Cross-site Scripting (XSS) - Stored in getgrav/grav

2

Valid Reported on Feb 19th 2022

Description

Stored XSS is a vulnerability in which the attacker can execute arbitrary javascript code in the victim's browser. The XSS payload is stored in a webpage and it gets executed whenever someone visits that webpage.
I used `&#10` (Line Feed character) in the `href` attribute of `<a>` tag to bypass the xss checks of `invalid_protocols` (e.g. javascript:) happening in the application.

Proof of Concept

STEP 1: A low-priv user create a page with the following payload:

```
<a href="javascript&#10:alert(document.domain)">CLICK HERE TO EXPLOIT THIS XSS</a>
```

STEP 2: Victim visit the page and click on `CLICK HERE TO EXPLOIT THIS XSS`
XSS alert will show the domain name.

Impact

Attacker can execute arbitrary javascript code in the victim's browser

Occurrences

Security.php L82-L239

CVE
CVE-2022-0743
(Published)

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

Severity
Medium (4.6)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

Fixed by

Djamil Legato
@w00fz
maintainer

This report was seen 543 times.

We are processing your report and will contact the **getgrav/grav** team within 24 hours.
9 months ago

We have contacted a member of the **getgrav/grav** team and are waiting to hear back
9 months ago

We have sent a follow up to the **getgrav/grav** team. We will try again in 7 days. 9 months ago

A **getgrav/grav** maintainer validated this vulnerability 9 months ago

Rohan Sharma has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Djamil Legato 9 months ago Maintainer

Thanks for this @r0hansh . I accepted it, however this is quite a stretch to be considered a medium severity vulnerability.
Looks like you have been reporting a bunch of variations of this vulnerability. consider it as such to be honest. Getting to be able to add that content requi bypassed several other level of security that Grav has in place, like, for instance, logging in. The

XSS detection is just a visual aid for content editors that admins can enable, and it is specifically for the optional admin plugin.

There are endless variations of what you have reported and we won't consider them vulnerabilities going forward.

Thanks.

Rohan Sharma 9 months ago Researcher

Hi Djamil,

This is my `second` submission to grav. Last time, you guys fixed the vulnerability and did not asked for retest. So, I tested your patch and found a bypass to exploit this vulnerability. I don't have the intent to submit same vulnerabilities again and again. It's just a bypass to what you guys fixed.

I started my research after reading this `medium` severity report:
https://huntr.dev/bounties/b1182515-d911-4da9-b4f7-b4c341a62a8d/. As mentioned a low-priv user, having access to create/update pages privilege can still exploit this vulnerability.

Since, it is your project, so I will respect your final decision on whether this class can be considered as a security bug or not.
I will be happy to retest this bug, once you fix it.

Djamil Legato 9 months ago Maintainer

Thanks Rohan,
I might have mistakenly thought you were the author of that other report you linked as well. In my eyes we just seem to only get reports about variations of this, which is exactly the point I was making above. There are just infinite variations and it is not as critical as a report like these make it sound. It certainly is not a medium severity security issue, if anything we would consider it as a bug and happily fix if reported via GitHub.

Appreciate your research on this though! I also proceeded fixing the issue, see https://github.com/getgrav/grav/commit/3dd0cabeac9835fe64dcb4b68c658b39f1f6be2f

Rohan Sharma 9 months ago Researcher

Hi Djamil,

the fix looks good to me.

We have sent a fix follow up to the **getgrav/grav** team. We will try again in 7 days. 9 months ago

Djamil Legato marked this as fixed in **1.7.31** with commit **3dd0ca** 9 months ago

Djamil Legato has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Security.php#L82-L239 has been validated ✔

Sign in to join this conversation