

TRANCA AS 5 PORTAS

DO *teu app*

Checklist de antes de publicar, com o pedido pronto pra IA consertar. Só testa o teu próprio app.

Nenhum conserto exige ser programador. Exige saber o que *pedir*.

[] 01 / 05

OPENAI · ANTHROPIC

Chave de API no navegador

Sintoma: a chave que paga a tua IA vai junto com o código do site. Qualquer um copia e gasta no teu cartão.

CHECA EM 1 MINUTO (DICA PRÁTICA)

Abre o teu site, aperta F12, vai em Sources e procura "sk-" em todos os arquivos.

CONCERTO: PEDE ASSIM

"Procure no meu projeto qualquer chave de API que vá para o navegador e mova para o servidor, em variável de ambiente."

Fonte: OpenAI, Best Practices for API Key Safety · Anthropic, API Key Best Practices

[] 02 / 05

SUPABASE

Banco sem RLS (Supabase)

Sintoma: sem a regra "cada um vê só o que é seu", quem tem o endereço do projeto lê, edita e apaga a tabela.

CHECA EM 1 MINUTO

No painel do Supabase, abre Advisors > Security. Ele aponta tabela pública sem RLS.

CONCERTO: PEDE ASSIM

"Liste as tabelas do meu Supabase sem RLS e escreva as regras para cada usuário ver e editar só os próprios dados. Me mostre antes de aplicar."

Atenção: a chave publicável (antiga "anon") pode ir pro navegador só porque o RLS protege as tabelas. A chave secreta (antiga "service_role") nunca.

Fonte: Supabase Docs, Row Level Security e Database Linter 0013

[] 03 / 05

UBUNTU · OWASP

Servidor sem firewall

SÓ SE TU TEM VPS

Sintoma: o firewall do Ubuntu vem desligado e todas as portas ficam à mostra.

CHECA EM 1 MINUTO, NO TERMINAL DO SERVIDOR

```
sudo ufw status verbose
```

Se aparecer "inactive", está desligado.

CONSERTO: PEDE ASSIM

```
"Configure o firewall do meu servidor: libere só 22, 80 e 443, começando pela 22."
```

Cuidado: libera a 22 ANTES de ligar o firewall, senão tu te tranca pra fora do servidor.

Quem publica em Vercel, Netlify ou Lovable não mexe nisso.

Fonte: Ubuntu Server Docs, Firewalls (UFW) · OWASP Top 10:2025 A02

[] 04 / 05

OWASP

Formulário que aceita tudo (SQL injection)

Sintoma: alguém escreve um comando no lugar do nome e o banco obedece.

CHECA EM 1 MINUTO: PERGUNTA PRA IA QUE FEZ O APP (DICA PRÁTICA)

```
"Este projeto usa consulta parametrizada ou ORM em todas as consultas? Tem validação no servidor?"
```

CONSERTO: PEDE ASSIM

```
"Troque toda consulta montada com texto por consulta parametrizada ou ORM e valide os dados no servidor."
```

Por que no servidor: a validação da tela pode ser pulada.

Fonte: OWASP SQL Injection Prevention Cheat Sheet · OWASP Top 10:2025 A05 · OWASP Input Validation Cheat Sheet

AS 5 DE UMA VEZ

MODELO

Cola no teu agente

```
"Revise meu app procurando 5 portas abertas: chave de API no navegador, tabela sem RLS, servidor sem firewall, consulta sem parâmetro e configuração de teste no ar. Me mostre a lista antes de corrigir."
```

Depois corrige uma por vez.

[] 05 / 05

OWASP

Configuração de teste no ar

Sintoma: o ensaio foi pro ar: senha padrão, login desligado, CORS liberado pra qualquer site, segredo de teste.

CHECA ANTES DE CADA PUBLICAÇÃO

- [] senha padrão trocada?
- [] login ligado?
- [] CORS só com o teu domínio?
- [] chaves do ar diferentes das de teste?

CONCERTO: PEDE ASSIM

"Confira senhas padrão, login, CORS e chaves do meu app e me mostre tudo o que ainda está em modo de teste."

Fonte: OWASP Top 10:2025 A02 Security Misconfiguration · OWASP HTML5 Security Cheat Sheet (CORS)

PRA IR *além*

INSECURE DEFAULTS

TRAIL OF BITS

Insecure Defaults OFICIAL

Da Trail of Bits, empresa de segurança. No Claude Code, caça a porta 5 sozinho.

DENTRO DO CLAUDE CODE, UMA LINHA DE CADA VEZ

```
/plugin marketplace add trailofbits/skills  
/plugin install insecure-defaults  
/insecure-defaults:audit
```

Gasta bem mais uso do plano que um comando comum (roda vários agentes).

github.com/trailofbits/skills/tree/main/plugins/insecure-defaults

STRIX

CÓDIGO ABERTO

Strix COMUNIDADE

Teste de invasão feito por IA, código aberto. Precisa de Docker e de uma chave de IA paga.

Só no teu próprio app: testar sistema dos outros sem autorização é crime na maioria dos países.

github.com/usestrix/strix

Quer aprender a construir com segurança, em português?

Lista de espera do **Prosperando com IA**: aliceallgayer.com.br/Lista?de=prosperando