

Resumen de Resultados de Pruebas

SISTEMA GASOLINERA

Fecha de creación	25/10/2025
Analista de aseguramiento de calidad	María José Véliz Ochoa

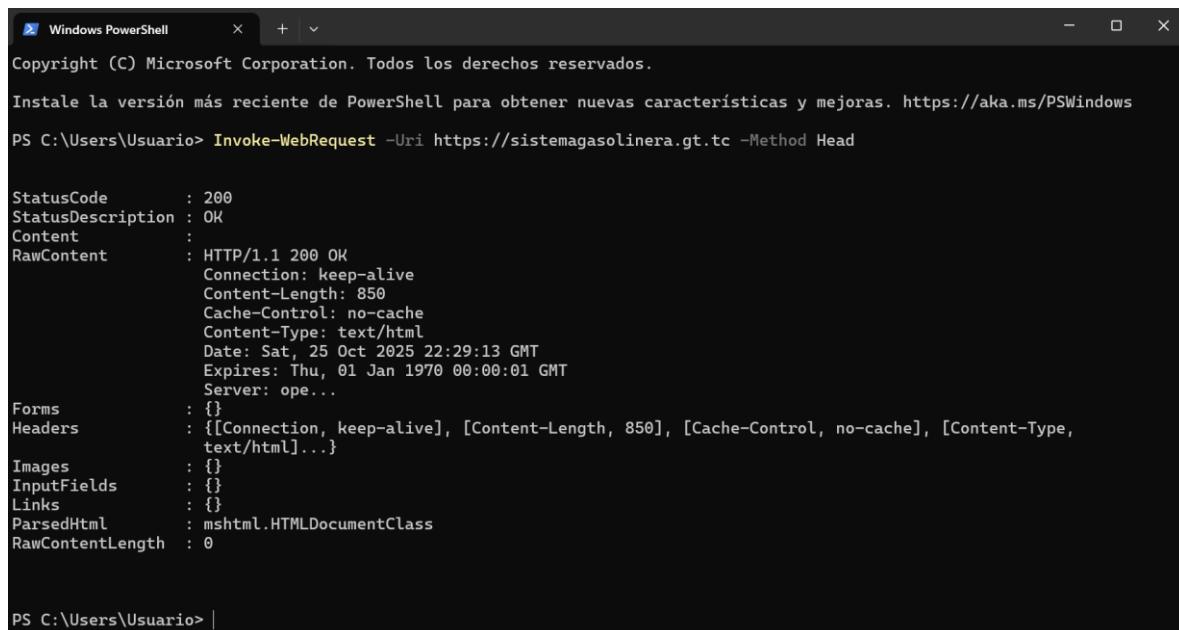
Análisis De Pruebas De Seguridad

1. Escaneo del sistema.

Verificación de disponibilidad del sitio mediante PowerShell: Se ejecutó el siguiente comando en PowerShell para comprobar el estado del servidor y la accesibilidad del dominio antes del análisis:

```
Invoke-WebRequest -Uri https://sistemagasolinera.gt.tc -Method Head
```

El comando devolvió un StatusCode 200, lo que confirma que el servidor responde correctamente y está en línea. Se visualizaron también los encabezados HTTP del sitio, tales como Content-Type, Cache-Control, y Connection.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.
Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows
PS C:\Users\Usuario> Invoke-WebRequest -Uri https://sistemagasolinera.gt.tc -Method Head

StatusCode        : 200
StatusDescription : OK
Content          :
RawContent       : HTTP/1.1 200 OK
                  Connection: keep-alive
                  Content-Length: 850
                  Cache-Control: no-cache
                  Content-Type: text/html
                  Date: Sat, 25 Oct 2025 22:29:13 GMT
                  Expires: Thu, 01 Jan 1970 00:00:01 GMT
                  Server: ope...
Forms            : {}
Headers          : {[Connection, keep-alive], [Content-Length, 850], [Cache-Control, no-cache], [Content-Type, text/html]...}
Images           : {}
InputFields      : {}
Links            : {}
ParsedHtml       : mshtml.HTMLDocumentClass
RawContentLength : 0

PS C:\Users\Usuario> |
```

Inicio del escáner OWASP ZAP: Se abrió la herramienta OWASP ZAP 2.16.1, seleccionando la opción “Escaneo Automático” para iniciar una nueva sesión de análisis. En esta etapa, se validó que la interfaz se encontrara lista para realizar el escaneo sobre la aplicación web seleccionada.

The screenshot shows the ZAP 2.16.1 interface. The top menu bar includes Archivo, Editar, Ver, Analizar, Informe, Herramientas, Importar, Exportar, En línea, and Ayuda. The title bar says "Sesión sin Nombre - Prueba@seguridad - ZAP 2.16.1". The left sidebar has sections for Sitios, Contextos (with "Contenido predeterminado" selected), and Sitios. The main content area features a "Bienvenido a ZAP" header, a brief introduction about ZAP being an integrated penetration testing tool, and three buttons: "Escáner Automatiz.", "Exploración Manual", and "Saber Más". Below this is a "Noticias" section with a link to "ZAP 2.16.1 is available now" and a "Saber Más" button. At the bottom, there's a table with columns: ID, Fuente, Petición (Tiempo), Método, URL, Código, Razón, RTT, Respuesta (Tamaño del cuerpo), Alerta mayor, Nota, and Etiquetas. A filter bar at the bottom left says "Filtro: APAGADO" and "Exportar".

Configuración de exploración manual: Desde la ventana de Exploración Manual, se ingresó la URL del sistema (<https://sistemasgasolinera.gt.tc>) en el campo “URL a explorar”. Se habilitó la opción HUD (Heads Up Display) para visualizar las alertas directamente desde el navegador durante el recorrido de la aplicación.

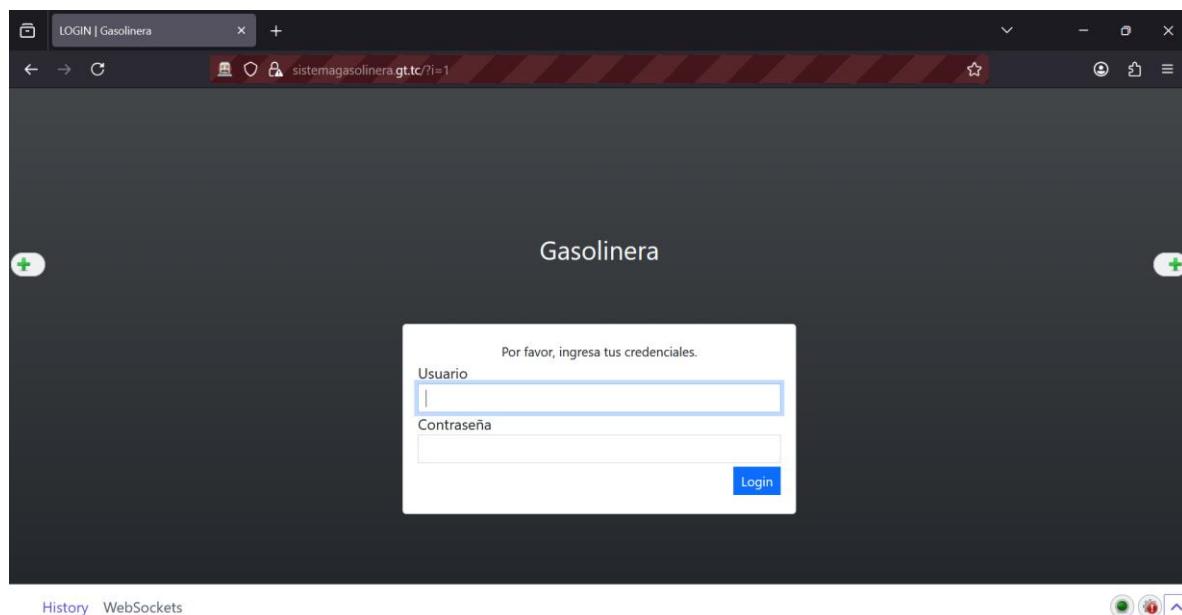
El navegador configurado fue Firefox, iniciado desde la interfaz de ZAP. Se muestra la URL registrada y lista para el proceso de exploración y recolección de posibles vulnerabilidades.

Prueba de navegación y autenticación: ZAP abrió el sitio en modo exploración. En el navegador, se visualizó la página de inicio de sesión del sistema “Gasolinera”, donde el usuario debe ingresar credenciales.

Durante esta fase, ZAP analizó los formularios, las peticiones y las cabeceras HTTP para identificar fallos potenciales, como:

- Transmisión de credenciales sin cifrado HTTPS
- Formularios vulnerables a inyección de código
- Falta de validación en campos de usuario o contraseña

Se observa la interfaz del sistema con el formulario de inicio de sesión, bajo el monitoreo activo de ZAP.



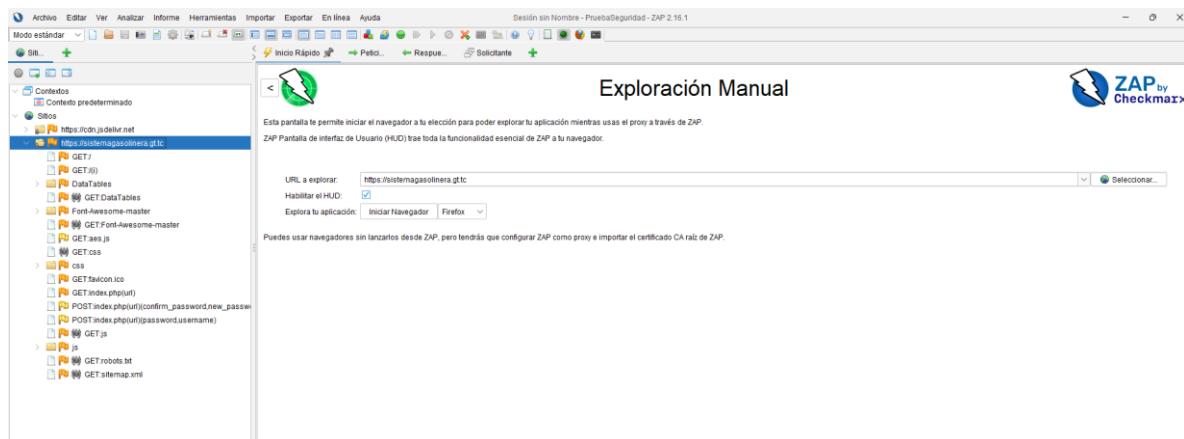
2. Resultados del escaneo de seguridad

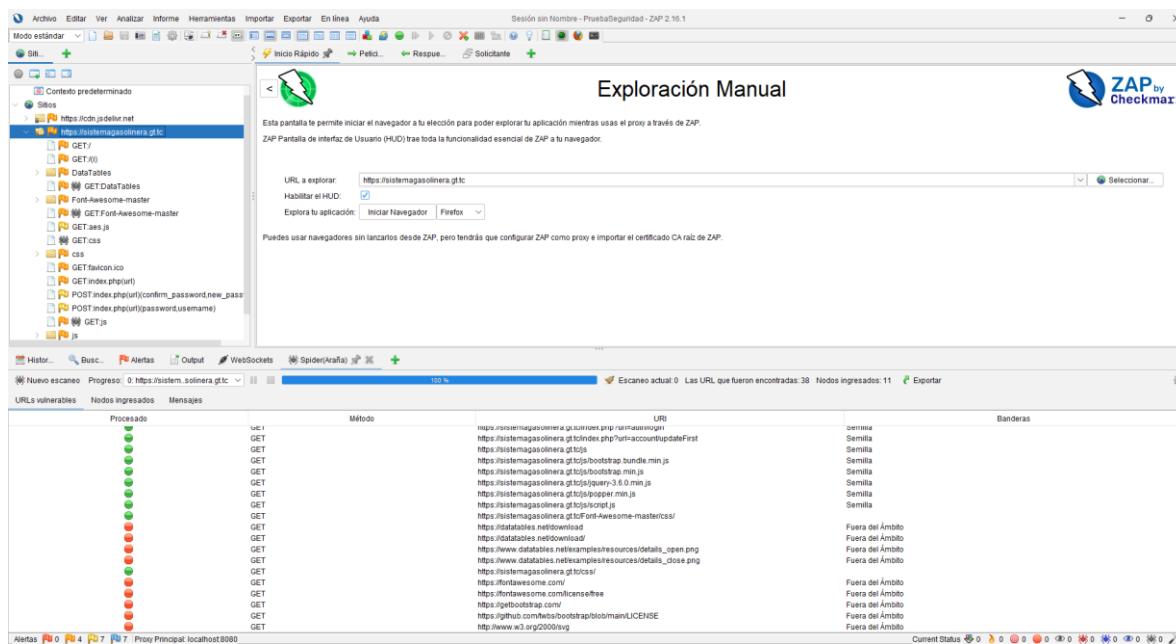
Después de la configuración inicial del entorno, se procedió con la exploración manual y el escaneo completo del sitio <https://sistemagasolinera.gt.tc> mediante OWASP ZAP. El sistema respondió correctamente a las solicitudes, y el análisis permitió identificar diversos puntos de atención clasificados por nivel de riesgo.

