OWASP Top 10 es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la organización OWASP. Esta lista se publica y actualiza cada año por dicha organización

El objetivo de este proyecto según la OWASP top 10(2013), es crear conciencia acerca de la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones. Así mismo estos riesgos de seguridad son referenciados en artículos científicos, tesis de pregrado y postgrado, libros de seguridad y organizaciones como MITRE, SANS, PCI DSS, DISA, FCT

A01:2021-Broken Access Control

Sube desde la quinta posición; El 94 % de las aplicaciones se probaron en busca de algún tipo de control de acceso roto. Las 34 enumeraciones de debilidades comunes (CWE) asignadas al control de acceso roto tuvieron más ocurrencias en las aplicaciones que cualquier otra categoría.

A02:2021-Cryptographic Failures

Sube una posición al n.º 2, anteriormente conocido como Exposición de datos confidenciales, que era un síntoma general en lugar de una causa raíz. El enfoque renovado aquí está en las fallas relacionadas con la criptografía que a menudo conducen a la exposición de datos confidenciales o al compromiso del sistema.

A03:2021-Injection.

Se desliza hacia abajo hasta la tercera posición. El 94 % de las aplicaciones se probaron para detectar algún tipo de inyección, y los 33 CWE asignados a esta categoría tienen la segunda mayor cantidad de casos en las aplicaciones. Cross-site Scripting ahora es parte de esta categoría en esta edición.

A04:2021-Insecure Design

Es una nueva categoría para 2021, con un enfoque en los riesgos relacionados con fallas de diseño. Si realmente queremos "mover a la izquierda" como industria, se requiere un mayor uso del modelado de amenazas, patrones y principios de diseño seguro y arquitecturas de referencia.

A05:2021-Security Misconfiguration.

Sube desde el #6 en la edición anterior; El 90 % de las aplicaciones se probaron para detectar algún tipo de error de configuración. Con más cambios en el software altamente configurable, no sorprende ver que esta categoría sube. La categoría anterior para entidades externas XML (XXE) ahora forma parte de esta categoría.

A06:2021-Vulnerable and Outdated Components

Anteriormente se tituló Uso de componentes con vulnerabilidades conocidas y ocupa el segundo lugar en la encuesta de la comunidad Top 10, pero también tenía suficientes datos para llegar al Top 10 a través del análisis de datos. Esta categoría sube del puesto 9 en 2017 y es un problema conocido que nos cuesta probar y evaluar el riesgo. Es la única categoría que no tiene vulnerabilidades y exposiciones comunes (CVE) asignadas a los CWE incluidos, por lo que en sus puntajes se tienen en cuenta un exploit predeterminado y pesos de impacto de 5.0.

A07:2021-Identification and Authentication Failures

Anteriormente era autenticación rota y se está deslizando hacia abajo desde la segunda posición, y ahora incluye CWE que están más relacionados con fallas de identificación. Esta categoría sigue siendo una parte integral del Top 10, pero la mayor disponibilidad de marcos estandarizados parece estar ayudando.

A08:2021-Software and Data Integrity Failures

Es una nueva categoría para 2021, que se enfoca en hacer suposiciones relacionadas con actualizaciones de software, datos críticos y canalizaciones de CI/CD sin verificar la integridad. Uno de los impactos ponderados más altos de los datos de Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) asignados a los 10 CWE en esta categoría. La deserialización insegura de 2017 ahora forma parte de esta categoría más amplia.

A09:2021-Security Logging and Monitoring Failures

Anteriormente era Registro y monitoreo insuficientes y se agregó de la encuesta de la industria (n. ° 3), subiendo desde el n. ° 10 anterior. Esta categoría se expande para incluir más tipos de fallas, es difícil de probar y no está bien representada en los datos de CVE/CVSS. Sin embargo, las fallas en esta categoría pueden afectar directamente la visibilidad, las alertas de incidentes y el análisis forense.

A10:2021-Server-Side Request Forgery

Se agrega de la encuesta de la comunidad Top 10 (#1). Los datos muestran una tasa de incidencia relativamente baja con una cobertura de pruebas superior a la media, junto con calificaciones superiores a la media para el potencial de Explotación e Impacto. Esta categoría representa el escenario en el que los miembros de la comunidad de seguridad nos dicen que esto es importante, aunque no se ilustra en los datos en este momento.