

## Web Application Security

Ο στόχος του πρώτου project είναι να παίξετε το ρόλο και του αμυνόμενου και του επιτιθέμενου σε ένα περιβάλλον μιας πραγματικής web εφαρμογής. Στο project παίζουν ομάδες δύο ατόμων (ή και ενός ατόμου) η μια εναντίον της άλλης. Πρέπει να δηλώσετε τα μέλη της ομάδας και το όνομα της με ένα e-mail στο `csec.di@gmail.com` μέχρι την Πέμπτη 30.03.2017, 23:59. Το project απαιτεί τα παρακάτω:

- **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. Θα δοθούν ειδικές οδηγίες ανα ομάδα μέσω e-mail για το στήσιμο. Σημειώστε ότι το περιβάλλον που χρησιμοποιούμε για hosting, διάφορες προστασίες σε επίπεδο server δεν είναι διαθέσιμες. Κατά συνέπεια, μόνο σε επίπεδο κώδικα μπορείτε να προστατέψετε την εφαρμογή σας. 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 δοθεί 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 δοθεί με email το όνομα μιας αντίπαλης ομάδας. Μετά το web-war time-zero στις 18 Απριλίου 2017 23:59, θα έχετε τους εξής στόχους:
  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 to site, θα πρέπει να στείλετε ένα e-mail στο `csec.di@gmail.com` ανακοινώνοντας το είδος του defacement, το όνομά σας και το όνομα της αντίπαλης ομάδας (deface claim e-mail). 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 ότι θα τα καταφέρετε (αν οι αμυνόμενοι έχουν κάνει καλά

τη δουλειά τους). Θα πρέπει όμως να δοκιμάσετε όλες τις επιθέσεις. Υπόψη: ο χρήστης drunkadmin που διαχειριζόμαστε είναι αρκετά επιπόλαιος: συγκεκριμένα χρησιμοποιεί το e-mail csec.di@gmail.com και γενικώς αν του έρθει κάποιο e-mail που τον καλεί να πατήσει κάποιο link θα το πατήσει. Θα πρέπει πάντως να είστε συγκεκριμένοι (λ.χ. το e-mail σας με subject "drunkadmin" μπορεί να λέει: ``Αγαπητέ administrator του site της ομάδας XXX - έχουμε μια πολύ ωραία προσφορά για εσάς. Πατήστε στο link YYY για λεπτομέρειες. Μην τη χάσετε!").

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.

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 μοιρασθεί).

**Εξώφυλλο Project:** Το εξώφυλλο του project σας πρέπει να περιέχει τα ονόματά σας, τα ΑΜ σας, καθώς και τα στοιχεία "Project #1", "ΥΣ13 ΕΑΡΙΝΟ 2017".