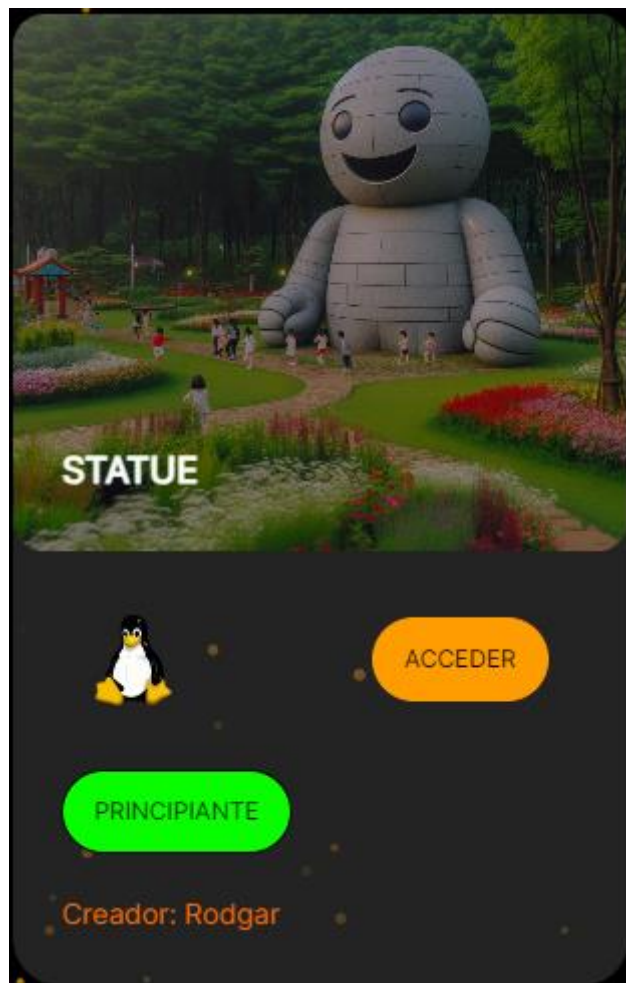


## STATUE



Ejecutamos nmap.

```
$ ../../obtain_data.sh 192.168.16.14
The ip_address '192.168.16.14' is valid
Executing sudo nmap -sS -sV -A -O -p- 192.168.16.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-29 22:40 CET
Nmap scan report for 192.168.16.14
Host is up (0.00077s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 c2:ac:cf:d7:65:58:4b:cf:a2:a1:cd:ff:db:25:b7:79 (ECDSA)
|_  256 e4:4a:ab:9d:d8:7b:8c:d9:6c:6c:9a:52:85:70:b4:8d (ED25519)
80/tcp    open  http      Apache httpd 2.4.58
|_ http-title: Index of /
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 08:00:27:99:7A:2E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: Host: 192.168.16.14; OS: Linux; CPE: cpe:/o:linux:linux_kernel

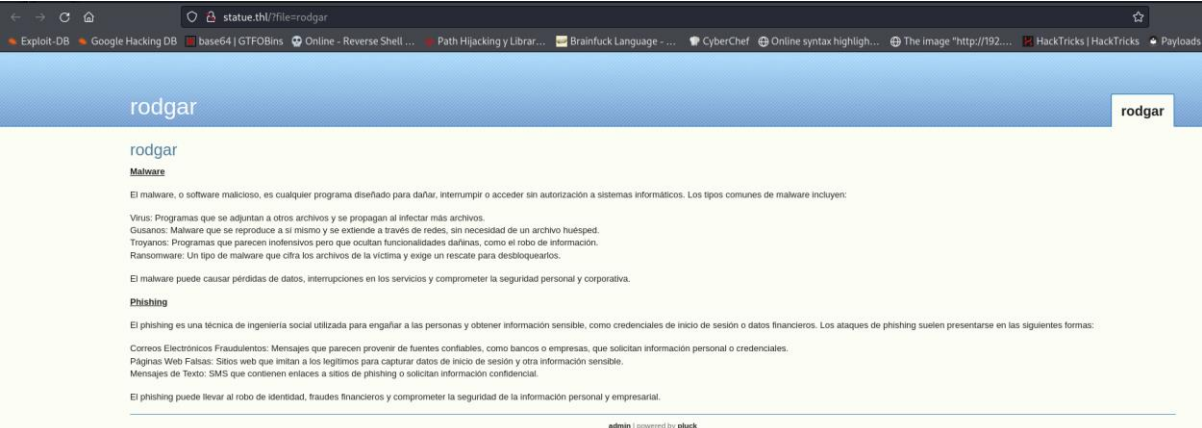
TRACEROUTE
HOP RTT      ADDRESS
1   0.77 ms  192.168.16.14
```

Para este ctf tendremos que añadir al fichero hosts el dominio por defecto de The hacker labs que es nombremáquina.thl

```
$ cat /etc/hosts | grep statue
192.168.16.14 statue.thl
```

Ahora si volvemos a ejecutar el mismo comando de nmap nos devuelve un fichero en la url del puerto 80 con el cual usaremos para avanzar con la máquina.

