New issue

Jump to bottom

Cross Site Script Vulnerability on "Shoutbox Admin" in PHP-Fusion feature 9.03.60 #2328

Closed r0ck3t1973 opened this issue on May 18, 2020 · 1 comment

r0ck3t1973 commented on May 18, 2020 • edited by RobiNN1

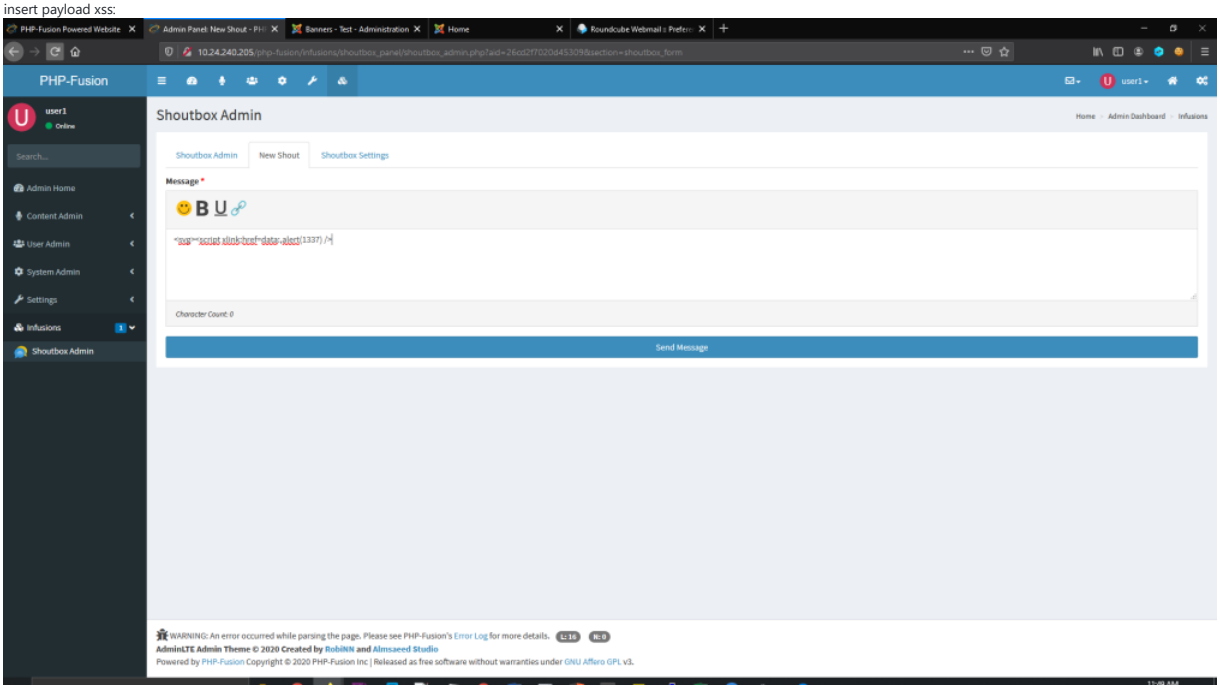
Describe the bug
An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Shoutbox" feature.

To Reproduce
Steps to reproduce the behavior:

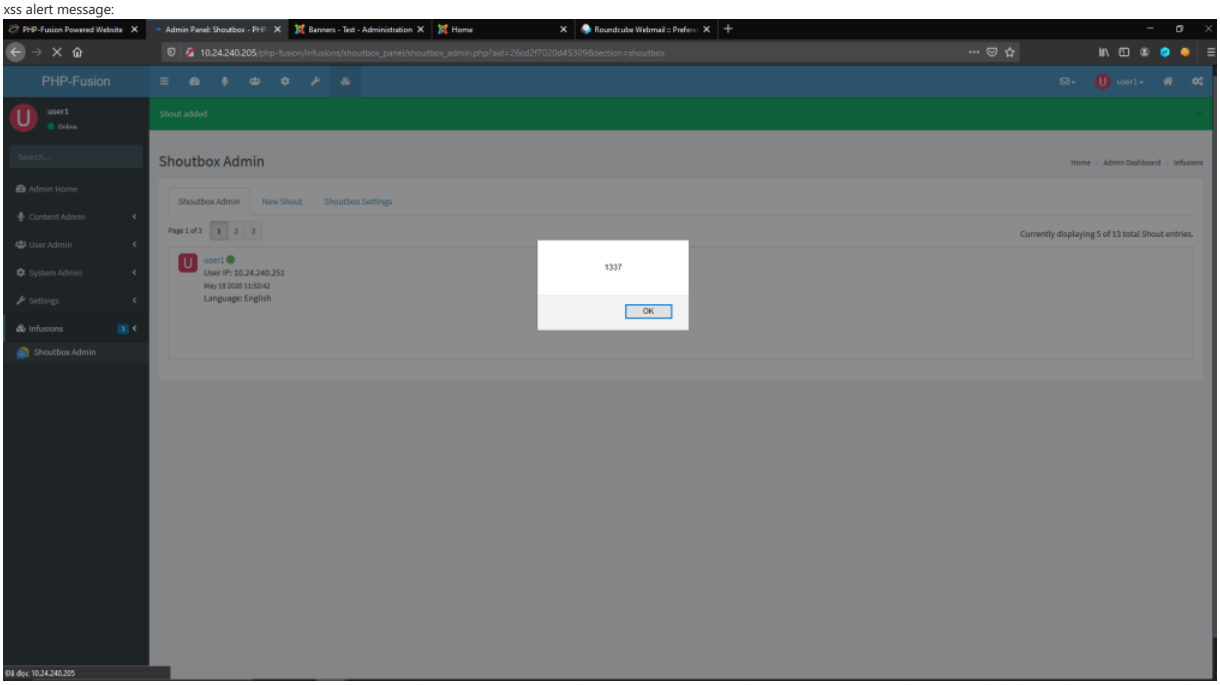
1. Login into the panel
2. Go to 'php-fusion/infusions/shoutbox_panel/shoutbox_admin.php'
3. Click on 'Infusion' -> 'Shoutbox Admin' -> 'New Shout'
4. Insert payload XSS:
   ```
   <svg><script xlink:href=data:,alert(1337) />
   ```
5. Send Message
6. xss alert message

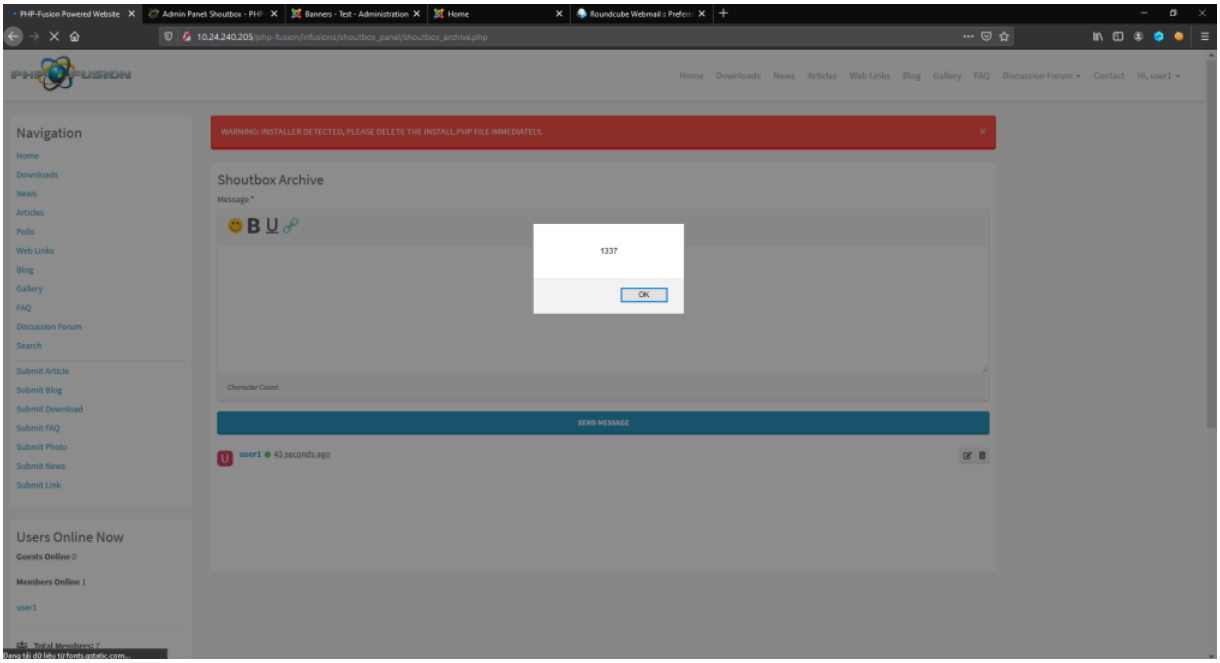
Impact
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Screenshots
insert payload xss:



xss alert message:





Desktop (please complete the following information):

- OS: Windows
- Browser: All
- Version

RobiNN1 added a commit that referenced this issue on May 18, 2020

`Fix xss #2326, #2328` bab89fb

RobiNN1 closed this as completed on May 18, 2020

---

r0ck3t1973 commented on Jun 7, 2020 Author

Hi **@RobiNN1**

Please note that all requests within a single browser session will share a single reference number and will only receive a confirmation email for the first request. If you refresh your browser or close and reopen your browser between each request, you will receive a new confirmation email and reservation number for each request.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants