

OFICINA DO BIRUTIA

Testes de segurança em sistemas seus

O Strix usa agentes de IA para testar a segurança da sua própria aplicação e sugerir correções. Só use em sistemas que são seus ou autorizados por escrito.

O Strix (repositório usestrix/strix, licença Apache-2.0, conferido no GitHub) reúne agentes de IA que testam a segurança de uma aplicação como um atacante faria: um reconhece, outro tenta explorar falhas, outro valida se o problema é real. No fim você recebe as vulnerabilidades encontradas, a prova de que existem e a orientação de correção. Segundo a referência, cobre falhas comuns da lista OWASP Top 10 e funciona com sites, APIs e código-fonte.

Regra principal

Use somente em sistemas que são seus ou que você tem autorização por escrito para testar. Testar sistema de terceiros sem permissão é crime em muitos países, inclusive no Brasil. Não aponte a ferramenta para sites de clientes, da empresa onde você trabalha ou de qualquer pessoa sem autorização formal.

O que você precisa

Docker em funcionamento e uma chave de API de um provedor de IA (que gera custos). No Windows, o projeto indica o WSL. Confira as instruções atuais na documentação oficial (docs.strix.ai) e leia o instalador antes de executar qualquer comando baixado da internet.

Passo a passo

1. Prepare um ambiente de teste

O ideal é testar uma cópia do seu sistema, não o ambiente em produção.

2. Instale e configure pela documentação oficial

Defina o provedor de IA e guarde a chave de forma segura.

3. Aponte para o seu próprio projeto

Use o comando da documentação, indicando a pasta do seu código ou o endereço do seu ambiente de teste.

4. Leia o relatório

Comece pelas falhas mais graves. Aplique as correções e rode de novo para confirmar que fecharam.

Pedido para entender o relatório

Pedido: Priorizar correções

> Aqui está o relatório de segurança da minha aplicação: [cole o relatório sem chaves nem dados reais]. Explique cada falha em português simples, diga o risco real, proponha a correção mais simples e ordene o que corrigir primeiro. Aponte o que precisa de revisão de um especialista.

Avisos

Nunca use em sistemas de terceiros sem autorização por escrito.

Teste em ambiente separado e com cópia dos dados; evite dados reais de clientes.

Os agentes podem executar ações no sistema testado: mantenha backup.

O resultado da IA é um apoio: falhas graves merecem revisão de um profissional de segurança.

Checklist final

[ ] O sistema é meu ou autorizado por escrito
[ ] Testei em ambiente separado, com backup
[ ] Li o instalador antes de rodar
[ ] Corrigi e testei de novo

Quem fez

Strix, de usestrix (github.com/usestrix/strix). Guia escrito pela Oficina do BirutIA, com apoio do material de Guilherme Morais (@guilhermemorais.ia), consultado como referência.

Oficina do BirutIA - material gratuito. Conferido em 28/10/2026. As ferramentas de IA mudam com frequência.

Quer automações para a sua empresa?
O BirutIA e a MLM Produções podem ajudar.
www.mlmproducoes.com.br