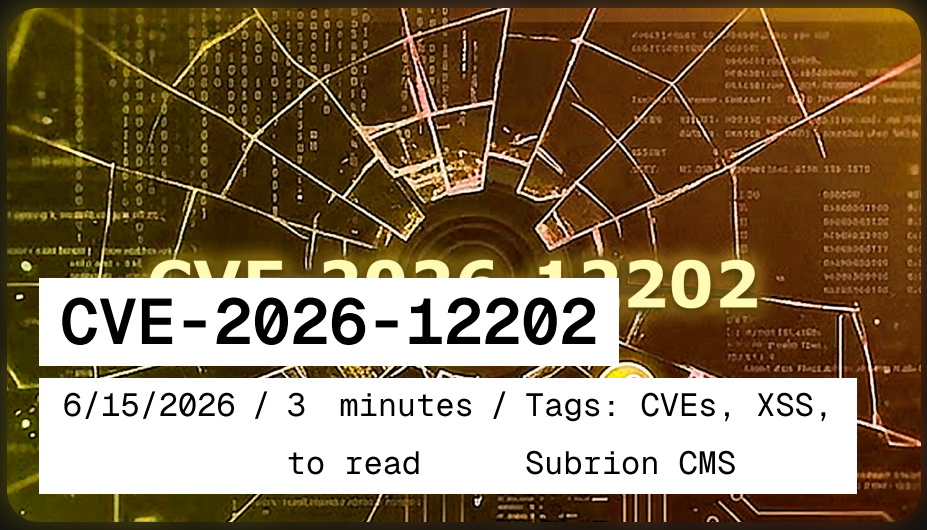
Socials

- GitHub
- LinkedIn
- Instagram
- Gmail



CVE-2026-12202

6/15/2026 / 3 minutes to read / Tags: CVEs, XSS, Subrion CMS

Introduction

While exploring Subrion CMS system, I discovered a stored XSS vulnerability in the `Blocks Page` endpoint. The `CSS class name` parameter, allows the injection of malicious scripts without any sanitization.

These scripts are stored in the database and executed automatically.

In this post, I'll walk you through the technical details, how the vulnerability was exploited (PoC), screenshots with real evidence, and the security risks it represents in real-world environments.

What is CVE-2026-12202?

The CVE-2026-12202 is a Stored Cross-Site Scripting (XSS) vulnerability found in the `Blocks Page` endpoint of the Subrion CMS application.

The `CSS class name` parameter fails to properly validate user inputs, allowing attackers to persist JavaScript payloads on the server. The malicious code is executed automatically.

Technical Details

» **Vulnerable Endpoint:** `Blocks Page`

» **Affected Parameter:** `CSS class name`

» **Payload Used:**

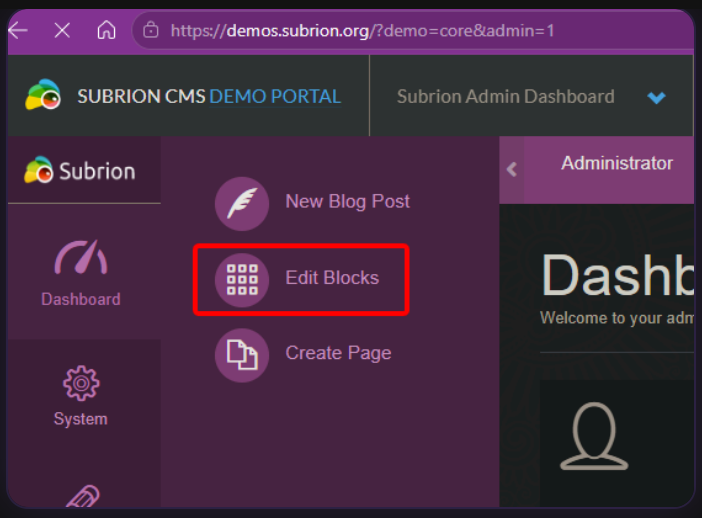
```
"><img src=x onerror=alert('CVE-Hunters2')>
```

Proof of Concept (PoC)

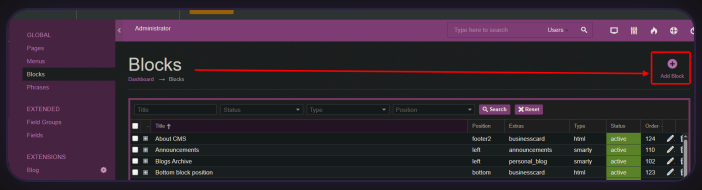
To reproduce the vulnerability:

» **Click on:** `"Edit Blocks"` button:

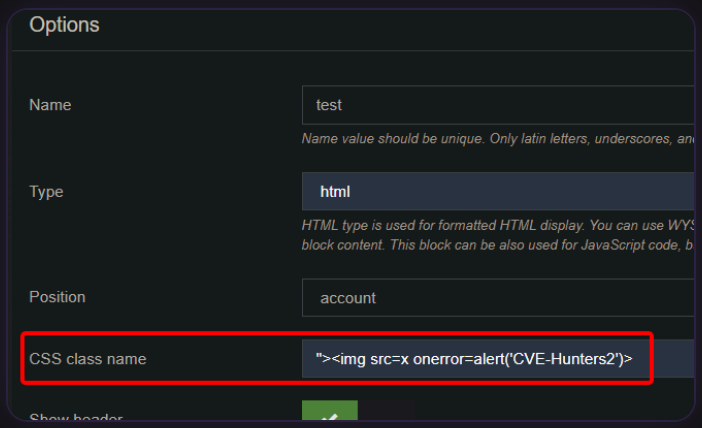
Table of contents



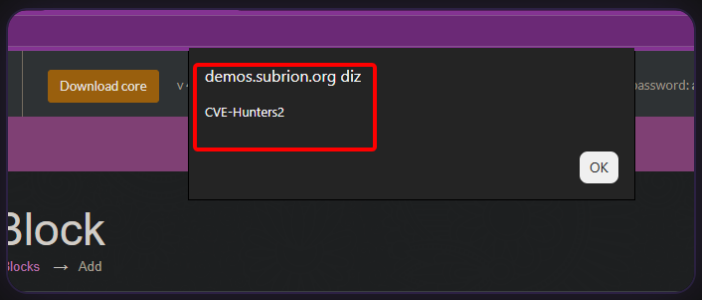
» **Add a Block:**



» **Insert the payload in the:** `“CSS class name”` field:



> Payload will execute automatically after save:



> You can access the full technical report with all step-by-step evidence here:
> `CVE-2026-12202 Report`

Impact

This Cross-Site Scripting (XSS) vulnerability can be exploited to:

- Steal session cookies (session hijacking);
- Install malware on victims' devices;
- Steal credentials stored in the browser;
- Redirect users to malicious websites;
- Deface the application interface;
- Damage the institutional reputation.

Official Sources

This vulnerability was reported responsibly and is publicly registered as:

> - `CVE-2026-12202 on CVE.org`
> - `VulDB Entry`

Credits

Discovered with💜 by Karina Gante.

LinkedIn ✿ GitHub ✿ Gmail ✿ Instagram

> ***Official Member of*** `CVE-Hunters` 🏹

← Back to blog