omeka / Omeka Public

Code Issues 98 Pull requests 36 Actions Projects Wiki ...

New issue

Jump to bottom

Stored XSS in the admin/files/edit page #935

Closed EvanYu0816 opened this issue on Feb 3, 2021 · 2 comments

EvanYu0816 commented on Feb 3, 2021

Hello Omeka Team!

I was looking through your application (V2.7.1), and I discovered a stored XSS bug at "admin/files/edit".
While most of the pages filter out tags that are not in the whitelist when "Use HTML" is on, "admin/files/edit" seems to allow them. My guess is that this is not the expected behavior?

POC:

1. Create an item with a file attachment
2. Edit the file
3. Place `<img src=x onerror=alert(1)>` in one of the fields and toggle "Use HTML" to on. (An alert should pop up now, but ignore that and save changes)
4. Access the page containing the file, and an alert should pop up.
5. (Optional) Switch to a different account to verify that this affects all users.

Impact: client-side code execution
This bug shouldn't be very dangerous since it is only available to contributors, admins, and superusers.
The session cookie is httponly, and the csrf tokens seem to be set properly (upon first glance).
However, the XSS bug can be leveraged in many other ways, and it could increase the impact of a future vulnerability. Therefore, it's probably better to have it fixed.

Please let me know if anything is unclear, or if this is not a legitimate issue.
Thanks in advance!

zerocrates closed this as completed in `08bfdf4` on Feb 3, 2021

zerocrates commented on Feb 3, 2021 Member

Thank you for the report.

It's definitely a bug. I think you're right about the fairly limited impact but we'll have this fix included in the next release, of course.

EvanYu0816 commented on Feb 3, 2021 Author

Thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants