# Informe de Análisis de Vulnerabilidades de Seguridad Web

## 1. Encabezado

Título del Documento: Informe de Análisis de Vulnerabilidades de Seguridad Web

Fecha del Análisis: [Fecha]

Responsable del Análisis: [Nombre y Contacto]

Cliente: [Nombre de la Organización o Proyecto]

## 2. Resumen Ejecutivo

Descripción breve del análisis realizado.

Resultados clave:

• Número de vulnerabilidades detectadas y su criticidad.

• Recomendaciones prioritarias.

## 3. Alcance

• Lista de aplicaciones, APIs o módulos analizados.

• Metodología empleada (manual, automatizada o híbrida).

• Herramientas utilizadas.

## 4. Detalles Técnicos

4.1. Vulnerabilidades Detectadas:

Para cada vulnerabilidad:

• Nombre: [Ejemplo: 'SQL Injection en el parámetro id'].

• Descripción: [Explicación de la falla encontrada].

• Vector de Ataque: [Cómo se explota la vulnerabilidad].

• Impacto: [Riesgos para el sistema o negocio].

• Severidad: [Alta, Media, Baja].

• Prueba de Concepto (PoC):

```  
[Comandos o ejemplos empleados para validar la vulnerabilidad]  
```

• Evidencia: [Capturas de pantalla o registros que respalden el hallazgo].

4.2. Vulnerabilidades No Confirmadas:

Listado de posibles fallos que requieren más validación.

## 5. Recomendaciones

• Corto Plazo: [Acciones inmediatas para mitigar riesgos].

• Mediano Plazo: [Cambios en la configuración del sistema o WAF].

• Largo Plazo: [Revisión de procesos y adopción de mejores prácticas].

## 6. Conclusiones

Resumen del análisis.

Beneficios esperados tras aplicar las recomendaciones.

## 7. Anexos

• Archivos de salida generados por herramientas (ej.: logs de SQLMap, informes de OWASP ZAP).

• Recursos adicionales (manuales, links a CVE relevantes).