

New issue

[Jump to bottom](#)

XSS vulnerabilities #219

✓ Closed

chluo911 opened this issue on Aug 22, 2021 · 0 comments

Labels

bug

chluo911 commented on Aug 22, 2021

Contributor

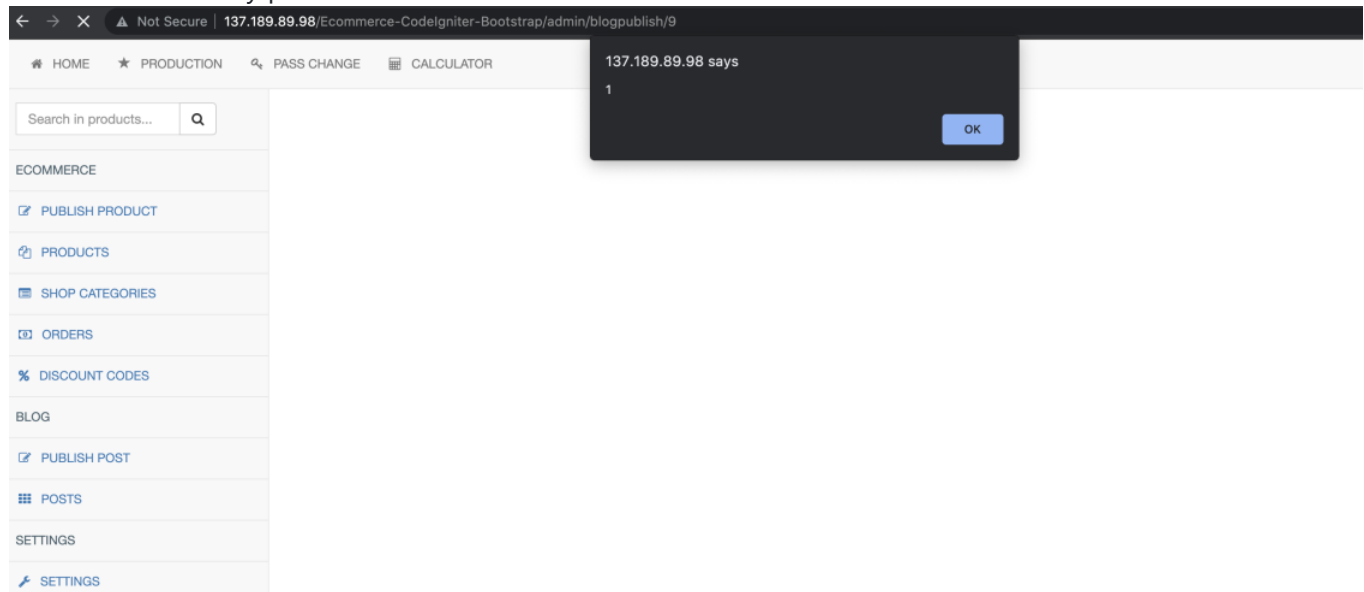
We found multiple XSS vulnerabilities in the latest version of Ecommerce-CodeIgniter-Bootstrap.

Technique details:

The vulnerabilities occur at `base_url()` function. We notice the user inputs (e.g., `$_POST`) are used as the parameter of `base_url()` function in many places (e.g., the 45th line in `/application/modules/admin/views/blog/blogpublish.php`), the program echo the return value of this function directly without proper sanitization. This would lead to XSS vulnerabilities.

Example:

We exploit the echo function in `/application/modules/admin/views/blog/blogpublish.php#45` line. The attacker can set `$_POST['img']` to `'q" onerror="javascript:alert(1)'`. Then the img tag becomes
Then he successfully performs a XSS attack.



The vulnerability has been fixed in [56465f](#) after we reported it to developers.



kirilkirkov added the `bug` label on Aug 23, 2021



kirilkirkov closed this as completed on Aug 23, 2021

Assignees

No one assigned

Labels

`bug`

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

