

New issue

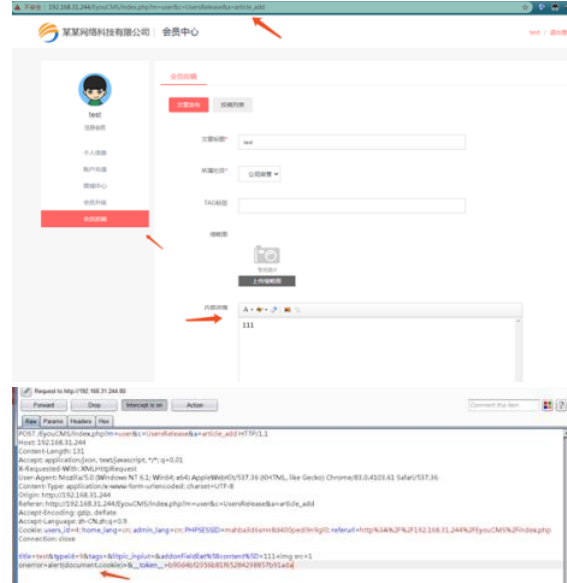
Jump to bottom

There is a Persistent Cross-Site Scripting in the member contributions. #12

Open wantwo3 opened this issue on May 28, 2020 · 0 comments

wantwo3 commented on May 28, 2020 · edited

Vulnerability found in Eyoucms1.4.6 and before.  
In the member center member contribution office, after editing the contribution content through the editor, intercept the data package, modify the parameter addonfieldext [content], and construct the payload "< img SRC = 1 onerror = alert ( document.cookie )>"



After the administrator logs in the background, when viewing the content submitted by the user, it triggers the payload to obtain the cookie information.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

