Broken Access Control vulnerability was found in "/smsa/add_subject.php" & "/smsa/add_subject_submit.php" in Kashipara Responsive School Management System v3.2.0 allows remote unauthenticated attackers to add a new subject entry via the direct URL access.

Affected Vendor: KASHIPARA (https://www.kashipara.com/)

Product Official Website URL: Responsive School Management System (https://www.kashipara.com/project/php/12362/responsive-school-management-system-php-project-source-code)

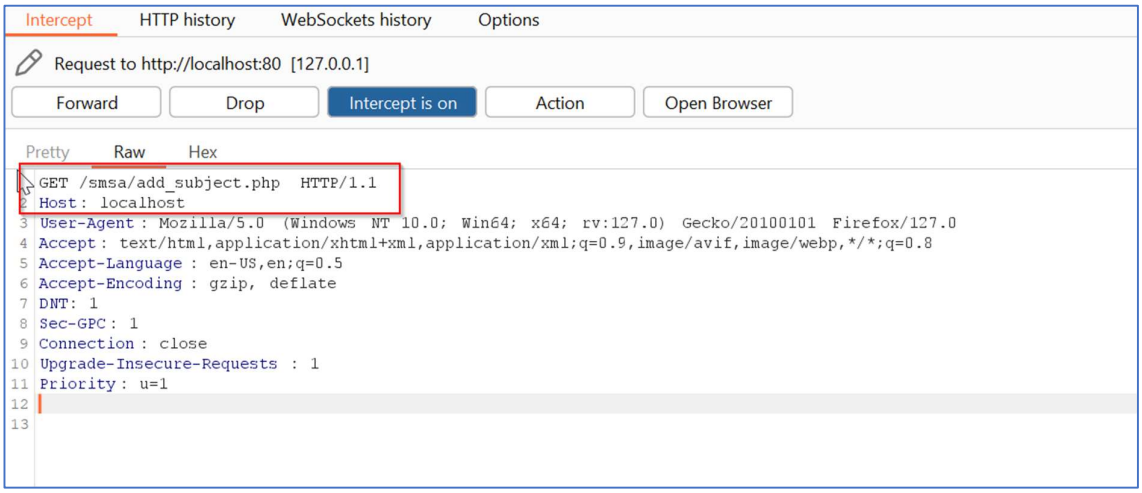
Version: 3.2.0

Affected Components:

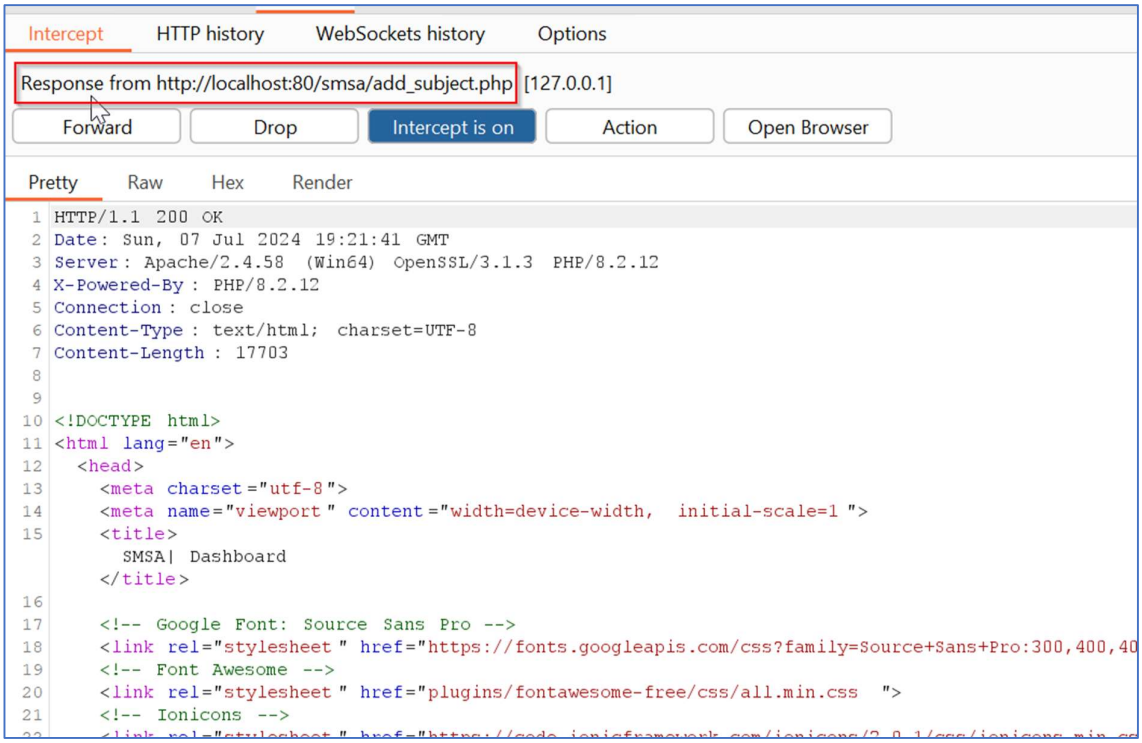
- **Affected Code Files:** "/smsa/add_subject.php" & "/smsa/add_subject_submit.php"

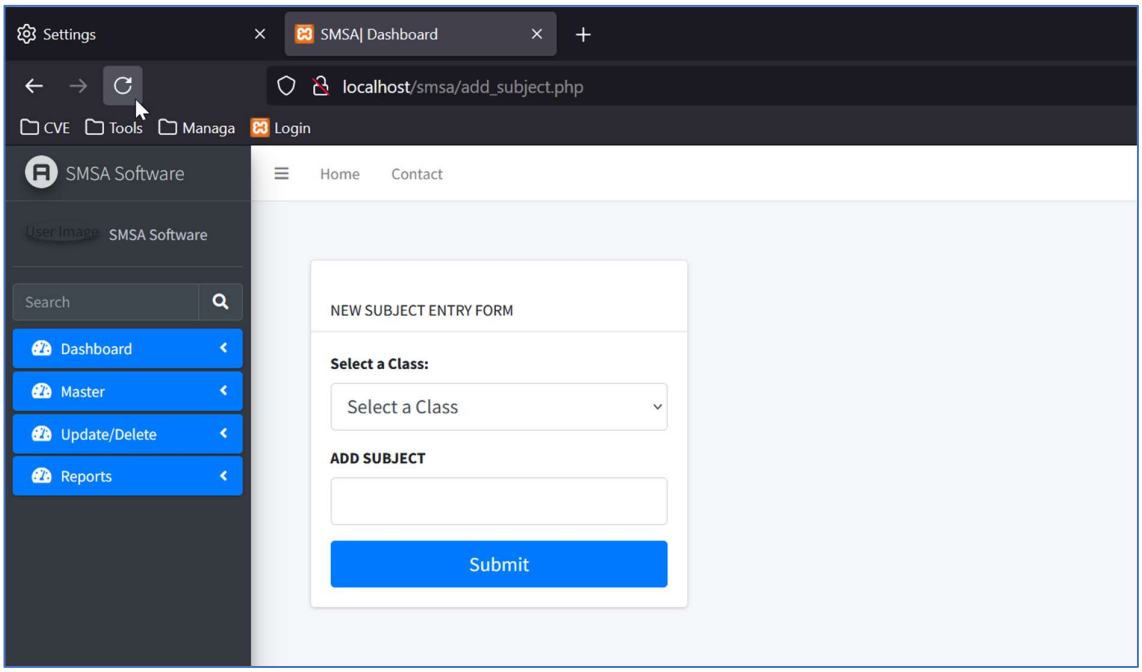
Steps:

1. Access the administrator "Add Subject" menu of the Responsive School Management System v3.2.0 without any need for login credentials. URL: http://localhost/smsa/add_subject.php

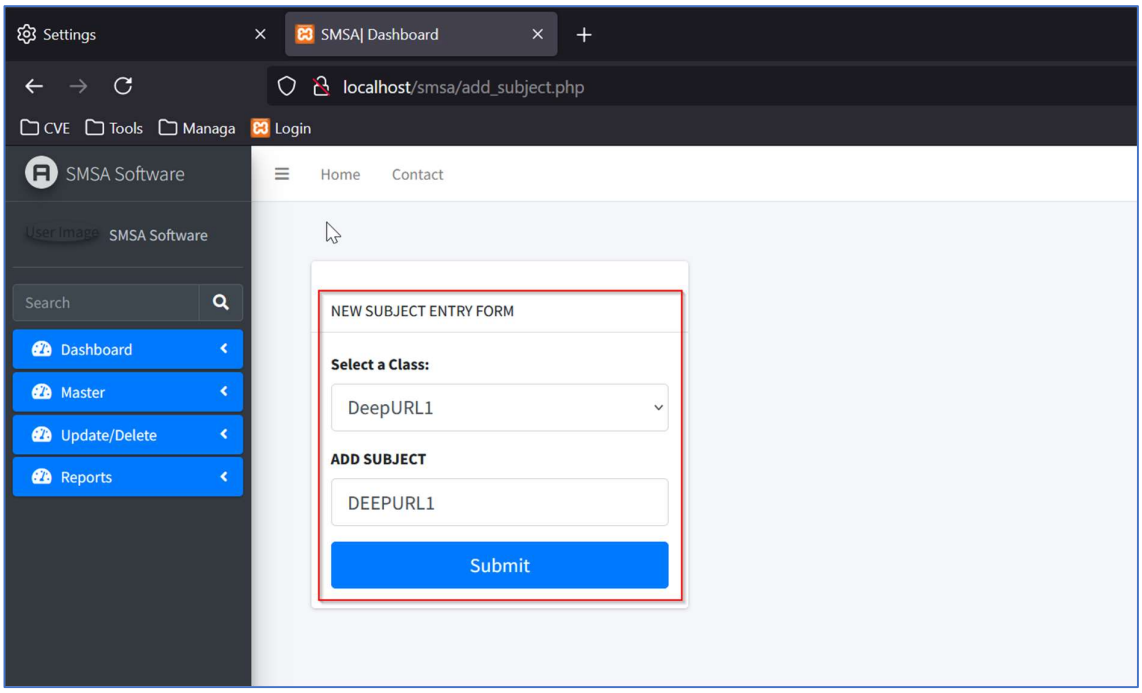


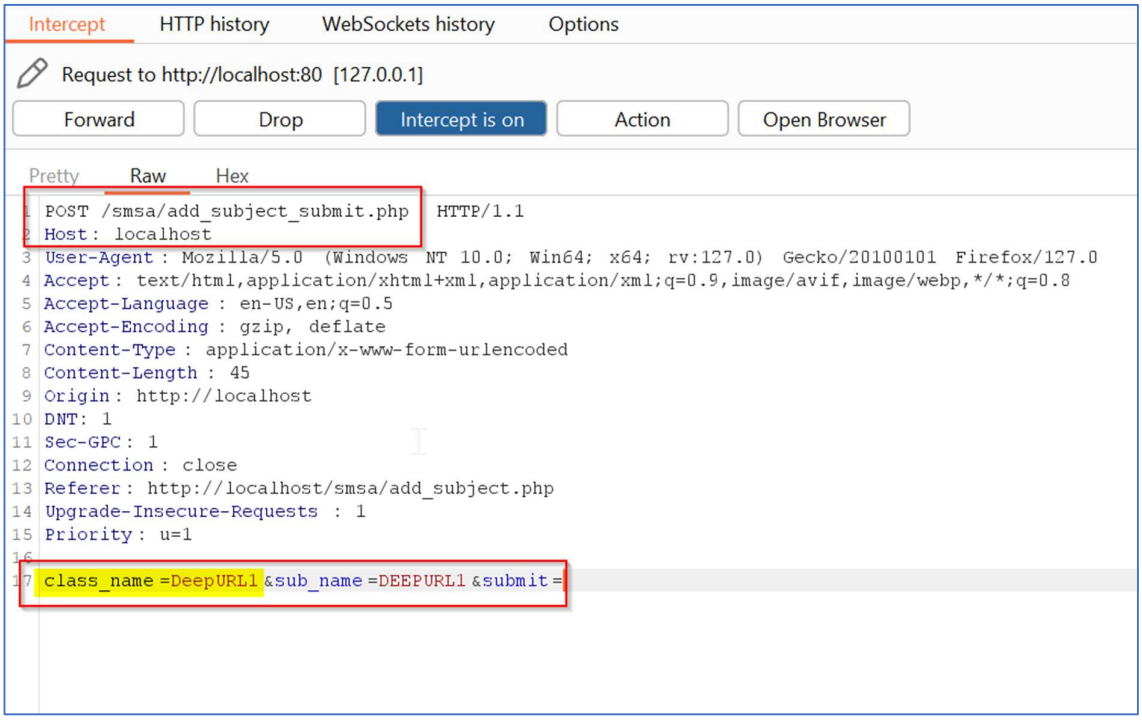
2. It was observed that the administrator “Add Subject” menu is accessible to the unauthenticated user without any need of valid login credentials.



