

Informe Análisis dinámico (DAST)

1. Ejecutivo

El análisis dinámico de seguridad identificó un total de 10 alertas. No se encontraron vulnerabilidades de riesgo "Alto". Aunque el número total de riesgos se mantiene estable respecto al reporte previo, se observa una mayor visibilidad de vulnerabilidades debido a una mejora significativa en la respuesta del servidor. El resumen de criticidad es el siguiente:

- **Riesgo Medio:** 3 alertas (30% del total).
- **Riesgo Bajo:** 3 alertas (30% del total).
- **Informativo:** 4 alertas (40% del total).

La superficie de ataque principal presenta debilidades en la configuración de encabezados de seguridad, lo que podría facilitar ataques de manipulación de contenido o interceptación de datos si no se corrigen.

2. Alcance

El escaneo se limitó a los siguientes activos:

- <https://www.ecuconsult.net>
- <https://firefox-settings-attachments.cdn.mozilla.net>

3. Metodología

Se utilizó la herramienta OWASP ZAP versión 2.17.0. El proceso consistió en un análisis DAST (Dynamic Application Security Testing) mediante el uso de escaneos pasivos para identificar configuraciones incorrectas en los encabezados de respuesta y posibles divulgaciones de información en los activos analizados.

- **Mejora en la conectividad:** La tasa de respuestas exitosas (status code 2xx) aumentó del 6% al 54%.
- **Reducción de redirecciones:** Las respuestas 3xx disminuyeron del 88% al 37%.
- **Rendimiento:** El 92% de las respuestas fueron catalogadas como lentas.

4. Estadísticas Activos

Distribución de alertas por sitio y nivel de riesgo:

Sitio	Medio	Bajo	Informativo	Total
www.ecuconsult.net	3	2	4	9
mozilla.net (CDN)	0	1	0	1

5. Informe Técnico

A continuación, se detallan los hallazgos con un incremento en la frecuencia de detección por tipo de alerta:

Activo	Vuln ID (CWE)	Descripción	Severidad	Frecuencia (Conteo)	Contingencia
www.ecuconsult.net	693	Content Security Policy (CSP) no configurada	Medio	3	Definir política CSP estricta.
www.ecuconsult.net	264	Configuración Incorrecta Cross-Domain	Medio	5	Restringir el acceso CORS.
www.ecuconsult.net	1021	Falta de cabecera Anti-Clickjacking	Medio	3	Configurar X-Frame-Options.
www.ecuconsult.net	693	Falta encabezado X-Content-Type-Options	Bajo	8	Añadir directiva nosniff.
www.ecuconsult.net	319	HSTS No Establecido	Bajo	5	Forzar HTTPS vía HSTS.

mozilla.net	497	Divulgación de Marcas de Tiempo - Unix	Bajo	3	Ofuscar marcas de tiempo.
www.ecuconsult.net	615	Comentarios sospechosos en JS	Info	1	Limpiar código en producción.
www.ecuconsult.net	525	Reexaminar Directivas de Control de Caché	Info	7	Optimizar headers de caché.