

*Capstone: Fase 2*

*–* *Pruebas de Vulnerabilidad, proyecto:*

“Delicias Caseras”

*Alumnos:*

* Patrick Fraga Larraín.
* Christopher Fraga Larraín.
* Diego Fernández Fuentes

*Profesor:* Luis Alberto Bravo Yanes.

*Asignatura: Capstone.*

*Sección:* PTY4614.

**Resumen del Proyecto**

El proyecto "Delicias Caseras" es una aplicación web desarrollada con Django y utiliza MySQL como base de datos. Este informe presenta los resultados de las pruebas de vulnerabilidad realizadas utilizando OWASP ZAP.

**Resultados de las Pruebas de Vulnerabilidad**

**Resumen de Alertas**

A continuación, se presenta un resumen del conteo de alertas por nivel de riesgo y confianza:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Confianza** | **Alto** | **Medio** | **Bajo** | **Total** |
| **Riesgo** |  |  |  |  |
| **Alto** | 0 | 0 | 0 | 0 |
| **Medio** | 0 | 1 | 0 | 1 |
| **Bajo** | 0 | 1 | 1 | 2 |
| **Informativo** | 0 | 0 | 2 | 3 |
| **Total** | 0 | 2 | 3 | 6 |

**Alertas por Sitio y Riesgo**

Las alertas se distribuyen de la siguiente manera para el sitio http://127.0.0.1:8000:

| **Riesgo** | **Alto** | **Medio** | **Bajo** | **Informativo** |
| --- | --- | --- | --- | --- |
| http://127.0.0.1:8000 | 0 | 1 | 2 | 3 |

**Detalle de Alertas**

A continuación, se presenta el conteo de alertas por tipo:

| **Tipo de Alerta** | **Riesgo** | **Conteo** |
| --- | --- | --- |
| Cabecera Content Security Policy (CSP) no configurada | Medio | 8 |
| Cookie Sin Flag HttpOnly | Bajo | 5 |
| El servidor filtra información de versión | Bajo | 10 |
| Petición de Autenticación Identificada | Informativo | 4 |
| Respuesta de Gestión de Sesión Identificada | Informativo | 7 |
| User Agent Fuzzer | Informativo | 12 |
| **Total** |  | **6** |

**Alertas Específicas**

1. **Cabecera Content Security Policy (CSP) no configurada**
   * **Riesgo:** Medio
   * **Confianza:** Alta
   * **Descripción:** La política de seguridad de contenido no está configurada, lo que puede permitir ataques de XSS.
   * **URL:** GET http://127.0.0.1:8000/robots.txt
2. **El servidor filtra información de versión**
   * **Riesgo:** Bajo
   * **Confianza:** Alta
   * **Descripción:** El servidor expone información sobre su versión, lo que puede ser aprovechado por atacantes.
   * **URL:** GET http://127.0.0.1:8000/media/platos/logo2.png
3. **Cookie Sin Flag HttpOnly**
   * **Riesgo:** Bajo
   * **Confianza:** Media
   * **Descripción:** Las cookies no están configuradas con el flag HttpOnly, lo que puede permitir el acceso a través de scripts.
   * **URL:** GET http://127.0.0.1:8000/registro/
4. **Petición de Autenticación Identificada**
   * **Riesgo:** Informativo
   * **Confianza:** Media
   * **Descripción:** Se identificó una petición de autenticación que puede ser susceptible a ataques.
   * **URL:** POST http://127.0.0.1:8000/registro/
5. **Respuesta de Gestión de Sesión Identificada**
   * **Riesgo:** Informativo
   * **Confianza:** Media
   * **Descripción:** Se identificó una respuesta de gestión de sesión que podría ser mejorada.
   * **URL:** GET http://127.0.0.1:8000/
6. **User Agent Fuzzer**
   * **Riesgo:** Informativo
   * **Confianza:** Baja
   * **Descripción:** Se identificó un fuzzing del User-Agent que puede ser un indicativo de exploración de vulnerabilidades.
   * **URL:** GET <http://127.0.0.1:8000/>

**Conclusión.**

El proyecto "Delicias Caseras" ha logrado superar exitosamente las expectativas planteadas durante las pruebas de seguridad, llevadas a cabo utilizando el programa ZAP (Zed Attack Proxy) versión 2.15.0. Este proceso de evaluación ha sido fundamental para asegurar la integridad y la protección de nuestra plataforma ante posibles amenazas.

Sin embargo, durante las pruebas se identificaron áreas que se tiene que mejorar como: Implementación de CSP, Configuración de Cookies, Ocultación de Información de Versión y Revisión de la Gestión de Sesiones

Aunque el proyecto "Delicias Caseras" ha mostrado resultados positivos en la prueba de seguridad, es necesario reconocer y abordar las áreas identificadas para fortalecer aún más la protección de nuestra aplicación.

Estas pruebas ayudan a asegurar la calidad del software, y evitar posibles ataques informáticos futuros para así brindarle más seguridad a nuestro cliente.