

# Anatomia de um ataque complexo

A person silhouette is shown from behind, reaching out to interact with a complex network diagram. The diagram consists of numerous interconnected hexagonal nodes, some of which are highlighted in blue and green, and are connected by a web of thin, light-colored lines. The background is a light gray, and the overall image has a technical, digital feel.

VIDEO REFERENCIA:[HTTPS://VIDEO-BR.CISCO.COM/DETAIL/VIDEO/5620318141001](https://video-br.cisco.com/detail/video/5620318141001)

# Tipo e Técnicas usadas para o ataque

## Ataque de injeção de I-Frame

**No ataque de injeção de IFrame, o cracker insere (injeta) um IFrame escondido e malicioso dentro de um site vulnerável.**

**➡ Assim, sempre que um usuário acessa o site, o navegador carrega também esse IFrame oculto, que aponta para um servidor malicioso.**

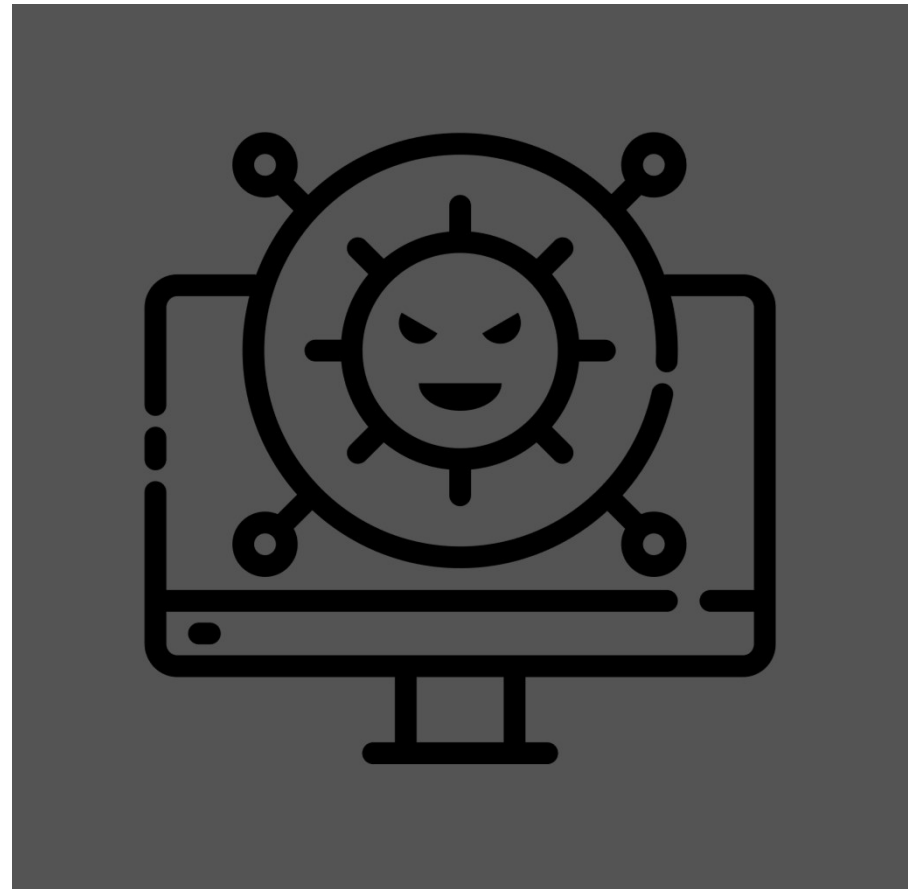


# Vulnerabilidades

## **Vulnerabilidades que permitem injeção de IFrame**

Um ataque de injeção de IFrame acontece principalmente quando o site:

- Não valida/sanitiza entradas (XSS).
- Tem falhas em banco de dados (SQL Injection).
- Usa plugins/CMS desatualizados.
- Permite upload de arquivos sem controle.
- Possui configurações fracas no servidor.
- Não implementa políticas de segurança no navegador (CSP).



# Motivação

**Financeira, a partir do momento que ele teve acesso a todos os documentos e arquivos da empresa aupticon, ele percebeu que poderia ganhar algum dinheiro com aquilo, e foi o que ele fez vendendo todas essas informações por 75 bitcoins.**

