

KNOWLEDGE BASE · PUBLIC DOCUMENT

SQL injection and XSS in plain words: what to ask your developer

Security

CODE

RLX-MZ-KB-1722

VERSION

v2026.10.15

COUNTRY · LANGUAGE

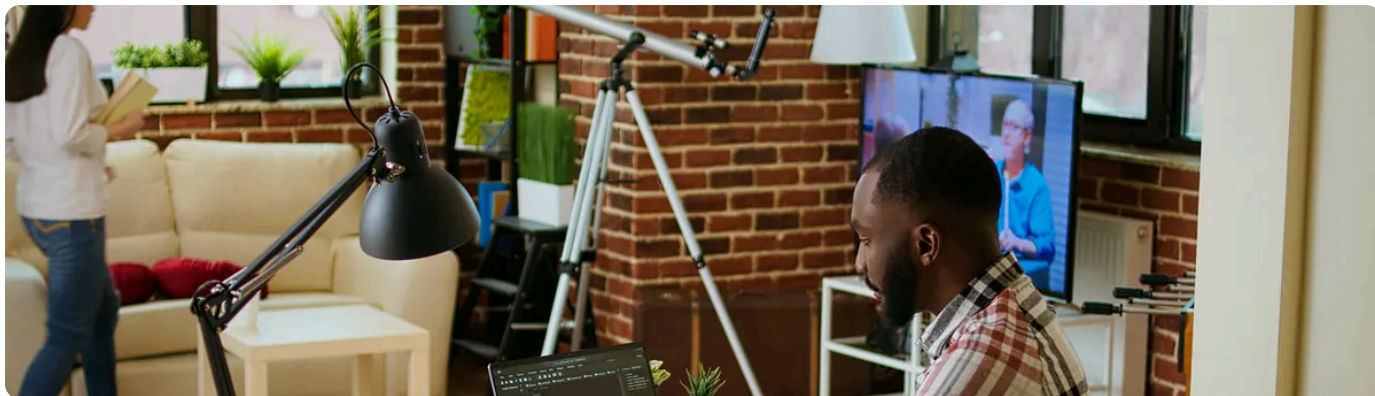
Mozambique · English

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

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



The short answer: SQL injection and XSS are two of the oldest attacks on websites, and they still work because they come from the same oversight: **trusting what the visitor types**. If your site is built with WordPress and maintained plugins, the risk is with whoever maintains them, and your job is to update. If it is custom-built, this article's questions are for whoever programmed it.

SQL injection

A search form puts what the visitor types inside a question to the database. If the program builds it by joining text, the visitor can type something that **changes the question itself**, for example to see other customers' data or delete tables. The defence is simple and well known: **prepared statements**, which keep the question and the data apart. In PHP, with PDO:

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

What you must never do is join the variable to the query text.

XSS (cross-site scripting)

If a page shows what someone wrote (a comment, a name) without protecting it, that someone can write **code** that then runs in the browser of whoever visits the page: stealing a session, showing a fake form, redirecting. The defence is to **escape everything you display**. In PHP:

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

In WordPress, the functions `esc_html()` and `esc_attr()` do the same.

Questions to ask your developer

1

“Do the database queries use parameters (prepared statements)?” If the answer is hesitant, that is a sign.

2

“Is everything displayed on the page escaped?” That includes what comes from forms, from the address and from the database.

3

“Do the forms validate what they receive, on the server?”

Validation in the browser can be bypassed. See **A website form that is safe and spam-free**.

4

“Does the database user have only the privileges it needs?” See **Creating a database user and giving it the right privileges**.

5

“Who updates the libraries and PHP?” Many attacks use known flaws in old versions.

What the hosting does and does not do

A web application firewall, such as ModSecurity, blocks many requests that look like these attacks. It is a safety net, not an excuse for poor programming: see **ModSecurity and web application firewalls**. Security headers also help limit the damage of an XSS: **Security headers explained**.

In WordPress, the most common cause is an outdated or abandoned plugin, not the core. See **An abandoned plugin or an old PHP version**. If the site has already been attacked, and the e-mail was hit, start with **Your e-mail account has been hacked**; either way, scan the site.

Have a custom-built site and want to know whether you should ask something? Open a ticket describing how it was built.

[Open a support ticket](#)

SEE ALSO

[A website form that is safe and spam-free: honeypot, captcha and validation](#)

[ModSecurity and web application firewalls: what they do, and what to do when one blocks you](#)

[Security headers explained: what they do and how to add them in .htaccess](#)

[An abandoned plugin or an old PHP version: how to spot the risks on your site](#)



Online version of this document

Interweb is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

Interweb Mozambique

RLX Holdings, S.A. • Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 • CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed