**Directory Listing Vulnerability** was found in the `/lms/admin/assets/`directory of the `Kashipara E-Learning Management System project v1.0`. This vulnerability allows remote attackers to access sensitive files and directories via the URL: `localhost/lms/admin/assets/`.

- **Official Website URL**

  [https://www.kashipara.com/project/php/13138/e-learning-management-system-php-project-source-code](https://www.kashipara.com/project/php/13138/e-learning-management-system-php-project-source-code)

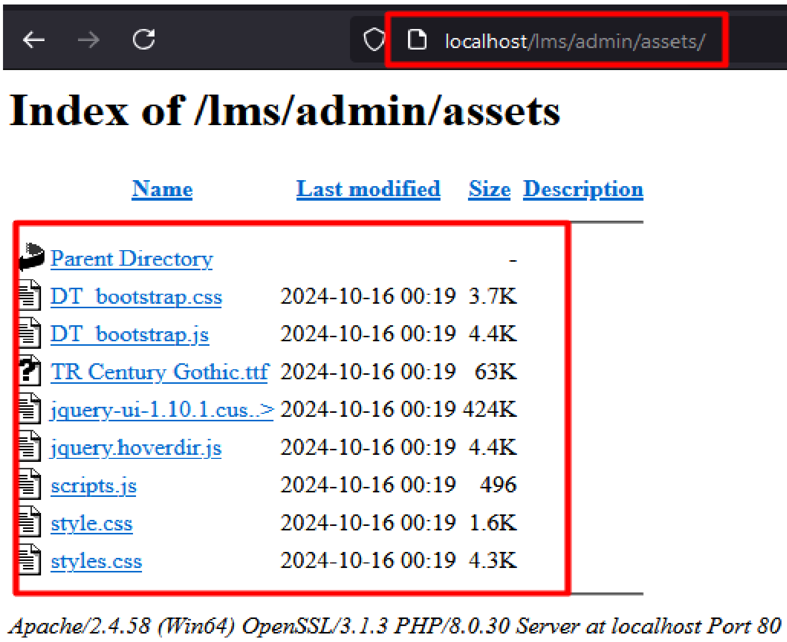
- **Affected Product Name**

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

| | |
|---|---|
| **Affected Vendor** | kashipara |
| **Affected Code File** | /lms/admin/assets/ |
| **Method** | GET |
| **Version** | V1.0 |

## Steps to Reproduce:

**Step 1**: Access [http://localhost/lms/admin/assets/](http://localhost/lms/admin/assets/) and observe the directory listing, which reveals sensitive files and directories.



localhost/lms/admin/assets/

# Index of /lms/admin/assets

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| DT_bootstrap.css | 2024-10-16 00:19 | 3.7K | |
| DT_bootstrap.js | 2024-10-16 00:19 | 4.4K | |
| TR Century Gothic.ttf | 2024-10-16 00:19 | 63K | |
| jquery-ui-1.10.1.cus..> | 2024-10-16 00:19 | 424K | |
| jquery.hoverdir.js | 2024-10-16 00:19 | 4.4K | |
| scripts.js | 2024-10-16 00:19 | 496 | |
| style.css | 2024-10-16 00:19 | 1.6K | |
| styles.css | 2024-10-16 00:19 | 4.3K | |

*Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at localhost Port 80*

## Mitigation/recommendations

- [https://portswigger.net/kb/issues/00600100_directory-listing](https://portswigger.net/kb/issues/00600100_directory-listing)
- [https://cwe.mitre.org/data/definitions/548.html](https://cwe.mitre.org/data/definitions/548.html)