

Broken Access Control vulnerability was found in “/smsa/view_subject.php” in Kashipara Responsive School Management System v3.2.0 allows remote unauthenticated attackers to view SUBJECT details 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>)

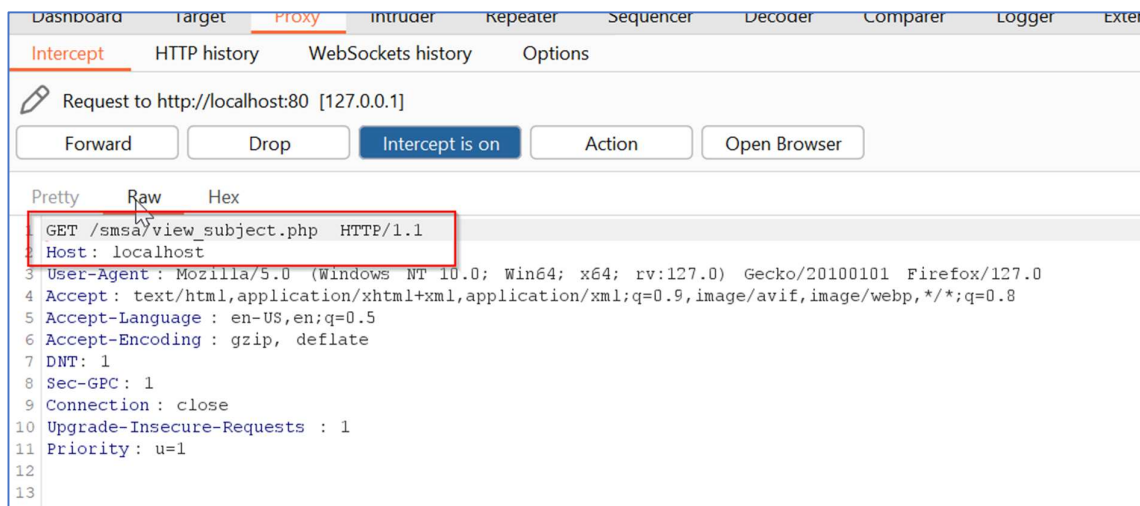
Version: 3.2.0

Affected Components:

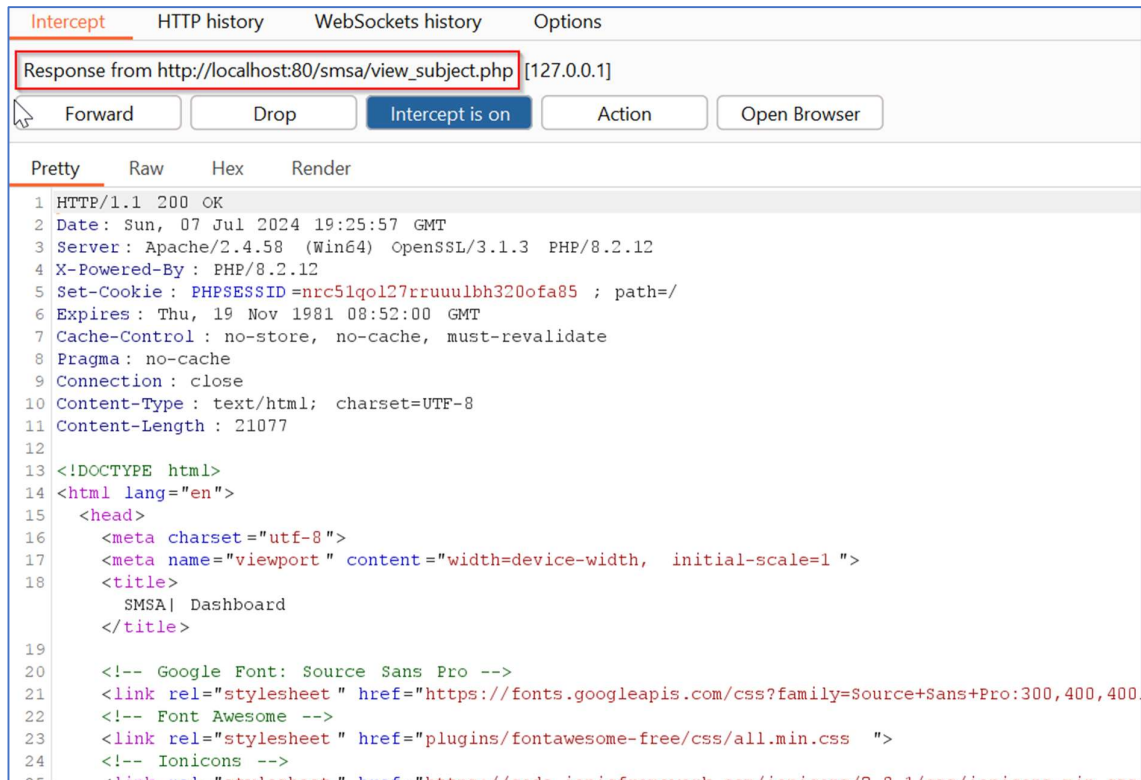
- **Affected Code Files:** “/smsa/view_subject.php”

Steps:

1. Access the administrator “View/update Subjects” menu of the Responsive School Management System v3.2.0 without any need for login credentials. URL: http://localhost/smsa/view_subject.php



2. It was observed that the administrator “View/update Subjects” menu is accessible to the unauthenticated user without any need of valid login credentials.



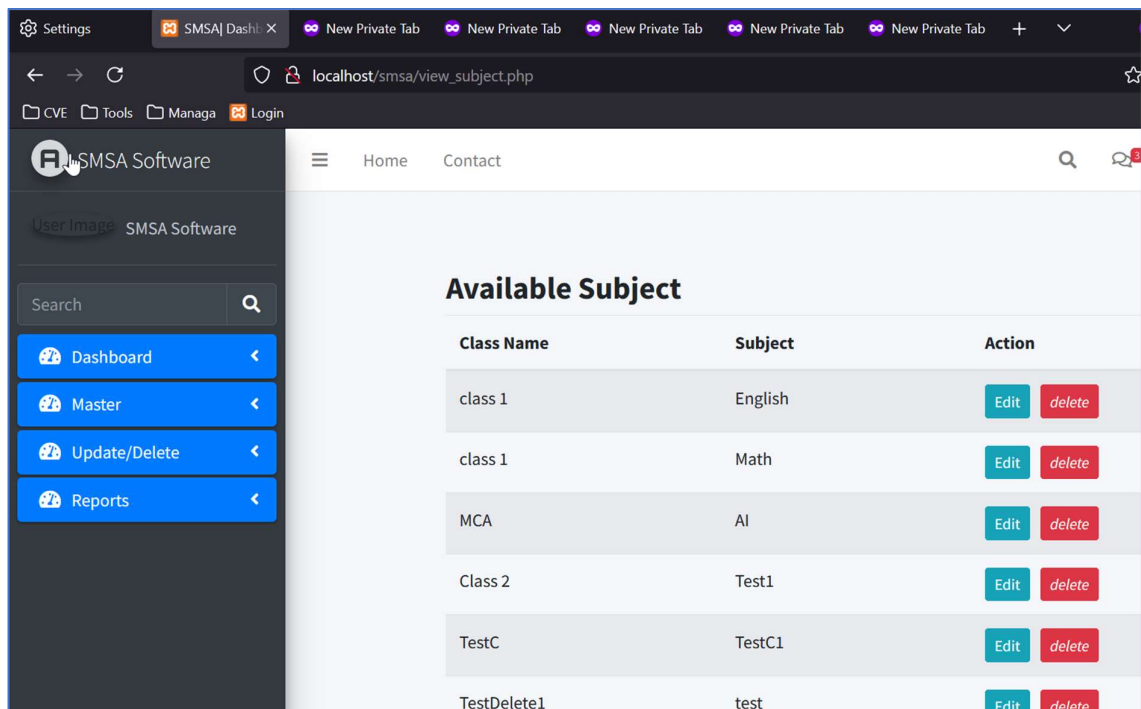
Intercept HTTP history WebSockets history Options

Response from http://localhost:80/smsa/view_subject.php [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sun, 07 Jul 2024 19:25:57 GMT
3 Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
4 X-Powered-By: PHP/8.2.12
5 Set-Cookie: PHPSESSID=nrc51qol27rruuulbh320ofa85 ; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 21077
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="utf-8">
17     <meta name="viewport" content="width=device-width, initial-scale=1">
18     <title>
19       SMSA| Dashboard
20     </title>
21
22     <!-- Google Font: Source Sans Pro -->
23     <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400,300">
24     <!-- Font Awesome -->
25     <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
26     <!-- Ionicons -->
27     <link rel="stylesheet" href="https://unpkg.com/ionicons@7.1.0/dist/ionicons.min.css">
```



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/