

实验报告

课程名称： 网络攻防技术

实验项目： 实验八：Web渗透

学 生 姓 名：

学 号：

二级学院名称：

专 业：

指 导 教 师：

# 1实验目的和要求

1）掌握DVWA演练系统的搭建；

2）掌握Burp Suite破解DVWA登录密码的方法；

3）掌握Burp Suite工具的使用。

# 2实验设备及材料

1）VMware虚拟机：VMware-workstation-full-14.1.3.zip

2）Kali虚拟机系统：Kali-linux-2018.1-vm-amd64.ova

3）Metasploitable靶机系统：Metasploitable-linux-2.0.0.zip

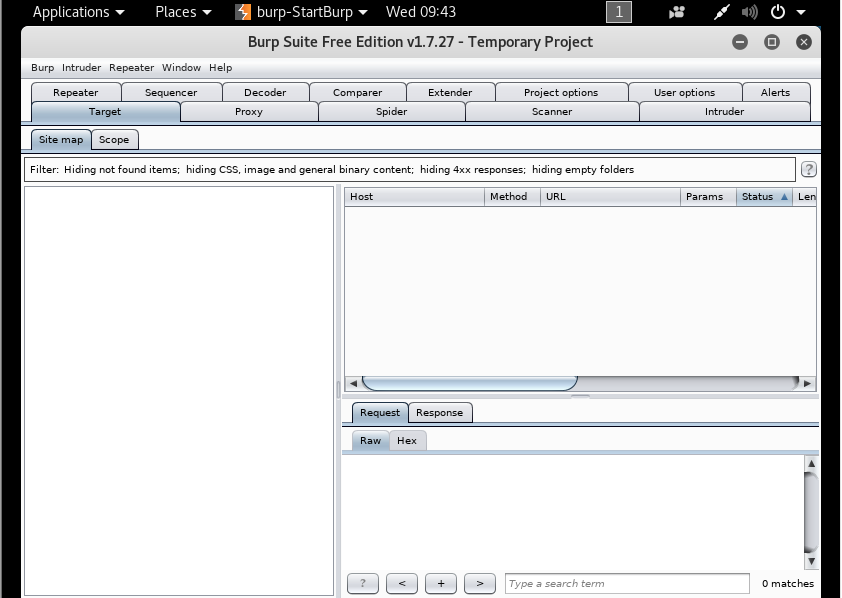
4）DVWA演练平台

5）Burp Suite工具

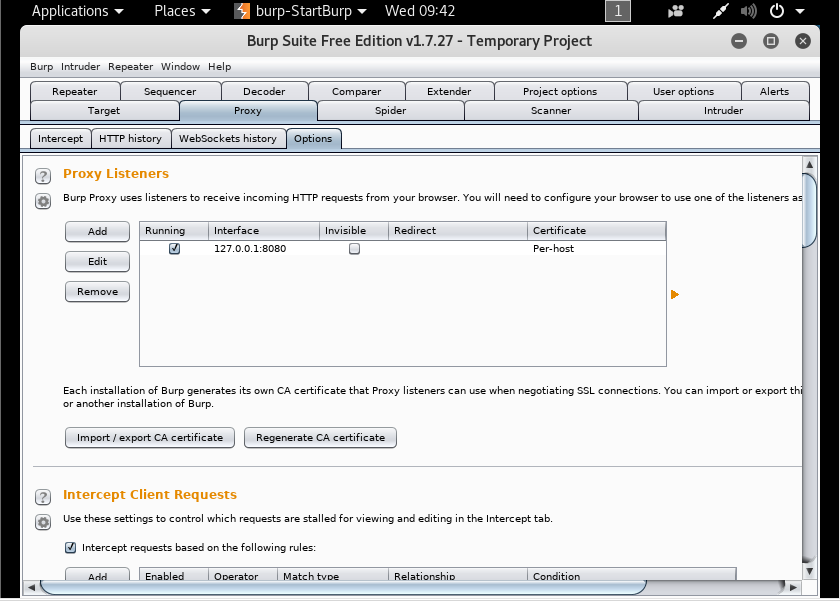
# 3实验内容

3.1采用Burp Suite暴力破解DVWA登录密码，步骤如下：

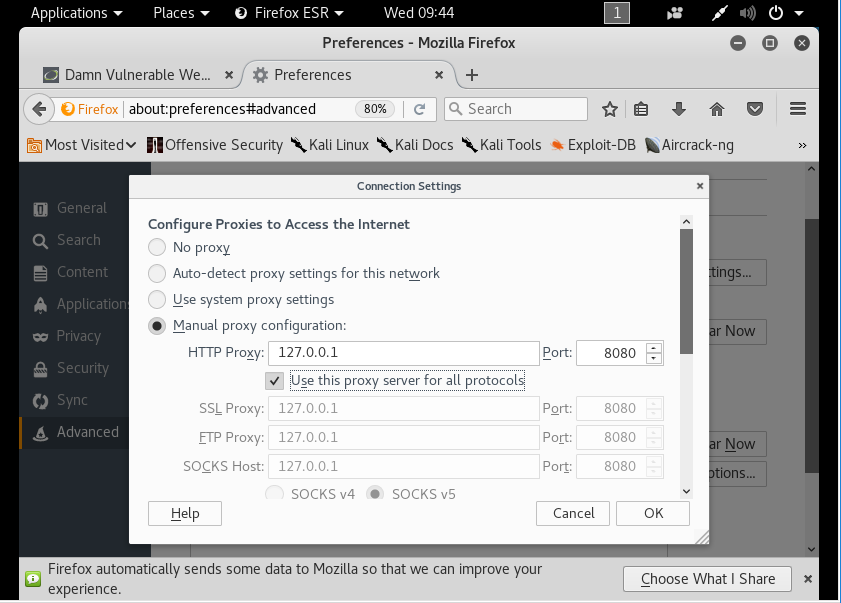
1）启动并初始化Burp Suite；



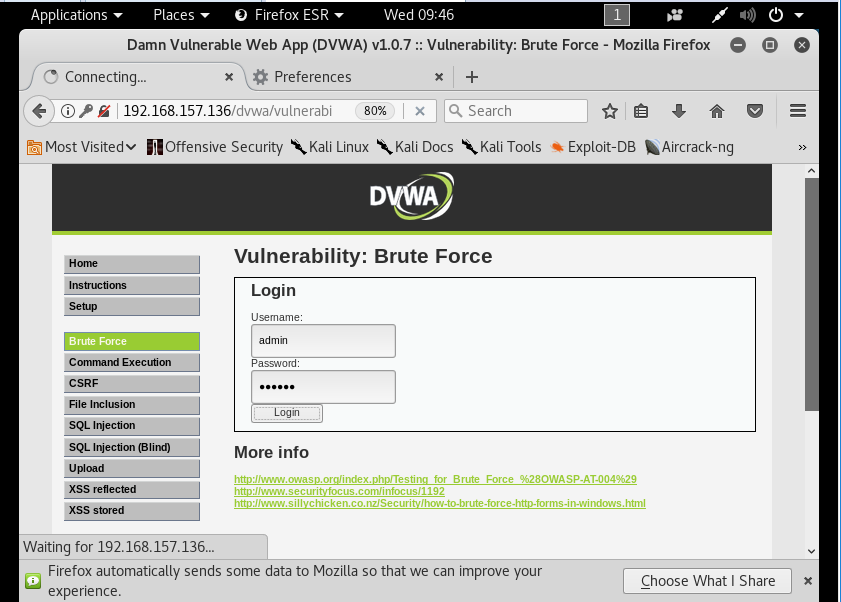
2）Burp Suite服务代理设置；



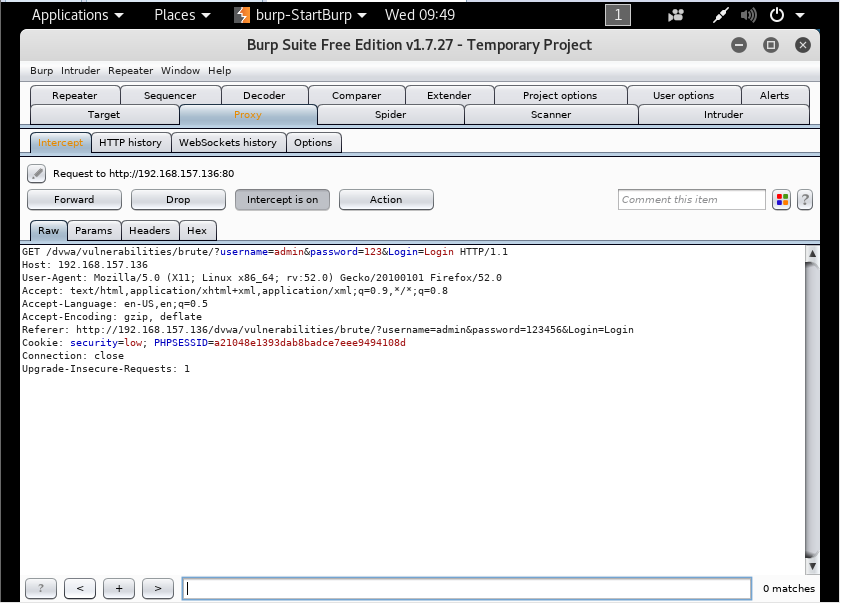
3）浏览器代理设置；



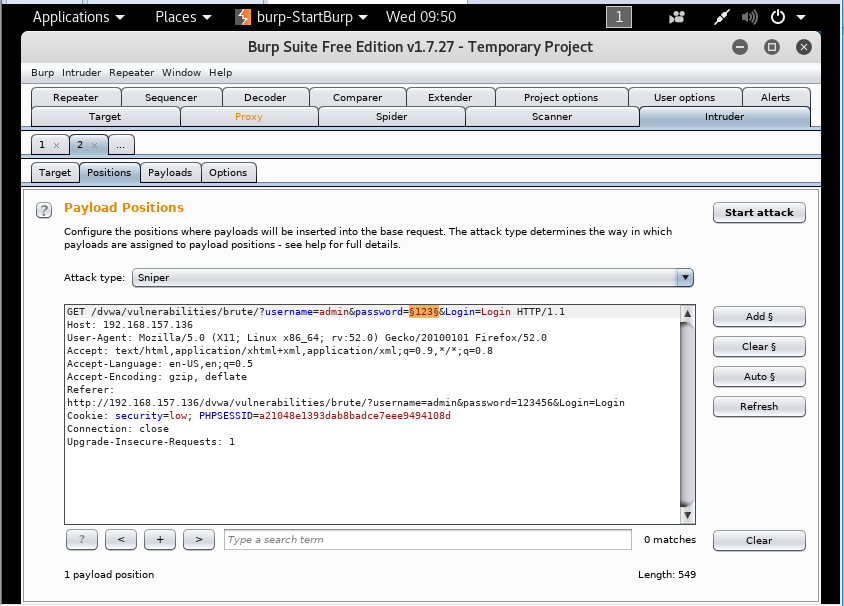
4）破解DVWA登录页面(仅password)。



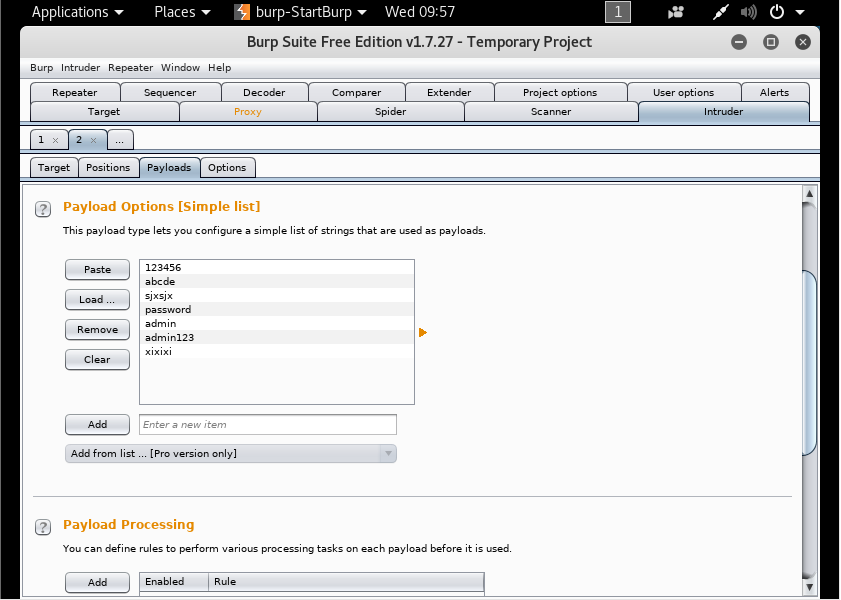
Burpsuite拦截登录页面：



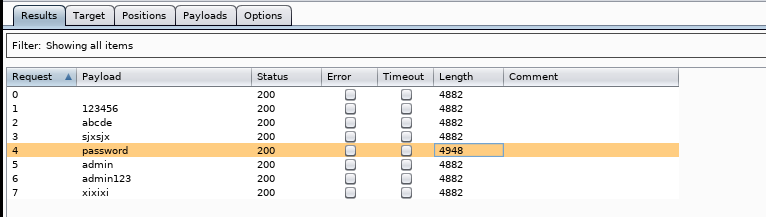
发送给攻击模块后确认密码变量



导入密码本

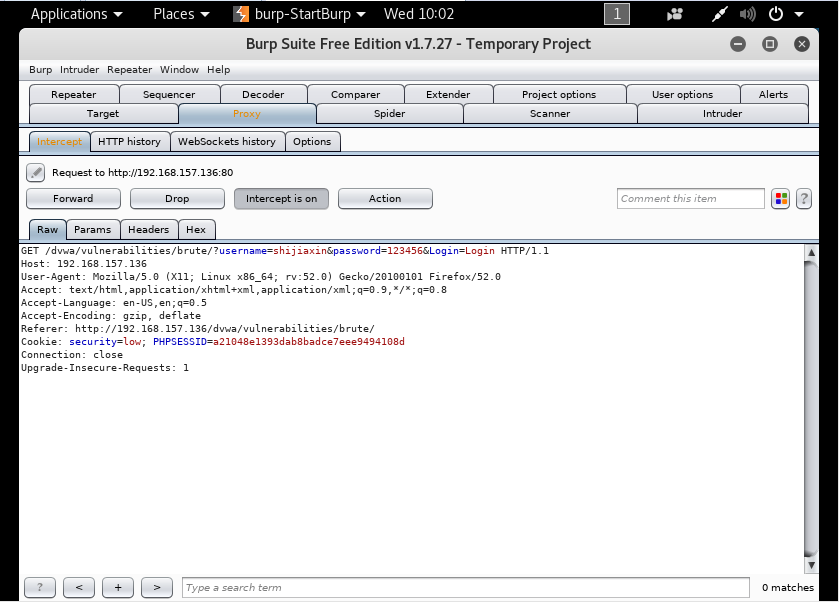


爆破结果

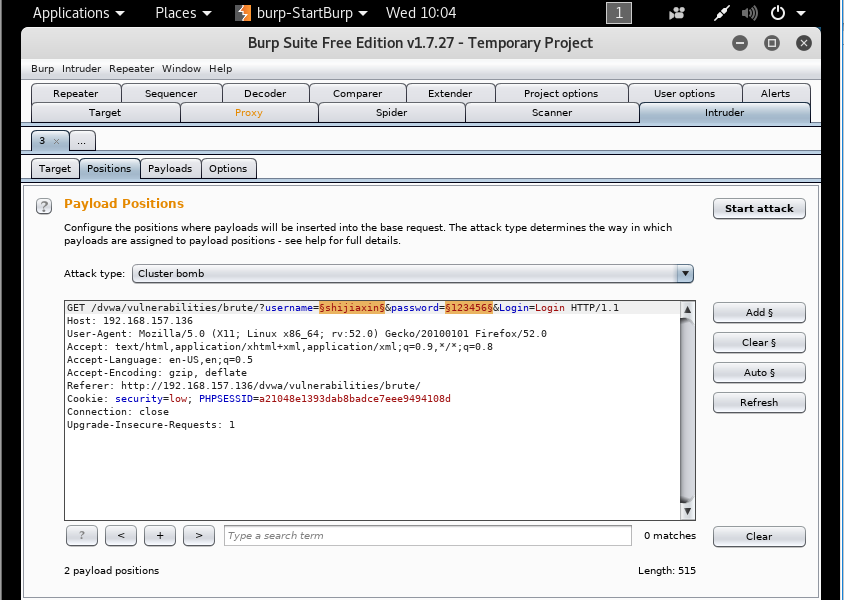


5）破解DVWA登录页面(name与password)。

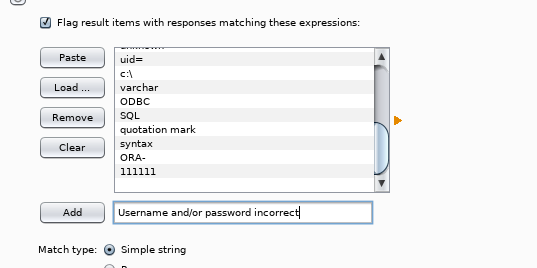
Username and/or password incorrect.



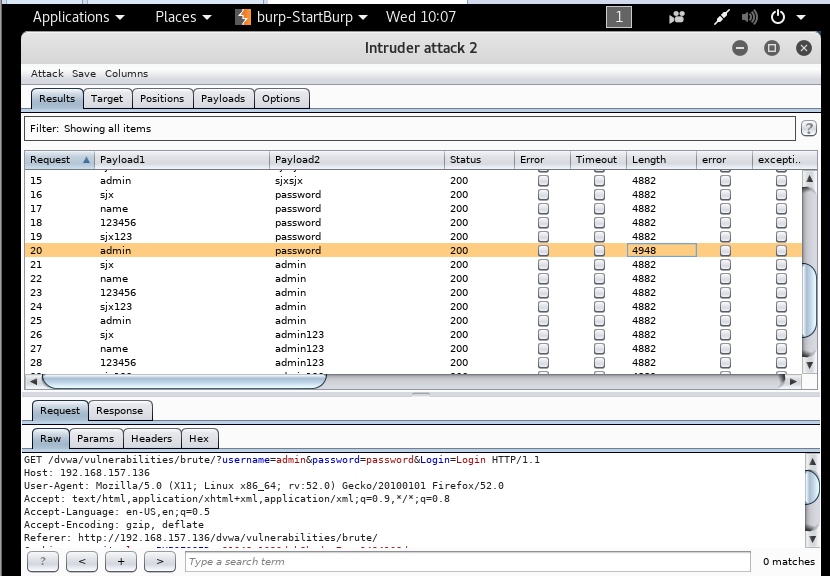
发送至攻击模块后选定攻击方式和变量



添加匹配结果



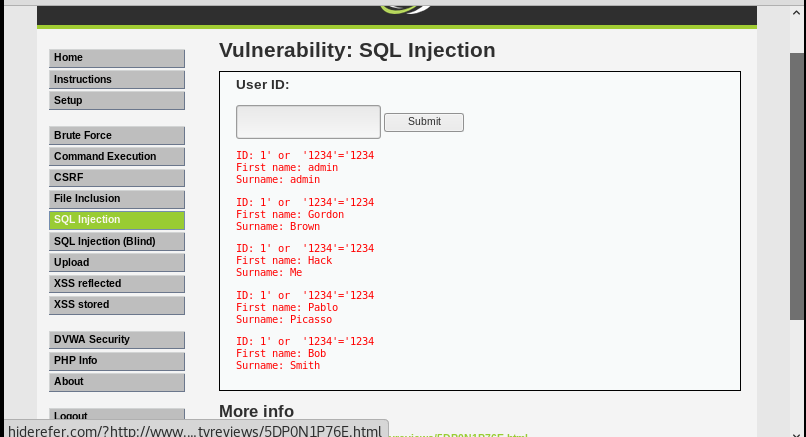
爆破结果



3.2对DVWA演练系统实施SQL注入攻击，步骤如下：

1）判断注入漏洞是否存在以及类型；

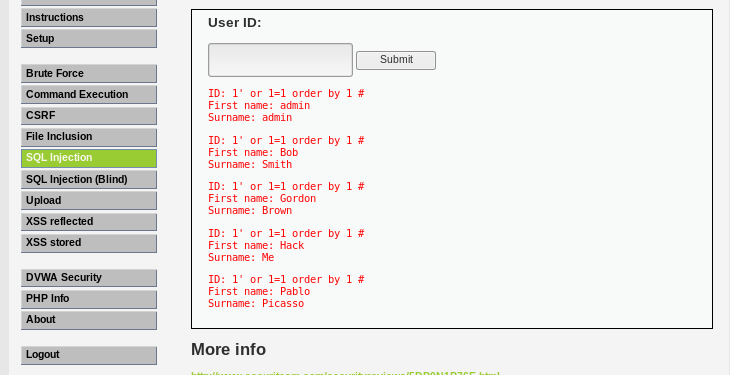




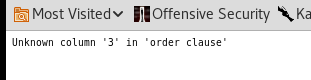
存在字符型注入漏洞

2）判断SQL查询语句中的字段数；

输入查询 1’ or 1 order by 1 #



查询3# 报错

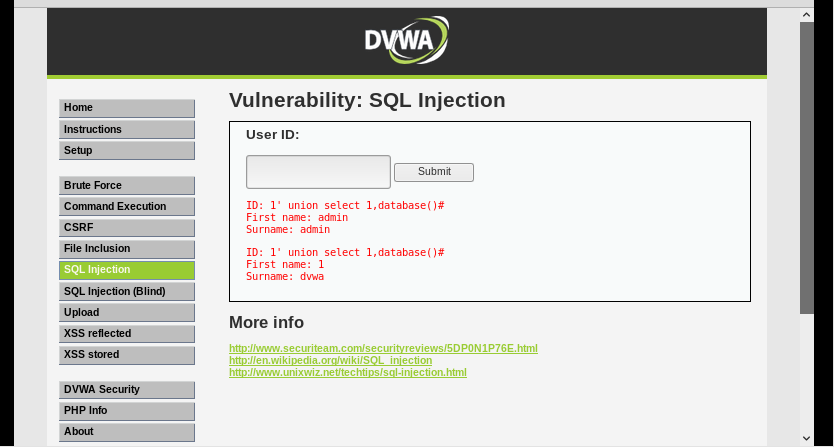


