

Tabnabbing via window.opener [bookwyrmsocial] in bookwyrmsocial/bookwyrmsocial

0



Valid

Reported on Aug 5th 2022

Description:

Hello @bookwyrmsocial I found a tabnabbing vulnerability. attack is possible due to `target=_blank` or Tab nabbing via window.opener.

VISIT:- <https://bookwyrmsocial/>

SUMMARY:

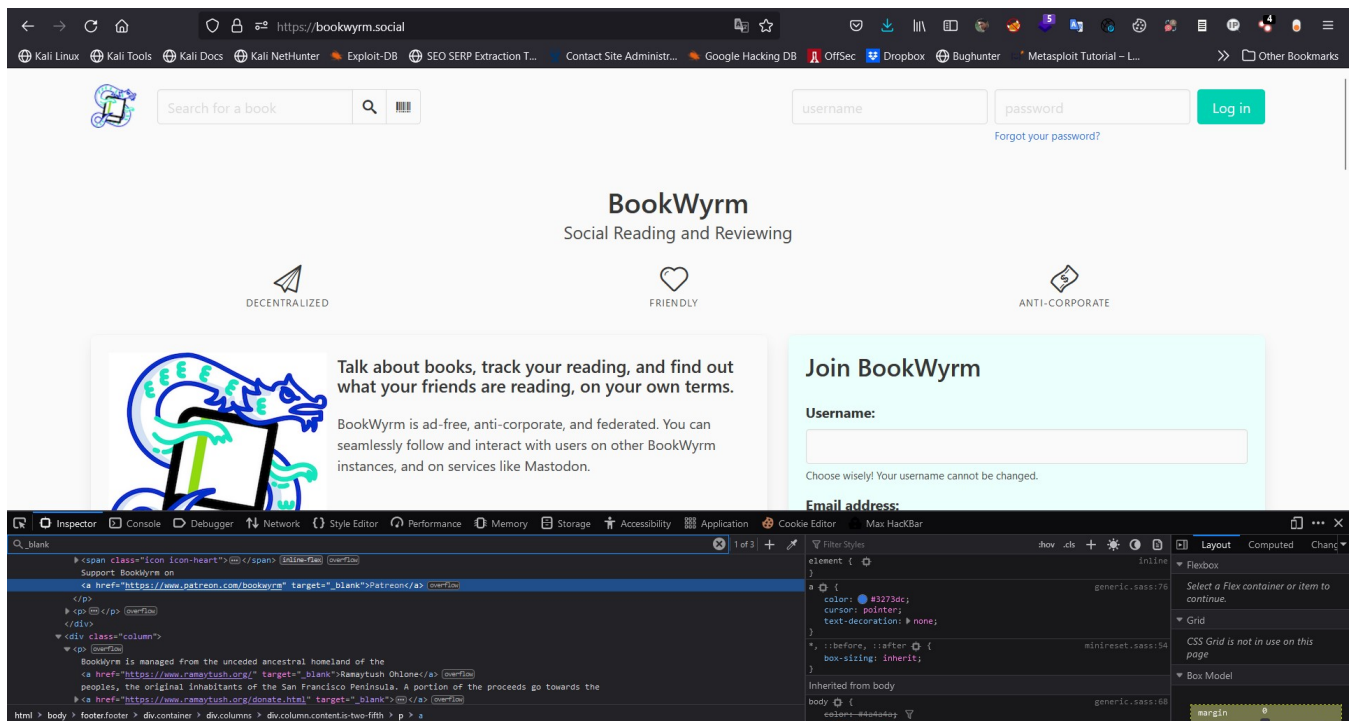
I was browsing the site and found a tabnabbing vulnerability . As per the observation I found that attack is possible due to `target=_blank` or Tab nabbing via window.opener. When you open a link in a new tab (`target="_blank"`), the page that opens in a new tab can access the initial tab and change it's location using the window.opener property.

STEPS TO REPRODUCE:

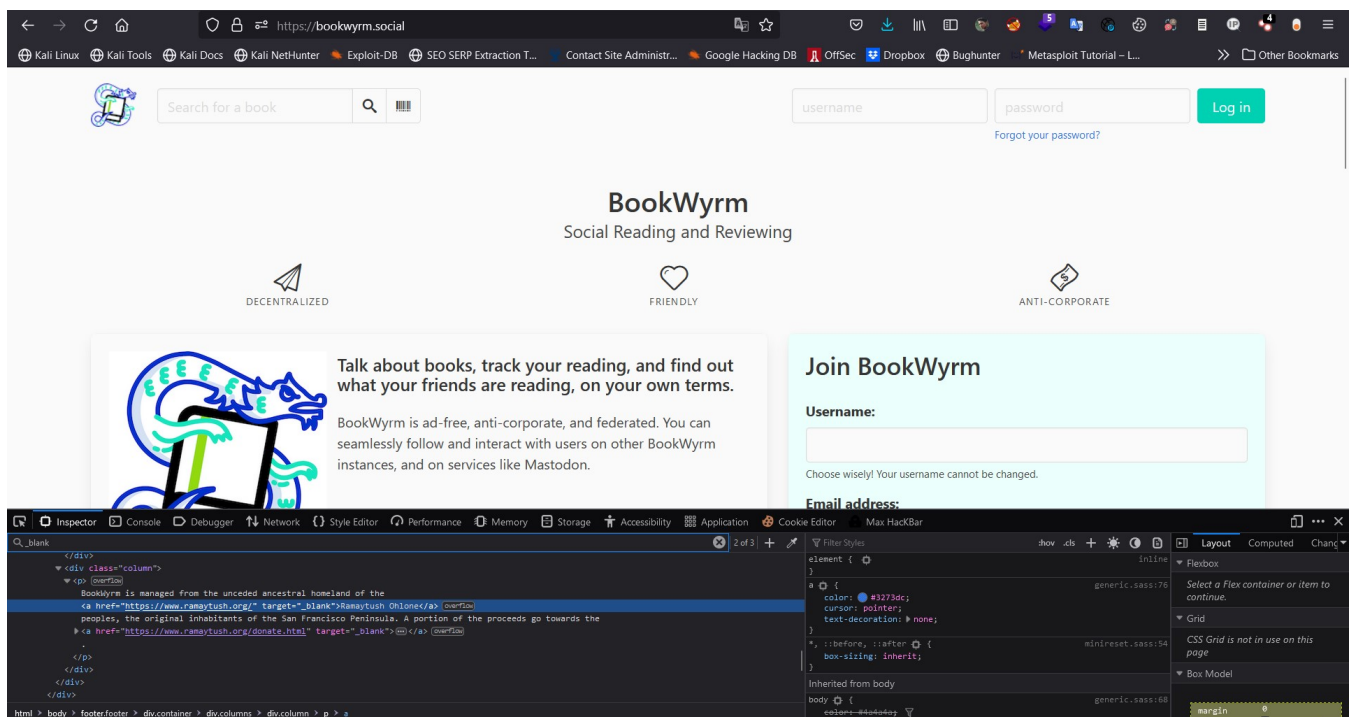
- 1- Open the website URL :- <https://bookwyrmsocial/>
- 2- Right-click and click on inspect element
- 3- Locate the cursor to Element Tab then do `CTRL+F` or Search for `target="_blank"`
- 4- If you get blank with a link it means website can be vulnerable like , open redirect like vulnerabilities
- 5- For More Details To Check the POC

POC Screenshot 1:

Chat with us



POC Screenshot 2:



MITIGATIONS:-

In order to mitigate this issue, developers are encouraged to use `rel="nofollow"` and `noreferrer` as follows: `<a target=" blank" class="btn external-url" href="#" https://evil.com "`

Chat with us

rel="nofollow noopener noreferrer"><i class="fa fa-external-link"></i>

Don't open links in new tabs using the target="_blank" Add attribute rel="noreferrer" which also disables referrer Set the window.opener attribute to null on the new tab before redirecting, like this: <script>var w=window.open(url, "target=_blank");w.opener= null;</script>

External links in main domain :

<https://www.patreon.com/bookwyrn>

<https://www.ramaytush.org/>

Impact

This type of Phishing has huge potential for tricking users that click on external links from this(your) website to be a victim of a scam page because the redirecting is made in the background, while the user is focused on another tab.

Occurrences

 dashboard.html L1-L147

References

- <https://hackerone.com/reports/179568>

CVE

CVE-2022-35953

(Published)

Vulnerability Type

CWE-601: Open Redirect

Severity

High (7.1)

Registry

Other

Affected Version

0.4.4

Visibility

Public

Chat with us

Status
Fixed

Found by



AGNIHACKERS

@agnihackers

amateur ✓



This report was seen 822 times.

We are processing your report and will contact the **bookwyrmsocial/bookwyrmsocial** team within 24 hours. 4 months ago

Mouse Reeve validated this vulnerability 4 months ago

AGNIHACKERS has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Mouse Reeve marked this as fixed in 0.4.5 with commit 1518db 4 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

dashboard.html#L1-L147 has been validated ✓

AGNIHACKERS 4 months ago

Researcher

@maintainer are you happy to assign a CVE? please confirm, then only admin can move further

AGNIHACKERS 4 months ago

Researcher

@admin can you pls assign a CVE for this?

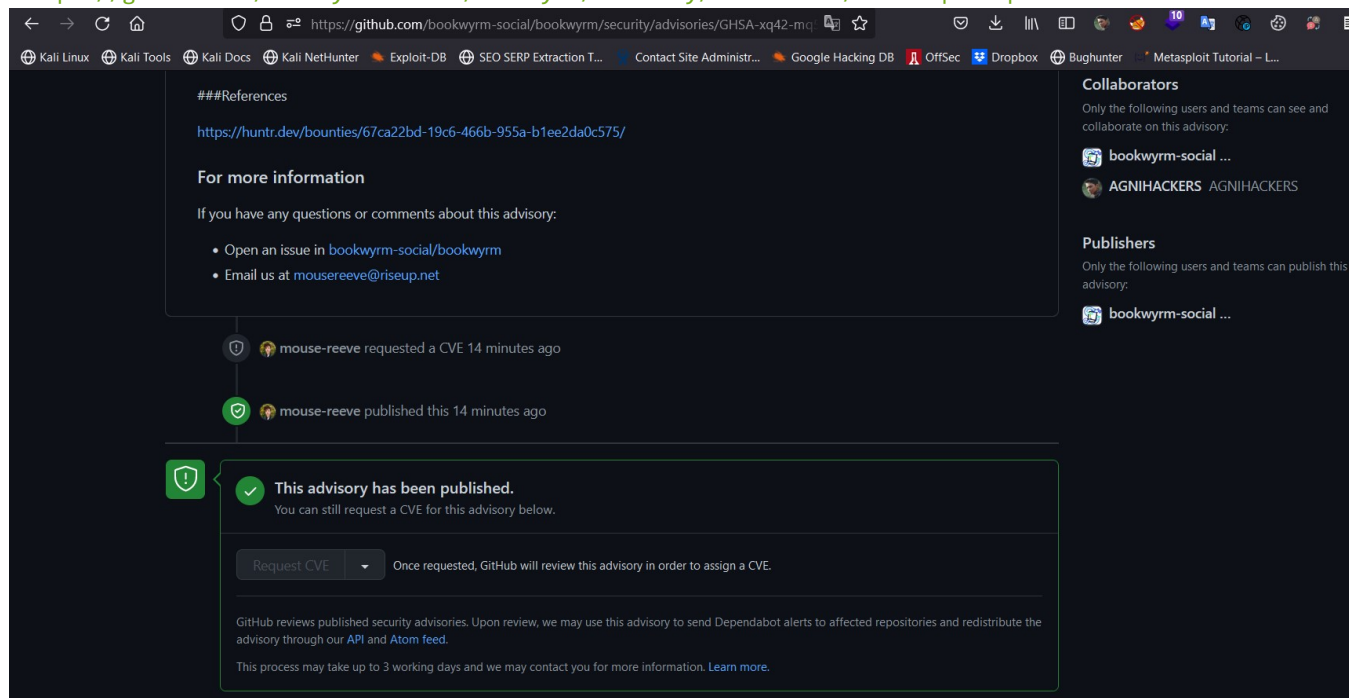
Chat with us

AGNIHACKERS 4 months ago

Researcher

@admin maintainer has requested a CVE via github
here is the link, check that:

<https://github.com/bookworm-social/bookworm/security/advisories/GHSA-xq42-mq5w-m24x>



So can we assign a CVE here?

Akshay Ravi 4 months ago

Hey, in this case the maintainer has created and published security advisory only, the github staffs will verify this and assign CVE later(it may takes time accordingly), once the CVE is assigned by github, you can add the CVE number here and request admin for adding that to your profile

AGNIHACKERS 4 months ago

Researcher

Okay @Akshay Ravi

Jamie Slome 4 months ago

Admin

Hi 🙌 Once the CVE is added to the GitHub Security Advisory, we can add it to this report. Please let me know once it receives a CVE number :)

Chat with us

AGNIHACKERS 4 months ago

Researcher

@admin [CVE-2022-35953](#) has assigned for this issue, can you please add this CVE on this report(CVE ID)

<https://github.com/bookworm-social/bookworm/security/advisories/GHSA-xq42-mq5w-m24x>

<https://huntr.dev/bounties/67ca22bd-19c6-466b-955a-b1ee2da0c575/>

For more information

If you have any questions or comments about this advisory:

- Open an issue in [bookworm-social/bookworm](#)
- Email us at mousereeve@riseup.net

Only the following users and teams can see and collaborate on this advisory:

- bookworm-social ...
- AGNIHACKERS AGNIHACKERS

Publishers

Only the following users and teams can publish this advisory:

- bookworm-social ...

mouse-reeve requested a CVE 3 days ago

mouse-reeve published this 3 days ago

github-staff assigned CVE-2022-35953 20 minutes ago

github-staff commented 20 minutes ago

GitHub has issued [CVE-2022-35953](#) for this Security Advisory after reviewing it for compliance with CVE rules. Since you've already published this Security Advisory, we'll publish this CVE to the [CVE List](#).

Thank you for making the open source ecosystem more secure by fixing and responsibly disclosing this vulnerability.

Jamie Slome 4 months ago

[Admin](#)

Sorted - the CVE has now been added to this report ♥

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us