Broken Access Control vulnerability was found in "/smsa/admin_teacher_register_approval.php" and "/smsa/admin_teacher_register_approval_submit.php" in Kashipara Responsive School Management System v3.2.0 allows remote unauthenticated attackers to view and approve the Teacher registration 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)

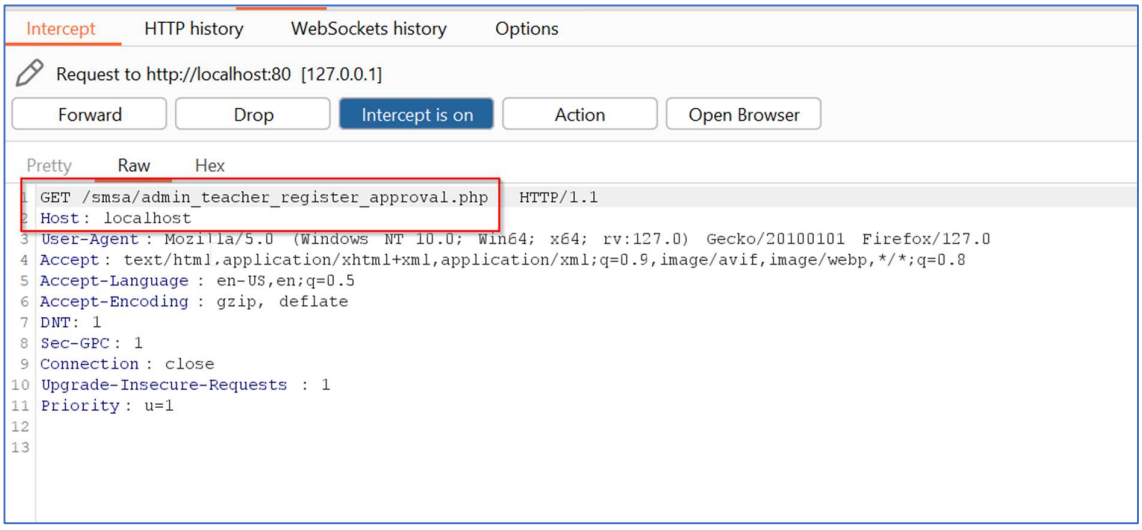
Version: 3.2.0

Affected Components:

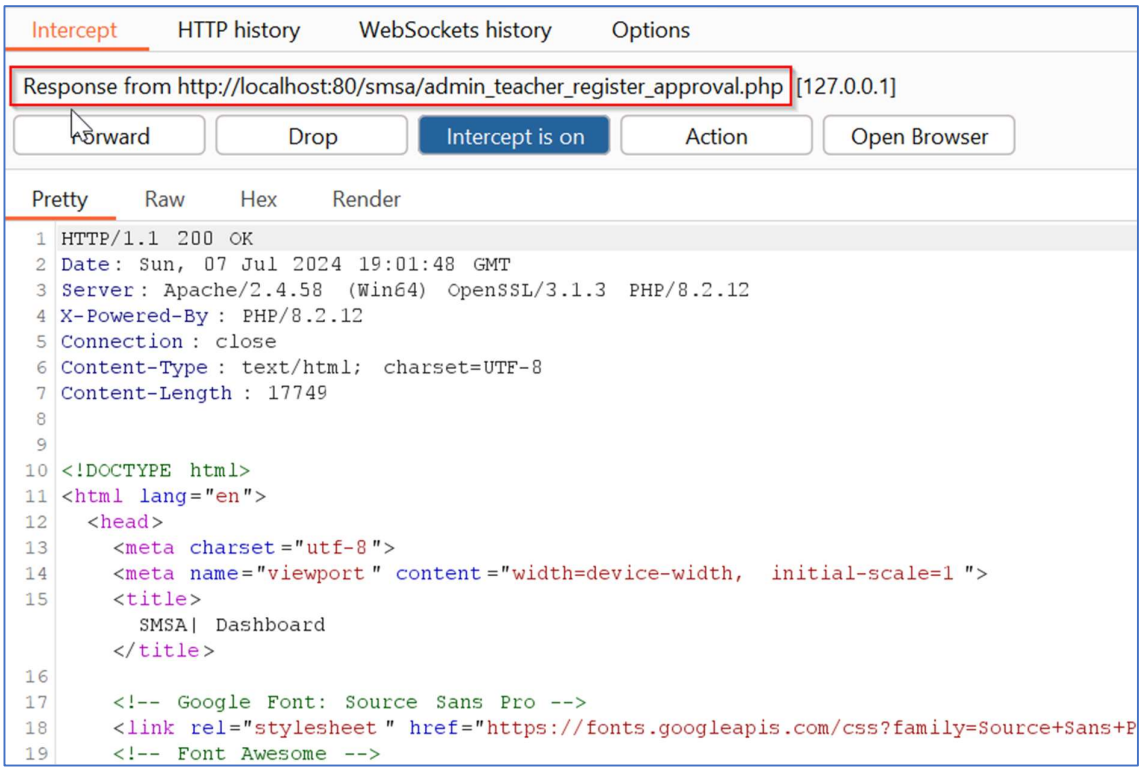
- **Affected Code Files:** "/smsa/admin_teacher_register_approval.php" and "/smsa/admin_teacher_register_approval_submit.php"

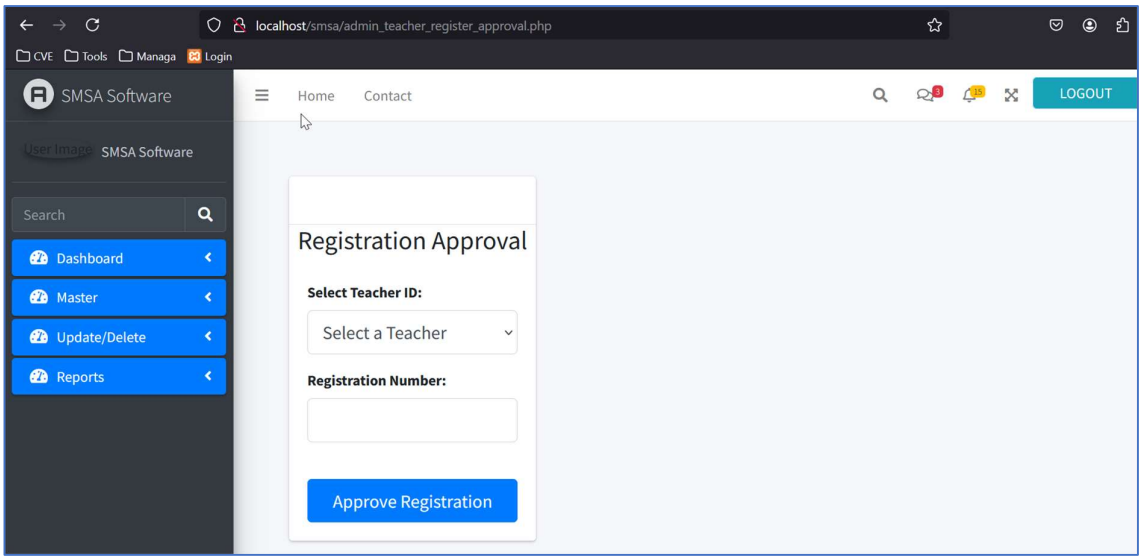
Steps:

1. Access the "Teacher Registration Approval" URL of the Responsive School Management System v3.2.0 without any need for login credentials. URL: http://localhost/smsa/admin_teacher_register_approval.php.

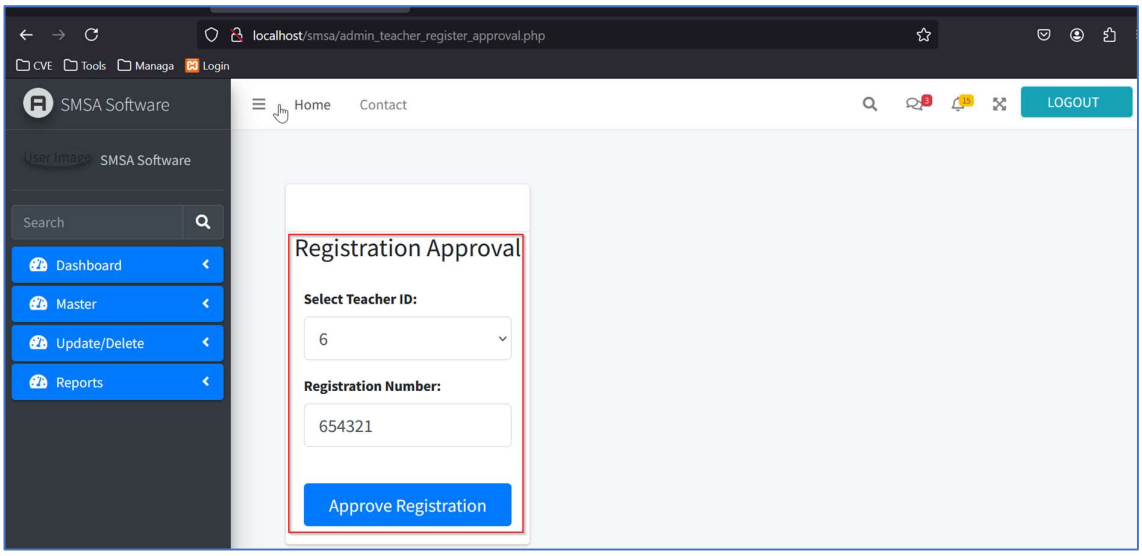


2. It was observed that the “Teacher Registration Approval” data is displayed to the unauthenticated user without any need of valid login credentials.

