

OAuth



Tópicos

- O que é OAuth ?
- Como OAuth funciona
- Reconhecendo vulnerabilidades OAuth
- Como descobrir se uma aplicação usa OAuth
- Casos de Exploração
- Boas Práticas de Mitigação



O que é o OAuth ?



OAuth Authentication

- OAuth Authentication - Open Authorization
- Protocolo que permite uma aplicação acessar recursos de outra aplicação em nome de um usuário sem ter de usar as credenciais desse usuário
- Caso seja autorizado, recebe um token de acesso com acessos limitados
- Credenciais do usuário != Token de Acesso

Token de Acesso

O token de acesso é uma chave, tipo um pin, que permite que outra aplicação realize ações em nome do usuário que liberou esse token

As informações dos usuário ficam protegidas, garantindo a segurança do usuário ao executar uma aplicação



Como funciona ?

Principais grupos

Cliente

- É o app que quer acessar os dados
- É quem pede autorização do usuário pra usar os dados

Usuário

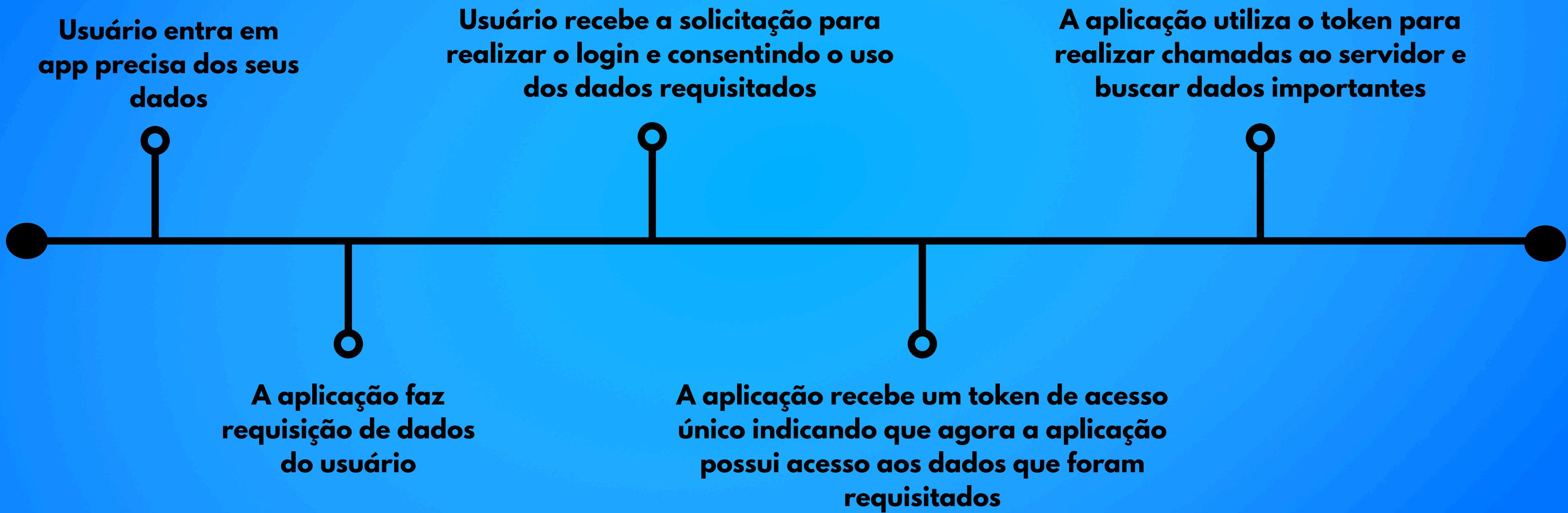
- É a pessoa dona dos dados
- É quem concede a permissão para acesso aos dados

