.12 stacked queries'

[15:41:54] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'

[15:41:59] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[15:42:04] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'

[15:42:09] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[15:42:14] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'

[15:42:19] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[15:42:24] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[15:42:33] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'

[15:42:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'

[15:42:47] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'

[15:42:52] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'

[15:43:00] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'

[15:43:10] [INFO] testing 'MySQL AND time-based blind (ELT)'

[15:43:19] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[15:43:28] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[15:43:37] [INFO] testing 'Oracle AND time-based blind'

[15:43:46] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'

[15:43:46] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)'

[15:43:47] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'

[15:43:47] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'

[15:43:47] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'

[15:43:48] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'

[15:43:49] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'

[15:43:49] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'

[15:43:50] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'

[15:43:51] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[15:44:09] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'

[15:44:27] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[15:44:46] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'

[15:45:04] [WARNING] parameter 'User-Agent' does not seem to be injectable

[15:45:04] [INFO] testing if parameter 'Referer' is dynamic

[15:45:04] [WARNING] parameter 'Referer' does not appear to be dynamic

[15:45:05] [WARNING] heuristic (basic) test shows that parameter 'Referer' might not be injectable

[15:45:05] [INFO] testing for SQL injection on parameter 'Referer'

[15:45:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[15:45:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'

[15:45:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'

[15:46:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'

[15:46:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'

[15:46:30] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'

[15:46:58] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'

[15:47:26] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'

[15:47:54] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[15:48:22] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[15:48:24] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'

[15:48:25] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'

[15:48:26] [INFO] testing 'Oracle boolean-based blind - Parameter replace'

[15:48:27] [INFO] testing 'Informix boolean-based blind - Parameter replace'

[15:48:29] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'

[15:48:30] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'

[15:48:31] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'

[15:48:32] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'

[15:48:34] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'

[15:48:35] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[15:48:37] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'

[15:48:40] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'

[15:48:40] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'

[15:48:42] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'

[15:48:45] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'

[15:48:47] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'

[15:49:15] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'

[15:49:29] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'

[15:49:44] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[15:49:53] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[15:50:02] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

[15:50:11] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[15:50:20] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[15:50:28] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[15:50:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'

[15:50:46] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'

[15:50:55] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[15:51:04] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)'

[15:51:13] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'

[15:51:22] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'

[15:51:31] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'

[15:51:40] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'

[15:51:49] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'

[15:51:58] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'

[15:52:07] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'

[15:52:16] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'

[15:52:16] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'

[15:52:17] [INFO] testing 'PostgreSQL error-based - Parameter replace'

[15:52:17] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'

[15:52:17] [INFO] testing 'Oracle error-based - Parameter replace'

[15:52:18] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'

[15:52:19] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'

[15:52:19] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'

[15:52:20] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'

[15:52:25] [INFO] testing 'Generic inline queries'

[15:52:25] [INFO] testing 'MySQL inline queries'

[15:52:26] [INFO] testing 'PostgreSQL inline queries'

[15:52:26] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'

[15:52:27] [INFO] testing 'Oracle inline queries'

[15:52:27] [INFO] testing 'SQLite inline queries'

[15:52:27] [INFO] testing 'Firebird inline queries'

[15:52:28] [INFO] testing 'ClickHouse inline queries'

[15:52:28] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'

[15:52:33] [INFO] testing 'MySQL >= 5.0.12 stacked queries'

[15:52:42] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'

[15:52:47] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[15:52:52] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'

[15:52:56] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[15:53:01] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'

[15:53:06] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[15:53:11] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[15:53:20] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'

[15:53:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'

[15:53:34] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'

[15:53:39] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'

[15:53:48] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'

[15:53:57] [INFO] testing 'MySQL AND time-based blind (ELT)'

[15:54:06] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[15:54:15] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[15:54:23] [INFO] testing 'Oracle AND time-based blind'

[15:54:33] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'

[15:54:33] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)'

[15:54:33] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'

[15:54:34] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'

[15:54:34] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'

[15:54:35] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'

[15:54:35] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'

[15:54:36] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'

[15:54:37] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'

[15:54:38] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[15:54:56] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'

[15:55:17] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'

[15:55:35] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'

