Bypass filter - Stored XSS in Resources in francoisjacquet/rosariosis

0

✓ Valid Reported on Jun 3rd 2022

Description

Website does incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. This fix for this bug `https://huntr.dev/bounties/dcf87c0b-6188-4817-8798-ef1e2581b15a/` can be bypassed using bellow payload

```
jAvAsCrIpT:alert(origin)
```

Steps to reproduce [it works on Firefox (not in chromium based browsers)]

1.Go to `https://www.rosariosis.org/demonstration/ and login with administrator account`
2.Go to `https://www.rosariosis.org/demonstration/Modules.php?modname=Resources/Resources.php`
3.Create new link with content `jAvAsCrIpT:alert(origin)`
4.Click the link and observe a pop up

Image POC

`https://drive.google.com/file/d/11F1mjqytYIgmMVtOEC4EbOHhvVi0pEPh/view?usp=sharing`
`https://drive.google.com/file/d/1dGPRWE6KRf2bfOezRblbWtHAwM1P29iL/view?usp=sharing`

Impact

User clicking the link can be affected by malicious javascript code created by the attacker.

Chat with us

CVE
CVE-2022-1997

(Published)

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

Severity
High (8.8)

Registry
Other

Affected Version
v8.9.6

Visibility
Public

Status
Fixed

Found by

Domiee13
@domiee13
pro

Fixed by

François Jacquet
@francoisjacquet
unranked

This report was seen 608 times.

We are processing your report and will contact the **francoisjacquet/rosariosis** team within 24 hours. 6 months ago

We have contacted a member of the **francoisjacquet/rosariosis** team and are waiting to hear back 6 months ago

François Jacquet validated this vulnerability 6 months ago

Domiee13 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

François Jacquet marked this as fixed in **9.0** with commit **6b22c0** 6 months ago

François Jacquet has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us