

ERRORES DE PROGRAMACIÓN SEGÚN CWE/SANS

DESARROLLO DE SOFTWARE SEGURO



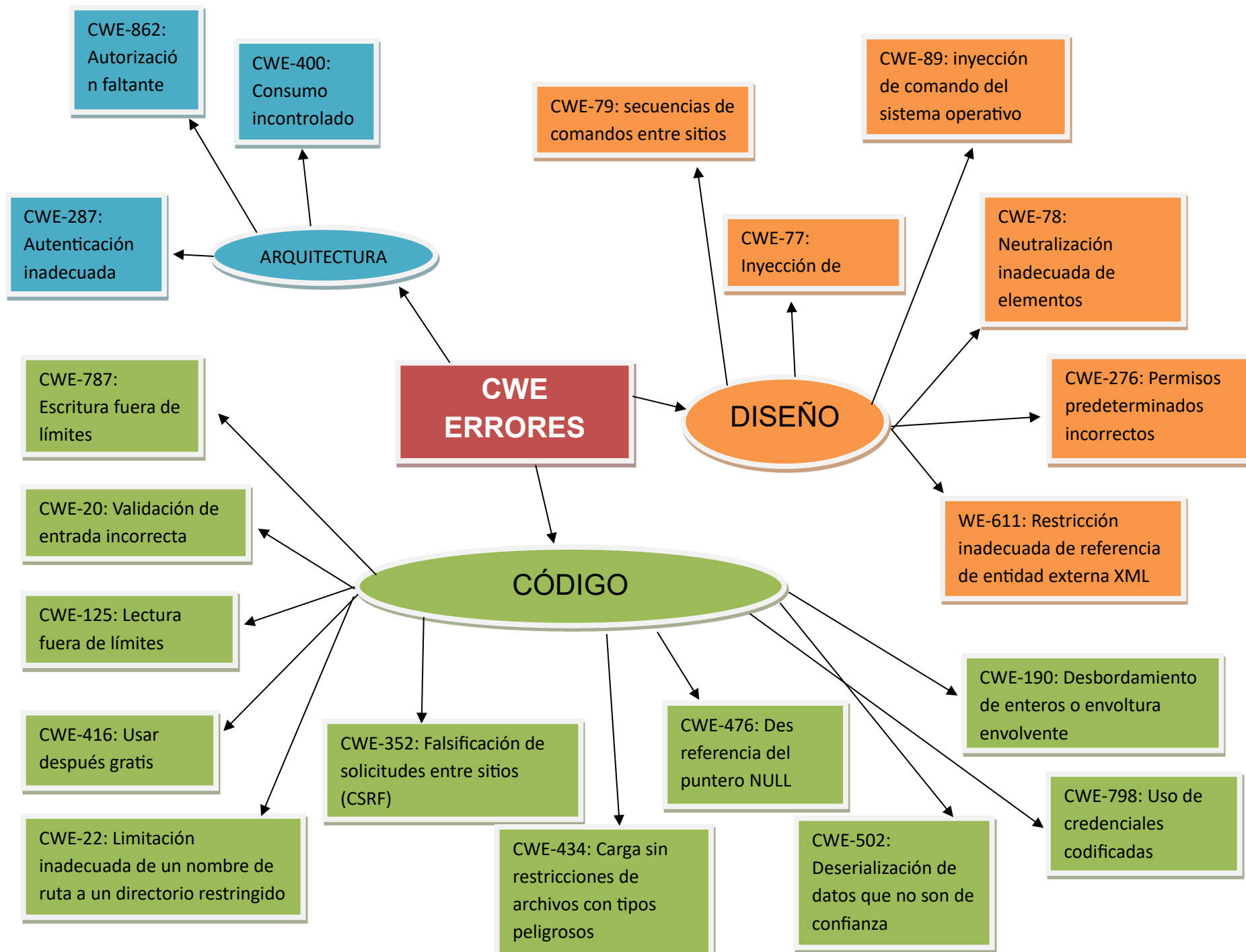
- Jorge Ibarra Peña
- 20310025
- 7°P
- Desarrollo de Software
- CETI COLOMOS

¿Qué beneficios tiene esta página para ti?

La lista CWE TOP 25 de errores de software más peligrosos beneficia a los desarrolladores al proporcionar conciencia de las vulnerabilidades críticas, priorizar correcciones, mejorar la calidad del código, facilitar el cumplimiento normativo, fortalecer la reputación, fomentar el aprendizaje continuo, ahorrar costos al prevenir problemas costosos y facilitar la comunicación interna y externa, lo que en última instancia conduce a aplicaciones más seguras y confiables.

¿Debilidad que NO ES DEBILIDAD y como solucionarla?

La CWE-862, "Autorización faltante", no representa una debilidad específica en la implementación de software, sino más bien una omisión de seguridad en el diseño del sistema. Para solucionar esta falta de autorización, es esencial implementar un sistema de autorización y autenticación sólido en tu aplicación, estableciendo roles y permisos para los usuarios, de modo que solo aquellos con los permisos adecuados puedan acceder y realizar acciones específicas en la aplicación. Aunque no es una debilidad en sí misma, la falta de autorización adecuada puede llevar a otras debilidades de seguridad, por lo que es crucial abordarla desde el principio para proteger eficazmente tus datos y recursos contra el acceso no autorizado.



CONCLUSIONES

la CWE TOP 25 es una lista clave que identifica las debilidades críticas en el software. Los desarrolladores pueden aprovecharla para priorizar correcciones, mejorar la calidad del código y garantizar la seguridad en todas las etapas del desarrollo. Al entender la clasificación en arquitectura, diseño y código, pueden abordar las debilidades desde el inicio, reduciendo el riesgo de problemas de seguridad en sus aplicaciones y construyendo software más seguro y confiable.