

[New issue](#)[Jump to bottom](#)

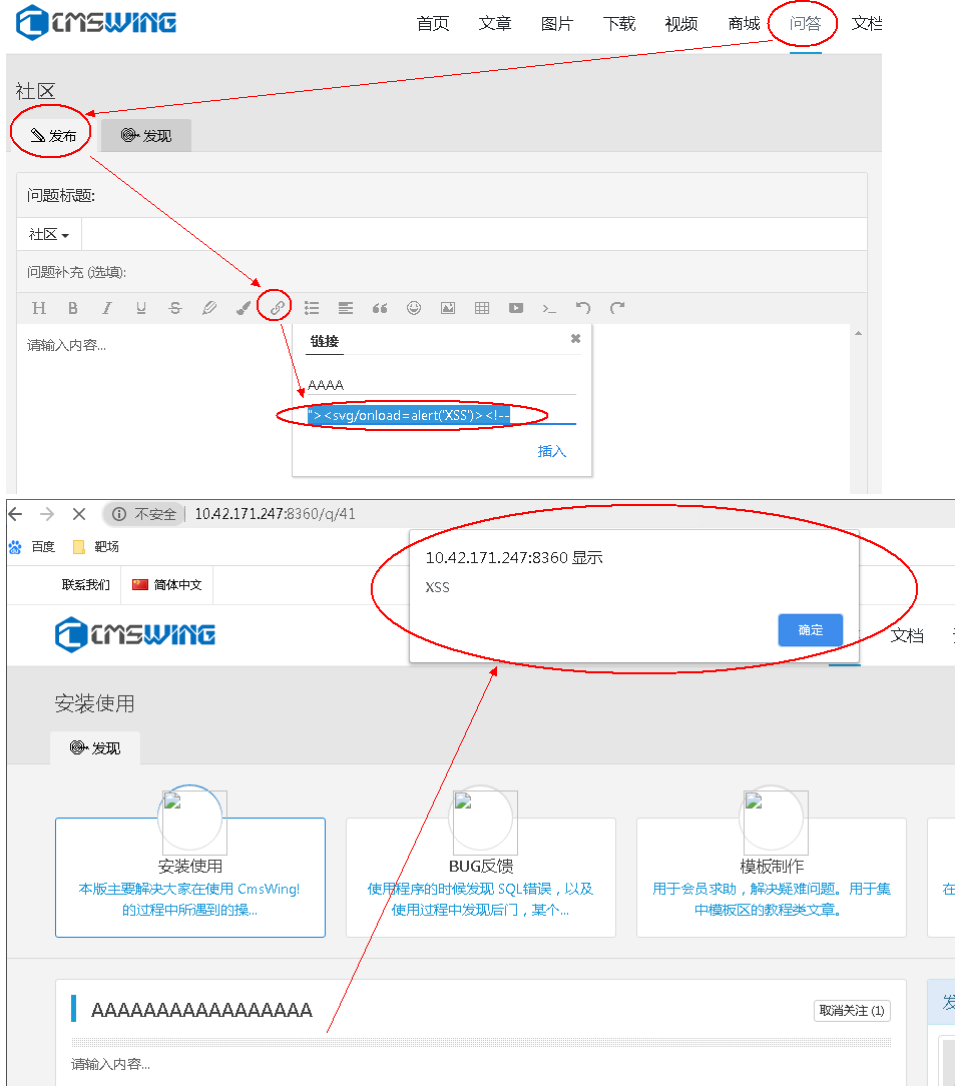
Vulnerability Report: CmsWing in version 1.3.7, there are two storage XSS vulnerabilities #54

[Open](#) zhooooou opened this issue on Aug 26, 2020 · 0 comments

zhooooou commented on Aug 26, 2020 · edited

The first XSS vulnerability

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 vulnerability

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.

The screenshot shows the CMSWING admin interface. The top navigation bar includes links for 联系我们, 简体中文, 会员中心, 我的中心, 个人设置, and 退出登录. The breadcrumb trail is 用户中心 / 内容管理 / 在线投稿 / 文章测试. The article form has a title field containing the payload `<script>alert(3)</script>`. The description field contains '111'. The cover field has a '选择图片' button. The content field has a rich text editor with '1111'. A browser alert box displays the number 3.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

