《漏洞利用及渗透测试基础》实验报告

姓名： 许健 学号：2013018 班级：信安班

**实验名称：**

SQL盲注

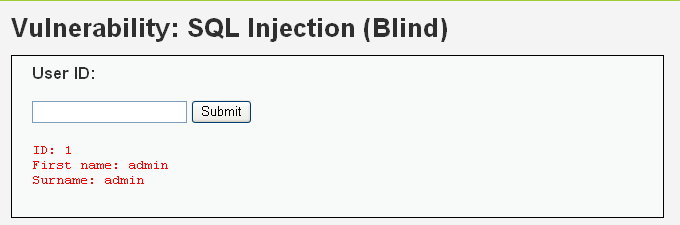
**实验要求：**

基于DVWA里的SQL盲注案例，实施手工盲注，参考书本，撰写实验报告。

**实验过程：**

1. **DVWA中的SQL Injection(Blind)实践**
2. 判断是否存在注入，注入是字符型还是数字型

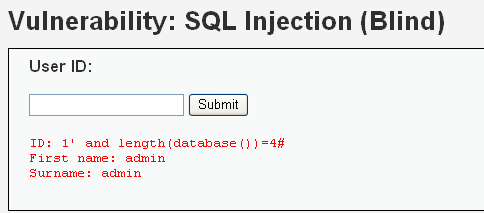
输入1，显示相应用户存在



输入1’ and 1=1#，存在

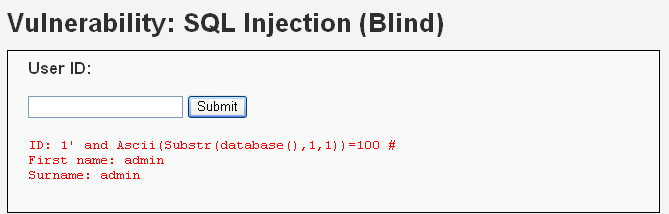
输入1’ and 1=2#，不存在，说明存在字符型的SQL盲注。

1. 猜解当前数据库名



说明数据库名长度为4。

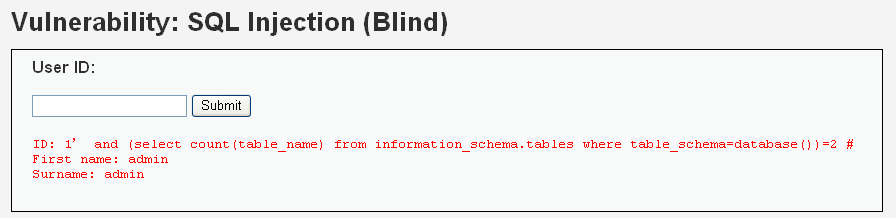
采用二分法去试每个字符的值，重复上述步骤得到完整的数据库名（dvwa）。



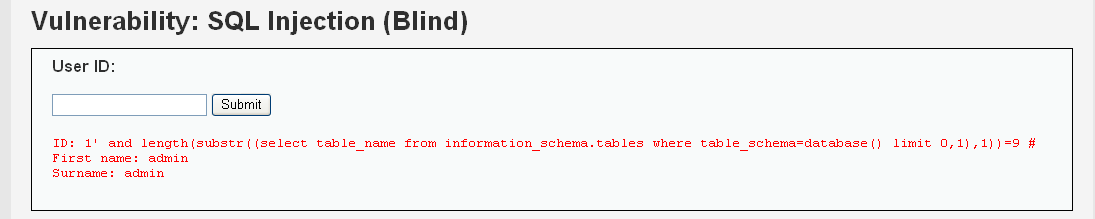
1. 猜解数据库中的表名

猜测数据库中表的个数

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



说明数据库中含有两张表。

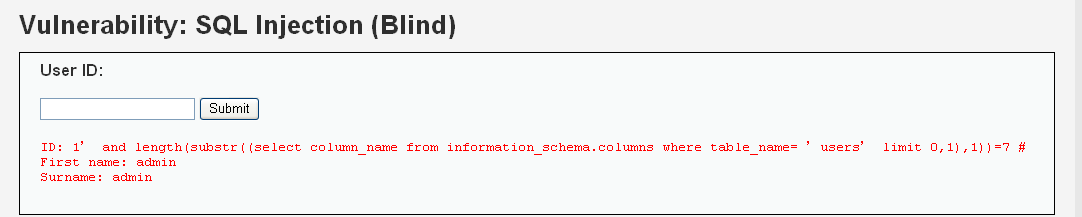


第一张表长度为9

然后使用二分法挨个去猜，猜出两张表为（guestbook、users）。

1. 猜解表中的字段

采用相同的方式，猜测字段的数量和字段的名字。表中的第一个字段含有7个字符。

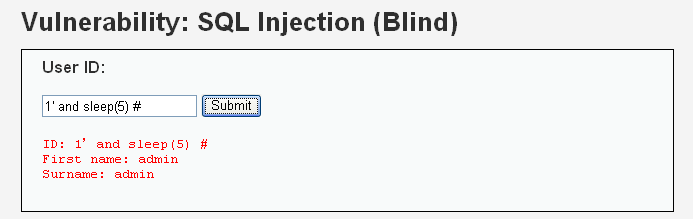


1. 猜解表中数据

继续使用二分法。比较耗费时间，可以使用SQLmap获取数据库中的表、列、数据。

1. **基于时间的SQL盲注**
2. 判断是否存在注入，注入是字符型还是数字型

输入1’and sleep(5) #，感觉到明显延迟，说明存在字符型的基于时间的盲注。



1. 猜解当前数据库名字长度

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

1. 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

通过延迟来判断是否正确，以此类推猜解表、字段和数据。

**心得体会：**

为了应对SQL盲注攻击，最好的方式是在确认客户端的输入合法之前，服务端拒绝进行关键性的处理操作。开发者要具有安全意识，程序要减少漏洞的存在。2

或者可以屏蔽出错信息，某些特殊的攻击若缺乏详细的错误信息则不能完成。屏蔽错误信息是在服务端处理完毕之后进行补救，攻击其实已经发生，只是企图阻止攻击者知道攻击的结果而已。