```
└─$ sudo ./../obtain_data.sh 192.168.16.14
[sudo] password for kali:
Valid IP address: 192.168.16.14
-----
Running Nmap Scan.
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 12:30 CET
Nmap scan report for statue.thl (192.168.16.14)
Host is up (0.00074s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 c2:ac:cf:d7:65:58:4b:cf:a2:a1:cd:ff:db:25:b7:79 (ECDSA)
|_  256 e4:4a:ab:9d:d8:7b:8c:d9:6c:6c:9a:52:85:70:b4:8d (ED25519)
80/tcp    open  http     Apache httpd 2.4.58
|_ http-title: rodgar - rodgar
|_ Requested resource was http://statue.thl/?file=rodgar
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-robots.txt: 2 disallowed entries
|_ /data/ /docs/
|_ http-cookie-flags:
|_   /:
|_     PHPSESSID:
|_       httponly flag not set
|_ http-generator: pluck 4.7.18
MAC Address: 08:00:27:99:7A:2E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: Host: 192.168.16.14; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```





Una vez tenemos añadido el dominio al fichero hosts, vamos a realizar una búsqueda de directorios y ficheros para intentar encontrar algo interesante.

```
/robots.txt (Status: 200) [Size: 2922]
/robots.txt (Status: 200) [Size: 47]
/robots.txt (Status: 200) [Size: 47]
/server-status (Status: 403) [Size: 275]
/templates (Status: 301) [Size: 312] [--> http://statue.thl/templates/]
Progress: 23070 / 23075 (99.98%)
=====
Finished
=====
(kali@kali) - [~/CTFs/statue]
$ gobuster dir -u statue.thl -w /usr/share/wordlists/dirb/common.txt -x html,md,txt,php
```

Lo interesante en este caso es el fichero README que al descargarlo vemos que esta codificado múltiples veces en base64, lo decodificamos.

```
$ cat README.md
Vm0wd2QyUXlVWGxWV0d4V1YwZDRWMVl3WkRSV01WbDNXA1JTVjAxV2JETlhhMUpUVjBaS2RHVkdX
bFp0YwtFeFZtcEJlRl15U2tWVQpiR2hVfFdZd2VGWnRjRXRUTVU1SVZtdFdVZ3BpVlZwVWZtMTRj
MDB4V25Sa1JVcHNvbXhzTlZVeWRGZFdVWEJwVWpKb2R5WkdXbGRkCk1WcFhWmJvVHVW1KVLdsVlVW
M2hMVTFaYWRHUKhkRmhSV0VKd1ZXMDFRMVZHWkZkYVJFSlRDbUpXV2toV01qVlRZV3hLVlZWc1Zs
VlcKYkZwNlZHeGFwVbZYVWtkYVJtUlDWMFZLZDFaWGNFdGlnbEp6VjJ0a1dHSkhVbkpEYXpGWFkw
Wm9WMDExVmxSWlYzaExwMFpXYzFacwPwbGNLVFRBME1GWkhLR0ZXYlZaWVZXdGtZVkp0VWxkV01G
WkxAREZhV0d0RmRHbE5iRXA2VmpKMGEbFduA2xSYmtwRVlycEdlbFl5CmRH0VhSMFY0WTBoS1dG
WnNjRXhwYWtaUFPfWktjd3BhUjJkTFdWUkNXazFHV2toa1IwWm9UV3MxTUZWdGRHRlpWa3B6WTBk
b1ZWwKYKU2t4YVJFwMhWMFV4VlZWdGRFNVdNVXBaVmpKMFLXSXlTa2RUYms1cVUwVndSVmxZY0Vb
bGJGbDVBbVJIT1ZoU01GWTBxVEJvUzFkRwpXbk5qUlhoV1lXdGFVRmw2Um1GamQzQlhZa2RPVEZa
R1VrSk5SVEZIVjJ0b2ExSXdXbTlVWjNNeFRVWldkR1JlZEZwV2EydzFXVlZhc1QxWXdNVWNLVjJ0
NFYySkdjSEpXTUdSWFwWktjMVZyTlZkaWEwcGFwTF3UzAxSFJYaFhibEpUVjBKNFYxbHJXbUZI
Vm14WlkwVmsKV0ZKc2JEVkrVlpJVDFab1UwMUdXVEJYVVKd1V6RmtSd3BYms1cVVsag9WMMWxY
ZEdGVlJtdzJVbTFHYW1RelFsaFphMlJQVkJVYQpSMVZyU2s1U1ZFwklWakowYjJFeFNYZFhiVVPY
WwXoTmVGVnFsB5qTVdSMFVteGFVMkpIZHpGWFZsWmhDbUV4V1hkTlZXTkxWakowCk5GWXlTa2Rq
U0VwWFRVWld0RlRpZV2tkak1WwNlUbfprYVZORlNrdfiVEYzVXpBMVNGTllhRlppYXpwWldWUktV
MVpXYkhSa1NHULQKVM0xNFdsa3dWbXNLWwtkS1IySkVWa1JpVmxwSlZERmFiMVV3TVVkwFZFSllW
a1ZLZGxwNlJscGxVWEJvWwtaYVZGbFVTbE5oUmxaeQpWbTVrVmxKc1ZqUlDnbmhQWcxUmVsRnNi
RnBpUjFGM1ZrVmFZUXBrUjFKSFdrWndWmkpJUWxsV2FrzbWakZWVZ0c1dsaGlWnBZClDXeFNS
MVPHVlhoWGVJWlVvVakZLU1ZReFdtRlViVY2VWd0d1YySkhVVEJEYkZGNFYxaGtUbFpYVGt4V2Fr
b3dDazVHYkZkVGEExcFKKwWxkb1dGUlZXbGRPUmaeLYydDBhazFWTlhsVWJGcHJZVlPpUmX0cmRG
ZGlWRVl6VlRkEmVGWxhXbGxoUmxcwF1YcFdXbGRXVWtkawpNVnBYWwtoU2ExTkhVbFFLVm0weE5G
ZHNhM2RXYlhoTFZqQmFTMLJlVWtWVWExSnBVakZKZDFaRVJtRmhNVkp6VTJ0YVdHRnNTbGhaCmJG
SkdUVVphVlZKdGRHcGtNMEpaV1ZSR2QxZFdiRlZVYKU1b1VteHdlQXBXUnpBMVYwWktkR1I2U2xa
aVZGwnlWbFJLVW1Wc1JuVlMKYkZwb1lUSTVNMVpyVm1GWlVYQllVbFJHUmxWdGVFdvVY1WkhW
Q1YyRnJhM2hXVWwSF16Rk9jMkZHV21sU01VcG9DbGRYZEdGawpNa1pIVmxoa1dHskLRbk5XYkZK
WFZqRlJlRmR1WkZkTmExWTFXa2h3UjFkR1duTlhiV2hFWWxWV05GWXhR3RVYkZwVWZhdDRWMkZy
CmIzZERhelZIVjFoc1ZHRXlVbkVLVldwS2IyRkdWbk5YkZdSUFVteHdlbFl5ZE0aE1VbDRVMnRr
VldKSFVuWldSekZMWkVaU2NWUnMKWkdsWFJVCe5Wa1pXYTF0dFZrZFdiR3hvVWpKNFZGbHNXa3RX
TVdSWFZXdbBhUXB0Vm13MFdXdG9TMVl4V2taWVGJGRkxWbTB3ZUU1SApWbk5YmxKc1UwZE9URlpY
WTNoVE1VbDVWR3RXVW1FeFNuQLdiWGgzVTJ4YVJWsnRSbWh0YTFwWVZqSjRjMVZ0UlhWUmJHeFhD
bUpZCmFHaGFSM2gzVWxaS2MyTkhhkR3R0TUVwUVZtcENWMMwXV2tkaVNFcGhVbnBzYjFwGdVHRmxa
M0JZWVRGd1VGWXdXa3RqTVdSMVlVWmEKYVZkRk1IaFhWbU40VlcxV2MxSnVbWdLVW14d2NGWnJW
bUZWVmxweVZtMUdhr1F6UWxsVmFrWmhVMFpaZVUxVVF5VmlWWEJlVmpGUwpRMVl5Um5KaU0yUlhz
V3RhVjFwV1dr0WpiVVPiVjIxc1UySnJTBhGEYkZwMFkwVTVWZ3B0UkVJMFdUQmFiMkpHU25SVmJH
eFdZV3RhCmFGVXdXbXQYkdSelDrZG9WmkV6UW1GV1ZtTjRVakZaZVZKWWJGwlhSMUpGV1Zod1Yx
TkdWwGxrUjNSb1lrVndTRmxyVmpSV01VcHoKQ2xkc1VrUm1WVEUwVlRKMGEYRnNTa2RqUlRoTFZs
ZDBhMDVHU2xkYVNGWnBUVEpTVVZac1ZURmtWbFpIVlZoa1ZHUXlPRGxEwNowOQpDZz09Cg==
```

Operations	Recipe	Input
Search...	<code>A-Za-z0-9+/=</code>	Vm5KvL3sVjRwMnhPYw1ReLfbFp1R1F3VkvVaYQpKR1JHwKZW2JlQlWako0VjFVeVnswLh1VvpYwXSR1ZGVXhXbU2UJFKSVQxmfFUBU6Umtw2JHUTBdbFF4V1hktLZXTkxWakowCk5GbfTa1pYlDowFRwLdORLZz2t6ak1VNXlUbFpRYZORlNrdfd1VEY2VTJzeFYxwLlHrLppYxpWlDwUkdkMvpYXkhsa1NHU1QKvM0xNFds3dwbXNLVjBaS2RHUKVua13pujFjd1ZERmFHVJ2U2taWGFsS1hZbFJgTUzaVj3tdGpKw0J2wKRGd1dwbFVUBES9UmwepApwRzA1V6ZkdGR6S121VfZyV1RKUmvSRmVSbFpoyT1Bm1ZrVmfZUXBYU1RGR1VteEtUbUvS5ZhpCV2Ffa3hWepHyZFoc2FGmL5MUpocLdXG6FKMkZHV1hkW6JlQnMwBFJXVjFReFduZFdNa1Y1WkhW61dGwNXMwHEYlVnFYxagTubFpYVGT4V2Frb3dDazVHV1hsVGEyUnEKYwPkb2FGvNnXBGRPUmxwe1Yydg6thMU14U2ktkVnWJHUNZWRZFLZEEZScVRSZGLXRUPNVKZWa1NtVkdmbGxouJjJ4VF1SmktWmRXVwT0aOpNVmw0WntoS1YxWkZXbFfLVM0weESHVnNXbL3sU8d0TFZrY3hTMU15VgtWUmEXsnBwbXh3U2xaRVj3tRmhNa1pYVjJ4c1VtRXpRb6XCaJYaGhaR3h3U1ZKc2NHdGTNMEpQVmpCV1lWlkd1SEphUnpsb1VteGF1Z3BYTFwUFYwWktjMwR1YUZAaVdFMHhXVnN4Vw1Wc1JuUmgKUmxcFZrVnFVVLpyVn1GaGQzQLlVakZhu0Z2eU1UQ1V1VXBHvjFSQ1YyRnJ1M2RXYWtaV1pWk6jBUZHv21sU2JrSLhDbFp0Y0U5VgpnRE10WtBab2JGsnRVbGxWYmtaAFUwmtjBGR2WkdoV2EzQmFwWmN4UjFzeVjYbFZXR1JFWHwV1NGVXlK3R0yKwWsfLrVjRWMUpzCldSUKR1VTE0VTJ9a2F5SkdjRThLVld0a056S1daSFZpTTJ5UVZsVTFKV1ZHVHvkvGQy0D1DZz09Cg=
Favourites	<input type="checkbox"/> Strict mode From Base64 Alphabet: A-Za-z0-9+/= <input checked="" type="checkbox"/> Remove non-alphabet chars	
To Base64	<input type="checkbox"/> Strict mode From Base64 Alphabet: A-Za-z0-9+/= <input checked="" type="checkbox"/> Remove non-alphabet chars	
From Base64		
To Hex		
From Hex		
To Hexdump		
From Hexdump		
URL Decode		
Regular expression		
Entropy		
		Output fideicomiso

Lo que obtenemos es la contraseña de login.php

←
→
↻
🏠
🛡️
🔑
statue.thl/login.php

🔥 Exploit-DB
🔥 Google Hacking DB
🔲 base64 | GTF0Bins
👤 Online - Reverse Sh

**pluck** log in

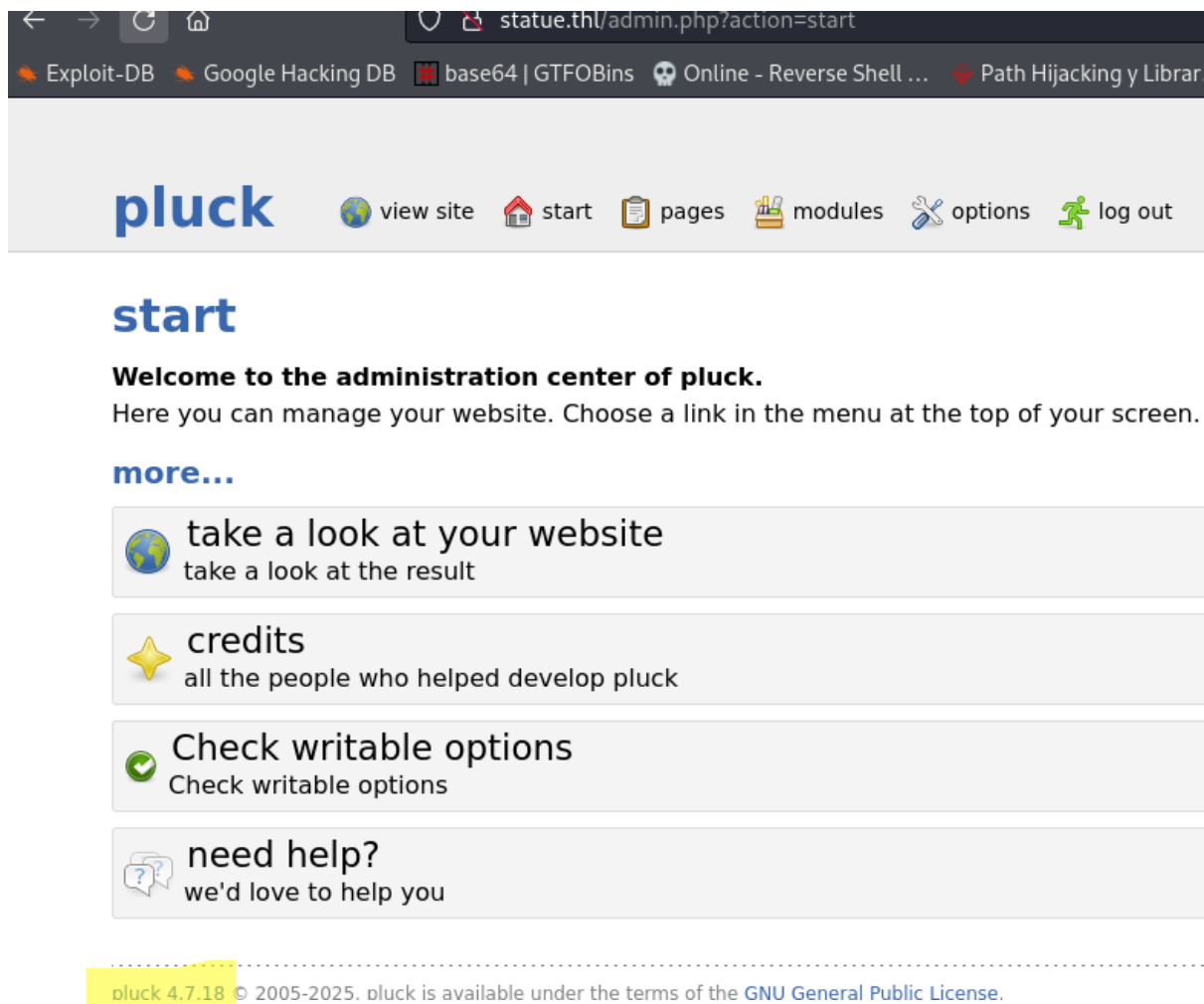
**password**

●●●●●●●●●●

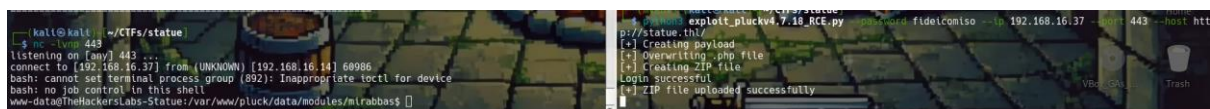
👍 Log in



Una vez dentro, vemos la versión del software, el cual podremos aprovechar para acceder a la máquina.



Personalmente usé el siguiente [script](#) para realizar el ataque. Que realmente lo que hace es generar un zip malicioso para posteriormente generar una reversehell.



Buscando por el sistema encontramos un directorio dentro de /var/www que llama bastante la atención y que dentro contiene un fichero donde tenemos una key codificada varias veces en base64 y una pass que no sabemos en qué está codificada.

También se comprueba que existe un usuario charles en el sistema.

```
www-data@TheHackersLabs-Statue:/var/www/Charles-Wheatstone$ cat pass.txt
Pass KIBPKSAFMT0IQL

Key Vm0xd1MyUXhVWghYV0d4VfLUSm9WbGx0ZUV0V01XeHpXa2M1YwXadFVuaFZNVkpUVlVaYVZrNVlW
bFpTYkVZelZUTmtkbEJSYnowSwo=

www-data@TheHackersLabs-Statue:/var/www/Charles-Wheatstone$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1::/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
syslog:x:103:104::/nonexistent:/usr/sbin/nologin
uidd:x:104:105:/run/uidd:/usr/sbin/nologin
tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin
tss:x:106:108:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:107:109:/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
charles:x:1001:1001:/home/charles:/bin/sh
```

Buscando el nombre de directorio en la red encontramos que fue responsable de un cifrado llamado Playfair.

https://es.wikipedia.org/wiki/Charles\_Wheatstone#Criptografia

acking DB | base64 | GTF0Bins | Online - Reverse Shell ... | Path Hijacking y Librar... | Brainfuck Language - ... | CyberChef | Online syntax highligh... | The image "http://

Contenidos

ocultar

Inicio

Biografía

El ingenio notable de Wheatstone también se mostró en la invención de cifrados. Fue responsable del inusual cifrado de **Playfair**, llamado así en honor a su amigo Lord Playfair. Fue utilizado por los militares de varias naciones al menos durante la Primera Guerra Mundial, y se sabe que fue utilizado durante la Segunda Guerra Mundial por los servicios de inteligencia británicos.<sup>16</sup>

Ahora, sabiendo esto y habiendo decodificado la key. Solo queda decodificar la cadena que nos falta.

Download CyberChef

Last build: 2 months ago · Version 10 is here! Read about the new features here

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

Remove non-alphabet chars

Strict mode

From Base64

Alphabet  
A-Za-z0-9+/=

Remove non-alphabet chars

Strict mode

From Base64

Alphabet  
A-Za-z0-9+/=

Remove non-alphabet chars

Strict mode

Input

Vm0xd1MyUXhVwGhYV6d4VF1USe9wbGx8ZUV0V81XeHpXa2M1YvXadFVuaFZNVkptVlVaYVZrNVlWbFpTYKVZeLZUTmtkbEJSYnowSwo=

Output

guardar

# Playfair cipher

Encrypt Decrypt

KIBPKSAFMTOIQL

Clear Options

## Result

INCOMPRENSIBLE

## Encryption key

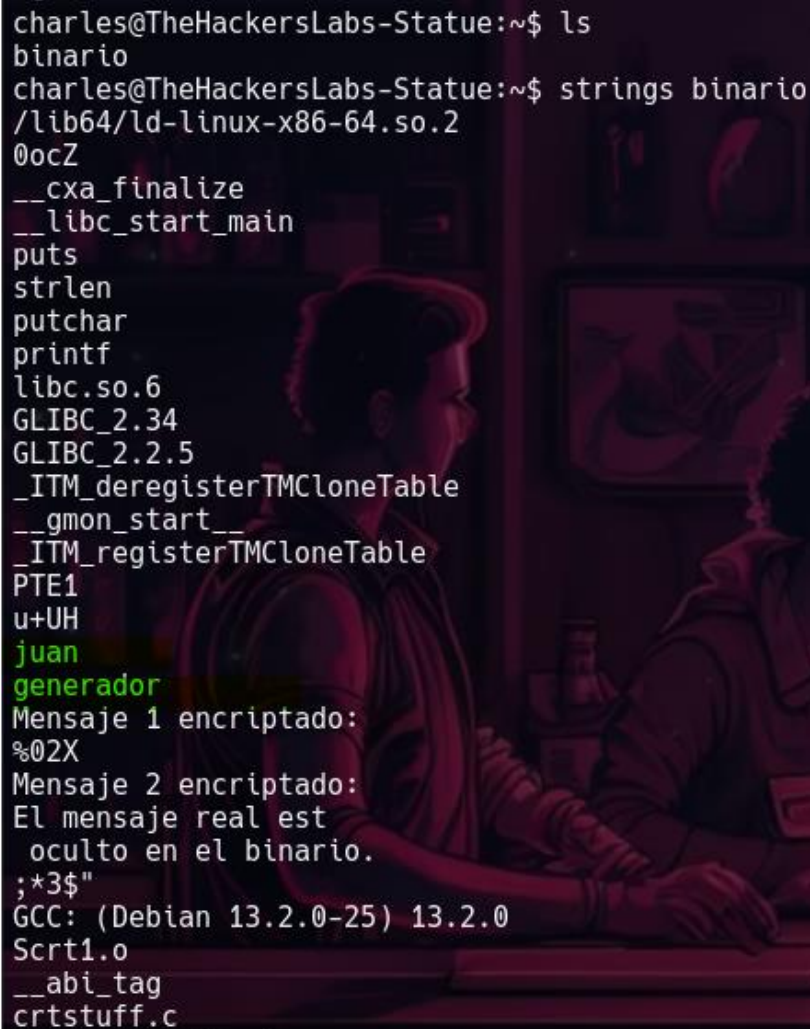
guardar

Ahora introducimos la contraseña (en minúsculas) y somos charles.

