

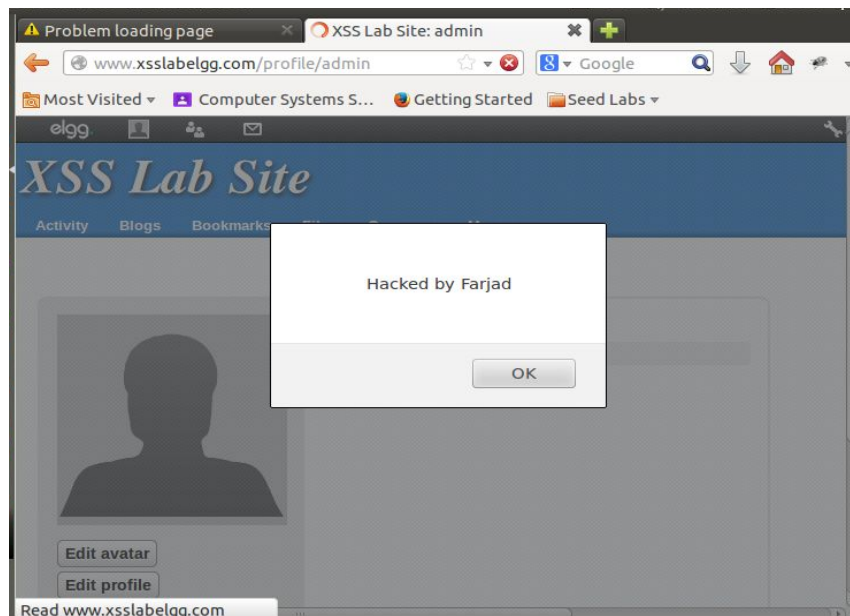
Lab 2

Sheikh Muhammad Farjad
CS-16059
Section A
Batch 2016-17

Course Instructor: Sir Umar Iftikhar
Computer Systems Security

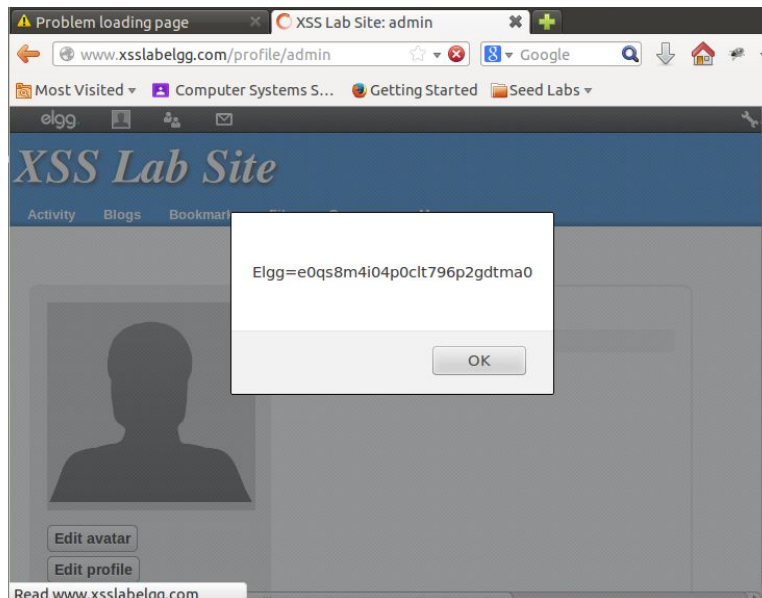
Task 1: Posting a Malicious Message to Display an Alert Window

In this task, Elgg profile was embedded with `<script> alert('Hacked by Farjad'); </script>`, which is a javascript code snippet for popping the dialogue box containing the string passed to alert.



Task 2: Posting a Malicious Message to Display Cookies

It is similar to task 1, but this task displayed the cookie information in the popped-up dialogue box, and the following command was embedded in the Elgg profile: `<script> alert(document.cookie); </script>`



Task 3: Stealing Cookies from the Victim's Machine

In this task, a listener program **echoserv** was initiated on port 5555 of the attacker machine. The Elgg profile was embedded with javascript that was responsible for sending document.cookie information to the attacker machine via GET request because the embedded javascript contained an img tag for communicating with the attacker machine.

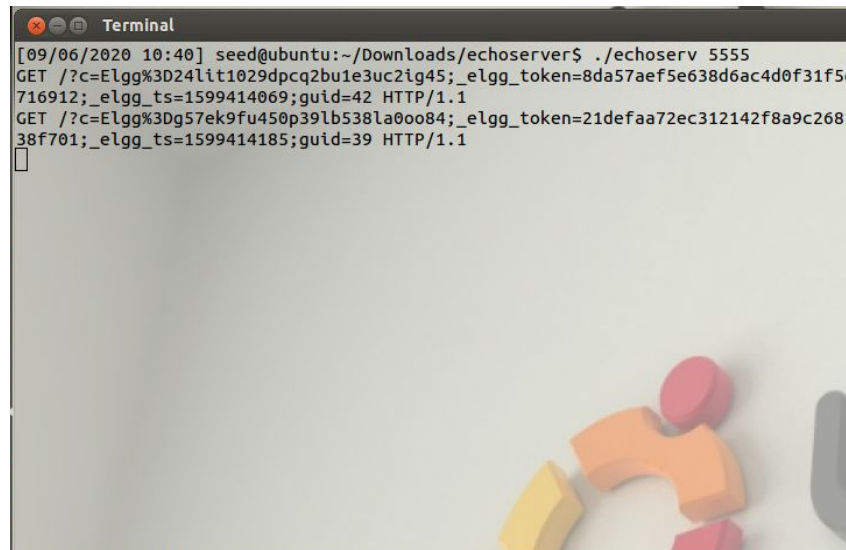
A terminal window titled "Terminal" with standard Ubuntu window controls. It shows the execution of the echoserv program on port 5555 and the receipt of an HTTP GET request from a victim's machine.

```
Terminal
[09/06/2020 10:11] seed@ubuntu:~/Downloads/echoserver$ ./echoserv 5555
GET /?c=Elgg%3D8jje95euqimoief1oorvkj7er6 HTTP/1.1

/Attacker Machine Farjad^[OF]
```

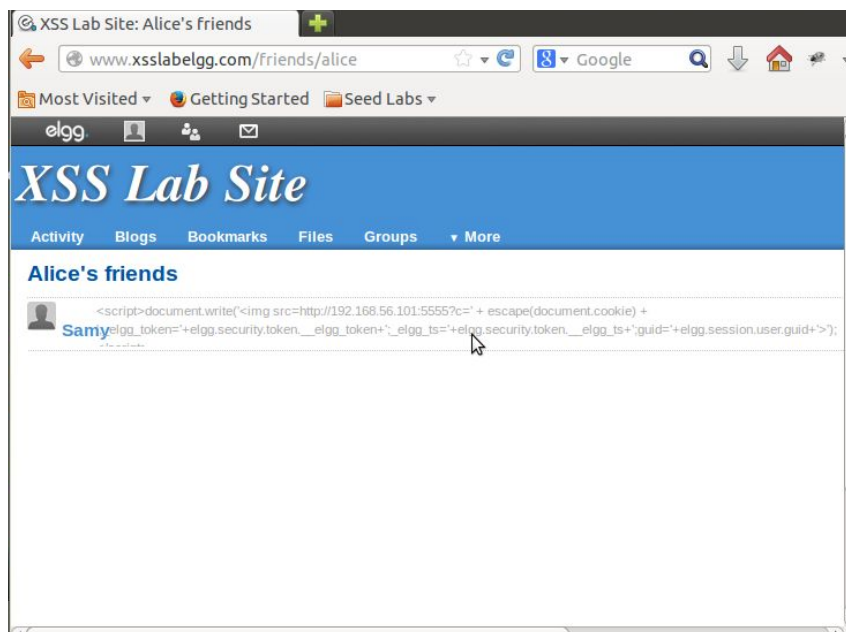
Task 4: Session Hijacking using the Stolen Cookies

In this task, the session of Alice was hijacked from VM1. In VM2, Samy's profile was embedded with javascript which was to send data to VM1 (attacker machine). After embedding the javascript, Alice's account was opened in VM2 and then Samy's profile was visited from Alice's account. During this activity, a listening server was initiated in VM1, which was receiving the information being sent from embedded javascript in Samy's profile.



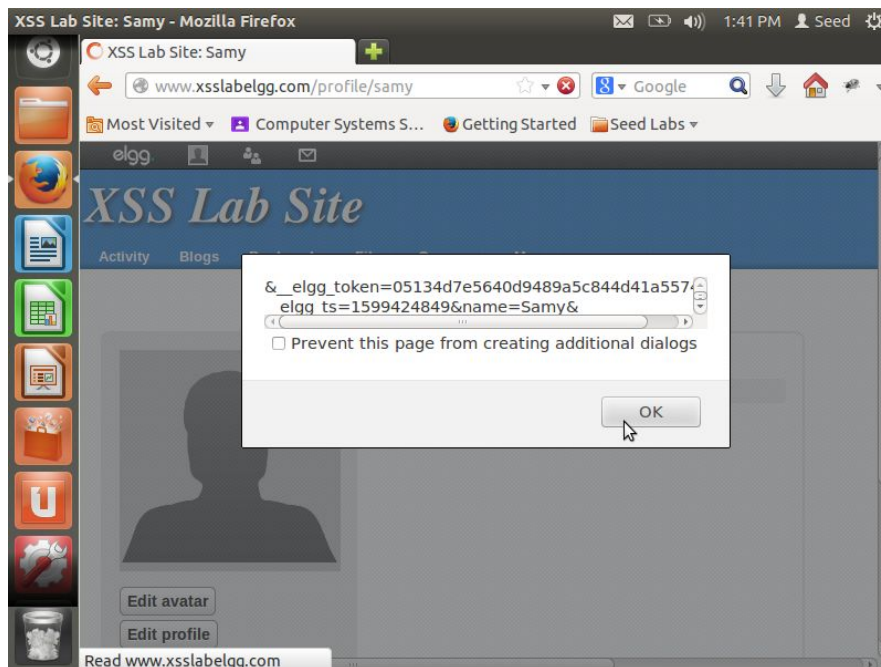
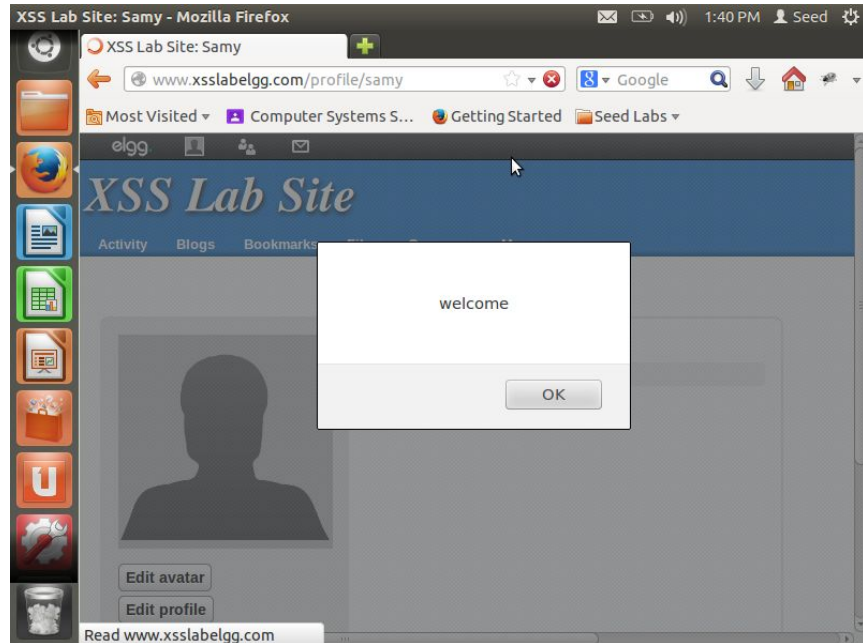
```
Terminal
[09/06/2020 10:40] seed@ubuntu:~/Downloads/echoserver$ ./echoserv 5555
GET /?c=Elgg%3D24lit1029dpcq2bu1e3uc2ig45;_elgg_token=8da57aef5e638d6ac4d0f31f5d716912;_elgg_ts=1599414069;guid=42 HTTP/1.1
GET /?c=Elgg%3Dg57ek9fu450p39lb538la0oo84;_elgg_token=21defaa72ec312142f8a9c268138f701;_elgg_ts=1599414185;guid=39 HTTP/1.1
```

After gathering the information like cookie, token and ts, these values were fed into HTTPSimpleForge.java program in VM1 (attacker machine). This program added the Samy into the friend list of Alice.



Task 5

In this task, the samy's profile was embedded with javascript that was responsible for running the malicious program saved as **addfriend.js**. After embedding the javascript into samy's profile, the visit to samy's profile behaved in the following ways:



Task 6

In this task, the samy's profile was embedded with javascript that was responsible for running the malicious program saved as **addfriendworm.js**. After embedding the javascript into samy's profile, the visit to samy's profile behaved in the following ways:

