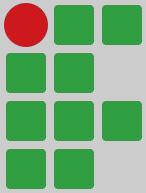


INSTITUTO FEDERAL
Pará

Broken Access Control

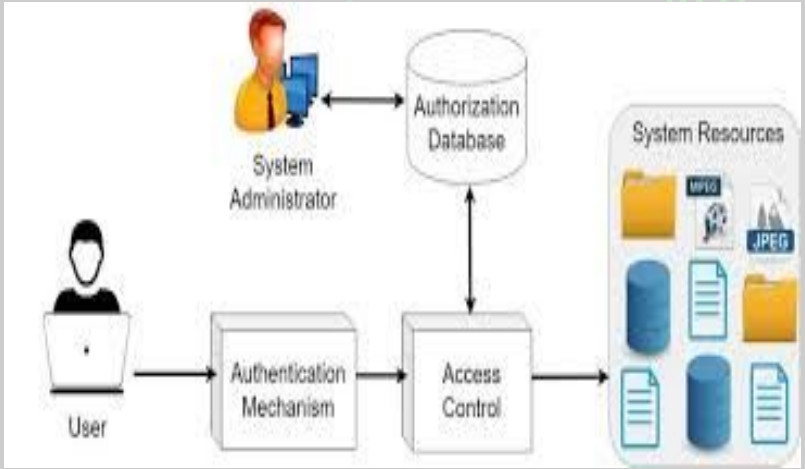
Engenharia de Software II
DOCENTE: Clóvis Maxwell Andrade Martins
DISCENTES: Denis de Castro Silva, Elton Carlos Viana Pantoja, Júlio Rodrigues Matos, Mayco Viana da Silva

Controle de Acesso

- Conjunto de mecanismos e políticas que **restringe** ou **permite** a usuários (ou sistemas) acessar e manipular recursos em uma infraestrutura de TI.

- **Controles Físicos**: São barreiras que limitam o contato ou acesso direto à informação ou à infraestrutura (que garante a existência da informação) que a suporta.

- **Controles Lógicos**: São barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta à alteração não autorizada por elemento mal intencionado.



Os Pilares do Controle de Acesso

Autenticação (Authentication)

- Processo de verificar a identidade do usuário ou sistema. Responde à pergunta: *"Você é quem diz ser?"*
- Mecanismos Comuns: Senhas, tokens (2FA), certificados digitais, biometria.
- Resultado: O sistema confirma a identidade do usuário para a próxima etapa.

Autorização (Authorization)

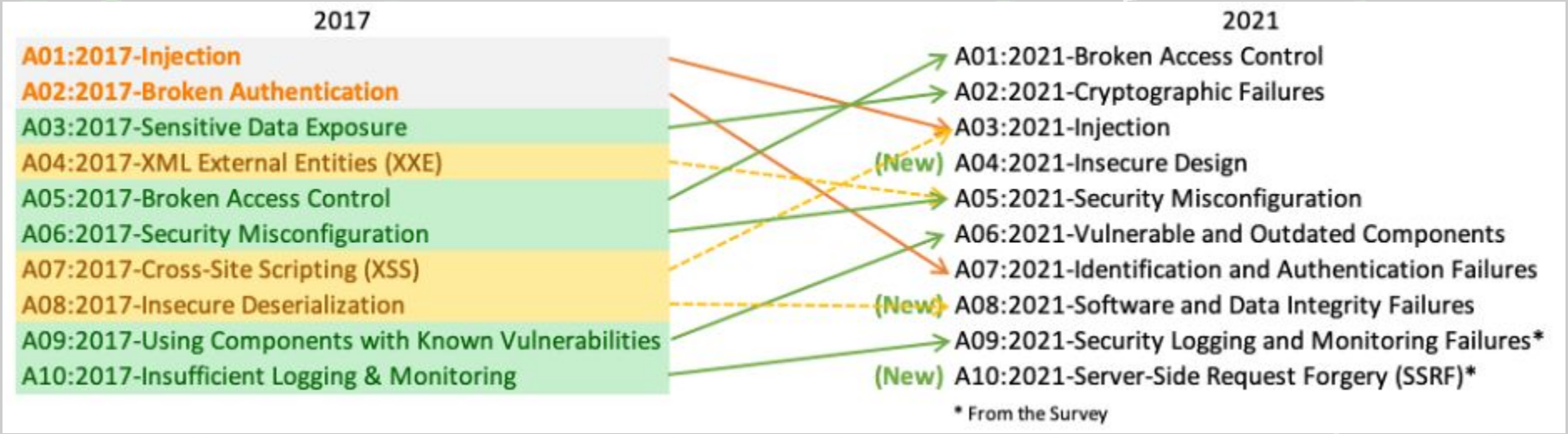
- Processo de determinar o que o usuário autenticado tem permissão para fazer. Responde à pergunta: *"Você tem permissão para esta ação?"*
- Mecanismos Comuns: Papéis (Roles), Grupos, Listas de Controle de Acesso (ACLs), Políticas.
- Resultado: O sistema concede ou nega o acesso a um recurso ou funcionalidade específica.

Auditoria (Accountability)

- Processo de rastrear e registrar as ações do usuário (ou sistema) dentro do ambiente. Responde à pergunta: *"O que foi feito e por quem?"*
- Mecanismos Comuns: Logs de sistema, trilhas de auditoria, monitoramento de atividades.
- Resultado: Permite a responsabilização e a detecção de atividades anormais ou maliciosas.

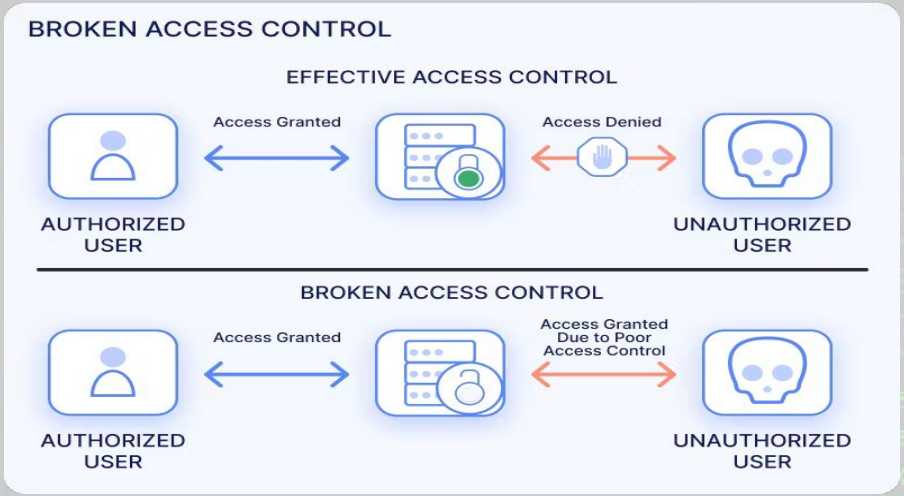
Broken Access Control

É uma vulnerabilidade de segurança que ocorre quando os mecanismos de autenticação e autorização de um sistema não são implementados corretamente, permitindo que usuários não autorizados acessem recursos ou realizem ações restritas.

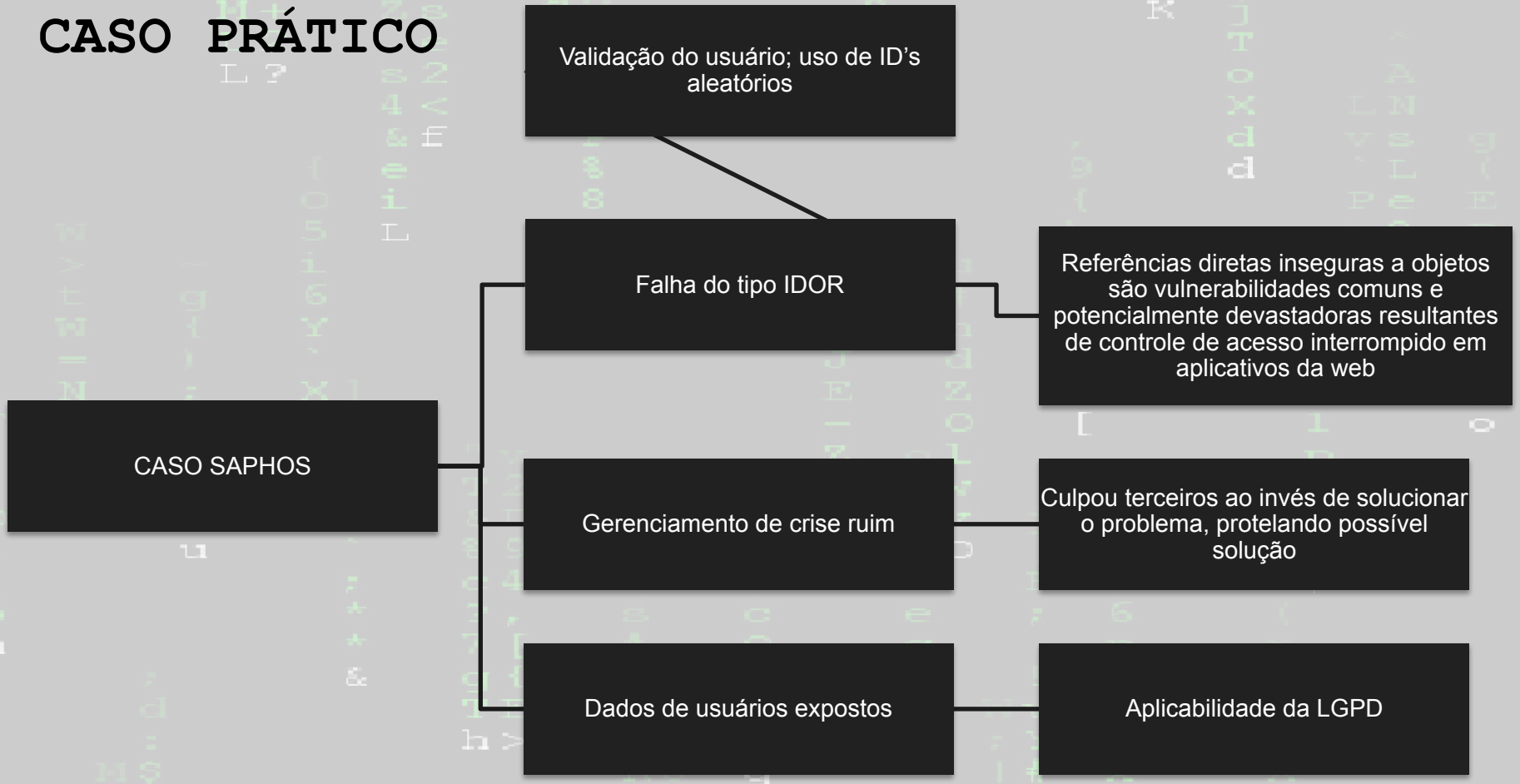


Tipos de Broken Access Control

- Manipulação do parâmetro
- Técnicas de Bypass do controle de acesso:
- Insecure Direct Object Reference (IDOR) / Broken Object Level Authorization (BOLA)



CASO PRÁTICO



Sapphos @sapphosapp2 · 8 de set

Sofremos uma tentativa por parte de um grupo de homens.

As medidas jurídicas já foram tomadas, e todas as informações foram retiradas do ar. Ninguém poderá ter acesso fora do aplicativo!

Importante: NENHUMA foto de documento da etapa de verificação foi acessada!

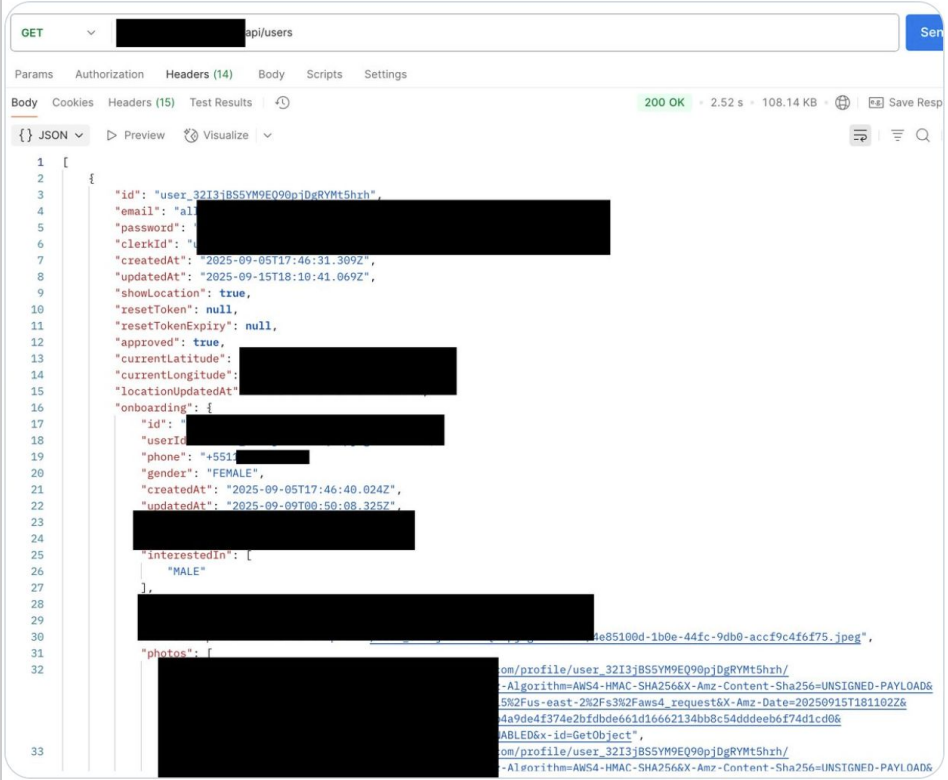
Os leitores adicionaram contexto que acharam que as pessoas poderiam gostar de saber

A empresa foi ALERTADA por profissionais de segurança da informação sobre uma maneira insegura de tratar dados cadastrais usada no Sapphos.

Não houve ataque, apenas apontamento de vulnerabilidade.

antonio realoficial.com.br | viral.day ✓
@acgfbr

achei uma falha 10x pior que da sapphos em um outro app, dessa vez nao vou reportar



3:12 PM · 15 de set de 2025 · **130,5 mil** Visualizações

Como Identificar e prevenir

Sempre verifique no servidor: A validação deve ocorrer no servidor, e não no navegador do usuário.

Negue por padrão: O acesso deve ser negado, a menos que haja uma permissão explícita.

Nunca confie no usuário: Valide sempre os dados que vêm das requisições (como IDs de URL).

Menos é mais: Dê aos usuários apenas as permissões essenciais para o trabalho deles.

Monitore e registre: Fique de olho em atividades suspeitas de acesso.

Faça testes: Realize testes de segurança e revisões de código regularmente.

Conclusão

A quebra de controle de acesso é uma vulnerabilidade crítica que expõe sistemas e dados, permitindo que atacantes executem ações para as quais não têm permissão. Ela pode se manifestar de diversas formas, desde a manipulação de URLs até a exploração de configurações incorretas de permissões, e suas consequências podem ser devastadoras, incluindo roubo de dados, fraude e perda de confiança, pois LGPD exige que as organizações adotem medidas técnicas e administrativas robustas para proteger os dados pessoais dos usuários de sistema. Portanto, a implementação de mecanismos de segurança robustos e a validação rigorosa de cada requisição são fundamentais para proteger as aplicações.