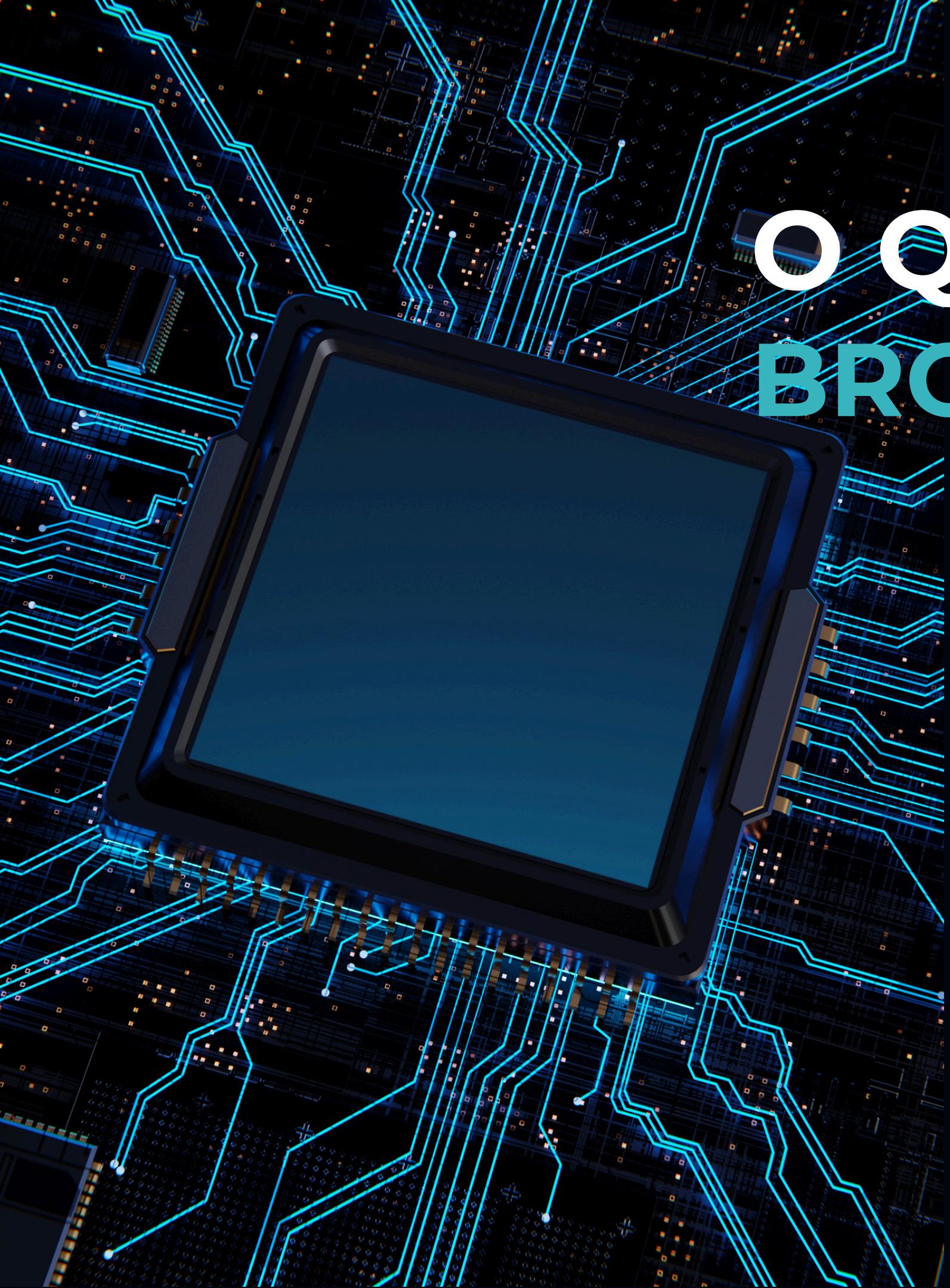




BROKEN ACCESS CONTROL

A falha número 1 da OWASP



O QUE É O BROKEN ACCESS CONTROL?



Broken Access Control é uma falha de segurança que acontece quando um sistema não controla corretamente o acesso dos usuários, permitindo que eles realizem ações ou consultem informações além do que deveriam. Essa vulnerabilidade ocupa o primeiro lugar no ranking OWASP Top 10 de 2021 devido à sua alta frequência e ao impacto que pode causar em aplicações.

COMO ACONTECE?

Esse tipo de falha pode ocorrer de várias maneiras. Algumas comuns incluem a alteração de identificadores em URLs para acessar dados de outros usuários, a elevação de privilégios que transforma um usuário comum em administrador, a manipulação de cookies e tokens de sessão ou até a falta de validações no backend, quando a aplicação confia apenas no front-end. Em todos os casos, o invasor ultrapassa barreiras de segurança e acessa informações sigilosas.



IDOR (INSECURE DIRECT OBJECT REFERENCE)

IDOR é um tipo de Broken Access Control em que o sistema usa identificadores previsíveis, como números de ID, sem verificar se o usuário tem permissão de acesso.

Assim, basta alterar valores em URLs ou requisições para visualizar dados de outras pessoas.

Insecure Direct Object Reference (IDOR) Vulnerability

1. Hacker identifies web application using direct object reference(s) and requests verified information.

`https://banksite.com/account?Id=1234` ✓



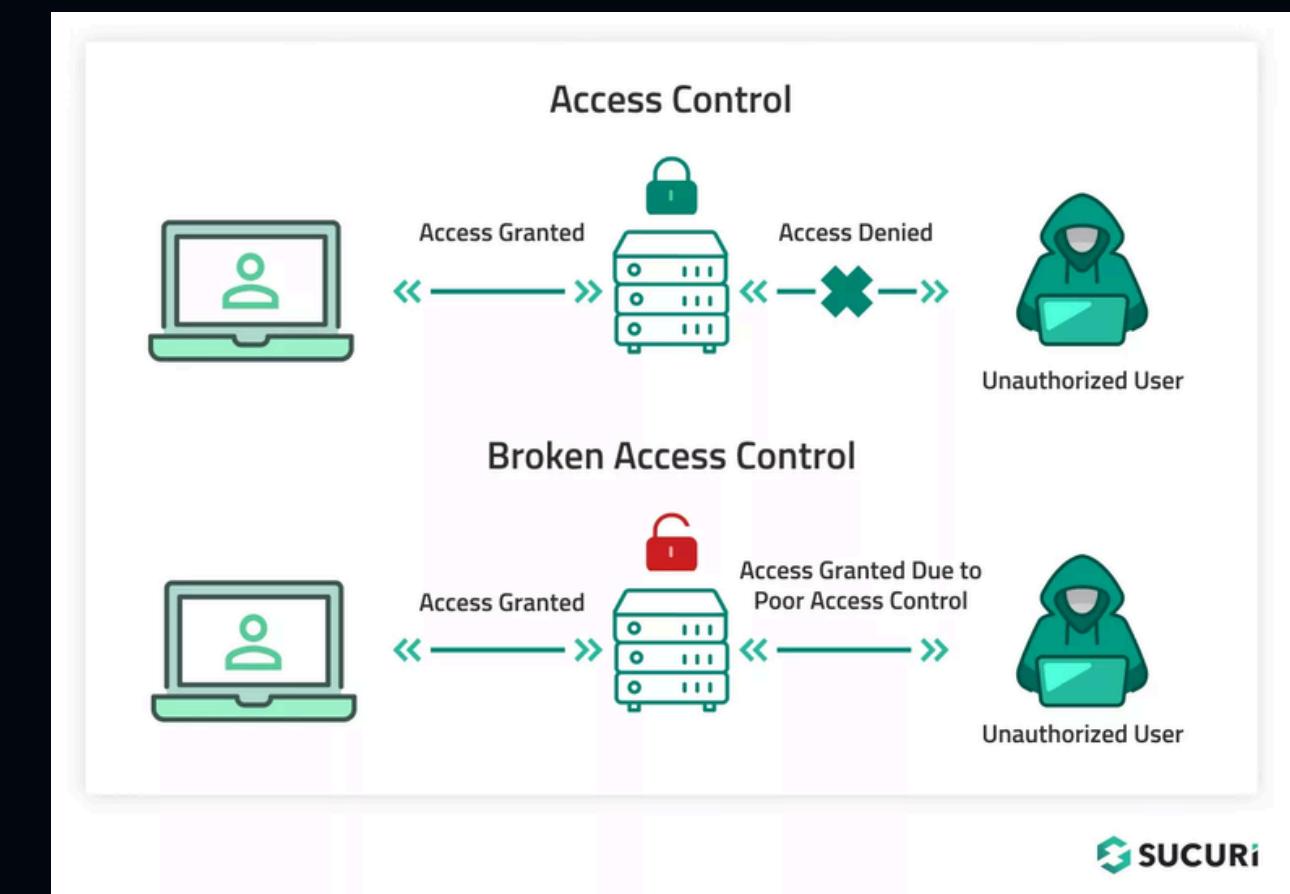
3. Direct object reference entity is manipulated and http request is performed again.

`https://banksite.com/account?Id=1235` ✓

2. Valid http request is executed and direct object reference entity is revealed.
4. http request is performed without user verification and hacker is granted access to sensitive information.

COMO TRATAR ESSA VULNERABILIDADE?

A prevenção passa pela aplicação do princípio do menor privilégio, garantindo que cada usuário só tenha acesso ao que realmente precisa. Além disso, a política de negar por padrão deve ser seguida, permitindo apenas o que for explicitamente autorizado. Todas as validações precisam ser feitas no backend, e sessões ou tokens devem ser configurados de forma segura, com expiração e invalidação. Auditorias, testes e monitoramento constantes também são essenciais para identificar e corrigir falhas antes que sejam exploradas.





EMPRESAS VÍTIMAS DO BROKEN ACCESS CONTROL

Grandes empresas também já sofreram com falhas de Broken Access Control e problemas de controle de acesso. Esses casos mostram que a vulnerabilidade não afeta apenas sistemas pequenos ou mal estruturados, mas pode comprometer até mesmo organizações globais com bilhões de usuários e altos investimentos em segurança.

Uber

O invasor conseguiu acesso inicial explorando a fadiga de autenticação multifator (MFA), induzindo o funcionário a aprovar notificações indevidas.

Reddit

O invasor criou uma página falsa que imitava o portal interno da empresa, roubando credenciais e tokens de autenticação.

Dell

As investigações apontam para uma falha em API ou permissões mal configuradas, permitindo acesso não autorizado a informações internas.