**O que é OWASP**

A OWASP (Open Web Application Security Project) é uma organização sem fins lucrativos focada em melhorar a segurança de software. A OWASP fornece recursos, ferramentas e informações para ajudar organizações a desenvolver, adquirir e manter software seguro. Ela é conhecida por suas listas "Top 10" de vulnerabilidades de segurança em aplicações web, assim como suas ferramentas e guias de boas práticas para desenvolvedores, testadores e profissionais de segurança. As iniciativas da OWASP visam aumentar a conscientização sobre segurança de software e promover práticas recomendadas para proteger aplicações contra ameaças.

**Listar os TOP 10 dos maiores riscos de segurança**

Atualmente, a OWASP (Open Web Application Security Project) mantém a lista "OWASP Top 10", que identifica as dez principais vulnerabilidades de segurança em aplicações web. Aqui estão os itens da lista mais recente (a partir do meu último treinamento em janeiro de 2022):

1. Injection (Injeção): Vulnerabilidades de injeção, como SQL, NoSQL, ou mesmo LDAP, permitem que um invasor injete comandos não autorizados em uma aplicação.
2. Broken Authentication (Autenticação Quebrada): Falhas nesse aspecto podem permitir que invasores comprometam senhas, chaves de sessão ou outras informações de autenticação de usuários.
3. Sensitive Data Exposure (Exposição de Dados Sensíveis): Se dados sensíveis, como informações de cartão de crédito ou senhas, não são adequadamente protegidos, eles podem ser acessados por invasores.
4. XML External Entities (XXE): Essa vulnerabilidade permite que um invasor cause a leitura de arquivos remotos ou mesmo a execução de código remoto.
5. Broken Access Control (Controle de Acesso Quebrado): Se as regras de acesso não são implementadas corretamente, usuários não autorizados podem acessar funcionalidades restritas.
6. Security Misconfiguration (Configuração de Segurança Incorreta): Configurações incorretas, como configurações padrão não alteradas ou configurações excessivamente permissivas, podem deixar a aplicação vulnerável a ataques.
7. Cross-Site Scripting (XSS): Nesse tipo de ataque, os invasores injetam scripts maliciosos em páginas web visualizadas por outros usuários.
8. Insecure Deserialization (Deserialização Insegura): Se a deserialização de dados não é feita de forma segura, isso pode levar a ataques de execução de código remoto.
9. Using Components with Known Vulnerabilities (Uso de Componentes com Vulnerabilidades Conhecidas): Se a aplicação usa bibliotecas ou componentes com vulnerabilidades conhecidas, ela pode ser explorada por invasores.
10. Insufficient Logging & Monitoring (Logs e Monitoramento Insuficientes): A falta de registros adequados e monitoramento pode dificultar a detecção de ataques e responder a eles de forma eficaz.