New issue

Jump to bottom

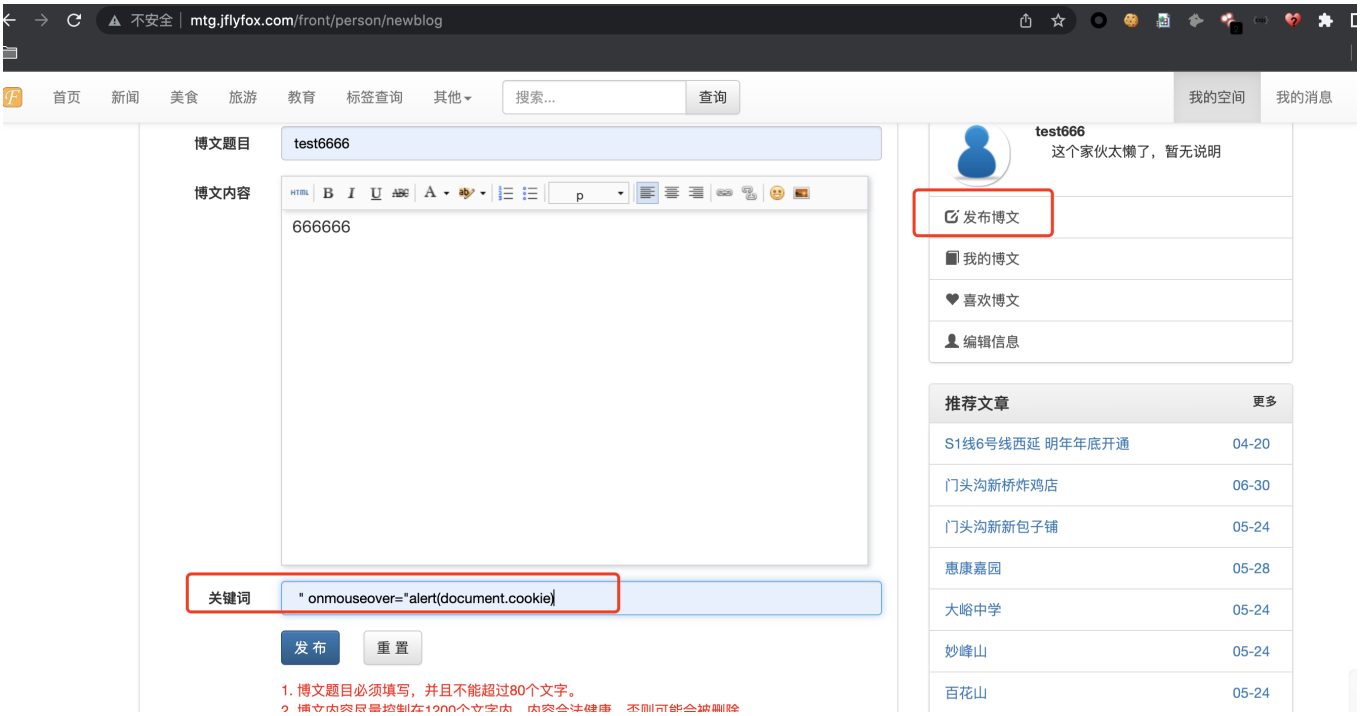
XSS vulnerability stored in the publish blog module of Jfinal_cms V5.1.0 #39

Open **arongmh** opened this issue on Jun 10 · 1 comment

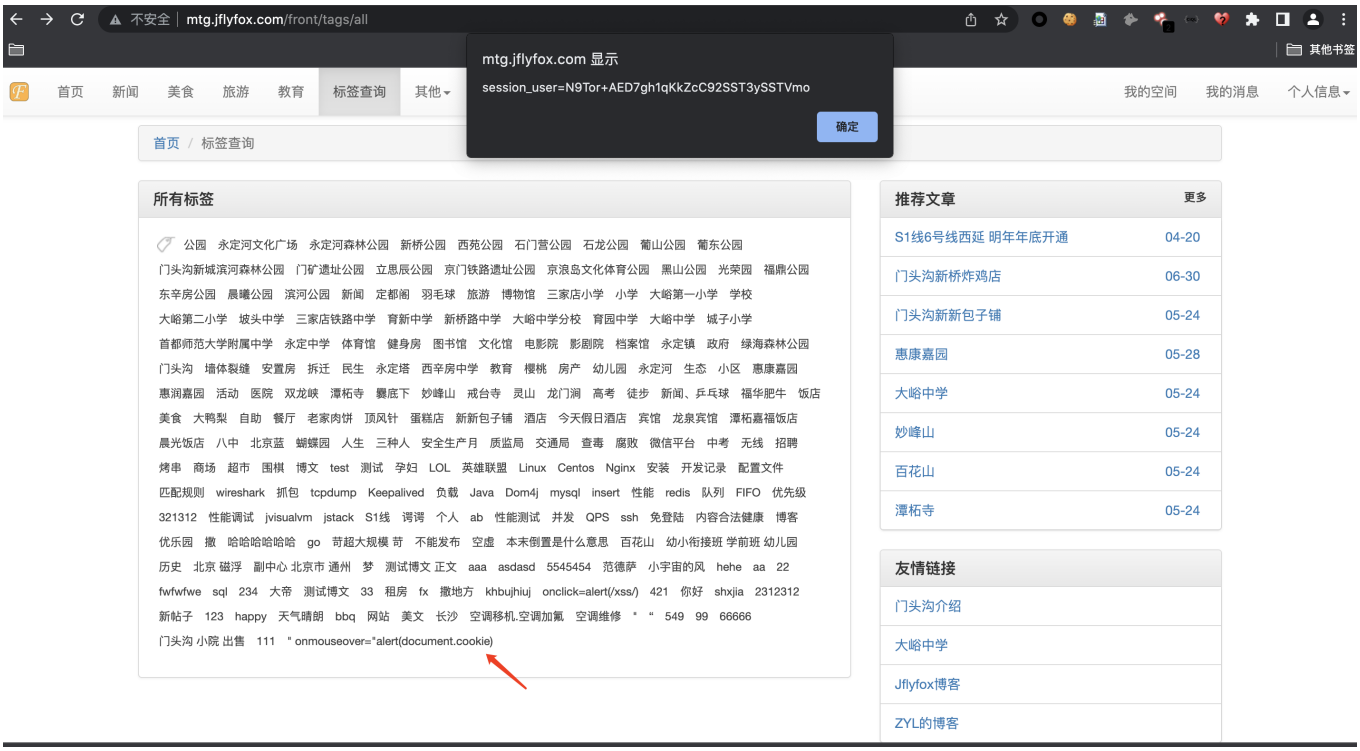
arongmh commented on Jun 10

There is a stored XSS vulnerability in JFinal_cms 's publish blog module. An attacker can insert malicious XSS code into the keyword field. When the user views the content of the article in the foreground, the malicious XSS code is triggered successfully.

payload: `" onmouseover="alert(document.cookie)`



Successfully executed malicious XSS code:



bharathmohanraj mentioned this issue on Jul 11

Issue ID: CVE-2022-33113 #44

Closed

bharathmohanraj commented on Jul 11 • edited

Fix for this issue #39 is available in pull request #44 https://github-com.translate.goog/jflyfox/jfinal_cms/pull/44

bmohanr-techie mentioned this issue on Jul 27

CVE-2022-33113 - Jfinal CMS v5.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the keyword text field under the publish blog module. #47

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants