THE OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

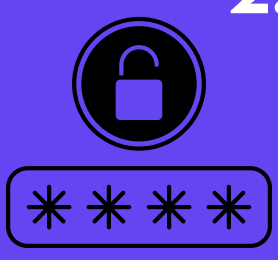
¿QUE ES OWASP?

El Proyecto abierto de seguridad de aplicaciones web, o OWASP, es una organización internacional sin ánimo de lucro dedicada a la seguridad de las aplicaciones web. Uno de los principios fundamentales del OWASP es que todos sus materiales están disponibles de forma gratuita y son fácilmente accesibles en su sitio web

1.-EXPOSICIÓN DE DATOS INESTABLES

Si las aplicaciones web no protegen los datos confidenciales, como la información financiera y las contraseñas, los atacantes pueden acceder a esos datos y venderlos o utilizarlos con fines maliciosos

2.-AUTENTICACIÓN COLAPSADA

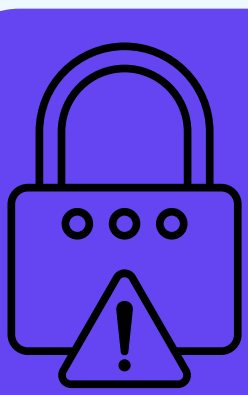


Las vulnerabilidades en los sistemas de autenticación (login) pueden dar a los atacantes acceso a las cuentas de los usuarios e incluso la capacidad de poner en riesgo todo un sistema mediante el uso de una cuenta de administrador

3.-ENTIDADES EXTERNAS

Canaliza la entrada XML. Esta entrada puede hacer referencia a una entidad externa, que intenta aprovecharse de una vulnerabilidad en el analizador

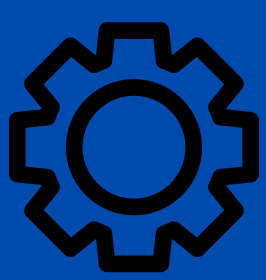
4.-CONTROL DE ACCESO ROTO



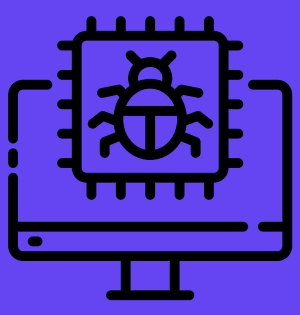
el control de acceso roto generalmente resulta de regulaciones de acceso de usuarios insuficientemente implementadas.

5.-CONFIGURACIÓN INCORRECTA DE LA SEGURIDAD

Son provocados por configuraciones de morosidad inadecuadas o inseguras, almacenamiento en la nube pública o señales de error crípticas



6.-CROSS-SITE SCRIPTING



Cuando una aplicación entrega datos que no son de confianza a un navegador web sin realizar la validación o escape necesarios, se produce una vulnerabilidad XSS

7.-DESERIALIZACIÓN INSEGURA

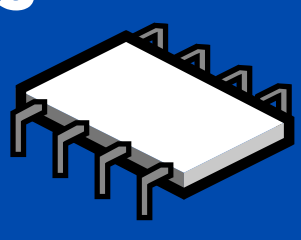
Resulta en situaciones de ejecución remota de código. Estas debilidades permiten que se lleven a cabo ataques de repetición, inyección y escalada de ventajas incluso si no se realiza la ejecución remota de código

8.-REGISTRO Y MONITOREO INSUFICIENTES

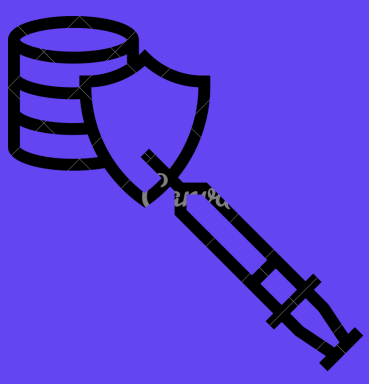
Puede resultar difícil o incluso imposible identificar atacantes o detectar ataques con un registro y monitoreo insuficientes

9.-USO DE COMPONENTES CON VULNERABILIDADES CONOCIDAS

Un ataque que aproveche con éxito un componente débil puede provocar una toma de control del servidor o una pérdida significativa de datos.



10.-INYECCIÓN

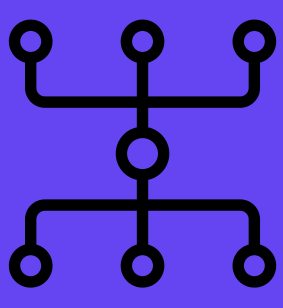


La entrega de datos no confiables a un intérprete como parte de un comando o consulta puede provocar problemas de inyección en SQL, NoSQL, OS y LDAP

OWASP DEPENDENCY-CHECK

Es una herramienta de análisis de composición de software (SCA) que intenta detectar vulnerabilidades divulgadas públicamente contenidas en las dependencias de un proyecto. Son provocados por configuraciones de morosidad inadecuadas o inseguras, almacenamiento en la nube pública o señales de error crípticas

OWASP AMASS



Amass es una herramienta que realiza el mapeo de la red de superficie de ataque y el descubrimiento de activos externos utilizando técnicas de recolección de información de código abierto y reconocimiento activo

OWASP OWTF

Es un proyecto centrado en la eficiencia de las pruebas de penetración y la alineación de las pruebas de seguridad con los estándares de seguridad como: la guía de pruebas