



Fundamentos de Redes e Segurança na Web

Arquitetura TCP/IP

REDE/ACESSO >>> Interface física

INTERNET >>> IP

TRANSPORTE >>> TCP | UDP

APLICAÇÃO >>> HTTP, HTTPS, FTP

Por que é Importante?

Base de toda internet - comunicação universal

Transmissão confiável - garante chegada dos dados

Conectividade global - redes diferentes se comunicam





HTTP vs HTTPS



HTTP - Comunicação Básica

Requisição:

Método (GET, POST, PUT, DELETE)

Caminho do recurso

Cabeçalhos + corpo da mensagem

HTTPS - Comunicação Segura

SSL/TLS: Criptografia na transmissão

Uso obrigatório: Senhas, dados pessoais, transações

Proteção: Impede interceptação e modificação



Vulnerabilidades Críticas - Parte 1



SQL Injection

Ataque: Código SQL malicioso em formulários

Exemplo: admin'; DROP TABLE usuarios;

Consequência: Controle total do banco de dados

Cross-Site Scripting (XSS)

Ataque: Scripts maliciosos executados no navegador

Tipos: Stored, Reflected, DOM

Consequência: Roubo de sessões e cookies

💡 **Prevenção:** Validação rigorosa + prepared statements + sanitização



Vulnerabilidades Críticas - Parte 2

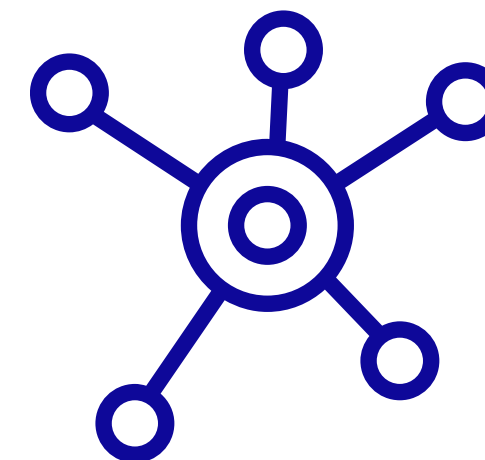
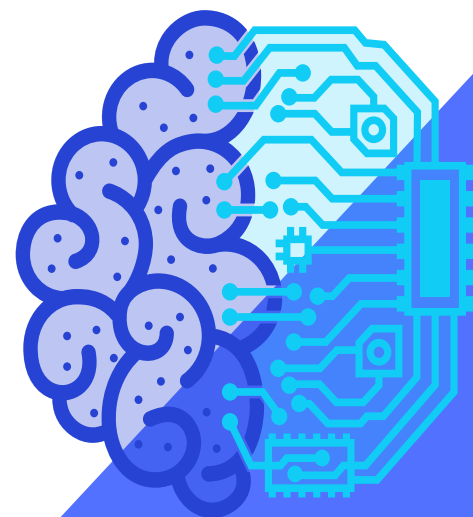


CSRF (Cross-Site Request Forgery)

Ataque: Ações forçadas em usuários autenticados

Cenário: Link malicioso → transferência bancária automática

Condição: Usuário logado + ação não verificada



DoS/DDoS

DoS: Ataque único esgotando recursos do servidor

DDoS: Ataque coordenado usando botnet
Resultado: Serviço completamente indisponível.

💡 **Prevenção:** Tokens CSRF + rate limiting + verificação dupla





Boas Práticas de Segurança

Autenticação Forte

Senhas robustas: 12+ caracteres, múltiplos tipos

MFA: Algo que sabe + tem + é

Rate limiting: 5 tentativas → bloqueio 15min



Validação e Sanitização

Zero Trust: Nunca confiar em dados externos

Dupla validação: Cliente (UX) + Servidor (segurança)

Whitelist: Preferir valores permitidos

Criptografia

Simétrica: AES-256 (rápida, grandes volumes)

Assimétrica: RSA-2048 (troca inicial de chaves)



Obrigado!

