

New issue

[Jump to bottom](#)

Cross Site Scripting Vulnerability on "Import subscribers" feature in PHPList 3.5.4 upload file SVG. #678

🔒 Closed Songohan22 opened this issue on Jun 7, 2020 · 2 comments

Songohan22 commented on Jun 7, 2020

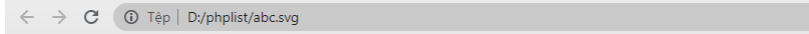
Describe the bug

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

To Reproduce

Steps to reproduce the behavior:

1. Log into the panel.
2. Go to "/admin/?page=import2&tk=93e3e3e3bbd0bd48b788a384c549813b"
3. Click "Browse"
4. Import payload file SVG:



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<svg xmlns="http://www.w3.org/2000/svg" onload="alert(document.domain)"/>
```

5. Click button "Import"
6. Click select "Email".
7. Click button "CONTINUE"
8. View the preview to trigger XSS.
9. View the preview to get in request and such Stored XSS.

Expected behavior

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.

Impact

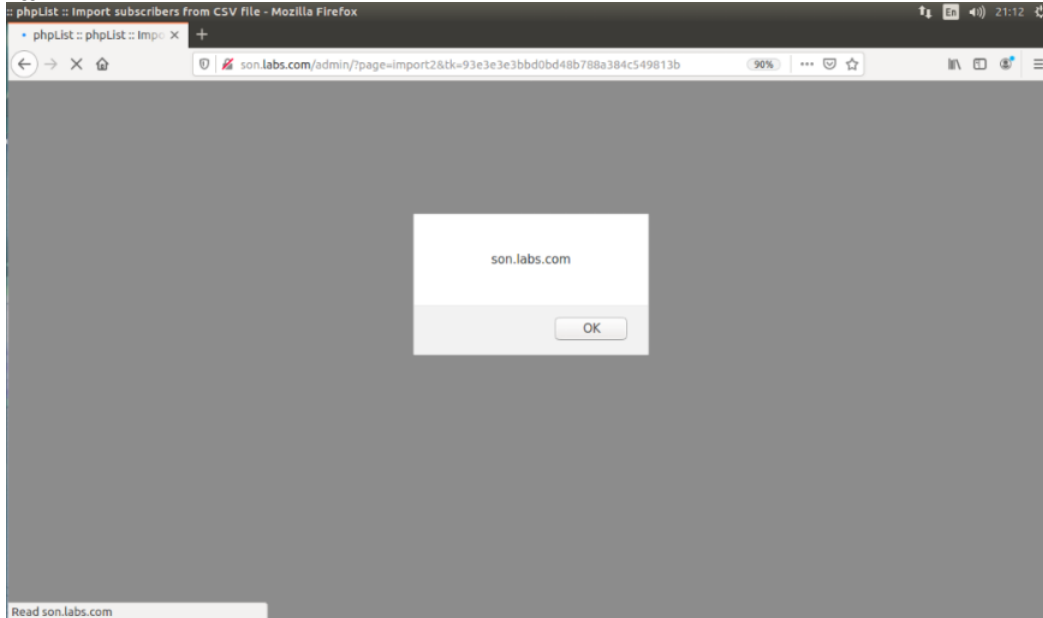
Commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Screenshots

The screenshots illustrate the steps to import subscribers into phpList:

- Step 1:** The user is on the 'Import subscribers' page. The sidebar menu on the left has 'Import subscribers' highlighted with a red box and a red arrow labeled '1'. The main content area shows a message: 'The pageroot in your config does not match the current location. Check your config file.' Below this, it says 'Please choose one of the import methods below' and lists three options: 'Copy and paste list of email addresses', 'Import by uploading a file with email addresses', and 'Import by uploading a CSV file with email addresses and additional data'. The third option is highlighted with a red box and a red number '2'.
- Step 2:** The user has selected 'Import by uploading a CSV file with email addresses and additional data'. The page shows a warning: 'Warning: the file needs to be plain text. Do not upload binary files like a Word Document.' Below this, there is a 'File containing emails:' section with a 'Browse...' button and the filename 'abc.svg' highlighted with a red box and a red number '3'. The page also lists server limits: 'Maximum size of a total data sent to server: 8M', 'Maximum size of each individual file: 2M', and 'phpList will not process files larger than 5MB'. There are several checkboxes for 'Field Delimiter' (default is TAB), 'Test output', 'Show Warnings', 'Omit Invalid', 'Assign Invalid' (with a dropdown set to 'Invalid email [number]'), 'Overwrite Existing', and 'Retain Old Email'.
- Step 3:** The user has clicked the 'Import' button, which is highlighted with a red box and a red number '4'. The page now shows 'Import subscribers from CSV file' and a message: 'The pageroot in your config does not match the current location. Check your config file.' Below this, it says 'Reading emails from file ...ok, 1 lines' and 'Please identify the target of the following unknown columns'. There is a 'Reset Import session' button. The 'Import Attributes' section has a 'select' dropdown menu with 'Email' selected, highlighted with a red box and a red number '5'. At the bottom, there is a 'CONTINUE' button highlighted with a red box and a red number '6'.

Trigger XSS



Desktop (please complete the following information):

- OS: Ubuntu
- Browser: Firefox
- Version: 76.0.1

Songohan22 commented on Jun 7, 2020

Author


Hi @michield @suelaP
Please review it! Thanks



michield commented on Jun 12, 2020

Member

This is resolved with [bf445db](#)

 **michield** closed this as completed on Jun 12, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

