New issue

Jump to bottom

Cross Site Script Vulnerability on "Main settings" #2320

Closed **Songohan22** opened this issue on May 14, 2020 · 4 comments

Songohan22 commented on May 14, 2020 • edited

Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Main" feature

To Reproduce
Steps to reproduce the behavior:

1. Log into the panel.
2. Go to "administration/settings_main.php"
3. Click edit on "Site footer"
4. Insert payload:
   ! [ ] (https://github.com/Songohan22/PHP_Furion/blob/master/4.PNG)
   <img src=xx onmouseover=alert('xss')>
5. Click: "Save Setting"
6. Login as member
7. Go to Site footer
8. XSS Alert Message

Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page.

Screenshots

1. Go to "administration/settings_main.php"
   ! [ ] (https://github.com/Songohan22/PHP_Furion/blob/master/1.PNG)
2. Insert payload: <img src=xx onmouseover=alert('xss')> on "Site footer"
   ! [ ] (https://github.com/Songohan22/PHP_Furion/blob/master/2.PNG)
3. XSS Alert Message
   ! [ ] (https://github.com/Songohan22/PHP_Furion/blob/master/3.PNG)

Desktop (please complete the following information):

- OS: Kali
- Browser: Firefox
- Version of Browser: 68.6

RobiNN1 commented on May 14, 2020 • edited — Contributor

This is not a really big problem, only a trusted person has access to this section... Big problem is if you find XSS as a member without admin rights.

RobiNN1 changed the title ~~Cross Site Script Vulnerability on "Main" in PHP-Fusion 9.0.35~~ **Cross Site Script Vulnerability on "Main settings"** on May 14, 2020

Songohan22 commented on May 14, 2020 • edited — Author

@RobiNN1 thank you for reply
"This is not a really big problem, only a trusted person has access to this section... Big problem is if you find XSS as a member without admin rights."
Yep....But I think you still fix it
Impacts: Stored XSS, with remote code execution on the victim's browser, such as stealing credentials, sessions, or delivering malware to the victim.

Thank you.

RobiNN1 commented on May 14, 2020 — Contributor

php-fusion/php-fusion@ 5a024ca

1

RobiNN1 closed this as completed on May 14, 2020

Songohan22 commented on May 14, 2020 — Author

@RobiNN1
You work very well. I will retest this issue.
Thank you.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants