KeepCoding Bootcamp Ciberseguridad | Edición IX

Informe Pentesting Collecto.es

CONFIDENCIAL

Auditores:

Oscar Uriel Tobar Rios
David Groning Hernández
Andres Jesus Ricaurte Valera

Fecha del Informe: 19/06/2025

Contenido

Declaración de confidencialidad

Este documento es propiedad exclusiva de KeepCoding y Martin Rivas que es el administrador de collecto.es. Este documento contiene información confidencial y de propiedad exclusiva. La duplicación, distribución o uso, total o parcial, en cualquier forma, requiere el consentimiento de KeepCoding y Martin Rivas que es el administrador de collecto.es.

KeepCoding puede compartir este documento con auditores bajo acuerdos de confidencialidad para demostrar el cumplimiento de los requisitos de prueba de penetración.

Descargo de responsabilidad

Una prueba de penetración se considera una instantánea en el tiempo. Los hallazgos y recomendaciones reflejan la información recopilada durante la evaluación y no los cambios o modificaciones realizados fuera de ese período.

Los compromisos con límite de tiempo no permiten una evaluación completa de todos los controles de seguridad. KeepCoding priorizó la evaluación para identificar los controles de seguridad más débiles que

un atacante podría explotar. KeepCoding recomienda realizar evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuo de los controles.

Información de Contacto

Nombre	Cargo	Correo
Collecto.es		
Martin Rivas	Administrador de collecto.es	martin.rivas.r@hotmail.com
KeepCoding		
Oscar Uriel Tobar Rios	Penetration Tester	oscartobarrios@gmail.com
David	Penetration Tester	davidgroninghernandez@gmail.com
Andres Jesus Ricaurte Valera	Penetration Tester	andresricv@outlook.es

1. Ámbito y Alcance de la Auditoría

- **Objetivo:** El objetivo de esta auditoría es hacer un pestenting para el sitio web collecto.es, en el marco del proyecto de Pentesting del BootCamp de Ciberseguridad IX de Keepcoding, identificando las vulnerabilidades de este sitio.

- **Alcance:** Vamos a realizar una evaluación de seguridad sobre el sitio **https://collecto.es**, enfocada en identificar vulnerabilidades en la aplicación web, sus funcionalidades y posibles subdominios públicos relacionados. El análisis se centrará en el entorno de producción, sin afectar la disponibilidad del servicio ni los datos reales de usuarios.

  La prueba incluirá formularios, flujos de autenticación, APIs visibles y componentes web accesibles desde el navegador, siguiendo los controles del estándar **OWASP Web Security Testing Guide (WSTG)**.

  No se realizarán ataques de denegación de servicio, ingeniería social, ni pruebas sobre infraestructura interna o apps móviles sin autorización previa. Todas las acciones serán controladas, legales y con el consentimiento del responsable del sitio.

2. Clasificación de los Hallazgos

La siguiente tabla define los niveles de gravedad y el rango de puntuación CVSS correspondiente que se utilizan en todo el documento para evaluar la vulnerabilidad y el impacto del riesgo.

Severidad	CVSS V3 Score Range	Definición
Crítico	9.0-10.0	La explotación es sencilla y suele provocar una vulneración a nivel del sistema. Se recomienda elaborar un plan de acción y aplicar el parche de inmediato.
Alto	7.0-8.9	La explotación es más difícil, pero podría provocar privilegios elevados y, potencialmente, una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y aplicar el parche lo antes posible.
Medio	4.0-6.9	Existen vulnerabilidades, pero no se pueden explotar ni requieren medidas adicionales, como ingeniería social. Se recomienda elaborar un plan de acción y aplicar parches después de que se hayan resuelto los problemas de alta prioridad.
Bajo	0.1-3.9	Las vulnerabilidades no se pueden explotar, pero reducirían la superficie de ataque de una organización. Se recomienda elaborar un plan de acción y aplicar parches durante la próxima ventana de mantenimiento.
Informativo	N/A	No existe vulnerabilidad. Se proporciona información adicional sobre elementos detectados durante las pruebas, controles estrictos y documentación adicional.

Risk Factors

El riesgo se mide por dos factores: probabilidad e impacto:

Probabilidad

La probabilidad mide la posibilidad de que se explote una vulnerabilidad. Las clasificaciones se otorgan en función de la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno del cliente.

Impacto

El impacto mide el efecto de la vulnerabilidad potencial en las operaciones, incluida la confidencialidad, integridad y disponibilidad de los sistemas y/o datos del cliente, el daño a la reputación y la pérdida financiera.

3. Alcance

Evaluación	Detalles
https://collecto.es	Página de producción del sitio

Exclusiones del Alcance

A solicitud de KeepCoding no realizó ninguno de los siguientes ataques durante las pruebas:

- Ataques Denial of Service (DoS)
- Phishing/Ingeniería Social

Todos los demás ataques no especificados anteriormente fueron permitidos por KeepCoding.

---

4. Informe Ejecutivo

Breve Resumen del Proceso Realizado

Se evaluó la postura de seguridad interna de collecto.es a través de pruebas de penetración del 29 de mayo al 18 de junio de 2025. Las siguientes secciones brindan una descripción general de alto nivel de las vulnerabilidades descubiertas, los intentos exitosos y fallidos, y las fortalezas y debilidades.

La auditoría se realizó en un entorno productivo. Sobre el sitio collecto.es se hizo inicialmente un trabajo de Reconocimiento (Information Gathering) y luego se procedió a hacer un trabajo de reconocimiento de las vulnerabilidades solicitadas para este informe así como su explotación.

Alcance y limitaciones de tiempo

El alcance durante el compromiso no permitió la denegación de servicio o la ingeniería social en todos los componentes de prueba.

Se establecieron limitaciones de tiempo para las pruebas. Se permitió la prueba de penetración de la red interna durante diez (20) días calendario.

Resumen de la prueba

Durante el análisis de seguridad de aplicaciones y APIs, se identificaron múltiples vulnerabilidades que afectan directamente la confidencialidad, integridad y control de acceso de la página **collecto.es**. Estas fallas representan un riesgo alto, especialmente en entornos donde se manejan datos sensibles de usuarios o se proveen servicios expuestos a internet como la página web productiva de Collecto.es

CWE-200 – Exposure of Sensitive Information to an Unauthorized Actor

- **Descripción**: La aplicación expone datos sensibles (como tokens, correos, IDs o configuraciones internas) a actores no autorizados.
- **Riesgo**: Permite que atacantes accedan o infieran información crítica sin autenticación válida.
- **Impacto**: Compromiso de cuentas, ingeniería social, escalación de privilegios.

---

2. OWASP API A3:2019 – Excessive Data Exposure

- **Descripción**: Las APIs devuelven más datos de los necesarios, incluso si el frontend no los muestra.
- **Riesgo**: Usuarios maliciosos pueden interceptar respuestas y obtener información adicional no autorizada.
- **Impacto**: Fuga de datos personales, explotación de endpoints ocultos.

---

3. CWE-269 – Improper Privilege Management

- **Descripción**: Un usuario con privilegios limitados puede realizar acciones reservadas a roles superiores (como eliminar recursos ajenos).
- **Riesgo**: Violación del principio de privilegio mínimo.
- **Impacto**: Borrado de datos, modificación no autorizada de recursos, acceso no intencionado a funciones administrativas.

---

4. CWE-916 – Use of Password Hash With Insufficient Computational Effort

- **Descripción**: Las contraseñas son almacenadas con algoritmos de hash débiles (e.g., SHA-1, MD5) o sin mecanismos como salting y key stretching.
- **Riesgo**: Facilita ataques de diccionario o fuerza bruta si se filtra la base de datos.
- **Impacto**: Compromiso masivo de cuentas de usuario ante brechas de seguridad.

---

5. CVE-2025-22387 – Session Token en URL (Optimizely)

- **Descripción**: La aplicación expone tokens de sesión directamente en las URLs.
- **Riesgo**: Las URLs pueden ser registradas en logs, historiales o referers, exponiendo la sesión activa a terceros.
- **Impacto**: Secuestro de sesión, acceso no autorizado a cuentas.

---

6. CVE-2024-28238 – JWT Expuesto por Parámetro GET (Directus)

- **Descripción**: El sistema entrega tokens JWT en parámetros de URL GET en respuestas públicas.
- **Riesgo**: Permite la exposición de autenticación persistente a actores no autorizados.
- **Impacto**: Pérdida de control de sesión, acceso no autorizado a interfaces administrativas.

Notas y recomendaciones del auditor

- Aplicar el principio de **mínimo privilegio** y control estricto por roles.
- Validar siempre el destinatario de los datos antes de responder desde la API.
- Usar funciones robustas de hashing (e.g., Argon2, bcrypt) con sal y múltiples rondas.
- Nunca exponer tokens o IDs sensibles en URLs (usar cabeceras o cookies seguras).
- Realizar pruebas automáticas de seguridad en pipelines CI/CD.

Resumen de vulnerabilidades

Las siguientes tablas ilustran las vulnerabilidades encontradas por impacto y las soluciones recomendadas

5	8	4	0	0
Critico	Alta	Medio	Baja	Informativa

Hallazgo	Severidad	Recomendación
H-001: Exportar usuarios del sistema	Crítico	Realizar un parche urgente para corregir el sistema
H-002: Protección CSRF	Crítico	Implementar tokens anti-CSRF (por ejemplo, CSRF tokens únicos por sesión y solicitud) y verificar su validez

		en el servidor. Además, usar el atributo SameSite en las cookies para limitar su envío automático entre dominios.
H-003: Credenciales adivinables	Crítico	Exigir una contraseña con más longitud, caracteres especiales y que sea alfanumérica.
H-004: Se puede crear un usuario Administrador	Crítico	Restringir la creación de usuarios administradores exclusivamente a procesos internos autenticados y autorizados. Validar en el backend el rol asignado en cada solicitud y aplicar controles estrictos de autorización.
H-005: Falta de definición de directiva sin respaldo	Crítico	Definir correctamente todas las directivas críticas de la política CSP, incluyendo frame-ancestors y form-action, para reducir la exposición a ataques como clickjacking o envío de formularios maliciosos.
H-006: La longitud de password de los usuarios es insuficiente	Alta	Exigir una longitud mínima de al menos 12 caracteres para contraseñas, junto con políticas de complejidad que incluyan letras mayúsculas, minúsculas, números y caracteres especiales.
H-007: Que puede crear un usuario sin autenticar el correo de alta	Alta	El ID de sesión nunca debe estar en la URL, ya que puede quedar expuesto a través del historial del navegador, registros de proxy, referers HTTP, o incluso por terceros si el usuario comparte un enlace
H-008: Se pueden borrar los artículos	Alta	Se recomienda utilizar la api con DELETE usado el control de propiedad del recurso y con validación completa del JWT/tokens, para evitar que se use inadecuadamente .
H-009: ID de sesión en la reescritura de URL	Alta	Para contenido seguro, ponga el ID de sesión en una cookie. Para ser aún más seguro considere usar una combinación de cookie y URL rewrite.
H-010: ID de sesión en la Reescritura de URL(2)	Alta	Para mayor seguridad, almacene el ID de sesión en una cookie. Para reforzarla aún más, puede combinar cookies con reescritura de URL.

H-011: Encabezado de seguridad de transporte estricto no establecido	Alta	Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. Está configurado para aplicar Strict-Transport-Security.
H-012: Filtración del ubuntu (nginx) corriendo la web	Alta	Oculte cabeceras y mensajes de error del servidor, use páginas de error personalizadas, mantenga actualizados los servicios expuestos y restrinja el acceso a directorios no públicos si no son necesarios.
H-013: Enumeración de Directorios Web sensibles (Directory Brute Forcing)	Alta	Ocultar cabeceras y mensajes de error predeterminados del servidor web. Configurar páginas de error personalizadas que no revelen información sensible.
H-014: Cabecera política de seguridad de contenidos (CSP) no configurada	Medio	Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.
H-015: Falta de cabecera Anti-Clickjacking	Medio	Configure en su sitio/aplicación las cabeceras Content-Security-Policy o X-Frame-Options para prevenir el uso no autorizado en iframes. Use SAMEORIGIN sí solo su propio sitio debe incrustar la página, DENY si no debe incrustarse, o la directiva frame-ancestors como alternativa moderna.
H-016: El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP “”X-Powered-By””	Medio	Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para suprimir las cabeceras "X-Powered-By".
H-017: Falta encabezado X-Content-Type-Options	Medio	Configure correctamente el encabezado Content-Type y establezca X-Content-Type-Options: nosniff para evitar que los navegadores realicen MIME-sniffing. Además, promueva el uso de navegadores modernos que respeten estos encabezados.

5. Hallazgos Técnicos

5.1 Hallazgo H-001: Exportar usuarios del sistema (Crítica).

Descripción:	El sitio de collecto.es, permite que cualquier usuario con un navegador partida consultar los datos de todos los usuarios, tales como el correo, el teléfono, el nombre el apellido y todos los datos reportados de los usuarios
Severidad:	Crítico
Riesgo:	Se puede acceder al https://collecto.es/api/users y descargar la base de datos de usuarios del sistema
Herramientas:	Navegador Web
Referencias:	• CWE-200: Exposure of Sensitive Information to an Unauthorized Actor. • OWASP API Security Top 10 – A3:2019 – Excessive Data Exposure

.

5.1.1 Evidencia

5.1.2 Recomendación

Se debe revisar el uso de APIS utilizando protección para todas las APIs

- Usar JWT en cookies, siempre implementa protección CSRF.
- Usar JWT en Authorization header, el riesgo de CSRF es mucho menor, porque las cabeceras personalizadas no se envían automáticamente por navegadores desde sitios externos.

5.2 Hallazgo H-002: Protección de falsificación de solicitud entre sitios CSRF (Crítica).

Descripción:	Cuando el token JWT está en una cookie, los navegadores lo incluye automáticamente en las solicitudes, incluso si se hacen desde un sitio malicioso (si no hay protección adecuada). Eso significa que un atacante podría, por ejemplo, enviar una solicitud PUT al backend en nombre del usuario, si este tiene la sesión iniciada Sin esta validación, un atacante puede enviar formularios desde otro dominio, y si el navegador incluye las cookies, podrá ejecutar acciones peligrosas en nombre del usuario (como cambiar anuncios, borrar cuentas, subir precios, etc.).
Severidad:	Crítico
Riesgo:	La falsificación de solicitud entre sitios (CSRF), también conocida como XSRF, Sea Surf o Session Riding, es un vector de ataque que engaña a un navegador web para que ejecute una acción no deseada en una aplicación en la que el usuario ha iniciado sesión . Un ataque CSRF exitoso puede ser devastador tanto para la empresa como para el usuario
Herramientas:	Burn Suite.
Referencias:	OWASP – Cross-Site Request Forgery (CSRF)

5.2.1 Evidencia

Se hace una solicitud PUT autenticada con un JWT en una cookie, y se origina desde el frontend en https://collecto.es. Esto tiene implicaciones importantes de seguridad si no se restringe debidamente el acceso a través de CORS y SameSite, ya que el simple uso de cookies no es suficiente para evitar ataques de tipo CSRF (Cross-Site Request Forgery)

5.2.2 Recomendación

- Usar JWT en cookies, siempre implementa protección CSRF.

- Usar JWT en Authorization header, el riesgo de CSRF es mucho menor, porque las cabeceras personalizadas no se envían automáticamente por navegadores desde sitios externos.

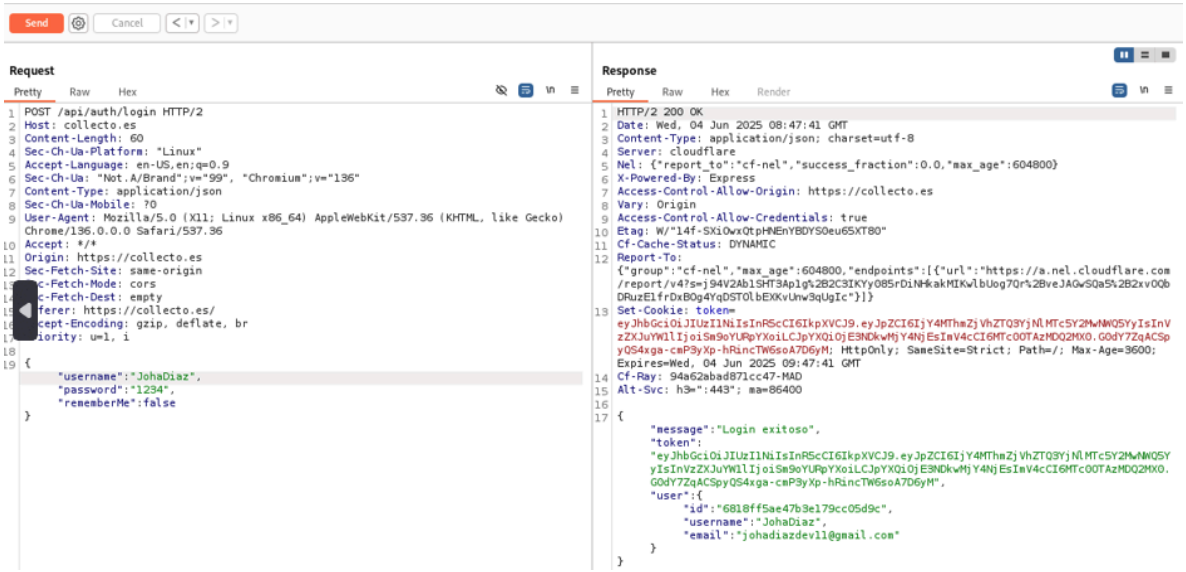
Configurar la cookie JWT con:

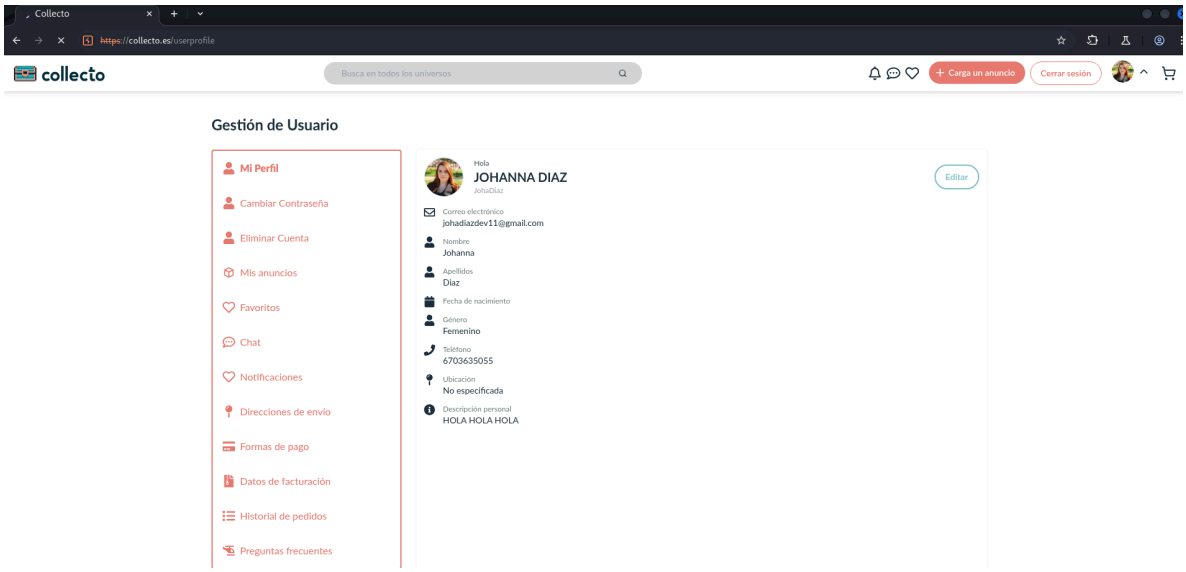
- HttpOnly
- Secure
- SameSite=Strict (o Lax)

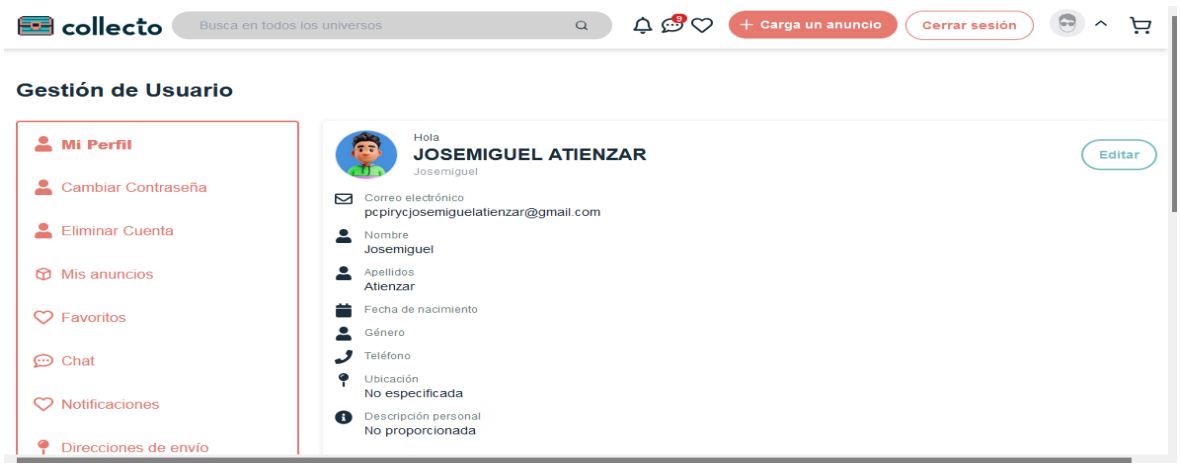
5.3 Hallazgo H-003: Credenciales adivinables. (Crítica)

Descripción:	Durante la fase de evaluación de autenticación en la aplicación web Collecto.es, se identificó que algunas cuentas de usuario utilizan contraseñas extremadamente débiles, específicamente la combinación 1234. Este tipo de contraseñas son ampliamente conocidas y utilizadas en ataques de fuerza bruta o adivinación manual, ya que forman parte de listas comunes de contraseñas débiles.
Severidad:	Crítico
Riesgo:	Adivinación de credenciales, modificación de contraseñas de usuarios y acceso no autorizado a datos personales, como formas de pago, direcciones y otra información sensible de los usuarios del sitio web.
Herramientas:	Burp Suite y Navegador Web
Referencias:	• OWASP Top 10 – A07:2021 – Identification and Authentication Failures. • OWASP ASVS v4.0.3 – V2.1 Password Security • Have I Been Pwned – Passwords API / listas de contraseñas comprometidas. • No aplica un CVE específico porque se trata de una mala práctica de configuración y gestión de usuarios.

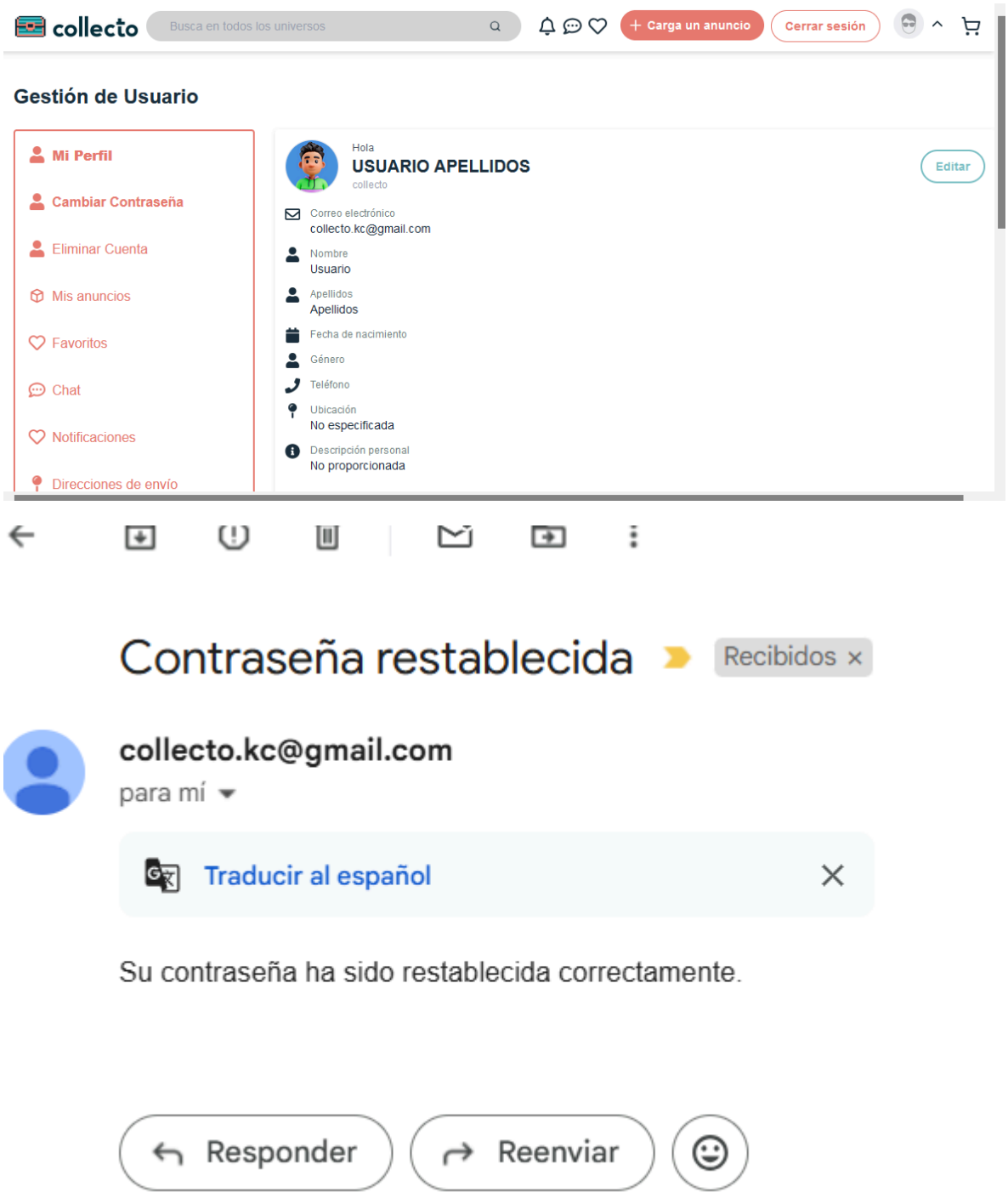
5.3.1 Evidencia







Se logra acceder al usuario, el cual tiene como correo electrónico el correo que envía la recuperación de contraseñas.



5.3.2 Recomendación

Se recomienda implementar las siguientes medidas para prevenir el uso de credenciales débiles o adivinadas:

Política de contraseñas seguras:

- Requerir contraseñas con al menos 8 caracteres.
- Incluir una combinación de letras mayúsculas, minúsculas, números y símbolos.
- Prohibir contraseñas comunes (como 1234, admin, password, etc.), usando listas negras de contraseñas conocidas (como las de Have I Been Pwned).

Bloqueo y protección ante intentos fallidos:

- Implementar un límite de intentos de inicio de sesión (por ejemplo, 5 intentos fallidos).
- Aplicar bloqueo temporal de cuenta o mostrar un CAPTCHA tras múltiples intentos fallidos.

Autenticación multifactor (MFA):

- Ofrecer (y preferiblemente requerir) el uso de un segundo factor de autenticación, como un código por SMS o una aplicación de autenticación.

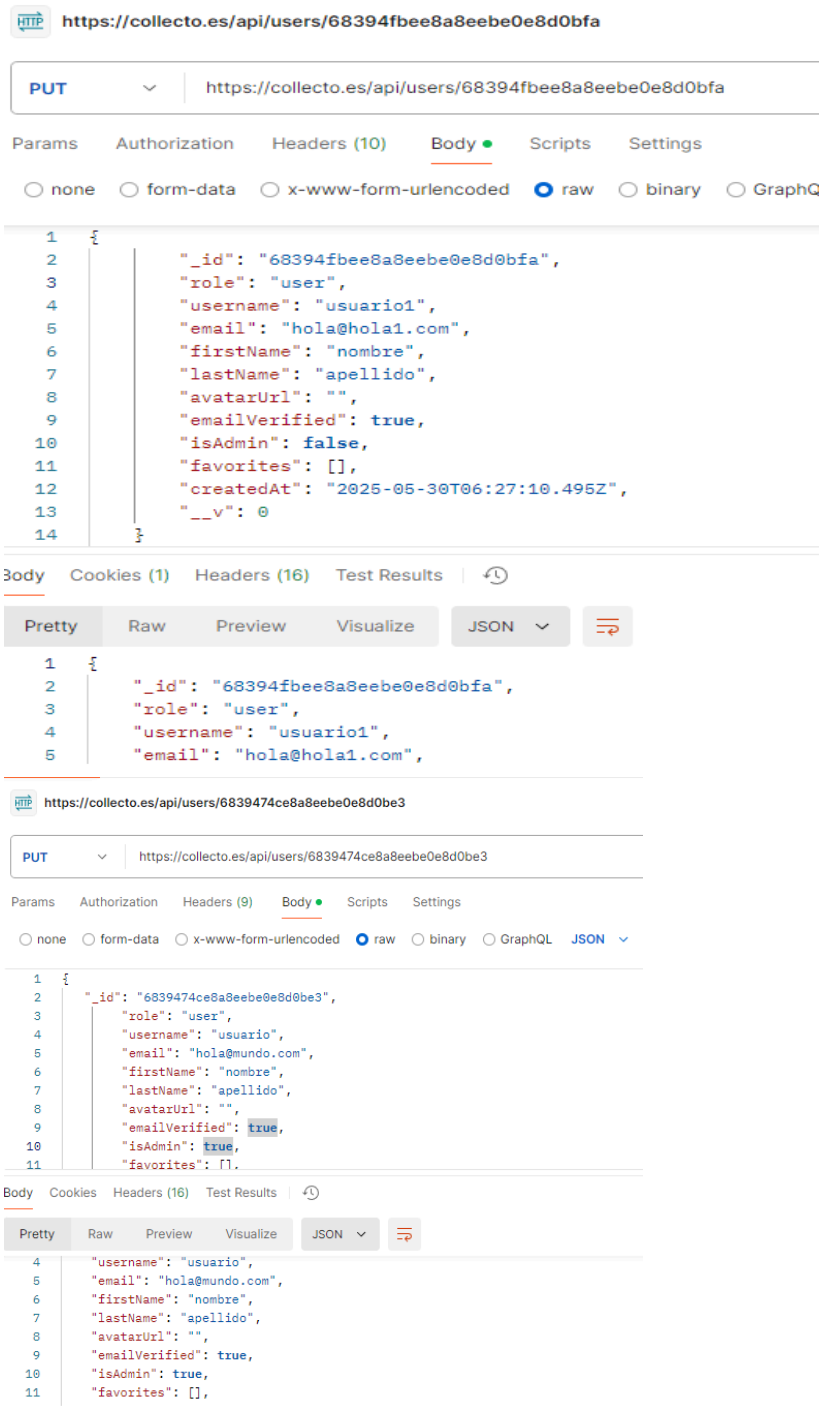
Revisión y restablecimiento de credenciales actuales:

- Realizar una auditoría de cuentas existentes para detectar y forzar el cambio de contraseñas débiles o predecibles.

5.4 Hallazgo H-004: Se púede crear un usuario Administrador (Crítica)

Descripción:	Se puede cambiar el estado a un usuario para poder cambiar a sus privilegios como administrador
Severidad:	Crítico
Riesgo:	Permitir la creación no autorizada de cuentas con privilegios administrativos es una de las fallas más graves en una aplicación web.
Herramientas:	Burn Suite.
Referencias:	● OWASP Top 10 – A01:2021 – Broken Access Control https://owasp.org/Top10/A01_2021-Broken_Access_Control/ ● CWE-269: Improper Privilege Management ● https://cwe.mitre.org/data/definitions/269.html ● CWE-284: Improper Access Control ● https://cwe.mitre.org/data/definitions/284.html

5.4.1 Evidencia



5.4.2 Recomendación

Control estricto del rol asignado en la creación de usuarios:

- Validar siempre en el servidor que ningún usuario pueda asignarse a sí mismo, ni mediante manipulación de parámetros, un rol con privilegios elevados (por ejemplo, admin o superuser).

- Ignorar cualquier valor de rol recibido desde el cliente y definirlo únicamente desde el backend, según el contexto y permisos del usuario autenticado.

Restringir la creación de cuentas administrativas:

- La creación de usuarios con privilegios administrativos debe estar limitada a:
    - Usuarios ya autenticados y autorizados como administradores.
    - Procesos internos bajo control estricto (por ejemplo, desde un panel interno protegido o por línea de comandos).
- Implementar autenticación multifactor (MFA) obligatoria para administradores.

Auditoría y registro de acciones sensibles:

- Registrar todos los eventos relacionados con la creación o modificación de cuentas con privilegios elevados.

- Establecer alertas en tiempo real si se detecta actividad inusual, como la creación de un nuevo administrador.

Revisión de roles y políticas de autorización:

- Aplicar el principio de **mínimos privilegios (PoLP)**: cada usuario debe tener solo los permisos necesarios para realizar su función.

- Realizar una revisión de todos los roles existentes en el sistema para verificar que no haya accesos excesivos o mal configurados.

5.5 Hallazgo H-005: Falta de definición de directiva sin respaldo (Crítica)

Descripción:	La Política de Seguridad de Contenido no define una de las directivas sin respaldo. Omitirlas o excluirlas equivale a permitir cualquier cosa. Las directivas: frame-ancestors, form-action están entre las directivas que no recurren a default-src.
Severidad:	Crítica
Riesgo:	La falta de definición explícita de las directivas frame-ancestors y form-action permite que el sitio sea embebido en páginas externas (clickjacking) y que los formularios puedan enviar datos a cualquier dominio, lo que puede facilitar ataques de phishing o fuga de información sensible.
Sistema:	https://collecto.es/api/
Herramientas:	ZAP PROXY

5.5.1 Evidencia

Request

Línea de solicitud y sección de encabezado (262 bytes)

```
GET https://collecto.es/api/ HTTP/1.1
host: collecto.es
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://collecto.es/api
```

Response

Línea de estado y sección de encabezado (775 bytes)

```
HTTP/1.1 404 Not Found
Date: Sun, 01 Jun 2025 19:46:08 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Server: cloudflare
Nel:
{"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
X-Powered-By: Express
Access-Control-Allow-Origin: https://collecto.es
Vary: Origin
Vary: accept-encoding
```

```
Access-Control-Allow-Credentials: true
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Cf-Cache-Status: DYNAMIC
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a
.nel.cloudflare.com/report/v4?s=oKkR3iUOl95TM4rkL1QtYETKoJKfdDY5H
%2Fr8DCbJTJcxyI1WSlVEz%2FNfSLDlCt%2FekY2N1XGrCdbXACdx1RTVxps%2B7y
pmAsOo%2FX3t"}]}
CF-RAY: 949137204aec1e3d-MIA
alt-svc: h3=":443"; ma=86400
content-length: 143
```

Cuerpo de la respuesta (143 bytes)

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>Cannot GET /api/</pre>
</body>
</html>

PARAMETRO
Content-Security-Policy

EVIDENCIA
default-src 'none'
```

5.5.2 Recomendación

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado apropiadamente para establecer la cabecera de Política de Seguridad de Contenido.

5.6 Hallazgo H-006: La longitud de password de los usuarios es insuficiente (Alto).

Descripción:	Para crear un usuario solo se requiere un password de 4 caracteres. Esto facilita ataques de fuerza bruta o adivinación de credenciales, especialmente si las contraseñas son cortas y previsibles (como "1234" o "admin"). La ausencia de políticas estrictas de complejidad y longitud mínima debilita la autenticación del sistema.
Severidad:	Alto
Riesgo:	Los atacantes pueden comprometer cuentas mediante ataques de fuerza bruta o diccionario, accediendo a datos sensibles o tomando control de cuentas de usuarios o administradores.
Herramientas:	Navegador Web
Referencias:	CWE-916: Use of Password Hash With Insufficient Computational Effort

5.6.1 Evidencia

5.6.2 Recomendación

Para fortalecer la seguridad de las cuentas de usuario, se recomienda implementar una política robusta de contraseñas que incluya:

- **Longitud mínima de 12 caracteres.**
- **Requisitos de complejidad**, como la inclusión de al menos:
    - Una letra mayúscula.
    - Una letra minúscula.
    - Un número.
    - Un carácter especial (@, #, %, etc.).
- **Rechazar contraseñas comunes o comprometidas**, utilizando listas negras (como Have I Been Pwned o listas OWASP).
- **Aplicar controles en el lado del servidor**, para evitar que usuarios modifiquen las restricciones mediante manipulación de formularios.

- **Permitir autenticación multifactor (MFA)** para reducir el riesgo en caso de contraseñas débiles o robadas.

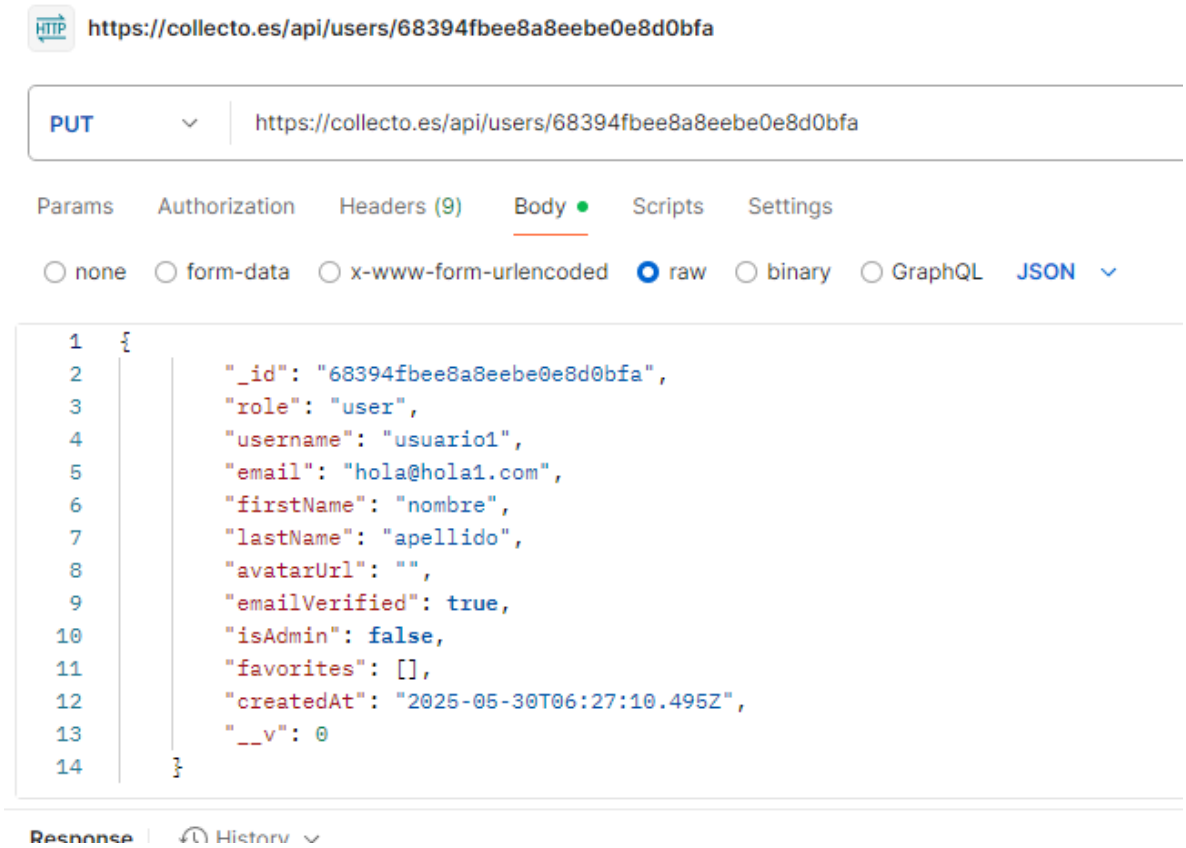
- **Mostrar a los usuarios indicadores de fuerza de contraseña** durante el registro o cambio de contraseña.

5.7 Hallazgo H-007: Que puede crear un usuario sin autenticar el correo de alta (Alta)

Descripción:	Al crear un usuario, el sistema espera que el usuario reciba un correo electrónico para verificar que sea un correo válido. Cuando el usuario recibe el correo de validación la página de collecto activa el nuevo usuario. Sin embargo se determinó que es posible utilizar un correo que no exista para poder crear un usuario en el sistema, y utilizando una API https://collecto.es/api/users se pueden modifiquen los datos del usuario y habilitarlo sin necesidad de que el usuario reciba la activación.
Severidad:	Alta
Riesgo:	La api de usuarios se puede modificar por usuarios no autorizados, permitiendo alterar la información de los usuarios
Sistema:	en el usuario usuario1 se puede cambiar https://collecto.es/api/users/68394fbee8a8eebe0e8d0bfa
Herramientas:	Postman
Referencias:	CVE-2025-22387 CVE-2024-28238

5.7.1 Evidencia

En el usuario usuario1 se puede cambiar la información del usuario utilizando un PUT para el API
https://collecto.es/api/users/68394fbee8a8eebe0e8d0bfa



5.7.2 Recomendación

Eliminar la reescritura de URL para sesiones:

El ID de sesión nunca debe estar en la URL, ya que puede quedar expuesto a través del historial del navegador, registros de proxy, referers HTTP, o incluso por terceros si el usuario comparte un enlace.

Usar cookies para mantener sesiones:

Las cookies permiten manejar el ID de sesión de manera más segura. Deben tener activados los siguientes atributos:

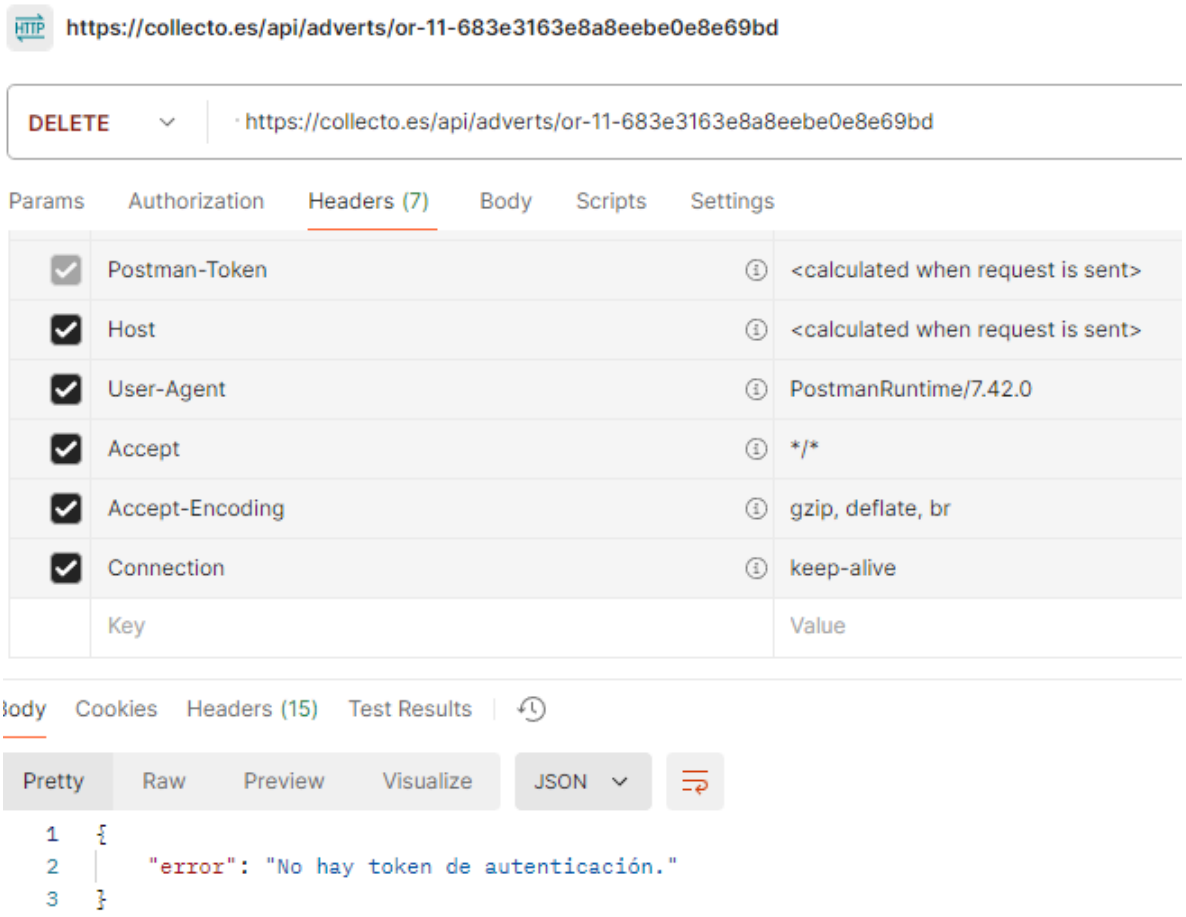
- HttpOnly: evita el acceso al ID de sesión mediante JavaScript.
- Secure: garantiza que la cookie solo se envíe a través de HTTPS.

- SameSite=Strict o Lax: protege frente a ataques CSRF.

5.8 Hallazgo H-008: Se pueden borrar los Artículos (Alta)

Descripción:	Al utilizar el verbo DELETE en la API https://collecto.es/api/adverts se puede eliminar el articulo de otro usuario sin tener las credenciales para ello. Para esto solamente se debe utilizar el token de un usuario activo, cambiar el nombre del usuario que está dentro del token y suplantar al usuario dueño del anuncio, con esto es posible eliminar el articulo
Severidad:	Alta
Riesgo:	Eliminación de datos criticos de la pagina sin autorización
Sistema:	Collecto.es/api
Herramientas:	Postman
Referencias:	CVE-2024-12267

5.8.1 Evidencia



5.8.2 Recomendación

Se recomienda utilizar la api con DELETE usado el control de propiedad del recurso y con validación completa del JWT/tokens, para evitar que se use inadecuadamente .

5.9 Hallazgo H-009: ID de sesión en la Reescritura de URL (Alto)

Descripción:	La reescritura de URL se utiliza para rastrear el ID de sesión del usuario. El ID de sesión puede ser revelado a través del encabezado cross-site referer. Además, el ID de sesión puede almacenarse en el historial del navegador o en los registros del servidor.
Severidad:	Alta
Riesgo:	El uso de reescritura de URL para manejar el ID de sesión expone la sesión del usuario a posibles robos, ya que puede filtrarse a través del historial, registros del servidor o encabezados Referer. Esto puede permitir a un atacante secuestrar sesiones y acceder a cuentas sin autorización.
Sistema:	https://collecto.es/socket.io
Herramientas:	ZAP PROXY
Referencias:	https://seclists.org/webappsec/2002/q4/111 https://cwe.mitre.org/data/definitions/598.html

5.9.1 Evidencia

Request

Línea de solicitud y sección de encabezado

GET
https://collecto.es/socket.io/?EIO=4&transport=websocket&sid=YwYodGgcUsJCcjweAAS_
HTTP/1.1
host: collecto.es
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-WebSocket-Version: 13
Origin: https://collecto.es
Sec-WebSocket-Key: swU4gsqJOHMqYmudgSSAzQ==
Connection: keep-alive, Upgrade
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: websocket
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket

Response

Línea de solicitud y sección de encabezado

HTTP/1.1 400 Bad Request

Date: Tue, 10 Jun 2025 19:22:10 GMT
Content-Type: text/html
Connection: keep-alive
cf-cache-status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=x%2FaJqZO4GIJNGew%2BK0ZDf%2Bd9FHKz3F1D1KSGlx4iMM3PAR8u27mxgJ10SSAPv9wrZLxa4pq41N14Lw5J41%2FkQ224vOgAeHM%2BWYJcNUNQ8unrWS9fn2k53xnWQ1qfYA%3D%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 94db3c656acce2d1-GIG
alt-svc: h3=":443"; ma=86400
server-timing:
cfL4;desc="?proto=TCP&rtt=146165&min_rtt=146113&rtt_var=41185&sent=6&recv=8&lost=0&retrans=0&sent_bytes=3110&recv_bytes=1353&delivery_rate=28700&cwnd=41&unsent_bytes=0&cid=10611168aeb312b8&ts=531&x=0"
content-length: 18

5.9.2 Recomendación

Eliminar la reescritura de URL para sesiones:

El ID de sesión nunca debe estar en la URL, ya que puede quedar expuesto a través del historial del navegador, registros de proxy, referers HTTP, o incluso por terceros si el usuario comparte un enlace.

Usar cookies para mantener sesiones:

Las cookies permiten manejar el ID de sesión de manera más segura. Deben tener activados los siguientes atributos:

- HttpOnly: evita el acceso al ID de sesión mediante JavaScript.
- Secure: garantiza que la cookie solo se envíe a través de HTTPS.
- SameSite=Strict o Lax: protege frente a ataques CSRF.

Revisar configuraciones de frameworks y servidores:

Muchos frameworks habilitan la reescritura de URL por defecto si las cookies están desactivadas. Asegúrate de que esta opción este deshabilitada.

Implementar expiración de sesión y regeneración del ID:

Siempre regenerar el ID de sesión después de la autenticación para prevenir ataques de fijación de sesión (session fixation).

5.10 Hallazgo H-010: ID de sesión en la Reescritura de URL (Alta)

Descripción:	La reescritura de URL se utiliza para rastrear el ID de sesión del usuario. El ID de sesión puede ser revelado a través del encabezado cross-site referer. Además, el ID de sesión puede almacenarse en el historial del navegador o en los registros del servidor.
Severidad:	Alta
Riesgo:	Se puede utilizar el ID de session del usuario para exponer informacion
Sistema:	https://collecto.es/socket.io/?EIO=4&transport=websocket&sid=elnTi3Cg2SMQDAkvAADm
Herramientas:	ZAP Proxy
Referencias:	■ CWE-598 ■ OWASP_2021_A01 ■ WSTG-v42-SESS-04 ■ OWASP_2017_A03

5.10.1 Evidencia

Request

Línea de solicitud y sección de encabezado (523 bytes)

```
GET
https://collecto.es/socket.io/?EIO=4&transport=websocket&sid=elnTi3Cg2SMQDA
kvAADm HTTP/1.1
host: collecto.es
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Sec-WebSocket-Version: 13
Origin: https://collecto.es
Sec-WebSocket-Key: YXGxdV96Ku+fosijasybTA==
Connection: keep-alive, Upgrade
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: websocket
Sec-Fetch-Site: same-origin
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket
```

Response

Línea de estado y sección de encabezado (915 bytes)

```
HTTP/1.1 101 Switching Protocols
Date: Sun, 01 Jun 2025 19:46:18 GMT
Connection: upgrade
Upgrade: websocket
Sec-WebSocket-Accept: E9ug/YXFnD94jQ7JKND0o24xw/A=
Access-Control-Allow-Origin: https://collecto.es
Vary: Origin
Access-Control-Allow-Credentials: true
cf-cache-status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=cEVO%2B1
iU0bz9A6e03ZWHNc0a78qFKa33xNIO66l83oK44yz6we6uHJsi4TqKuTEPxDCU5AXTjzkWX%2B8
HfUnr16Ga8CAS9zmVJmCPIGIhiIJVa6OIOXgXEp8%2FrRa0vQ%3D%3D"}],"group":"cf-nel"
,"max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 9491375ffd6021e7-MIA
alt-svc: h3=":443"; ma=86400
server-timing:
cfL4;desc="?proto=TCP&rtt=62419&min_rtt=62316&rtt_var=23575&sent=6&recv=7&l
ost=0&retrans=0&sent_bytes=3112&recv_bytes=1098&delivery_rate=66515&cwnd=25
0&unsent_bytes=0&cid=7d72b3a594e0917a&ts=204&x=0"

PARAMETRO : sid
Evidencia: elnTi3Cg2SMQDAkvAADm
```

5.10.2 Recomendación

Para contenido seguro, ponga el ID de sesión en una cookie. Para ser aún más seguro, considere usar una combinación de cookies y reescritura de URL.

5.11 Hallazgo H-011: Encabezado de seguridad de transporte estricto no establecido (Alta)

Descripción:	HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL). HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797.
Severidad:	Alta
Riesgo:	Los navegadores pueden intentar inicialmente conectarse a través de HTTP (no cifrado). Esto **abre una ventana de oportunidad para ataques Man-in-the-Middle (MitM)**, especialmente en redes públicas o comprometidas
Sistema:	https://collecto.es
Herramientas:	ZAP PROXY

Referencias:	■ OWASP_2021_A05 ■ CWE-319 ■ OWASP_2017_A06

▪

5.11.1 Evidencia

Request

Línea de solicitud y sección de encabezado (223 bytes)

```
GET https://collecto.es HTTP/1.1
host: collecto.es
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```

Response

Línea de estado y sección de encabezado (592 bytes)

```
HTTP/1.1 200 OK
Date: Sun, 01 Jun 2025 19:46:06 GMT
Content-Type: text/html
Connection: keep-alive
Server: cloudflare
Last-Modified: Thu, 08 May 2025 17:54:30 GMT
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.clo
udflare.com/report/v4?s=Kq5SpwSBUHtXPgUxfzXXaCl0zCG3ly7Dni9YV0r%2BT%2FNzH
q0BKYFAE9haDDcK9stOE7kuExZhwN%2BA3dzaThgUHnNnFm%2BEzPHWwexk"}]}
Vary: accept-encoding
Cf-Cache-Status: DYNAMIC
CF-RAY: 94913714dc9fb7f2-MIA
alt-svc: h3=":443"; ma=86400
content-length: 890
```

Cuerpo de la respuesta (890 bytes)

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" type="image/svg+xml" href="/collecto-favicon.png" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0"
/>

    <link rel="preconnect" href="https://fonts.googleapis.com" />
    <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin
/>
```

```
    <link

href="https://fonts.googleapis.com/css2?family=Quicksand:wght@300;500;700
&display=swap"
      rel="stylesheet"
    />
    <link

href="https://fonts.googleapis.com/css2?family=Material+Symbols+Outlined"
      rel="stylesheet"
    />

    <title>Collecto</title>
    <script type="module" crossorigin
src="/assets/index-Cd4kMVDa.js"></script>
    <link rel="stylesheet" crossorigin href="/assets/index-Dqo59u5u.css">
  </head>
  <body>
    <div id="root"></div>

  </body>
</html>
```

5.11.2 Recomendación

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. Está configurado para aplicar Strict-Transport-Security.

5.12 Hallazgo H-012: Filtración del ubuntu(nginx) corriendo la web (Alta).

Descripción:	Se detectó que al acceder a ciertos directorios del sitio web, como **/assets/**, el servidor responde con un mensaje de error 403 Forbidden que incluye detalles sobre la infraestructura, específicamente la versión del servidor web y el sistema operativo: **nginx/1.24.0 (Ubuntu)**.
Severidad:	Alta
Riesgo:	Un atacante puede utilizar esta información para buscar vulnerabilidades específicas de esa versión de Nginx o del sistema operativo.
Sistema:	https://collecto.es/assets/
Herramientas:	Navegador Web
Referencias:	OWASP - Information Disclosure

	Hardening Nginx - Disable Server Tokens

5.12.1 Evidencia

5.12.2 Recomendación

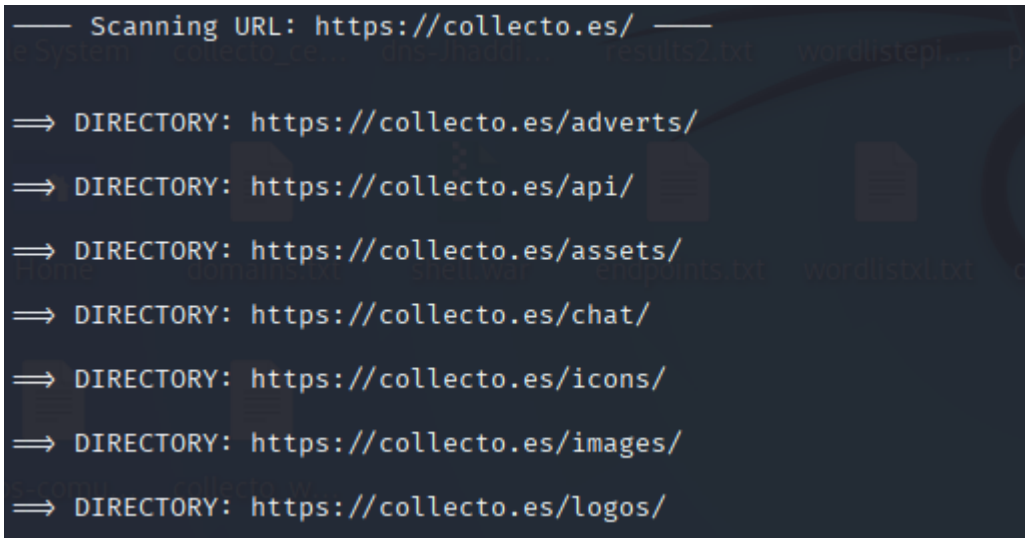
- Ocultar cabeceras y mensajes de error predeterminados del servidor web.
- Configurar páginas de error personalizadas que no revelen información sensible.
- Actualizar regularmente los servicios expuestos, en especial si las versiones reveladas ya no reciben soporte o contienen CVEs conocidos.
- Deshabilitar el acceso directo a directorios no públicos, si no se requiere.

5.13 Hallazgo H-013: Enumeración de Directorios Web sensibles (Directory Brute Forcing) (Alta).

Descripción:	Durante una revisión de seguridad, se identificó que el servidor web permite la enumeración de directorios mediante fuerza bruta utilizando herramientas como **dirb**.
Severidad:	Alta
Riesgo:	Permite descubrir rutas no listadas públicamente, lo cual puede proporcionar información sensible o no destinada a ser expuesta. https://collecto.es/adverts/ https://collecto.es/api/

	https://collecto.es/assets/ https://collecto.es/chat/ https://collecto.es/icons/ https://collecto.es/images/ https://collecto.es/logos/ https://collecto.es/users/
Herramientas:	dirb
Referencias:	OWASP - Directory Listing

5.13.1 Evidencia



5.13.2 Recomendación

- Deshabilitar listado de directorios en el servidor web si está habilitado.
- Ofuscación y control de acceso a rutas sensibles, usando autenticación o tokenización.
- Validación de permisos y autenticación adecuada para cada recurso expuesto.
- Monitorización de escaneos o patrones de fuerza bruta mediante herramientas de detección de amenazas o WAF.

5.14 Hallazgo H-014: Cabecera Política de seguridad de contenidos (CSP) no configurada (Medio)

Descripción:	La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.
Severidad:	Alta
Riesgo:	La falta de una Política de Seguridad de Contenido (CSP) en el sitio expone al navegador del usuario a la ejecución de scripts maliciosos mediante ataques como Cross-Site Scripting (XSS), permitiendo a un atacante robar información sensible como cookies o tokens de sesión, cargar contenido desde dominios no confiables, suplantar la identidad del usuario y realizar acciones en su nombre.
Sistema:	https://collecto.es/
Herramientas:	ZAP PROXY

5.14.1 Evidencia

Request

Línea de solicitud y sección de encabezado (223 bytes)

```
GET https://collecto.es HTTP/1.1
host: collecto.es
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

Response

Línea de estado y sección de encabezado (592 bytes)

```
HTTP/1.1 200 OK
Date: Sun, 01 Jun 2025 19:46:06 GMT
Content-Type: text/html
Connection: keep-alive
Server: cloudflare
Last-Modified: Thu, 08 May 2025 17:54:30 GMT
Nel:
{"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a
.nel.cloudflare.com/report/v4?s=Kq5SpwSBUHtXPgUxfzXXaCl0zCG3ly7Dn
i9YV0r%2BT%2FNzHq0BKYFAE9haDDcK9stOE7kuExZhwN%2BA3dzaThgUHnNnFm%2
BEzPHWwexk"}]}
Vary: accept-encoding
Cf-Cache-Status: DYNAMIC
CF-RAY: 94913714dc9fb7f2-MIA
alt-svc: h3=":443"; ma=86400
content-length: 890
```

Cuerpo de la respuesta (890 bytes)

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" type="image/svg+xml"
href="/collecto-favicon.png" />
    <meta name="viewport" content="width=device-width,
initial-scale=1.0" />

    <link rel="preconnect" href="https://fonts.googleapis.com" />
    <link rel="preconnect" href="https://fonts.gstatic.com"
crossorigin />

    <link

href="https://fonts.googleapis.com/css2?family=Quicksand:wght@300;
500;700&display=swap"
      rel="stylesheet"
    />
    <link

href="https://fonts.googleapis.com/css2?family=Material+Symbols+Ou
tlined"
      rel="stylesheet"
    />

    <title>Collecto</title>
```

```
    <script type="module" crossorigin
src="/assets/index-Cd4kMVDa.js"></script>
    <link rel="stylesheet" crossorigin
href="/assets/index-Dqo59u5u.css">
  </head>
  <body>
    <div id="root"></div>

  </body>
</html>
```

5.14.2 Recomendación

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.

5.15 Hallazgo H-015: Falta de cabecera Anti-Clickjacking (Media)

Descripción:	La respuesta no protege contra ataques de "ClickJacking". Debes incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.
Severidad:	Media
Riesgo:	Clickjacking es una técnica de ataque en la que un atacante embebe el sitio legítimo dentro de un <iframe> oculto o transparente sobre una página controlada por él. Esto permite engañar al usuario para que haga clic en elementos del sitio real (como botones de “Aceptar”, “Pagar”, o “Eliminar cuenta”) sin saberlo.
Sistema:	https://collecto.es
Herramientas:	Zap Proxy
Referencias:	■ OWASP_2021_A05 ■ CWE-1021 ■ WSTG-v42-CLNT-09 ■ OWASP_2017_A06

5.15.1 Evidencia

Request

Línea de solicitud y sección de encabezado (223 bytes)

```
GET https://collecto.es HTTP/1.1
```

```
host: collecto.es
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

Response

Línea de estado y sección de encabezado (592 bytes)

```
HTTP/1.1 200 OK
Date: Sun, 01 Jun 2025 19:46:06 GMT
Content-Type: text/html
Connection: keep-alive
Server: cloudflare
Last-Modified: Thu, 08 May 2025 17:54:30 GMT
Nel:
{"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.
nel.cloudflare.com/report/v4?s=Kq5SpwSBUHtXPgUxfzXXaCl0zCG3ly7Dni9
YV0r%2BT%2FNzHq0BKYFAE9haDDcK9stOE7kuExZhwN%2BA3dzaThgUHnNnFm%2BEz
PHWwexk"}]}
Vary: accept-encoding
Cf-Cache-Status: DYNAMIC
CF-RAY: 94913714dc9fb7f2-MIA
alt-svc: h3=":443"; ma=86400
content-length: 890
```

Cuerpo de la respuesta (890 bytes)

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" type="image/svg+xml"
href="/collecto-favicon.png" />
    <meta name="viewport" content="width=device-width,
initial-scale=1.0" />

    <link rel="preconnect" href="https://fonts.googleapis.com" />
    <link rel="preconnect" href="https://fonts.gstatic.com"
crossorigin />

    <link

href="https://fonts.googleapis.com/css2?family=Quicksand:wght@300;
500;700&display=swap"
      rel="stylesheet"
    />
```

```
    <link

href="https://fonts.googleapis.com/css2?family=Material+Symbols+Ou
tlined"
      rel="stylesheet"
    />

    <title>Collecto</title>
    <script type="module" crossorigin
src="/assets/index-Cd4kMVDa.js"></script>
    <link rel="stylesheet" crossorigin
href="/assets/index-Dqo59u5u.css">
  </head>
  <body>
    <div id="root"></div>

  </body>
</html>
```

5.15.2 Recomendación

Los navegadores web modernos admiten las cabeceras HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que una de ellas esté configurada en todas las páginas web devueltas por su sitio/aplicación.

Si espera que la página esté marcada solo por páginas en su servidor (por ejemplo, si forma parte de un FRAMESET), utilice SAMEORIGIN; De lo contrario, si no espera que la página esté marcada, utilice DENY. Alternativamente, considere implementar la directiva "frame-ancestors" de la Política de Seguridad de Contenidos-

5.16 Hallazgo H-016: El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ''''X-Powered-By'''' (Medio)

Descripción:	El servidor de la web/aplicación está divulgando información mediante uno o más encabezados de respuesta HTTP ""X-Powered-By"". El acceso a tal información podría facilitarle a los atacantes la identificación de otros marcos/componentes de los que su aplicación web depende y las vulnerabilidades a las que pueden estar sujetos tales componentes.
Severidad:	Media
Riesgo:	Permite que el sitio web sea incrustado en un iframe por sitios externos, lo que lo hace vulnerable a ataques de clickjacking. En este tipo de ataque, un usuario puede ser engañado para hacer clic en elementos ocultos del sitio legítimo

	mientras cree que está interactuando con otro contenido, lo que puede llevar a acciones no deseadas, como cambios en configuraciones, compras no autorizadas o envío de información sensible, afectando la integridad de las acciones del usuario y la confianza en el sitio.
Sistema:	https://collecto.es/api/
Herramientas:	ZAP PROXY
Referencias:	■ OWASP_2021_A01 ■ WSTG-v42-INFO-08 ■ OWASP_2017_A03 ■ CWE-497

5.16.1 Evidencia

Request

Línea de solicitud y sección de encabezado (262 bytes)

```
GET https://collecto.es/api/ HTTP/1.1
host: collecto.es
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://collecto.es/api
```

Response

Línea de estado y sección de encabezado (775 bytes)

```
HTTP/1.1 404 Not Found
Date: Sun, 01 Jun 2025 19:46:08 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Server: cloudflare
Nel: {"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
X-Powered-By: Express
Access-Control-Allow-Origin: https://collecto.es
Vary: Origin
Vary: accept-encoding
Access-Control-Allow-Credentials: true
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Cf-Cache-Status: DYNAMIC
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.clo
udflare.com/report/v4?s=oKkR3iUOl95TM4rkL1QtYETKoJKfdDY5H%2Fr8DCbJTJcxyI1
WSlVEz%2FNfSLDlCt%2FekY2N1XGrCdbXACdx1RTVxps%2B7ypmAsOo%2FX3t"}]}
CF-RAY: 949137204aec1e3d-MIA
alt-svc: h3=":443"; ma=86400
content-length: 143
```

Cuerpo de la respuesta (143 bytes)

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>Cannot GET /api/</pre>
</body>
</html>
```

5.16.2 Recomendación

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para suprimir las cabeceras "X-Powered-By".

5.17 Hallazgo H-017: Falta encabezado X-Content-Type-Options (Media)

Descripción:	La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing. Este problema aún se aplica a las páginas de tipo error (401, 403, 500, etc.), ya que esas páginas a menudo se ven afectadas por problemas de inyección, en cuyo caso aún existe la preocupación de que los navegadores husmeen las páginas lejos de su tipo de contenido real. En el umbral «Alto» esta regla de análisis no alertará sobre respuestas de error del cliente o servidor.
Severidad:	Media
Riesgo:	Permite que ciertos navegadores, especialmente versiones antiguas de Internet Explorer y Chrome, realicen MIME-sniffing, lo que podría llevar a que interpreten

	archivos como un tipo de contenido distinto al declarado. Esto puede ser aprovechado por un atacante para ejecutar código malicioso en el navegador del usuario, especialmente si logra inyectar contenido en una página o respuesta de error, lo que representa un riesgo de ejecución de scripts no autorizados y de exposición a vulnerabilidades de tipo XSS o de descarga de archivos maliciosos disfrazados.
Sistema:	*https://collecto.es*
Herramientas:	ZAP PROXY
Referencias:	CVE-2011-2523

5.17.1 Evidencia

Request

Línea de solicitud y sección de encabezado (223 bytes)

```
GET https://collecto.es HTTP/1.1
host: collecto.es
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```

Response

Línea de estado y sección de encabezado (592 bytes)

```
HTTP/1.1 200 OK
Date: Sun, 01 Jun 2025 19:46:06 GMT
Content-Type: text/html
Connection: keep-alive
Server: cloudflare
Last-Modified: Thu, 08 May 2025 17:54:30 GMT
Nel:
{"report_to":"cf-nel","success_fraction":0.0,"max_age":604800}
Report-To:
{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.
nel.cloudflare.com/report/v4?s=Kq5SpwSBUHtXPgUxfzXXaCl0zCG3ly7Dni9
YV0r%2BT%2FNzHq0BKYFAE9haDDcK9stOE7kuExZhwN%2BA3dzaThgUHnNnFm%2BEz
PHWwexk"}]}
Vary: accept-encoding
Cf-Cache-Status: DYNAMIC
CF-RAY: 94913714dc9fb7f2-MIA
alt-svc: h3=":443"; ma=86400
content-length: 890
```

Cuerpo de la respuesta (890 bytes)

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" type="image/svg+xml"
href="/collecto-favicon.png" />
    <meta name="viewport" content="width=device-width,
initial-scale=1.0" />

    <link rel="preconnect" href="https://fonts.googleapis.com" />
    <link rel="preconnect" href="https://fonts.gstatic.com"
crossorigin />

    <link

href="https://fonts.googleapis.com/css2?family=Quicksand:wght@300;
500;700&display=swap"
      rel="stylesheet"
    />
    <link

href="https://fonts.googleapis.com/css2?family=Material+Symbols+Ou
tlined"
      rel="stylesheet"
    />

    <title>Collecto</title>
    <script type="module" crossorigin
src="/assets/index-Cd4kMVDa.js"></script>
    <link rel="stylesheet" crossorigin
href="/assets/index-Dqo59u5u.css">
  </head>
  <body>
    <div id="root"></div>

  </body>
</html>
```

