

# OWASP TOP 10

## RISCO A RISCO

PREPARE-SE  
PARA O  
PIOR



Gabriel Lucas

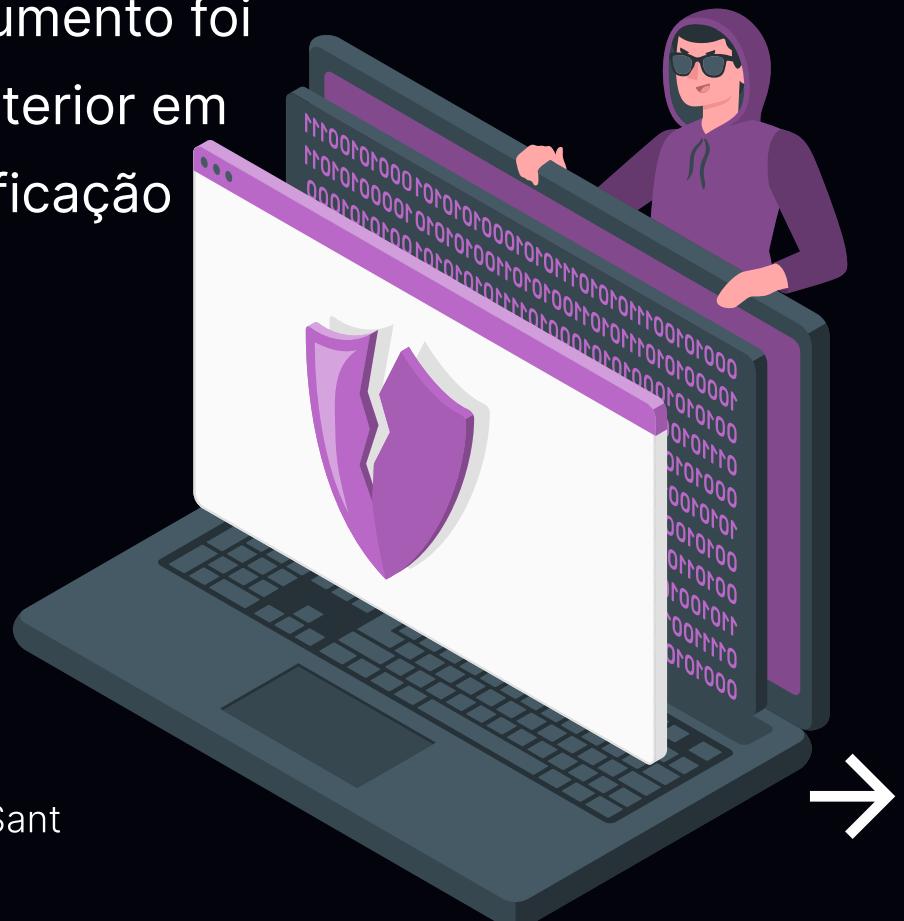
[github.com/GabrielDSant](https://github.com/GabrielDSant)



# Você já ouviu falar do OWASP Top 10 ?

O OWASP Top 10 é um documento de conscientização para desenvolvedores de aplicativos da web. Ele representa um amplo consenso sobre os 10 riscos de segurança mais críticos para aplicativos da web.

A ultima versão do documento foi lançada em 2021 e a anterior em 2017. Seguindo a classificação do documento de 2021, vamos conhecer sobre o risco top 3 ?



**Gabriel Lucas**

[github.com/GabrieIDSant](https://github.com/GabrieIDSant)



## Top 3 - Injection

### Do que se trata ?

Acontece quando dados não confiáveis são enviados propositalmente para um intérprete, no formato de uma consulta ou inserido como parte de um comando. Estas injeções de comandos ou scripts são perigosas e hostis, pois podem direcionar a aplicação a executar comandos que não foram previstos. O que acarreta em acesso a informações de forma não autorizada.



**Gabriel Lucas**

[github.com/GabrieIDSant](https://github.com/GabrieIDSant)

## Um aplicativo é vulnerável a ataques quando:

- Os dados fornecidos pelo usuário não são validados, filtrados ou higienizados pelo aplicativo.
- Consultas dinâmicas ou chamadas não parametrizadas sem escape sensível ao contexto são usadas diretamente no interpretador.
- Dados hostis são usados em parâmetros de pesquisa de mapeamento relacional de objeto (ORM) para extrair registros confidenciais adicionais.
- Dados hostis são usados diretamente ou concatenados. O SQL ou comando contém a estrutura e os dados maliciosos em consultas dinâmicas, comandos ou procedimentos armazenados.



**Gabriel Lucas**

[github.com/GabrieIDSant](https://github.com/GabrieIDSant)

## **Como prevenir que a vulnerabilidade aconteça:**

- A opção preferencial é usar uma API segura, que evite totalmente o uso do interpretador, forneça uma interface parametrizada.
- Use validação de entrada positiva do lado do servidor.
- Para quaisquer consultas dinâmicas residuais, escape caracteres especiais usando a sintaxe de escape específica para esse interpretador.
- Use LIMIT e outros controles SQL nas consultas para evitar a divulgação em massa de registros em caso de injeção de SQL.



**Gabriel Lucas**

[github.com/GabrieIDSant](https://github.com/GabrieIDSant)



**Se você gostou deste conteúdo** ❤

**Se tem algo para me contar** 💬



**Muito obrigado pela atenção!**

**FIM**