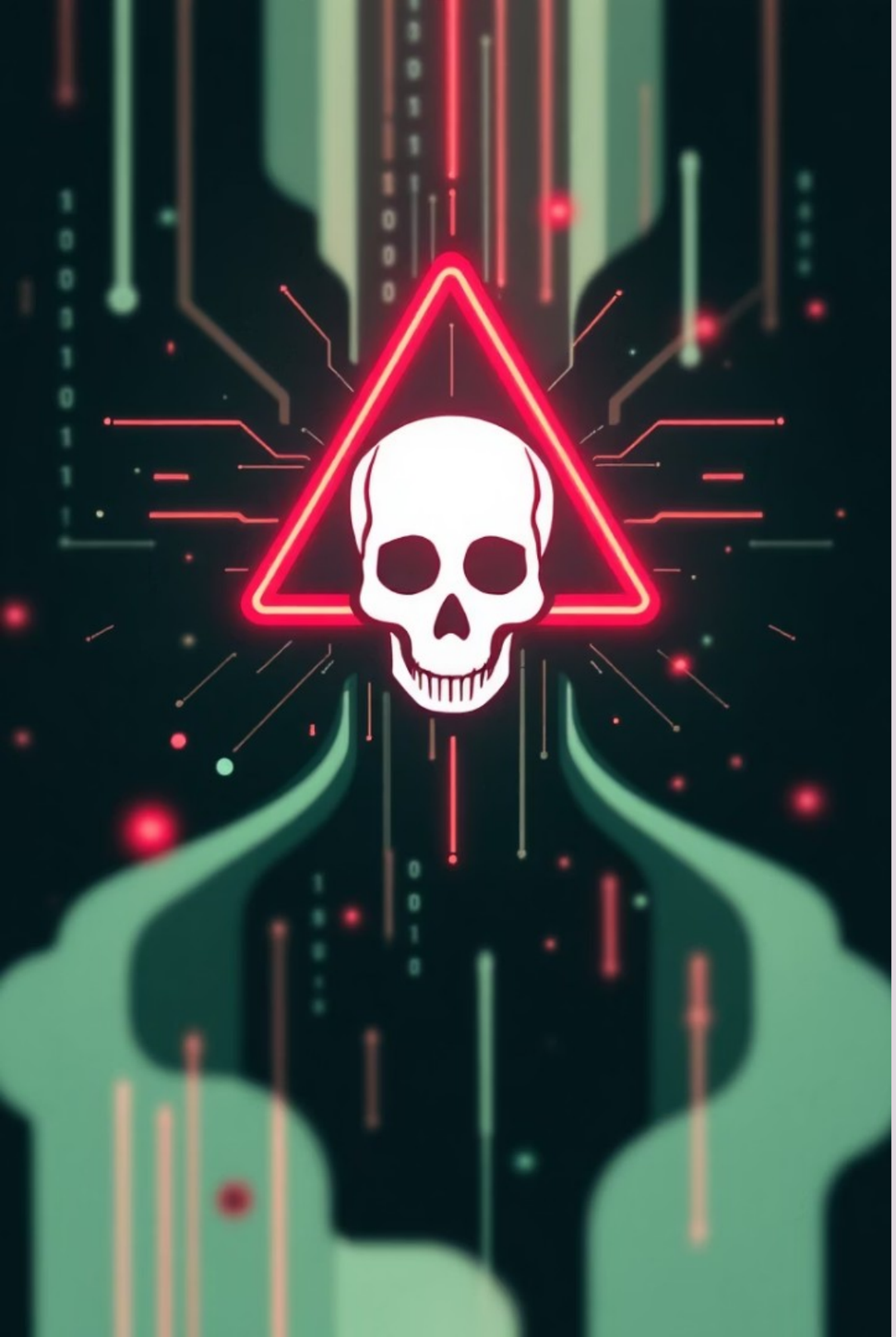
Live JWT

por Thiago Leite e Carvalho

Conteúdo

- Segurança de aplicações (web)
- O que é autenticação e autorização?
- Principais tipos de protocolo de autenticação
- Token: O que é? e Tipos
- JWT
- Exemplo em Spring (sem SpringSecutity)



Segurança de aplicações (web)

Acesso Não Autorizado

Pode levar à exposição de dados confidenciais e sensíveis.

Violações de Dados

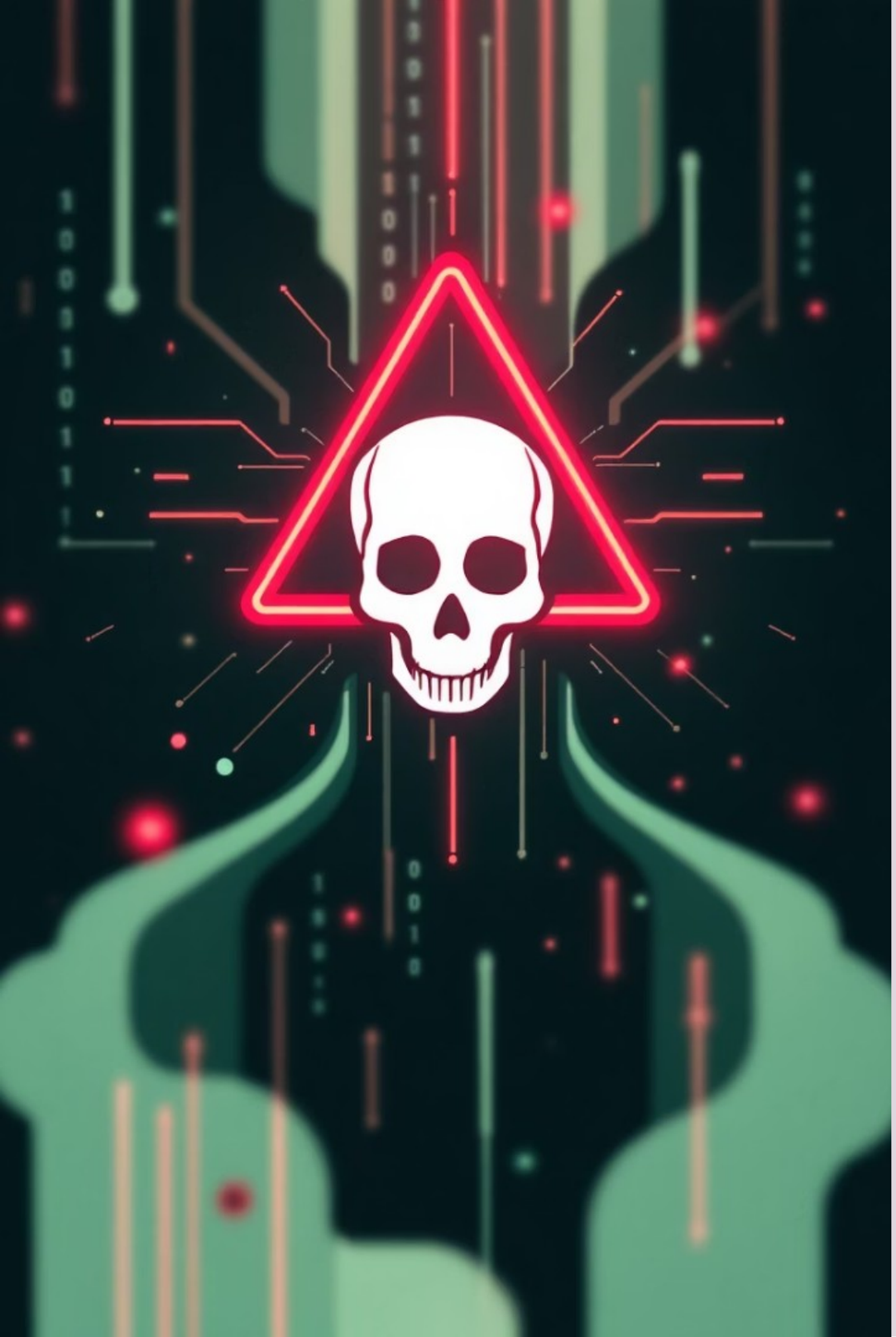
Comprometem a privacidade e integridade das informações.

Ataques de Injeção

Como SQL e comandos, exploram falhas de validação.

