stored xss in getgrav/grav

Valid Reported on Mar 26th 2022

0

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

Proof of Concept

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

```
a'"></title></script><img src=x onerror=confirm(document.domain)></p>
```

2. Victim visit the page and see xss is executed
XSS alert will show the domain name.

Impact

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

Occurrences

Security.php L32-L78 Security.php L150-L265 Security.php L83-L143

CVE
CVE-2022-1173
(Published)

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

Severity
High (8.2)

High (8.2)

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

Fixed by

Matias Griese
@mahagr
maintainer

This report was seen 533 times.

We are processing your report and will contact the **getgrav/grav** team within 24 hours. 8 months ago

We have contacted a member of the **getgrav/grav** team and are waiting to hear back 8 months ago

We have sent a follow up to the **getgrav/grav** team. We will try again in 7 days. 8 months ago

A **getgrav/grav** maintainer modified the report 8 months ago

A **getgrav/grav** maintainer 8 months ago Maintainer

I consider admin privileges to be high -- you do need an admin account to perform this attack.

I was able to reproduce the issue.

A **getgrav/grav** maintainer validated this vulnerability 8 months ago

ranjit-git has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Matias Griese 8 months ago Maintainer

Should be fixed now, waiting for a release.

We have sent a fix follow up to the **getgrav/grav** team. We will try again in 7 days. 8 months ago

We have sent a second fix follow up to the **getgrav/grav** team. We will try again in 10 days. 8 months ago

We have sent a third and final fix follow up to the **getgrav/grav** team. This report is now considered stale. 7 months ago

Matias Griese marked this as fixed in **1.7.33** with commit **1c0ed4** 7 months ago

Matias Griese has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Security.php#L32-L78 has been validated ✓

Security.php#L83-L143 has been validated ✓

Security.php#L150-L265 has been validated ✓

Sign in to join this conversation