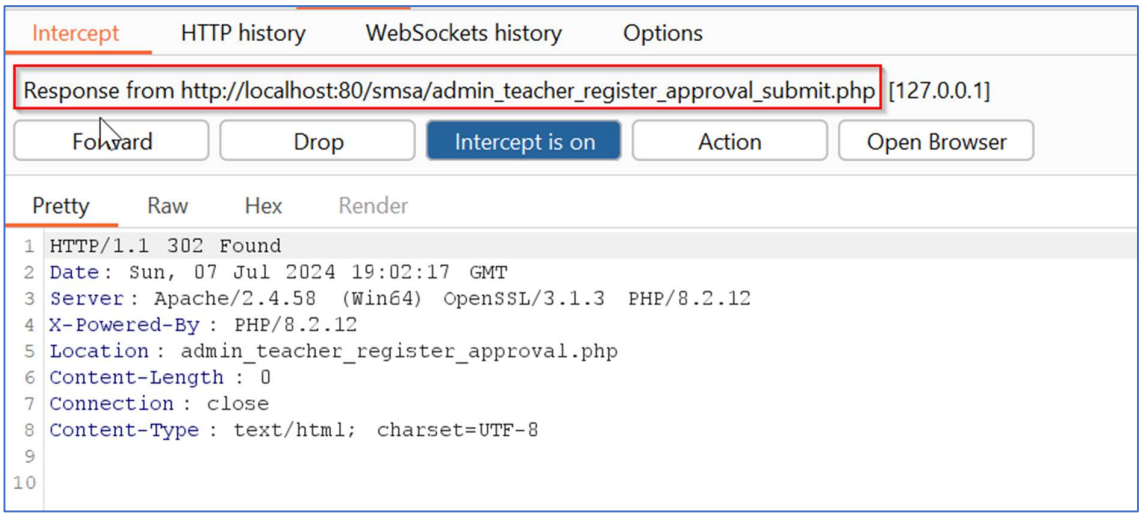


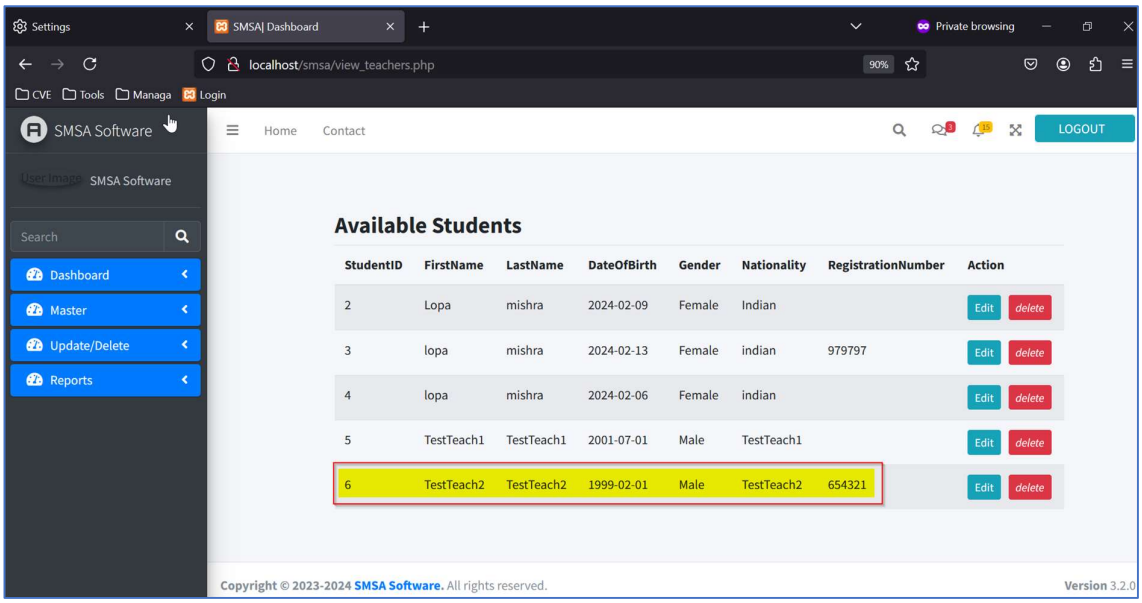


3. Now select any “Teacher ID” from the dropdown and enter the “Registration Number”. Click “Approve Registration” button. We selected “**Teacher ID = 6”**.



4. It was observed that the unauthenticated user is able to perform the “Teacher Registration Approval” process for the “**Teacher ID = 6”** 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/