Stored Cross-Site Scripting (XSS) in Blocks Plugin

Summary

A Stored Cross-Site Scripting (XSS) vulnerability was identified in `Blocks Plugin` of the FluentCMS application. This vulnerability allows attackers to inject malicious scripts into the plugin. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk.

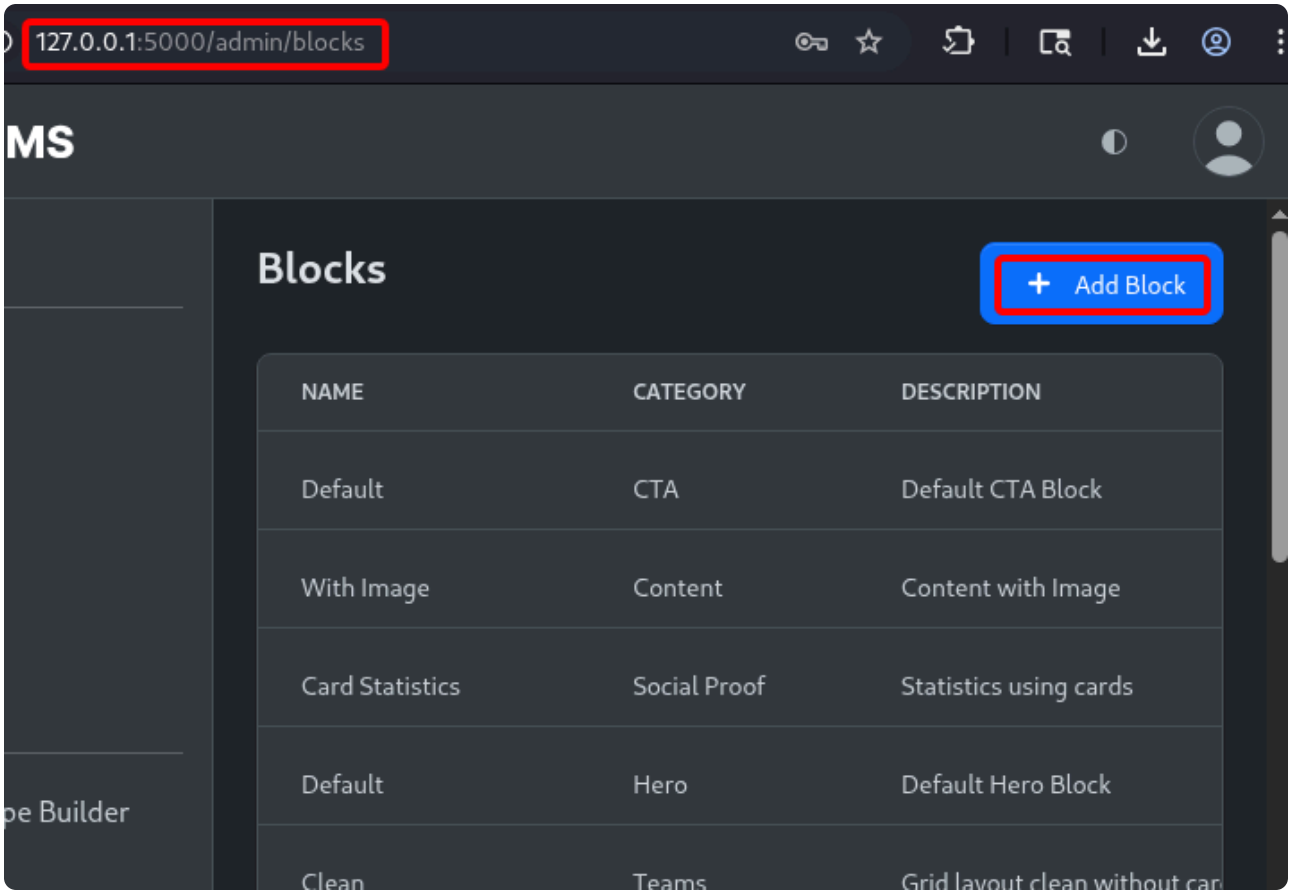
Details

The application fails to properly validate and sanitize user inputs in the `Blocks Plugin` . This lack of validation allows attackers to inject malicious scripts, which are then stored on the server. Whenever the affected page is accessed, the malicious payload is executed in the victim's browser, potentially compromising the user's data and system.

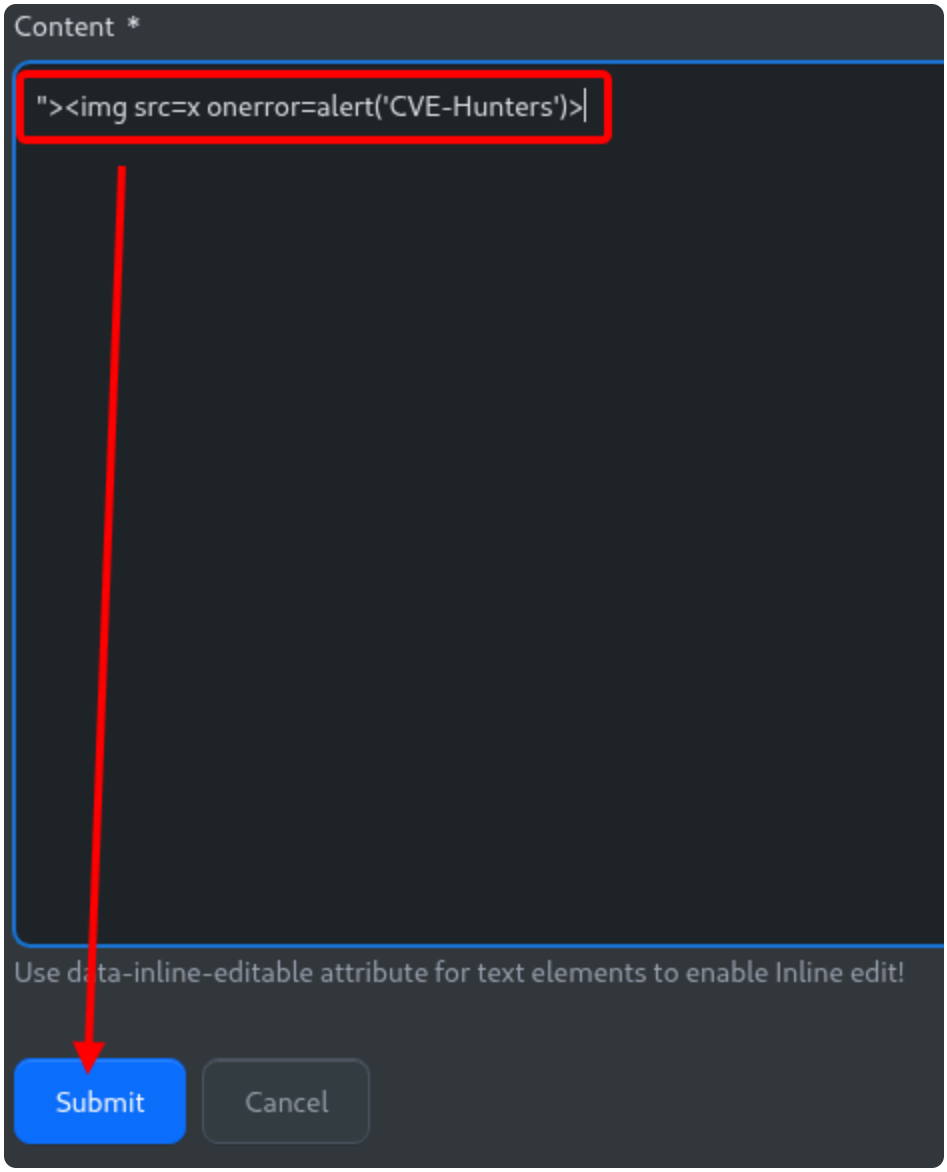
PoC

Step by Step:

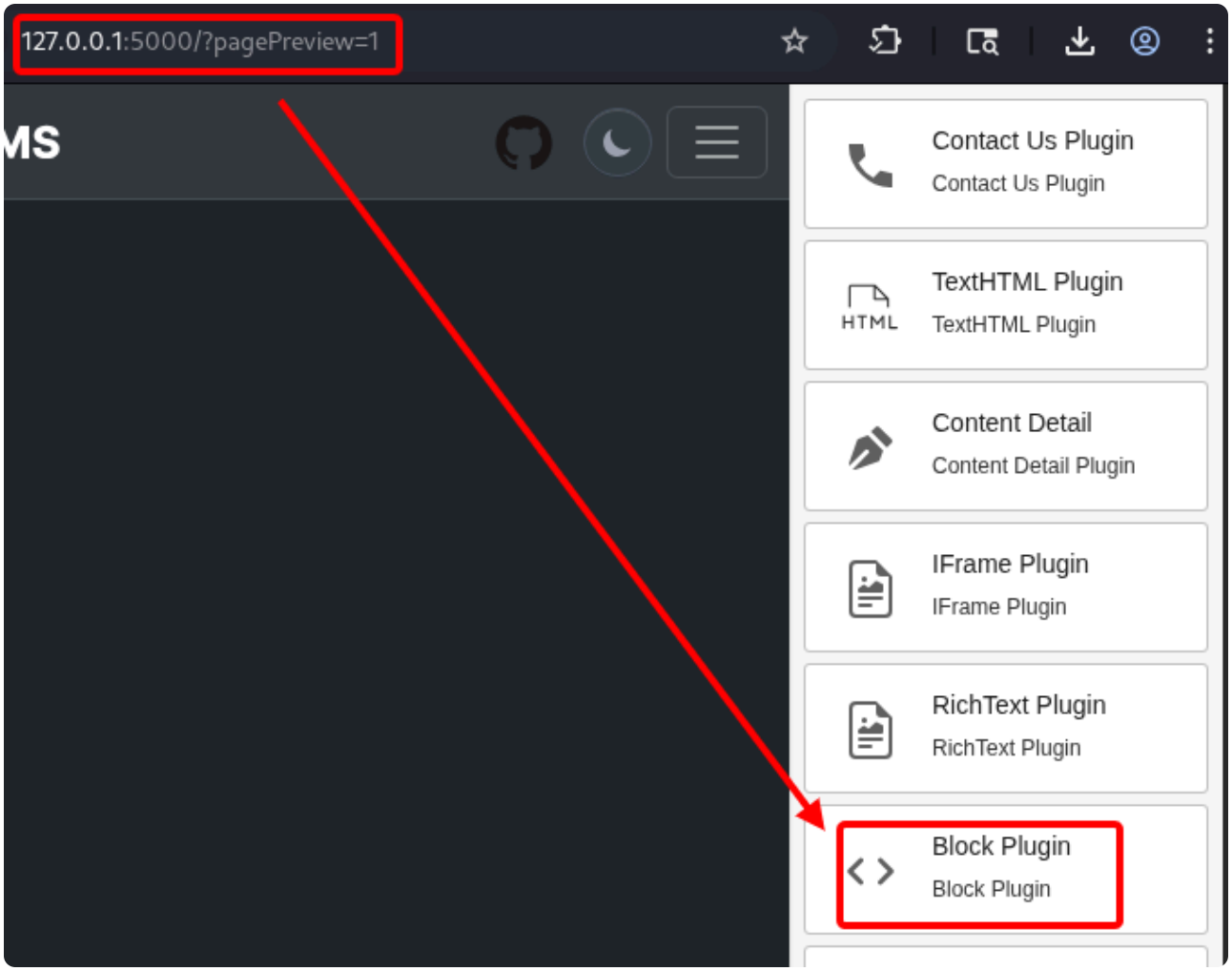
Authenticate with admin account and acess `Blocks menu` . Click on `"Add Block"` button to setup a new entry:



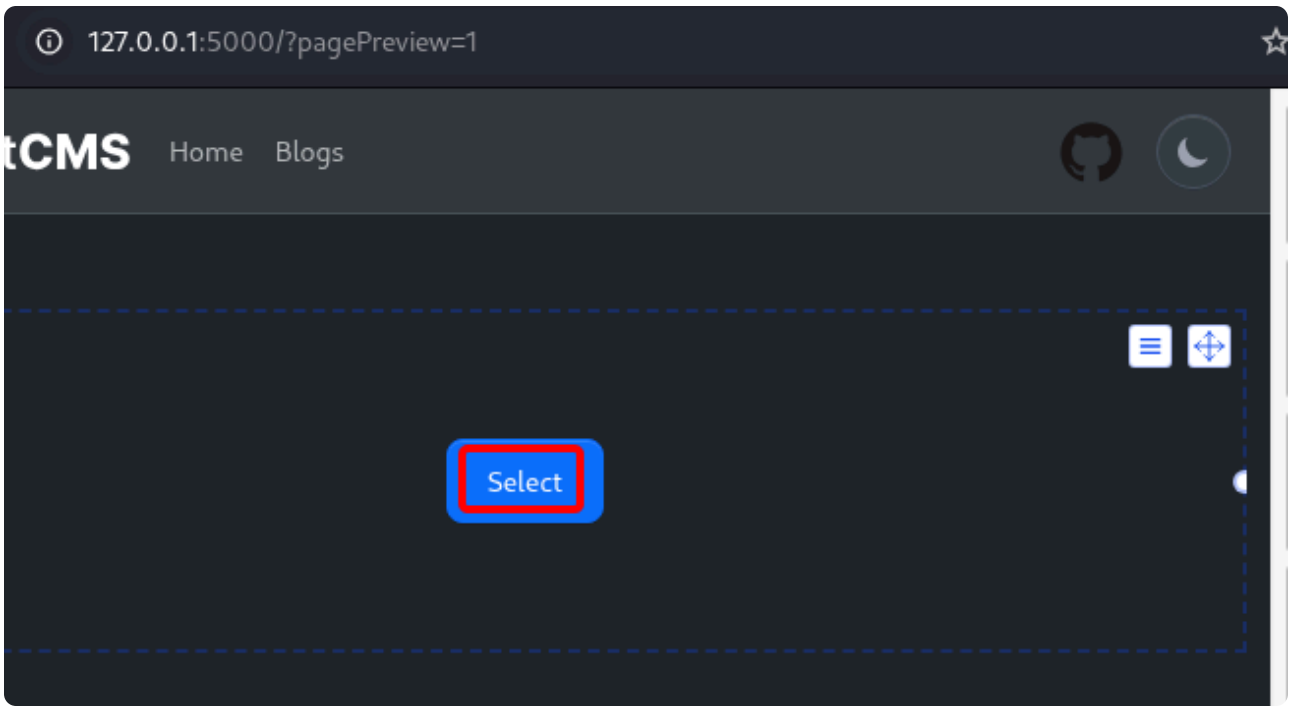
Insert the payload in field `"Content"` and type any value in another fields, click on `"Submit"` :



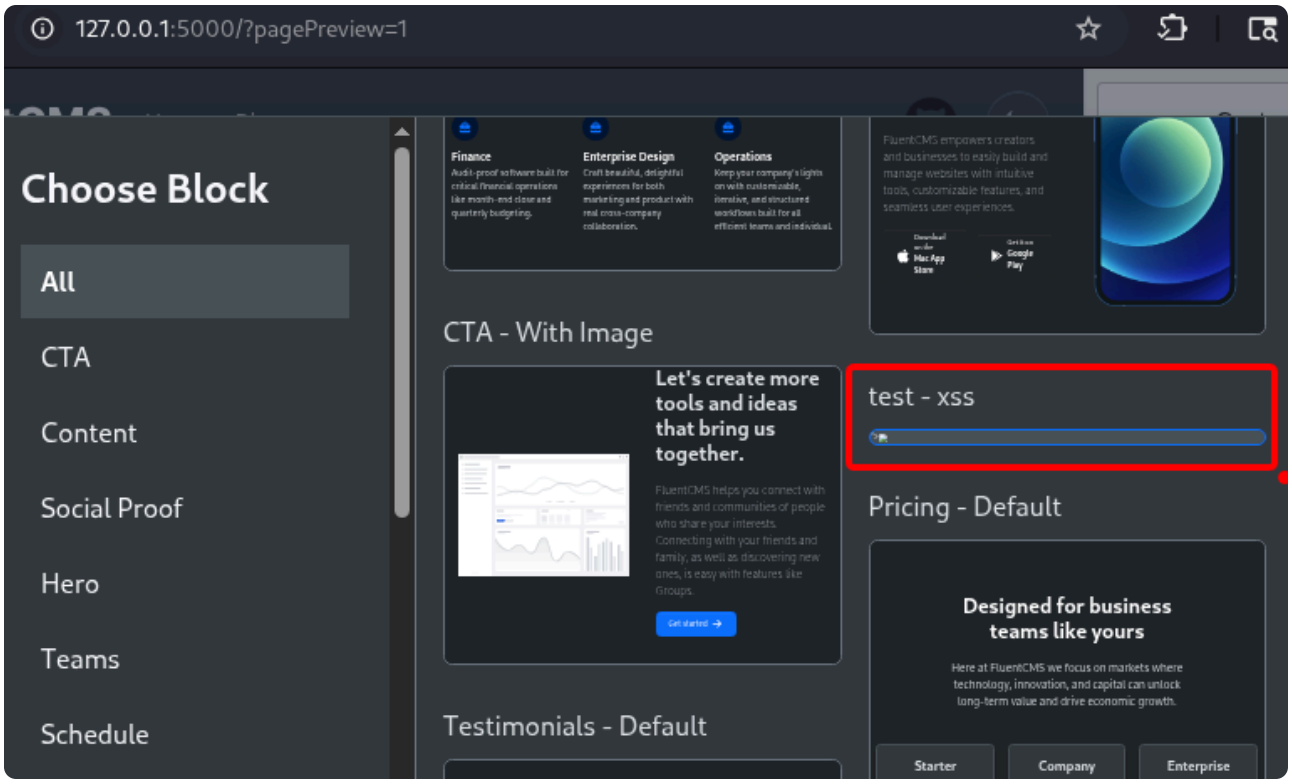
Then, access page preview by this endpoint: `"/?pagePreview=1"` . Drag and drop the Block Plugin in any place at the page:



Click on `"Select"` button:



Select the Block that was set up before:



At least, access the page like an usual user and the script will execute automatically:

Payload:

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

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.
- Misdirecting users: Attackers can change the instructions given to users who visit the target website, misdirecting their behavior.
- Damaging a business's reputation: Attackers can damage a business's image or spread misinformation by defacing a corporate website.

Finder

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

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