Cross-Site Request Forgery (CSRF) in bookstackapp/bookstack

0

✓ Valid Reported on Nov 10th 2021

Description

Login CSRF via /register/confirm/{token} endpoint.

Proof of Concept

1: Register account with the same username as our victim, an email confirmation will take place
2: Retrieve token from email.
3: Send a link http://[BOOKSTACK_APP_URL]/register/confirm/{token} to user.
4: When the user clicks the link, they will be logged into the account, even if they already have an active session on Bookstack.

Impact

This vulnerability can be used to trick the user into unknowingly logging into an attacker account. They might then perform sensitive actions which will then be logged into the attacker's account. This can be chained with the fact that Bookstack allows duplicate usernames and hence the victim might believe the attacker account is actually theirs.

Recommended Fix

There are two possible remediations I can think of for this: A) Use a middle page for confirming the email and then logging in (for example, a showConfirm and then a confirm action) B) Do not login the user after email confirmation. Additionally may want to prevent duplicate usernames to prevent confusion.

Occurrences

RegistrationService.php L85L124

prevent duplicate username registration

ConfirmEmailController.php L80L83

prevent logging in after email confirmation

CVE
CVE-2021-3944
(Published)

Vulnerability Type
CWE-352: Cross-Site Request Forgery (CSRF)

Severity
Low (3.1)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

Dan Brown
@ssddanbrown
maintainer

This report was seen 241 times.

We are processing your report and will contact the bookstackapp/bookstack team within 24 hours. a year ago

Chat with us

Dan Brown a year ago

Thanks for re-opening, Copying my message from the other submission below for context. Will validate and add this to our next release milestone.

I guess it could be an potential attack vector although would need to be quite targeted and on an instance with open registration. Don't think it's worth rushing out a patch release for this one but instead look to address for next feature release (Still within the next month though). I'll probably prefer option B (Require re-login) although we'll need to add some messaging to communicate the journey to users. As part of this I'll do a bit of an audit for other similar login scenarios.

In regards to usernames, thanks for the advice but these aren't actually intended to be 'username' handles, but represent the user's actual name. It's not something I'd want to be forcing uniqueness upon.

Dan Brown validated this vulnerability a year ago

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Dan Brown a year ago

Thanks again @haxatron for discovering and reporting

Dan Brown marked this as fixed in 21.11 with commit 88e6f9 a year ago

Dan Brown has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

RegistrationService.php#L85L124 has been validated ✓

ConfirmEmailController.php#L80L83 has been validated ✓

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team