wuzhicms / **wuzhicms** Public

Code   **Issues** 96   Pull requests 2   Actions   Projects   Wiki   ···

New issue

Jump to bottom

A stored XSS vulnerability in WUZHI CMS v4.1.0 #180

Open **loong716** opened this issue on Jul 9, 2019 · 0 comments

loong716 commented on Jul 9, 2019 • edited

This XSS vulnerability was found in the system bulletin(系统公告) in the background.

payload:

> </textarea><details open="" ontoggle=alert(document.cookie)><textarea>

First we can write payload with a low-privileged user named 'test'.As an attacker, you can change a title to prompt an administrator to click on this page.

alt

Then log in to the admin account and click the change(修改) button to pop up the admin's cookie.

alt

alt

The reason for the vulnerability is that php code uses blacklists to filter JS code, resulting in poor filtering.

This method can be used to steal admin's cookie.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant