Informe de Pruebas de Seguridad al Sistema Web de Ventas CorpERP

Iteración 01 - Evaluación del frontend e infraestructura de despliegue

Versión 1.0

Elaborado por:	Revisado por:	Aprobado por:
EDISON JUNIOR PAUCAR HUANCAR	KUKING ÑAHUI PANLLO	PENDIENTE
Fecha: 12/08/2026	Fecha: 12/08/2026	Fecha: -

HISTORIAL DE REVISIONES

Versión	Autor	Descripción	Fecha	Revisado por	Fecha de Revisión
Versión 1.0	Edison Junior Paucar Huancar	Informe de Pruebas de Seguridad al Sistema Web de Ventas CorpERP - Iteración 01	12/08/2026	Kuking Ñahui Panllo	12/08/2026

ÍNDICE

INFORME DE PRUEBAS DE SEGURIDAD

1. INTRODUCCIÓN

La presente evaluación corresponde a la primera iteración de pruebas de seguridad del Sistema Web de Ventas CorpERP. El trabajo se orientó a identificar debilidades visibles desde el frontend, revisar la configuración HTTP del aplicativo y levantar información técnica verificable del entorno donde se encuentran desplegados los componentes del sistema.

Las pruebas se ejecutaron en un entorno autorizado de desarrollo y pruebas. Se utilizó OWASP ZAP para la exploración manual, análisis pasivo y escaneo activo controlado del frontend; Developer Tools del navegador para inspección complementaria; Portainer y acceso SSH mediante Tabby para reconocer la infraestructura Docker, redes, puertos y características del servidor.

Esta iteración no constituye una evaluación exhaustiva de la seguridad de todas las APIs. Las pruebas manuales de autenticación, sesiones, autorización y lógica de negocio de cada microservicio quedan definidas para una segunda iteración mediante Burp Suite Community.

Proyecto	Sistema Web de Ventas CorpERP
Tipo de proyecto	Sistema web empresarial con arquitectura de microservicios
Aplicación y acceso	Frontend disponible; acceso autorizado a Portainer y servidor Linux vía SSH
Documentación API/Swagger	No incluida como fuente de prueba en esta iteración; se conoce su uso durante el desarrollo
Equipo de pruebas	Edison Junior Paucar Huancar

1.1 Objetivo de las Pruebas de Seguridad

- Identificar de forma temprana debilidades de seguridad presentes en el frontend y en su configuración HTTP.
- Reconocer la arquitectura real de despliegue del sistema y establecer los activos que deberán ser evaluados en pruebas posteriores.
- Clasificar los hallazgos según su nivel de riesgo y plantear recomendaciones de corrección verificables.
- Definir el alcance de una segunda iteración enfocada en autenticación, sesiones, autorización y APIs de los microservicios.

1.2 Alcance

En esta iteración se revisó el frontend CorpERP accesible en el entorno interno a través de http://192.171.100.56:3050, tomando el módulo de Login como punto de entrada. El análisis alcanzó los recursos JavaScript y CSS cargados por la aplicación, cabeceras HTTP, servidor web y dependencias observadas durante la navegación.

Asimismo, se realizó reconocimiento de infraestructura sobre el servidor 192.171.100.56, la plataforma Docker, Portainer, redes de contenedores y reglas básicas de firewalld. Los seis microservicios fueron identificados técnicamente, pero sus endpoints no fueron sometidos aún a pruebas manuales de autorización o manipulación de parámetros.

No se realizaron pruebas destructivas, fuerza bruta, modificación de datos productivos ni explotación de servicios de infraestructura. Las alertas generadas sobre dominios de terceros (por ejemplo unpkg.com y fonts.gstatic.com) fueron excluidas del conteo de hallazgos del sistema CorpERP.

2. ENTORNO DE PRUEBAS

2.1 Servidor de aplicaciones

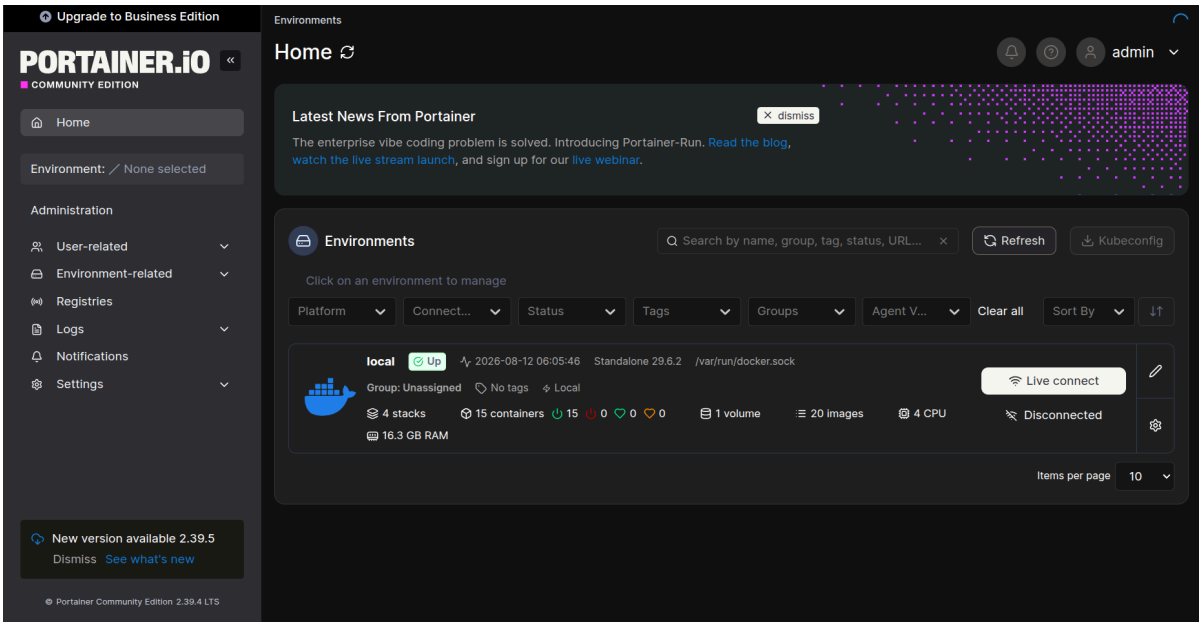
Configuración del Servidor de Aplicaciones	
Fabricante / Modelo	Dell Inc. / PowerEdge R250
Sistema operativo	Rocky Linux 10.2 (Red Quartz)
Kernel	Linux 6.12.0-124.8.1.el10_1.x86_64
Arquitectura	x86-64
Procesador	Intel(R) Xeon(R) E-2324G CPU @ 3.10 GHz
CPU	4 núcleos / 1 socket / 1 hilo por núcleo
Memoria	15 GiB de RAM; 7.8 GiB de swap
Almacenamiento	Disco físico de 3.6 TB; LVM con /, swap y /home
Interfaz principal	eno8303 - 192.171.100.56/22

2.2 Plataforma Docker y Portainer

Plataforma de Contenedores	
Motor	Docker Engine - Community 29.6.2
API Docker	1.55

containerd / runc	containerd v2.2.6 / runc 1.3.6
Driver de almacenamiento	overlayfs
Contenedores	15 totales; 15 en ejecución; 0 detenidos
Imágenes	20 imágenes
Administración	Portainer Community Edition 2.39.4 LTS
Stacks observados	bd-noveno-dev, microservicios-dev, portal-noveno-dev y tienda

Evidencia de reconocimiento de infraestructura mediante Portainer.



2.3 Arquitectura de microservicios

La arquitectura observada separa el frontend de la red Docker donde se encuentran los microservicios y sus bases de datos. Los servicios del backend se publican mediante puertos del host, permitiendo que el frontend y otros clientes autorizados consuman sus APIs.

Componente	Contenedor	Imagen	Puerto publicado	Red Docker	Persistencia asociada
Frontend	frontend_app	tienda-mi-frontend	3050 -> 80	tienda_default	Portal CorpERP
Ventas	ms-ventas	serversideup/php:8.3-cli	9020 -> 8000	noveno-b	MariaDB 11.4 / 9002 -> 3306
Clientes	ms-clientes	ms-clientes:latest	9040 -> 3000	noveno-b	PostgreSQL 18.2 / 9004 -> 5432
Almacén	ms-almacen	ms-almacen:latest	9030 -> 3000	noveno-b	MariaDB 11.4 / 9003 -> 3306
Caja	ms-caja	ms-caja:latest	9051 -> 8000	noveno-b	MariaDB 11.4 / 9007 -> 3306
Facturación	ms-facturacion	serversideup/php:8.4-cli	9010 -> 8000	noveno-b	MariaDB 11.4 / 9001 -> 3306
Administración	ms-administracion	ms-administracion:3.2	9026 -> 8000	noveno-b	MariaDB 11.4 / 9006 -> 3306

2.4 Red y controles de acceso

Configuración de Red Relevante para las Pruebas de Seguridad	
Red principal	eno8303 - 192.171.100.56/22 - zona firewalld public
Red Docker noveno-b	192.169.30.0/24 - microservicios, bases de datos y portal web
Red Docker tienda_default	172.18.0.0/16 - frontend_app en 172.18.0.2
docker0	172.17.0.0/16
WireGuard	wg0 - 10.20.0.1/24
VPN/overlay observada	zteywyccii - 10.89.82.240/24 - zona trusted (target ACCEPT)
SSH	22/tcp en escucha
firewalld	Activo; zona public sobre eno8303 y zona trusted sobre zteywyccii
Puertos permitidos en public	9001/tcp, 9020/tcp, 9030/tcp, 9051/tcp, 51820/udp y 9993/udp, además de servicios cockpit, dhcpv6-client y ssh

Implicancia para seguridad: el reconocimiento confirma que el frontend, los microservicios y las bases de datos tienen superficies de exposición diferentes. La siguiente iteración deberá validar desde qué redes son alcanzables los puertos publicados, si cada API exige autenticación y si los controles de autorización se aplican en el backend y no únicamente en la interfaz Angular.

Observación pendiente de validación: la base de datos de Facturación se publica como 0.0.0.0:9001 -> 3306/tcp y el puerto 9001/tcp está permitido en la zona public de firewalld. Este punto se registra para verificación de alcance desde una estación cliente; no se contabiliza todavía como vulnerabilidad confirmada.

3. HERRAMIENTAS DE PRUEBAS

3.1 Developer Tools del navegador

Utilizado para la inspección manual de solicitudes HTTP, recursos frontend, cabeceras de respuesta y dependencias externas. Permitió confirmar el acceso al entorno interno por HTTP, observar los recursos cargados y verificar información del servidor expuesta en las respuestas.

3.2 OWASP ZAP 2.17.0

Herramienta principal de evaluación del frontend. Se empleó como proxy para exploración manual, análisis pasivo y posteriormente Automated Scan con Spider, Client Spider y Active Scan controlado. Los hallazgos reportados en la sección 4 fueron depurados para excluir alertas correspondientes a dominios de terceros.

3.3 Portainer Community Edition

Utilizado para reconocer la plataforma Docker, stacks, contenedores, imágenes, redes y puertos publicados. Su información fue contrastada con comandos ejecutados directamente en el servidor.

3.4 Tabby / SSH

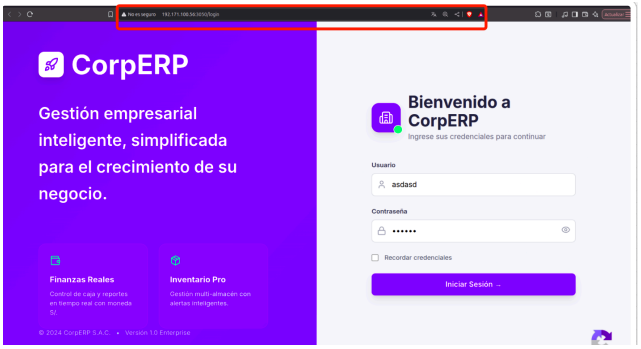
Cliente de terminal utilizado para acceder de forma autorizada al servidor Linux y obtener información del sistema operativo, hardware, Docker, interfaces de red, puertos en escucha y configuración de firewalld.

3.5 Burp Suite Community - Iteración 02

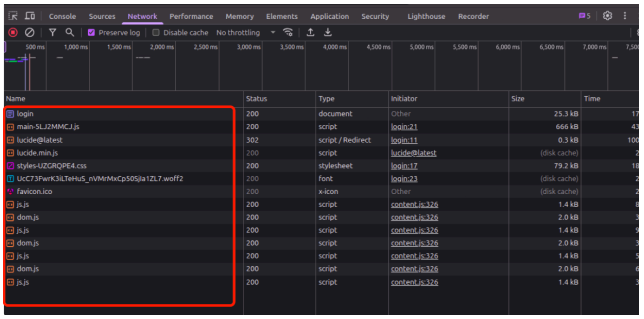
Herramienta planificada para la siguiente versión del informe. Se utilizará para capturar y reproducir peticiones HTTP hacia los microservicios, evaluar autenticación, tokens o cookies de sesión, autorización por roles, exposición de datos, CORS y validación de parámetros. No se presentan resultados de Burp Suite en la Iteración 01 porque la ejecución aún no se realizó.

EVIDENCIAS COMPLEMENTARIAS DE INSPECCIÓN MANUAL

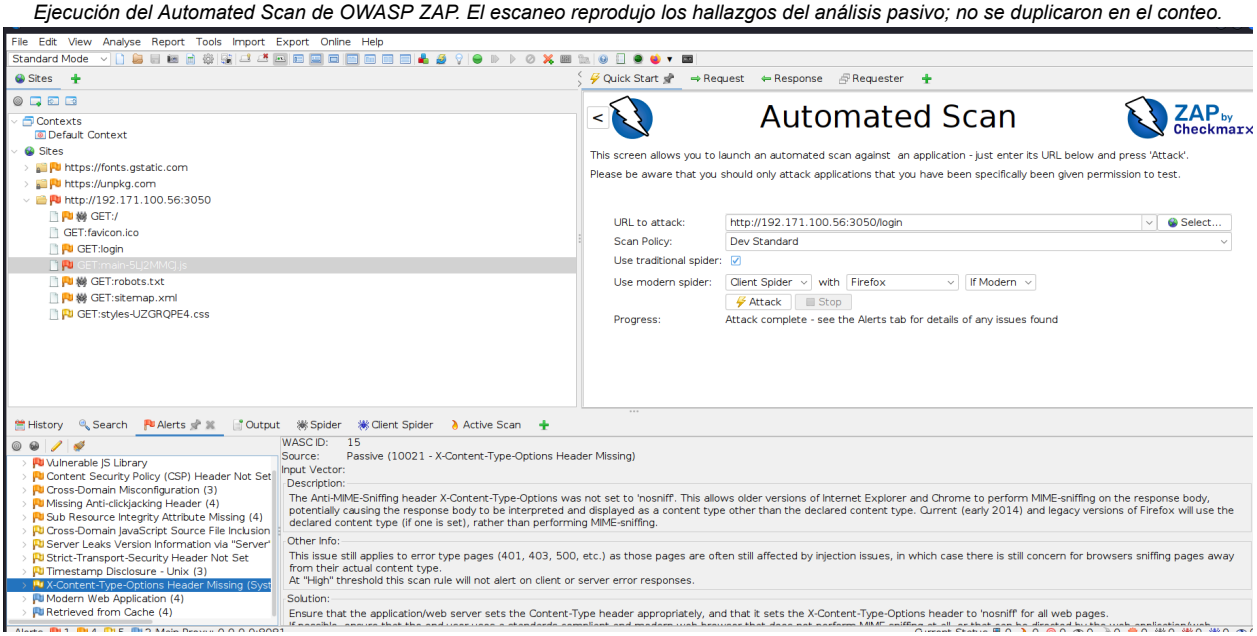
Inspección del acceso HTTP al frontend interno.



Recursos frontend observados en Network.



Ejecución del Automated Scan de OWASP ZAP. El escaneo reprodujo los hallazgos del análisis pasivo; no se duplicaron en el conteo.



4. REPORTE DE ESCANEO

REPORTE DE HALLAZGOS

ANALIZADO POR:	Edison Junior Paucar Huancar
REVISADO POR:	Kuking Ñahui Panllo
FECHA DE REVISIÓN:	12/08/2026
NOMBRE DEL SISTEMA:	Sistema Web de Ventas CorpERP
NÚMERO DE ITERACIÓN:	01
ENTORNO EVALUADO:	Frontend interno 192.171.100.56:3050 e infraestructura Docker del servidor 192.171.100.56
MÓDULOS REVISADOS:	Frontend/Login y recursos estáticos; reconocimiento de seis microservicios. Pruebas API detalladas: pendientes.

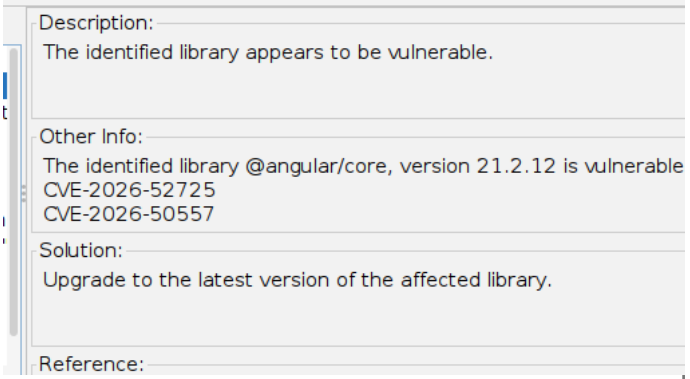
4.1 RESUMEN EJECUTIVO

Nivel de Riesgo	Número de Alertas
MUY ALTO	00
ALTO	01
MODERADO	02
BAJO	02
TOTAL	05

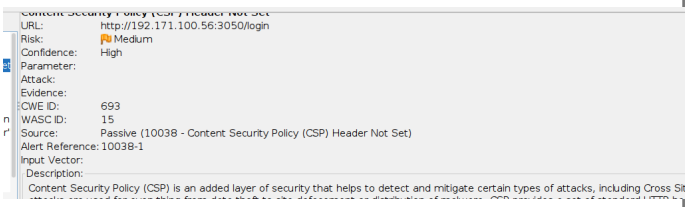
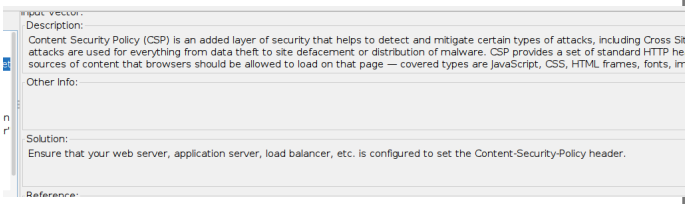
Criterio de valoración: se conserva el enfoque del informe de referencia mediante R = Po x Σ(C,I,D). Para esta iteración se emplearon los rangos: MUY ALTO >= 30, ALTO 24-29, MODERADO 13-23 y BAJO <= 12. La severidad técnica de ZAP y su nivel de confianza se conservaron como elementos de apoyo a la clasificación.

Criterio de depuración: no se contabilizaron como hallazgos de CorpERP las alertas CORS generadas por ZAP sobre fonts.gstatic.com y unpkg.com, debido a que corresponden a recursos de terceros. El Automated Scan repitió principalmente las alertas ya encontradas y por ello no se registraron duplicados.

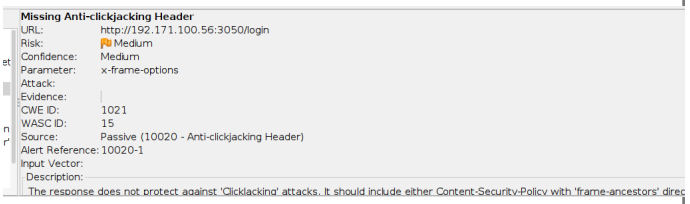
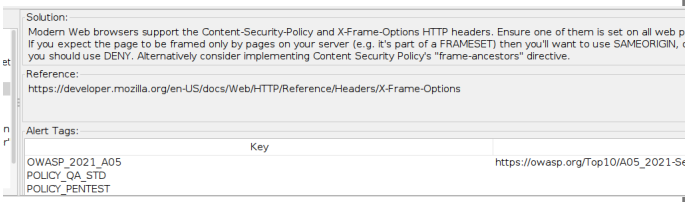
HALLAZGO 01

HALLAZGO	01
ACTIVO O RECURSO COMPROMETIDO	Frontend del Sistema Web CorpERP - recurso JavaScript main-5LJ2MMCJ.js.
PILARES DE S.I. AFECTADOS	Confidencialidad: 2 | Integridad: 2 | Disponibilidad: 1
CATEGORÍA	**Componentes vulnerables y desactualizados**
VULNERABILIDAD ENCONTRADA	**Uso de componente JavaScript asociado a vulnerabilidades conocidas**
COMPONENTE	@angular/core, versión 21.2.12
AMENAZA	El análisis pasivo de OWASP ZAP, mediante la regla Vulnerable JS Library (Retire.js), identificó la versión 21.2.12 de @angular/core y la asoció con vulnerabilidades conocidas. La permanencia de componentes afectados por vulnerabilidades reportadas aumenta la posibilidad de que un atacante aproveche debilidades conocidas cuando se presenten las condiciones necesarias.
RIESGO	Un componente frontend vulnerable puede ampliar la superficie de ataque y afectar la seguridad del navegador o de las funciones que dependan de dicho componente. El impacto efectivo depende de cada vulnerabilidad y de la forma en que Angular sea utilizado por la aplicación; la prueba realizada identifica la condición de exposición, no demuestra explotación.
NIVEL DE RIESGO	**25 (ALTO) Po:5 ; I: Σ(C,I,D) 5 | ZAP: High | Confianza: Medium**
RECOMENDACIONES DE LA SOLUCIÓN	Revisar las vulnerabilidades asociadas por ZAP a la versión identificada y actualizar @angular/core a una versión corregida y compatible con el proyecto. Ejecutar pruebas funcionales y de seguridad posteriores a la actualización para verificar que no se introduzcan incompatibilidades.
EVIDENCIAS (Imagen, fragmento de código, alertas, entre otros que sustente la vulnerabilidad)	*Alerta principal: biblioteca JavaScript vulnerable.*  *Detalle de @angular/core 21.2.12 y vulnerabilidades asociadas por ZAP.* 
Referencia	OWASP Top 10 A06:2021 - Componentes vulnerables y desactualizados. CVE asociados por ZAP/Retire.js: CVE-2026-52725, CVE-2026-50557 y CVE-2026-54267.
CWE Id	CWE-1395
WASC Id	-
Plugin Id	10003
ESTADO	**PENDIENTE DE RESOLVER**

