A stored Cross-Site Scripting (XSS) vulnerability exists in the section where new items are added.This stored XSS vulnerability can cause pop-ups and the theft of administrator cookies, significantly affecting the website's normal functionality.

impacted versions

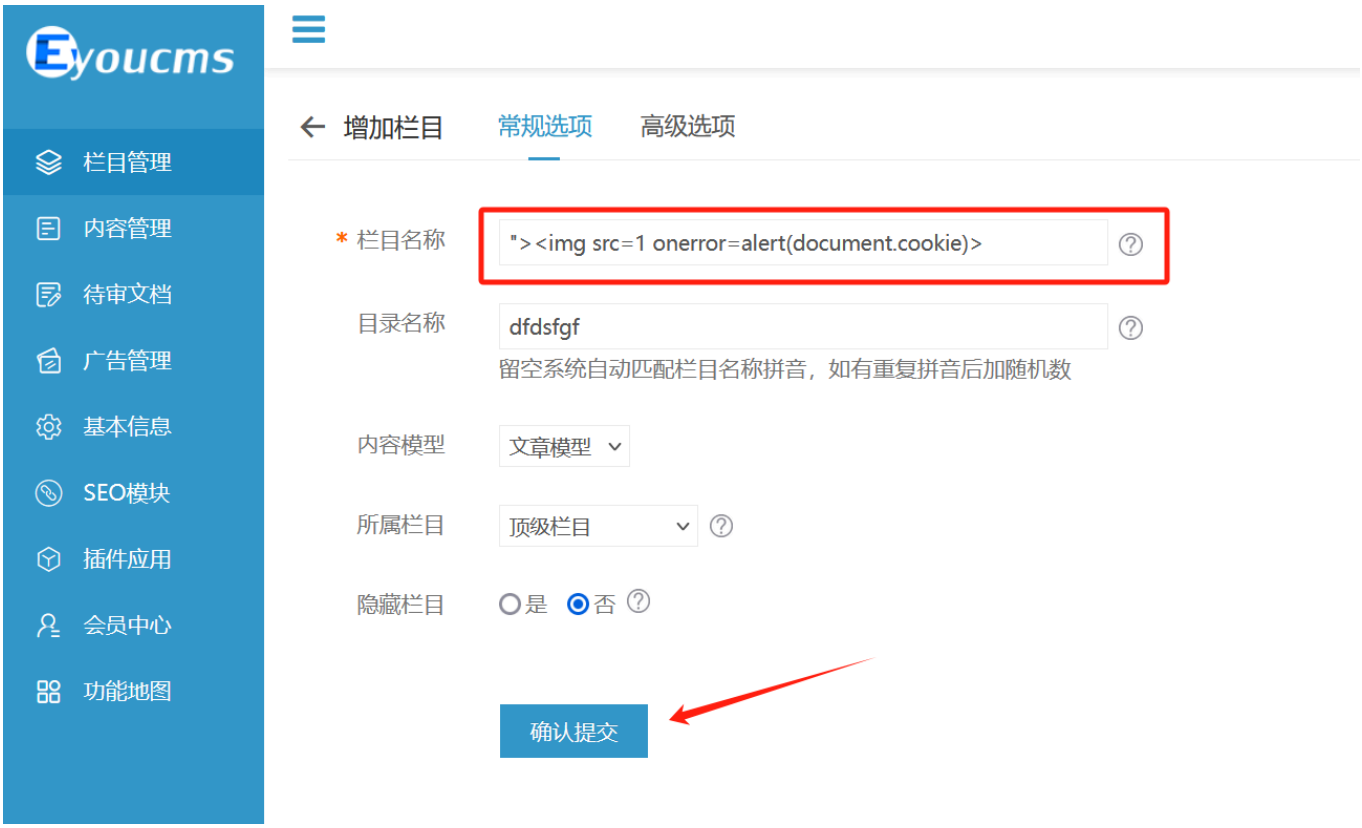
Hello, I found Stored XSS in EyouCMS version V1.6.7-UTF8-SP1_0802
https://www.eyoucms.com/

Here are the complete attack steps

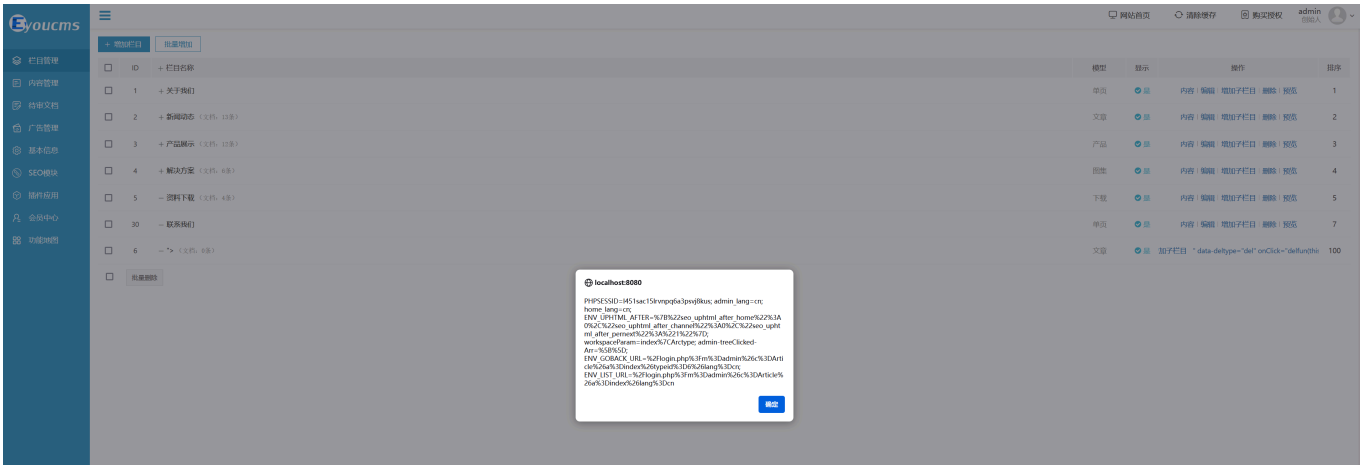
1. Please log in to the backend and follow the steps illustrated in the image to add a new section.

2. Enter a malicious payload in the section name field, fill in the other options as you wish, and submit when finished.

```
"><img src=1 onerror=alert(document.cookie)>
```



3. After submission is successful and the page redirects, a popup appears, indicating that the admin's cookie information has been successfully obtained.



recommendations for remediation

1. To mitigate security risks, apply input filtering to ensure that any JavaScript tags are disabled or sanitized before they are processed by the system.