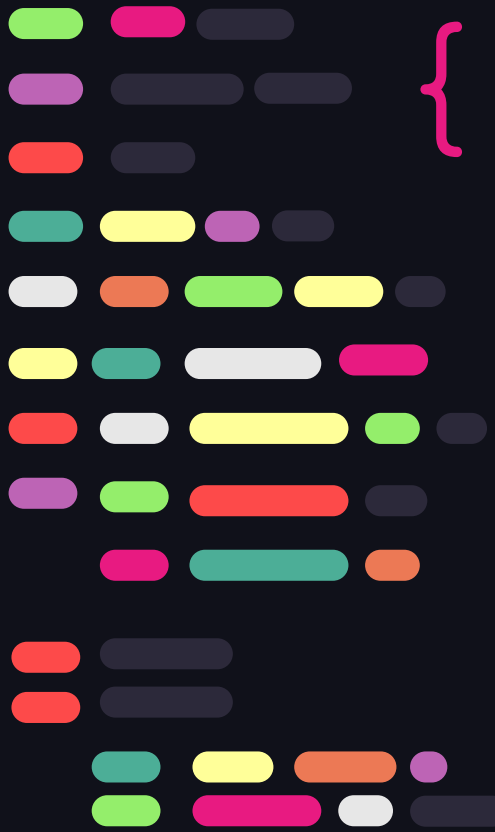


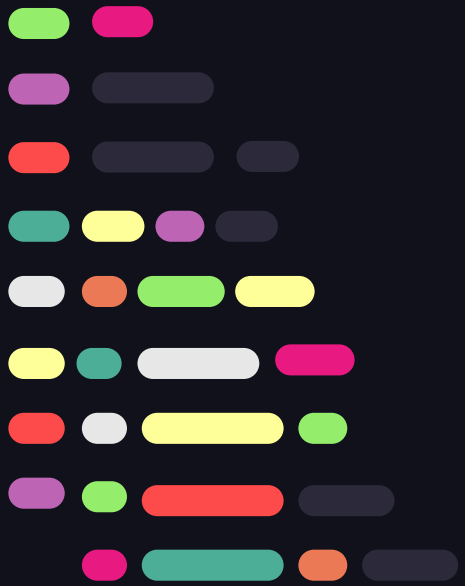
Guia com medidas protetivas de um site

Gabriel Vitor Siqueira Costa, Gustavo Ferreira França de Abreu, Gustavo Teixeira Rocha Araujo, João Victor Teixeira Gomes Cota, Luiz Guilherme Vilaça de Moraes, Rafael Colombo Fernandes Silva

Introdução

A segurança de sites é essencial para proteger informações na era digital. Com o aumento dos ataques cibernéticos, é necessário implementar medidas que garantam confiabilidade, integridade e disponibilidade dos sistemas.

Ataques mais comuns



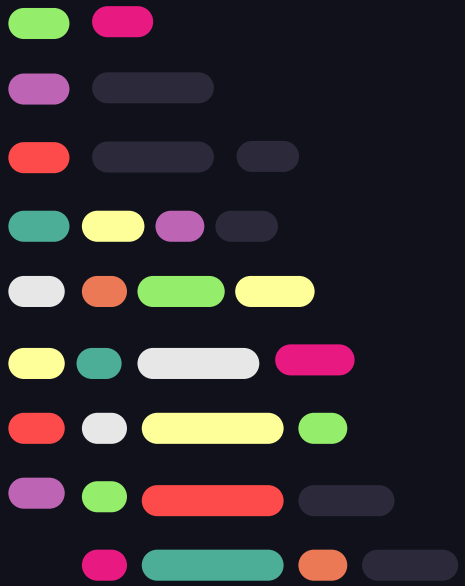
01 Sql Injection

O invasor envia comandos maliciosos ao banco por meio de formulários ou URLs. Pode ler, alterar ou apagar dados. Exemplo: inserir ' OR '1'='1 no login para enganar a autenticação, fazendo o sistema aceitar a entrada como verdadeira.

02 Brute Force

Um programa testa milhares ou milhões de senhas automaticamente até encontrar a correta.

Ataques mais comuns

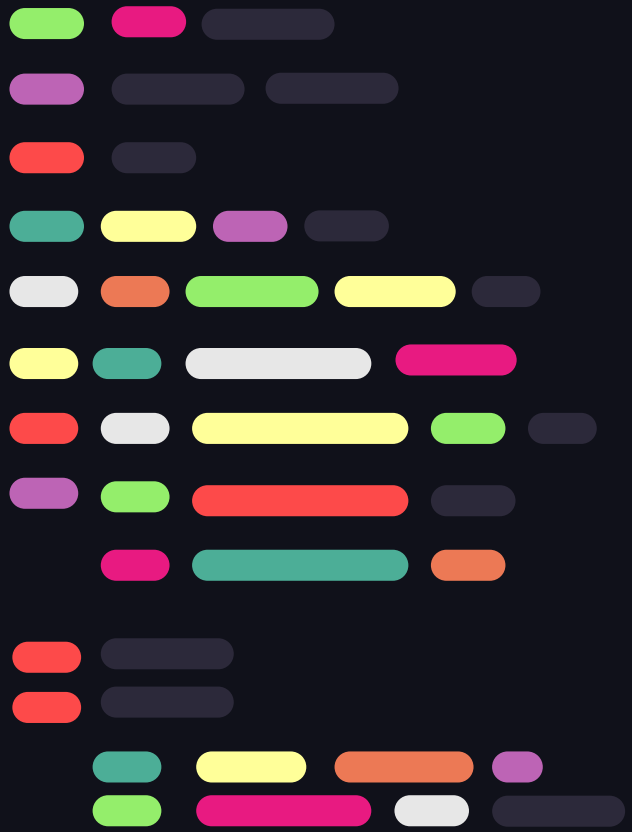


03 Trojan Horse (cavalo de troia)

Malware que se disfarça de programa legítimo para enganar o usuário. Após instalado, permite controle do sistema, roubo de dados ou instalação de outros vírus.

04 Phishing

Ataque onde o criminoso se passa por uma pessoa ou empresa confiável.
Objetivo: roubar senhas, dados bancários, códigos de verificação e outras informações sensíveis.



Como se previnir

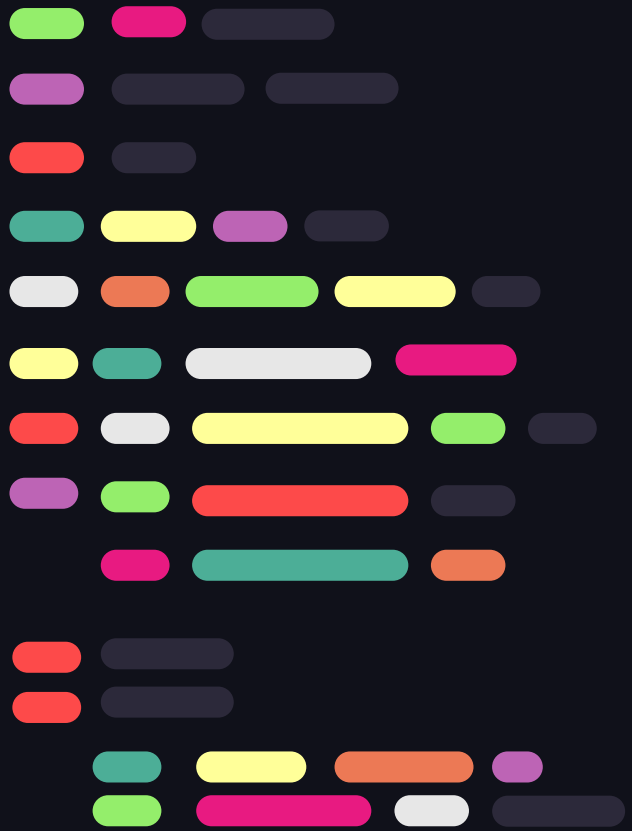
Prevenção: SQL Injection

Uso de consultas preparadas que separam o comando SQL dos dados do usuário.

Impede que entradas maliciosas sejam interpretadas como código SQL.

Prevenção: Trojan Horse - Verificação

Técnica Manter o antivírus sempre atualizado para detectar e remover trojans antes que causem danos ao sistema.



Como se previnir

Prevenção: Brute Force - Rate Limiting
Limita o número de tentativas de login em um curto período. Reduz a chance de programas testarem milhares de senhas seguidas. Exemplo de bloqueios progressivos após tentativas incorretas:

1ª e 2ª → permite continuar

3ª → aviso

4ª → bloqueio de 5 min

5ª → bloqueio de 30 min

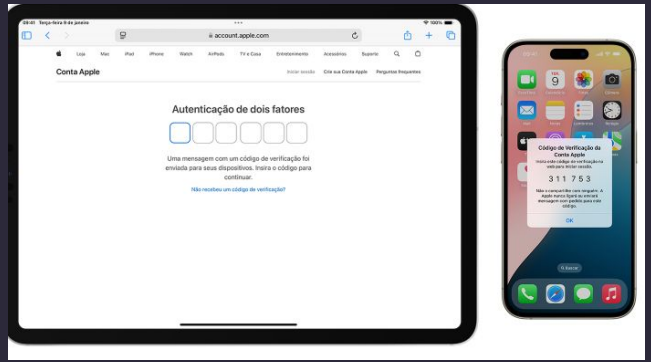
6ª → bloqueio de 24 h

Como se previnir

Prevenção: Phishing - Autenticação de Dois

Fatores (2FA) Exige dois elementos: algo que você sabe (senha) + algo que você possui (código temporário) ou é (biometria).

Mesmo que a senha seja roubada, o atacante não consegue acessar a conta sem o segundo fator.



Conclusão

A prevenção geral depende diretamente da educação do usuário, pois, mesmo com sistemas avançados de proteção, ele ainda é o elo mais vulnerável. A falta de atenção pode resultar em cliques em links maliciosos, downloads perigosos e exposição de informações sensíveis. Por isso, combinar boas práticas de uso com medidas técnicas é fundamental para fortalecer a segurança digital. Manter sistemas atualizados, reconhecer mensagens suspeitas, evitar anexos desconhecidos e utilizar conexões seguras (HTTPS) são ações essenciais no dia a dia. Assim, concluímos que a união entre a educação do usuário e sistemas confiáveis cria um ambiente muito mais protegido e resistente a ataques.