ΥΣ13 Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων

- Εαρινό Εξάμηνο 2018-2019
- Διδάσκων: Κώστας Χατζηκοκολάκης
- Εργασία 1 : Web Application Security
  - Ανακοινώθηκε : 27 Μαρτίου 2019
  - Προθεσμία παράδοσης: 25 Απριλίου 2019, 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

Στο project παίζει η μία ομάδα εναντίον της άλλης. Οι ομάδες πρέπει να είναι των 2 ατόμων (ή ενός αν προτιμάτε), και πρέπει να δηλωθούν μέχρι τις 30/3 στο αντίστοιχο post στο piazza.

Προστασία

Θα προμηθευτείτε την εφαρμογή GUNet eClass version 2.3 από το site:

`http://www.openeclass.org/παλαιότερες-εκδόσεις`

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. Ειδικές οδηγίες για το στήσιμο θα σας σταλούν ξεχωριστά. 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 17 Απριλίου 2019 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.project@gmail.com 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

Πρέπει να παραδώσετε μια αναφορά (report) που να εξηγεί: (1) τι είδους αλλαγές κάνατε στον κώδικα για να προστατέψετε το site σας (από την κάθε επίθεση), (2) τι είδους επιθέσεις δοκιμάσατε στο αντίπαλο site και αν αυτές πέτυχαν. Η αναφορά θα σταλεί στο `ys13.project@gmail.com`.

Εξώφυλλο Project: Το εξώφυλλο του project σας πρέπει να περιέχει τα ονόματά σας, τα ΑΜ σας, καθώς και τα στοιχεία: ”Project #1”, ”Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων”, ”ΕΑΡΙΝΟ 2018”.