OWASP Top 10 - Què és i Per què és Important

Què és l'OWASP Top 10?

L'OWASP Top 10 és un informe periòdic publicat per l'Open Web Application Security Project (OWASP) que identifica i prioritza les vulnerabilitats més crítiques en aplicacions web. És considerat un estàndard de referència per a desenvolupadors i professionals de seguretat que busquen millorar la seguretat del programari.

Paràmetres d'una Vulnerabilitat en l'OWASP Top 10

Cada vulnerabilitat identificada en l'OWASP Top 10 inclou una sèrie de paràmetres que ajuden a entendre la seva gravetat, prevalença i impacte. A continuació, es descriuen aquests paràmetres:

1. Factores: Indica quants factors s'han tingut en compte per avaluar la vulnerabilitat, com la gravetat del risc, la probabilitat d'explotació i l'impacte potencial.

2. CWEs mapeadas: Mostra quants CWEs (Common Weakness Enumeration) estan associats amb aquesta vulnerabilitat, proporcionant informació detallada sobre les debilitats específiques.

3. Tasa de incidencia máx: Percentatge màxim d'incidència observada d'aquesta vulnerabilitat en les aplicacions analitzades.

4. Tasa de incidencia prom: Percentatge mitjà d'incidència d'aquesta vulnerabilitat en totes les aplicacions analitzades.

5. Explotabilidad ponderada prom: Una escala (de 0 a 10) que mesura la facilitat amb què es pot explotar aquesta vulnerabilitat.

6. Impacto ponderado prom: Una escala (de 0 a 10) que mesura el potencial impacte de la vulnerabilitat si és explotada.

7. Cobertura máx i prom: Percentatge de cobertura màxima i mitjana d'aquesta vulnerabilitat en les aplicacions analitzades.

8. Incidencias totales: Nombre total d'incidències detectades d'aquesta vulnerabilitat en totes les aplicacions analitzades.

9. Total CVEs: Nombre total de CVEs (Common Vulnerabilities and Exposures) associats amb aquesta vulnerabilitat, amb exemples reals i documentació pública.

Per què l'OWASP Top 10 del 2021?

L'edició del 2021 és la versió més recent de l'OWASP Top 10. Tot i que OWASP actualitza aquesta llista periòdicament, el procés d'actualització és rigorós i inclou diverses fases: recopilació de dades, normalització, anàlisi, redacció, enquestes industrials, revisió pública i traduccions. Aquest procés assegura que la llista reflecteixi amb precisió les amenaces actuals més significatives.

Actualment, l'OWASP està treballant en la propera edició, prevista per al 2025. Mentrestant, l'edició del 2021 continua sent una referència essencial per comprendre i mitigar les vulnerabilitats més crítiques en aplicacions web.