SQL injection vulnerability in "/music/ajax.php?action=login" of the Kashipara Music Management System v1.0 allows remote attackers to execute arbitrary SQL commands and bypass Login via the “email” parameter. This is a critical vulnerability.

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)

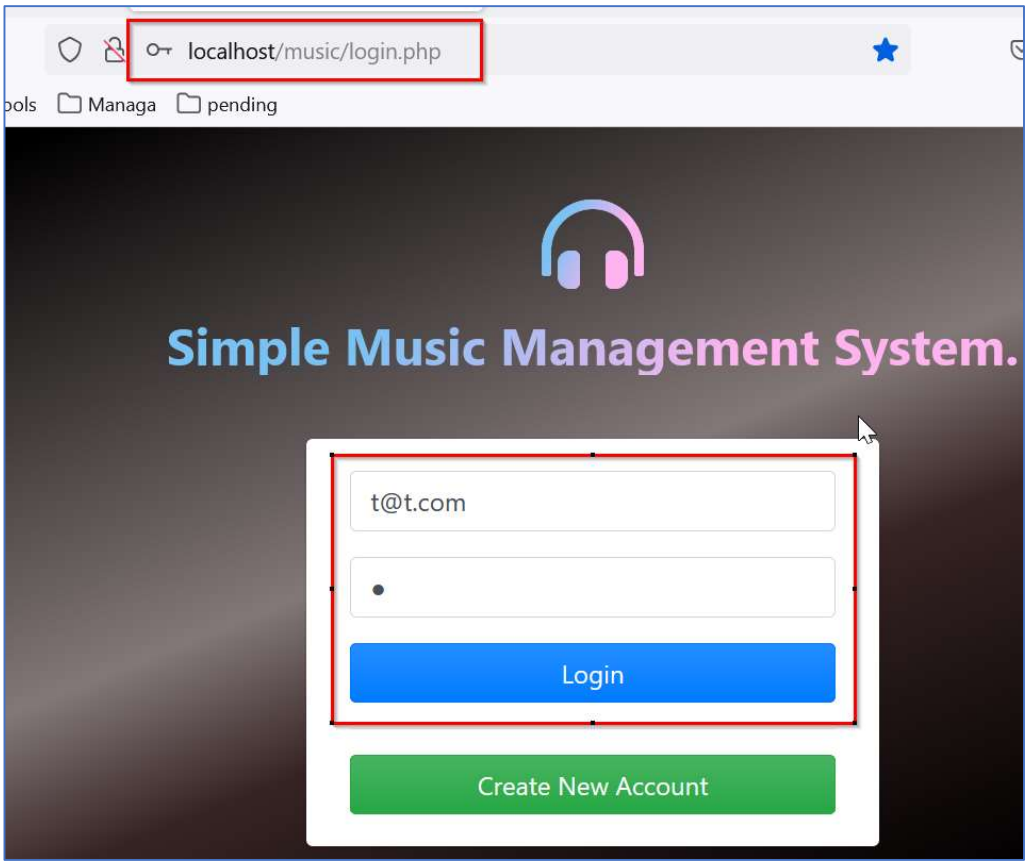
Version: 1.0

Affected Components:

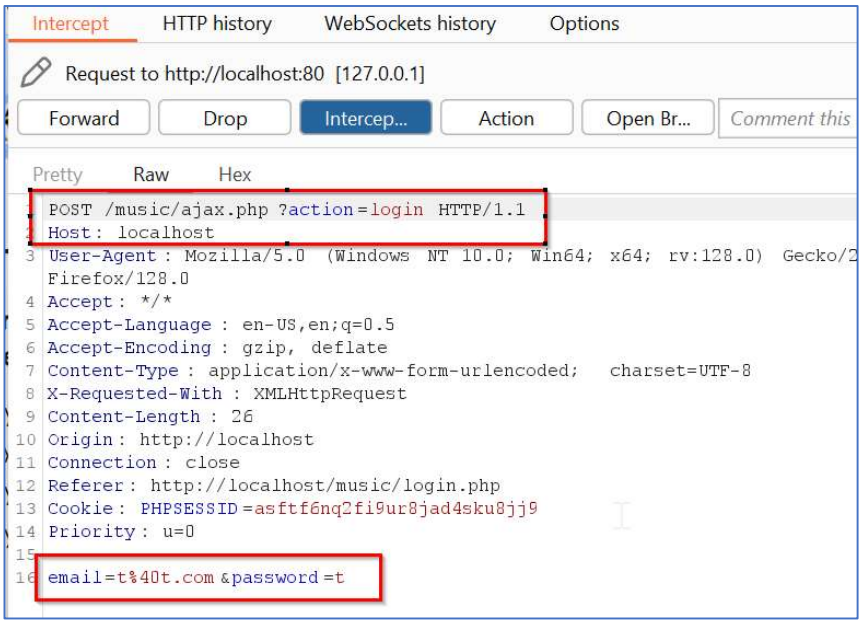
- **Affected Code File:** /music/ajax.php?action=login
- **Affected Parameter:** “email” parameter

Steps:

1. Access the login page of Music Management System v1.0 (URL: http://localhost/music/login.php)
2. Enter any random value in Username and the Password textbox. Click “Login” button.

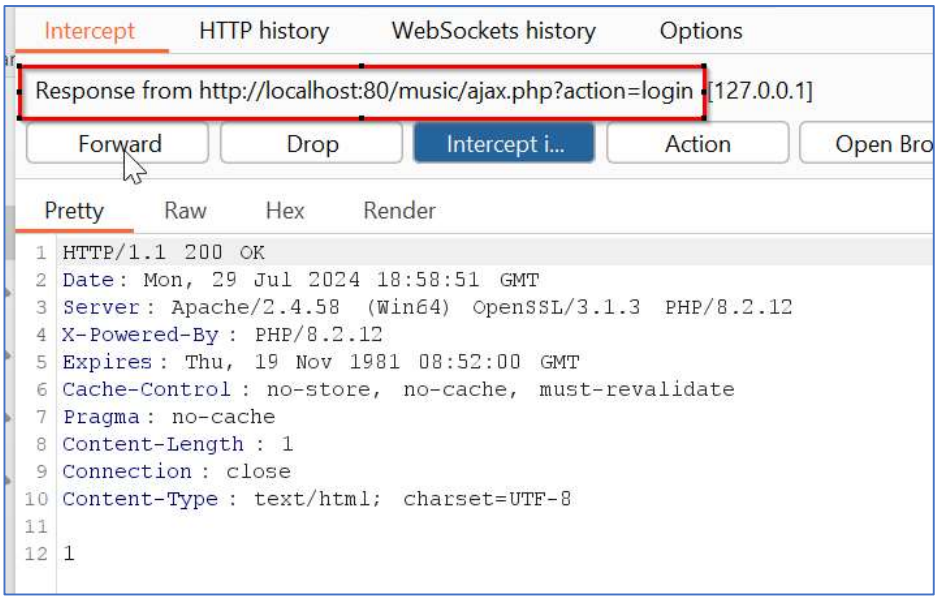


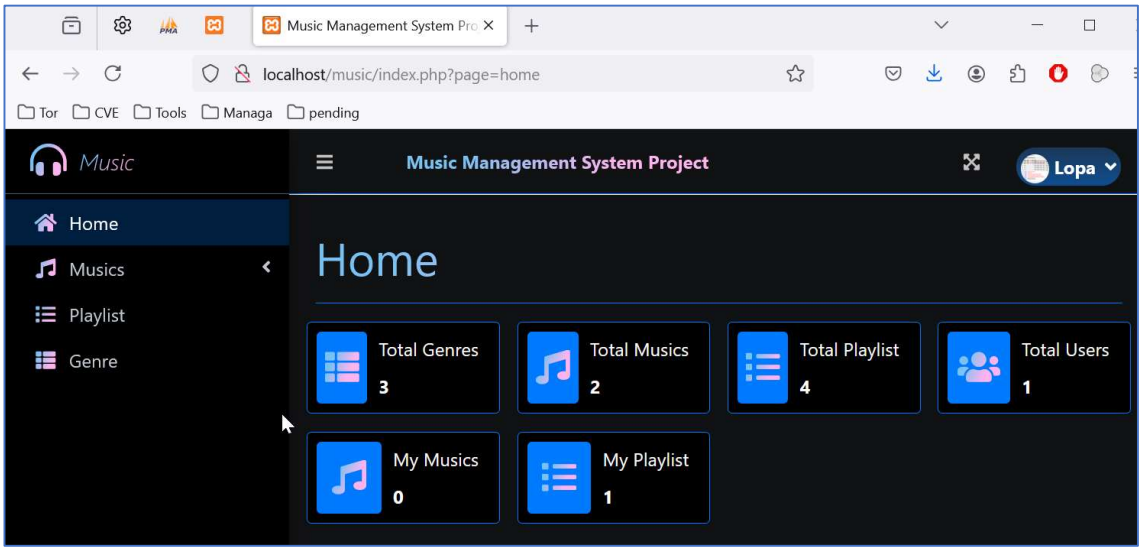
3. Capture the HTTP request going towards server in Burp Suite.



4. In this HTTP POST request parameter “email”, add the SQL command: ***t’+OR+’1’=’1’#***

5. This will bypass the LOGIN validation and allow us to login into the application.





Solution/Good Reads:

User parameterized SQL queries instead of the dynamic SQL queries.

- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html