# Cross Site Script Vulnerability on "Registration Settings" #2323

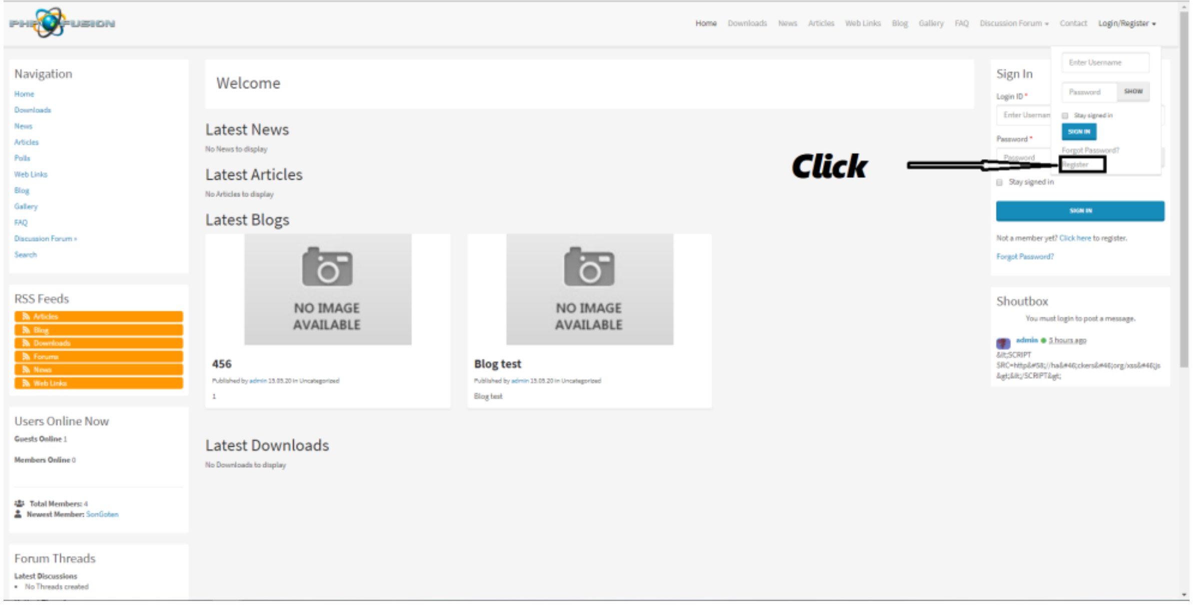
Closed   **Songohan22** opened this issue on May 15, 2020 · 1 comment

**Songohan22** commented on May 15, 2020

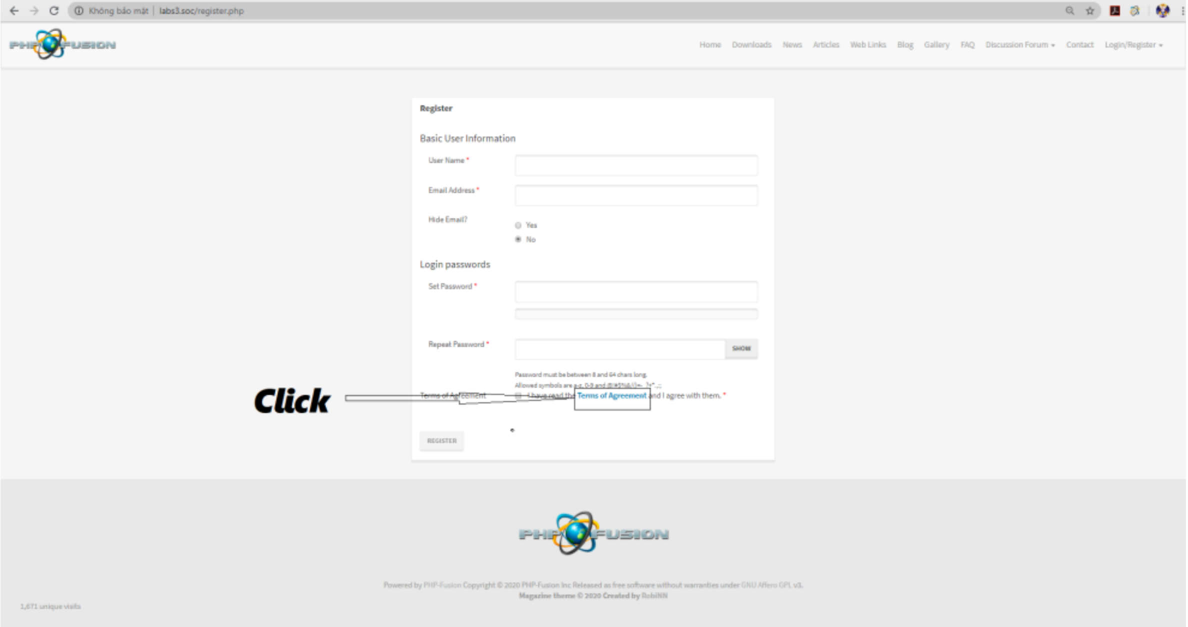
**Describe the bug**
An authent.icated malicious user can take advantage of a Stored XSS vulnerability in the "Registration Settings" feature.

**To Reproduce**
Steps to reproduce the behavior:

1. Log into the panel.
2. Go to "/administration/settings_registration.php"
3. Click on Registration.
4. Insert payload:
   `<img src=xx onmouseover=alert('xss')> </img>`
5. Click "Save Setting"
6. Go to "/home.php", click Register



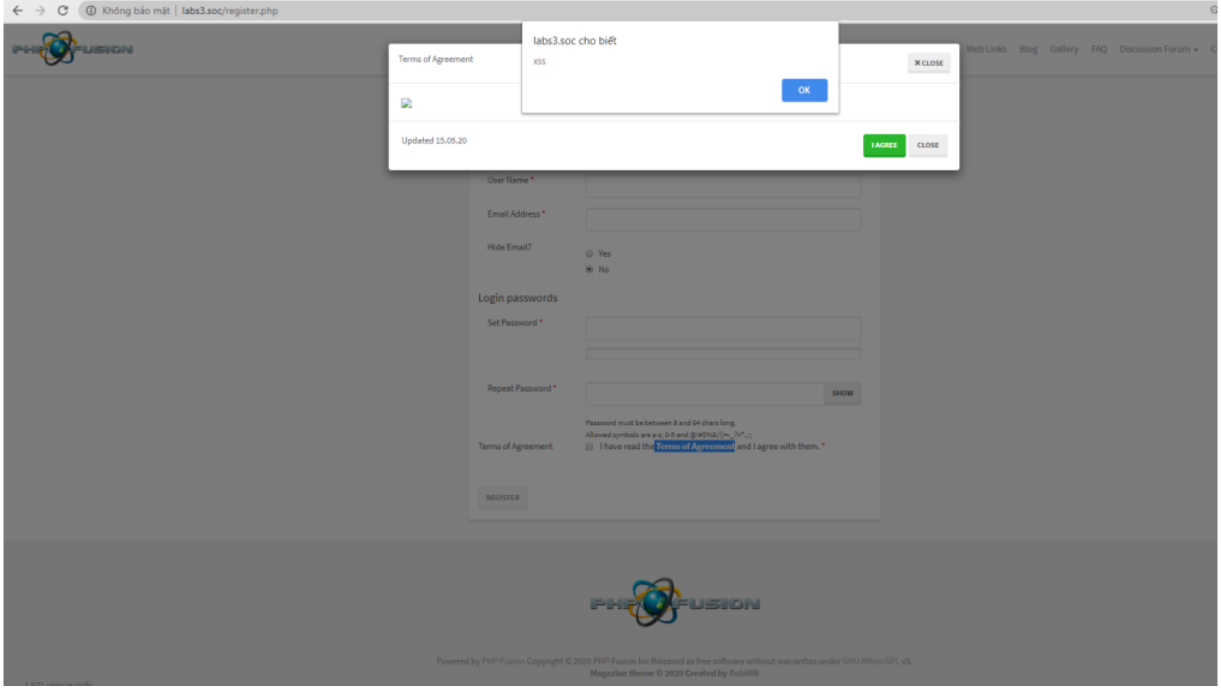
7. Click " Terms of Agreement"



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**
XSS Alert Message:



Không bảo mật | labs3.soc/register.php

labs3.soc cho biết

XSS

Terms of Agreement

Updated 15.05.20

User Name *

Email Address *

Hide Email? ○ Yes ● No

Login passwords

Set Password *

Repeat Password *

Password must be between 8 and 64 chars long.
Allowed symbols are a-z, 0-9 and @!#$%&/()=-_?+*.,:;

Terms of Agreement □ I have read the Terms of Agreement and I agree with them. *

Powered by PHP-Fusion Copyright © 2020 PHP-Fusion Inc Released as free software without warranties under GNU Affero GPL v3.
Magazine theme © 2020 Created by RobiNN

**Desktop (please complete the following information):**

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

**RobiNN1** commented on May 15, 2020 Contributor

did you really download the latest version?

R **RobiNN1** closed this as completed on May 15, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants