Εργαστήριο Δικτύων
Τμήμα Μηχανικών Η/Υ & Πληροφορικής Πανεπιστήμιο Πατρών

Ερωτήσεις κατανόησης και Εργασία για το μάθημα:
Σύγχρονες Εφαρμογές Ασφάλειας Δικτύων

7η Εργασία – Ασφάλεια Web-Εφαρμογών.

Εισαγωγή
Η ασφάλεια των Web εφαρμογών είναι η πρακτική της προστασίας των ιστότοπων, των εφαρμογών και των API από επιθέσεις. Στόχος είναι να διατηρηθούν σε λειτουργία οι υπηρεσίες της εφαρμογής και να προστατευτούν οι clients που την χρησιμοποιούν.

Ποιοι είναι οι συνηθισμένοι κίνδυνοι ασφαλείας εφαρμογών στο διαδίκτυο;

Οι εφαρμογές ιστού ενδέχεται να αντιμετωπίσουν έναν ποικίλο αριθμό και τύπων επίθεσης ανάλογα με τους στόχους του εισβολέα, τη φύση του έργου του στοχευμένου οργανισμού και τα ιδιαίτερα κενά ασφαλείας της εφαρμογής. Οι συνήθεις τύποι επίθεσης περιλαμβάνουν:

Zero-day vulnerabilities: Αυτά είναι τρωτά σημεία άγνωστα στους κατασκευαστές μιας εφαρμογής και οι οποίες έτσι δεν διαθέτουν διαθέσιμη λύση. Οι επιθέσεις αναζητούν να εκμεταλλευτούν γρήγορα αυτά τα τρωτά σημεία και συχνά επιδιώκοντας να αποφύγουν την προστασία ασφαλείας.

Cross site scripting (XSS): XSS είναι μια ευπάθεια που επιτρέπει σε έναν εισβολέα να εισάγει client-side scripts από την πλευρά του πελάτη σε μια ιστοσελίδα προκειμένου να αποκτήσει πρόσβαση σε σημαντικές πληροφορίες άμεσα, να μιμείται τον χρήστη ή να εξαπατήσει τον χρήστη για να αποκαλύψει σημαντικές πληροφορίες.

SQL injection (SQi):SQi είναι μια μέθοδος με την οποία ένας εισβολέας εκμεταλλεύεται τα τρωτά σημεία με τον τρόπο που μια βάση δεδομένων εκτελεί ερωτήματα αναζήτησης. Οι επιτιθέμενοι χρησιμοποιούν το SQI για να αποκτήσουν πρόσβαση σε μη εξουσιοδοτημένες πληροφορίες, να τροποποιήσουν ή να δημιουργήσουν νέα δικαιώματα χρήστη ή να χειρίζονται με άλλο τρόπο ή να καταστρέφουν ευαίσθητα δεδομένα.

Denial-of-service (DoS) / distributed denial-of-service (DDoS) attacks: Μέσα από μια ποικιλία ενεργειών, οι επιτιθέμενοι είναι σε θέση να υπερφορτώσουν έναν στοχευμένο διακομιστή ή την γύρω υποδομή του με διαφορετικούς τύπους δεδομένων. Όταν ένας διακομιστής δεν είναι πλέον σε θέση να επεξεργάζεται αποτελεσματικά τα εισερχόμενα αιτήματα, αρχίζει να συμπεριφέρεται αργή και τελικά να αρνηθεί την υπηρεσία σε εισερχόμενες αιτήσεις από νόμιμους χρήστες.

Buffer overflow: Η υπερχείλιση buffer είναι μια ανωμαλία που συμβαίνει όταν το λογισμικό γράφει δεδομένα σε ένα καθορισμένο χώρο στη μνήμη γνωστή ως buffer. Η υπερχείλιση της χωρητικότητας του buffer έχει ως αποτέλεσμα τις παρακείμενες θέσεις μνήμης να αντικατασταθούν με δεδομένα. Αυτή η συμπεριφορά μπορεί να εκμεταλλευτεί για την έγχυση κακόβουλου κώδικα στη μνήμη, ενδεχομένως δημιουργώντας ευπάθεια στο στοχευμένο μηχάνημα.

Cross-site request forgery (CSRF): Η πλαστογραφία αίτησης συνεπάγεται την εξαπάτηση ενός χρήστη ια να υποβάλει ένα αίτημα που χρησιμοποιεί τον έλεγχο ταυτότητας ή την

εξουσιοδότησή του. Αξιοποιώντας τα προνόμια λογαριασμού ενός χρήστη, ένας εισβολέας είναι σε θέση να στείλει ένα αίτημα που μεταμφιέζεται ως χρήστης. Μόλις ο λογαριασμός ενός χρήστη παραβιαστεί, ο επιτιθέμενος μπορεί να εξαλείψει, να καταστρέψει ή να τροποποιήσει σημαντικές πληροφορίες. Οι εξαιρετικά προνομιούχοι λογαριασμοί, όπως οι διαχειριστές ή τα στελέχη, είναι συνήθως στόχοι.

HTTP cookies**:** Ένα HTTP cookie (Cookie Web, Cookie Browser) είναι ένα μικρό κομμάτι δεδομένων που στέλνει ένας διακομιστής στο πρόγραμμα περιήγησης ιστού του χρήστη. Το πρόγραμμα περιήγησης μπορεί να αποθηκεύσει το cookie και να το στείλει πίσω στον ίδιο διακομιστή με μεταγενέστερα αιτήματα.

Συνήθως, ένα HTTP cookie χρησιμοποιείται για να πει εάν δύο αιτήματα προέρχονται από το ίδιο πρόγραμμα περιήγησης διατηρώντας πχ ενός χρήστη συνδεδεμένο. Αποθηκεύει δλδ πληροφορίες κατάστασης (stateful information) για να της χρησιμοποιήσει σε ένα πρωτόκολλο stateless (χωρίς έλεγχο πρότερης κατάστασης) όπως είναι το http πρωτόκολλο.

Μερικές εφαρμογές των HTTP cookies αφορούν την διαχείριση μας http σύνδεσης, το *tracking* ενός χρήστη αλλά και την προσωποποιημένη αντιμετώπιση (Personalization) ενός χρήστη (πχ για διαφημίσεις).

Cookie theft and hijacking. Υπάρχουν διάφορες τεχνικές κλοπής των **HTTP cookies**. Οι μέθοδοι δεν είναι δύσκολο να εφαρμοστούν και μπορούν να προκαλέσουν σημαντική ζημιά σε έναν χρήστη ή έναν οργανισμό. Τα cookies που περιέχουν ευαίσθητες πληροφορίες, όπως ονόματα χρήστη, κωδικούς πρόσβασης και αναγνωριστικά περιόδου σύνδεσης, μπορούν να κλαπούν, χρησιμοποιώντας αυτά τα εργαλεία μόλις μεταφορτωθούν από έναν ιστότοπο σε ένα πρόγραμμα περιήγησης στο Web ή έχουν πρόσβαση μέσω ενός σκληρού δίσκου υπολογιστή.

Page scraping: Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν bots για να κλέψουν περιεχόμενο από ιστοσελίδες σε μεγάλη κλίμακα. Μπορούν να χρησιμοποιήσουν αυτό το περιεχόμενο για να κερδίσουν ένα πλεονέκτημα τιμολόγησης έναντι ενός ανταγωνιστή, μιμούνται τον ιδιοκτήτη της σελίδας για κακόβουλους σκοπούς ή άλλους λόγους.

Third-party code abuse: Πολλές σύγχρονες εφαρμογές ιστού χρησιμοποιούν μια ποικιλία εργαλείων τρίτου μέρους-για παράδειγμα, έναν ιστότοπο ηλεκτρονικού εμπορίου] (https://www.cloudflare.com/ecommerce/) χρησιμοποιώντας ένα εργαλείο επεξεργασίας πληρωμών τρίτων. Εάν οι επιτιθέμενοι βρουν μια ευπάθεια σε ένα από αυτά τα εργαλεία, μπορεί να είναι σε θέση να θέσουν σε κίνδυνο το εργαλείο και να κλέψουν τα δεδομένα που επεξεργάζονται, να αποτρέψουν τη λειτουργία τους ή να το χρησιμοποιήσουν για να εισαγάγουν κακόβουλο κώδικα αλλού στην εφαρμογή. Οι επιθέσεις Magecart, οι οποίες κλέβουν τα δεδομένα πιστωτικών καρτών από τους επεξεργαστές πληρωμών, αποτελούν παράδειγμα αυτού του τύπου επίθεσης. Αυτές οι επιθέσεις θεωρούνται επίσης ότι είναι επιθέσεις εφοδιαστικής αλυσίδας προγράμματος περιήγησης.

Εργαλεία

1. **Ανάλυση Ασφάλειας Ιστοσελίδων από την Mozilla.**

Το παρατηρητήριο της Mozilla αναλύει τις ευπάθειες μιας ιστοσελίδας και βοηθάει διαχειριστές συστημάτων και επαγγελματίες ασφαλείας πώς να διαμορφώσουν τους ιστότοπούς τους με ασφάλεια και ασφάλεια.
https://observatory.mozilla.org/

2. **Ανάλυση επικεφαλίδων HTTP**.

Η εταιρεία https://probely.com/ εξειδικεύεται στην ανάπτυξη σαρωτών ευπαθειών web εφαρμογών και API για προγραμματιστές. Διατηρεί το site https://securityheaders.com/ που βοηθάει την προστασία από κακόβουλες ενέργειες επί των HTTP headers.
Οι επικεφαλίδες HTTP αφήνουν τον πελάτη και τον διακομιστή να ανταλλάξουν πρόσθετες πληροφορίες με ένα HTTP request ή response. Μια επικεφαλίδα HTTP αποτελείται από το case-insensitive όνομα της, ακολουθούμενη από ένα ":", και μετά την τιμή του.

3. **Ανάλυση πιστοποιητικού**

Η εταιρεία https://www.ssllabs.com/ παρέχει εργαλεία ανάλυσης του πρωτοκόλλου ασφαλείας SSL πχ *SSL Labs APIs, SSL/TLS Deployment Best Practices, SSL Server Test, HTTP Client Fingerprinting Using SSL Handshake Analysi, SSL Client Test, etc*
(https://www.ssllabs.com/projects/index.html)

Παρέχει δωρεάν την ανάλυση ενός πιστοποιητικού μιας ιστοσελίδας: https://www.ssllabs.com/ssltest/

(μπορείτε να αναλύσετε και τον browser σας:
https://www.ssllabs.com/ssltest/viewMyClient.html)

4. **Ανάλυση χρήσης/υποστήριξης ciphersuites**

Η ιστοσελίδα https://cryptcheck.fr/ αναλύει ποια ciphersuites υποστηρίζει μια web-εφαρμογή.

Εργασία

1. Στην εικονική μηχανή που ήδη έχετε στην υπηρεσία του okeanos-knossos εγκαταστήστε το λογισμικό Apache (https://httpd.apache.org/). Το λογισμικό είναι από τα πλέον γνωστά και ευρέως χρησιμοποιούμενα λογισμικά για υλοποίηση web-Servers.
2. Χρησιμοποιώντας την έτοιμη σουίτα κατασκευής ιστοσελίδων joomla ή wordpress αναπτύξτε μια προσωποποιημένη ιστοσελίδα.
3. Εκδώστε ένα δωρεάν FQDN (πχ από εδώ: **www.dnsexit.com**) και εισάγετε το στον web-server σας. Εκδώστε ένα δωρεάν certificate από τον οργανισμό Let'Encrypt και ρυθμίστε το κατάλληλα στον web-server σας.
4. Τροποποιείστε κατάλληλα τον web-server σας να υποστηρίζει https συνδέσεις.
5. Τροποποιείστε κατάλληλα τον web-server σας να υποστηρίζει redirection από http => https συνδέσεις.
6. Τροποποιείστε κατάλληλα το firewall σας να επιτρέπει πρόσβαση στα ports 443,80.

Διαμορφώστε τις παραμέτρους του λογισμικού Apache, για

- την μεγιστοποίηση της βαθμολογίας στο παρατηρητήριο της Mozilla. (https://observatory.mozilla.org/)

Την υποστήριξη μόνο TLSv1.3 πρωτοκόλλου και μόνο των recommended cipher suite του TLS1.2. (https://cryptcheck.fr/)

- Μεγιστοποίηση της προστασίας των HTTP επικεφαλίδων (https://securityheaders.com/)
- Πραγματοποιήστε ανάλυση του πιστοποιητικού (https://www.ssllabs.com/ssltest/)

Υπόδειξη:
Τα αρχεία που πρέπει να τροποποιήσετε είναι:
/etc/apache2/apache2.conf (παραμετροποίηση http headere)
/etc/apache2/mods-enabled/ssl.conf (παραμετροποίηση ciphersuites)
/etc/apache2/sites-enabled/default-ssl.conf (εισαγωγή πιστοποιητικού που θα χρησιμοποιεί)
/etc/apache2/sites-enabled/000-default.conf (redirection)

Σημείωση:
Εκτός από το παρατηρητήριο της Mozilla μπορείτε να πειραματιστείτε με τα παρακάτω εργαλεία:
https://github.com/drwetter/testssl.sh
https://github.com/narbehaj/ssl-checker
https://portswigger.net/burp/communitydownload (Burp Suite Community Edition)