

OWASP TOP 10

RISCO A RISCO

PREPARE-SE
PARA O
PIOR



Gabriel Lucas

github.com/GabrielDSant

instagram.com/cybersec_sant



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/GabrielDSant

instagram.com/cybersec_sant



Top 6 - Vulnerable and Outdated Components

Do que se trata ?

Essa categoria possui uma relação direta com o grande aumento da utilização de componentes e bibliotecas de terceiros sem a correta validação de segurança, o que pode gerar grandes volumes de vulnerabilidades em aplicações. Essa vulnerabilidade se mostra quando o usuário tem desconhecimento da versão do sistema utilizado, se está atualizado ou não, se varreduras periódicas não são feitas, assim como outras medidas de proteção periódicas.



Gabriel Lucas

github.com/GabrielDSant

instagram.com/cybersec_sant

Você provavelmente está vulnerável quando:

- Se você não conhece as versões de todos os componentes que usa (tanto do lado do cliente quanto do lado do servidor). Isso inclui componentes que você usa diretamente, bem como dependências aninhadas.
- Se o software for vulnerável, sem suporte ou desatualizado. Isso inclui o sistema operacional, servidor de aplicativos/web, sistema de gerenciamento de banco de dados (DBMS), aplicativos, APIs e todos os componentes, ambientes de tempo de execução e bibliotecas.
- Se você não verificar vulnerabilidades regularmente e assinar boletins de segurança relacionados aos componentes que usa.
- Se os desenvolvedores de software não testarem a compatibilidade de bibliotecas atualizadas, atualizadas ou corrigidas.



Gabriel Lucas

github.com/GabrielDSant

instagram.com/cybersec_sant



Como prevenir que aconteça:

Deve haver um processo de gerenciamento de patches para:

- Remova dependências não utilizadas, recursos, componentes, arquivos e documentação desnecessários.
- Faça um inventário contínuo das versões de componentes do lado do cliente e do lado do servidor (por exemplo, estruturas, bibliotecas) e suas dependências usando ferramentas como versões, verificação de dependência OWASP, retire.js etc. Monitore continuamente fontes como Vulnerabilidade e exposições comuns (CVE) e National Vulnerability Database (NVD) para vulnerabilidades nos componentes. Use ferramentas de análise de composição de software para automatizar o processo.
- Obtenha apenas componentes de fontes oficiais em links seguros.



Gabriel Lucas

github.com/GabrielDSant

instagram.com/cybersec_sant



Se você gostou deste conteúdo ❤

Se tem algo para me contar 💬



Muito obrigado pela atenção!

FIM