

New issue

[Jump to bottom](#)

BBCode URL Tag Script Injection "Shoutbox" PHP Fusion 9.0.36 #2329

🔒 Closed Songohan22 opened this issue on May 18, 2020 · 5 comments

Songohan22 commented on May 18, 2020 • edited by RobiNN1

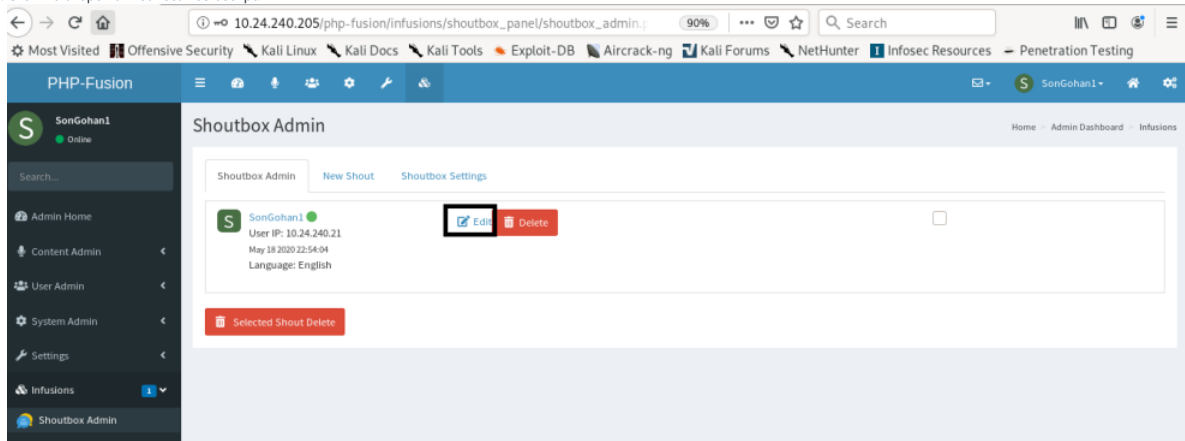
Describe the bug

BBCode URL Tag Script Injection "Shoutbox Admin"

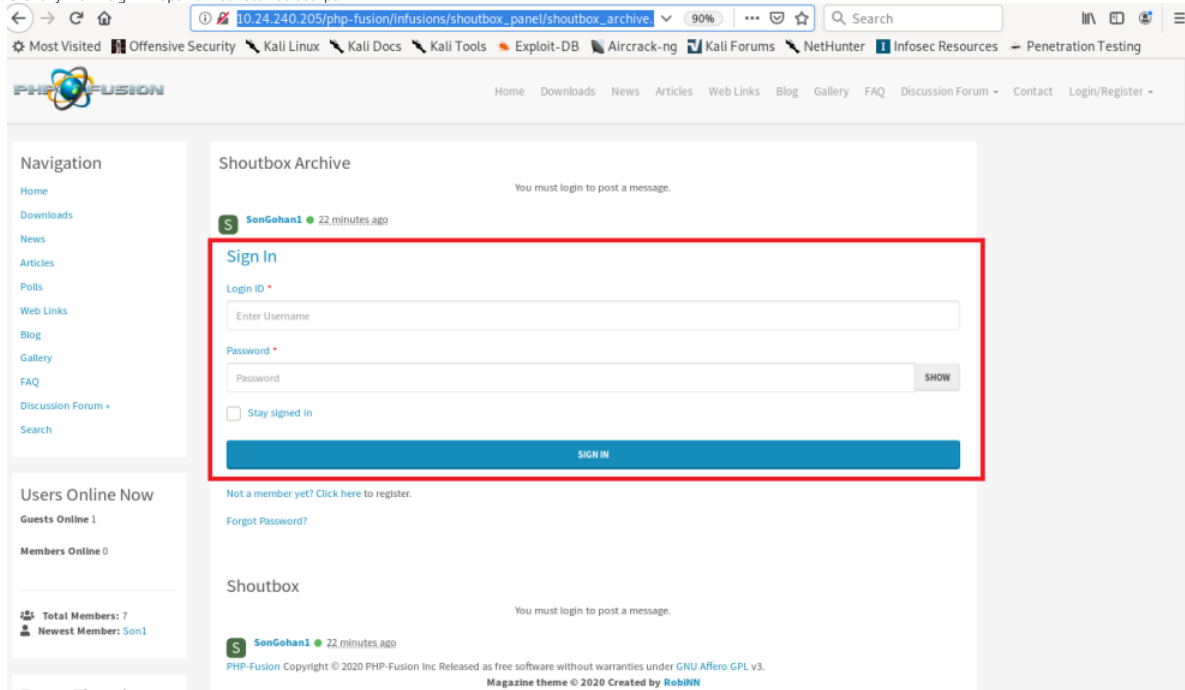
To Reproduce

Steps to reproduce the behavior:

1. Log into the panel.
2. Go to "/php-fusion/infusions/shoutbox_panel/shoutbox_admin.php"
3. Click "New Shout"
4. Insert script injection: `[url]https://nvd.nist.gov?url onmouseover=javascript:alert(String.fromCharCode(88,83,83));[/url][url]`
5. Click " Send Message"
6. Click "Edit" open url redirect insert script.



7. Logout user.
8. Access link "/php-fusion/infusions/shoutbox_panel/shoutbox_archive.php"
9. Click any "Form Sign In" open url redirect insert script.



Impact

An attacker can use this vulnerability to redirect users to other malicious websites, which can be used for phishing and similar attacks.

Video POC

Video POC link: <https://drive.google.com/open?id=1g9x6B-K338qzHjWtbEHCadpyPLx-daX>

Desktop (please complete the following information):

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

RobiNN1 commented on May 18, 2020

Contributor

lol you really don't trust your administrators 🤔

Songohan22 commented on May 18, 2020

Author

@RobiNN1

It can be sent from one member.

I will record the video and send it back to you.

Very sorry if the above description is not correct.

Thank you.

RobiNN1 commented on May 18, 2020

Contributor

No need, issue is confirmed.

  Songohan22 changed the title **BBCode URL Tag Script Injection "Shoutbox Admin" PHP Fusion 9.0.36** BBCode URL Tag Script Injection "Shoutbox" PHP Fusion 9.0.36 on May 18, 2020

Songohan22 commented on May 18, 2020

Author

@RobiNN1,

I Hope you fix it ASAP!

Thank you.

r0ck3t1973 commented on May 19, 2020

Hi @RobiNN1

also: Impact: <https://jeffchannell.com/Other/bbcode-xss-howto.html>

 RobiNN1 added a commit that referenced this issue on May 19, 2020

 Fix #2329, #2330

9ee14d4

 RobiNN1 closed this as completed on May 19, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