Negação de Serviço

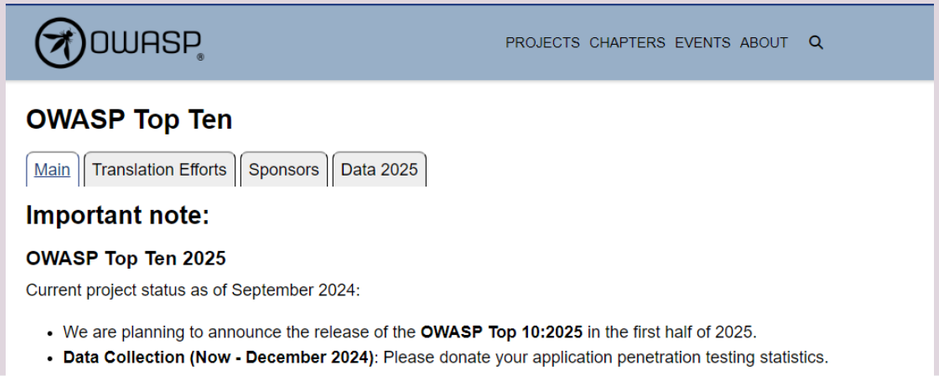
Ataques DoS sobrecarregam APIs, causando interrupções.



Segurança de aplicações (web)

- https://owasp.org/

- https://owasp.org/www-project-top-ten/



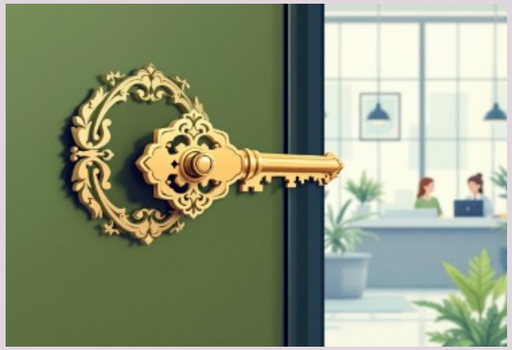
O que é autenticação e autorização?

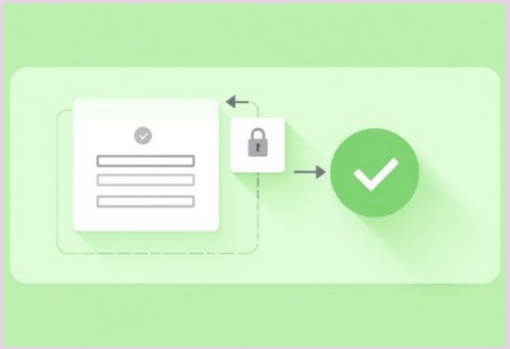
Autenticação

Verifica a identidade de usuários e softwares. É o primeiro passo e garante que apenas entidades legítimas interajam com a API.

Autorização

Respeita níveis de acesso e permissões, quais impedem uso indevido. Assegura que usuários acessem apenas o que lhes é permitido.





Protocolos de autenticação.

- Kerberos
- OpenID Connect
- SSH
- Basic Authentication
- LDAP
- OAuth 2.0

O que é um token?

String de dados que permite que um usuário acesse recursos de um software sem ter que inserir suas credenciais de login a cada vez.

Tipos de token

- Opaco
- JWT

Opaco

ory_at_JGhESDjKfHMQ8Wcy0cC3.hIQxGmX37ydn8WmKAnlD3U

JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

Resumo

Característica	Opaco	JWT
Armazenamento de Dados	No servidor	No próprio token
Tamanho	Menor	Maior
Validação	Requer consulta ao servidor	Pode ser validado localmente
Revogação	Mais fácil	Mais difícil
Segurança	Potencialmente mais seguro (sem vazamento de dados)	Assinado para garantir integridade

O que é JWT?

JWT(Json Web Token) é um token baseado no padrão aberto RFC 7519. Contém todas as informações necessárias, sem a necessidade de consultas ao banco. Permite enviar atributos (claims) sobre a entidade ou o token.

Estrutura do JWT

Header

Contém o tipo do token (JWT) e o algoritmo de assinatura (ex: HS256).

```
base64enc({
    "alg":  "HS256",
    "typ":  "JWT"
})
```

Payload

Dados (claims) da entidade. Nunca inclua segredos aqui.

```
base64enc({
      "iss": "toptal.com",
      "exp": 1426420800,
      "company": "Toptal",
      "awesome": true
})
```

Signature

Verifica a integridade e autenticidade do token.

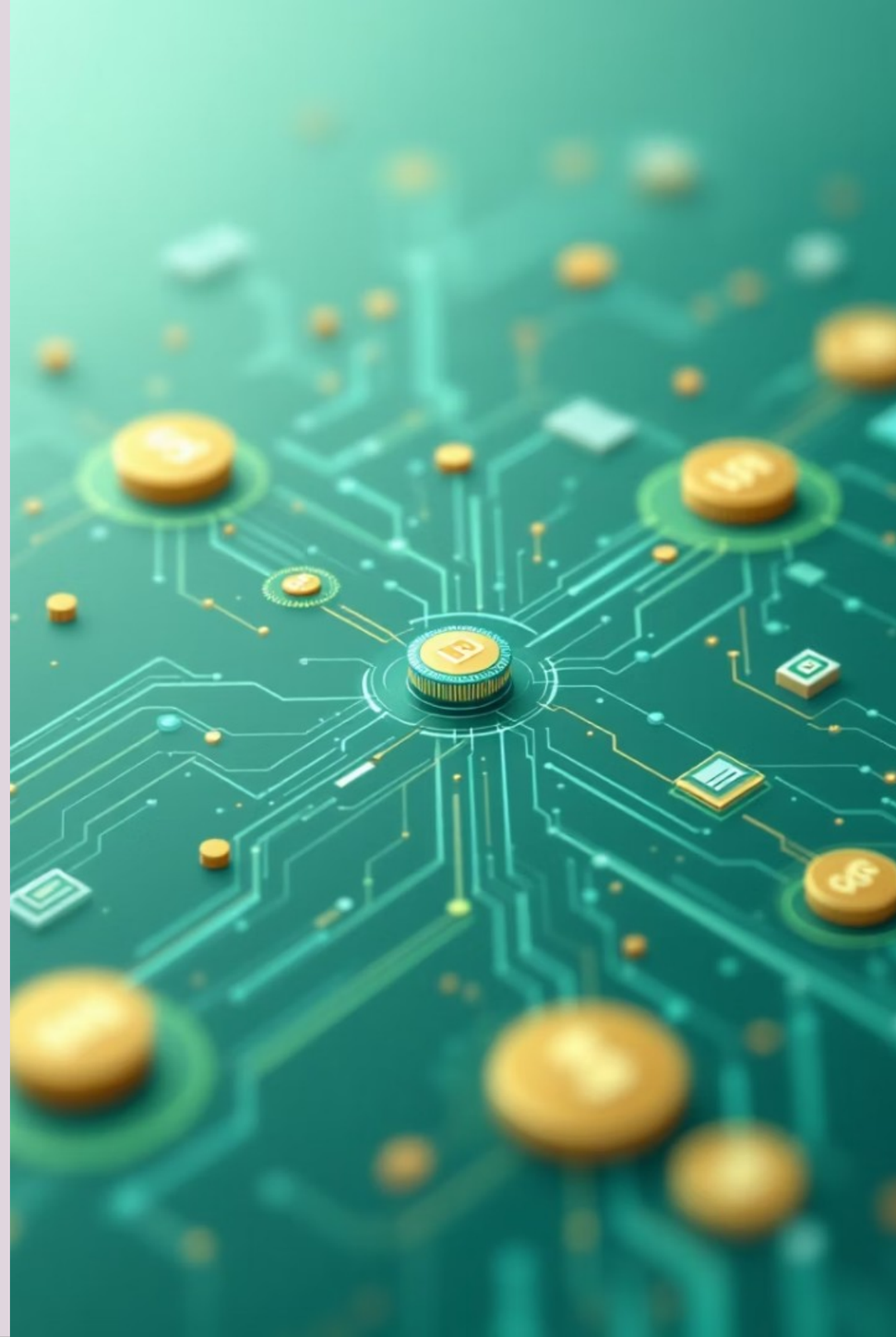
```
HMACSHA256(
 base64enc(header)
 + '.' +,
 base64enc(payload)
 , secretKey)
```

JWT

Estrutura do JWT

Payload

Sigla	Descrição	Objetivo
iss	Issuer	Identificar o emissor do token
sub	Subject	Identificar o solicitante do token
aud	Audience	Similar ao subject
exp	Expiration	Tempo de expiração
nbf	Not before	Indica o momento de inicio de uso
iat	Issued at	Indica o momento de criação
jti	JWT ID	Identificador único



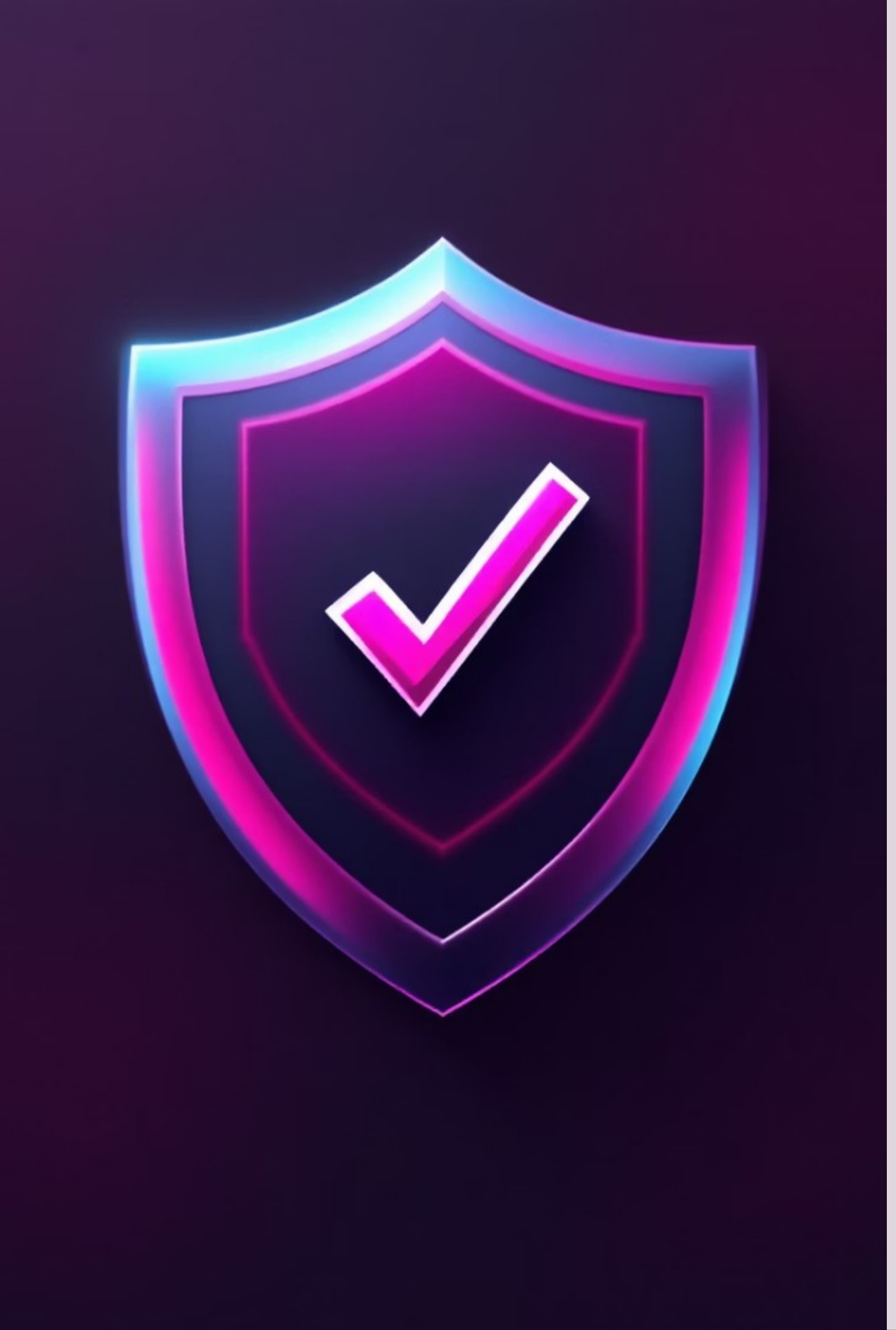
Uso prático em APIs

O JWT é enviado no cabeçalho HTTP: **Authorization: Bearer <token>**.

Reduz a necessidade de consultas ao banco de dados para cada autenticação.

Totalmente compatível com fluxos **OAuth 2.0** e **OpenID Connect**.

Ideal para aplicações **Web** e **Mobile**.



Melhores práticas de segurança

Não coloque dados sensíveis no token

Evite informações confidenciais no payload.

Tokens com expiração curta

Defina um tempo de vida breve para os tokens.

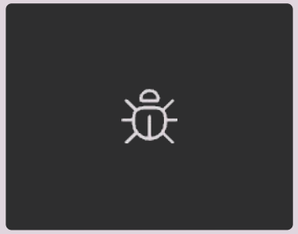
Assinar tokens

Use algoritmos robustos como HMAC/SHA256 ou RSA.

Validar assinatura e expiração

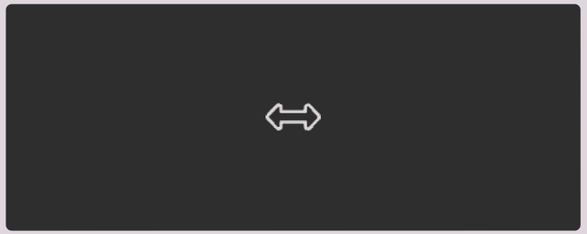
Sempre verifique a validade do token no servidor.

Atenção a armadilhas comuns



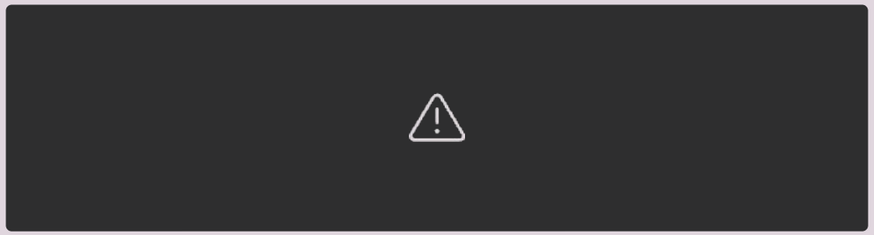
Evitar localStorage

Não armazene JWTs no localStorage devido a riscos XSS.



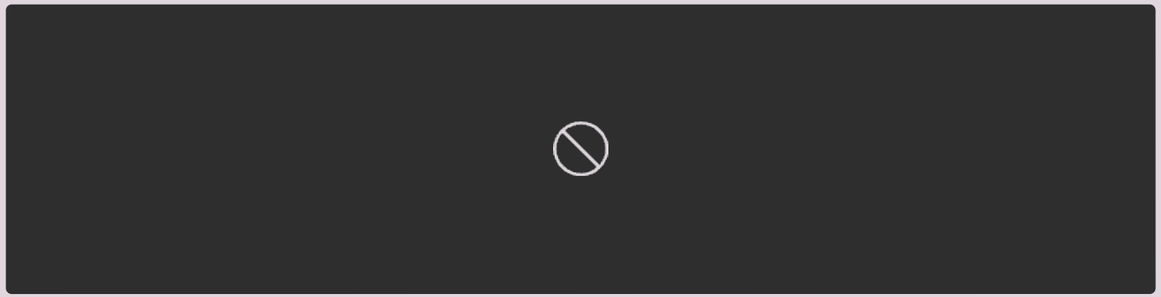
Cuidado com tamanho

Monitore o tamanho do token no cabeçalho (limite ~8KB).



Sem permissões excessivas

Conceda apenas as permissões mínimas necessárias.



Revogar tokens rapidamente

Implemente um mecanismo de revogação para tokens comprometidos.

Prática

Obrigado!

https://www.youtube.com/@thiagoleiteecarvalho

https://www.linkedin.com/in/thiago-leite-e-carvalho-1b337b127/

https://github.com/thiagoleitecarvalho

thiagoleiteecarvalho@gmail.com