| | |
|---|---|
| *Πανεπιστήμιο Αθηνών* | Εαρινό 2014 |
| ΥΣ13 Ασφάλεια Υπολογιστικών Συστημάτων | ΚΙΑΓΙΑΣ |
| Due: `27.07.2011` | Project #4 |

**Hacking στο Web**

Ο στόχος του τέταρτου project είναι να βρεθείτε ταυτόχρονα σαν επιτιθέμενοι και αμυνόμενοι σε ένα περιβάλλον μιας πραγματικής εφαρμογής Web. Στο project παίζουν ομάδες δύο ατόμων (ή και ενός ατόμου) η μία εναντίον της άλλης. Πρέπει να δηλώσετε τα μέλη της ομάδας και το όνομα με ένα e-mail στο `csec.di@gmail.com` μέχρι τη Δευτέρα 30.6.2014, 23:59. Το project απαιτεί τα εξής:

- (Εγκατάσταση) Θα προμηθευτείτε και θα στήσετε την εφαρμογή GUNet eClass version 1.7.3. Η εφαρμογή θα στηθεί με shared hosting στο server του μαθήματος (θα δωθούν ειδικοί λογαριασμοί ανα ομάδα μέσω e-mail για το στήσιμο). Όταν κάνετε την εγκατάσταση προσέξτε το *Website title* θα πρέπει να είναι το όνομα της ομάδας σας.

- (Χρήστες) Θα πρέπει να δημιουργήσετε ένα χρήστη με όνομα ``drunkadmin'' που να έχει administrator privileges. Οι χρήστες/φοιτητές (students) θα πρέπει να μπορούν να κάνουν registration (εγγραφή χρηστών μέσω αίτησης: off). Το όνομα της πλατφόρμας θα είναι το όνομα της ομάδας.

  Τα password του drunkadmin θα δωθεί απο εμάς - όταν είστε έτοιμοι στείλτε e-mail στο `csec.di@gmail.com` για να σας στείλουμε το password που θα πρέπει να χρησιμοποιήσετε.

  Επίσης θα πρέπει να δημιουργήσετε ένα μάθημα με περιεχόμενο δικό σας με τις εξής λειτουργίες: ανταλλαγή αρχείων, περιοχή συζητήσεων, κουβέντα. Επίσης θα πρέπει η λειτουργία ``εργασίες μαθήματος'' να είναι ενεργοποιημένη και να δημιουργήσετε μια εργασία με προθεσμία τέλος Ιουλίου.

- (Προστασία) Θα πρέπει να ελέγξετε τον κώδικα για πιθανά προβλήματα ασφάλειας. Συγκεκριμένα μας ενδιαφέρουν SQL injection, cross site scripting (xss), και cross site request forgeries (xsrf). Αλλα μπορείτε να επεκταθείτε και σε οποιοδήποτε άλλο πρόβλημα της web εφαρμογής. Σημειώστε ότι το περιβάλλον που χρησιμοποιούμε για hosting, διάφορες προστασίες σε επίπεδο server δεν είναι διαθέσιμες - οπότε **μόνο** σε επίπεδο κώδικα μπορείτε να προστατέψετε την εφαρμογή σας.

- (Επιθέση) Θα σας δωθεί το όνομα μιας αντίπαλης ομάδας. Μετά το web-war time-zero (θα ανακοινωθεί στο forum), 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. Το defacement μπορεί να γίνει παίρνοντας administrator access. Μόλις κάνετε deface το site πρέπει να στείλετε ένα e-mail στο `csec.di@gmail.com` ανακοινώνοντας το είδος του defacement, το όνομα 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** (αμα ξέρετε τι κάνετε) δηλαδή, να πείτε αν γίνει το $x$ τότε το site θα γίνει defaced με τον τρόπο $y$. Σχετικά με τον ορισμό του είναι defacement : οποιαδήποτε αλλαγή που μπορεί να γίνει σε administrator level (και μπορείτε να είστε όσο creative θέλετε).

Για να επιτύχετε αυτούς τους στόχους θα πρέπει να χρησιμοποιήσετε sql injection, xss ή και csrf. Δεν είναι απαραίτητο οτι θα τα καταφέρετε (αν οι αμυνόμενοι έχουν κάνει καλά τη δουλειά τους). Θα πρέπει πάντως να δοκιμάσετε επιθέσεις εναντίον της βάσης (injection) καθώς και εναντίον χρηστών. Ο χρήστης drunkadmin που διαχειριζόμαστε είναι αρκετά χαζος: 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 (π.χ. το e-mail σας 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 που να εξηγεί (1) τι είδους αλλαγές κάνατε στον κώδικα για να προστατέψετε το site σας, (2) τι είδους επιθέσεις δοκιμάσατε στο αντίπαλο site.

**Καθυστερημένες Υποβολές Project**. Μπορείτε να χρησιμοποίησετε μέχρι 10 μέρες για να καθύστερησετε την παράδωση ενος project (συνολικά για όλο το εξάμηνο). Η ημερομηνία υποβολής κρίνεται η ημερομηνία που παρδίνεται το e-mail σας στον server.

**Εξώφυλλο Project.** Το εξώφυλλο του project σας πρέπει να περιέχει το όνομα σας, το ΑΜ σας, καθώς και τα στοιχεία "Project #4", "ΥΣ13 ΕΑΡΙΝΟ 2014" καθώς και μια ένδειξη για το πόσες μέρες καθυστέρησης χρησιμοποιήθηκαν (`0` αν καμμία).