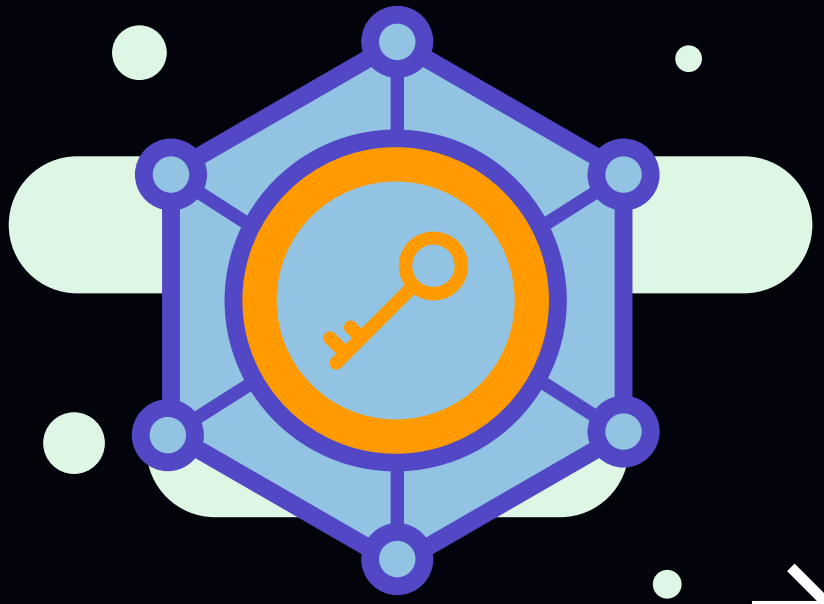
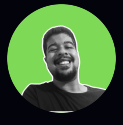
OWASP TOP 10
RISCO A RISCO

PREPARE-SE PARA O PIOR

2



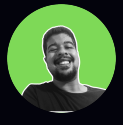


Gabriel Lucas
github.com/GabrielDSant

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 2 ?



Gabriel Lucas
github.com/GabrielDSant

Top 2 - Cryptographic Failures

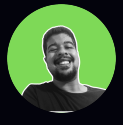
Do que se trata ?

È uma falha que acontece quando processos relacionados a criptografia não funcionam da forma correta.
Esse problema de proteção também pode acarretar na exposição de dados confidenciais, tanto da empresa, quanto de clientes, ou a estruturas do sistema, que ficam comprometidas sem seu “filtro” de acesso.

Gabriel Lucas
github.com/GabrielDSant

Brechas para vulnerabilidade cryptographic failures:

- Algum algoritmo ou protocolo criptográfico antigo ou fraco estar sendo usado por padrão.
- Usar chaves criptográficas padrão, chaves criptográficas fracas serem geradas e reutilizadas, o gerenciamento ou rotação de chaves está ausente.
- As chaves criptográficas serem verificadas nos repositórios de código-fonte.
- O certificado do servidor recebido e a cadeia de confiança estarem indevidamente validados
- A possibilidade de mensagens de erro criptográficas ou informações de canal lateral poderem ser exploradas.
- Etc...



Gabriel Lucas
github.com/GabrielDSant

Como prevenir que a vulnerabilidade aconteça:

- Descarte dados desnecessários o mais rápido possível. Os dados que não são retidos não podem ser roubados.
- Certifique-se de criptografar todos os dados confidenciais em repouso.
- Garantir que algoritmos, protocolos e chaves padrão atualizados e fortes estejam em vigor; use o gerenciamento de chaves adequado.
- Criptografe todos os dados em trânsito com protocolos seguros, como TLS com cifras de sigilo de encaminhamento (FS), priorização de cifras pelo servidor e parâmetros seguros. Imponha a criptografia usando diretivas como HTTP Strict Transport Security (HSTS).
- Etc...

Gabriel Lucas
github.com/GabrielDSant

Se você gostou deste conteúdo ♡

Se tem algo para me contar 🗨

Muito obrigado pela atenção!

Gabriel Lucas
github.com/GabrielDSant

FIM