所以只有两个字段

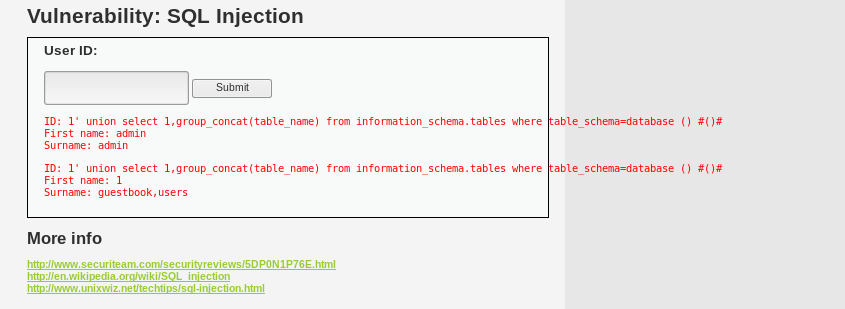
3）确定显示的字段顺序；



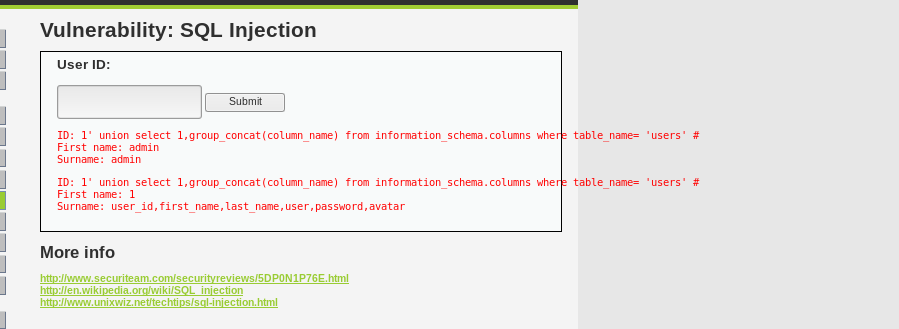
4）获取当前数据库；



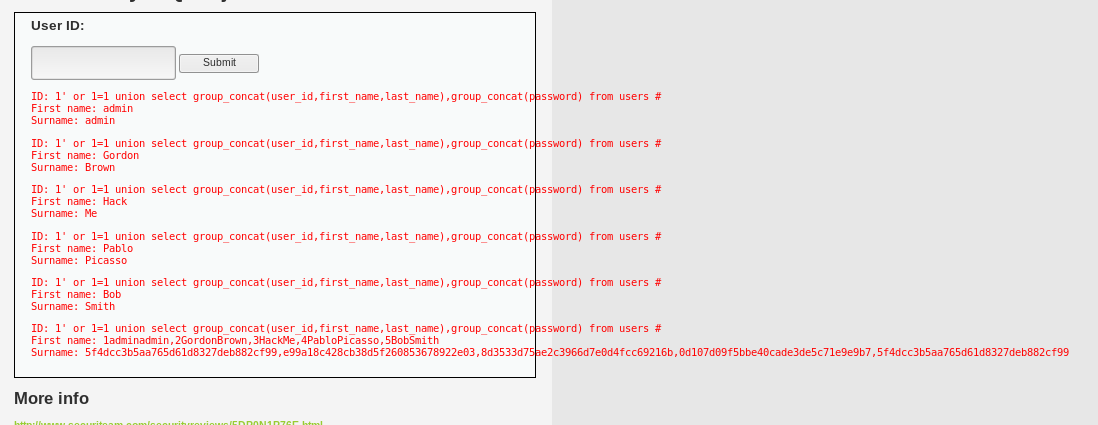
5）获取数据库中的表；



6）获取表中的字段名；



7）读取数据表中的数据。



# 4实验总结

本次实验利用DVWA靶场联系了密码爆破和sql注入的攻击方式。其中，在完成burpsuite实验后，如果不关闭窗口或者停止捕获窗口，浏览器的刷新速度会很慢。关闭burpsuite之后，浏览器的代理也需要关闭，不然无法刷新其他的攻击靶场服务。