## 1. Injection

## 2. Broken Authentication

## 3. Sensitive Data Exposure

## 4. XML External Entities (XXE)

## 5. Broken Access Control

## 6. Security Misconfiguration

## 7. Cross-Site Scripting (XSS)

## 8. Insecure Deserialization

## 9. Using Components with Known Vulnerabilities

## 10. Insufficient Logging & Monitoring

injeção: Os ataques de injeção ocorrem quando o código malicioso é injetado em uma aplicação para obter acesso a dados, modificar dados ou executar comandos. Para explorar e entender os ataques de injeção, deve-se procurar por qualquer entrada de usuário que seja usada para gerar comandos SQL, NoSQL, OS ou LDAP.

Autenticação Quebrada: A autenticação quebrada ocorre quando os sistemas de autenticação não são implementados corretamente, permitindo que os atacantes ganhem acesso às contas de usuários. Para explorar e entender a autenticação quebrada, deve-se procurar por senhas fracas, gerenciamento de sessão fraco e armazenamento inseguro de credenciais de usuário.

Exposição de Dados Sensíveis: A exposição de dados sensíveis ocorre quando uma aplicação não protege adequadamente os dados sensíveis, como senhas, números de segurança social e números de cartão de crédito. Para explorar e entender a exposição de dados sensíveis, deve-se procurar por armazenamento e transmissão inseguros de dados sensíveis.

Entidades Externas de XML (XXE): Os ataques de Entidades Externas de XML (XXE) ocorrem quando uma aplicação analisa um documento XML e permite que um atacante execute código malicioso ou acesse dados sensíveis. Para explorar e entender os ataques XXE, deve-se procurar por qualquer código de análise XML que seja vulnerável a ataques XXE.

Controle de Acesso Quebrado: O controle de acesso quebrado ocorre quando uma aplicação não aplica corretamente as restrições de controle de acesso. Para explorar e entender o controle de acesso quebrado, deve-se procurar por qualquer entrada de usuário que seja usada para controlar o acesso sem validação adequada. Misconfiguração de Segurança: A misconfiguração de segurança ocorre quando uma aplicação não é configurada corretamente, resultando em dados e serviços expostos. Para explorar e entender a misconfiguração de segurança, deve-se procurar por quaisquer configurações de segurança incorretas, como portas abertas, senhas fracas e protocolos inseguros.

Cross-Site Scripting (XSS): Os ataques de Cross-Site Scripting (XSS) ocorrem quando um atacante insere código malicioso no código cliente de uma aplicação. Para explorar e entender os ataques XSS, deve-se procurar por qualquer entrada de usuário que seja usada para gerar código malicioso.

Deserialização Insegura: A deserialização insegura ocorre quando uma aplicação deserializa dados não confiáveis. Para explorar e entender a deserialização insegura, deve-se procurar por qualquer código de deserialização que seja vulnerável a ataques.

Usando Componentes com Vulnerabilidades Conhecidas: O uso de componentes com vulnerabilidades conhecidas ocorre quando uma aplicação usa componentes (como bibliotecas e frameworks) que possuem vulnerabilidades conhecidas. Para explorar e entender o uso de componentes com vulnerabilidades conhecidas, deve-se procurar por quaisquer componentes que possuam vulnerabilidades conhecidas e garantir que eles estejam atualizados para a versão mais recente.

Logging & Monitoramento Insuficiente: O logging & monitoramento insuficiente ocorre quando uma aplicação não registra e monitora adequadamente a atividade da aplicação. Para explorar e entender o logging & monitoramento insuficiente, deve-se procurar por quaisquer registros ausentes, configurações de log fracas e falta de mecanismos de alerta