Tabnabbing via window.opener [bookwyrm.social] in bookwyrm-social/bookwyrm

0

Valid Reported on Aug 5th 2022

Description:

Hello @bookwyrm-social I found a tabnabbing vulnerability. attack is possible due to `taget=_blank` or Tab nabbing via window.opener.

VISIT:- `https://bookwyrm.social/`

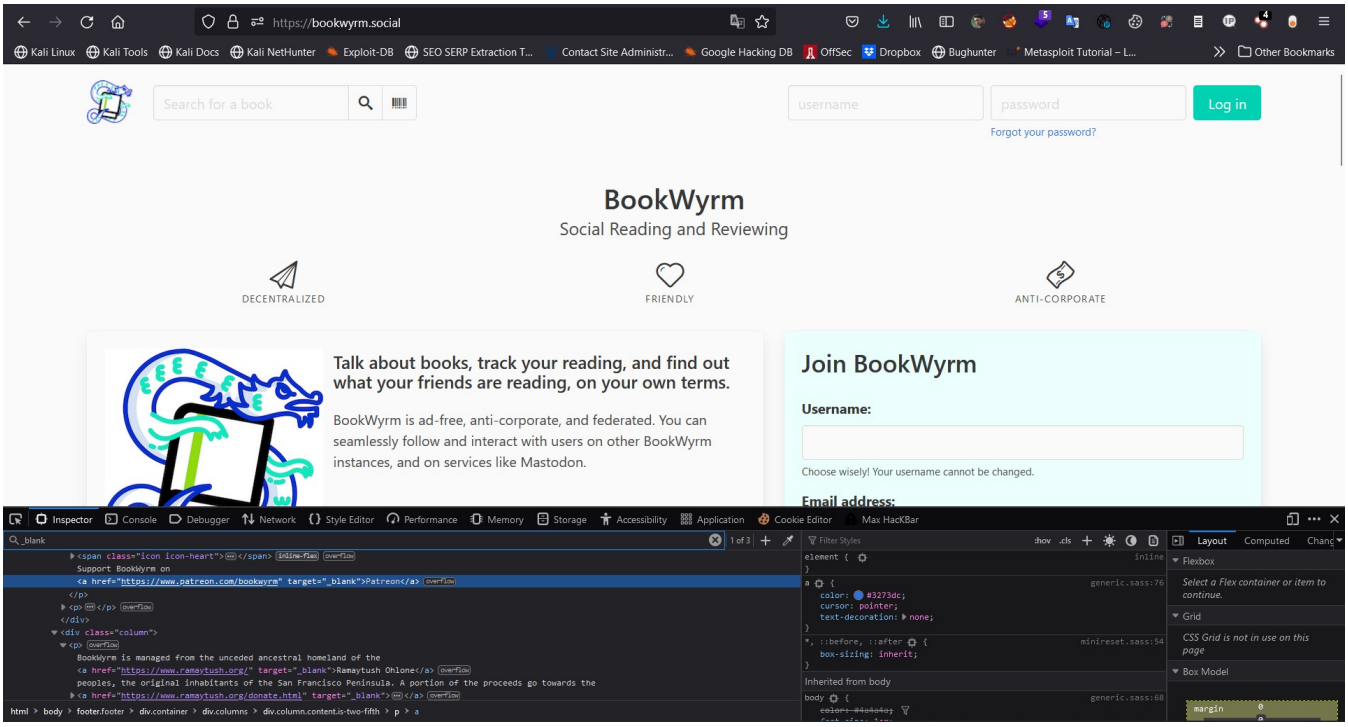
SUMMARY:

I was browsing the site and found a tabnabbing vulnerability . As per the observation I found that attack is possible due to taget=_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.

