Parte 1: Introdução ao Controle de Acesso Quebrado

- Definição: ocorre quando a aplicação permite que os usuários acessem dados ou funcionalidades sem permissão.
- Importância: é uma das vulnerabilidades mais críticas segundo o OWASP Top 10.
- remover alteração no URL).Exemplo simples: um usuário altera a URL para acessar informações de outro (/conta?id=124).

Parte 2: Exemplos Reais de Falhas

- Manipulação de URL: alteração de parâmetros do usuário para acesso a dados de terceiros.
- Acesso a funcionalidades ocultas: uma funcionalidade não aparece na interface, mas está disponível via requisição direta.
- Elevação de privilégios: um usuário comum tenta executar ações administrativas.
- casal de mudarAlteração de cookies ou tokens: mude role=userpara role=adminganhar privilégios.

Parte 3: Como Prevenir sobre Controle de Acesso Quebrado

- Negação por padrão: bloqueie tudo por padrão e libere apenas o que for necessário.
- Validação no servidor: nunca confie em verificações feitas no lado do cliente.
- Verificação por recurso: valide se o usuário tem permissão para acessar o recurso solicitado.
- Regras centralizadas: mantenha as regras de controle de acesso organizado e de auditorias fáceis.

Parte 4: Testando e Detectando Vulnerabilidades

- Testes manuais: simular alterações em URLs, configurações e funções do usuário.
- Equipamentos de automação:

    - OWASP ZAP
    - Suíte Burp
- Revisão de código: analisar trechos onde as tarefas são aplicadas.

Parte 5: Impactos e Consequências

- Vazamento de dados temporário.
- Acesso não autorizado a contas e funcionalidades restritas.
- Possibilidade de controle total da aplicação.
- Danos à confiança da empresa e exposição a deliberações legais.