Servidor

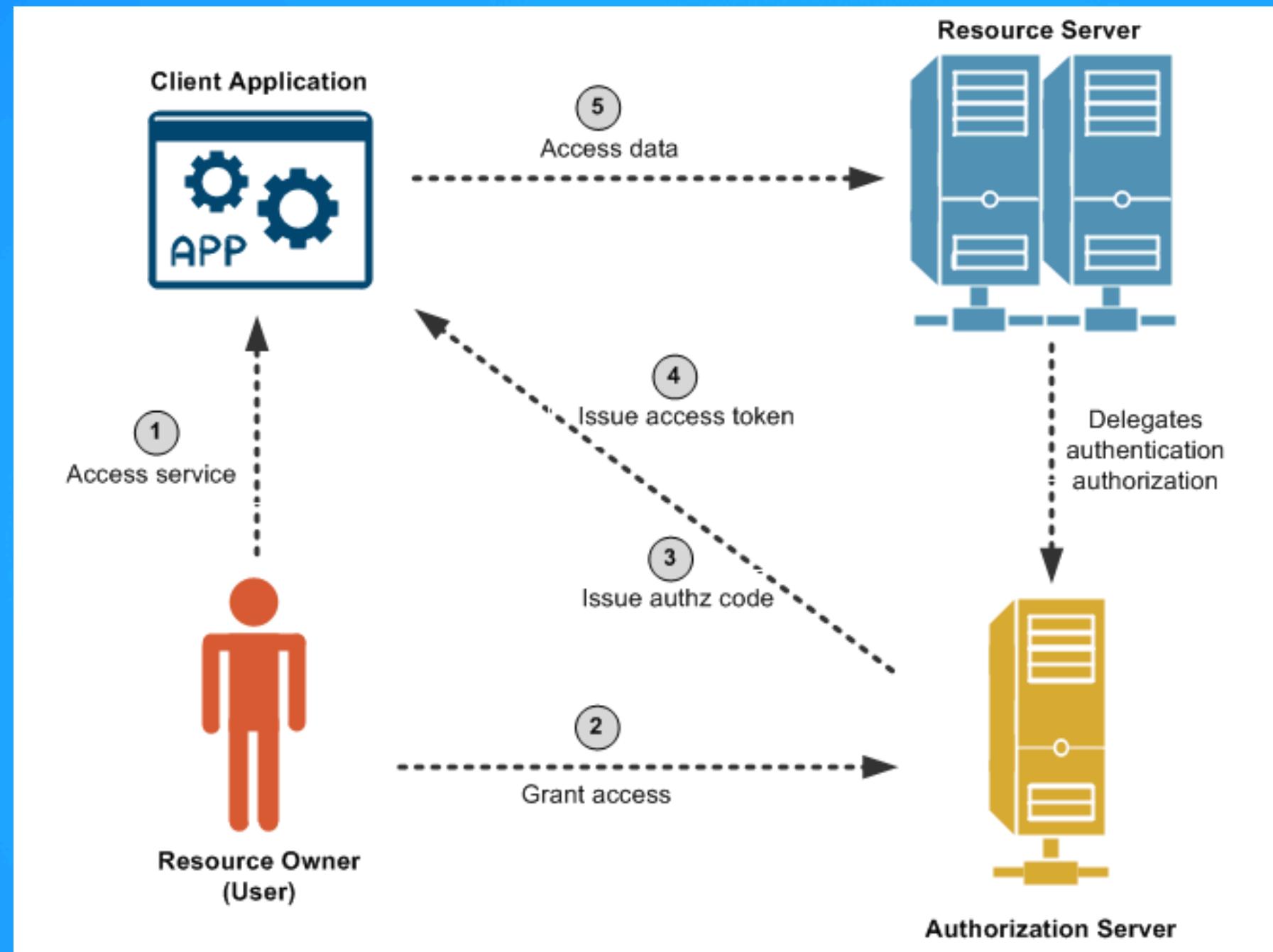
- É quem guarda os dados protegidos do usuário
- Libera quando recebe um token de acesso

Fluxo do OAuth

Como o OAuth funciona



Como o OAuth funciona



Vulnerabilidades OAuth

OAuth - Vulnerabilidades

Embora o OAuth seja relativamente seguro, uma implementação inadequada pode deixar o usuário vulnerável a ameaças.

As vulnerabilidades (geralmente) não surgem de falhas no protocolo, mas sim na sua aplicação e configuração.

É essencial saber reconhecer os padrões de implementação inseguros para proteger o sistema.

Principais vulnerabilidades

Redirect URI
não validado

Uso de
Implicit Flow

Falta de state no
Authorization Code
Flow

Troca de código
sem PKCE

Como saber se uma aplicação usa OAuth ?

OAuth

- A fim de identificar se uma aplicação usa ou não OAuth, existem algumas maneiras de descobrir essa informação

Fluxo de Login*

Redirects na URL

Chamadas no navegador

Headers e Tokens

Documentação/
endpoints
públicos

Comportamento
do Logout

Casos de exploração

Casos de exploração

Microsoft

- "Phishing com OAuth"
- APT29
- Engenharia social com pessoas de cargo alto

Google

- Endpoint OAuth não documentado
- "MultiLogin"
- Sequestro de sessões de usuários

Magalu

- Erro de implementação
- Erro expôs as "chaves de API" do sistema que usava OAuth

Boas práticas (Mitigação)

Boas Práticas

**Validação
Robusta**

**Hashing dos
dados de sessão**

**Garantir que o token está ligado ao
`client_id` enviado para o servidor**

Boas Práticas

O segredo do cliente não deve ser exposto

Whitelist de URLs válidas para redirecionamento

Garantir que os códigos de autorização não sejam vazados com carregamentos externos

FIM DA APRESENTAÇÃO

