Stored Cross-Site Scripting (XSS) in endpoint `Blocks` field `CSS class name`

Summary

A Stored Cross-Site Scripting (XSS) vulnerability was identified in the `Blocks` endpoint of the **Subrion CMS** application. This vulnerability allows attackers to inject malicious scripts into the `CSS class name` field. The injected scripts are stored on the server and executed automatically.

Details

Vulnerable Endpoint: `Blocks`

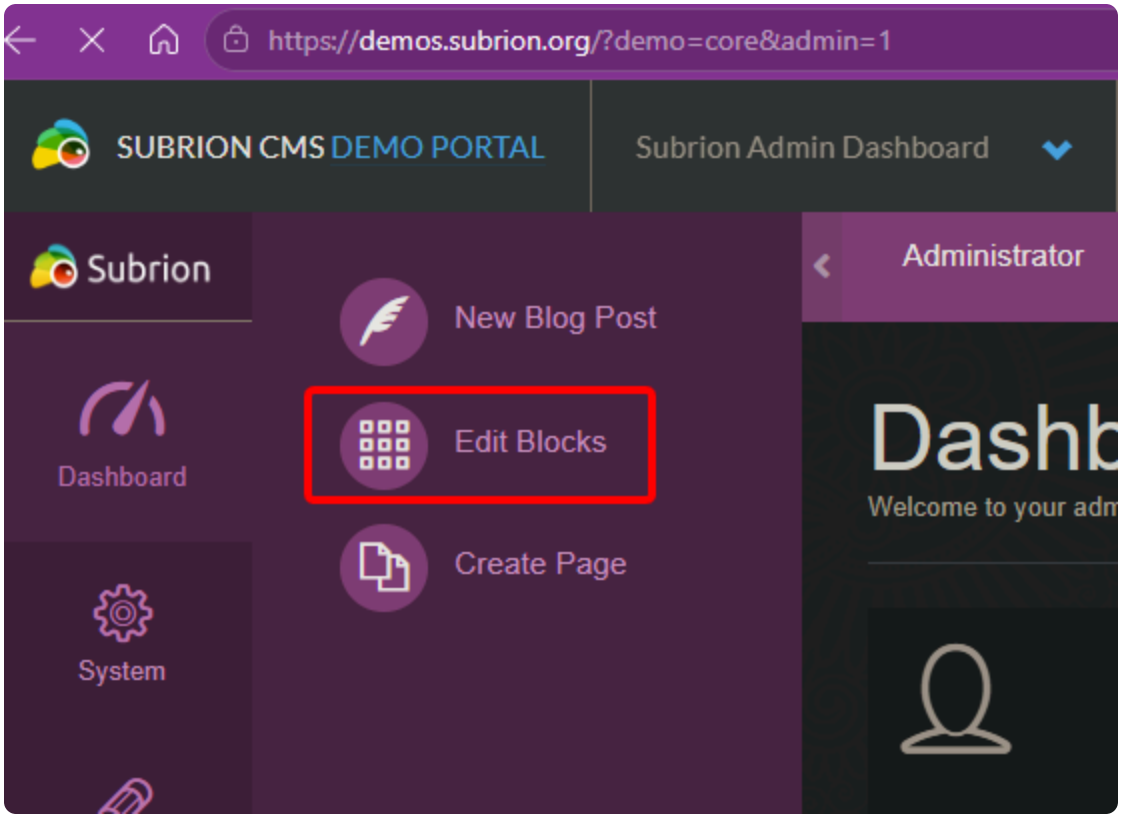
Parameter: `CSS class name`

The application fails to properly validate and sanitize user inputs in the `CSS class name` field. This lack of validation allows attackers to inject malicious scripts, which are then stored on the server.

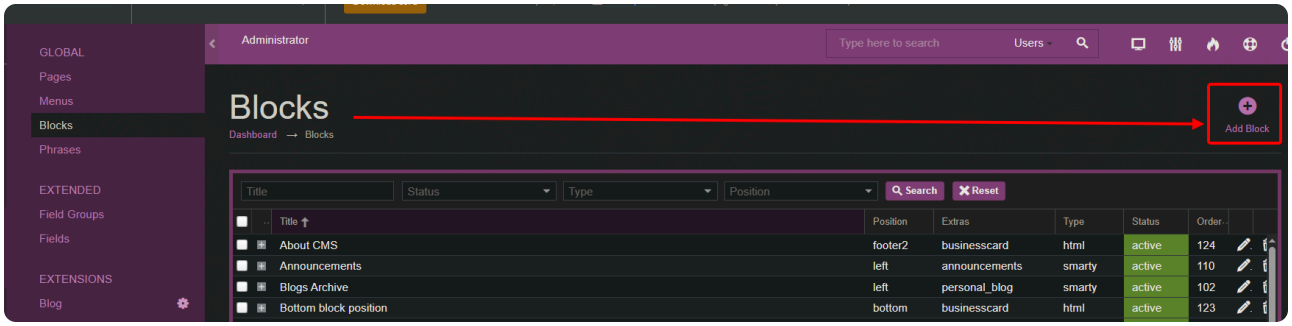
PoC

Step by Step:

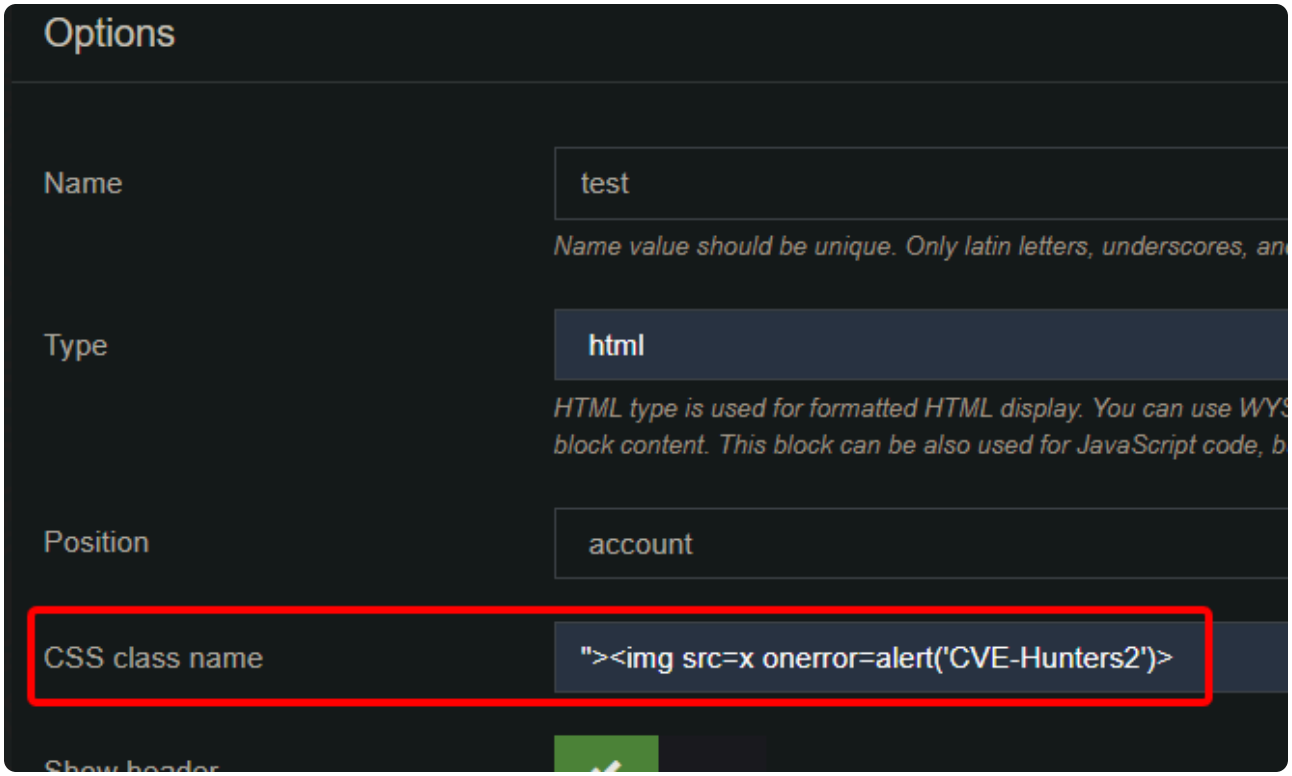
Access admin dashboard and click on `"Edit Blocks"` button:



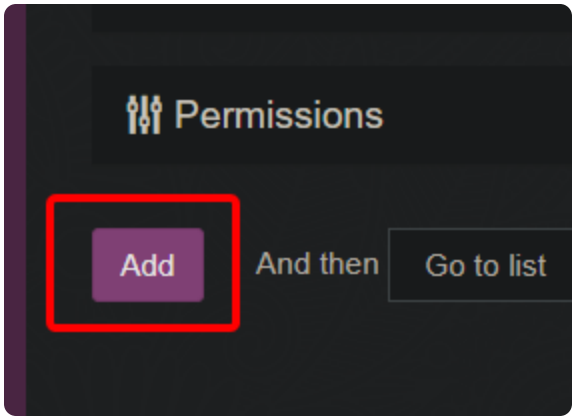
In `"Blocks"` page, click on `"Add Block"` button to setup a new entry:



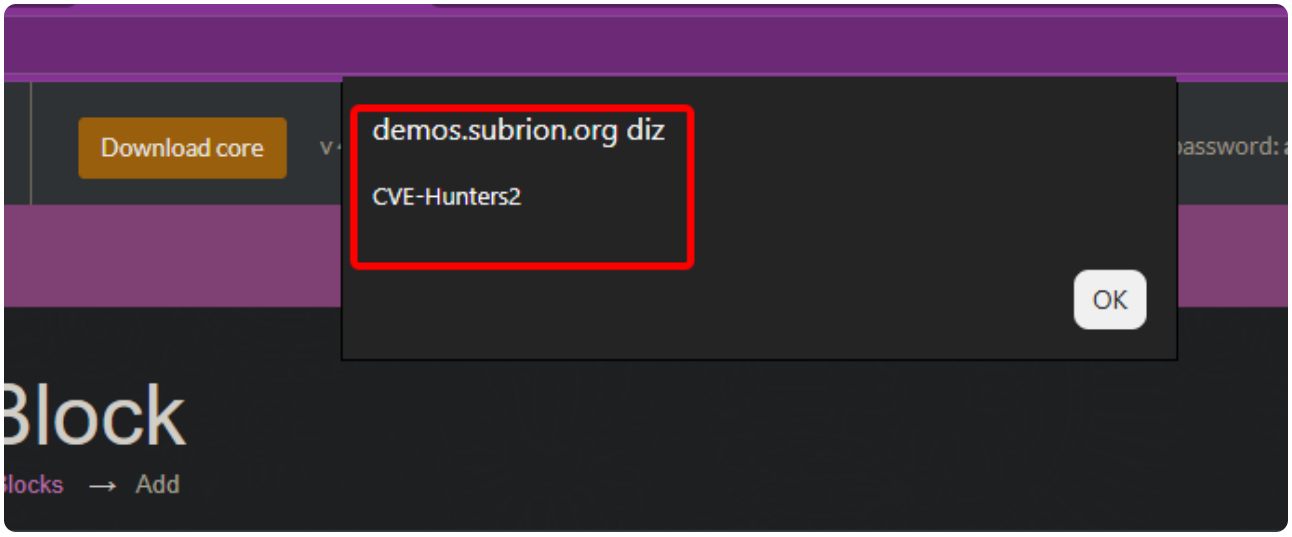
Insert the payload in the `"CSS class name"` field and type anything on another required fields:



Scroll down and click on "Add":



The payload will be activated automatically:



Payload:

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

Impact

- Stealing session cookies: Attackers can use stolen session cookies to hijack a user's session and perform actions on their behalf;
- Downloading malware: Attackers can trick users into downloading and installing malware on their computers;
- Hijacking browsers: Attackers can hijack a user's browser or deliver browser-based exploits;
- Stealing credentials: Attackers can steal a user's credentials;
- Obtaining sensitive information: Attackers can obtain sensitive information stored in a user's account or in their browser;
- Defacing websites: Attackers can deface a website by altering its content.

Finder

Discovered with💜 by Karina Gante (https://karinagante.github.io/).

> *Official Member of CVE-Hunters (https://www.cvehunters.com/)* 🏹