

OWASP TOP 10

RISCO A RISCO

PREPARE-SE
PARA O
PIOR



Gabriel Lucas

github.com/GabrieIDSant



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 4 ?



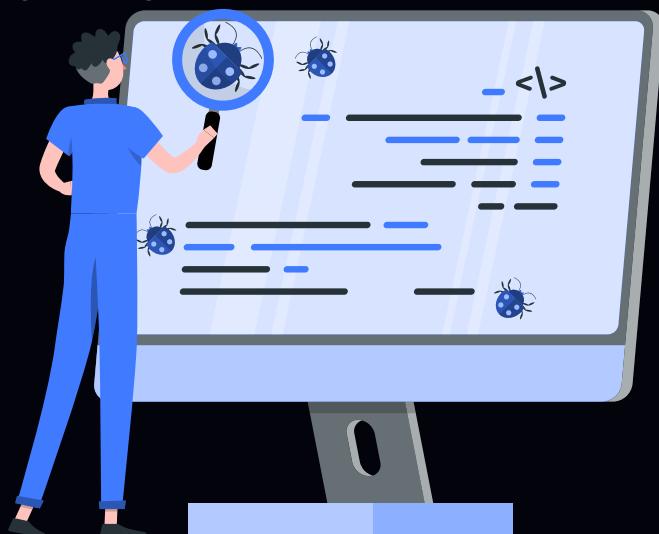
Gabriel Lucas

github.com/GabrieIDSant

Top 4 - Insecure Design

Do que se trata ?

Vulnerabilidades de design inseguro surgem quando desenvolvedores, QA e/ou equipes de segurança não conseguem antecipar e avaliar ameaças durante a fase de design de código. É importante ressaltar que o design inseguro apresenta alto risco, visto que não pode ser corrigido facilmente. Isso acontece pois os controles de segurança para defesa contra os ataques específicos ainda não foram criados. A ideia é que, para evoluir exige mais uso de modelagem de ameaças, padrões e princípios de design seguro e arquiteturas de referência.



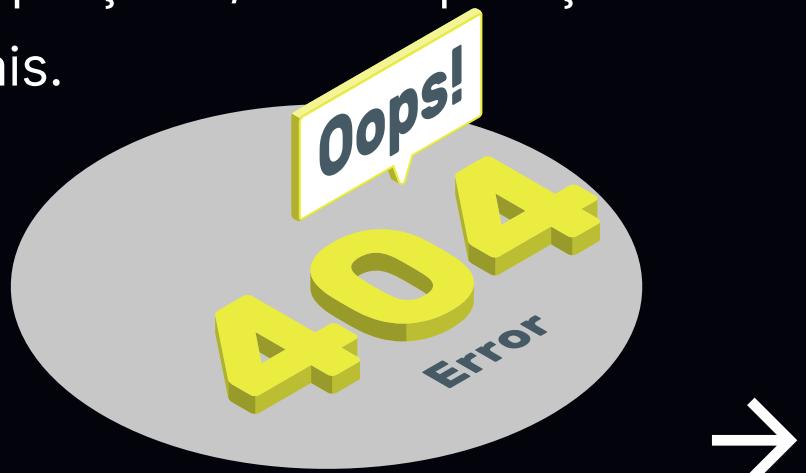
Gabriel Lucas

github.com/GabrieIDSant



Um aplicativo é vulnerável a ataques quando:

- O software emite uma mensagem de erro que contenha informações confidenciais.
- Em um aplicativo que usa um banco de dados SQL sem validação adequada, um invasor pode injetar código malicioso para visualizar dados do banco de dados.
- O app combina dados confiáveis e não confiáveis na mesma estrutura de dados ou mensagem estruturada.
- Embora o app transmita ou salve credenciais de autenticação, ele o faz de maneira insegura, o que o torna vulnerável à interceptação e/ou recuperação não autorizada das credenciais.



Gabriel Lucas

github.com/GabrielDSant



Como prevenir que a vulnerabilidade aconteça:

- Estabeleça e use um ciclo de vida de desenvolvimento seguro com profissionais da AppSec para ajudar a avaliar e projetar controles relacionados à segurança e privacidade
- Estabeleça e use uma biblioteca de padrões de projeto seguros ou componentes prontos para uso de estradas pavimentadas
- Use a modelagem de ameaças para autenticação crítica, controle de acesso, lógica de negócios e fluxos de chaves
- Integre verificações de plausibilidade do front-end ao back-end
- Limitar o consumo de recursos por usuário ou serviço



Gabriel Lucas

github.com/GabrieIDSant



Se você gostou deste conteúdo ❤

Se tem algo para me contar 💬



Muito obrigado pela atenção!

FIM