Unrestricted Upload of File with Dangerous Type in bookstackapp/bookstack

0

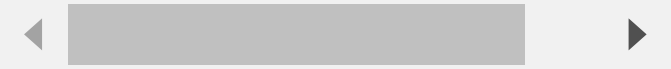
Valid Reported on Oct 25th 2021

Description

The image extension validation service for Base64 image extraction in new Bookstack version is flawed as it uses the vulnerable trim function. This allows attackers to upload malicious files with broken extension, such as pngr, and browsers will interpret broken extension hosted on the server as HTML.

Payload 1

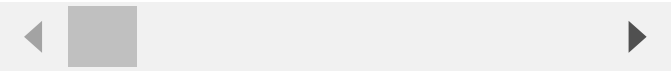
```
POST /api/pages
{
    "book_id": 1,
    "name": "My API Page",
    "html": "<img src='
    "tags": [
        {"name": "Category", "value": "Not Bad Content"},
        {"name": "Rating", "value": "Average"}
    ]
}
```



See that the file is stored on the server, an attacker can send this file to others to perform reflected XSS. The CSP does not help because CSP is on application layer and hence not applied to static files.

Payload 2

```
POST /api/pages
{
    "book_id": 1,
    "name": "My API Page",
    "html": "<img src='
    "tags": [
        {"name": "Category", "value": "Not Bad Content"},
        {"name": "Rating", "value": "Average"}
    ]
}
```



This creates a phishing page on the server, we can modify where the credentials are sent to if we want

Root Cause

There is a subtle difference between single-quoted strings (literals) and double-quoted strings. In double-quoted strings \r\n will be interpreted as carriage-return and newline, but in single-quoted literals the characters will be interpreted as-is. Bookstack uses the trim function with only single-quoted string, so attackers can bypass the file validation check.

```
in_array(trim($extension, '. \t\n\r\0\x0B'), static::$supportedExtensions);
```

So if the $extension = pngr, then the trim function will strip the 'r' character so that it becomes png and thus gets validated.

Impact

An attacker with page edit permissions can upload files to:
1: Host phishing pages and obtain password of admin users
2: Javascript execution (XSS) to get the cookie.

Occurrences

ImageRepo.php L41

CVE
CVE-2021-3906
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Medium (5.4)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

haxatron
@haxatron
pro

This report was seen 419 times.

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

haxatron submitted a **patch** a year ago

haxatron a year ago — Researcher

fix located here:
https://github.com/Haxatron/BookStack/commit/64937ab826b56d086af9ecea532510d37520ebc8

haxatron modified the report a year ago

haxatron modified the report a year ago

haxatron modified the report a year ago

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 — Maintainer

Thanks once again @haxatron. Good spot, That's what I get for paying more attention to syntax standards.

Fix looks good of course, will confirm that off when ready to deploy the update with the fix. Just want to keep it relatively private until then.

haxatron a year ago — Researcher

No problem! Thanks for reviewing this report!

Dan Brown marked this as fixed with commit **64937a** a year ago

haxatron has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

ImageRepo.php#L41 has been validated ✓

Jamie Slome a year ago — Admin

CVE published!

Sign in to join this conversation