[15:55:54] [WARNING] parameter 'Referer' does not seem to be injectable

[15:55:54] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests

[*] ending @ 15:55:54 /2023-08-01/

ΠΑΡΑΡΤΗΜΑ 3

Με το πέρας της σάρωσης του SQLMap εμφάνισε τα εξης

┌──(kali㉿kali)-[~]

└─$ sqlmap -u "http://192.168.2.4/joomla/?p=1" –dbs

[*] starting @ 15:06:38 /2023-08-01/

[15:06:38] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('2d412d72d2c16e16e1686a7bdb4a445a=1iimqlv0kso...62ekt3dtkk'). Do you want to use those [Y/n] y

[15:06:41] [INFO] testing if the target URL content is stable

[15:06:41] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'

how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c

[15:06:45] [INFO] testing if GET parameter 'p' is dynamic

[15:06:45] [WARNING] GET parameter 'p' does not appear to be dynamic

[15:06:46] [WARNING] heuristic (basic) test shows that GET parameter 'p' might not be injectable

[15:06:47] [INFO] testing for SQL injection on GET parameter 'p'

[15:06:47] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[15:06:47] [WARNING] reflective value(s) found and filtering out

[15:06:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[15:06:56] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[15:06:58] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[15:07:00] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[15:07:02] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[15:07:04] [INFO] testing 'Generic inline queries'

[15:07:04] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[15:07:06] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[15:07:07] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[15:07:09] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[15:07:11] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[15:07:13] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[15:07:15] [INFO] testing 'Oracle AND time-based blind'

it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y

[15:08:48] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[15:08:52] [WARNING] GET parameter 'p' does not seem to be injectable

[15:08:52] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 15:08:52 /2023-08-01/

ΠΑΡΑΡΤΗΜΑ 4 – WSPscan

└─$ wpscan --url http://192.168.2.4/wordpress

WordPress Security Scanner by the WPScan Team

Version 3.8.22

Sponsored by Automattic - https://automattic.com/

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.2.4/wordpress/ [192.168.2.4]

[+] Started: Fri Jul 28 20:34:44 2023

Interesting Finding(s):

[+] Headers

| Interesting Entries:

| - Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

| - X-Powered-By: PHP/8.2.4

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.2.4/wordpress/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.2.4/wordpress/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.2.4/wordpress/wp-content/uploads/

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.2.4/wordpress/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.2.2 identified (Latest, released on 2023-05-20).

| Found By: Emoji Settings (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=6.2.2'

| Confirmed By: Meta Generator (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'WordPress 6.2.2'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] woocommerce

| Location: http://192.168.2.4/wordpress/wp-content/plugins/woocommerce/

| Last Updated: 2023-07-17T22:14:00.000Z

| [!] The version is out of date, the latest version is 7.9.0

|

| Found By: Meta Generator (Passive Detection)

|

| Version: 7.8.2 (100% confidence)

| Found By: Meta Generator (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'WooCommerce 7.8.2'

| Confirmed By:

| Readme - Stable Tag (Aggressive Detection)

| - http://192.168.2.4/wordpress/wp-content/plugins/woocommerce/readme.txt

| Readme - ChangeLog Section (Aggressive Detection)

| - http://192.168.2.4/wordpress/wp-content/plugins/woocommerce/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 28 20:35:48 2023

[+] Requests Done: 166

[+] Cached Requests: 4

[+] Data Sent: 43.934 KB

[+] Data Received: 341.629 KB

[+] Memory used: 211.75 MB

[+] Elapsed time: 00:01:03

WordPress Security Scanner by the WPScan Team

Version 3.8.22

Sponsored by Automattic - https://automattic.com/

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.2.4/wordpress/ [192.168.2.4]

[+] Started: Fri Jul 28 20:43:45 2023

Interesting Finding(s):

[+] Headers

| Interesting Entries:

| - Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

| - X-Powered-By: PHP/8.2.4

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.2.4/wordpress/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.2.4/wordpress/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.2.4/wordpress/wp-content/uploads/

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.2.4/wordpress/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.2.2 identified (Latest, released on 2023-05-20).

| Found By: Emoji Settings (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=6.2.2'

| Confirmed By: Meta Generator (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'WordPress 6.2.2'

[i] The main theme could not be detected.

[+] Enumerating Most Popular Plugins (via Passive Methods)

[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] woocommerce

| Location: http://192.168.2.4/wordpress/wp-content/plugins/woocommerce/

| Last Updated: 2023-07-17T22:14:00.000Z

| [!] The version is out of date, the latest version is 7.9.0

|

| Found By: Meta Generator (Passive Detection)

|

| Version: 7.8.2 (100% confidence)

| Found By: Meta Generator (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'WooCommerce 7.8.2'

| Confirmed By:

| Readme - Stable Tag (Aggressive Detection)

| - http://192.168.2.4/wordpress/wp-content/plugins/woocommerce/readme.txt

| Readme - ChangeLog Section (Aggressive Detection)

| - http://192.168.2.4/wordpress/wp-content/plugins/woocommerce/readme.txt

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 28 20:43:49 2023

[+] Requests Done: 2

[+] Cached Requests: 29

[+] Data Sent: 640 B

[+] Data Received: 46.556 KB

[+] Memory used: 220.723 MB

[+] Elapsed time: 00:00:03

.

Με το πέρας της σάρωσης το WPScan εμφάνισε τα εξής :

$ wpscan --url http://192.168.2.4/wordpress --enumerate t

WordPress Security Scanner by the WPScan Team

Version 3.8.22

Sponsored by Automattic - https://automattic.com/

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.2.4/wordpress/ [192.168.2.4]

[+] Started: Fri Jul 28 21:05:40 2023

Interesting Finding(s):

[+] Headers

| Interesting Entries:

| - Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

| - X-Powered-By: PHP/8.2.4

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.2.4/wordpress/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.2.4/wordpress/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.2.4/wordpress/wp-content/uploads/

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.2.4/wordpress/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.2.2 identified (Latest, released on 2023-05-20).

| Found By: Emoji Settings (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=6.2.2'

| Confirmed By: Meta Generator (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'WordPress 6.2.2'

[i] The main theme could not be detected.

[+] Enumerating Most Popular Themes (via Passive and Aggressive Methods)

Checking Known Locations - Time: 00:00:04 <> (11 / 400) 2.75% ETA: 00:02:3 Checking Known Locations - Time: 00:00:04 <> (12 / 400) 3.00% ETA: 00:02:3 Checking Known Locations - Time: 00:00:05 <> (16 / 400) 4.00% ETA: 00:02:1 Checking Known Locations - Time: 00:00:06 <> (17 / 400) 4.25% ETA: 00:02:1 Checking Known Locations - Time: 00:00:07 <> (21 / 400) 5.25% ETA: 00:02:0 Checking Known Locations - Time: 00:00:07 <> (22 / 400) 5.50% ETA: 00:02:1 Checking Known Locations - Time: 00:00:08 <> (26 / 400) 6.50% ETA: 00:02:0 Checking Known Locations - Time: 00:00:08 <> (27 / 400) 6.75% ETA: 00:02:0 Checking Known Locations - Time: 00:00:10 <> (31 / 400) 7.75% ETA: 00:02:0 Checking Known Locations - Time: 00:00:10 <> (32 / 400) 8.00% ETA: 00:02:0 Checking Known Locations - Time: 00:00:11 <> (36 / 400) 9.00% ETA: 00:01:5 Checking Known Locations - Time: 00:00:11 <> (37 / 400) 9.25% ETA: 00:01:5 Checking Known Locations - Time: 00:00:12 <> (41 / 400) 10.25% ETA: 00:01:5 Checking Known Locations - Time: 00:00:13 <> (42 / 400) 10.50% ETA: 00:01:5 Checking Known Locations - Time: 00:00:14 <> (46 / 400) 11.50% ETA: 00:01:5 Checking Known Locations - Time: 00:00:14 <> (47 / 400) 11.75% ETA: 00:01:5 Checking Known Locations - Time: 00:00:15 <> (51 / 400) 12.75% ETA: 00:01:4 Checking Known Locations - Time: 00:00:16 <> (52 / 400) 13.00% ETA: 00:01:4 Checking Known Locations - Time: 00:00:16 <> (53 / 400) 13.25% ETA: 00:01:4 Checking Known Locations - Time: 00:00:16 <> (55 / 400) 13.75% ETA: 00:01:4 Checking Known Locations - Time: 00:00:17 <> (56 / 400) 14.00% ETA: 00:01:4 Checking Known Locations - Time: 00:00:17 <> (57 / 400) 14.25% ETA: 00:01:4 Checking Known Locations - Time: 00:00:19 <> (61 / 400) 15.25% ETA: 00:01:4 Checking Known Locations - Time: 00:00:19 <> (62 / 400) 15.50% ETA: 00:01:4 Checking Known Locations - Time: 00:00:19 <> (63 / 400) 15.75% ETA: 00:01:4 Checking Known Locations - Time: 00:00:19 <> (64 / 400) 16.00%

ETA: 00:01:4 Checking Known Locations - Time: 00:00:19 <> (65 / 400) 16.25% ETA: 00:01:3 Checking Known Locations - Time: 00:00:20 <> (66 / 400) 16.50% ETA: 00:01:4 Checking Known Locations - Time: 00:00:20 <> (67 / 400) 16.75% ETA: 00:01:4 Checking Known Locations - Time: 00:00:20 <> (68 / 400) 17.00% ETA: 00:01:4 Checking Known Locations - Time: 00:00:20 <> (69 / 400) 17.25% ETA: 00:01:4 Checking Known Locations - Time: 00:00:20 <> (70 / 400) 17.50% ETA: 00:01:3 Checking Known Locations - Time: 00:00:22 <> (71 / 400) 17.75% ETA: 00:01:4 Checking Known Locations - Time: 00:00:22 <> (74 / 400) 18.50% ETA: 00:01:3 Checking Known Locations - Time: 00:00:22 <> (75 / 400) 18.75% ETA: 00:01:3 Checking Known Locations - Time: 00:00:23 <> (76 / 400) 19.00% ETA: 00:01:4 Checking Known Locations - Time: 00:00:23 <> (80 / 400) 20.00% ETA: 00:01:3 Checking Known Locations - Time: 00:00:25 <> (81 / 400) 20.25% ETA: 00:01:4 Checking Known Locations - Time: 00:00:25 <> (82 / 400) 20.50% ETA: 00:01:4 Checking Known Locations - Time: 00:00:25 <> (83 / 400) 20.75% ETA: 00:01:3 Checking Known Locations - Time: 00:00:26 <> (84 / 400) 21.00% ETA: 00:01:3 Checking Known Locations - Time: 00:00:26 <> (85 / 400) 21.25% ETA: 00:01:3 Checking Known Locations - Time: 00:00:27 <> (86 / 400) 21.50% ETA: 00:01:4 Checking Known Locations - Time: 00:00:27 <> (89 / 400) 22.25% ETA: 00:01:3 Checking Known Locations - Time: 00:00:27 <> (90 / 400) 22.50% ETA: 00:01:3 Checking Known Locations - Time: 00:00:29 <> (91 / 400) 22.75% ETA: 00:01:3 Checking Known Locations - Time: 00:00:29 <> (95 / 400) 23.75% ETA: 00:01:3 Checking Known Locations - Time: 00:00:31 <> (96 / 400) 24.00% ETA: 00:01:3 Checking Known Locations - Time: 00:00:31 <> (100 / 400) 25.00% ETA: 00:01: Checking Known Locations - Time: 00:00:32 <> (101 / 400) 25.25% ETA: 00:01: Checking Known Locations - Time: 00:00:32 <> (105 / 400) 26.25% ETA: 00:01: Checking Known Locations - Time: 00:00:34 <> (106 / 400) 26.50% ETA: 00:01: Checking Known Locations - Time: 00:00:36 <> (111 / 400) 27.75% ETA: 00:01: Checking Known Locations - Time: 00:00:37 <> (116 / 400) 29.00% ETA: 00:01: Checking Known Locations - Time: 00:00:39 <> (121 / 400) 30.25% ETA: 00:01: Checking Known Locations - Time: 00:00:39 <> (123 / 400) 30.75% ETA: 00:01: Checking Known Locations - Time: 00:00:39 <> (125 / 400) 31.25% ETA: 00:01: Checking Known Locations - Time: 00:00:40 <> (126 / 400) 31.50% ETA: 00:01: Checking Known Locations - Time: 00:00:42 <> (131 / 400) 32.75% ETA: 00:01: Checking Known Locations - Time: 00:00:43 <> (136 / 400) 34.00% ETA: 00:01: Checking Known Locations - Time: 00:00:45 <> (141 / 400)

35.25% ETA: 00:01: Checking Known Locations - Time: 00:00:45 <> (145 / 400) 36.25% ETA: 00:01: Checking Known Locations - Time: 00:00:47 <> (146 / 400) 36.50% ETA: 00:01: Checking Known Locations - Time: 00:00:48 <> (151 / 400) 37.75% ETA: 00:01: Checking Known Locations - Time: 00:00:50 <> (156 / 400) 39.00% ETA: 00:01: Checking Known Locations - Time: 00:00:51 <> (160 / 400) 40.00% ETA: 00:01: Checking Known Locations - Time: 00:00:51 <> (161 / 400) 40.25% ETA: 00:01: Checking Known Locations - Time: 00:00:52 <> (165 / 400) 41.25% ETA: 00:01: Checking Known Locations - Time: 00:00:53 <> (166 / 400) 41.50% ETA: 00:01: Checking Known Locations - Time: 00:00:54 <> (170 / 400) 42.50% ETA: 00:01: Checking Known Locations - Time: 00:00:54 <> (171 / 400) 42.75% ETA: 00:01: Checking Known Locations - Time: 00:00:56 <> (175 / 400) 43.75% ETA: 00:01: Checking Known Locations - Time: 00:00:56 <> (176 / 400) 44.00% ETA: 00:01: Checking Known Locations - Time: 00:00:57 <> (180 / 400) 45.00% ETA: 00:01: Checking Known Locations - Time: 00:00:57 <> (181 / 400) 45.25% ETA: 00:01: Checking Known Locations - Time: 00:00:58 <> (185 / 400) 46.25% ETA: 00:01: Checking Known Locations - Time: 00:00:59 <> (186 / 400) 46.50% ETA: 00:01: Checking Known Locations - Time: 00:01:00 <> (190 / 400) 47.50% ETA: 00:01: Checking Known Locations - Time: 00:01:01 <> (191 / 400) 47.75% ETA: 00:01: Checking Known Locations - Time: 00:01:01 <> (193 / 400) 48.25% ETA: 00:01: Checking Known Locations - Time: 00:01:01 <> (194 / 400) 48.50% ETA: 00:01: Checking Known Locations - Time: 00:01:02 <> (195 / 400) 48.75% ETA: 00:01: Checking Known Locations - Time: 00:01:02 <> (196 / 400) 49.00% ETA: 00:01: Checking Known Locations - Time: 00:01:02 <> (199 / 400) 49.75% ETA: 00:01: Checking Known Locations - Time: 00:01:03 <> (200 / 400) 50.00% ETA: 00:01: Checking Known Locations - Time: 00:01:04 <> (201 / 400) 50.25% ETA: 00:01: Checking Known Locations - Time: 00:01:05 <> (205 / 400) 51.25% ETA: 00:01: Checking Known Locations - Time: 00:01:05 <> (206 / 400) 51.50% ETA: 00:01: Checking Known Locations - Time: 00:01:06 <> (210 / 400) 52.50% ETA: 00:01: Checking Known Locations - Time: 00:01:07 <> (211 / 400) 52.75% ETA: 00:01: Checking Known Locations - Time: 00:01:08 <> (215 / 400) 53.75% ETA: 00:00: Checking Known Locations - Time: 00:01:08 <> (216 / 400) 54.00% ETA: 00:00: Checking Known Locations - Time: 00:01:08 <> (219 / 400) 54.75% ETA: 00:00: Checking Known Locations - Time: 00:01:09 <> (220 / 400) 55.00% ETA: 00:00: Checking Known Locations - Time: 00:01:09 <> (221 / 400) 55.25% ETA: 00:00: Checking Known Locations - Time: 00:01:09 <>

(224 / 400) 56.00% ETA: 00:00: Checking Known Locations - Time: 00:01:11 <> (225 / 400) 56.25% ETA: 00:00: Checking Known Locations - Time: 00:01:11 <> (226 / 400) 56.50% ETA: 00:00: Checking Known Locations - Time: 00:01:11 <> (228 / 400) 57.00% ETA: 00:00: Checking Known Locations - Time: 00:01:12 <> (230 / 400) 57.50% ETA: 00:00: Checking Known Locations - Time: 00:01:12 <> (231 / 400) 57.75% ETA: 00:00: Checking Known Locations - Time: 00:01:12 <> (232 / 400) 58.00% ETA: 00:00: Checking Known Locations - Time: 00:01:12 <> (233 / 400) 58.25% ETA: 00:00: Checking Known Locations - Time: 00:01:12 <> (234 / 400) 58.50% ETA: 00:00: Checking Known Locations - Time: 00:01:14 <> (235 / 400) 58.75% ETA: 00:00: Checking Known Locations - Time: 00:01:14 <> (239 / 400) 59.75% ETA: 00:00: Checking Known Locations - Time: 00:01:15 <> (240 / 400) 60.00% ETA: 00:00: Checking Known Locations - Time: 00:01:17 <> (245 / 400) 61.25% ETA: 00:00: Checking Known Locations - Time: 00:01:17 <> (249 / 400) 62.25% ETA: 00:00: Checking Known Locations - Time: 00:01:18 <> (250 / 400) 62.50% ETA: 00:00: Checking Known Locations - Time: 00:01:20 <> (ETA: 00:00: Checking Known Locations - Time: 00:01:25 <> (275 / 400) 68.75% ETA: 00:00: Checking Known Locations - Time: 00:01:27 <> (280 / 400) 70.00% ETA: 00:00: Checking Known Locations - Time: 00:01:28 <> (285 / 400) 71.25% ETA: 00:00: Checking Known Locations - Time: 00:01:30 <> (290 / 400) 72.50% ETA: 00:00: Checking Known Locations - Time: 00:01:30 <> (294 / 400) 73.50% ETA: 00:00: Checking Known Locations - Time: 00:01:32 <> (295 / 400) 73.75% ETA: 00:00: Checking Known Locations - Time: 00:01:33 <> (300 / 400) 75.00% ETA: 00:00: Checking Known Locations - Time: 00:01:35 <> (305 / 400) 76.25% ETA: 00:00: Checking Known Locations - Time: 00:01:35 <> (306 / 400) 76.50% ETA: 00:00: Checking Known Locations - Time: 00:01:35 <> (308 / 400) 77.00% ETA: 00:00: Checking Known Locations - Time: 00:01:36 <> (309 / 400) 77.25% ETA: 00:00: Checking Known Locations - Time: 00:01:37 <> (310 / 400) 77.50% ETA: 00:00: Checking Known Locations - Time: 00:01:37 <> (312 / 400) 78.00% ETA: 00:00: Checking Known Locations - Time: 00:01:37 <> (313 / 400) 78.25% ETA: 00:00: Checking Known Locations - Time: 00:01:37 <> (314 / 400) 78.50% ETA: 00:00: Checking Known Locations - Time: 00:01:39 <> (315 / 400) 78.75% ETA: 00:00: Checking Known Locations - Time: 00:01:39 <> (319 / 400) 79.75% ETA: 00:00: Checking Known Locations - Time: 00:01:40 <> (320 / 400) 80.00% ETA: 00:00: Checking Known Locations - Time: 00:01:41 <> (324 / 400) 81.00% ETA: 00:00: Checking Known Locations - Time: 00:01:42 <> (325 / 400)

81.25% ETA: 00:00: Checking Known Locations - Time: 00:01:42 <> (329 / 400) 82.25% ETA: 00:00: Checking Known Locations - Time: 00:01:44 <> (330 / 400) 82.50% ETA: 00:00: Checking Known Locations - Time: 00:01:44 <> (334 / 400) 83.50% ETA: 00:00: Checking Known Locations - Time: 00:01:45 <> (335 / 400) 83.75% ETA: 00:00: Checking Known Locations - Time: 00:01:45 <> (338 / 400) 84.50% ETA: 00:00: Checking Known Locations - Time: 00:01:45 <> (339 / 400) 84.75% ETA: 00:00: Checking Known Locations - Time: 00:01:46 <> (340 / 400) 85.00% ETA: 00:00: Checking Known Locations - Time: 00:01:47 <> (344 / 400) 86.00% ETA: 00:00: Checking Known Locations - Time: 00:01:48 <> (345 / 400) 86.25% ETA: 00:00: Checking Known Locations - Time: 00:01:48 <> (349 / 400) 87.25% ETA: 00:00: Checking Known Locations - Time: 00:01:49 <> (350 / 400) 87.50% ETA: 00:00: Checking Known Locations - Time: 00:01:50 <> (353 / 400) 88.25% ETA: 00:00: Checking Known Locations - Time: 00:01:50 <> (354 / 400) 88.50% ETA: 00:00: Checking Known Locations - Time: 00:01:51 <> (355 / 400) 88.75% ETA: 00:00: Checking Known Locations - Time: 00:01:51 <> (358 / 400) 89.50% ETA: 00:00: Checking Known Locations - Time: 00:01:52 <> (359 / 400) 89.75% ETA: 00:00: Checking Known Locations - Time: 00:01:53 <> (360 / 400) 90.00% ETA: 00:00: Checking Known Locations - Time: 00:01:53 <> (363 / 400) 90.75% ETA: 00:00: Checking Known Locations - Time: 00:01:53 <> (364 / 400) 91.00% ETA: 00:00: Checking Known Locations - Time: 00:01:55 <> (365 / 400) 91.25% ETA: 00:00: Checking Known Locations - Time: 00:01:55 <> (369 / 400) 92.25% ETA: 00:00: Checking Known Locations - Time: 00:01:55 <> (370 / 400) 92.50% ETA: 00:00: Checking Known Locations - Time: 00:01:56 <> (371 / 400) 92.75% ETA: 00:00: Checking Known Locations - Time: 00:01:56 <> (375 / 400) 93.75% ETA: 00:00: Checking Known Locations - Time: 00:01:57 <> (376 / 400) 94.00% ETA: 00:00: Checking Known Locations - Time: 00:01:58 <> (380 / 400) 95.00% ETA: 00:00: Checking Known Locations - Time: 00:01:59 <> (381 / 400) 95.25% ETA: 00:00: Checking Known Locations - Time: 00:02:01 <> (386 / 400) 96.50% ETA: 00:00: Checking Known Locations - Time: 00:02:01 <> (389 / 400) 97.25% ETA: 00:00: Checking Known Locations - Time: 00:02:02 <> (391 / 400) 97.75% ETA: 00:00: Checking Known Locations - Time: 00:02:02 <> (392 / 400) 98.00% ETA: 00:00: Checking Known Locations - Time: 00:02:04 <> (396 / 400) 99.00% ETA: 00:00: Checking Known Locations - Time: 00:02:04 <> (397 / 400) 99.25% ETA: 00:00: Checking Known Locations - Time: 00:02:04 <> (400 / 400) 100.00% Time: 00:02:04

[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] Theme(s) Identified:

[+] twentytwentyone

| Location: http://192.168.2.4/wordpress/wp-content/themes/twentytwentyone/

| Latest Version: 1.8 (up to date)

| Last Updated: 2023-03-29T00:00:00.000Z

| Readme: http://192.168.2.4/wordpress/wp-content/themes/twentytwentyone/readme.txt

255 / 400) 63.75% ETA: 00:00: Checking Known Locations - Time: 00:01:21 <> (260 / 400) 65.00% ETA: 00:00: Checking Known Locations - Time: 00:01:22 <> (265 / 400) 66.25% ETA: 00:00: Checking Known Locations - Time: 00:01:22 <> (268 / 400) 67.00% ETA: 00:00: Checking Known Locations - Time: 00:01:24 <> (270 / 400) 67.50% ETA: 00:00: Checking Known Locations - Time: 00:01:24 <> (274 / 400) 68.50%

| Style URL: http://192.168.2.4/wordpress/wp-content/themes/twentytwentyone/style.css

| Style Name: Twenty Twenty-One

| Style URI: https://wordpress.org/themes/twentytwentyone/

| Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block editor your best brush. Wi...

| Author: the WordPress team

| Author URI: https://wordpress.org/

|

| Found By: Known Locations (Aggressive Detection)

| - http://192.168.2.4/wordpress/wp-content/themes/twentytwentyone/, status: 200

|

| Version: 1.8 (80% confidence)

| Found By: Style (Passive Detection)

| - http://192.168.2.4/wordpress/wp-content/themes/twentytwentyone/style.css, Match: 'Version: 1.8'

[+] twentytwentythree

| Location: http://192.168.2.4/wordpress/wp-content/themes/twentytwentythree/

| Latest Version: 1.1 (up to date)

| Last Updated: 2023-03-29T00:00:00.000Z

| Readme: http://192.168.2.4/wordpress/wp-content/themes/twentytwentythree/readme.txt

| [!] Directory listing is enabled

| Style URL: http://192.168.2.4/wordpress/wp-content/themes/twentytwentythree/style.css

| Style Name: Twenty Twenty-Three

| Style URI: https://wordpress.org/themes/twentytwentythree

| Description: Twenty Twenty-Three is designed to take advantage of the new design tools introduced in WordPress 6....

| Author: the WordPress team

| Author URI: https://wordpress.org

|

| Found By: Known Locations (Aggressive Detection)

| - http://192.168.2.4/wordpress/wp-content/themes/twentytwentythree/, status: 200

|

| Version: 1.1 (80% confidence)

| Found By: Style (Passive Detection)

| - http://192.168.2.4/wordpress/wp-content/themes/twentytwentythree/style.css, Match: 'Version: 1.1'

[+] twentytwentytwo

| Location: http://192.168.2.4/wordpress/wp-content/themes/twentytwentytwo/

| Latest Version: 1.4 (up to date)

| Last Updated: 2023-03-29T00:00:00.000Z

| Readme: http://192.168.2.4/wordpress/wp-content/themes/twentytwentytwo/readme.txt

| Style URL: http://192.168.2.4/wordpress/wp-content/themes/twentytwentytwo/style.css

| Style Name: Twenty Twenty-Two

| Style URI: https://wordpress.org/themes/twentytwentytwo/

| Description: Built on a solidly designed foundation, Twenty Twenty-Two embraces the idea that everyone deserves a...

| Author: the WordPress team

| Author URI: https://wordpress.org/

|

| Found By: Known Locations (Aggressive Detection)

| - http://192.168.2.4/wordpress/wp-content/themes/twentytwentytwo/, status: 200

|

| Version: 1.4 (80% confidence)

| Found By: Style (Passive Detection)

| - http://192.168.2.4/wordpress/wp-content/themes/twentytwentytwo/style.css, Match: 'Version: 1.4'

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 28 21:08:09 2023

[+] Requests Done: 438

[+] Cached Requests: 10

[+] Data Sent: 123.266 KB

[+] Data Received: 575.862 KB

[+] Memory used: 175.434 MB

[+] Elapsed time: 00:02:29

Παράρτημα 5: WPS

Με το πέρας της σάρωσης το WPScan εμφάνισε τα εξής :

└$ wpscan --url http://192.168.2.4/wordpress --enumerate u

WordPress Security Scanner by the WPScan Team

Version 3.8.22

Sponsored by Automattic - https://automattic.com/

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.2.4/wordpress/ [192.168.2.4]

[+] Started: Fri Jul 28 21:14:07 2023

Interesting Finding(s):

[+] Headers

| Interesting Entries:

| - Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

| - X-Powered-By: PHP/8.2.4

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.2.4/wordpress/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.2.4/wordpress/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.2.4/wordpress/wp-content/uploads/

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.2.4/wordpress/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.2.2 identified (Latest, released on 2023-05-20).

| Found By: Emoji Settings (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=6.2.2'

| Confirmed By: Meta Generator (Passive Detection)

| - http://192.168.2.4/wordpress/, Match: 'WordPress 6.2.2'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs - Time: 00:00:04 <> (10 / 10) 100.00% Time: 00:00:04

[i] User(s) Identified:

[+] admin

| Found By: Wp Json Api (Aggressive Detection)

| - http://192.168.2.4/wordpress/wp-json/wp/v2/users/?per_page=100&page=1

| Confirmed By:

| Rss Generator (Aggressive Detection)

| Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 28 21:14:25 2023

[+] Requests Done: 20

[+] Cached Requests: 28

[+] Data Sent: 5.532 KB

[+] Data Received: 208.508 KB

[+] Memory used: 139.469 MB

[+] Elapsed time: 00:00:17