huntr

Cross-site Scripting (XSS) - Stored in francoisjacquet/rosariosis

0

✓ Valid Reported on Nov 27th 2021

Description

I found XSS in the file upload function of the message function.

Proof of Concept

Step

1.First, access the latest version of the demo environment.
`"Https://www.rosariosis.org/demonstration/index.php"`
2.Then log in with your student account. `Student: username and password “student“`
3.After logging in, access "MESSAGING > Write" from the menu on the left.
(`/demonstration/Modules.php?modname=Messaging/Write.php`)
4.Then enter the title and message as appropriate.
5.Now upload the SVG file containing XSS to "File Attached".
6.Finally, select "Teach Teacher" as the destination and send.
7.Log in from here with your teacher's account. `Teacher: username and password “teacher“`
8.After logging in, access "MESSAGING > Messages" from the menu and select the message you just sent.
9.Then click on the last attached file and a pop-up screen will appear.

Summary

-Endpoint: `POST /demonstration/Modules.php?modname=Messaging/Write.php&search_modfunc=list&recipients_key=staff_id&subject=<title>&message=<message>&recipients_ids[0]=2&send=Send`
-Attachment: `SVG file`
-Test Payload: `<script type="text/javascript">alert(document.cookie)</scri`

Impact

This vulnerability can steal a user's cookie.

References

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)

CVE
CVE-2022-3072
(Published)

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

Severity
High (8)

Visibility
Public

Status
Fixed

Found by

morioka12
@scgajge12
unranked

Fixed by

François Jacquet
@francoisjacquet
unranked

This report was seen 860 times.

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

Chat with us

morioka12 modified the report a year ago

François 7 months ago

Maintainer

Hello @scgajge12

Thank you very much for your report.
SVG upload has been disabled for now.
I may introduce SVG sanitize routine in the future.

François Jacquet validated this vulnerability 7 months ago

morioka12 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

François Jacquet marked this as fixed in 8.9.3 with commit dcd3b8 7 months ago

François Jacquet has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

morioka12 3 months ago

Researcher

@maintainer , I would be glad if you could approve for CVE.

morioka12 3 months ago

Researcher

@admin can you pls assign a CVE for this?

Jamie Slome 3 months ago

Admin

Same here, I would recommend dropping a comment on the commit SHA as we require the maintainer(s) go ahead to publish a CVE 👍

François 3 months ago

Maintainer

@morioka12 I approve the CVE.

morioka12 3 months ago Researcher

Thanks to François Jacquet for the approval.

@admin , I got approval from the maintainer.

Jamie Slome 3 months ago Admin

The CVE has been assigned and will be published automatically in the next couple of hours 👍

morioka12 3 months ago Researcher

Thank you very much !

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

Chat with us