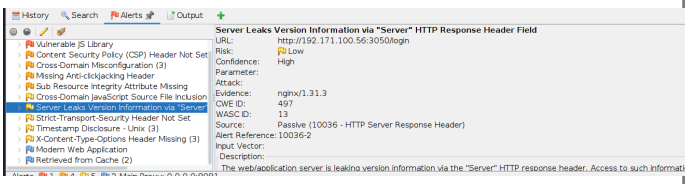
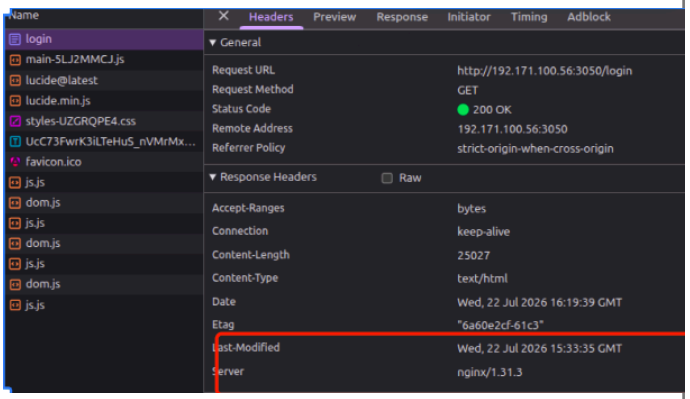
HALLAZGO 02

HALLAZGO	02
ACTIVO O RECURSO COMPROMETIDO	Módulo de autenticación (Login) - http://192.171.100.56:3050/login
PILARES DE S.I. AFECTADOS	Confidencialidad: 2 | Integridad: 2 | Disponibilidad: 1
CATEGORÍA	**Configuración de seguridad incorrecta**
VULNERABILIDAD ENCONTRADA	**Ausencia de la cabecera Content-Security-Policy (CSP)**
COMPONENTE	Cabeceras de seguridad HTTP del frontend
AMENAZA	La respuesta del módulo de autenticación no incorpora la cabecera Content-Security-Policy. La ausencia de esta política elimina una capa adicional de control del navegador destinada a restringir las fuentes autorizadas para scripts, estilos, imágenes y otros recursos.
RIESGO	Si existiera una vulnerabilidad de inyección de contenido o Cross-Site Scripting (XSS), la falta de una CSP adecuada podría incrementar el impacto al no existir restricciones adicionales del navegador sobre los recursos y scripts que pueden ejecutarse.
NIVEL DE RIESGO	**20 (MODERADO) Po:4 ; I: Σ(C,I,D) 5 | ZAP: Medium | Confianza: High**
RECOMENDACIONES DE LA SOLUCIÓN	Implementar Content-Security-Policy en el servidor que publica el frontend y definir únicamente los orígenes necesarios para scripts, estilos, imágenes, fuentes y conexiones. Validar la política en un entorno de pruebas antes de desplegarla para evitar afectar funciones legítimas.
EVIDENCIAS (Imagen, fragmento de código, alertas, entre otros que sustente la vulnerabilidad)	*Alerta CSP Header Not Set sobre el módulo Login.*  *Descripción y recomendación de OWASP ZAP.* 
Referencia	OWASP Top 10 A05:2021 - Configuración de seguridad incorrecta
CWE Id	CWE-693
WASC Id	15
Plugin Id	10038
ESTADO	**PENDIENTE DE RESOLVER**

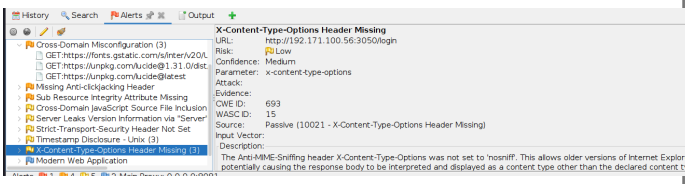
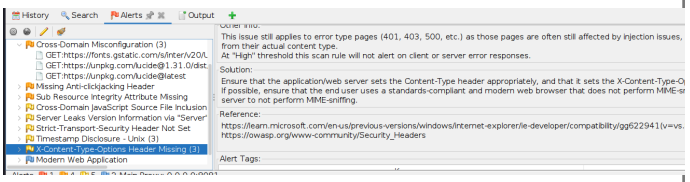
HALLAZGO 03

HALLAZGO	03
ACTIVO O RECURSO COMPROMETIDO	Módulo de autenticación (Login) - http://192.171.100.56:3050/login
PILARES DE S.I. AFECTADOS	Confidencialidad: 1 | Integridad: 2 | Disponibilidad: 1
CATEGORÍA	**Configuración de seguridad incorrecta**
VULNERABILIDAD ENCONTRADA	**Ausencia de mecanismos de protección contra Clickjacking**
COMPONENTE	Cabecera X-Frame-Options / directiva CSP frame-ancestors
AMENAZA	OWASP ZAP identificó que la respuesta del módulo de autenticación no incorpora X-Frame-Options ni una política equivalente mediante Content-Security-Policy que restrinja la inclusión de la página en marcos externos. Esto puede permitir que la interfaz sea incrustada en una página controlada por un tercero.
RIESGO	Un atacante podría intentar superponer la interfaz legítima dentro de un iframe y engañar al usuario para que ejecute acciones diferentes a las que percibe. Este vector de Clickjacking afecta principalmente la integridad de la interacción del usuario.
NIVEL DE RIESGO	**16 (MODERADO) Po:4 ; I: Σ(C,I,D) 4 | ZAP: Medium | Confianza: Medium**
RECOMENDACIONES DE LA SOLUCIÓN	Implementar X-Frame-Options con una política adecuada como DENY o SAMEORIGIN según las necesidades de negocio. Como mecanismo moderno, definir además frame-ancestors dentro de Content-Security-Policy y limitar los orígenes autorizados.
EVIDENCIAS (Imagen, fragmento de código, alertas, entre otros que sustente la vulnerabilidad)	*Alerta Missing Anti-clickjacking Header.*  Missing Anti-clickjacking Header URL: http://192.171.100.56:3050/login Risk: Medium Confidence: Medium Parameter: x-frame-options Attack: Evidence: CWE ID: 1021 WASC ID: 15 Source: Passive (10020 - Anti-clickjacking Header) Alert Reference: 10020-1 Input Vector: Description: The response does not protect against 'Clicklacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' direc *Recomendación de X-Frame-Options o CSP frame-ancestors.*  Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web p If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive. Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options Alert Tags: Key OWASP_2021_A05 https://owasp.org/Top10/A05_2021-Se POLICY_QA_STD POLICY_PENTEST
Referencia	OWASP Top 10 A05:2021 - Configuración de seguridad incorrecta
CWE Id	CWE-1021
WASC Id	15
Plugin Id	10020
ESTADO	**PENDIENTE DE RESOLVER**

HALLAZGO 04

HALLAZGO	04
ACTIVO O RECURSO COMPROMETIDO	Módulo de autenticación y servidor web del frontend - http://192.171.100.56:3050/login
PILARES DE S.I. AFECTADOS	Confidencialidad: 2 | Integridad: 1 | Disponibilidad: 1
CATEGORÍA	**Configuración de seguridad incorrecta / divulgación de información**
VULNERABILIDAD ENCONTRADA	**Divulgación de versión del servidor mediante la cabecera HTTP Server**
COMPONENTE	Servidor web Nginx
AMENAZA	La respuesta HTTP revela el producto y la versión exacta del servidor mediante el valor nginx/1.31.3. Esta información puede ser utilizada durante actividades de reconocimiento para perfilar la infraestructura y buscar vulnerabilidades conocidas relacionadas con la tecnología observada.
RIESGO	La divulgación de versión no demuestra por sí sola una vulnerabilidad explotable, pero proporciona información innecesaria que puede facilitar ataques dirigidos y reducir el esfuerzo de reconocimiento de un tercero.
NIVEL DE RIESGO	**12 (BAJO) Po:3 ; I: Σ(C,I,D) 4 | ZAP: Low | Confianza: High**
RECOMENDACIONES DE LA SOLUCIÓN	Configurar el servidor web o proxy para evitar revelar información innecesaria de producto y versión mediante la cabecera Server. Complementar esta medida con una política de actualización y parches del servidor web.
EVIDENCIAS (Imagen, fragmento de código, alertas, entre otros que sustente la vulnerabilidad)	*ZAP identifica la evidencia nginx/1.31.3 en la cabecera Server.*  *Developer Tools confirma el encabezado Server: nginx/1.31.3.* 
Referencia	OWASP Top 10 A05:2021 - Configuración de seguridad incorrecta
CWE Id	CWE-497
WASC Id	13
Plugin Id	10036
ESTADO	**PENDIENTE DE RESOLVER**

HALLAZGO 05

HALLAZGO	05
ACTIVO O RECURSO COMPROMETIDO	Módulo de autenticación (Login) - http://192.171.100.56:3050/login
PILARES DE S.I. AFECTADOS	Confidencialidad: 1 | Integridad: 1 | Disponibilidad: 1
CATEGORÍA	**Configuración de seguridad incorrecta**
VULNERABILIDAD ENCONTRADA	**Ausencia de la cabecera HTTP X-Content-Type-Options**
COMPONENTE	Cabeceras HTTP de seguridad del frontend
AMENAZA	OWASP ZAP identificó que la respuesta HTTP del módulo de autenticación no incluye X-Content-Type-Options con el valor nosniff. La ausencia de esta configuración permite que determinados navegadores intenten interpretar el contenido como un tipo MIME distinto al declarado.
RIESGO	En ciertos escenarios, la interpretación incorrecta del tipo de contenido puede favorecer la representación o ejecución de contenido de una forma no prevista. El riesgo es limitado en navegadores modernos, pero la ausencia de esta cabecera reduce el endurecimiento HTTP del sistema.
NIVEL DE RIESGO	**9 (BAJO) Po:3 ; I: Σ(C,I,D) 3 | ZAP: Low | Confianza: Medium**
RECOMENDACIONES DE LA SOLUCIÓN	Configurar el servidor web para incluir X-Content-Type-Options: nosniff en las respuestas del sistema y verificar que cada recurso sea servido con un encabezado Content-Type correcto.
EVIDENCIAS (Imagen, fragmento de código, alertas, entre otros que sustente la vulnerabilidad)	*Alerta X-Content-Type-Options Header Missing.*  *Recomendación de configurar X-Content-Type-Options: nosniff.* 
Referencia	OWASP Top 10 A05:2021 - Configuración de seguridad incorrecta
CWE Id	CWE-693
WASC Id	15
Plugin Id	10021
ESTADO	**PENDIENTE DE RESOLVER**

4.2 Pruebas planificadas sobre microservicios - Iteración 02

La arquitectura ya identificada permite definir una segunda iteración enfocada en la comunicación frontend-backend. Burp Suite Community se utilizará como proxy de interceptación y herramienta de repetición de solicitudes. El objetivo será verificar controles de seguridad en las APIs sin afectar información real.

Ámbito	Prueba prevista	Evidencia esperada
Autenticación / Administración	Identificar endpoint de login, tipo de token o cookie, mensajes de error y comportamiento al retirar credenciales.	HTTP History + Repeater; códigos 200/401/403 y respuesta sanitizada.
Ventas	Validar autorización, parámetros de cantidad/precio y acceso según rol usando registros de prueba.	Petición original vs. petición modificada de forma controlada.
Clientes	Validar acceso a datos personales, filtrado de campos y control de acceso por usuario/rol.	Respuesta con y sin autorización; revisión de exposición de campos.
Almacén	Validar operaciones de stock, categorías y movimientos; rechazo de valores no válidos.	Solicitudes API y respuestas de validación.
Caja	Validar apertura/cierre y operaciones sensibles según rol.	Respuestas de autorización y reglas de negocio.
Facturación	Validar integridad de totales, estado y permisos de emisión/consulta.	Comparación de solicitud del frontend con validación del backend.
Todos los microservicios	Revisar CORS real de las APIs, cabeceras, errores, autenticación y métodos permitidos.	Capturas Burp de Request/Response y matriz por microservicio.

5. CONCLUSIONES

- Se identificó 01 hallazgo de nivel ALTO, 02 hallazgos de nivel MODERADO y 02 hallazgos de nivel BAJO en el frontend evaluado mediante OWASP ZAP.
- La evaluación actual se concentró en el frontend, sus recursos y configuración HTTP; por tanto, los resultados no representan todavía una evaluación integral de los seis microservicios.
- El reconocimiento por Portainer y SSH permitió establecer con datos verificables la arquitectura del sistema: un frontend separado, seis microservicios, seis bases de datos, redes Docker diferenciadas y publicación de servicios mediante puertos del host.
- Las alertas CORS detectadas sobre recursos de terceros fueron excluidas para evitar atribuir falsos positivos al sistema CorpERP.
- La siguiente iteración deberá priorizar las APIs y controles de autorización mediante Burp Suite, utilizando la arquitectura levantada en este informe como guía de cobertura.

6. RECOMENDACIONES

- Subsanar los cinco hallazgos descritos en el punto 4 y repetir el escaneo de OWASP ZAP para verificar la corrección.
- Actualizar el componente Angular identificado por ZAP, priorizando una versión corregida y compatible con el frontend.
- Implementar una política de cabeceras de seguridad coherente: Content-Security-Policy, protección anti-clickjacking y X-Content-Type-Options, además de reducir la divulgación de versión del servidor.
- Mantener HTTPS como requisito para ambientes accesibles fuera del entorno interno de desarrollo y revisar la exposición de los puertos publicados por Docker respecto de las reglas de firewalld.
- En la Iteración 02, ejecutar pruebas con Burp Suite sobre autenticación, sesiones, autorización por roles, manejo de errores, CORS y lógica de negocio de cada microservicio.
- Validar específicamente la necesidad de exponer los puertos de bases de datos en el host. Cuando no exista una necesidad operativa, limitar el acceso a redes internas o a orígenes explícitamente autorizados.