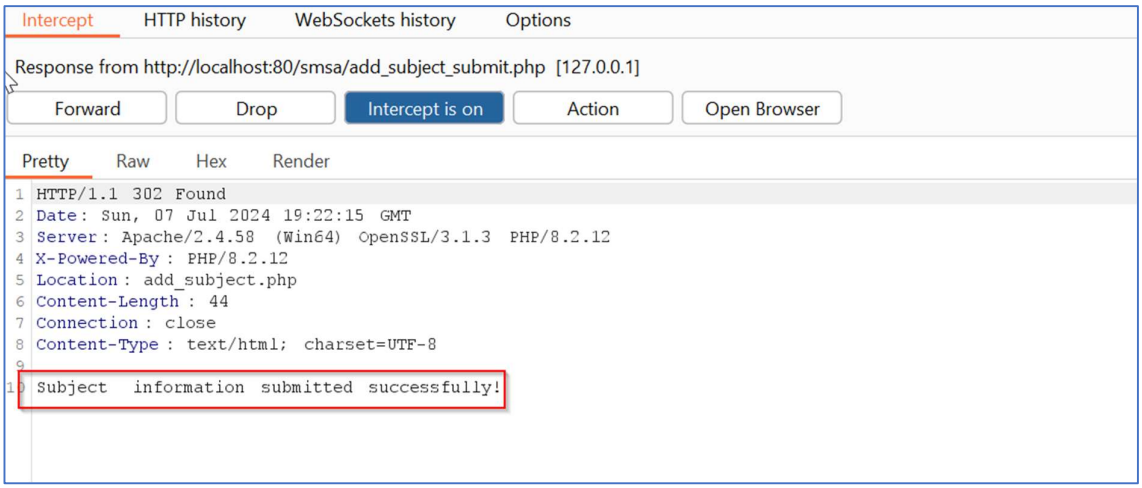


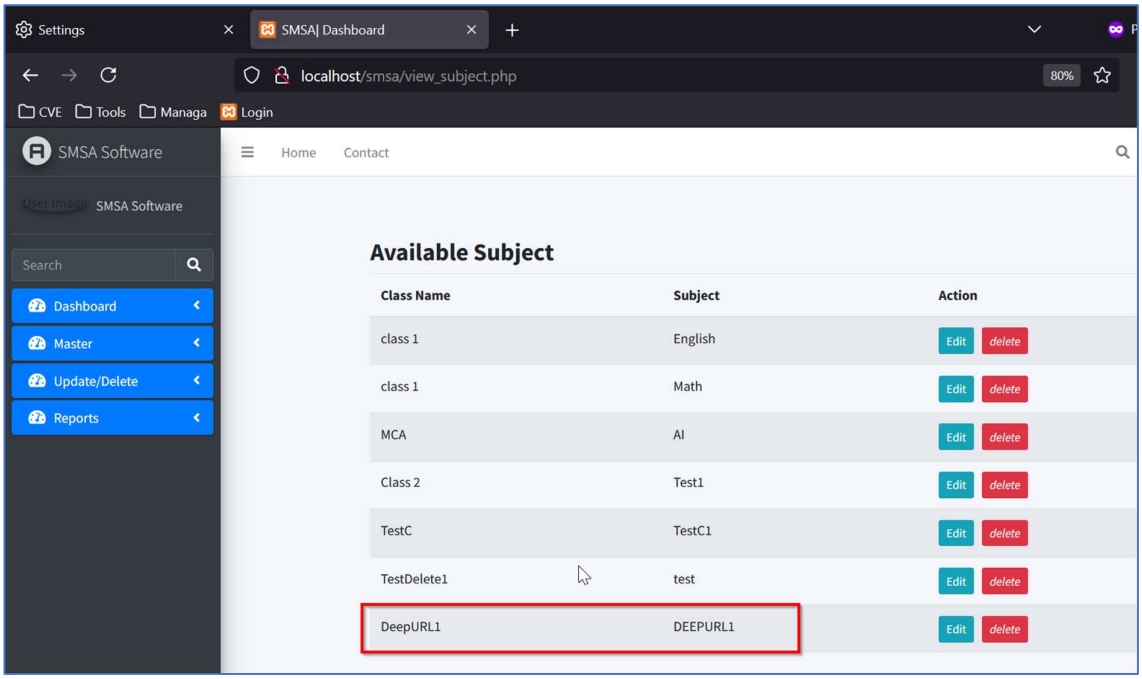
3. Now try to create a new subject "**DeepURL1**" by entering the relevant details in the "New Subject Entry Form" and click "Submit" button.





4. It was observed that the unauthenticated user is able to create a new subject "**DeepURL1**" without any need of valid login credentials.





Solution/Good Reads:

Application should make sure that only the valid authenticated & authorized user is allowed to access the post login data and perform the relevant post login activities. Validate the session cookie and user permissions at server side for each request before responding with the post login data and allowing the post login activities.

https://owasp.org/Top10/A01_2021-Broken_Access_Control/