

New issue Jump to bottom

## Cross Site Script Vulnerability on "Subscribers Lists" feature in phplist version 3.5.3 #666

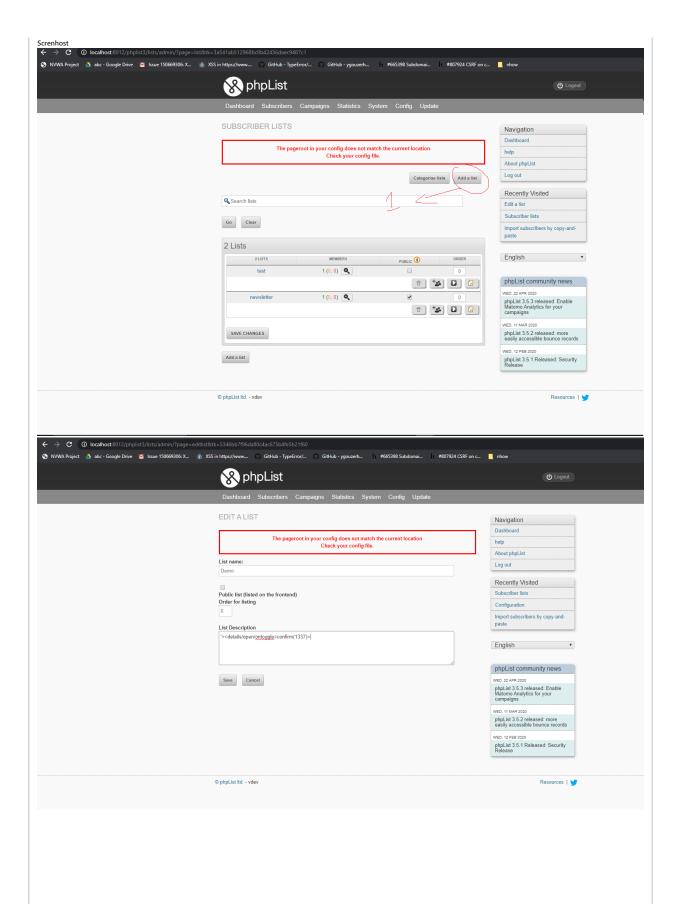
⊙ Closed r0ck3t1973 opened this issue on May 25, 2020 · 4 comments

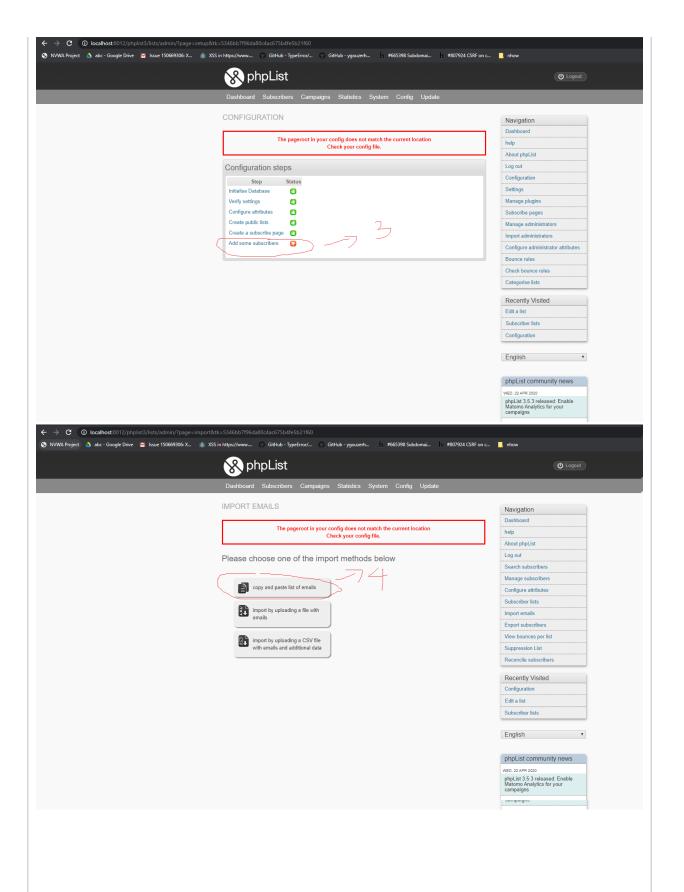
r0ck3t1973 commented on May 25, 2020 • edited ▼ Describe the bug An authenticated malicious user can take advantage of a Stored XSS vulnerability in the "Subscribers Lists" feature. To Reproduce

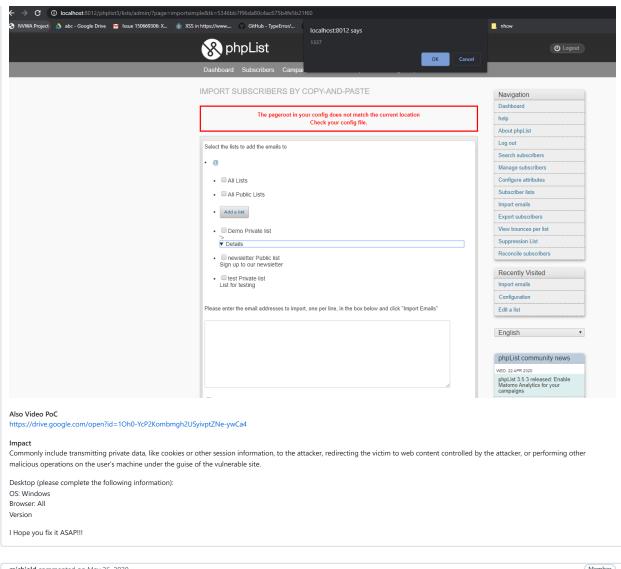
- 1. Login into the panel phplist
- 2. Go to 'phplist3/lists/admin/?page=list&tk=5346bb7f96da80c4ac675b4fe5b21f60'
- 3. Click 'Subscribers Lists' -> 'Add a lists'
- 4. Insert Payload XSS: 'to email address(es)'
- '> < details/open/ontoggle=confirm(1337)>
- 5. Save -> Click 'Config' -> 'Add some subscribers'
- 6. xss alert message

## Expected behavior

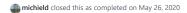
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page











r0ck3t1973 commented on May 26, 2020

Hi @michield , I found a small bug "Subscribers Lists"!

