Πανεπιστήμιο Αθηνών	Εαρινό 2018
ΥΣ13 Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων	Δ. Μητρόπουλος
Ημερομηνία Παράδοσης: `25.4.2018`	Project #1

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 παίζει η μία ομάδα εναντίον της άλλης και 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. Ειδικές οδηγίες για το στήσιμο υπάρχουν στο τέλος της εκφώνησης της εργασίας (ΠΑΡΑΡΤΗΜΑ). 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 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 2018 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 `csec.uoa@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 οτι 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.uoa@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. Η αναφορά θα σταλεί στο `csec.uoa@gmail.com`.

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).

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".

ΠΑΡΑΡΤΗΜΑ

Οδηγίες για την εγκατάσταση της εφαρμογής

Θα λάβετε σχετικό email με τα στοιχεία που χρειάζεστε. Το email θα έχει τίτλο: "**Battle Royal Credentials**". Όπου **team_pass** είναι το password που σας έχει δοθεί και **team_name** το όνομα της ομάδας σας.

Βήμα 1:
Στην γραμμή εντολών δίνετε:

ssh **team_name**@**team_name**.csec.gr

Βάζετε ως password το **team_pass** που σας έχει δοθεί.

Βήμα 2:
Κάνετε copy τον κώδικά σας στον φάκελο:

/var/www/eclass/**team_name**.csec.gr/

Προσοχή: Εαν ο κώδικάς σας βρίσκεται στον φάκελο **tmp**, δεν κάνετε τον φάκελο copy αλλά τα περιεχόμενά του. Κοινώς, εαν θέλουμε να ανεβάσουμε το eclass ακριβώς όπως το κατεβάσαμε από το site του GUNet θα κάναμε copy ότι θα βρίσκαμε στο φάκελο **openeclass-2.3**. Εαν δηλαδή δεν έχετε αλλάξει το όνομα του top directory (ασχέτως αν αλλάξατε τον κώδικα) και βρίσκεστε στο directory που έχει μέσα τον φάκελο, θα πρέπει να τρέξετε την ακόλουθη εντολή:

scp -r /openeclass-2.3/. **team_name**@**team_name**.csec.gr:/var/www/eclass/**team_name**.csec.gr

Βήμα 3:
Θα μπορείτε πλέον να δείτε την εφαρμογή σας στο ακόλουθο URL:

team_name.csec.gr

1. Ξεκινάτε το στήσιμο πατώντας το κόκκινο link (Οδηγός Εγκατάστασης).
2. Επιλέγετε "Ελληνικά" και πατάτε **Επόμενο Βήμα**.
3. Στα **απαιτούμενα** PHP Modules θα πρέπει να βλέπετε παντού OK. Πατάτε και πάλι **Επόμενο Βήμα**.
4. Στην "Άδεια Χρήσης" πατάτε **Αποδοχή**.
5. Στις "Ρυθμίσεις της MySQL" βάζετε: (1) στο "Εξυπηρέτης Βάσης Δεδομένων" τον **εξυπηρετητή που σας εστάλει στο email** και (2) στο "Συνθηματικό για τη Βάση Δεδομένων" βάζετε το **team_pass**. Αφήνετε τα υπόλοιπα όπως είναι και πατάτε **Επόμενο Βήμα**.
6. Στην επόμενη σελίδα βάζετε ως "Όνομα Χρήστη του Διαχειριστή" το **drunkadmin** και ως "Συνθηματικό του Διαχειριστή" το **team_pass**. Αφήνετε τα υπόλοιπα όπως είναι και πατάτε **Επόμενο Βήμα**.
7. Στην επόμενη σελίδα ("Τελευταίος έλεγχος πριν την εγκατάσταση") πατάτε "Εγκατάσταση του Open eClass".

8. Εαν όλα έχουν πάει καλά θα δείτε το μήνυμα που σας γνωστοποιεί πως η εγκατάσταση έχει ολοκληρωθεί με επιτυχία. Πατάτε "Είσοδος στο Open eClass".

Βήμα 4:
Προχωράτε ως drunkadmin για να φτιάξετε αυτά που έχουν ζητηθεί στην εκφώνηση (μάθημα με περιεχόμενο δικό σας κλπ. -- δείτε το κομμάτι "Εγκατάσταση" της εκφώνησης).