Imagen que contiene copa, interior

Descripción generada con confianza muy alta

**PENTEST**

**RESUMEN TÉCNICO DE**

**VULNERABILIDADES Y HALLAZGOS**

**MAYO, 2025**

**Victor campos / Sergio garduño / Daniela campos**

[v.campos@consultora-tecnologica.site](mailto:v.campos@consultora-tecnologica.site) [/sergio.garduno@consultora-tecnologica.site](mailto:/sergio.garduno@consultora-tecnologica.site)/teach.lead@consultora-tecnologica.site **T.** 55 49526429

|  |  |
| --- | --- |
| **Propiedades del Documento Título** | **Reporte Pentest caja negra / Gris** |
| **Versión** | 1.0 |
| **Autor** | victor campos/ Daniela campos |
| **Pentester** | sergio garduño |
| **Revisado Por** | VICTOR CAMPOS |
| **Aprobado por** |  |
| **Clasi**fi**cación** | Confidencial |

Contenido

[1. RESUMEN EJECUTIVO 4](#_Toc201237517)

[1.1. OBJETIVO 4](#_Toc201237518)

[1.2. ALCANCE 4](#_Toc201237519)

[1.3. METODOLOGIA 6](#_Toc201237520)

[2. HALLAZGOS 7](#_Toc201237521)

[2.1. RECONOCIMIENTO DEL ACTIVO 7](#_Toc201237522)

[2.2. FTP expuesto 8](#_Toc201237523)

[2.3. SSH expuesto 9](#_Toc201237524)

[2.4. Puerto 443 o servicio HTTPS 11](#_Toc201237525)

[2.5. Puerto RTSP 16](#_Toc201237526)

[2.6. Puerto 3306 mysql 18](#_Toc201237527)

[2.7. Ingreso por SSH con un usuario sin privilegios. 20](#_Toc201237528)

[2.8. Aprovechamiento de CVEs identificados 21](#_Toc201237529)

[2.8.1 ¿Escalamiento de privilegios? 21](#_Toc201237530)

[2.9. ¿Entonces qué podemos explotar? 23](#_Toc201237531)

[2. VULNERABILIDADES 27](#_Toc201237532)

[2.1. DESCRIPCION DE VULNERABILIDADES 28](#_Toc201237533)

[2.1.1. Linux Distros Unpatched Vulnerability : CVE-2024-26720 29](#_Toc201237534)

[2.1.2. Linux Distros Unpatched Vulnerability : CVE-2013-7445 30](#_Toc201237535)

[2.1.3. Linux Distros Unpatched Vulnerability : CVE-2018-12931 30](#_Toc201237536)

[2.1.4. Linux Distros Unpatched Vulnerability : CVE-2018-12930 31](#_Toc201237537)

[2.1.5. Linux Distros Unpatched Vulnerability : CVE-2019-15794 32](#_Toc201237538)

[2.1.6. Linux Distros Unpatched Vulnerability : CVE-2019-19814 32](#_Toc201237539)

[2.1.7. Linux Distros Unpatched Vulnerability : CVE-2016-2568 33](#_Toc201237540)

[2.1.8. Linux Distros Unpatched Vulnerability : CVE-2016-8660 33](#_Toc201237541)

[2.1.9. Linux Distros Unpatched Vulnerability : CVE-2017-13693 34](#_Toc201237542)

[2.1.10. Linux Distros Unpatched Vulnerability : CVE-2017-13165 34](#_Toc201237543)

[2.1.11. Linux Distros Unpatched Vulnerability : CVE-2018-12928 35](#_Toc201237544)

[2.1.12. Linux Distros Unpatched Vulnerability : CVE-2015-7837 35](#_Toc201237545)

[2.1.13. Linux Distros Unpatched Vulnerability : CVE-2015-8553 36](#_Toc201237546)

[2.1.14. Linux Distros Unpatched Vulnerability : CVE-2017-0537 36](#_Toc201237547)

[2.1.15. Linux Distros Unpatched Vulnerability : CVE-2020-14304 37](#_Toc201237548)

[2.1.16. Linux Distros Unpatched Vulnerability : CVE-2020-35501 38](#_Toc201237549)

[2.1.17. PostgreSQL Client/Server Installed (Linux) 38](#_Toc201237550)

[2.1.18. Docker Container File Change Detection 39](#_Toc201237551)

[2.1.19. Software Enumeration (SSH 39](#_Toc201237552)

[2.1.20. VMWare Tools or Open VM Tools Installed (Linux) 40](#_Toc201237553)

[2.1.21. Tukaani XZ Utils Installed (Linux / Unix) 40](#_Toc201237554)

[2.1.22. Apache Log4j Installed (Linux / Unix) 41](#_Toc201237555)

[2.1.23. Containerd Installed (Linux) 42](#_Toc201237556)

[2.1.24. MySQL Server Installed (Linux) 42](#_Toc201237557)

[3. VULNERABILIDADES de aplicativo web 43](#_Toc201237558)

[3.1.1. Missing HTTP Strict Transport Security Policy 43](#_Toc201237559)

[**3.1.2.** **PHP Input Variables Exceeded** 45](#_Toc201237560)

[3.1.3. Cookie Without HttpOnly Flag Detected 46](#_Toc201237561)

[**3.1.4.** **Cookie Without Secure Flag Detected** 48](#_Toc201237562)

[3.1.5. Missing 'X-Frame-Options' Header 49](#_Toc201237563)

[3.1.6. Missing 'X-Content-Type-Options' Header Policy 51](#_Toc201237564)

[3.1.7. SSL/TLS Weak Cipher Suites Supported 52](#_Toc201237565)

[3.1.8. Missing 'Cache-Control' Header 55](#_Toc201237566)

[3.1.9. Missing Content Security Policy 56](#_Toc201237567)

[3.1.10. HTTP Header Information Disclosure 58](#_Toc201237568)

[4. HALLAZGOS APLICATIVO WEB 60](#_Toc201237569)

[5. Anexo 62](#_Toc201237570)

# RESUMEN EJECUTIVO

**Tecnología-Consultoría realizó** pruebas de intrusión a la red **Interna** donde se aloja el servidor con IP 195.35.14.19 en el tenan de la nube.

El propósito de estas actividades fue conocer el estado de seguridad de los activos evaluados, mediante la simulación de las actividades que realizaría un usuario malintencionado, buscando comprometer al activo bajo evaluación perteneciente a **CGA-ASOCIADOS**.

Las pruebas de intrusión se efectuaron mediante el uso de herramientas automáticas especializadas, así como con la ejecución de diversas validaciones de forma manual, a fin de evaluar el comportamiento del activo antes señalado.

## 1.1. OBJETIVO

El objetivo principal del ejercicio es conocer el estado de seguridad de la infraestructura mediante la ejecución de pruebas de intrusión que permitan determinar si existen vulnerabilidades que pudieran facilitar alguna intrusión interna y/o el compromiso de información.

A continuación, se presentan los objetivos particulares de las pruebas de intrusión:

● Simular las actividades que realizan los usuarios malintencionados (atacantes/ciberdelincuentes) para comprometer los activos tecnológicos y de información bajo evaluación.

● Identificar y aprovechar las vulnerabilidades presentes en los activos tecnológicos y de información bajo evaluación.

● Informar de manera ejecutiva sobre los hallazgos realizados durante las pruebas realizadas, clasificándolos por su severidad y en el caso de las vulnerabilidades por su prioridad de remediación.

● Documentar los detalles técnicos de los hallazgos realizados durante las pruebas de intrusión para los cuales se emitirán algunas recomendaciones que permitan aminorar o mitigar el riesgo inherente a cada uno de ellos.

● Reporte de radiación de vulnerabilidades que se entregará de forma detallada los pasos a seguir para remediar las vulnerabilidades que se encontraron en las pruebas realizadas, este documento se entregará en un documento anexo a este reporte.

## 1.2. ALCANCE

El Alcance de las pruebas de intrusión efectuadas para **CGA-ASOCIADOS** se detalla a continuación:

|  |  |
| --- | --- |
| Rubro | Detalle |
| Activos | Las pruebas de instrucción se centraron en la ip proporcionada por CGA-ASOCIADOS 195.35.14.19. |
| Periodo de ejecución de pruebas | Las pruebas de instrucción fueron realizadas en el periodo comprendido del 21 de abril a las 9:00 am al 27 de mayo del 2025 |
| Tipo de pruebas | Pruebas de intrusión considerando el análisis de vulnerabilidades, gestión de configuraciones vulnerables (configuraciones predeterminadas), autenticación, manipulación de parámetros, revisión de versiones de aplicativos vulnerables, uso de técnicas específicas de ataques en función de la información obtenida durante las actividades de reconocimiento. |
| Tipo de análisis | ● Desde el punto de vista del conocimiento previo: **Caja Negra/Gris**  ● Desde el punto de vista del nivel de intrusión: **Pruebas de intrusión (hackeo ético)**  ● Desde el punto de vista del origen de las pruebas: **Interna**  ● Desde el punto de vista del tipo de pruebas: **Híbridas (automáticas y manuales)** |
| Ámbito | Los activos evaluados durante las pruebas de instrucción están disponibles dentro de la red interna del tenan asignado a la ip 195.35.14.0/24 |
| Equipamiento y herramientas utilizadas durante las pruebas | Para las pruebas manuales se utilizó:  **● Kali Linux**  Durante la prueba automatizada se utilizó:  **● Tenable** |
| Reglas de compromiso | Entre las reglas de **compromiso** determinadas en la metodología utilizada, se destaca la que atañe a la realización de pruebas de seguridad pasiva, es decir, sin comprometer la ***integridad*** ni la ***disponibilidad*** de los activos bajo análisis. |

## 1.3. METODOLOGIA

La metodología empleada por **Tecnología Consultoría consiste** en la integración y adaptación de diversos marcos de referencias y estándares aceptados y reconocidos por la industria (NIST 800- 115, PTES, EC-Council/CEH y OWASP).



El siguiente gráfico muestra de forma esquematizada y de alto nivel, los procesos y actividades involucrados durante el servicio a realizar.

El siguiente gráfico muestra de forma esquematizada y de alto nivel, los procesos y actividades involucrados durante el servicio a realizar.

Texto

El contenido generado por IA puede ser incorrecto.

# HALLAZGOS

A continuación, se definen algunos conceptos que resultarán útiles para la comprensión de los elementos que se van a tratar a lo largo de todo el documento.

## RECONOCIMIENTO DEL ACTIVO

En la realización del pentest, una de las partes importantes es reconocer el objetivo al cual se le realizara dicha acción.

Desde un **punto de vista técnico**, la **fase de reconocimiento** (o *reconnaissance*) en un pentest (prueba de penetración) es **la primera etapa del ciclo de ataque ético**, cuyo objetivo es **recolectar toda la información posible sobre el objetivo** antes de intentar una intrusión. Esta fase se divide comúnmente en dos subfases:

Reconocimiento activo y pasivo.

Actualmente se está realizando un tipo de reconocimiento activo en el cual el objetivo se Involucra **interacción directa con el sistema objetivo**. Es más detectable, pero suele ser más preciso.

Y el tipo de información a buscar es el siguiente:

* Direcciones IP activas y rangos.
* Puertos y servicios abiertos.
* Sistemas operativos y versiones.
* Aplicaciones web y frameworks.
* Infraestructura de red (firewalls, IDS/IPS).
* Usuarios o nombres de dominio.
* Vulnerabilidades potenciales (sin aún explotarlas).

Durante la fase de reconocimiento de la ip 195.35.14.19 la cual es el objetivo para realizar dicho pentest se tuvo lo siguiente.



Se realizo un escaneo a la ip y se encontró que cuenta con algunos servicios expuestos a internet.

Texto

El contenido generado por IA puede ser incorrecto.

Durante este primer paso encontramos protocolos importantes para varios vectores de ataque.

Una vez detectado estos protocolos que están expuestos se procede a tratar de identificar las versiones del mismo y si es posible que en el reconocimiento se tenga el acceso a alguna vulnerabilidad.

## FTP expuesto

Se detecta servicio FTP.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Aun con la detección del servicio FTP, se identifica que el primer protocolo está bien configurado porque te cierra las sesiones anónimas que es uno de los primeros pasos a realizar.

Texto

El contenido generado por IA puede ser incorrecto.

Por lo que es un buen punto de configuración de parte del administrador. Sin embargo, se recomienda utilizar otros servicios que sustituya a FTP como SFTP.

## SSH expuesto

Posterior se intentó realizar la identificación del protocolo SSH (puerto 22)

Texto

El contenido generado por IA puede ser incorrecto.

De la seguridad que pudimos observar en el puerto SSH

Es el siguiente:

**Kex Algorithms (Intercambio de claves):**

* Usa algoritmos **modernos y fuertes** como:
  + sntrup761x25519-sha512@openssh.com (post-cuántico + x25519)
  + curve25519 y ecdh-sha2-\* (seguros)
* Solo **uno potencialmente débil**:
  + diffie-hellman-group14-sha256 es decente, **mejor que SHA1**, pero no lo más moderno.

**Key Algorithms:**

* Usa rsa-sha2, ecdsa, y ed25519 → todos seguros y actuales.

**Encryption Algorithms:**

* chacha20-poly1305, aes-gcm, y aes-ctr → **seguros** y modernos.

**MAC Algorithms:**

* Incluye:
  + hmac-sha1
  + hmac-sha1-etm@openssh.com

Aunque SHA-1 no es crítico en MACs, **ya no se recomienda**. Podría ser el punto más débil aquí.

**Compresión:**

* none y zlib@openssh.com → normal, sin riesgos conocidos si no hay canales MiTM.

**Conclusión:**

Este servidor **no tiene una configuración insegura** de SSH, así que:

No es viable un ataque de downgrade, ni MiTM trivial.

El único detalle es que acepta SHA1, pero no es suficiente para explotar algo directamente.

## Puerto 443 o servicio HTTPS

Durante la fase de reconocimiento uno de los puertos básicos que cualquier aplicación web tiene es el puerto SSL.

Se realizar una fase de reconocimiento sobre las ciphers.

Texto

El contenido generado por IA puede ser incorrecto.

**✅ Seguridad del cifrado:**

* Usa solo **TLS 1.2 y 1.3**, nada de SSL ni TLS 1.0/1.1 → eso está muy bien en temas de configuración.
* Cifrado fuerte:
  + AES-GCM, ChaCha20-Poly1305, ECDHE\_RSA → todos con calificación **A**.
* No se encontraron **cifrados débiles o vulnerables**.

No parece haber vector directo de ataque desde SSL/TLS. Lo cual es un Buen trabajo del administrador.

**¿Qué significa ese certificado “TRAEFIK DEFAULT CERT”?**

Esto es **muy interesante**:

* TRAEFIK es un **proxy reverso y balanceador de carga** muy usado en despliegues con contenedores como **Docker** o **Kubernetes**.
* El nombre del cert y el **DNS alternativo** apuntan a una app que probablemente está detrás de un **proxy Traefik**, corriendo en contenedores.

**Esto sugiere que hay varios servicios corriendo en backends internos**, posiblemente con rutas como:

cpp

https://195.35.14.19/dashboard

https://195.35.14.19/api

<https://195.35.14.19:3000/>

Se reviso la información obtenida lo cual es correcta.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Sitio web

El contenido generado por IA puede ser incorrecto.

Al parece esta página de **Dockploy** es una herramienta diseñada para facilitar el **despliegue automatizado de contenedores Docker** en entornos de desarrollo o producción. El nombre es una combinación de "Docker" y "Deploy". Aunque existen varios proyectos o scripts con ese nombre en GitHub o en otros sitios.

Por lo que aquí se intentó ocupar los mismos scripts para detectar si estaba por default el login de dockploy.

Texto

El contenido generado por IA puede ser incorrecto.

Se intenta de igual manera tratar de enumerar los archivos potenciales en los cuales se puede obtener información sobre la app

Texto

El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.

## Puerto RTSP

Se realiza un escáner para el protocolo rtsp , es un protocolo propio de cámaras de video en el cual se observan algunos accesos.

Texto

El contenido generado por IA puede ser incorrecto.

Se realizan intentos para ver si dio algunas rutas de video en vivo o en su caso nos pida autenticación.

Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.

Así como intentar vulnerar el protocolo para poder inyectar código y poder obtener la imagen de la cámara, lo cual es un buen punto para la configuración porque no se pudo inyectar algún template.

Texto

El contenido generado por IA puede ser incorrecto.

## Puerto 3306 mysql

**Resumen del puerto 3306:**

* **MySQL versión:** 8.0.41-0ubuntu0.24.04.1
* **Sistema:** Probablemente Ubuntu 24.04
* **Autenticación:** Usa caching\_sha2\_password (es el método de login por defecto en MySQL 8).
* **Servicio está abierto al mundo** (eso ya es mala práctica de seguridad).

Imagen en blanco y negro

El contenido generado por IA puede ser incorrecto.

En este punto debido a que es un servicio se hicieron 2 test , los cuales consistieron en enviar un ataque de fuerza bruta a logueo anónimos y otro un ataque con más envió de autenticaciones.

Texto

El contenido generado por IA puede ser incorrecto.

Y en la segunda fase fue enviar un intento, pero con intentos de logueo mayores.

Texto

El contenido generado por IA puede ser incorrecto.

## Ingreso por SSH con un usuario sin privilegios.

Derivado de un pentest de caja gris, con un usuario normal sin privilegios se intenta buscar y tratar de realizar el escalado de privilegios

En primer lugar, necesitamos saber a que sistema estamos auditando, en este caso es un servidor Ubuntu.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Tienes un sistema nuevo donde muchas **CVE antiguas (2013–2023)** ya no son explotables directamente, **a menos que**:

* Se haya instalado software vulnerable (ej: aplicaciones web antiguas, versiones viejas de Apache, etc).
* El kernel se haya recompilado con fallos o no se haya parcheado.

**PROTECCIONES PRESENTES**

* AppArmor está habilitado, pero tu proceso no tiene perfil (unconfined) → no limita tu ejecución.
* Seccomp está **deshabilitado**.
* User namespaces y Cgroup2 habilitados → pueden permitir ciertos bypasses con exploits modernos.
* Kernel moderno 6.8.0 reduce muchas posibilidades, pero sigue expuesto si hay una mala configuración de Docker o servicios.

Dentro de los primeros pasos como empresa auditora del pentester , teniendo un usuario valido buscaremos malas configuración o archivos que tengan muchos permisos de escritura y lectura. Por lo que se buscará automáticamente vulnerabilidades locales, binarios mal configurados, servicios, sudoers, permisos especiales, y mucho más.

## Aprovechamiento de CVEs identificados

De las vulnerabilidades detectadas se toma el Top para explotarlas, sin embargo, se observa que no pueden explotarse ya que algunas son un riesgo solo si tienen otros servicios configurados, como java, tomcat, apache, etc. que permita el aprovechamiento de la detección.

| **CVE** | **Tipo** | **¿Explotable en kernel 6.8?** |
| --- | --- | --- |
| CVE-2020-14356 | Escalada en mremap() | ❌ Parcheado desde kernel 5.9+ |
| CVE-2013-7445 | Use-after-free en pppolac | ❌ Parcheado hace años |
| CVE-2019-15794 | Stack overflow (vhost\_net) | ❌ Kernel parchado |

**Conclusión**: Todas estas **ya no son explotables** directamente en tu sistema por el kernel actualizado que se encontró. El kernel actual es 6.8.0-57.59, sin embargo, se recomienda actualizar a 6.8.0-58.60

## ¿Escalamiento de privilegios?

Una vez que se obtuvo ayuda con el análisis de vulnerabilidades se intento realizar un escalamiento de privilegios aprovechando el tema de que faltan algunos parches en el sistema .

Para esto se ocupo la plataforma de metasploit con un modulo de Ubuntu ya que es el sistema operativo en el cual esta alojado el sistema operativo



Una vez dentro se envio el ataque para poder escalar privilegios con el usuario que nos proporcionaron si permisos.

Se ejecuta el payload intentando escalar privilegios.

Texto

El contenido generado por IA puede ser incorrecto.

Como podemos observar derivado que los archivos comunes están bien configurados y no se encontró algún archivo con permisos 777 , el payload practicament no se pudo crear una sesión.

Esto derivado de la buena configuración del servidor y el kernel actualizado.

## ¿Entonces qué podemos explotar?

Dependerá de lo que la búsqueda encuentre. Las posibilidades más comunes:

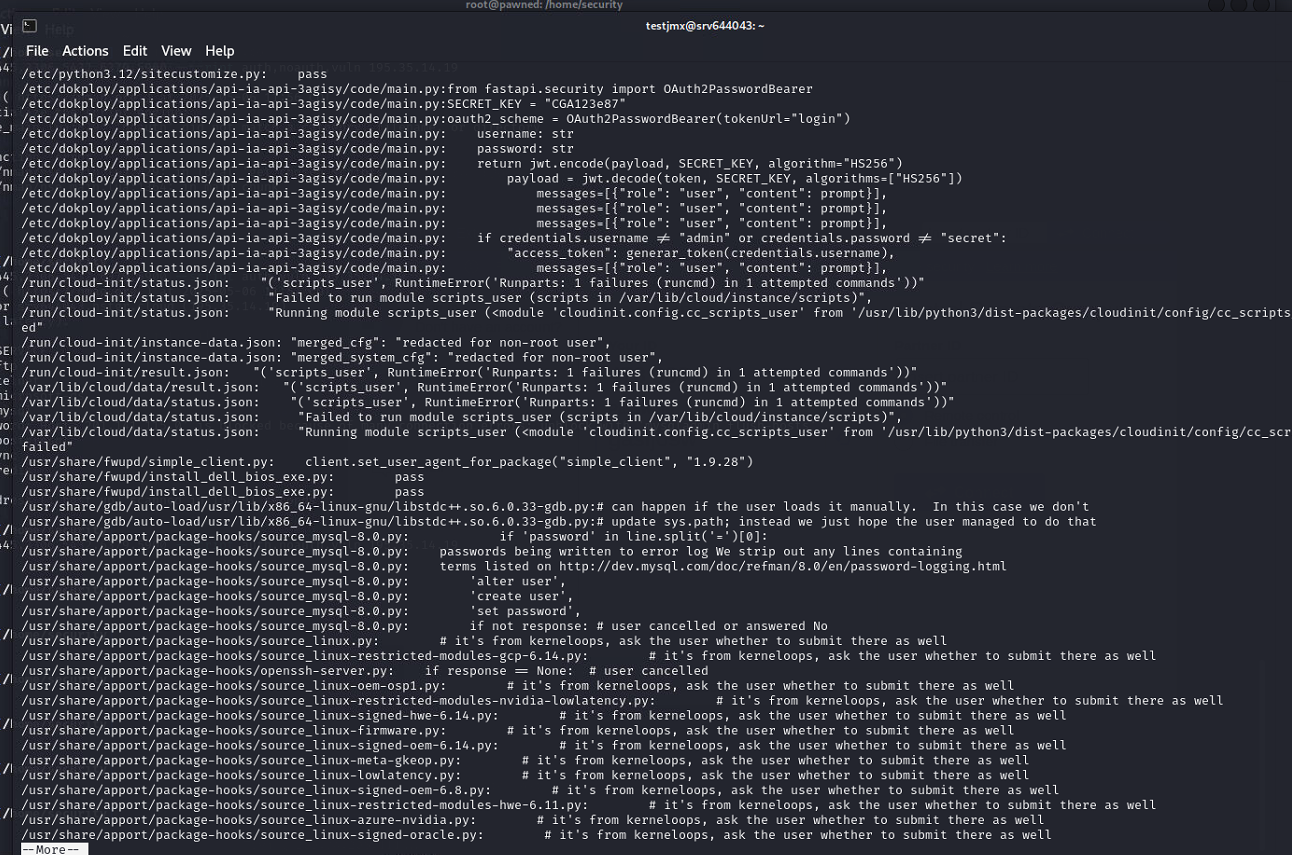
* Binarios con cap\_setuid=ep
* Archivos de contraseñas en texto plano
* Crontabs mal configurados
* Comandos disponibles con sudo sin contraseña
* Servicios expuestos en red (como web apps con bugs)

1. Se encontró que con un usuario normal sin privilegios si se pudo descargar una herramienta para hacer una búsqueda muy rápida de archivos con texto plano y demás.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Dentro de lo que la herramienta encontró, se muestran unas credenciales en texto plano en un archivo de configuración, así como una secret key.



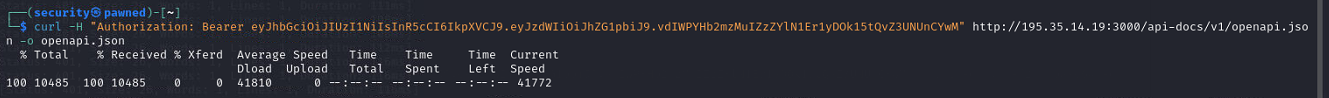
Una vez obteniendo esas credenciales y ese secret\_key las ocuparemos para intentar levantar una instancia en Docker sin que contemos con las credenciales de acceso a dockploy.

Por lo que se generó un pequeño script para que nos proporcione un token.

Texto

El contenido generado por IA puede ser incorrecto.

Una vez obtenido el token se procede a validar si tuviéramos el acceso al panel admin el cual no esta autorizado.



Posteriormente se realiza un fuzzing para enumerar los sitios válidos.

Texto

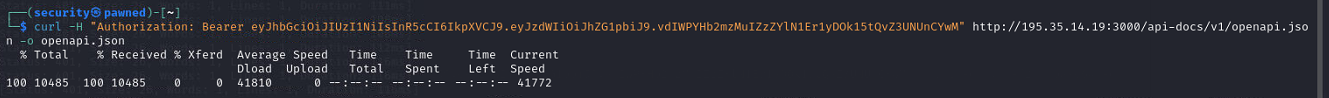
El contenido generado por IA puede ser incorrecto.

Con esta información lo que indica es lo siguiente:

El fuzzing fue exitoso: se descubrieron una **gran cantidad de endpoints válidos**, todos respondiendo con 401 Unauthorized. Esto indica que:

1. **Los endpoints existen.**
2. **El token actual no tiene autorización suficiente** para acceder a esos recursos.
3. **La respuesta uniforme (401, 26 bytes)** sugiere autenticación requerida, pero no autenticación inválida, lo cual es clave.

Una vez obtenido ese resultado extraemos una información del Docker.



Para su posterior análisis en JQ.

**¿Qué se puede hacer con este token?**

Depende del **contexto de seguridad del backend**, pero en general, podrías:

**1. Usarlo para acceder a recursos protegidos (como hiciste en /api-docs/v1/openapi.json)**

* Aunque da error 401 en muchos endpoints, **el servidor lo reconoce como válido**, solo que probablemente espera más permisos o configuración adicional.

**2. Atacar por debilidades en la firma**

* La firma final (el tercer bloque del JWT) **usa HMAC SHA-256** (HS256) y parece ser un token **auto-firmado**, lo que **abre la puerta a varios vectores de ataque si el secreto es débil o predecible**.

Ejemplos:

* + **Ataque por diccionario** para encontrar el secreto y **firmar tus propios tokens**.
  + Si el backend **acepta algoritmos inseguros** (como cambiar alg a "none"), podrías **forjar un token válido sin firma** (vulnerabilidad clásica).

# VULNERABILIDADES

Una vulnerabilidad es una debilidad, brecha o fallo en un sistema, aplicación, servicio o protocolo la cual puede ser explotada por un atacante con el fin de poner en riesgo su confidencialidad, integridad o disponibilidad.

Las vulnerabilidades pueden surgir por múltiples causas como: errores en el código, configuraciones inseguras, permisos mal definidos, protocolos obsoletos e inseguros, o incluso debilidades en el diseño del software o hardware.

Durante el proceso del ejercicio realizado de pentesting en su infraestructura, se identificaron vulnerabilidades que pueden comprometer la seguridad de sus sistemas y datos de nivel de riesgo: **Crítico**, **Alto**, **Medio** y **Bajo/informativo** las cuales se exponen en el siguiente apartado.

En total se encontraron 1035 vulnerabilidades:

Gráfico, Gráfico circular

El contenido generado por IA puede ser incorrecto.

En la siguiente tabla se muestra la lista de vulnerabilidades que se encontraron las cuales se detallan a continuación. Debido a que en su totalidad las vulnerabilidades son similares, se describen aquí solo un top 5 de cada vulnerabilidad y en un reporte anexo dedicado exclusivamente a vulnerabilidades y generado por la herramienta Tenable, se anexara el detalle del total de vulnerabilidades. “Linux\_proyect\_Jumex\_by\_agent\_tecnics.pdf”

|  |  |
| --- | --- |
| Tabla de vulnerabilidades | |
| Severidad | Vulnerabilidad |
| Critical 9.8 | Linux Distros Unpatched Vulnerability : CVE-2024-26720 |
| High 7.8 | Linux Distros Unpatched Vulnerability : CVE-2013-7445 |
| High 7.2 | Linux Distros Unpatched Vulnerability : CVE-2018-12931 |
| High 7.2 | Linux Distros Unpatched Vulnerability : CVE-2018-12930 |
| High 7.2 | Linux Distros Unpatched Vulnerability : CVE-2019-15794 |
| High 9.3 | Linux Distros Unpatched Vulnerability : CVE-2019-19814 |
| Medium 4.4 | Linux Distros Unpatched Vulnerability : CVE-2016-2568 |
| Medium 4.9 | Linux Distros Unpatched Vulnerability : CVE-2016-8660 |
| Medium 4.9 | Linux Distros Unpatched Vulnerability : CVE-2017-13693 |
| Medium 4.6 | Linux Distros Unpatched Vulnerability : CVE-2017-13165 |
| Medium 4.9 | Linux Distros Unpatched Vulnerability : CVE-2018-12928 |
| Low 2.1 | Linux Distros Unpatched Vulnerability : CVE-2015-7837 |
| Low 2.1 | Linux Distros Unpatched Vulnerability : CVE-2015-8553 |
| Low 2.1 | Linux Distros Unpatched Vulnerability : CVE-2017-0537 |
| Low 2.1 | Linux Distros Unpatched Vulnerability : CVE-2020-14304 |
| Low 2.1 | Linux Distros Unpatched Vulnerability : CVE-2020-35501 |
| Inf | PostgreSQL Client/Server Installed (Linux) |
| Inf | Docker Container File Change Detection |
| Inf | Software Enumeration (SSH) |
| Inf | VMWare Tools or Open VM Tools Installed (Linux) |
| Inf | Tukaani XZ Utils Installed (Linux / Unix) |
| Inf | Apache Log4j Installed (Linux / Unix) |
| Inf | Containerd Installed (Linux) |
| Inf | MySQL Server Installed (Linux) |

## DESCRIPCION DE VULNERABILIDADES

El objetivo de esta sección es proporcionar una descripción técnica y detallada de las vulnerabilidades identificadas, permitiendo a su equipo técnico entender cuál fue la causa del hallazgo y explotación, así como el impacto potencial de cada vulnerabilidad y ayudarlos a tomar medidas para mitigarlas.

En cada resumen de la vulnerabilidad se describen lo siguiente:

● **Severidad:** es el puntaje de criticidad que se le otorga a la vulnerabilidad encontrada, este puntaje se basa en la puntuación de CVSS para cada vulnerabilidad específica en 4 niveles con los siguientes grado de riesgos: **Crítico (9.0 - 10.0)**, **Alto (7.0 - 8.9)**, **Medio (4.0 - 6.9), Bajo (0.1 - 3.9)**

**● Vulnerabilidad:** se refiere al nombre de la vulnerabilidad que fue encontrada, de acuerdo a la vulnerabilidad en algunos casos se hace referencia a su CVE.

**● Activos:** es el número de activos en donde se encontró la vulnerabilidad que se está reportando.

● **Resumen de la vulnerabilidad:** descripción de la vulnerabilidad encontrada, incluyendo información sobre la causa raíz, el impacto potencial y las condiciones necesarias para su explotación.

**● Mapa del hallazgo/vulnerabilidad:** muestra de forma gráfica qué pasos siguió el ataque.

● **Riesgo:** describe el alcance que podría tener la vulnerabilidad en caso de que sea explotada por un atacante.

● **Nivel de acceso:** se indica el nivel de acceso usado para realizar la prueba del pentest. ○ **NO AUTENTICADO:** se indica cuando en el pentest no se uso ninguna información de credenciales de acceso más que las que se encontraron resultado del sniffing

○ **AUTENTICADO:** se indica cuando se usan credenciales proporcionadas por el cliente para ingresar en el pentest y validar el alcance de las credenciales proporcionadas.

**● Explotación:** muestra las técnicas usadas para poder realizar la explotación de la vulnerabilidad encontrada

**● Hallazgos relacionados (ataques):** se enlistan los ataques que se relacionan después de explotar la vulnerabilidad.

**● Activos:** se muestra la lista de direcciones IP en las que se encontró la vulnerabilidad.

**● Vector de ataque:** muestra el vector en base del CVSS en donde se determina evaluando la explotabilidad de una vulnerabilidad, su impacto en la confidencialidad, integridad y disponibilidad (tríada CIA) y su alcance. Factores como el vector de ataque, los privilegios requeridos y el posible impacto en todo el sistema se evalúan para generar una puntuación de severidad de 0 a 10.

● **Referencias:** Enlaces a recursos externos, como bases de datos de vulnerabilidades o sitios web de seguridad, que proporcionan información adicional sobre la vulnerabilidad.

### Linux Distros Unpatched Vulnerability : CVE-2024-26720

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **9.8** | Linux Distros Unpatched Vulnerability : CVE-2024-26720 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  El kernel:mm/writeback: Corrige posibles vulnerabilidades y malas configuraciones. | | |
| **Mapa de hallazgos** | | |
| Remote  La versión del paquete de encabezados del kernel de Linux (Linux-libc-dev-6.8.0-57.59) en Ubuntu 24.04, se publicó el 31 de marzo del 2025, se sugiere actualizar por la versión liberada 6.8.0-58.60  La versión **linux-tools-common 6.8.0-57.59** es un paquete de herramientas del kernel de Linux publicado para Ubuntu 24.04 LTS (Noble Numbat) el **31 de marzo de 2025**. Este paquete proporciona las partes independientes de la arquitectura para herramientas específicas de la versión del kernel.  Desde su lanzamiento, la versión **6.8.0-57.59** ha sido **reemplazada por versiones más recientes**, como la **6.8.0-58.60**, que incluyen correcciones de seguridad y mejoras adicionales. Es recomendable mantener el sistema actualizado para beneficiarse de estas mejoras. | | |

### Linux Distros Unpatched Vulnerability : CVE-2013-7445

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **7.8** | Linux Distros Unpatched Vulnerability : CVE-2013-7445 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - El subsistema Direct Rendering Manager (DRM) en el kernel de Linux a través de 4.x maneja mal las solicitudes de objetos Graphics Execution Manager (GEM), lo que permite a los atacantes dependientes del contexto causar una denegación de servicio (consumo de memoria) a través de una aplicación que procesa datos gráficos, como lo demuestra el código JavaScript que crea muchos elementos CANVAS para ser renderizados por Chrome o Firefox. (CVE-2013-7445) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2018-12931

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **7.2** | Linux Distros Unpatched Vulnerability : CVE-2018-12931 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - ntfs\_attr\_find en el controlador del sistema de archivos ntfs.ko en el kernel de Linux 4.15.0 permite a los atacantes desencadenar una escritura fuera de los límites basada en la pila y causar una denegación de servicio (kernel oops o kernel panic) o posiblemente tener otro impacto no especificado a través de un sistema de archivos ntfs crafted. (CVE-2018-12931) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2018-12930

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **7.2** | Linux Distros Unpatched Vulnerability : CVE-2018-12930 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  -ntfs\_end\_buffer\_async\_read en el controlador del sistema de archivos ntfs.ko en el kernel de Linux 4.15.0 permite a los atacantes desencadenar una escritura fuera de los límites basada en la pila y causar una denegación de servicio (kernel oops o kernel panic) o posiblemente tener otro impacto no especificado a través de un sistema de archivos ntfs crafted. (CVE-2018-12930) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2019-15794

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **7.2** | Linux Distros Unpatched Vulnerability : CVE-2019-15794 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - Overlayfs en el kernel de Linux y shiftfs, un parche no suministrado al kernel de Linux incluido en las series de kernel Ubuntu 5.0 y 5.3, ambos reemplazan vma->vm\_file en sus manejadores mmap. En caso de error, el valor original no se restaura, y la referencia se pone para el archivo al que apunta vm\_file. En los núcleos upstream esto no es un problema, ya que ningún llamador hace referencia a vm\_file después de que call\_mmap() devuelva un error. Sin embargo, los parches aufs cambian mmap\_region() para reemplazar fput() usando una variable local con vma\_fput(), que fput() vm\_file, lo que lleva a un desbordamiento de refcount. (CVE-2019-15794) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2019-19814

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **9.3** | Linux Distros Unpatched Vulnerability : CVE-2019-19814 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - En el kernel 5.0.21, montar una imagen de sistema de archivos f2fs crafteada puede causar acceso de escritura \_\_remove\_dirty\_segment slab-out-of-bounds porque un arreglo está limitado por el número de tipos sucios (8) pero el índice del arreglo puede exceder esto. (CVE-2019-19814) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2016-2568

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **4.4** | Linux Distros Unpatched Vulnerability: CVE-2016-2568 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - pkexec, cuando se utiliza con --user nonpriv, permite a los usuarios locales escapar a la sesión principal a través de una llamada ioctl TIOCSTI crafteada, que empuja caracteres al búfer de entrada del terminal. (CVE-2016-2568) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2016-8660

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **4.9** | Linux Distros Unpatched Vulnerability : CVE-2016-8660 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - El subsistema XFS en el kernel de Linux a través de 4.8.2 permite a los usuarios locales causar una denegación de servicio (falla fdatasync y caída del sistema) utilizando el grupo vfs syscall en el programa trinity, relacionado con un error de orden de bloqueo de página en la implementación de agujero de búsqueda/datos XFS. (CVE-2016-8660) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2017-13693

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **4.9** | Linux Distros Unpatched Vulnerability : CVE-2017-13693 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - La función acpi\_ds\_create\_operands() en drivers/acpi/acpica/dsutils.c en el kernel de Linux a través de 4.12.9 no vacía la caché de operandos y causa un volcado de pila del kernel, lo que permite a los usuarios locales obtener información sensible de la memoria del kernel y eludir el mecanismo de protección KASLR (en el kernel a través de 4.9) a través de una tabla ACPI crafteada. (CVE-2017-13693) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2017-13165

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **4.6** | Linux Distros Unpatched Vulnerability : CVE-2017-13165 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - Una vulnerabilidad de elevación de privilegios en el sistema de archivos del kernel. Producto: Android. Versiones: Kernel de Android. ID de Android A-31269937. (CVE-2017-13165) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2018-12928

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **4.9** | Linux Distros Unpatched Vulnerability : CVE-2018-12928 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - En el kernel de Linux 4.15.0, se descubrió una desviación del puntero NULL en hfs\_ext\_read\_extent en hfs.ko. Esto puede ocurrir durante un montaje de un sistema de archivos hfs crafted. (CVE-2018-12928) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2015-7837

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.1** | Linux Distros Unpatched Vulnerability : CVE-2015-7837 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - El kernel de Linux, cuando se utiliza en Red Hat Enterprise Linux 7, kernel-rt, y Enterprise MRG 2 y cuando se arranca con UEFI Secure Boot habilitado, permite a los usuarios locales eludir las restricciones securelevel/secureboot previstas aprovechando el manejo incorrecto de secure\_boot flag a través de kexec reboot. (CVE-2015-7837) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2015-8553

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.1** | Linux Distros Unpatched Vulnerability : CVE-2015-8553 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - Xen permite a los usuarios del SO invitado obtener información confidencial de ubicaciones no inicializadas en la memoria del kernel del SO anfitrión al no habilitar los bits de control de decodificación de memoria y E/S. NOTA: esta vulnerabilidad existe debido a una corrección incompleta de CVE-2015-0777. (CVE-2015-8553) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2017-0537

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | Linux Distros Unpatched Vulnerability : CVE-2017-0537 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - Una vulnerabilidad de divulgación de información en el controlador de gadgets USB del kernel podría permitir a una aplicación maliciosa local acceder a datos fuera de sus niveles de permiso. Este problema está clasificado como Moderado porque primero requiere comprometer un proceso privilegiado. Producto: Android. Versiones: Kernel-3.18. ID de Android: A-31614969. (CVE-2017-0537) | | |
| **Mapa de hallazgos** | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2020-14304

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.1** | Linux Distros Unpatched Vulnerability : CVE-2020-14304 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - Se encontró una falla de divulgación de memoria en los controladores ethernet del kernel de Linux, en la forma en que lee datos de la EEPROM del dispositivo. Este fallo permite a un usuario local leer valores no inicializados de la memoria del kernel. La mayor amenaza de esta vulnerabilidad es para la confidencialidad. (CVE-2020-14304) | | |
| **Mapa de hallazgos** | | |
|  | | |
|  | | |

### Linux Distros Unpatched Vulnerability : CVE-2020-35501

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **3.6** | Linux Distros Unpatched Vulnerability : CVE-2020-35501 | 1 |
| **Resumen de vulnerabilidad** | | |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  - Se ha encontrado un fallo en la implementación de reglas de auditoría en los núcleos de Linux, donde una llamada al sistema puede no ser registrada correctamente por el subsistema de auditoría (CVE-2020-35501). | | |
| **Mapa de hallazgos** | | |
|  | | |

### PostgreSQL Client/Server Installed (Linux)

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **0** | PostgreSQL Client/Server Installed (Linux) | 1 |
| **Resumen de vulnerabilidad** | | |
| Dos instancias detectadas de PostgreSQL fueron detectadas, se recomienda validar que el servicio es necesario para las políticas internas y de ser necesario el aplicativo, se recomienda eliminar una de las versiones. | | |
| **Mapa de hallazgos** | | |
|  | | |

### Docker Container File Change Detection

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **0** | Docker Container File Change Detection | 1 |
| **Resumen de vulnerabilidad** | | |
| Se detecta servicio de contenedores Docker. Se recomienda validar si esta dentro de las funciones del servidor, y de ser así, se recomienda aplicar las configuraciones de seguridad sugeridas por el proveedor. | | |
| **Mapa de hallazgos** | | |
|  | | |

### Software Enumeration (SSH

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **0** | Software Enumeration (SSH) | 1 |
| **Resumen de vulnerabilidad** | | |
| Se puede enumerar el software instalado via ssh por un host remoto. Se recomienda remover en software que no entra en cumplimiento con la organización. | | |
| **Mapa de hallazgos** | | |
|  | | |

### VMWare Tools or Open VM Tools Installed (Linux)

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **0** | VMWare Tools or Open VM Tools Installed (Linux) | 1 |
| **Resumen de vulnerabilidad** | | |
| Se detecta herramienta para equipos creación de equipos virtuales VMWare. Se recomienda validar si cumple con las políticas de la organización, y aplicar las mejores recomendaciones de seguridad por el fabricante para la herramienta | | |
| **Mapa de hallazgos** | | |
|  | | |

### Tukaani XZ Utils Installed (Linux / Unix)

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **0** | Tukaani XZ Utils Installed (Linux / Unix) | 1 |
| **Resumen de vulnerabilidad** | | |
| Se detecta herramienta de compresión de datos, con versión 5.6.1, para esta versión se descubrió una vulnerabilidad de puerta trasera, se recomienda aplicar los últimos parches y versiones de la aplicación. | | |
| **Mapa de hallazgos** | | |
|  | | |

### Apache Log4j Installed (Linux / Unix)

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **0** | Apache Log4j Installed (Linux / Unix) | 1 |
| **Resumen de vulnerabilidad** | | |
| Se detecta biblioteca de registros utilizada por java. Debido a que no es posible obtener la versión, se recomienda utilizar versiones 2.17.2 o superior. | | |
| **Mapa de hallazgos** | | |
|  | | |

### Containerd Installed (Linux)

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **0** | Containerd Installed (Linux) | 1 |
| **Resumen de vulnerabilidad** | | |
| Se detecta containerd instalado, es crucial mantenerlo seguro, actualizado y bien configurado, especialmente si se utiliza como runtime de contenedores, se recomienda desactivas funciones innecesarias y no utilizar usuario con altos privilegios. | | |
| **Mapa de hallazgos** | | |
|  | | |

### MySQL Server Installed (Linux)

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **0** | MySQL Server Installed (Linux) | 1 |
| **Resumen de vulnerabilidad** | | |
| Se detecta MySQL servers instalado. Se recomienda utilizar solo un gestor de base de datos y tener actualizado a ultimas versiones y configurado en base a las mejores practicas del fabricante, | | |
| **Mapa de hallazgos** | | |
|  | | |

# VULNERABILIDADES de aplicativo web

En la siguiente tabla se muestra la lista de vulnerabilidades que se encontraron en el aplicativo web <https://jmx.ambiente-de-pruebas-devcts.site> las cuales se detallan a continuación.

|  |  |
| --- | --- |
| Tabla de vulnerabilidades | |
| Severidad | Vulnerabilidad |
| Medium 5.8 | Missing HTTP Strict Transport Security Policy |
| Medium 5.0 | PHP Input Variables Exceeded |
| Low 2.6 | Cookie Without HttpOnly Flag Detected |
| Low 2.6 | Cookie Without Secure Flag Detected |
| Low 2.6 | Missing 'X-Frame-Options' Header |
| Low 2.6 | Missing 'X-Content-Type-Options' Header Policy |
| Low 2.6 | SSL/TLS Weak Cipher Suites Supported |
| Low 2.6 | Missing 'Cache-Control' Header |
| Low 2.6 | Missing Content Security Policy |
| Low 2.6 | HTTP Header Information Disclosure |

### Missing HTTP Strict Transport Security Policy

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **5.8** | Missing HTTP Strict Transport Security Policy | 1 |
| **Resumen de vulnerabilidad** | | |
| En el resultado de escaneo se detecta que la aplicación <https://jmx.ambiente-de-pruebas-devcts.site> usa el servicio https, sin embargo, no usa el encabezado HSTS  HSTS (HTTP Strict Transport Security) es un encabezado de seguridad que indica a los navegadores que solo debe comunicarse con un sitio usando HTTPS. Para prevenir ataques como:   * **Downgrade attacks** (forzar uso de HTTP en lugar de HTTPS) * **Cookie hijacking** * **SSL stripping** (ataques del tipo MITM como los realizados con herramientas como sslstrip)   Aunque tengas HTTPS habilitado, si no usas HSTS, un atacante podría interceptar tráfico antes de que se establezca la conexión segura.  Se sugiere añadir encabezados a la respuesta del servidor. Ejemplo:  Strict-Transport-Security: max-age=31536000; includeSubDomains; preload | | |
| **Mapa de hallazgos** | | |
|  | | |
|  | | |
|  | | |

* + 1. **PHP Input Variables Exceeded**

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **5.0** | PHP Input Variables Exceeded | 1 |
| **Resumen de vulnerabilidad** | | |
| Por defecto, PHP acepta un máximo de 1000 variables en una petición. Si hay más variables de entrada de las especificadas, se emite un E\_WARNING, y más variables de entrada son truncadas de la petición dependiendo de la configuración del servidor y el código de la aplicación, esto puede tener varios impactos tales como eludir la llamada a una función.  Se sugiere desactivar la visualización de todos los avisos, advertencias y errores. Configurar la aplicación para que registre dichos mensajes en un archivo. También es necesaria una revisión del código para comprobar el impacto que puede tener en la aplicación. | | |
| **Mapa de hallazgos** | | |
|  | | |
|  | | |
|  | | |

### Cookie Without HttpOnly Flag Detected

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | Cookie Without HttpOnly Flag Detected | 1 |
| **Resumen de vulnerabilidad** | | |
| El indicador HttpOnly ayuda a evitar que los scripts del cliente (como JavaScript) accedan a la cookie y la utilicen.  Esto puede ayudar a evitar que los ataques XSS se dirijan a las cookies que contienen el testigo de sesión del cliente.  Para remediar esto se sugiere determinar si algún script del lado del cliente (como JavaScript) necesita acceder a la cookie y si no es así, establecer la bandera HttpOnly. | | |
| **Mapa de hallazgos** | | |
|  | | |

* + 1. **Cookie Without Secure Flag Detected**

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | Cookie Without Secure Flag Detected | 1 |
| **Resumen de vulnerabilidad** | | |
| Cuando se establece la bandera `secure` en una cookie, el navegador evitará que se envíe a través de un canal de texto claro (HTTP) y sólo permitirá que se envíe cuando se utilice un canal cifrado (HTTPS).  En el resultado del escaneo se descubrió que el servidor había establecido una cookie sin la bandera de seguridad. Aunque la configuración inicial de esta cookie se realizó a través de una conexión HTTPS, cualquier enlace HTTP al mismo servidor hará que la cookie se envíe en texto claro.  Se sugiere que si la cookie contiene información sensible, entonces el servidor debe asegurarse de que la cookie tiene la bandera `secure` activada. | | |
| **Mapa de hallazgos** | | |
|  | | |

### Missing 'X-Frame-Options' Header

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | Missing 'X-Frame-Options' Header | 1 |
| **Resumen de vulnerabilidad** | | |
| Se detecta que no se utiliza X-frame-Options, este encabezado evita que un sitio web sea incrustado en un <iframe> de otro sitio, lo cual protege contra ataques "clickjacking"  El clickjaking es cuando un atacante puede incrustar tu sitio dentro de un iframe y engañar a los usuarios para que hagan clic en botones que en realidad están en tu aplicación (por ejemplo: “Eliminar cuenta”, “Hacer transferencia”, etc.).  Se recomienda agregar al encabezado:  Header always set X-Frame-Options "DENY" | | |
| **Mapa de hallazgos** | | |
|  | | |

### Missing 'X-Content-Type-Options' Header Policy

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | Missing ‘X-Content-Type-Options’ Header Policy | 1 |
| **Resumen de vulnerabilidad** | | |
| Se detecta que el servidor no devuelve un encabezado correcto 'X-Content-Type-Options', lo que significa que el sitio web podría correr el riesgo de un ataque de secuencia de comandos entre sitios (XSS)  El utilizar X-Content-Type-Options, protege contra:   * Ejecutar archivos maliciosos como scripts. * Ataques de tipo MIME-type confusión, donde un archivo puede ejecutarse como JavaScript.   Se sugiere agregar cadenas de encabezados  Header set X-Content-Type-Options "nosniff" - Solución en apache, | | |
| **Mapa de hallazgos** | | |
|  | | |

### SSL/TLS Weak Cipher Suites Supported

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | SSL/TLS Weak Cipher Suites Supported | 1 |
| **Resumen de vulnerabilidad** | | |
| El host remoto admite el uso de cifrados SSL/TLS que ofrecen un cifrado débil (incluidos los cifrados RC4 y 3DES).  Se sugiere reconfigurar la aplicación afectada, si es posible, para evitar el uso de cifrados débiles. | | |
| **Mapa de hallazgos** | | |
|  | | |
| Aunque la configuracion es buena del aplicativo web, se detectan cifrados debiles, se requiere deshabilitar. | | |

### Missing 'Cache-Control' Header

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | Missing ‘Cache-Control’ Header | 1 |
| **Resumen de vulnerabilidad** | | |
| El servidor no devolvió o devolvió una cabecera “Cache-Control” inválida, lo que significa que la página que contiene información sensible (contraseña, tarjeta de crédito, datos personales, número de la seguridad social, etc.) podría almacenarse en el disco del lado del cliente y quedar expuesta a personas no autorizadas.  La cabecera HTTP “Cache-Control” se utiliza para especificar directivas para los mecanismos de almacenamiento en caché.  Se sugiere configurar su servidor web para que incluya una cabecera “Cache-Control” con las directivas apropiadas. Si la página contiene información sensible, el valor de «Cache-Control» debe ser «no-store» y el valor de la cabecera “Pragma” debe ser «no-cache». | | |
| **Mapa de hallazgos** | | |
|  | | |

### Missing Content Security Policy

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | Missing Content Security Policy | 1 |
| **Resumen de vulnerabilidad** | | |
| La Política de Seguridad de Contenidos (CSP) es un estándar de seguridad web que ayuda a mitigar ataques como el cross-site scripting (XSS), clickjacking o problemas de contenido mixto. CSP proporciona mecanismos a los sitios web para restringir el contenido que los navegadores podrán cargar.  No se ha detectado ningún encabezado CSP en este host.  Se sugiere configurar la Política de Seguridad de Contenidos en su sitio web añadiendo la cabecera HTTP “Content-Security-Policy” o la metaetiqueta http-equiv=“Content-Security-Policy”. | | |
| **Mapa de hallazgos** | | |
|  | | |

### HTTP Header Information Disclosure

|  |  |  |
| --- | --- | --- |
| **Severidad** | **Vulnerabilidad** | **Activo** |
| **2.6** | HTTP Header Information Disclosure | 1 |
| **Resumen de vulnerabilidad** | | |
| Las cabeceras HTTP enviadas por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor y las tecnologías utilizadas por el servidor web.  Se sugiere modificar las cabeceras HTTP del servidor web para que no revelen información detallada sobre el servidor web subyacente. | | |
| **Mapa de hallazgos** | | |
|  | | |

# HALLAZGOS APLICATIVO WEB

En la realización del pentest, una de las partes importantes es reconocer el objetivo al cual se le realizará dicha acción.

En este caso, se trabajó sobre el activo correspondiente a la dirección IP **195.35.14.19**, que aloja el sitio https://jmx.ambiente-de-pruebas-devcts.site. Durante el reconocimiento activo con herramientas como **Burp Suite**, fue posible identificar mecanismos de autenticación válidos y estructuras html, sin embargo, al intentar avanzar en la fase de evaluación de seguridad a nivel de sesión o inyección, se detectó que el sistema está protegido por un esquema de **autenticación multifactor (MFA)**.

Texto

El contenido generado por IA puede ser incorrecto.

El activo evaluado fue la IP **195.35.14.19**, correspondiente al entorno de pruebas del sitio https://jmx.ambiente-de-pruebas-devcts.site. A lo largo del proceso, se utilizaron diversas herramientas de evaluación como:

* **Burp Suite Community**, para interceptar solicitudes HTTP/S y analizar estructuras de autenticación, parámetros y cabeceras.
* **WhatWeb** y **Wappalyzer**, para identificar tecnologías utilizadas en el backend y frontend.
* **Nmap** con scripts NSE (Nmap Scripting Engine), para escanear puertos y servicios activos.

A través de Burp Suite se logró interceptar y analizar la solicitud de inicio de sesión, así como estructuras típicas de APIs REST. Sin embargo, al intentar simular un inicio de sesión válido o enviar credenciales a través del endpoint, el sistema respondió con un mensaje explícito indicando la necesidad de completar un segundo factor de autenticación (MFA), como se muestra en la imagen correspondiente del presente documento.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

El mecanismo MFA implementado bloqueó de forma efectiva el avance de la validación posterior mediante herramientas automatizadas y manuales. Esta barrera impidió el acceso a secciones autenticadas de la plataforma, donde comúnmente se encuentran controles susceptibles a vulnerabilidades como inyecciones SQL, secuestro de sesión, control de accesos rotos, entre otros.

Esta situación demuestra que la plataforma cuenta con un esquema de **autenticación robusto**, alineado con buenas prácticas de seguridad como las promovidas por el OWASP (A07: Identification and Authentication Failures), lo cual **aumenta significativamente el nivel de protección frente a ataques externos**.

Por lo tanto, se concluye que **el uso efectivo de MFA limita la superficie de ataque y protege las rutas críticas de autenticación**, razón por la cual **no fue posible continuar con pruebas avanzadas.**

# Anexo

Para detalle de todas las vulnerabilidades encontradas, referirse al anexo **“Linux\_proyect\_Jumex\_by\_agent\_tecnics.pdf”**

Por otra parte, se realiza escaneo de cumplimiento basados en el marco de referencias **CIS\_Ubuntu\_Linux\_24.04\_LTS\_v1.0.0\_L1\_Server.audit from CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0,** lo recomendable es mitigar las 84 misconfiguration detectadas según lo recomendado por el reporte anexo

**“Linux\_proyect\_Jumex\_Policy\_Compliance\_qbthqx.pdf”**

También se ejecutan escaneos de vulnerabilidades para aplicativos Web utilizando el TOP 10 OWASP.

**“WAS\_Jumex\_jmx.ambiente-de-pruebas-devcts.site.pdf”,** escaneo sin autenticación

**“WAS\_jumex-web\_app.pdf”** escaneo con autenticación.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.