New issue

Jump to bottom

Reflected XSS vulnerability in wcms/wcms/wex/cssjs.php #9

Open nenf opened this issue on Jul 20, 2020 · 0 comments

nenf commented on Jul 20, 2020

Hi, dev team!

There is Reflected XSS vulnerability in `wcms/wcms/wex/cssjs.php` file.

The vulnerable code is:

64: `type='<?php echo $_GET['type'];?>'>`

Example POC: Just send any js code in `type` parameter like: `type=<script>alert()</script>`

Reflected cross-site scripting (or XSS) arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way. If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user.

To prevent xss use next manual: https://portswigger.net/web-security/cross-site-scripting/preventing.

Please let me know about any fixes, I would like to register CVE number.

nenf changed the title ~~Reflected XSS vulnerability~~ **Reflected XSS vulnerability in wcms/wcms/wex/cssjs.php** on Jul 20, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant