Cross-site Scripting (XSS) - Reflected in janeczku/calibre-web

0

Valid Reported on Jan 16th 2022

Description

There is a reflected XSS vulnerability on the site calibre-web.

Proof of Concept

```
1. go to the calibre e-book management
2. create a new book give the title name <script src=1 href=1 onerror="java
3. and give the title sort name <script src=1 href=1 onerror="javascript:al
4. save and go to the website
5.go to Author
6.press one of the books
7. then right click and press inspect element
8. then press Author/strored

Video POC: https://drive.google.com/file/d/1umL5Vk5ezXxIA3nm43fPWl-FiD0Uy77
```

Impact

Reflected XSS allows attackers to misguide vistors of a website, steal cookies, and send arbitrary requests.

CVE
CVE-2022-0352
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
High (8.5)

Visibility
Public

Status
Fixed

Found by

siyah.A
@alicaz
unranked

This report was seen 382 times.

We are processing your report and will contact the **janeczku/calibre-web** team within 24 hours.
10 months ago

We have contacted a member of the **janeczku/calibre-web** team and are waiting to hear back
10 months ago

janeczku 10 months ago Maintainer

I can't reproduce it. There is something wrong in the code, I agree to that. If I open the author view with the book I see a '">' on top of the cover, and clicking on the cover no longer opens a dialog (books detail dialog), instead the books detail view (the one with the blue Download buttons) it opened as new page. No java-script is executed. I tested it with the newest commit on master. Checked browsers are Firefox (96.0.1) and Chromium (97.0.4692.71). Both on Linux Mint 20.4. You video only shows the second part of the problem. The link to open authors normally ends with an authot ID, the only link without ID is for author 1. Does this also happen with other books than the first one?

We have sent a follow up to the **janeczku/calibre-web** team. We will try again in 7 days.
10 months ago

janeczku validated this vulnerability 10 months ago

siyah.A has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

janeczku marked this as fixed in 0.6.16 with commit 6bf075 10 months ago

The fix bounty has been dropped ×

This vulnerability will not receive a CVE ×

Sign in to join this conversation