Auditoría Web

Informe Técnico

Indice

Informe Técnico..... 1
Indice.....2
Información General..... 3
Objetivos de la Auditoría.....3
Alcance de la Auditoría.....3
Metodología..... 4
Hallazgos.....4
Nmap:.....4
Gobuster:.....5
SQL Injection.....5
Escalada de Privilegios..... 6
Flag 1..... 9
Flag 2..... 9
Hash de Contraseña..... 10
Sistema Operativo.....10
Vulnerabilidades.....10
Mitigación.....10
SQL Injection.....10
Reboot de Password.....10
Exploración.....10
Exposición de Hash.....10
Sistema Operativo..... 11
Conclusiones.....11
Agradecimiento a los organizadores.....11

Información General

- **Empresa Auditada:** INETUM
- **Fecha de Auditoría:** 10/03/2024 - 13/03/2024
- **Auditores:**
    - Facundo Santana
    - José Tipaldi
    - Aitor Segura
    - Sergio Chacon
    - Steven Vasquez Marin
- **Versión del Informe:** v1.0

Objetivos de la Auditoría

1. Llevar a cabo todas las fases del pentesting.
    a. Reconocimiento (Reconnaissance)
    b. Exploración (Scanning)
    c. Obtención de Acceso (Gaining Access)
    d. Mantenimiento de Acceso (Maintaining Access)
    e. Enumeración (Enumeration)
    f. Escalamiento de Privilegios (Privilege Escalation)
    g. Exfiltración de Datos (Data Exfiltration)
    h. Informe y Documentación (Reporting and Documentation)
2. Conseguir todas las flags.
3. Elaborar un informe final.
    a. Enumerar todas las vulnerabilidades encontradas.
    b. Dónde se han encontrado.
    c. Cómo se han encontrado.
    d. Cómo se han explotado - PoC
    e. Potencial impacto dentro del sistema - CVSS
    f. Recomendaciones.

Alcance de la Auditoría

El alcance de la auditoría web en la competencia de hackatón se centra en la evaluación presentada en forma de un CTF.

El objetivo principal es obtener todas las flags distribuidas en la infraestructura de la aplicación web, simbolizando la identificación y explotación de posibles vulnerabilidades. Al finalizar, se espera que los participantes elaboren un informe final detallando las técnicas utilizadas, las vulnerabilidades descubiertas y las recomendaciones de mitigación para mejorar la seguridad de la presencia web de la empresa simulada.

Metodología

Durante la auditoría, fue crucial utilizar una combinación de herramientas automatizadas y técnicas manuales para identificar y explotar vulnerabilidades de manera efectiva.

- **Gobuster**: Gobuster fue utilizado para realizar una exploración de directorios y archivos en el servidor web objetivo.

- **Reinicio de Contraseña del Usuario Root**: Se llevó a cabo un reinicio de contraseña para el usuario root con el objetivo de explorar posibles vulnerabilidades en la gestión de contraseñas y para evaluar la seguridad de los controles de acceso del sistema.

- **Exploración**: Se realizó exploraciones utilizando herramientas de escaneo de red y escaneo de puertos para identificar servicios en ejecución y posibles vulnerabilidades en el sistema objetivo.

- **Pivoting entre Usuarios (Movimiento Lateral)**: Se realizó pivoting entre usuarios para evaluar la seguridad de los controles de acceso y la gestión de privilegios en el sistema.

- **Inyección de SQL (SQLi) dentro de la Web**: Se llevó a cabo una inyección de SQL dentro de la aplicación web objetivo. Este método implicó la inserción de consultas SQL maliciosas a través del formulario web para obtener acceso no autorizado a la web para obtener datos sensibles.

Hallazgos

Nmap:

- Gracias al nmap pudimos obtener la información de los puertos que estaban abiertos, los servicios a los que corresponden y las versiones de cada uno de ellos.
    - -**sS** → servicio de cada puerto.
    - **-sV** → versión de cada puerto.
    - **-oN** “nombre del archivo” → guardar el escaneo en un archivo.

```
common.txt  decode  escaneo  hash  hydra.restore
❯ cat escaneo
       File: escaneo
   1   # Nmap 7.94SVN scan initiated Mon Mar 11 16:42:14 2024 as: nmap -sS -sV -oN escaneo 100.80.57.75
   2   Nmap scan report for 100.80.57.75
   3   Host is up (0.00042s latency).
   4   Not shown: 998 closed tcp ports (reset)
   5   PORT   STATE SERVICE VERSION
   6   22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
   7   80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
   8   MAC Address: 00:0C:29:B8:8A:0B (VMware)
   9   Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
  10
  11   Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
  12   # Nmap done at Mon Mar 11 16:42:21 2024 -- 1 IP address (1 host up) scanned in 7.48 seconds
```

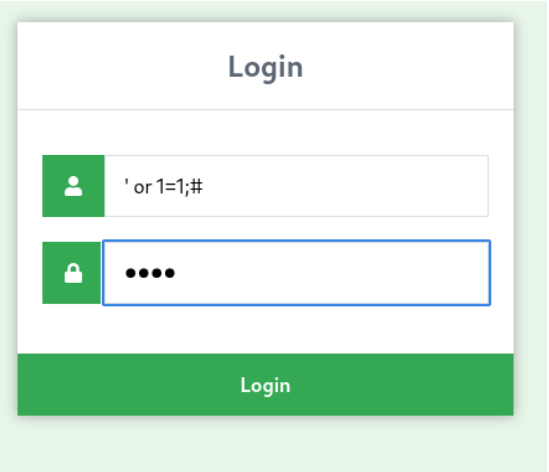
Gobuster:

- Con el gobuster podemos analizar a fondo la estructura de la web. Este nos permite mediante un ataque de fuerza bruta de diccionario, un escaneo de directorios o archivos.
    - **-u** → indicamos la web que queremos analizar.
    - **-w** → indicamos el diccionario de fuerza bruta que vamos a utilizar.
    - **-x** → indicamos los tipos de archivos que queremos que busque.

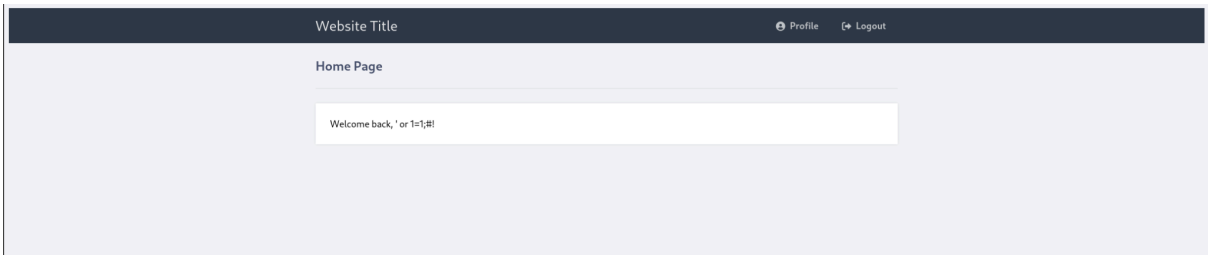
```
❯ gobuster dir -u http://192.168.1.88 -w common.txt -x txt,php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.88
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta.html            (Status: 403) [Size: 277]
/.hta.php             (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/.hta.txt             (Status: 403) [Size: 277]
/.htaccess.html       (Status: 403) [Size: 277]
/home.php             (Status: 302) [Size: 0] [--> index.php]
/index.html           (Status: 200) [Size: 733]
/index.html           (Status: 200) [Size: 733]
/logout.php           (Status: 302) [Size: 0] [--> index.html]
/myphpnuke.php        (Status: 401) [Size: 24]
/profile.php          (Status: 302) [Size: 0] [--> index.html]
/server-status        (Status: 403) [Size: 277]
Progress: 18920 / 18924 (99.98%)
===============================================================
Finished
===============================================================
```

SQL Injection

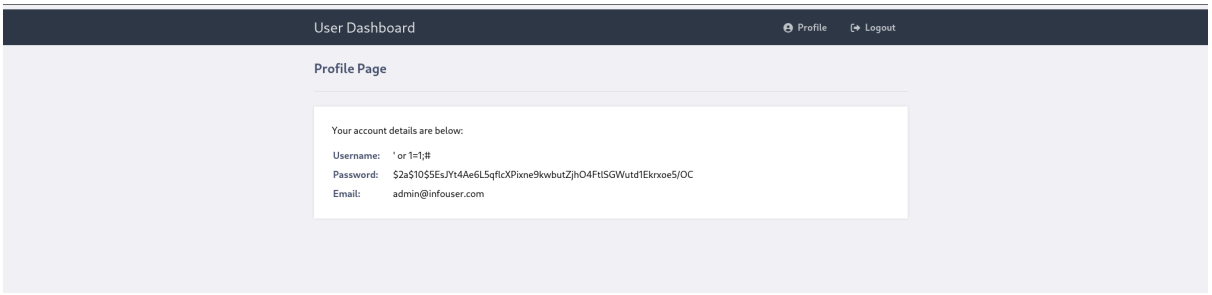
- Se logró corromper mediante SQL Injection, el inicio de sesión del usuario “admin”, en la aplicación web.



En el usuario escribimos la inyección y en la contraseña lo que queramos y finalmente le damos enter.



Entramos a la web y nos dirigimos al apartado profile para ver a qué usuario le corresponde la información.

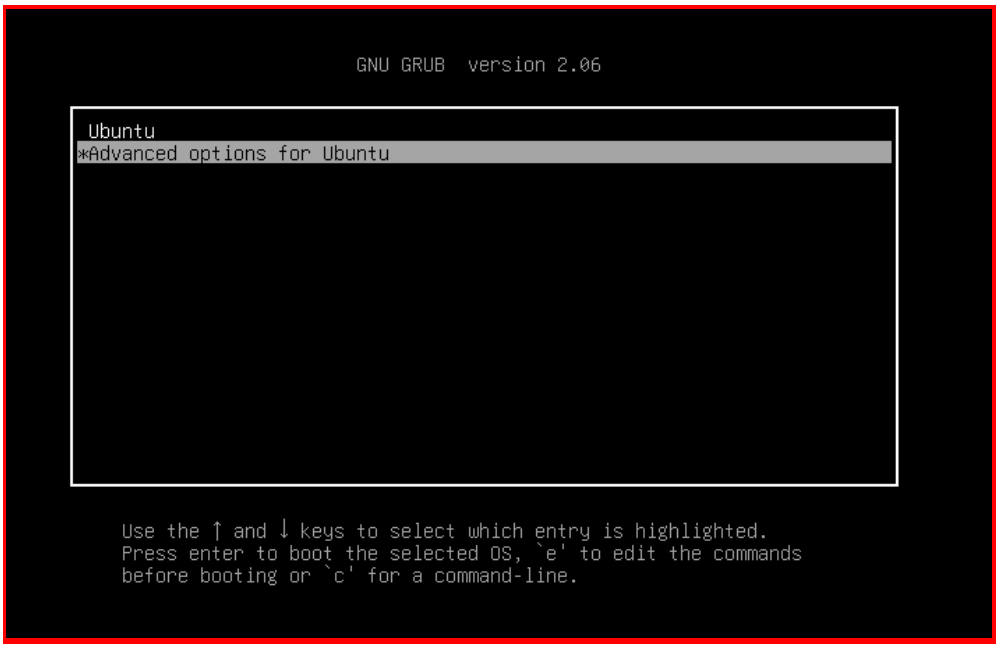


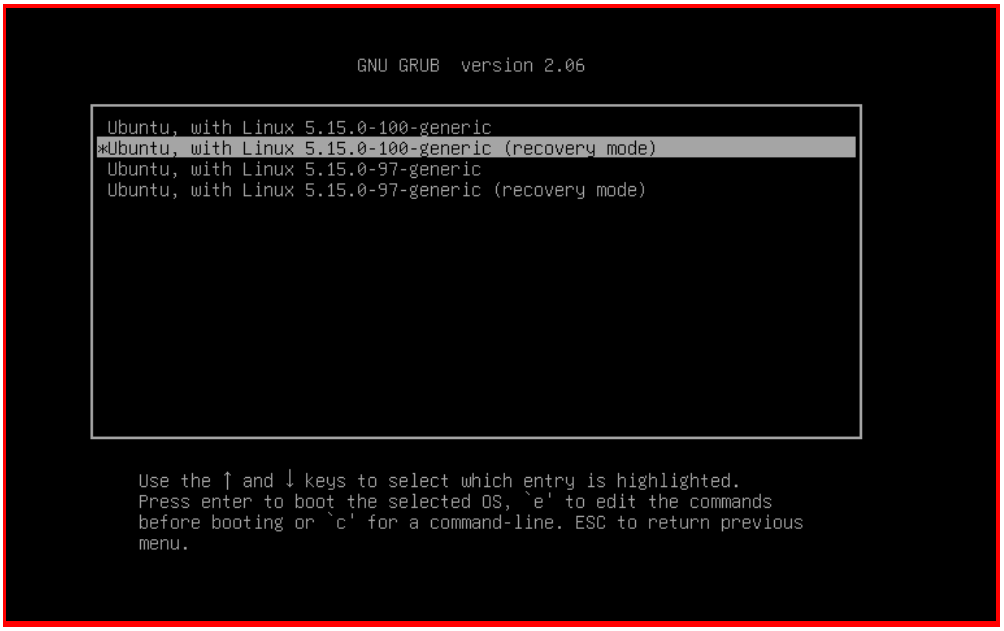
Con esto vemos que corresponde al usuario y nos da el hash de la contraseña de este. El usuario a quién le corresponde es el administrador. El hash está en SHA256.

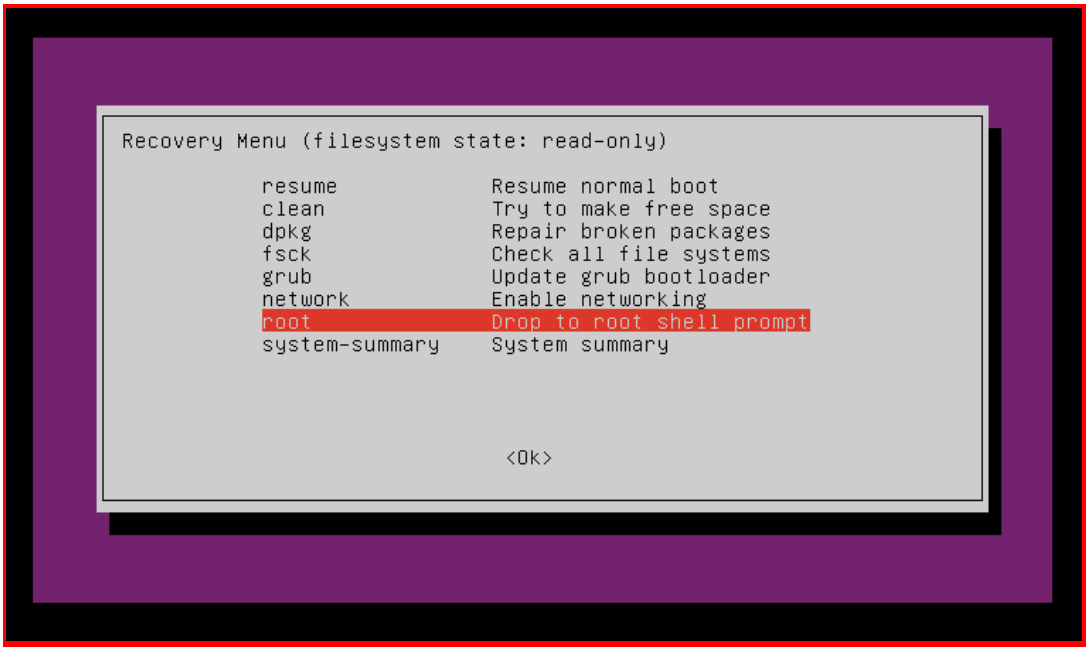
Escalada de Privilegios

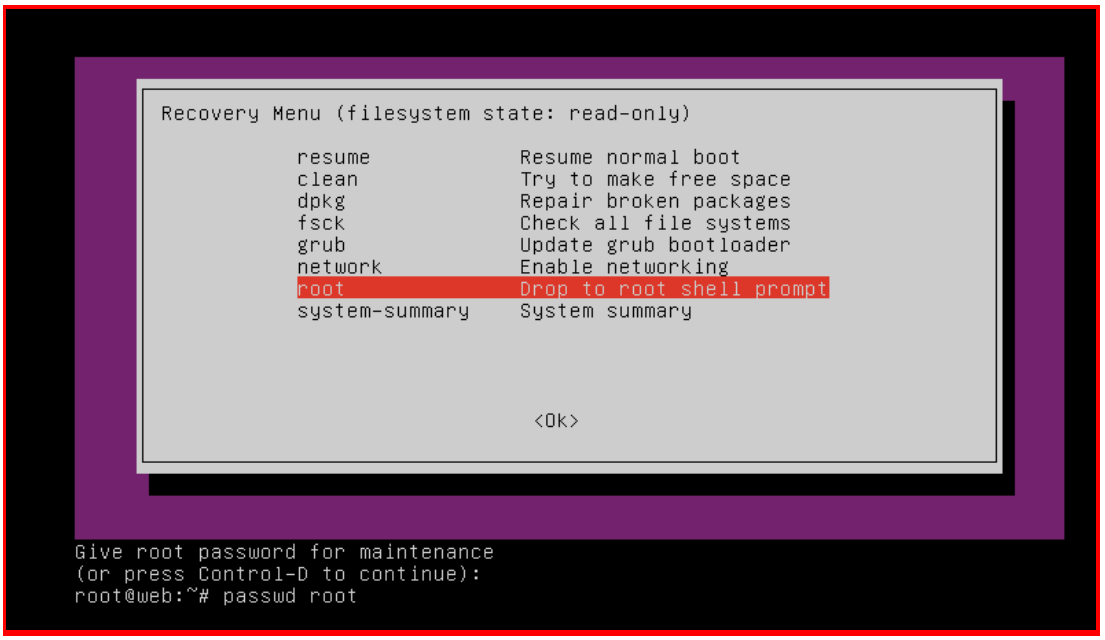
- Mediante un reboot de password del usuario “root” en el “Recovery Mode”, se logró tener acceso a la máquina con el máximo de privilegios. Pasos:

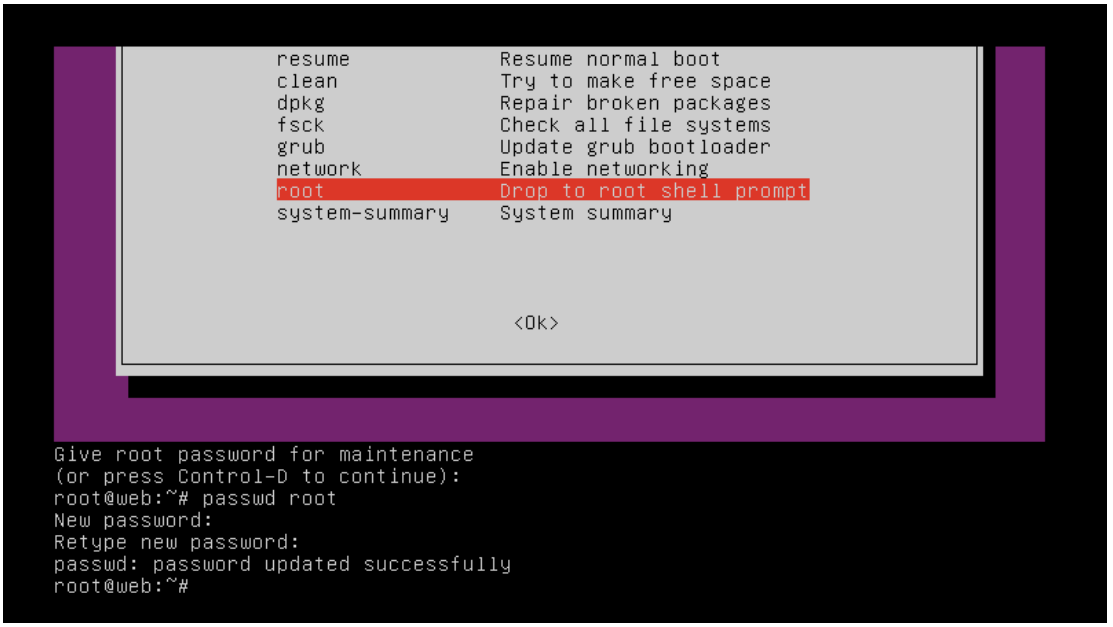
1. Reiniciar Ubuntu.
2. Pulsamos ESC + MAYUS, para obtener las opciones avanzadas del sistema en el kernel (núcleo) de Linux.
3. Ingresamos al “Recovery Mode”.
4. Nos desplazamos hasta la opción “root - Drop to root shell prompt”
5. Ejecutamos el comando “passwd root”, para cambiar la contraseña del usuario root.
6. Ingresamos y confirmamos la contraseña.
7. Ejecutamos el comando “reboot”, para reiniciar el sistema.
8. Ingresamos con la nueva credencial del usuario root.





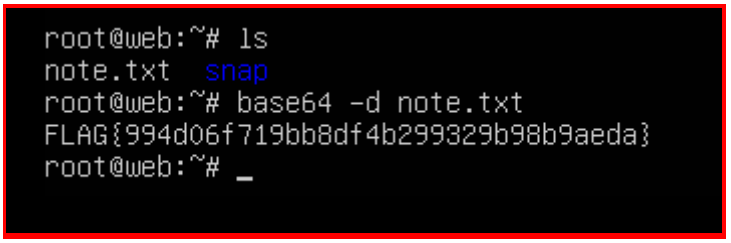

Recovery Menu (filesystem state: read-only)
resume Resume normal boot
clean Try to make free space
dpkg Repair broken packages
fsck Check all file systems
grub Update grub bootloader
network Enable networking
root Drop to root shell prompt
system-summary System summary
<Ok>


Recovery Menu (filesystem state: read-only)
resume Resume normal boot
clean Try to make free space
dpkg Repair broken packages
fsck Check all file systems
grub Update grub bootloader
network Enable networking
root Drop to root shell prompt
system-summary System summary
<Ok>
Give root password for maintenance
(or press Control-D to continue):
root@web:~# passwd root



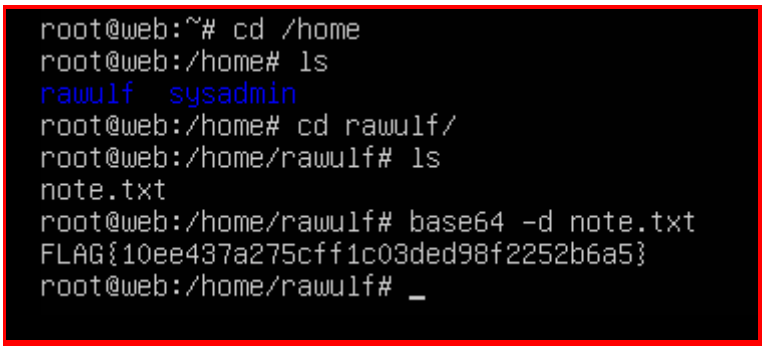
Flag 1

- Mediante exploración entre archivos, ficheros y directorios, se logró obtener la primera flag, que utiliza un cifrado base64.



Flag 2

- Mediante exploración en el directorio “home”, se encontró la segunda flag que utiliza un cifrado base64.



Hash de Contraseña

- En el apartado “my profile” del usuario ADMIN, se obtuvo el hash de contraseña de dicho usuario.

Sistema Operativo

- Ubuntu 22.04.4.
- CVE’s:
    - CVE-2023-38647
    - CVE-2023-38648
    - CVE-2023-38649

Vulnerabilidades

- Web vulnerable SQL Injection.
- No dispone de seguridad de acceso a “Recovery Mode”.
- Información sensible expuesta.
- No se limita el acceso a archivos y directorios.
- Sistema Operativo “Ubuntu” v.22.04.4, que presenta diversas vulnerabilidades conocidas y con una criticidad ALTA.

Mitigación

- Utilización de Firewall.
- Implementar seguridad en Kernel.
- Utilización de Endpoint.
- Formación y concientización en Ciberseguridad.

SQL Injection

- Sanitizar y validar los inputs en la aplicación web.
- Implementación de WAF.

Reboot de Password

- Reforzar en la BIOS el ingreso a “Recovery Mode”.
- Implementación de políticas de contraseñas robustas.
- Implementación de políticas de gestión de contraseñas.

Exploración

- Restringir el acceso a directorios y archivos sensibles mediante permisos.

Exposición de Hash

- No exponer datos sensibles del usuario.
- Utilizar 2FA, en caso de robo de credenciales o acceso mediante SQL Injection.

Sistema Operativo

- Actualización del sistema y parches de seguridad.

Conclusiones

Se identificaron varias vulnerabilidades significativas dentro de la máquina virtual proporcionada para la evaluación. Se encontró una vulnerabilidad de inyección SQL en la aplicación web, lo que potencialmente permite a un atacante acceder y manipular la base de datos. Además, se observó la ausencia de medidas de seguridad adecuadas para el acceso al modo de recuperación. Se identificó la exposición de información sensible y la falta de restricciones de acceso a archivos y directorios, lo que podría facilitar a un atacante el acceso no autorizado a datos críticos.

Para mitigar estos riesgos, se recomienda implementar medidas como la validación y sanitización de entradas en la aplicación web, el fortalecimiento de las políticas de contraseñas y la restricción del acceso a archivos sensibles mediante permisos adecuados. Además, se sugiere la implementación de autenticación de dos factores (2FA) en caso de exposición de credenciales o acceso mediante inyección SQL.

Agradecimiento a los organizadores

Nos gustaría expresar nuestro sincero agradecimiento a las empresas organizadoras del evento por ofrecer esta emocionante competencia. La organización de este evento nos brinda una valiosa oportunidad para poner a prueba nuestras habilidades. Agradecemos su compromiso con la comunidad de ciberseguridad y esperamos volver a trabajar juntos en el futuro.