



**U.A.S.L.P**

**Actividad - OWASP y otras fuentes**

**Quintero Llamas Leonardo Damián**

**Facultad de Ingeniería**

**Área de Ciencias de la Computación**

**Ing. Sistemas Inteligentes**

**Principios de seguridad informática**

**Docente: Silva Trujillo Alejandra Guadalupe**

**Hora: 9:00-10:00**

**Fecha de entrega: 18 de noviembre de 2024**

**Contenido**

**Preguntas del Cuestionario**

1. **¿Qué es OWASP y cuál es su misión en el ámbito de la seguridad de aplicaciones web?**

   OWASP es una organización global enfocada en mejorar la seguridad del software. Su objetivo principal es sensibilizar sobre la importancia de la seguridad en aplicaciones web, ofreciendo recursos gratuitos, como guías, herramientas y documentación, para ayudar a desarrolladores y organizaciones a proteger sus aplicaciones contra amenazas de seguridad.

2. **¿Por qué es fundamental que los desarrolladores conozcan el OWASP Top 10 y cómo puede ayudarles en su trabajo diario?**

   Es fundamental que los desarrolladores lo conozcan porque es un listado que recoge las diez vulnerabilidades más críticas y frecuentes en aplicaciones web este proporciona un marco de referencia para identificar y mitigar riesgos comunes, ayudando a que integren medidas de protección desde la fase de codificación y eviten errores que podrían llevar a vulnerabilidades.

3. **¿Qué criterios utiliza OWASP para clasificar las vulnerabilidades de seguridad en el OWASP Top 10?**

   OWASP clasifica las vulnerabilidades según una combinación de datos estadísticos, análisis de expertos y estudios sobre incidentes de seguridad reales. Los criterios de evaluación incluyen la frecuencia de aparición de la vulnerabilidad, su facilidad de explotación, el daño que podría causar y su relevancia en el entorno de desarrollo moderno.

4. **¿Cómo puede el uso de la base de datos de OWASP prevenir vulnerabilidades durante el ciclo de desarrollo de software?**

   Utilizar la base de conocimientos de OWASP en el ciclo de desarrollo de software permite a los equipos identificar y corregir problemas potenciales de seguridad antes de que se conviertan en vulnerabilidades explotables. Las guías y herramientas proporcionadas por OWASP ayudan a implementar prácticas de desarrollo seguro desde la planificación y el diseño, hasta las pruebas y el despliegue.

5. **¿Qué diferencia existe entre las vulnerabilidades catalogadas por OWASP y aquellas en la base de datos CVE (Common Vulnerabilities and Exposures)?**

   OWASP se centra en definir y explicar las principales amenazas y debilidades que afectan a las aplicaciones web en general, basándose en prácticas comunes y casos de uso. La base de datos CVE, por otro lado, es un repositorio gestionado por MITRE que ofrece detalles específicos y únicos de vulnerabilidades conocidas en software, cada una con un identificador de CVE.

6. **¿Qué son los "proyectos de herramientas" de OWASP y cómo pueden ayudar a los equipos de seguridad en sus evaluaciones de seguridad?**

   Los proyectos de herramientas de OWASP son soluciones de software de código abierto que ayudan a los equipos de seguridad a evaluar y mejorar la seguridad de sus aplicaciones. OWASP ZAP es una herramienta para pruebas de penetración, y OWASP Dependency-Check detecta bibliotecas de software con vulnerabilidades conocidas. Estas herramientas proporcionan a los equipos un medio eficiente para identificar y remediar fallos de seguridad.

7. **¿De qué manera pueden los desarrolladores y profesionales de seguridad involucrarse en la comunidad OWASP para mejorar sus prácticas de seguridad?**

   Los desarrolladores y profesionales en seguridad pueden unirse a la comunidad OWASP asistiendo a eventos de capítulos locales, participando en proyectos colaborativos de código abierto, compartiendo investigaciones y contribuyendo con documentación y nuevas ideas. Estas actividades fomentan la colaboración y el aprendizaje continuo sobre las mejores prácticas y los últimos avances en seguridad.

8. **Además de OWASP, ¿qué otros estándares o marcos existen para promover la seguridad en el desarrollo de software (como CIS, NIST, ISO 27001)?**

   Estándares y marcos reconocidos existentes:

- **CIS:** Proporciona benchmarks y guías de configuración segura.
- **NIST:** El marco de ciberseguridad de NIST proporciona un enfoque estructurado para gestionar el riesgo de seguridad.

- **ISO 27001**: Es un estándar de gestión de seguridad de la información que ayuda a proteger los datos y la privacidad.
- **SANS Institute**: Ofrece materiales de formación y mejores prácticas en ciberseguridad.

9. **¿Cuál es la diferencia entre una vulnerabilidad de seguridad y una debilidad en el contexto de las guías de OWASP?**