Ejecución del escaneo: Se inició la exploración del dominio principal, donde OWASP ZAP analizó los recursos disponibles (GET, POST, PUT) y generó una lista de URLs procesadas. Durante el análisis, la herramienta detectó 11 nodos ingresados y múltiples rutas internas del sistema (formularios, scripts, y cabeceras de sesión).

Descripción técnica:

- Modo: Exploración manual
- URL escaneada: <https://sistemagasolinera.gt.tc>
- Tipo de métodos analizados: GET, POST
- Total de peticiones procesadas: 23
- Alertas detectadas: 18





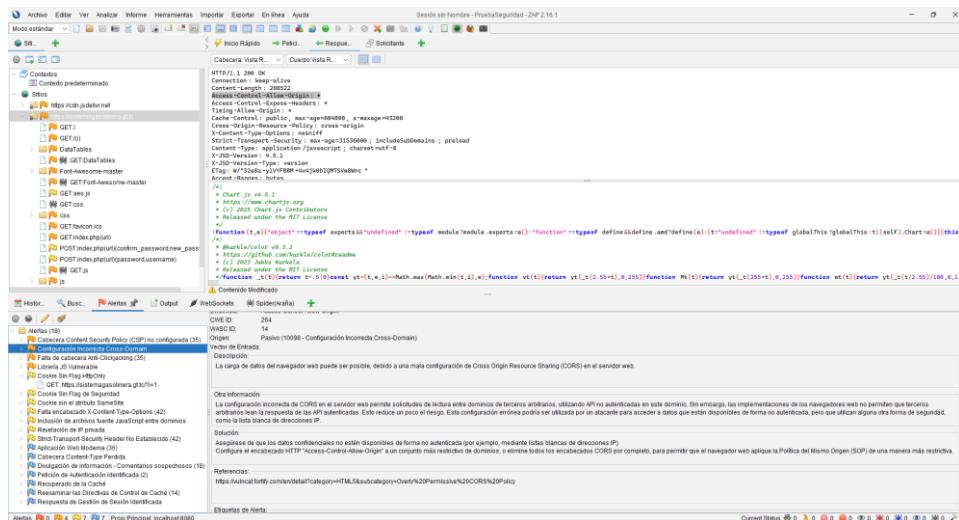
Identificación de vulnerabilidades: OWASP ZAP detectó las siguientes vulnerabilidades durante el análisis de cabeceras y contenido HTML:

Nivel	Tipo de vulnerabilidad	Descripción	Estado
Media	Falta de cabecera de política de seguridad de contenido (CSP)	El servidor no establece la cabecera Content-Security-Policy, lo que permite ataques XSS o inyección de scripts externos.	Pendiente
Media	Configuración incorrecta de política CORS (Cross-Origin Resource Sharing)	Permite que recursos externos accedan a datos del sistema, exponiendo información a dominios no autorizados.	Pendiente
Baja	Cookie sin atributo HttpOnly	Las cookies pueden ser accedidas por JavaScript, lo que representa riesgo ante ataques XSS o robo de sesión.	Pendiente
Baja	Falta de cabeceras complementarias (X-Frame-Options, X-Content-Type-Options)	Aumenta la exposición del sitio a ataques de clickjacking o MIME sniffing.	Observación

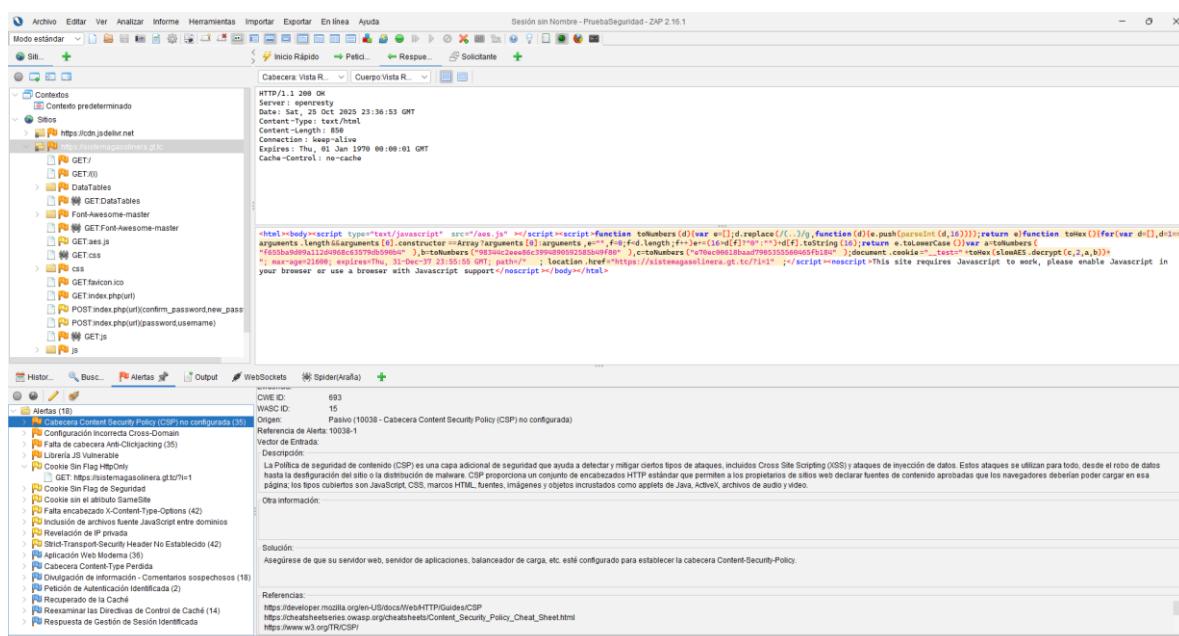
Análisis detallado de alertas:

- a. **Configuración incorrecta CORS:** ZAP detectó que el servidor no restringe adecuadamente los orígenes permitidos, lo cual podría permitir a otros dominios acceder a recursos internos.

El mensaje de alerta indica riesgo Cross-Domain Configuration Error (10098) con nivel Alto.



- b. Falta de Content-Security-Policy (CSP):** El sitio carece de la cabecera Content-Security-Policy, necesaria para proteger contra ataques de inyección de scripts. ZAP recomienda configurar esta cabecera desde el servidor o entorno de despliegue.



- c. **Cookie sin atributo HttpOnly:** Las cookies analizadas no contienen el atributo HttpOnly, permitiendo que scripts maliciosos puedan acceder a las sesiones activas.

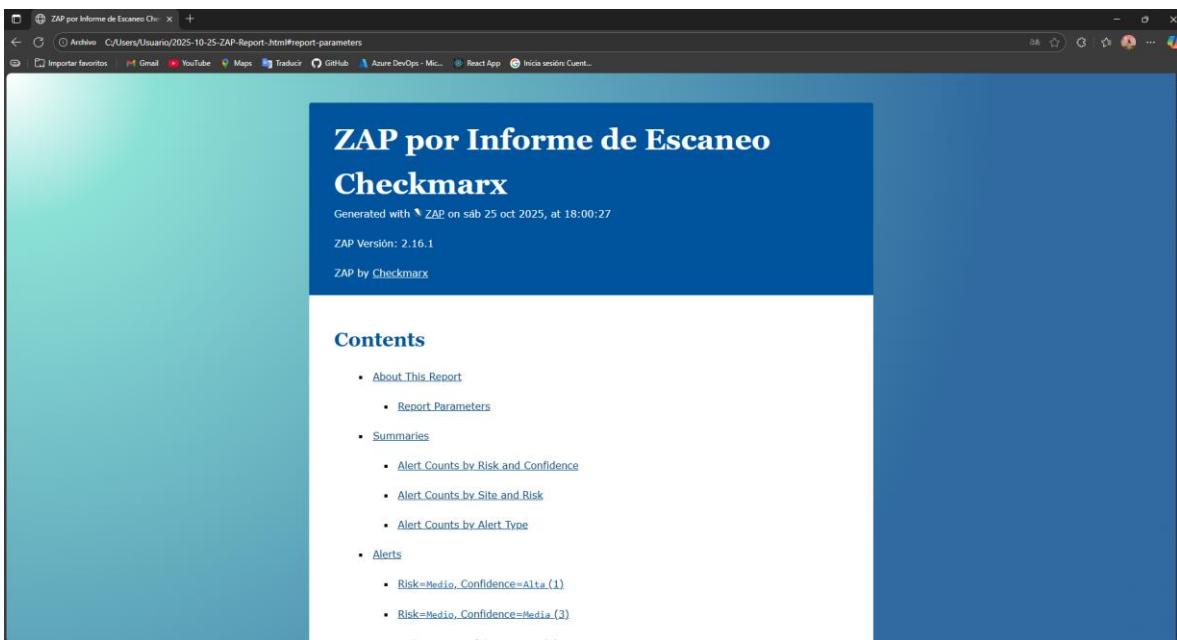
The screenshot shows the OWASP ZAP interface with the 'Alerts' tab active. There are 18 alerts listed. One alert is detailed, showing it's a 'Cookie Sin Flag HttpOnly' issue (Passive, 10010 - Cookie Sin Flag HttpOnly) with CWE ID 100 and WASC ID 13. It describes a cookie being set with the HttpOnly flag, which allows JavaScript to access the cookie. The 'Solutions' section suggests ensuring the flag is set for all cookies.

Evaluación general e informe: El panel de alertas de ZAP muestra un total de **18 alertas**, clasificadas de la siguiente forma:

- **4 Medias**
- **14 Bajas o informativas**

Resumen técnico:

- Escaneo ejecutado con proxy local (localhost:8080)
- Exploración manual con navegador Firefox
- OWASP ZAP versión: 2.16.1
- Estado final: Escaneo completado con éxito



LINK AL VIDEO PRUEBAS DE SEGURIDAD:

https://drive.google.com/file/d/1i6LQ5alq1axMyXPDP7ROBktF5jmkj6n-/view?usp=drive_link

LINK DEL REPORTE:

https://drive.google.com/file/d/1goh1Uxb4GxOaFFJGo_H-FHqiyI5AXCB2/view?usp=drive_link