```
www-data@TheHackersLabs-Statue:/home$ su charles
Password:
$ whoami
charles
$
```



En el directorio home del usuario charles tenemos un binario el cual no es muy legible, es por ello que vamos a usar el comando strings para que no salga solo la parte “legible”. Como previamente vimos que aparte de charles habia un usuario que se llamaba juan vamos a probar con la contraseña “generador”

A terminal window with a dark background featuring a cyberpunk-style illustration of two people at a bar. The terminal text is as follows:

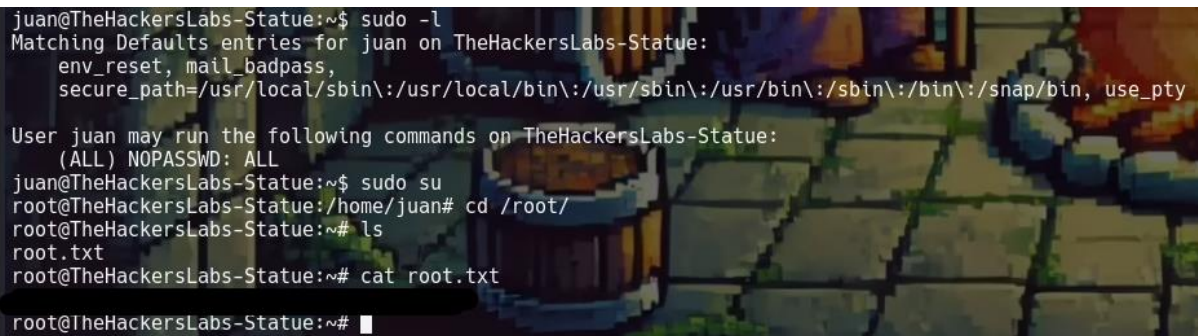
```
charles@TheHackersLabs-Statue:~$ ls
binario
charles@TheHackersLabs-Statue:~$ strings binario
/lib64/ld-linux-x86-64.so.2
0ocZ
__cxa_finalize
__libc_start_main
puts
strlen
putchar
printf
libc.so.6
GLIBC_2.34
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
juan
generador
Mensaje 1 encriptado:
%02X
Mensaje 2 encriptado:
El mensaje real est
oculto en el binario.
;*3$"
GCC: (Debian 13.2.0-25) 13.2.0
Scrt1.o
__abi_tag
crtstuff.c
```

```
juan@TheHackersLabs-Statue:/home/charles$ whoami
juan
juan@TheHackersLabs-Statue:/home/charles$
```

Obtenemos la flag de user.

```
charles@TheHackersLabs-Statue:~$ cat user.txt
```

Con el usuario juan miramos que comandos podemos usar como sudo y puesto que podemos con todos, realizamos sudo su y somos root para obtener la flag.

A terminal window with a dark background and a colorful, abstract pattern on the right side. The text shows a user named 'juan' at a machine named 'TheHackersLabs-Statue' running 'sudo -l'. The output lists permissions for 'juan', including 'env\_reset', 'mail\_badpass', and a specific 'secure\_path'. Then, 'juan' runs 'sudo su', becoming 'root'. The prompt changes from '~\$' to '~#'. The user then runs 'cd /root/' and 'ls', showing 'root.txt'. Finally, they run 'cat root.txt' and the prompt returns to '~#'.

```
juan@TheHackersLabs-Statue:~$ sudo -l
Matching Defaults entries for juan on TheHackersLabs-Statue:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User juan may run the following commands on TheHackersLabs-Statue:
    (ALL) NOPASSWD: ALL
juan@TheHackersLabs-Statue:~$ sudo su
root@TheHackersLabs-Statue:/home/juan# cd /root/
root@TheHackersLabs-Statue:~# ls
root.txt
root@TheHackersLabs-Statue:~# cat root.txt
root@TheHackersLabs-Statue:~#
```