ΥΣ13 Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων

- Εαρινό Εξάμηνο 2019-2020
- Διδάσκων: Κώστας Χατζηκοκολάκης
- Εργασία 1 : Web Application Security
  - Ανακοινώθηκε : 26 Μαρτίου 2020
  - Προθεσμία παράδοσης: 26 Απριλίου 2020, 23:59

Ο στόχος του πρώτου project είναι να παίξετε το ρόλο και του αμυνόμενου και του επιτιθέμενου σε ένα περιβάλλον μιας πραγματικής web εφαρμογής.

Ομάδες & github repository

Στο project παίζει η μία ομάδα εναντίον της άλλης. Οι ομάδες πρέπει να είναι των 2 ατόμων (ένα άτομο μόνο του είναι δυνατό να συμμετέχει αλλά δε συστήνεται, επίσης 3 άτομα είναι δυνατό με αυστηρότερη βαθμολογία).

Κάθε ομάδα θα έχει το δικό της github repository με τα αρχεία της εργασίας. Θα σας δοθεί σύντομα ένα url εγγραφής, από το οποίο

- Θα αντιστοιχήσετε το github account σας με το ΑΜ σας (αν το ΑΜ σας δεν εμφανίζεται μην συνεχίσετε αλλά επικοινωνήστε με τον διδάσκοντα!)
- Θα δημιουργήσετε νέα ομάδα ή θα γραφτείτε σε μία υπάρχουσα (συννενοηθείτε μεταξύ σας πριν από αυτό το βήμα)

Το repository της ομάδας θα είναι ίδιο με το παρακάτω, το οποίο αν θέλετε μπορείτε να χρησιμοποιήσετε μέχρι να γίνετι η εγγραφή. Περιέχει απλά μια παλιά έκδοση του eclass, με κάποια μικρά patches.

`https://github.com/chatziko-ys13/openeclass`

Virtual Machines

Θα σας δοθούν μέσω piazza δύο ειδών vms από τα οποία μπορείτε να τρέχετε εύκολα το eclass

- Ενα VirtualBox vm για χρήστη στον προσωπικό σας υπολογιστή (μπορείτε να σετάρετε και το eclass εκτός vm, αλλά επειδή η έκδοση είναι πολύ παλιά πιθανότατα θα δυσκολευτείτε).

- Ενα online vm στο οποίο θα ανεβάσετε την εφαρμογή για τη δεύτερη φάση της εργασίας.

Προστασία

Θα πρέπει να **ελέγξετε τον κώδικα για πιθανά προβλήματα ασφάλειας**. Συγκεκριμένα μας ενδιαφέρουν SQL Injection, Cross-site Scripting (XSS), Cross-Site Request Forgery (CSRF) και Remote File Injection (RFI). Μπορείτε βέβαια να επεκταθείτε και σε οποιοδήποτε άλλο πρόβλημα της web εφαρμογής. Έπειτα θα πρέπει να **διορθώσετε τις ευπάθειες αυτές** χωρίς να αλλάξει η λειτουργικότητα της εφαρμογής.

Εγκατάσταση

Στη συνέχεια θα πρέπει να στήσετε την εφαρμογή. Οδηγίες για το στήσιμο θα σας σταλούν στο piazza. Αφού στήσετε την εφαρμογή θα πρέπει να δημιουργήσετε ένα χρήστη με username: "drunkadmin" που να έχει admin privileges. Οι χρήστες / φοιτητές (students) θα πρέπει να μπορούν να κάνουν registration (προσοχή – η εγγραφή χρηστών μέσω αίτησης δεν θα πρέπει να είναι ενεργοποιημένη). Το password του εκάστοτε drunkadmin θα δωθεί απο εμάς (θα βρίσκεται στο ίδιο e-mail που θα λάβετε για το στήσιμο). Επίσης, θα πρέπει να δημιουργήσετε ένα μάθημα με περιεχόμενο δικό σας με τις εξής λειτουργίες: "Ανταλλαγή Αρχείων", "Περιοχές Συζητήσεων", "Τηλεσυνεργασία". Τέλος, θα πρέπει η λειτουργία "Εργασίες" για το μάθημα αυτό, να είναι ενεργοποιημένη και να δημιουργήσετε μια εργασία με προθεσμία τέλος Απριλίου.

Επίθεση:

Θα σας δωθεί με email το όνομα μιας αντίπαλης ομάδας. Μετά το web-war time-zero στις **20 Απριλίου 2020 23:59**, θα έχετε τους εξής στόχους (σημείωση: μετά το time-zero δεν επιτρέπεται να ασχολείστε με την προστασία της εφαρμογής σας):

1. Να βρείτε το password ενός administrator της αντίπαλης εφαρμογής όπως αυτό αποθηκεύεται στη βάση.

2. Να κάνετε deface το αντίπαλο site. Σχετικά με τον ορισμό του τι είναι defacement: οποιαδήποτε αλλαγή που μπορεί να γίνει σε administrator level (και μπορείτε να είστε όσο δημιουργικοί θέλετε). Αφού καταφέρετε να πάρετε administrator access, και να κάνετε deface το site, θα πρέπει να στείλετε ένα e-mail στο ys13@chatzi.org ανακοινώνοντας το είδος του defacement, το όνομά σας και το όνομα της αντίπαλης ομάδας (deface claim email). Το deface δε θα γίνει δεκτό αν δεν το δούμε εμείς (σε περίπτωση που το δούμε πράγματι θα σταλεί ένα deface confirmation e-mail). Μπορείτε να στείλετε και deface claim εκ των προτέρων δηλαδή, να πείτε αν γίνει το x τότε το site θα γίνει defaced με τον τρόπο y. Για να επιτύχετε αυτούς τους στόχους θα πρέπει να χρησιμοποιήσετε SQL Injection, XSS, CSRF ή και RFI. Δεν είναι απαραίτητο οτι θα τα καταφέρετε (αν οι αμυνόμενοι έχουν κάνει καλά τη δουλειά τους). Θα πρέπει όμως

να δοκιμάσετε όλες τις επιθέσεις. Υπόψη: οχρήστης drunkadmin που διαχειριζόμαστε είναι αρκετά επιπόλαιος, και ανοίγει links που στέλνουν με email (θα σας δοθούν οδηγίες για το πώς ακριβώς επικοινωνείτε με τον drunkadmin).

Εαν υπάρξουν ομάδες οι οποίες επιβιώσουν του web-war, θα υπάρξει δεύτερος, bonus γύρος στον οποίο θα συνεχίσουν όσες ομάδες επιβιώσουν (για τον οποίο οι ημερομηνίες θα ανακοινωθούν). Στο δεύτερο γύρο όλοι θα είναι εναντίον όλων. Αν κάποια ομάδα (ή ομάδες) επιβιώσει και το δεύτερο γύρο θα έχει +0.5 μονάδα έξτρα στην τελική βαθμολογία (αν υπάρχουν παραπάνω από μια, το bonus θα μοιραστεί).

Παράδοση

Η παράδοση γίνεται μέσω github, απλά κάνετε push στο team repository πριν την τελική ημερομηνία. Μπορείτε να κάνετε όσα push θέλετε, η τελευταία έκδοση πριν τη λήξη θα ληφθεί υπόψη. Μπορείτε να κάνετε push και μετά τη λήξη, απλά οι αλλαγές θα αγνοηθούν. Στο τέλος της χρονιάς τα repositories θα διαγραφούν, μπορείτε να κάνετε φυσικά fork για να τα κρατήσετε.

Επίσης, στο **README.md πρέπει να παραδώσετε μια αναφορά** που:

1. Να περιέχει τα ονόματα και ΑΜ των μελών της ομάδας.
2. Να εξηγεί τι είδους αλλαγές κάνατε στον κώδικα για να προστατέψετε το site σας (από την κάθε επίθεση).
3. Να εξηγεί τι είδους επιθέσεις δοκιμάσατε στο αντίπαλο site και αν αυτές πέτυχαν.