Importância da Segurança da Informação no desenvolvimento de Aplicativos

Prof. Esp. Pedro Miho

Grupo 1: Introdução à Segurança da Informação no Desenvolvimento de Aplicativos

UMC UNIVERSIDADE

Conteúdo necessário:

- Conceito de Segurança da Informação: Explique o que é segurança da informação e sua importância no contexto do desenvolvimento de software.
- Princípios fundamentais (CID):
  - Confidencialidade: Como proteger os dados contra acessos não autorizados.
  - Integridade: Garantir que os dados não sejam alterados sem autorização.
  - Disponibilidade: Manter os serviços e sistemas sempre acessíveis aos usuários autorizados.
- Exemplos reais: Apresente 5 casos famosos de falhas de segurança, como:
  - Vazamento de dados da Facebook (exposição de milhões de contas).
  - Brecha no aplicativo da Uber que permitiu acesso não autorizado.
- Como cada ataque poderia ser evitado: Explique como cada ataque poderia ser evitado

Grupo 1: Introdução à Segurança da Informação no Desenvolvimento de Aplicativos

Conteúdo necessário:

- Impactos da falta de segurança: Aborde consequências como perda financeira, danos à reputação e sanções legais.

Grupo 2: Práticas Seguras no Desenvolvimento de Aplicativos

UMC UNIVERSIDADE

Conteúdo necessário:

- Segurança por design: Explique a importância de considerar a segurança desde o início do projeto.
- Autenticação e controle de acesso:
  - Implementação de autenticação multifator (MFA).
  - Utilização de padrões seguros como OAuth 2.0, OpenID Connect e SAML.
- Gerenciamento seguro de senhas e tokens:
  - Utilização de hashes e salt para proteger senhas.
  - Práticas seguras para armazenar e gerenciar tokens de sessão.
- Bibliotecas e frameworks seguros: Explique por que é importante escolher ferramentas confiáveis e atualizadas.

Grupo 3: Principais Ameaças e Vulnerabilidades

UMC UNIVERSIDADE

Conteúdo necessário

- Ataques comuns:
  - SQL Injection: Explique como funciona e demonstre um exemplo básico.
  - Cross-Site Scripting (XSS): Mostre como scripts maliciosos podem comprometer dados do usuário.
  - Cross-Site Request Forgery (CSRF): Demonstre como esse ataque pode forjar ações em nome do usuário.
- Vulnerabilidades em APIs: Explique como APIs mal configuradas podem expor dados sensíveis.
- Engenharia social: Apresente como criminosos enganam usuários para obter informações confidenciais.
- Exploração de falhas de configuração: Dê exemplos de permissões mal definidas e seus riscos.

Grupo 4: Ferramentas e Técnicas para Testes de Segurança

UMC UNIVERSIDADE

Conteúdo necessário:

- Conceito de Pentest (Teste de Penetração): Explique como esse processo é essencial para identificar vulnerabilidades.
- Ferramentas recomendadas:
  - OWASP ZAP e Burp Suite para análise de segurança em aplicações web.
  - Nmap para varredura de portas e serviços vulneráveis.
  - Nikto para detectar vulnerabilidades em servidores web.
- Testes durante o ciclo de desenvolvimento: Explique o conceito de DevSecOps e como integrar segurança no processo de CI/CD.
- Revisão de código: Enfatize a importância de revisar códigos para identificar brechas e falhas lógicas.

Grupo 5: Boas Práticas na Implantação e Manutenção

UMC UNIVERSIDADE

Conteúdo necessário:

- Configuração segura de servidores: Explique como ajustar permissões, proteger portas e desabilitar serviços desnecessários.
- Atualizações e aplicação de patches: Destaque a importância de manter software e bibliotecas sempre atualizadas.
- Monitoramento e resposta a incidentes:
  - Demonstre ferramentas como Splunk, Wazuh ou Graylog para detecção de ameaças.
- Backup e plano de recuperação de desastres:
  - Explique a importância de backups regulares e como implementá-los de forma segura.
  - Apresente a diferença entre Backup Full, Incremental e Diferencial.

Orientações para as Apresentações

Orientações para as Apresentações

- Divisão de responsabilidades: Cada integrante deve participar explicando uma parte do conteúdo.
- Exemplos práticos: Sempre que possível, incluir simulações ou demonstrações que ilustrem a teoria.
- Estrutura sugerida:
  - Introdução ao tema
  - Explicação teórica com exemplos
  - Demonstração prática ou estudo de caso
  - Conclusão destacando a importância do tema
- Uso de recursos visuais: Utilize slides, diagramas e gráficos para facilitar a compreensão.

Orientações para as Pesquisas

Cada grupo deverá realizar uma pesquisa sobre o tema designado, abordando os seguintes pontos:

- Introdução
  - Apresentar o tema e sua importância, destacando por que a segurança da informação é essencial no desenvolvimento de aplicativos.
- Desenvolvimento
  - Explorar o conteúdo específico do tema do grupo, explicando conceitos, práticas recomendadas, ferramentas e exemplos relevantes.
- Conclusão
  - Reforçar a importância do tema abordado e apresentar recomendações ou boas práticas para garantir a segurança da informação nos aplicativos.

Cada integrante do grupo deve contribuir na pesquisa e estar preparado para apresentar sua parte. Recomendo que utilizem exemplos práticos e recursos visuais para enriquecer a apresentação.