ΕΡΓΑΣΙΑ ΣΤΑ ΠΛΑΙΣΙΑ ΤΟΥ ΜΑΘΗΜΑΤΟΣ: ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

**Project #1**

****

**ΥΣ13 ΕΑΡΙΝΟ 2017**

σΠΥΡΟΣ ΑΝΑΣΤΑΣΙΟΥ 1115201300007

ΑΓΓΕΛΟΣ ΤΟΥΜΑΣΗΣ 1115201300177

**ΠΕΡΙΕΧΟΜΕΝΑ**

* **ΠΡΟΛΟΓΟΣ**
* **ΠΡΟΣΤΑΣΙΑ** 
  + *SQL Injection*
  + *Cross-site Scripting (XSS)*
  + *Cross-Site Request Forgery (CSRF)*
  + *Remote File Injection (RFI)*
* **ΕΠΙΘΕΣΗ** 
  + *SQL Injection*
  + *Cross-site Scripting (XSS)*
  + *Cross-Site Request Forgery (CSRF)*
  + *Remote File Injection (RFI)*
* **ΣΥΜΠΕΡΑΣΜΑΤΑ**
* **ΒΙΒΛΙΟΓΡΑΦΙΑ**

**ΠΡΟΛΟΓΟΣ**

Η εφαρμογή του eclass v2.3 ελέχθηκε για πιθανά προβλήματα ασφάλειας όπως ζητείται στην εκφώνηση. Τα προβλήματα είναι κατηγοριοποιημένα σε SQL Injection, Cross-site Scripting (XSS), Cross-Site Request Forgery (CSRF) και Remote File Injection (RFI). Γνώμονας της διόρθωσης αυτών των κενών ασφάλειας ήταν να παραμείνει η **λειτουργικότητα** της εφαρμογής όπως προσφέρεται.

**ΠΡΟΣΤΑΣΙΑ**

Το χρονικό διάστημα μέχρι τις 21 Απριλίου, αφιερώθηκε στην κατανόηση της λειτουργίας της εφαρμογής και τη μελέτη της προστασίας του μαζί με την επίλυση των προβλημάτων που παρουσιάζουμε παρακάτω.

**SQL Injection**

Ελεγχος συγκεκριμενων χαρακτηρων σε login,register και edit χρηστη , τα οποία δεν θα γίνονται αποδεχτά για να αποτραπούν τυχόν επιθέσεις.

Επίσης πολλά queries είχαν λάθος μορφή , και τροποποιήθηκαν με χρήση real\_escape\_string() , auto\_quotes() , δηλαδή φιλτράροντας το input\_value και κάνοντας το value string.

Ελαττωματικά queries βρέθηκαν κυρίως στα αρχεία :

* modules/phpbb/viewforum.php
* modules/phpbb/viewtopic.php
* modules/work/work.php

**Cross-site Scripting (XSS)**

Ξεκινώντας την εξερεύνηση τέτοιων ευπαθειών δοκιμάσαμε σε φόρμες με πεδία να γράψουμε html script της μορφής: <script> alert(‘ Problem here! ’); </script> , τα οποία στέλναμε, παρατηρώντας κάθε φορά το αποτέλεσμα τους όταν παρουσιάζονταν πίσω τα στοιχεία που δώσαμε. Το παραπάνω πρόκειται για *Persistent XSS*. Αρχεία με το παραπάνω πρόβλημα ήταν ……………………………………………………………………………………

Στη συνέχεια προσπαθήσαμε να προσθέσουμε στις καταλήξεις συνδέσμων με php αρχεία τα script tags και παρατηρήσαμε ότι η εκτενής χρήση της μεταβλητής $\_SERVER["PHP\_SELF"] οδηγούσε στην δυνατότητα ενός χρήστη να προσθέσει στο url κάτι της μορφής /%22%3E%3Cscript%3Ealert('hacked')%3C/script%3E το οποίο θα μεταφραζόταν σε /"><script>alert('hacked')</script> . Το αποτέλεσμα αυτής της ενέργειας θα ήταν να κλείνει σε forms το action κομμάτι και να προστίθεται ένα script που θα έκανε alert το μήνυμα hacked. Ο τρόπος για να αντιμετωπίσουμε αυτό το πρόβλημα σύμφωνα με το <https://www.w3schools.com/php/php_form_validation.asp> και τις διαφάνειες από την 2η διάλεξη του μαθήματος είναι η χρήση htmlspecialchars() όποτε και αυτό κάναμε.

Όπως αναφέρθηκε η λανθασμένη χρήση αυτής της μεταβλητής ήταν εκτενής, αλλά η διόρθωση βασικών αρχείων που γίνονταν include σε ακόμα περισσότερα διόρθωσε το πρόβλημα. Σημαντικά αρχεία που διορθώθηκαν ήταν τα:

* modules/dropbox/index.php
* modules/forum\_admin/forum\_admin.php
* include/baseTheme.php
* student\_view.php
* modules/agenda/myagenda.php
* modules/phpbb/ viewtopic
* modules/phpbb/ editpost
* modules/phpbb/index
* modules/phpbb/newtopic
* modules/phpbb/reply
* modules/phpbb/viewforum

Πέρα από τα παραπάνω διορθώθηκαν και τα εξής :

* modules/auth/newprof.php
* modules/auth/formuser.php
* modules/auth/contactprof.php
* modules/auth/courses.php
* modules/admin/eclassconf.php
* modules/admin/mailtoprof.php
* modules/admin/addfaculte.php
* modules/admin/change\_user.php
* modules/admin/adminannouncements.php
* modules/course\_tools/course\_tools.php
* modules/course\_info/delete\_course.php
* modules/unreguser/unreguser.php
* modules/unreguser/unregcours.php
* modules/user/user.php
* modules/profile/profile.php
* modules/create\_course/create\_course.php
* modules/course\_info/restore\_course.php
* modules/admin/cleanup.php
* modules/admin/infocours.php
* modules/course\_info/infocours.php
* modules/admin/newuseradmin.php
* modules/admin/multireguser.php
* modules/admin/edituser.php
* modules/admin/addusertocours.php
* modules/admin/quotacours.php

Εκ των οποίων μερικά έγιναν με τη σκέψη της σωστής χρήσης της μεταβλητής, άσχετα αν οδηγούσαν στην επιτυχή χρήση του script.

Τα παραπάνω αποτελούν δείγμα *Non-Persistent XSS*

Σημαντικό είναι να αναφέρουμε και το τρίτο είδος XSS το *DOM-based XSS*. Η και όχι?

………………………………………………………..

Same origin policy kai cookies????

**Cross-Site Request Forgery (CSRF)**

Ιδέα για το παρακάτω πρόβλημα αποτέλεσε ένας χρήστης ή ένας διαχειριστής που θα άνοιγε κάποιο link ή θα πατούσε submit σε κάποια κακόβουλη εφαρμογή το οποίο θα τον οδηγούσε να καταστρέψει ή να διαμορφώσει πράγματα για τον λογαριασμό του ή ακόμα και να τον διαγράψει τελείως.

H χρήση μεταβλητών όπως η $require\_login = true; (ή αντίστοιχα η $require\_admin = true; ), δεν είναι αρκετή αφού αν ο χρήστης είναι συνδεδεμένος στον λογαριασμό του σε άλλη καρτέλα στον ίδιο browser και ανοίξει το link, αυτό θα πετύχει το σκοπό του.

O τρόπος να αποφύγουμε κάτι τέτοιο (σύμφωνα με τις διαφάνειες της 3ης διάλεξης) είναι η χρήση ενός μυστικού (hidden) token που στέλνεται μαζί με την συμπλήρωση ενός form ή με την επιλογή ενός link από το eclass.

Έτσι κάναμε generate ένα token το οποίο στέλναμε μόλις ο χρήστης ήθελε να εκτελέσει κάποια συγκεκριμένη ενέργεια.

Ο τρόπος που έγινε generate το token είναι ως εξής:

$token = md5(uniqid(rand (), TRUE));

$\_SESSION['token'] = $token;

Και στέλνεται ως:

<input type="hidden" name="token" value="$token" />

Δυστυχώς το παραπάνω αντιμετωπίζει προβλήματα αφου:

Το αποτέλεσμα της rand() μπορεί να είναι προβλέψιμο, το uniqid() προσθέτει μόνο μέχρι 29 bits entropy και ο md5 δεν προσθέτει καθόλου entropy αφού λειτουργεί ντετερμινιστικά. Τρόποι να λυθούν αυτά θα ήταν η χρήση νεότερης έκδοσης της php ή εξωτερικές βιβλιοθήκες, όμως θεωρήθηκε ότι ξεφεύγουν από τον στόχο της εργασίας όποτε έγινε η παραδοχή ότι ο επιτιθέμενος δεν θα προσπαθήσει να βρει τον τρόπο με τον οποίο παράγονται τα token ώστε να τον μιμιθεί.

Εν συνεχεία, κατά την εκτέλεση του αιτήματος που γίνεται από τη φόρμα με κάποιο SQL query προσθέσαμε την συνθήκη:

if (isset($\_SESSION['token']) && $\_POST['token'] == $\_SESSION['token'])

Με το 2ο μέρος της συνθήκης τσεκάρουμε αν είναι ίδια τα token ώστε να αποφανθούμε αν πρόκειται για CSRF επίθεση. Το πρώτο μέρος υπάρχει στην περίπτωση που ο χρήστης δεν έχει πλοηγηθεί ακόμα στη συγκεκριμένη σελίδα που θα γίνει η επίθεση και έτσι δεν έχει αποκτήσει ακόμα token.

Αρχεία που τροποποιήσαμε είναι τα:

* modules/unreguser/unreguser.php
* modules/unreguser/unregcours.php
* modules/admin/unreguser.php

Στο οποίο δεν γινόταν η διαγραφή χρήστη με μαθήματα σωστά οπότε διορθώθηκε μόνο για τη διαγραφή χρήστη που δεν είναι εγγεγραμμένος σε κάποιο μάθημα ή έχουν διαγραφεί τα μαθήματα του από τον admin με άλλο τρόπο.

* modules/admin/delcours.php
* modules/admin/addfaculte.php
* modules/admin/change\_user.php
* modules/admin/adminannouncements.php
* modules/profile/profile.php
* modules/course\_info/infocours.php
* modules/course\_info/delete\_course.php
* modules/course\_info/refresh\_course.php
* modules/admin/eclassconf.php
* modules/course\_tools/course\_tools.php
* modules/course\_tools/course\_tools.php
* modules/course\_tools/course\_tools.php
* modules/course\_tools/course\_tools.php
* modules/create\_course/create\_course.php
* modules/auth/courses.php
* modules/admin/mailtoprof.php
* modules/course\_info/restore\_course.php
* modules/admin/cleanup.php
* modules/user/user.php
* modules/admin/newuseradmin.php
* modules/admin/multireguser.php
* modules/admin/password.php
* modules/admin/edituser.php
* modules/admin/statuscours.php
* modules/admin/infocours.php
* modules/admin/addusertocours.php
* modules/admin/quotacours.php

Όλα τα παραπάνω αποτελούν σημαντικά αρχεία για τα οποία σκεφτήκαμε επιθέσεις τις οποίες θα περιγράψουμε στη συνέχεια.

Από τα ονόματα τους είναι ήδη ευδιάκριτες ποιες θα είναι αυτές.

Ακόμα, αρχεία τα οποία θα μπορούσαν να αλλάξουν με την παραπάνω λογική θα ήταν

* modules/admin/search\_user.php
* modules/admin/searchcours.php
* modules/course\_info/archive\_course.php

Ακόμα και το αθώο myagenda.php!

Επίσης, πρέπει να αναφερθεί ότι στη σελίδα διαχείρισης του admin, στο αρχείο ρυθμίσεων παρουσιάζεται ο κωδικός του διαχειριστή. Μπορεί εκ πρώτης όψεως να μοιάζει ότι έχει αντικατασταθεί με κουκίδες αλλά στη πραγματικότητα αν δει κανείς την html της σελίδας θα παρατηρήσει ότι δίνεται σαν value. Στην περίπτωση του drunkadmin θα μπορούσε κανείς να πάρει τον κωδικό από αυτή τη φόρμα. Για να προστατευτούμε από αυτή την περίπτωση στέλνουμε έναν random generated κωδικό με μήκος όσο και ο πραγματικός κωδικός. Στην περίπτωση που ο admin πατήσει υποβολή χωρίς να κάνει αλλαγές στο πεδίο του κωδικού, θα σταλθεί ο πραγματικός κωδικός στη βάση και όχι ο random.

…………………more TODO κυριως σε αντμιν + συνδεση αντμιν σε χρηστη mainlib.php exei htmlspecial chars dikiat ous

**Remote File Injection (RFI)**

Το συγκεκριμένο πρόβλημα εμφανίζεται εξ ορισμού στην περιοχή Ανταλλαγής Αρχείων.

Τρόπος αντιμετώπισης του, είναι ο εκτενής έλεγχος των αρχείων που ανεβάζονται. Τόσο της κατάληξης τους (είδος αρχείων) όσο και των περιεχομένων τους, μιας και υπάρχει το ενδεχόμενο ένα αρχείο να μην περιέχει αυτά που θα έπρεπε αλλά κάποια επίθεση. Συμβουλευμένοι τις τακτικές που ακολούθησαν οι επόμενες εκδόσεις του eclass υπάρχει ένας πιο απλός τρόπος χειρισμού του, που είναι να κατεβαίνουν όλα τα αρχεία στον χρήστη και όχι μόνο συγκεκριμένοι τύποι αρχείων να ανοίγονται, όπως πραγματοποιήθηκε στην συγκεκριμένη έκδοση.

**ΕΠΙΘΕΣΗ**

Κατά τη φάση της επίθεσης (22 Απριλίου μέχρι 28 Απριλίου), η αντίπαλη ομάδα που μας δόθηκε ήταν η « » και ο κύριος στόχος μας ήταν να δούμε πόσες από τις ευπάθειες που αναφέραμε κατάφεραν να εντοπίσουν και να διορθώσουν.

**SQL Injection**

προβλημάτων που παρουσιάζουμε παρακάτω

**Cross-site Scripting (XSS)**

προβλημάτων που παρουσιάζουμε παρακάτω

**Cross-Site Request Forgery (CSRF)**

προβλημάτων που παρουσιάζουμε παρακάτω

**Remote File Injection (RFI)**

προβλημάτων που παρουσιάζουμε παρακάτω

**ΣΥΜΠΕΡΑΣΜΑΤΑ**

To eclass πρόκειται για μια πλατφόρμα η οποία δεν υλοποιήθηκε με σωστές αρχές και διαθέτει πολλά κενά ασφάλειας. Όλες οι ευπάθειες αντιμετωπίστηκαν στην παρούσα εργασία με τις γνώσεις από τις διαλέξεις του μαθήματος, όμως σε πραγματικές συνθήκες θα ήταν αναγκαία η αναβάθμιση της έκδοσης της php και η χρήση των τελευταίων τεχνολογιών που αυτή προσφέρει, για την μεγιστοποίηση της ασφάλειας του συστήματος. Δεν πρέπει όμως να παραληφθεί πως σωστές συναρτήσεις που υπήρχαν σε αρχεία όπως το include/lib/main.lib.php, δεν χρησιμοποιούνταν από αμέλεια των προγραμματιστών, δείχνοντας τη σημασία της εκπαίδευσης στο συγκεκριμένο τομέα.