

Account Takeover in bookwurm-social/bookwurm



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:

10. Intruder attack of https://book.dansmonorage.blue - Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
84	Award	200			11784	
85	Awesome	200			11784	
86	BACKUP	200			11784	
87	BASE	200			11784	
88	BATCH	200			11784	
89	BC4J	200			11784	
90	BIGO	200			11784	
91	BIOS	200			11784	
92	BIOSPASS	200			11784	
93	BRIDGE	200			11784	
94	Babies	200			11784	
95	Badboy	200			11784	
96	Bailey	200			11784	
97	Balls	200			11784	
98	Banana	200			11784	
99	Bananas	200			11784	
100	Bandit	200			11784	
101	P@sswOrd	302			775	

Request Response

Pretty Raw Hex Render

```

1 HTTP/2 302 Found
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Tue, 12 Jul 2022 04:06:40 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 0
6 Location: /get-started/profile
7 X-Frame-Options: DENY
8 Vary: Cookie, Accept-Language
9 Content-Language: en-us
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Set-Cookie: django_language=None; expires=Tue, 26 Jul 2022 04:06:40 GMT; Max-Age=1209600; Path=/
13 Set-Cookie: csrftoken=GRw5zr2kIbs5ZWcwi1WMq8FMVP4iQmTA1qfMsaKhx6PwuEi1Z8iAZKivvn3yIAc2; expires=Tue, 11 Jul 2023 04:06:40 GMT; Max-Age=31449600; Path=/; SameSite=Lax
14 Set-Cookie: sessionid=bg1l2mzdnp2k1y9xlg698lehbeop2y8; expires=Tue, 26 Jul 2022 04:06:40 GMT; HttpOnly; Max-Age=1209600; Path=/; SameSite=Lax
15 Strict-Transport-Security: max-age=31536000
16
17

```

Finished

Chat with us

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

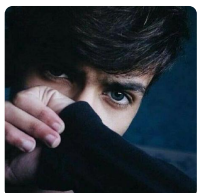
Visibility

Public

Status

Fixed

Found by



Akshay Ravi

@akshayravic09yc47

pro ▼

This report was seen 590 times.

We are processing your report and will contact the [bookwyrmsocial/bookwyrmsocial](#) team within 24 hours. 4 months ago

Chat with us

We have contacted a member of the **bookwyrmsocial/bookwyrms** team and are waiting to hear back 4 months ago

We have sent a follow up to the **bookwyrmsocial/bookwyrms** 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 **bookwyrmsocial/bookwyrms** 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 Reeve @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?

Chat with us

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/bookwyrms-social/bookwyrms/security/advisories/GHSA-jvp3-mqv8-5rjw>

Jamie Slome 4 months ago

Admin

CVE is attached to the report 👍

Chat with us

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

2022 © 4l8sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

part of 4l8sec

company

about

team

Chat with us

[privacy policy](#)

[Chat with us](#)