

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Injeção de SQL e XSS em palavras simples: o que pedir a quem programa o seu site

Segurança

CÓDIGO

RLX-MZ-KB-1722

VERSÃO

v2026.10.15

PAÍS · IDIOMA

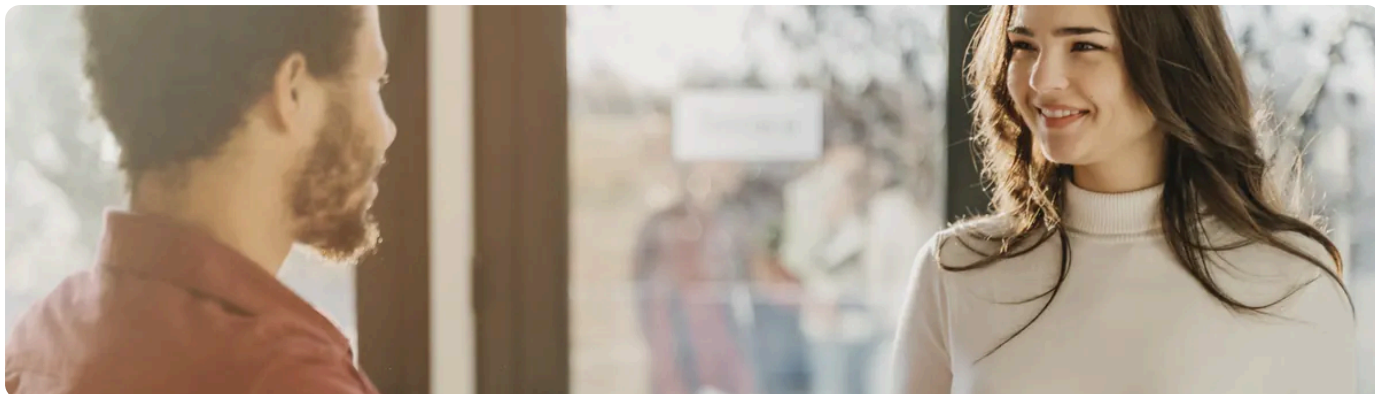
Moçambique · Português

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

<https://www.meu.interweb.co.mz/knowledgebase/1722>



A resposta curta: a **injeção de SQL** e o **XSS** são dois dos ataques mais antigos a sites, e continuam a funcionar porque nascem de um mesmo descuido: **confiar no que o visitante escreve**. Se o seu site é feito com WordPress e plugins mantidos, o risco é de quem os mantém, e o seu trabalho é atualizar. Se é feito por medida, as duas perguntas deste artigo são para quem o programou.

Injeção de SQL

Um formulário de pesquisa mete o que o visitante escreve dentro de uma pergunta à base de dados. Se o programa a monta juntando texto, o visitante pode escrever algo que **muda a própria pergunta**, por exemplo para ver dados de outros clientes ou apagar tabelas. A defesa é simples e conhecida: **consultas preparadas**, que mantêm a pergunta e os dados separados. Em PHP, com o PDO:

```
$st = $pdo->prepare("SELECT * FROM clientes WHERE email = ?");  
$st->execute([$email]);
```

O que nunca se deve fazer é juntar a variável ao texto da consulta.

XSS (cross-site scripting)

Se uma página mostra o que alguém escreveu (um comentário, um nome) sem o proteger, esse alguém pode escrever **código** que passa a correr no navegador de quem visita a página: roubar uma sessão, mostrar um formulário falso, redirecionar. A defesa é **escapar tudo o que se mostra**. Em PHP:

```
echo htmlspecialchars($nome, ENT_QUOTES, 'UTF-8');
```

No WordPress, as funções `esc_html()` e `esc_attr()` fazem o mesmo.

Perguntas para fazer a quem programa

1

«As consultas à base de dados usam parâmetros (consultas preparadas)?» Se a resposta for hesitante, é um sinal.

2

«**Tudo o que se mostra na página é escapado?**» Inclui o que vem de formulários, do endereço e da base de dados.

3

«**Os formulários validam o que recebem, no servidor?**» A validação no navegador pode ser contornada. Veja **Um formulário seguro e sem spam**.

4

«**O utilizador da base de dados só tem os privilégios de que precisa?**» Veja **Criar um utilizador da base de dados e dar-lhe os privilégios certos**.

5

«**Quem atualiza as bibliotecas e o PHP?**» Muitos ataques usam falhas conhecidas de versões antigas.

O que a hospedagem faz e não faz

Uma firewall de aplicações web, como o ModSecurity, bloqueia muitos pedidos que parecem estes ataques. É uma rede de segurança, e não uma desculpa para programar mal: veja **ModSecurity e firewalls de aplicações web**. Os cabeçalhos de segurança também ajudam a limitar o estrago de um XSS: **Cabeçalhos de segurança**.

No WordPress, a causa mais comum é um plugin desatualizado ou abandonado, e não o núcleo. Veja Plugin abandonado ou PHP antigo. Se o site já foi atacado e o e-mail foi atingido, comece por **A sua conta de e-mail foi pirateada**; em qualquer caso, analise o site.

Tem um site feito por medida e quer saber se lhe devia perguntar alguma coisa? Abra um pedido a descrever como foi feito.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

[Um formulário seguro e sem spam: honeypot, captcha e validação](#)

[ModSecurity e firewalls de aplicações web: o que fazem e o que fazer quando uma o bloqueia](#)

[Cabeçalhos de segurança: o que fazem e como os pôr no .htaccess](#)

[Plugin abandonado ou PHP antigo: como ver os riscos no seu site](#)



Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

Interweb Moçambique

RLX Holdings, S.A. • Grupo RLX Holdings

NUIT 401 191 607

NUEL 105 045 974

CAE 62022

SEDE Bairro 7 de Setembro
Vilankulo 1304 • CEP 0411-02, Inhambane, Moçambique

CONTACTOS info@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz

HORÁRIO 2ª. à 6ª. Feira - 08 à 16 Horas
Sábado & Domingo - Fechado