# Reflected Cross Site Scripting (XSS) vulnerability was found in " /smsa/student_login.php" in the Kashipara Responsive School Management System v3.2.0 allows remote attackers to execute arbitrary code via "error" URL parameter.

**Affected Vendor:** Kashipara (https://www.kashipara.com/)

**Product Official Website URL**: Responsive School Management System (https://www.kashipara.com/project/php/12362/responsive-school-management-system-php-project-source-code)

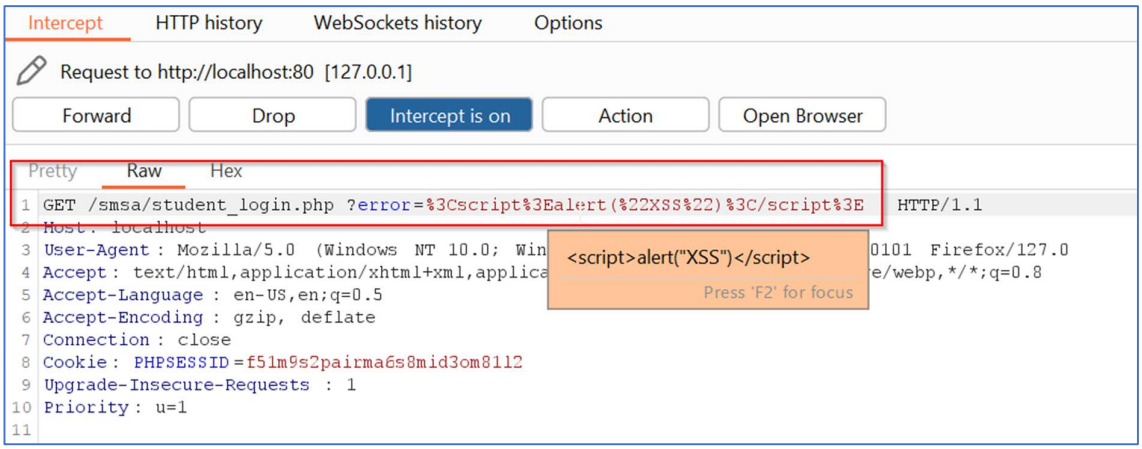
**Version:** 3.2.0

**Affected Components:**

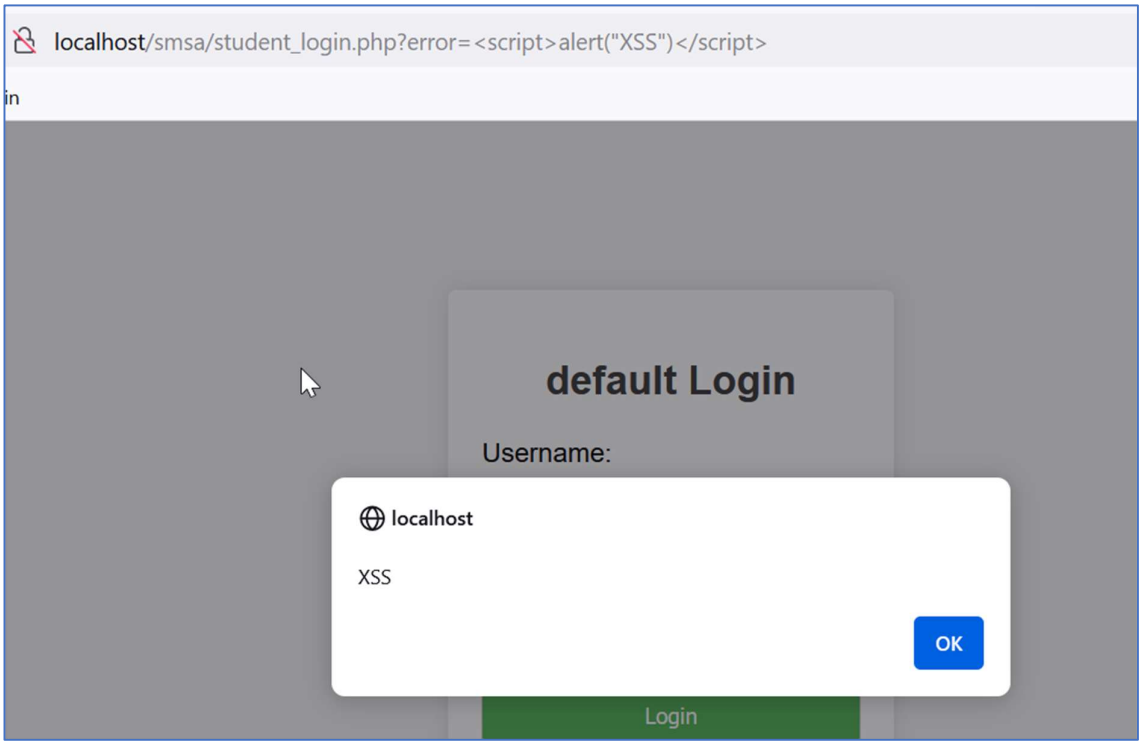
- Affected File: /smsa/student_login.php
- Affected Parameter: "error" URL parameter

**Steps:**

1. Access the URL: http://localhost/smsa/student_login.php?error=<script>alert("XSS")</script> in the browser. Note that we have inserted XSS script in "error" parameter.



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

**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