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

0

Valid Reported on Jan 2nd 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 `&#58` instead of `:` in the `href` attribute of `<a>` tag to bypass the xss checks happening in the application.

Proof of Concept

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

```
<a href="javascript&#58alert(document.domain)">CLICK HERE TO EXPLOIT THIS >
```

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-2022-0268
(Published)

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

Severity

Medium (5.7)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

Fixed by

Matias Griese
@mahagr
maintainer

This report was seen 377 times.

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

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

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

We have sent a second follow up to the **getgrav/grav** team. We will try again in 10 days.
10 months ago

Matias Griese validated this vulnerability 10 months ago

Rohan Sharma has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Matias Griese marked this as fixed in 1.7.28 with commit 6f2fa9 10 months ago

Matias Griese marked this as fixed in 1.7.28 with commit 0f2fd9 10 months ago

Matias Griese 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