Account Takeover in bookwyrm-social/bookwyrm

0

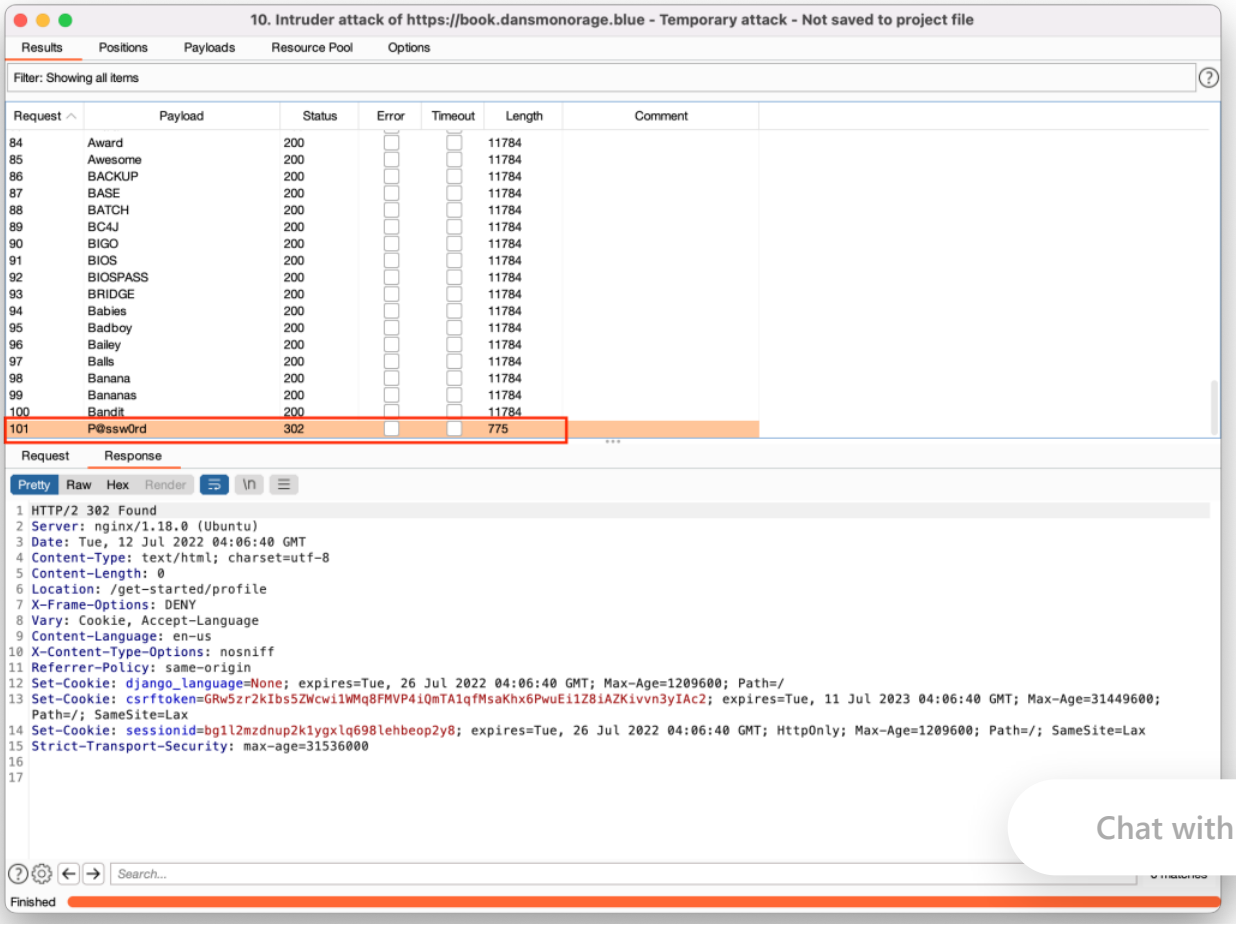
Valid Reported on Jul 12th 2022

Hello team, while i was testing on `https://book.dansmonorage.blue/login` i noticed that there is no ratelimit protection on POST login form, so an attacker can takeover the account by brute forcing the password field

Steps to reproduce:

go to `https://book.dansmonorage.blue/login`
Enter username and any password
Capture the request with burpsuite and start bruteforcing with our wordlist

POC Screenshot:



Patch recommendation:

Add ratelimit protecion on POST login endpoints/parameters

Impact

Account takeover

CVE
CVE-2022-35925
(Published)

Vulnerability Type
CWE-304: Missing Critical Step in Authentication

Severity
Critical (9.8)

Registry
Other

Affected Version
0.4.3

Visibility
Public

Status
Fixed

Found by

Akshay Ravi
@akshayravic09yc47
pro

We are processing your report and will contact the bookwyrm-social/book
hours. 4 months ago

We have contacted a member of the **bookwyrm-social/bookwyrm** team and are waiting to hear back 4 months ago

We have sent a follow up to the **bookwyrm-social/bookwyrm** team. We will try again in 7 days. 4 months ago

Akshay Ravi 4 months ago Researcher

Hello @maintainer any update on this?

We have sent a second follow up to the **bookwyrm-social/bookwyrm** team. We will try again in 10 days. 4 months ago

Mouse Reeve validated this vulnerability 4 months ago

Akshay Ravi 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 **7bbe42** 4 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Akshay Ravi 4 months ago Researcher

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

Akshay Ravi 4 months ago Researcher

@Mouse Revee @maintainer please confirm are you happy to assign a CVE? 😇

Akshay Ravi 4 months ago Researcher

@admin can you pls assign a CVE for this?

Jamie Slome 4 months ago Admin

We will wait for the maintainer to approve a CVE for this report and then proceed with one 👍

Mouse Reeve 4 months ago Maintainer

Sorry for the delay, I didn't get a notification about these comments. I've created a CVE for this and added Akshay as a collaborator.

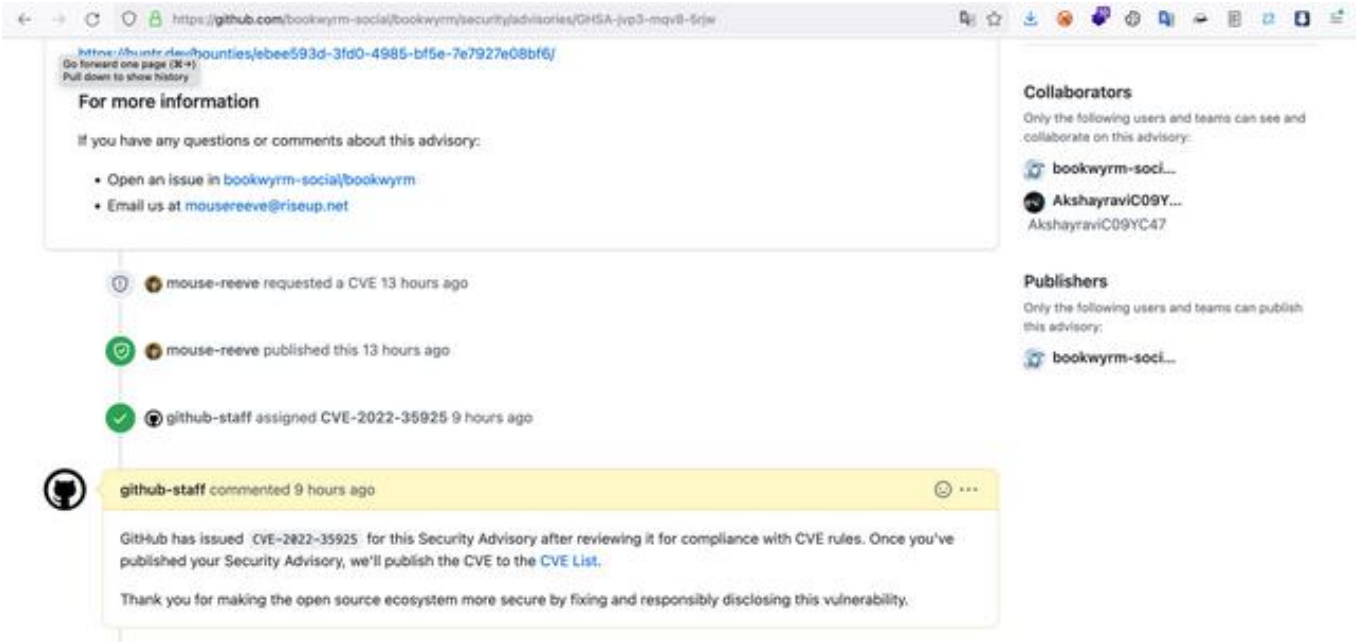
Jamie Slome 4 months ago Admin

Great 👍

Akshay Ravi 4 months ago Researcher

@admin `CVE-2022-35925` 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-jvp3-mqv8-5rjw
```



Jamie Slome 4 months ago Admin

CVE is attached to the report 👍

Jamie Slome 4 months ago Admin

@mouse - would you like me to assign a CVE to the other report or are you happy to do this via GitHub?

Mouse Reeve 4 months ago Maintainer

@jamieslome I'd be happy for you to do that. If it's preferable for me to do it in GitHub I can do that instead, just let me know, but otherwise I'll assume it's handled.

Jamie Slome 4 months ago Admin

@mouse-reeve - CVE is all sorted on the other report 👍 It should be published shortly - nothing to do on your end :)

Sign in to join this conversation

privacy policy

Chat with us