

New issue

# Cross Site Scripting Vulnerability on "Import Mail" feature in PHP List #667

**⊙ Closed Songohan22** opened this issue on May 26, 2020 · 2 comments

Songohan22 commented on May 26, 2020 • edited 🕶

## Describe the bug

An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Import Mail" feature.

## To Reproduce

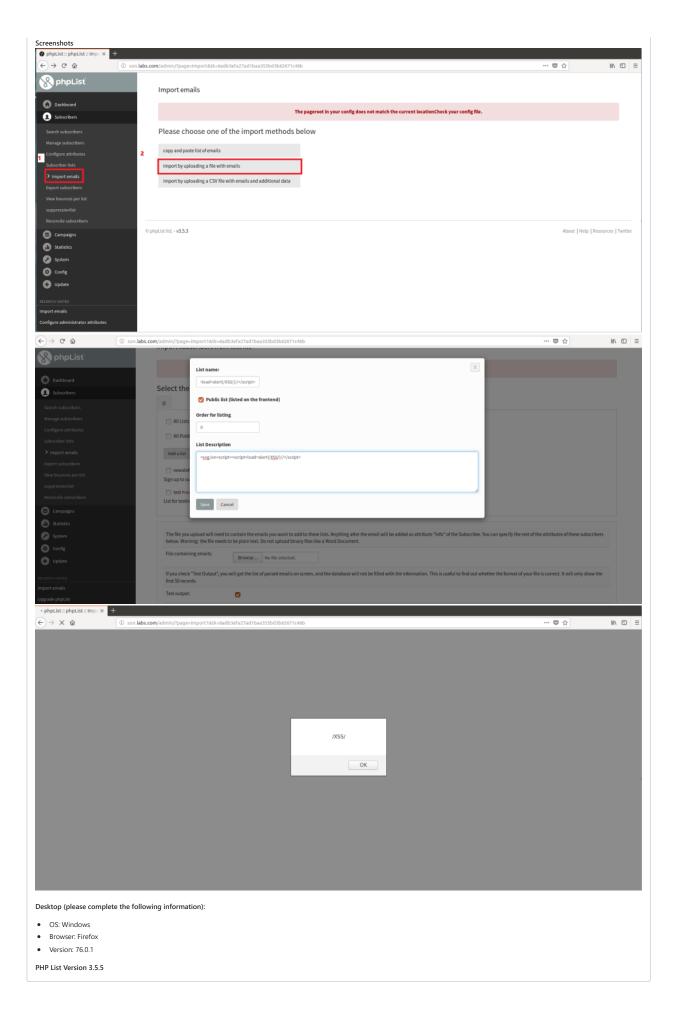
Steps to reproduce the behavior:

- 1. Log into the panel.
- 2. Go to "/admin/?page=import&tk=6adb3efa27ad1baa355bd3b62671c46b"
- 3. Click "import by uploading a file with emails"
- 4. Insert payload:
- <svg/on<script><script>load=alert('XSS')//</script>
- 5. Click "Save "
- 6. View the preview to trigger XSS.
- 7. View the preview to get in request and such Stored XSS

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

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.

Jump to bottom



Songohan22 changed the title Cross Site Scripting Vulnerability on "Import Mail" feature in Lavelite Cross Site Scripting Vulnerability on "Import Mail" feature in PHP List on May 26, 2020 Author Songohan22 commented on May 26, 2020 Hi @suap Please review it! Thanks michield commented on May 26, 2020 Member Resolved with 9c4515c 1 michield closed this as completed on May 26, 2020 Assignees No one assigned Labels None yet Projects None yet Milestone No milestone Development No branches or pull requests 2 participants