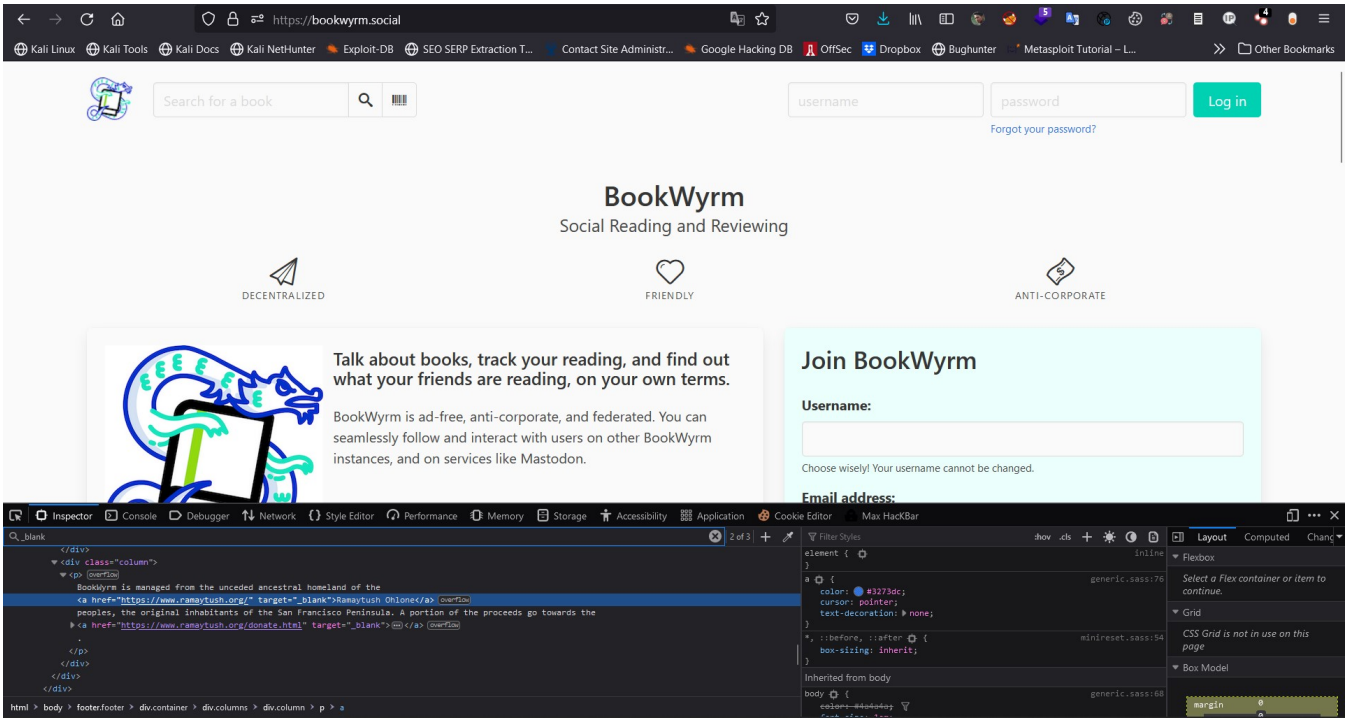
STEPS TO REPRODUCE:

1- Open the website URL :- `https://bookwyrm.social/`
2- Right-click and click on inspect element
3- Locate the cursor to Element Tab then do `CTRL+F or Search for taget="_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:



POC Screenshot 2:



MITIGATIONS:-

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

rel="nofollow noopener noreferrer">
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/bookwyrm
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

Status
Fixed

Found by

AGNIHACKERS
@agnihackers
amateur

This report was seen 822 times.

We are processing your report and will contact the **bookwyrm-social/bookwyrm** 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?

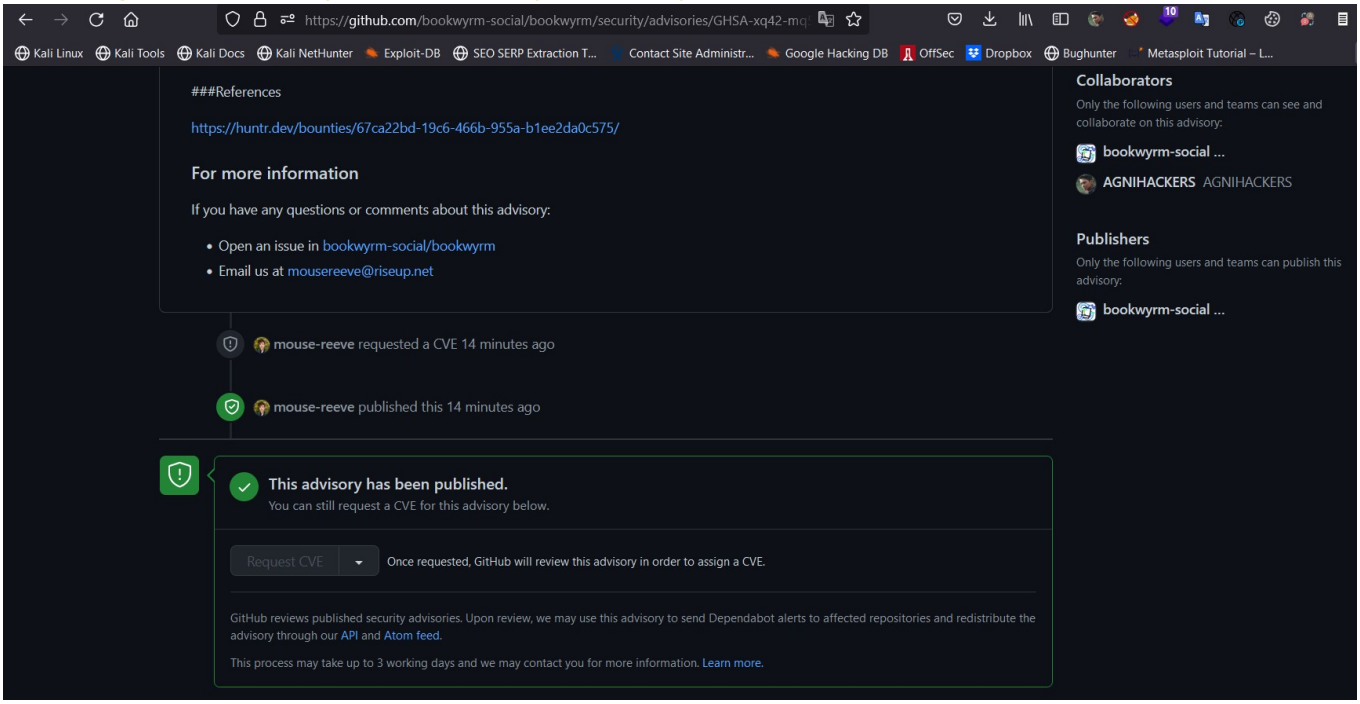
Chat with us

AGNIHACKERS 4 months ago Researcher

AGNIHACKERS 4 months ago Researcher

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

https://github.com/bookwyrm-social/bookwyrm/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

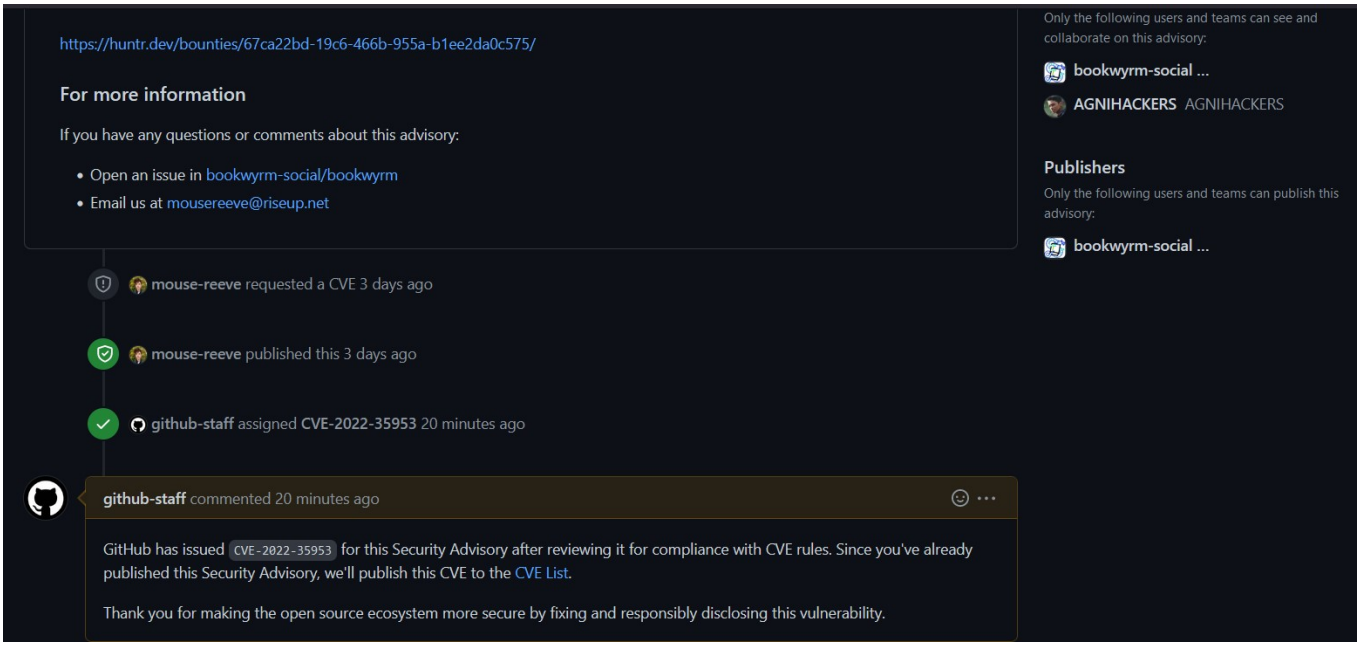
Jamie Slome 4 months ago Admin

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 :)

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/bookwyrm-social/bookwyrm/security/advisories/GHSA-xq42-mq5w-m24x`



Jamie Slome 4 months ago Admin

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

Sign in to join this conversation