Informe de Pruebas de Penetración - Análisis de Código Dinámico (DAST)

Informe Ejecutivo

Alcance

Se realizó un análisis dinámico de seguridad mediante herramientas de escaneo automatizado (ZAP - Zed Attack Proxy) sobre los siguientes activos:

- https://www.ecuconsult.net
- https://firefox.settings.services.mozilla.com
- https://firefox-settings-attachments.cdn.mozilla.net

Versión de herramienta: ZAP 2.17.0 by Checkmarx.

Metodología

El análisis se ejecutó mediante técnicas de escaneo dinámico pasivo, permitiendo la detección de:

- Configuraciones inseguras de encabezados HTTP.
- Políticas de seguridad del navegador no configuradas.
- Divulgación de información sensible.
- Deficiencias en mecanismos de protección contra ataques web.
- Prácticas inadecuadas de control de caché.

La evaluación no incluye pruebas activas de explotación ni modificación de datos en sistemas objetivo.

Estadística de Activos

Distribución de vulnerabilidades por sitio y nivel de riesgo

Sitio Evaluado	Riesgo Alto	Riesgo Medio	Riesgo Bajo	Informativo
https://www.ecuconsult.net	0	3	2	4

https://firefox-settings-attachments.cdn.mozilla.net	0	0	1	0
TOTALES	**0**	**3**	**3**	**4**

Resumen General:

- Total de vulnerabilidades identificadas: 10
- Vulnerabilidades críticas (Alto riesgo): 0 (0%)
- Vulnerabilidades medias (Riesgo Medio): 3 (30%)
- Vulnerabilidades bajas (Riesgo Bajo): 3 (30%)
- Hallazgos informativos: 4 (40%)

Informe Técnico

Detalle de Activos Analizados

Se evaluaron 3 dominios principales con énfasis en la aplicación web principal (https://www.ecuconsult.net), que fue objeto de 9 de las 10 vulnerabilidades detectadas, indicando una superficie de ataque significativa en el servidor principal.

Identificadores de Vulnerabilidades Críticas

Vulnerabilidades de Riesgo Medio

1. Cabecera Content Security Policy (CSP) no configurada

- **Identificador:** CSP-001
- **Severidad:** Media (10% de confianza Alta)
- **Ubicación:** https://www.ecuconsult.net
- **CWE ID:** 693
- **WASC ID:** 15

- **Descripción:** La política de seguridad de contenido (CSP) no está configurada, lo que permite potenciales ataques de inyección de scripts maliciosos. Sin CSP, los atacantes pueden ejecutar código JavaScript no autorizado en el contexto de la aplicación web [1].
- **Vector de Ataque:** Inyección de contenido malicioso mediante parámetros de entrada no validados.
- **Mecanismo de Contingencia:** Implementar encabezado CSP con directivas restrictivas tales como: `Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self'.`

2. Configuración Incorrecta Cross-Domain (CORS)

- **Identificador:** CORS-001
- **Severidad:** Media (20% de confianza Media)
- **Ubicación:** https://www.ecuconsult.net
- **CWE ID:** 264
- **WASC ID:** 14
- **Descripción:** La política de intercambio de recursos entre orígenes (CORS) está permisivamente configurada, permitiendo que dominios externos accedan a recursos restringidos. Esto puede facilitar ataques de falsificación de solicitudes entre sitios (CSRF) y acceso no autorizado a datos sensibles [1].
- **Vector de Ataque:** Solicitud de recursos desde origen malicioso aprovechando permisos CORS permisivos.
- **Mecanismo de Contingencia:** Restringir CORS a dominios específicos y confiables mediante configuración del encabezado `Access-Control-Allow-Origin.`

3. Falta de Cabecera Anti-Clickjacking

- **Identificador:** XFO-001

- **Severidad:** Media (30% de confianza Media)
- **Ubicación:** https://www.ecuconsult.net
- **CWE ID:** 1021
- **WASC ID:** 15
- **Descripción:** El encabezado X-Frame-Options no está presente, dejando la aplicación vulnerable a ataques de clickjacking donde un atacante puede incrustar la página en un iframe malicioso y engañar a usuarios para que realicen acciones no autorizadas [1].
- **Vector de Ataque:** Incrustar la aplicación web en un iframe dentro de un sitio malicioso, ocultando la interfaz real bajo una falsa interfaz.
- **Mecanismo de Contingencia:** Configurar encabezado `X-Frame-Options: DENY` o `X-Frame-Options: SAMEORIGIN` según requisitos de la aplicación.

Vulnerabilidades de Riesgo Bajo

4. Divulgación de Marcas de Tiempo - Unix

- **Identificador:** TS-001
- **Severidad:** Baja (40% de confianza Baja)
- **Ubicación:** https://firefox-settings-attachments.cdn.mozilla.net
- **CWE ID:** 497
- **WASC ID:** 13
- **Descripción:** Se detectó exposición de marcas de tiempo Unix en respuestas del servidor. Aunque tiene bajo impacto directo, puede proporcionar información útil a atacantes para sincronización de ataques y análisis de comportamiento del sistema [2].
- **Vector de Ataque:** Análisis de metadatos temporales para coordinar ataques.
- **Mecanismo de Contingencia:** Revisar y minimizar información de metadatos en respuestas HTTP.

5. Falta encabezado X-Content-Type-Options

- **Identificador:** XCT-001
- **Severidad:** Baja (10% de confianza Media)
- **Ubicación:** https://www.ecuconsult.net
- **CWE ID:** 693
- **WASC ID:** 15
- **Descripción:** El encabezado X-Content-Type-Options no está configurado, permitiendo que navegadores realicen "MIME sniffing". Los atacantes pueden servir archivos con tipo MIME incorrecto (ej: JavaScript como imagen) que el navegador interpretará como código ejecutable [2].
- **Vector de Ataque:** Carga de archivos con MIME type alterado para ejecutar código malicioso.
- **Mecanismo de Contingencia:** Configurar encabezado `X-Content-Type-Options: nosniff` en todas las respuestas HTTP.

6. Encabezado de Seguridad de Transporte Estricto No Establecido

- **Identificador:** HSTS-001
- **Severidad:** Baja (60% de confianza Alta)
- **Ubicación:** https://www.ecuconsult.net/robots.txt
- **CWE ID:** 319
- **WASC ID:** 15
- **Descripción:** HSTS (HTTP Strict Transport Security) no está habilitado. Sin este mecanismo, usuarios pueden ser redirigidos a versiones inseguras HTTP, exponiéndose a ataques de intermediarios (MITM) que intercepten tráfico no cifrado [2].
- **Vector de Ataque:** Intercepcción de tráfico no cifrado mediante técnicas de downgrade attack o ataques MITM.
- **Mecanismo de Contingencia:** Implementar encabezado `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`.

Hallazgos Informativos

Aplicación Web Moderna: Detectada arquitectura de aplicación web moderna, indicando uso de tecnologías contemporáneas.

Divulgación de Información en Comentarios: Se identificaron comentarios sospechosos en el código fuente (archivo /assets/index-BsTb9iap.js).

Control de Caché Inadecuado: La aplicación no implementa directivas de control de caché suficientemente restrictivas, permitiendo que contenido sensible se recupere desde memoria caché [3].

Conclusión

Se identificaron 3 vulnerabilidades de riesgo medio y 3 vulnerabilidades de riesgo bajo, ninguna de severidad crítica. Aunque no se detectaron vulnerabilidades de alto riesgo, las deficiencias en configuración de encabezados de seguridad requieren atención para fortalecer la postura defensiva de la aplicación web. La implementación de las recomendaciones propuestas reducirá significativamente la superficie de ataque y mejorará la protección contra vectores de ataque comunes.

Referencias

[1] OWASP. *Content Security Policy Cheat Sheet*. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

[2] Mozilla Developer Network. (2024*). HTTP Security Headers*. https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers

[3] IETF. (2020). *RFC 7234 - HTTP Caching*. https://datatracker.ietf.org/doc/html/rfc7234