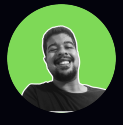
OWASP TOP 10

RISCO A RISCO

PREPARE-SE PARA O PIOR

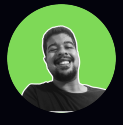


Gabriel Lucas
github.com/GabrielDSant

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 1 ?



Gabriel Lucas
github.com/GabrielDSant

Top 1 - Broken Access Control

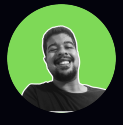
Do que se trata ?

O controle de acesso impõe a política para que os usuários não possam agir fora de suas permissões predefinidas. O broken access control acontece quando essas politicas falham, o que leva geralmente à divulgação, modificação ou destruição de informações por um usuário não autorizado.

Gabriel Lucas
github.com/GabrielDSant

Vulnerabilidades comuns de broken access control incluem:

- Permitir a visualização ou edição da conta de outra pessoa.
- Elevação de privilégio. Atuar como usuário sem estar conectado ou atuar como administrador quando estiver conectado como usuário.
- Acessando API com controles de acesso ausentes para POST, PUT e DELETE.
- Manipulação de metadados, como reproduzir ou adulterar um token de controle de acesso JSON Web Token (JWT), ou um cookie ou campo oculto manipulado para elevar privilégios ou abusar da invalidação de JWT.
- Etc...



Gabriel Lucas
github.com/GabrielDSant

Como prevenir que a vulnerabilidade aconteça:

- Desenvolver um documento com as políticas de acesso da aplicação, mapeando e clarificando todos os objetivos que devem ser atingidos.
- Evitar que simples mudanças de parâmetros (IDs, por exemplo) permitam que um usuário autenticado passe a referenciar um outro usuário.
- Garantir que URLs destinadas a usuários privilegiados não possam ser acessadas pelos demais usuários.

Gabriel Lucas
github.com/GabrielDSant

Se você gostou deste conteúdo ♡

Se tem algo para me contar 🗨

Muito obrigado pela atenção!

FIM