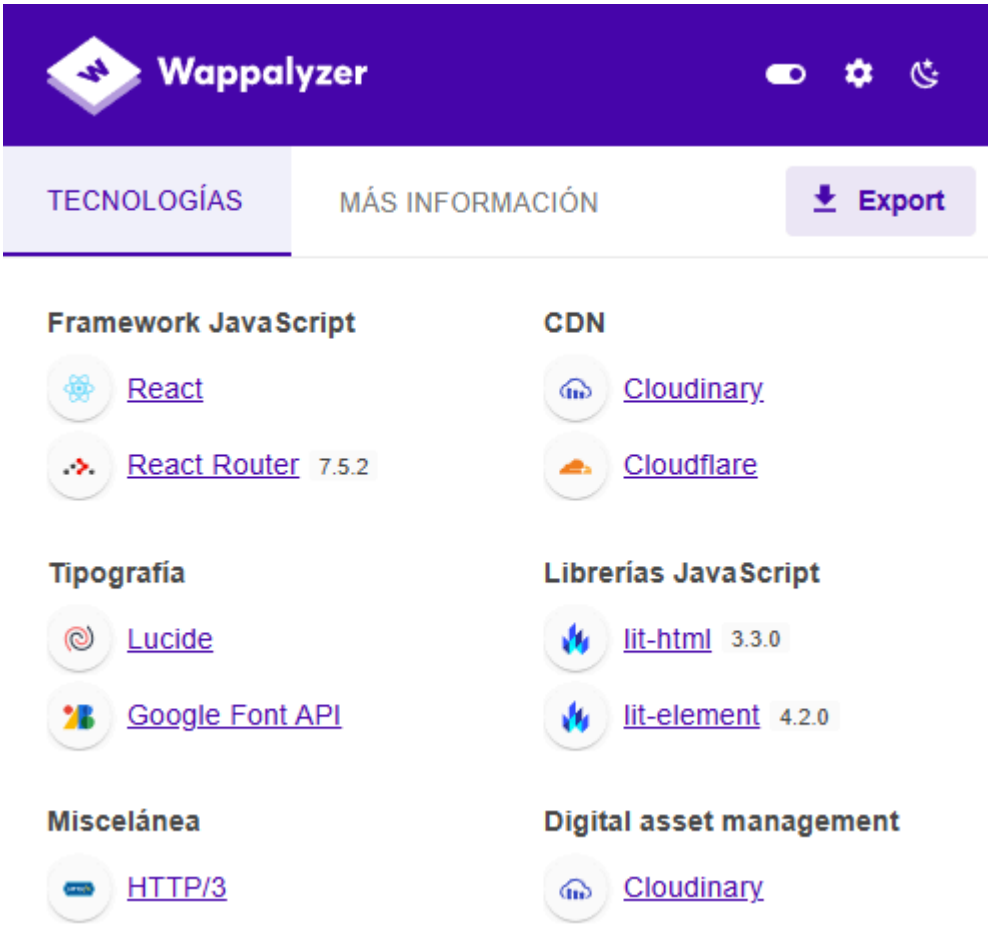
PARAMETRO: `x-content-type-options`

5.17.2 Recomendación

Asegúrese de que la aplicación/servidor web establece el encabezado Content-Type adecuadamente, y que establece el encabezado X-Content-Type-Options a 'nosniff' para todas las páginas web.

Si es posible, asegúrese de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realizan MIME-sniffing en absoluto, o que puede ser dirigido por la aplicación web/servidor web para que no realice MIME-sniffing.

6. Información



Fondo

Título del sitio	Coleccionista

Clasificación del sitio	No presente
Descripción	No presente
Fecha de primera visita	Junio de 2025
Idioma principal	Inglés

Red

Sitio	**https://collecto.es**
Propietario de Netblock	**Cloudflare, Inc.**
Empresa de hosting	Cloudflare
País anfitrión	**A NOSOTROS**
Dirección IPv4	104.21.64.1 (**Virus Total**)
Sistemas autónomos IPv4	**AS13335**
Dirección IPv6	2606:4700:3030:0:0:0:6815:7001
Sistemas autónomos IPv6	**AS13335**
DNS inverso	Desconocido
Dominio	**collecto.es**

Servidor de nombres	jarred.ns.cloudflare.com
Registrador de dominios	Desconocido
Organización del servidor de nombres	whois.cloudflare.com
Organización	Desconocido
Administrador de DNS	dns@cloudflare.com
Dominio de nivel superior	España (.es)
Extensiones de seguridad de DNS	Activado

Delegación de propiedad intelectual

SSL/TLS

Garantía	Validación de dominio
Nombre común	collecto.es
Organización	No presente
Estado	No presente
País	No presente
Unidad organizativa	No presente

Nombre alternativo del sujeto	**collecto.es** , *.collecto.es
Periodo de validez	Del 6 de mayo de 2025 al 4 de agosto de 2025 (2 meses, 4 semanas, 1 día)
Coincide con el nombre del host	Sí
Servidor	nube de llamas
Algoritmo de clave pública	id-ecPublicKey
Versión del protocolo	TLSv1.3
Longitud de la clave pública	256
Comprobación del certificado	OK
Algoritmo de firma	ecdsa-con-SHA256
Número de serie	0x5c0e037b5f3476971335753295f6fe58
Cifrar	TLS_AES_256_GCM_SHA384
Número de versión	0x02
Secreto perfecto hacia adelante	Sí
Extensiones TLS compatibles	Compartir clave **RFC8446** , versiones compatibles **con RFC8446 , nombre de servidor RFC4366** , negociación de protocolo de capa de aplicación **RFC7301** , solicitud de estado **RFC4366**

Negociación de protocolos de capa de aplicación	h2
Próxima negociación del protocolo	No presente
Organismo emisor	Servicios de confianza de Google
Nombre común del emisor	WE1
Unidad emisora	No presente
Ubicación del emisor	No presente
País emisor	A NOSOTROS
Estado del emisor	No presente
Listas de revocación de certificados	http://c.pki.goog/we1/fJedmL2peto.crl
Hash del certificado	9H6v0qKP9TT7tzq3p9GwPG6Xz0c
Hash de clave pública	db74c11098236f873eb68d68ab97d0b65646982f963bd878dd5c79b634512f9a
Servidores OCSP	http://o.pki.goog/s/we1/XA4
Respuesta de grapado de OCSP	Certificado válido
Datos OCSP generados	5 de junio de 2025, 12:51:21 GMT

Los datos de OCSP expiran	12 de junio de 2025, 11:51:20 GMT

Transparencia del certificado

Marcas de tiempo de certificados firmados (SCT)

Fuente	Registro	Marca de tiempo	Verificación de firma
Certificado	*Desconocido* zPsPaoVxCWX+lZtTzumyfCLphVwNl422qX5UwP5MDbA=	06/05/2025 08:12:21	*Desconocido*
Certificado	*Desconocido* EvFONL1TckyEBhnDjz96E/jntWKHiJxtMAWE6+WGJjo=	06/05/2025 08:12:21	*Desconocido*

SSLv3/CANICHE

Este sitio no admite el protocolo SSL versión 3.

Tecnología del sitio (obtenido 10/06/2025)

Acelerador HTTP

Un acelerador web es un servidor proxy que reduce los tiempos de acceso a los sitios web.

Tecnología	Descripción	Sitios populares que utilizan esta tecnología
Cloudflare	Red de distribución de contenido y servicio de servidor de	**www.perplexity.ai** , **erp.fxpro.com** , **stackoverflow.com**

	nombres de dominio distribuido

Lado del cliente

Incluye todas las tecnologías principales que se ejecutan en el navegador (como JavaScript y Adobe Flash).

Tecnología	Descripción	Sitios populares que utilizan esta tecnología
JavaScript	Lenguaje de programación ampliamente compatible que se utiliza comúnmente para impulsar contenido dinámico del lado del cliente en sitios web.	**www.netflix.com** , **www.linkedin.com** , **www.amazon.com**

Red de distribución de contenido

Una red de entrega de contenido (CDN) es un gran sistema distribuido de servidores implementados en múltiples centros de datos en Internet. El objetivo de una CDN es ofrecer contenido a los usuarios finales con alta disponibilidad y alto rendimiento.

Tecnología	Descripción	Sitios populares que utilizan esta tecnología
Cloudflare	Red de distribución de contenido y servicio de servidor de nombres de dominio distribuido	auth.openai.com , chat.deepseek.com

Codificación de caracteres

Un sistema de codificación de caracteres consiste en un código que empareja cada carácter de un repertorio dado con algo más, como un patrón de bits, una secuencia de números naturales, octetos o pulsos eléctricos, para facilitar la transmisión de datos (generalmente números o texto) a través de redes de telecomunicaciones o para el almacenamiento de datos.

Tecnología	Descripción	Sitios populares que utilizan esta tecnología
UTF8	Formato de transformación UCS de 8 bits	correo web.vinccihoteles.com

Compresión HTTP

La compresión HTTP es una capacidad que se puede incorporar en servidores web y clientes web para hacer un mejor uso del ancho de banda disponible y proporcionar mayores velocidades de transmisión entre ambos.

Tecnología	Descripción	Sitios populares que utilizan esta tecnología

Codificación de contenido Gzip	Protocolo de compresión HTTP Gzip	www.amazon.co.jp , www.amazon.com.mx , www.jobthai.com

Tipo de documento

Una declaración de tipo de documento, o DOCTYPE, es una instrucción que asocia un documento SGML o XML particular (por ejemplo, una página web) con una definición de tipo de documento (DTD).

Tecnología	Descripción	Sitios populares que utilizan esta tecnología
HTML5	Última revisión del estándar HTML, el principal lenguaje de marcado en la web	www.google.com , campus-1001.ammon.cloud , translate.google.com

HTML 5

HTML5 es un lenguaje de marcado para estructurar y presentar contenido para la World Wide Web y una tecnología fundamental de Internet. Es la quinta revisión del estándar HTML.

Tecnología	Descripción	Sitios populares que utilizan esta tecnología
Etiqueta meta de la ventana gráfica	Etiqueta HTML5 que se utiliza habitualmente para la optimización móvil	www.deepl.com , www.canva.com , t.corp.amazon.com

Uso de CSS

Hojas de estilo en cascada (CSS) es un lenguaje de hojas de estilo utilizado para describir la semántica de presentación (el aspecto y el formato) de un documento escrito en un lenguaje de marcado (como XHTML).

Tecnología	Descripción	Sitios populares que utilizan esta tecnología
Externo	Estilos definidos dentro de un archivo CSS externo	www.twitch.tv , chatgpt.com , discord.com

7. Descubrimiento

Puertos abiertos

Deben estar abiertos el puerto 80 y 443, no se han podido hallar más ya que está protegido por cloudflare.

Sistema Operativo

El sistema operativo encontrado fue nginx/1.24.0 (Ubuntu)

---

8. Herramientas Utilizadas

- Zap Proxy
- Sqlmap: Se utilizó para revisar las rutas del sitio
- dirb: Se utilizó para enumerar los directorios.
- Nmap: Se utilizó para la enumeración de puertos y proceso de extracción de la información del sistema operativo
- Burp proxy: Capturas de tráfico y modificación de los request al servidor

- Hydra: ataques de fuerza bruta
- Greenbone Security Assistant Version 23.3 (Antes OpenVas)
- Metasploit 6.4.45: Framework
- NetDiscover: Exploración de equipos en la red kali
