VULNERABILIADADES TOP 10 2017 VS 2021 OWASP

JULIAN ANDRES PEREIRA PLATA – 1015476906

Primero que todo hay que hablar de la OWASP, este es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. Es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP, su comunidad está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.

El OWASP Top 10 es un documento de concienciación estándar para desarrolladores y seguridad de aplicaciones web. Representa un amplio consenso sobre los riesgos de seguridad más críticos para las aplicaciones web. Reconocido mundialmente por los desarrolladores como el primer paso hacia una codificación más segura.

Las empresas deben adoptar este documento y comenzar el proceso de garantizar que sus aplicaciones web minimicen estos riesgos. Usar OWASP Top 10 es quizás el primer paso más efectivo para cambiar la cultura de desarrollo de software dentro de su organización a una que produzca código más seguro.

Teniendo ya claro que es el OWASP, su importancia, el top 10 y su uso ya podemos empezar a mirar sus diferencias y hacer un análisis entre esos dos años.

En cuanto a los principales cambios entre las versiones de las 10 vulnerabilidades top de OWASP, la lista de las 10 vulnerabilidades principales de 2017 incluía:

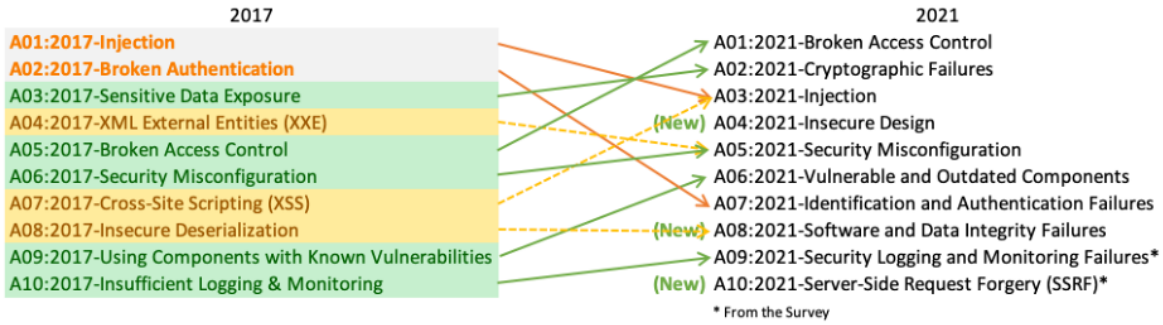
1. Inyección SQL
2. Autenticación y gestión de sesiones deficientes
3. XSS (Cross-Site Scripting)
4. Acceso no autorizado
5. Control de acceso roto
6. Vulnerabilidades de seguridad en componentes de terceros
7. Redirecciones y reenvíos no validados
8. Phishing y suplantación de identidad

9. Uso de criptografía débil
10. Fallos de seguridad en configuración y gestión

En la versión de 2021, la lista se ha actualizado a lo siguiente:

1. Inyección SQL
2. Autenticación y gestión de sesiones deficientes
3. XSS (Cross-Site Scripting)
4. Ataques a la lógica empresarial
5. Exposición de datos sensibles
6. Secuencias de comandos de servidor web (Web Server Request Forgery - SSRF)
7. Uso de componentes con vulnerabilidades conocidas
8. Insuficiente registro y monitorización
9. Autenticación de múltiples factores (MFA) vulnerada
10. Aplicaciones de baja calidad

Pero una diferencia más detallada se puede ver en la siguiente imagen:



Tomado de: https://owasp.org/www-project-top-ten/assets/images/mapping.png

La inclusión de la categoría A04:2021-Diseño Inseguro en el OWASP Top 10 es una novedad y se encuentra en el cuarto lugar. Esta categoría aborda los errores de diseño y fallas arquitectónicas que resultan en el diseño de un control inútil o faltante.

A diferencia de una implementación insegura que puede ser corregida fácilmente, solucionar un diseño inseguro puede resultar más complicado e incluso imposible.

Un ejemplo muy conocido de diseño inseguro es el método de "recuperación de contraseña basado en preguntas y respuestas", en el que se pregunta algo como "¿Cuál es el nombre de tu mascota favorita?". Sin embargo, muchas personas conocen el nombre de la mascota de otras personas. Además, es fácil de adivinar el nombre de la madre de alguien o su programa de televisión favorito, especialmente en la era de las redes sociales, donde toda esta información está disponible en línea.

La categoría A08:2021-Fallos en la Integridad de Datos y Software es otra de las novedades en el OWASP Top 10. Se refiere a problemas de seguridad que surgen cuando el código y la infraestructura no están protegidos contra violaciones de integridad. Estos problemas pueden ocurrir cuando una aplicación web depende de plugins, bibliotecas o módulos de fuentes, repositorios y redes de entrega de contenido no confiables.

Si una canalización de integración y entrega continua (CI/CD) no valida los recursos externos, esto puede generar vulnerabilidades de acceso no autorizado, código malicioso o compromiso del sistema. Otra situación que puede causar problemas es la falta de firma en las actualizaciones, algo que ocurre en muchos routers, decodificadores, firmware de dispositivos y otros dispositivos. En este caso, si el dispositivo realiza una actualización automática, un atacante puede cargar, distribuir y ejecutar su propia actualización maliciosa.

La última adición al OWASP Top 10 es A10:2021-Forjado de solicitudes en el lado del servidor (SSRF). Una vulnerabilidad de SSRF puede ocurrir cuando un atacante tiene control total o parcial sobre las solicitudes que envía una aplicación web. De esta manera, un posible atacante podría hacer que la aplicación web envíe solicitudes manipuladas a otros destinos o a sus propios recursos, lo que permitiría acceder a todo lo que el servidor tiene acceso. Esto permitiría a un atacante acceder a información que normalmente no sería accesible desde el exterior debido a un firewall, VPN o algún tipo de lista de control de acceso. Estos mecanismos de seguridad no funcionarían, ya que el servidor realiza estas solicitudes en su nombre.

Un ejemplo de SSRF sería si un atacante pudiera manipular una solicitud para que un servidor web envíe una solicitud a una red interna, como una base de datos. Si el servidor tiene acceso a la base de datos, el atacante podría obtener información confidencial de la base de datos.

El análisis de las vulnerabilidades en la lista OWASP Top 10 de 2021 revela tanto la continuidad como la evolución de los riesgos para la seguridad de las aplicaciones web. Por un lado, se mantienen algunas vulnerabilidades de la lista de 2017, como la inyección SQL y el XSS, lo que demuestra que estos riesgos persisten y siguen siendo explotados por los atacantes. Y por otro lado, nuevas entradas como los ataques a la lógica empresarial y la exposición de datos sensibles reflejan cómo los ciberdelincuentes han ido evolucionando sus técnicas para aprovecharse de las vulnerabilidades y acceder a información valiosa.

Es importante destacar que la lista de 2021 se enfoca no solo en las vulnerabilidades técnicas, sino también en el impacto empresarial que pueden tener. Esto muestra una mayor conciencia de que las vulnerabilidades pueden ser explotadas para acceder a datos sensibles y causar daños económicos y de reputación a las organizaciones. Además, la inclusión de "Aplicaciones de baja calidad" en la lista resalta la importancia de tener en cuenta la calidad de diseño e implementación en la seguridad de las aplicaciones.

En resumen, las organizaciones deben estar al tanto de estas amenazas y tomar medidas proactivas para minimizar los riesgos. Esto implica adoptar prácticas de desarrollo seguro, realizar pruebas regulares de seguridad y aplicar parches y actualizaciones a tiempo. Solo de esta manera se puede garantizar la protección de la información y la confianza de los clientes.

REFERENCIAS:

- https://owasp.org/www-project-top-ten/
- https://owasp.org/www-pdf-archive/Introduccion_a_la_OWASP.pdf
- https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf
- https://owasp.org/Top10/es/
- https://medium.com/digitalfrontiers/changes-in-owasp-top-10-2017-vs-2021-7cea4183288b