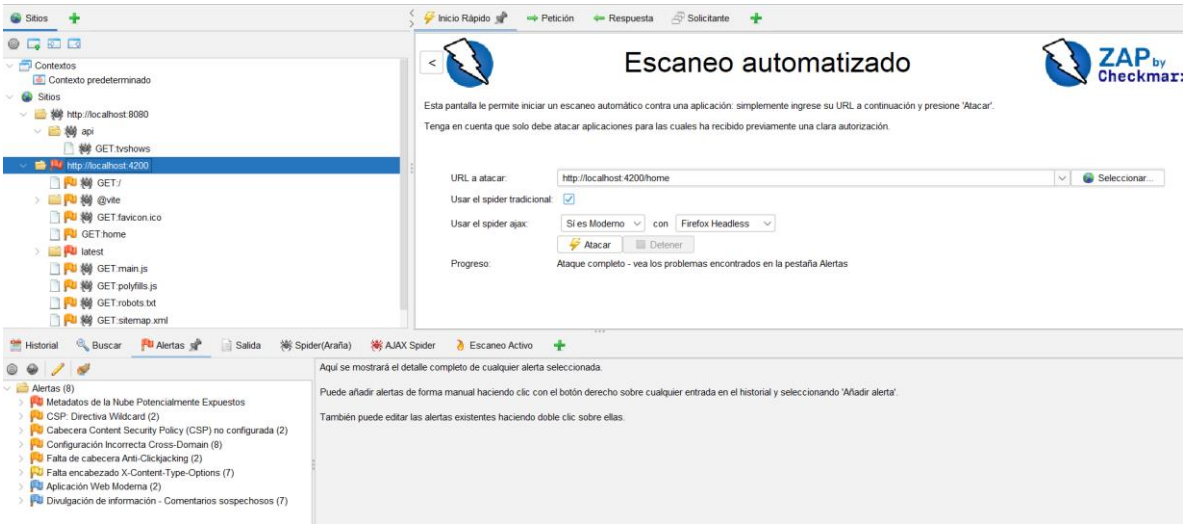
   Una vulnerabilidad es una falla en un sistema que puede ser explotada para comprometer su seguridad, mientras que una debilidad es una característica del diseño o la implementación que podría facilitar una vulnerabilidad si no se mitiga adecuadamente. Las guías de OWASP ayudan a identificar estas debilidades antes de que se conviertan en vulnerabilidades explotables.

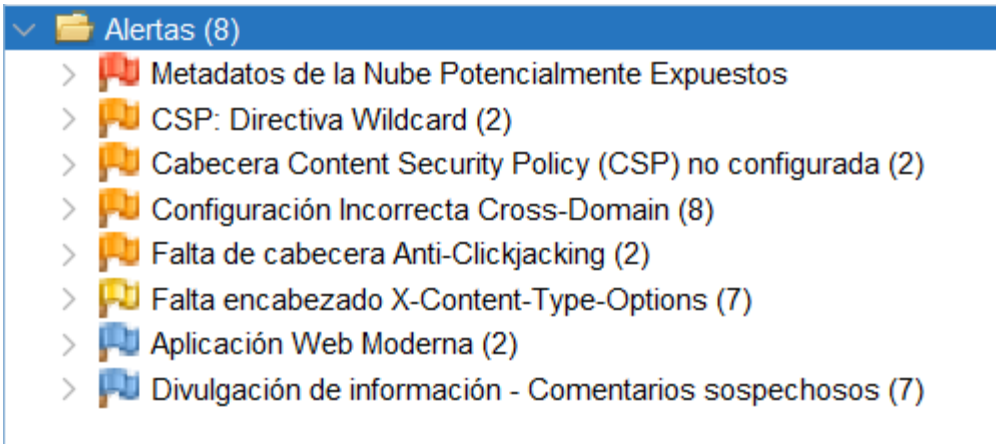
10. **¿Qué son los controles de seguridad recomendados por OWASP y cómo pueden ayudar a mitigar vulnerabilidades específicas en aplicaciones?**

    Los controles de seguridad de OWASP son recomendaciones y medidas prácticas que se pueden aplicar en el desarrollo de aplicaciones para prevenir o mitigar riesgos de seguridad. Incluyen políticas de validación de entradas, cifrado adecuado, gestión de autenticación y sesiones seguras, entre otros. Implementar estos controles reduce la probabilidad de que se exploten vulnerabilidades y mejora la resistencia de la aplicación frente a ataques.

## Actividades Prácticas

1. **Evaluación de Vulnerabilidades con OWASP ZAP:**




- Metadatos de la Nube Potencialmente Expuestos
  Mitigación: No confíe en ningún dato de usuario en las configuraciones de NGINX. En este caso, probablemente sea el uso de la variable $host que se establece desde el encabezado (header) 'Host' y puede estar controlado por un atacante.
- CSP: Directiva Wildcard
  Mitigación: Asegúrese de que su servidor web, servidor de aplicación, balanceador de carga, etc. está configurado apropiadamente para establecer la cabecera de Política de Seguridad de Contenido.
- Cabecera Content Security Policy (CSP) no configurada(2)
  Mitigación: Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.

- Configuración Incorrecta Cross-Domain(8)
  Mitigación: Asegúrese de que los datos confidenciales no estén disponibles de forma no autenticada (por ejemplo, mediante listas blancas de direcciones IP).
  Configure el encabezado HTTP "Access-Control-Allow-Origin" a un conjunto más restrictivo de dominios, o elimine todos los encabezados CORS por completo, para permitir que el navegador web aplique la Política del Mismo Origen (SOP) de una manera más restrictiva.
- Falta de cabecera Anti-Clickjacking (2)
  Mitigación: Los navegadores web modernos admiten las cabeceras HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que una de ellas está configurada en todas las páginas web devueltas por su sitio/aplicación.
  Si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, si forma parte de un FRAMESET), utilice SAMEORIGIN; de lo contrario, si no espera que la página esté enmarcada, utilice DENY. Alternativamente, considere implementar la directiva "frame-ancestors" de la Política de Seguridad de Contenidos.
- Falta encabezado X-Content-Type-Options (7)
  Asegúrese de que la aplicación/servidor web establece el encabezado Content-Type adecuadamente, y que establece el encabezado X-Content-Type-Options a 'nosniff' para todas las páginas web.
  Si es posible, asegúrese de que el usuario final utiliza un navegador web moderno y compatible con los estándares que no realiza MIME-sniffing en absoluto, o que puede ser dirigido por la aplicación web/servidor web para que no realice MIME-sniffing.