New issue

Jump to bottom

Security Issue - XSS #4888

Closed **bousalman** opened this issue on Feb 18, 2021 · 3 comments · Fixed by #4971

Labels security

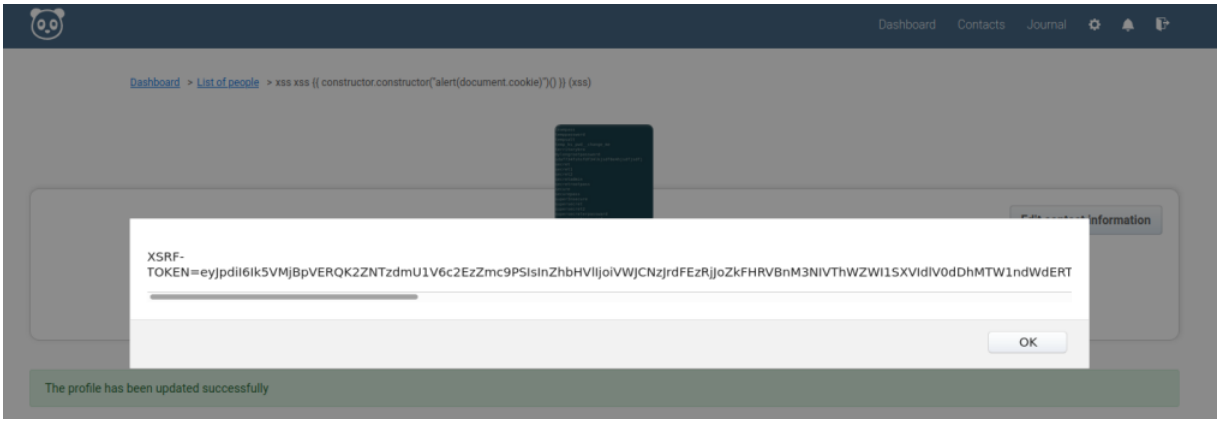
bousalman commented on Feb 18, 2021

Hi there,

I'm using the latest version of Monica PRM web application 2.19.1, deployed on my local Ubuntu machine. I would like to report to you the existing of Cross Site Scripting Vulnerability in the Contact Page.
The following fields of the Contact object can be used to host a stored XSS (First name, Middle name, Last name, Nickname & Description) and will be triggered each time you browse the contact webpage or trying to edit the details.
This happen because of the way that Vue.js do render the webpage and executing the XSS payload in the vulnerable fields.

the payload used in the POC:

```
{{ constructor.constructor("alert(document.cookie)")() }}
```



To mitigate this issue different safeguards can be implemented, please refer to this website for more details:
https://github.com/dotboris/vuejs-serverside-template-xss

Regards,

RMHogervorst commented on Feb 18, 2021

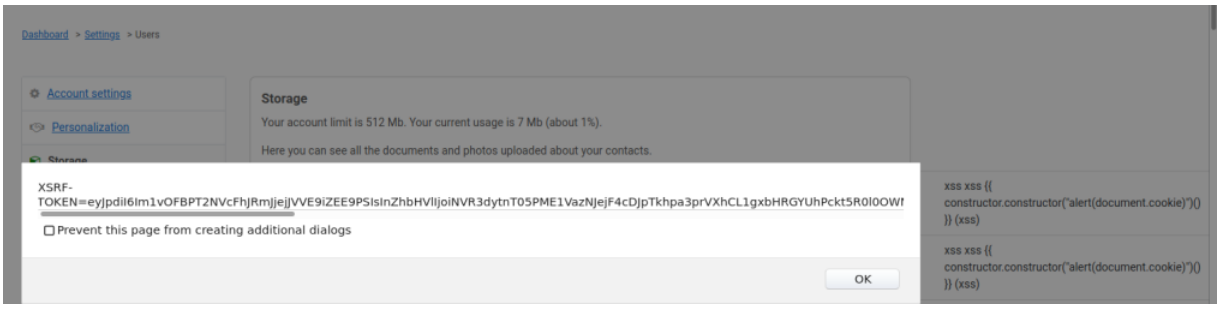
Is this related to #4543 ?

1

asbiin added the security label on Feb 20, 2021

bousalman commented on Feb 22, 2021 Author

@RMHogervorst
I am not aware of #4543 before However I can see after reading the the pull request that it's a different `Sink` .
Although We both use the same `Source` to host the payloads, the payload I used targets the Vue.js rendering engine and fire the XSS vulnerability on Contact page and also the /Storage endpoint in Settings:



1

asbiin mentioned this issue on Mar 17, 2021

refactor: fix audit logs display #4971

Merged

asbiin closed this as completed in #4971 on Mar 17, 2021

---

github-actions bot commented on May 1

This issue has been automatically locked since there
has not been any recent activity after it was closed.
Please open a new issue for related bugs.

github-actions bot locked as **resolved** and limited conversation to collaborators on May 1

Assignees

No one assigned

Labels

security

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

refactor: fix audit logs display
monicahq/monica

3 participants