1. Introdução (1 minuto)

Olá, meu nome é PEDRO e hoje eu vou falar sobre um dos maiores riscos de segurança em aplicações web segundo a OWASP: o Broken Access Control.

Esse é o número 1 do OWASP Top 10 – o ranking das principais vulnerabilidades em aplicações.

Mesmo com tanto avanço em segurança, esse problema ainda afeta milhares de sistemas no mundo todo e pode levar a sérios vazamentos de dados e comprometimento de sistemas.

2. O que é Broken Access Control? (2 minutos)

Broken Access Control significa falhas no controle de acesso, ou seja, quando um usuário consegue acessar funcionalidades ou dados que ele não deveria conseguir.

Por exemplo:

- Um usuário comum consegue acessar páginas de administrador.
- Alguém modifica um ID na URL para acessar informações de outro usuário.
- Um sistema não verifica se o usuário realmente tem permissão para realizar uma ação.

Essas falhas geralmente acontecem porque os controles de acesso não estão implementados corretamente no back-end, ou dependem apenas do front-end — o que é um erro.

3️⃣

3. Exemplos práticos (2 minutos)

VIDEO JÁ GRAVADO NA AULA

4. Impactos de segurança (1 minuto)

Os impactos do Broken Access Control podem ser críticos, como:

- Exposição de dados sensíveis de outros usuários.
- Alteração ou exclusão de informações importantes.
- Escalada de privilégios (ex: virar administrador).
- Comprometimento completo do sistema.

Casos como esse já afetaram empresas como a Facebook, Uber e Twitter — onde usuários acessaram dados privados ou realizaram ações que não deveriam.

5. Como prevenir? (2 minutos)

Prevenir Broken Access Control envolve boas práticas de segurança desde o desenvolvimento. Algumas medidas são:

- Implementar verificação de permissões no back-end (nunca só no front-end).
- Usar controle de sessão robusto para saber quem é o usuário autenticado.
- Bloquear acesso por padrão e só liberar quando for permitido (princípio do menor privilégio).
- Evitar usar IDs previsíveis nas URLs.
- Auditar e revisar regras de acesso regularmente.
- Utilizar frameworks que ofereçam controle de acesso embutido, como Spring Security, ASP.NET Identity, etc.

Também é essencial realizar testes de segurança, como testes manuais e automáticos com ferramentas como OWASP ZAP e Burp Suite.

3M

6. Dicas (1 minuto)

- A OWASP tem uma cheat sheet de Access Control com boas práticas.
- Há ferramentas como AuthZ e OPA (Open Policy Agent) que ajudam na gestão de permissões.
- Automatizar testes de permissão em APIs é fundamental, principalmente quando se usa REST ou GraphQL.

Dica final: documente claramente as permissões de cada tipo de usuário. A maioria das falhas de acesso vem da falta de clareza sobre quem pode o quê.

3M

7. Conclusão (1 minuto)

Em resumo, o Broken Access Control é uma vulnerabilidade muito comum e perigosa.

Ele pode permitir que usuários acessem dados ou funções que não deveriam, causando vazamentos e até invasões completas.

Com boas práticas de desenvolvimento seguro, testes e atenção às permissões, é possível evitar esse tipo de falha.

Obrigado por assistir! Se tiver dúvidas, pode entrar em contato comigo ou acessar o site da OWASP para saber mais.