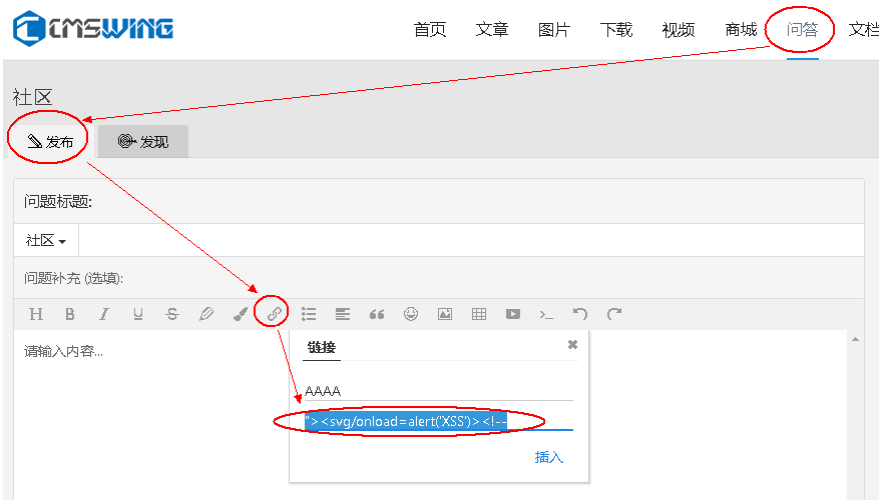
Vulnerability Report: CmsWing in version 1.3.7, there are two storage XSS vulnerabilities #54

Open **zhooooou** opened this issue on Aug 26, 2020 · 0 comments

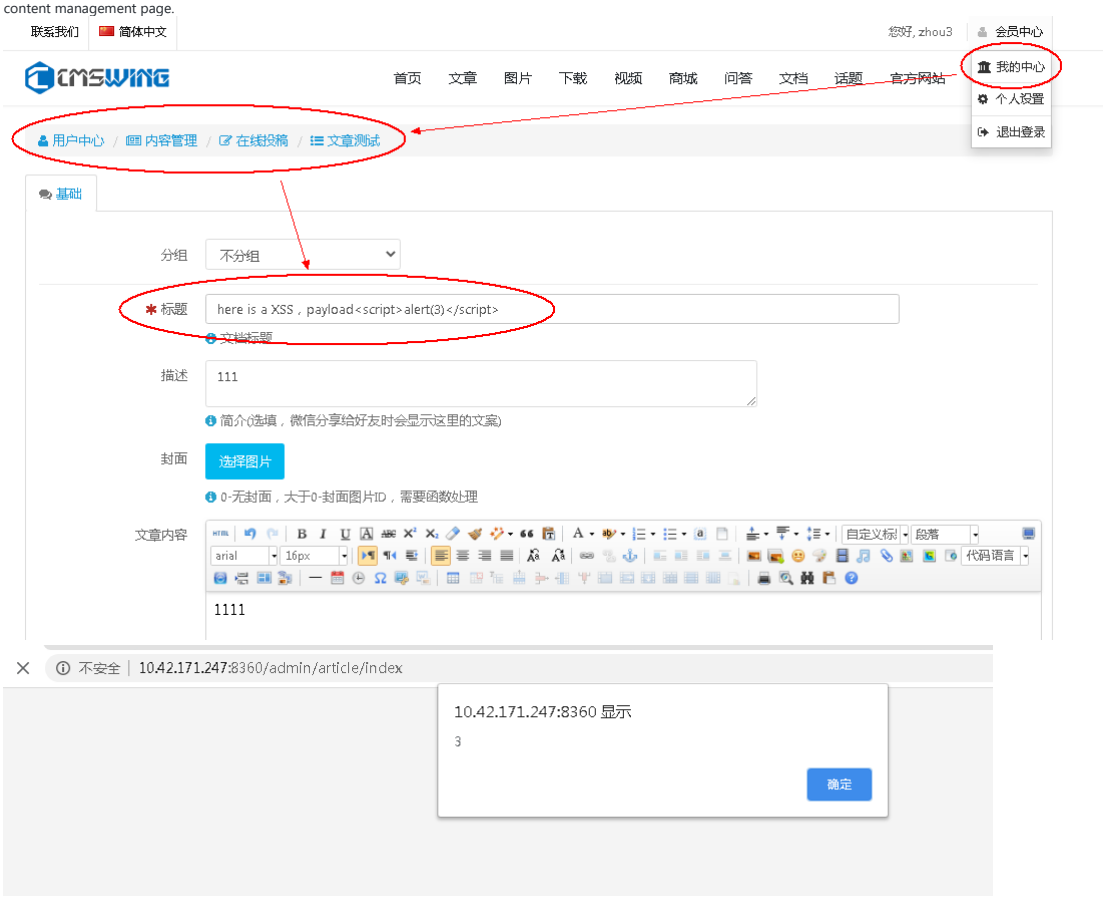
zhooooou commented on Aug 26, 2020 • edited

The first XSS vulnerablity

Question and answer module. In the Question supplement function, when inserting a link, fill in "> < SVG / onload = alert ('xss') > <! -- in the address item to form a stored XSS.This vulnerability can be triggered when any visitor views the issue



The second XSS vulnerablity
Stored XSS exists in the title item of online submission module, and the payload is as follows <script>alert (1)</script>
The specific location of the vulnerability is shown in the figure below,After the submission is approved by the admin user, the vulnerability will be triggered when the administrator opens the content management page.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant