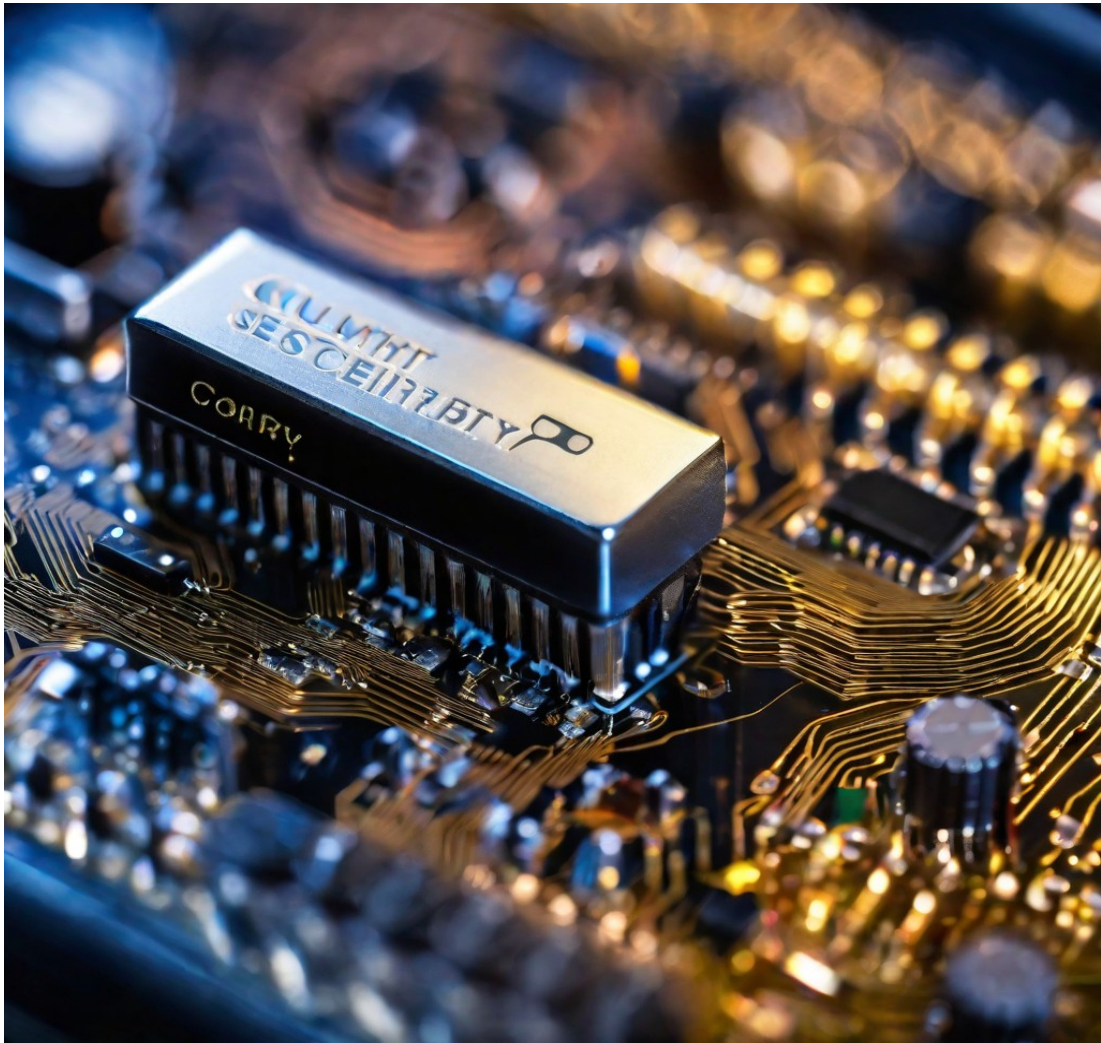
Qualidade de Produto de Sistemas de Software - Segurança

Bruno Leandro Diniz
Lucas Alush Barletta
Ygor Lopes Nakonieczni

Introdução

- Na era digital de hoje, a segurança nos sistemas de software é de extrema importância.
- Com a quantidade crescente de dados sensíveis armazenados e transmitidos eletronicamente, é crucial garantir que os sistemas de software estejam seguros e protegidos contra ameaças potenciais.



Visão Geral

- O que envolve o item de qualidade ?
- Problemas comuns de segurança
- Melhores práticas para desenvolvimento seguro de software
- Como atingir qualidade em segurança - Teste de Segurança
- Estudos de Caso

O que envolve o item de qualidade?

- A qualidade de segurança em sistemas de software envolve a identificação, prevenção, detecção e resposta a ameaças e vulnerabilidades que podem comprometer a segurança do sistema. Isso inclui medidas de segurança, como controle de acesso, criptografia, autenticação, autorização, monitoramento de eventos de segurança e proteção contra ameaças cibernéticas, como malware e ataques de hackers.

Problemas comuns de segurança:

Injeção de SQL - "SQL Injection"

- A SQLi é um tipo de vulnerabilidade em que um invasor usa uma parte do código SQL (Structured Query Language) para manipular um banco de dados e obter acesso a informações potencialmente valiosas. Esse é um dos tipos de ataque mais comuns e perigosos porque pode ser usado contra qualquer aplicação de Web ou site que utilize um banco de dados SQL (ou seja, a maioria deles).

Autenticação quebrada e gerenciamento de sessão

- A autenticação e o gerenciamento de sessões quebrados podem ocorrer quando os tokens de autenticação ou IDs de sessão não estão devidamente protegidos, permitindo que invasores sequestrem contas ou sessões de usuários.
- Isso pode resultar em acesso não autorizado a dados ou ações confidenciais.

Melhores práticas para desenvolvimento seguro de software

- Realizar auditorias de segurança e avaliações de risco regulares para identificar vulnerabilidades e ameaças potenciais.
- Implementar práticas de codificação seguras, como validação de entrada e tratamento de erros, para evitar problemas de segurança comuns, como injeção de SQL e scripts entre sites (XSS).
- Usar técnicas de criptografia e autenticação para proteger dados confidenciais, tanto em trânsito quanto em repouso.
- Manter-se atualizado com os patches e atualizações de segurança mais recentes para todos os componentes de software e bibliotecas usados em seu sistema.
- Treinar desenvolvedores e outras partes interessadas sobre práticas de codificação seguras e a importância da segurança no desenvolvimento de software.

Tipo de Testes de Segurança

- Teste de Penetração
- Verificação de Vulnerabilidade
- Revisionamentode Código
- Auditoria de Segurança

Teste de Penetração

- Simula o ataque a um sistema para identificar vulnerabilidades e avaliar a eficácia dos controles de segurança.

Verificação de Vulnerabilidade

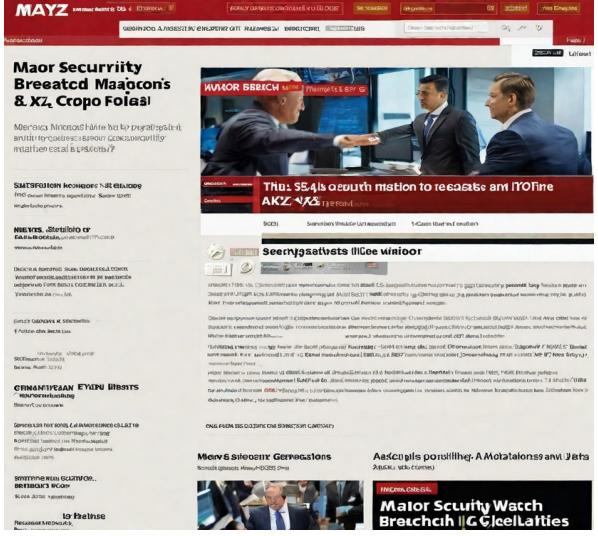
- Verificação automatizada de um sistema para detectar vulnerabilidades conhecidas e pontos fracos de segurança.

Revisionamento de Código

- Revisão manual ou automatizada do código-fonte para identificar possíveis falhas de segurança e erros de codificação.

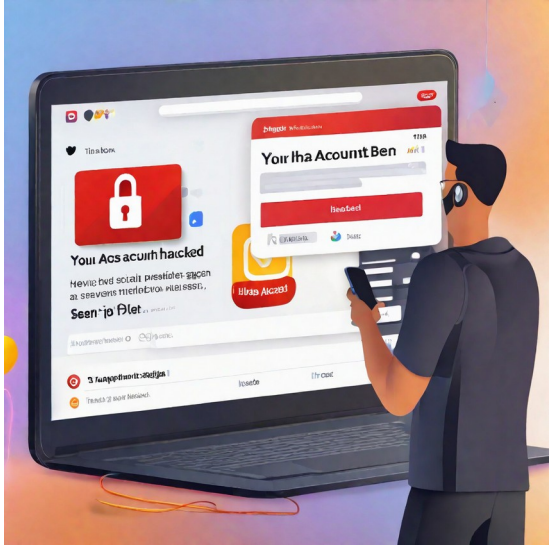
Auditoria de Segurança

- Avaliação abrangente da postura de segurança de um sistema, incluindo políticas, procedimentos e controles técnicos.



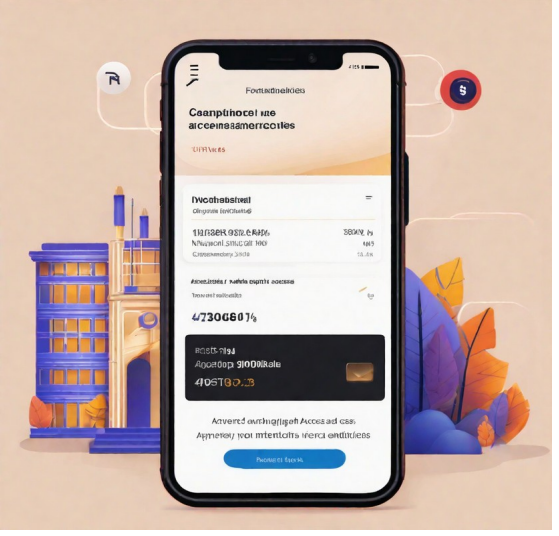
Estudo de Caso 1 - XYZ Corp Data Breach

- Em 2019, a XYZ Corp sofreu uma grande violação de dados que comprometeu as informações pessoais de milhões de clientes. Os hackers exploraram uma vulnerabilidade no sistema de software da empresa, que lhes permitiu obter acesso a dados confidenciais. A violação resultou na perda de confiança do cliente e em um impacto financeiro significativo para a empresa. Destacou a importância de implementar medidas de segurança robustas e de testar regularmente vulnerabilidades.



Estudo de Caso 2: Hacking de conta em plataforma mídia social

Em 2020, uma popular plataforma de mídia social sofreu uma série de invasões de contas que resultaram em acesso não autorizado aos dados do usuário. Os hackers usaram uma variedade de técnicas, incluindo phishing e adivinhação de senhas, para obter acesso às contas dos usuários. A plataforma foi criticada por não implementar medidas de segurança suficientemente fortes e por não fornecer suporte adequado aos utilizadores afetados. O incidente destacou a importância de educar os usuários sobre práticas seguras de senhas e implementar a autenticação multifatorial.



Estudo de Caso 3: Tentativa de acesso não autorizado no aplicativo bancário

- Em 2021, um aplicativo bancário detectou uma tentativa de acesso não autorizado ao seu sistema. As medidas de segurança do aplicativo, incluindo autenticação multifatorial e monitoramento em tempo real, conseguiram evitar a ocorrência da violação. O incidente destacou a importância da implementação de fortes medidas de segurança e do monitoramento regular de atividades suspeitas. Também demonstrou o valor de investir em práticas seguras de desenvolvimento de software.

Conclusão

- Em resumo, a segurança deve ser uma prioridade máxima no desenvolvimento de software.
- É importante compreender os problemas comuns de segurança e implementar as melhores práticas em todo o processo de desenvolvimento.
- Testes de segurança também devem ser realizados para garantir que o software esteja seguro antes de ser lançado.
- Estudos de caso demonstraram que as consequências de não dar prioridade à segurança podem ser graves, incluindo violações de dados e perdas financeiras.
- Ao implementar as melhores práticas e manter-se atualizado sobre as últimas tendências de segurança, os desenvolvedores de software podem ajudar a prevenir esses problemas e proteger os dados de seus usuários.