Stored Cross Site Scripting (XSS) vulnerability was found in "/admin/view-enquiry.php" in PHPGurukul Old Age Home Management System v1.0 allows remote attackers to execute arbitrary code via Contact Us page "message" POST parameter.

Affected Project: PHPGurukul Old Age Home Management System v1.0

Official Website: https://phpgurukul.com/old-age-home-management-system-using-php-and-mysql/

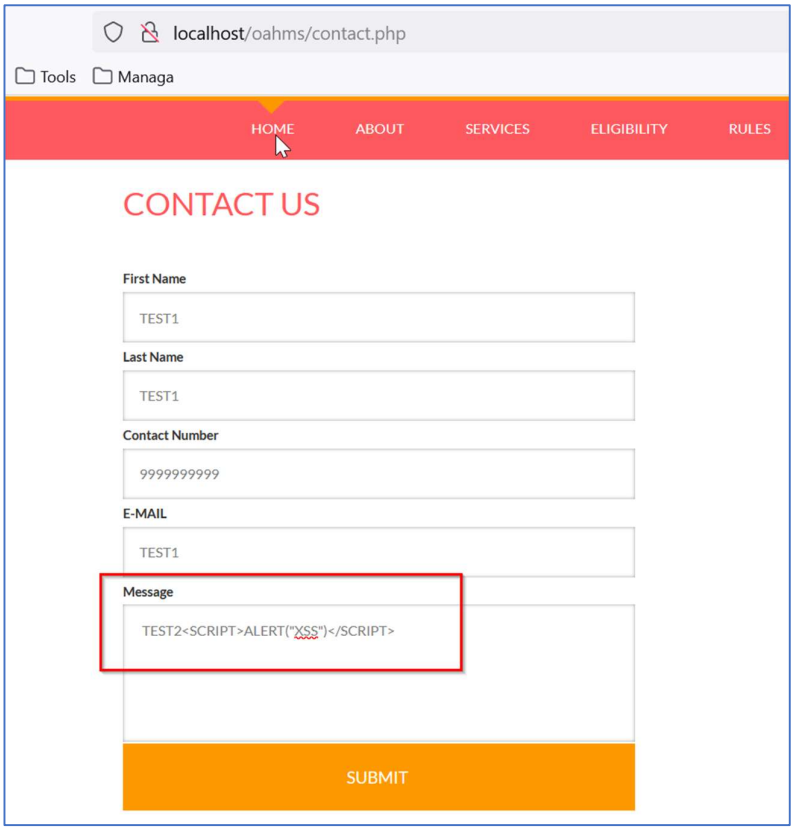
Version: 1.0

Affected Components:

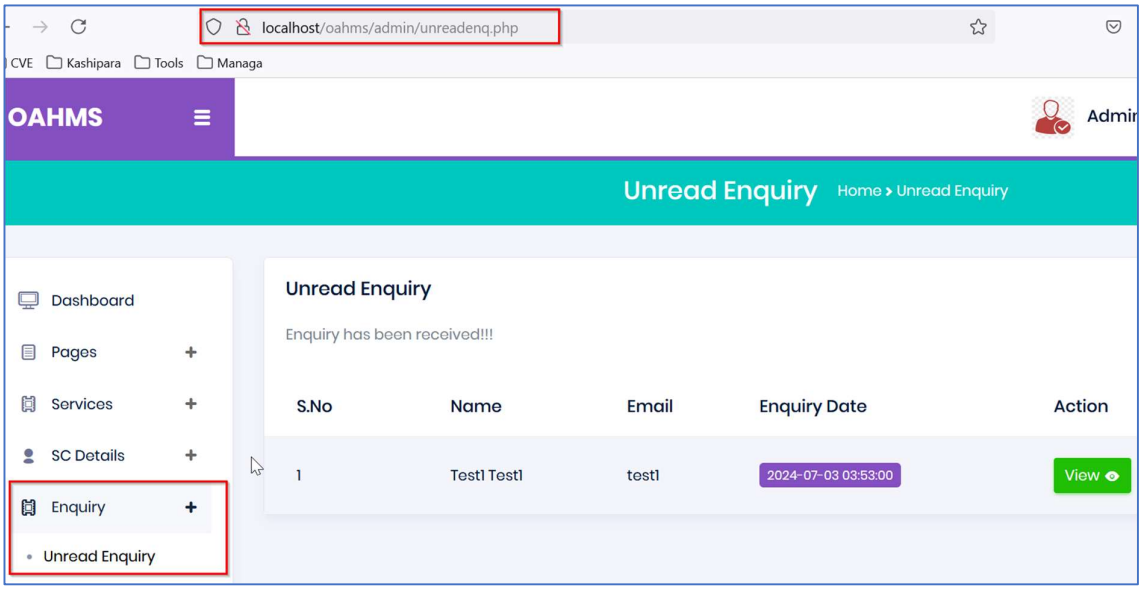
- **Affected Code File:** /admin/view-enquiry.php
- **Affected Parameter:** Contact Us page "message" POST parameter
- **Application URL:** http://localhost/oahms/admin/view-enquiry.php?viewid=5

Steps:

1. Access the “Contact Us” page URL: http://localhost/oahms/contact.php
2. Enter the XSS script ***Test2<script>alert("XSS")</script>*** in “Message” textbox. Enter the relevant sample data in other textboxes and submit the request.

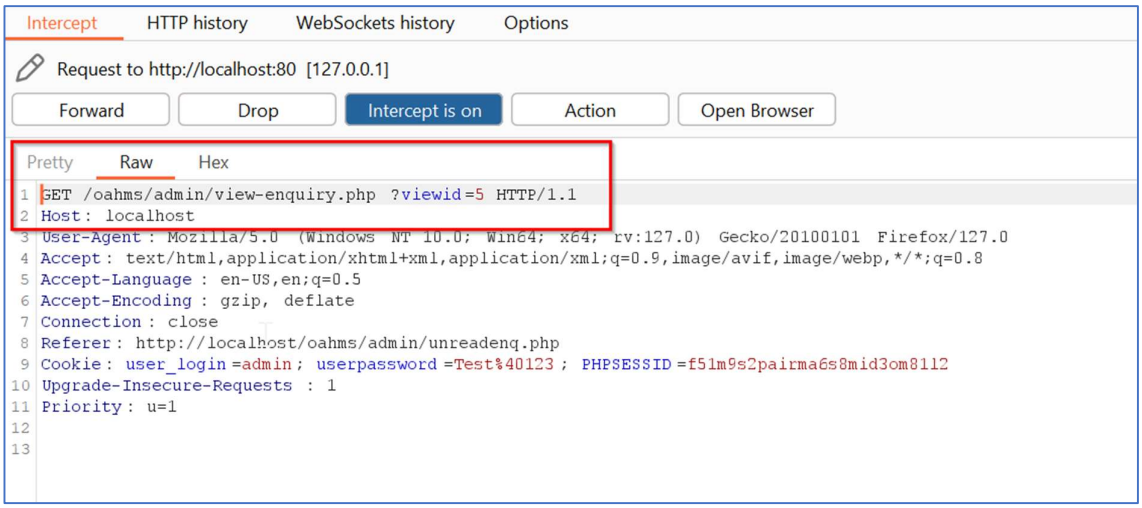


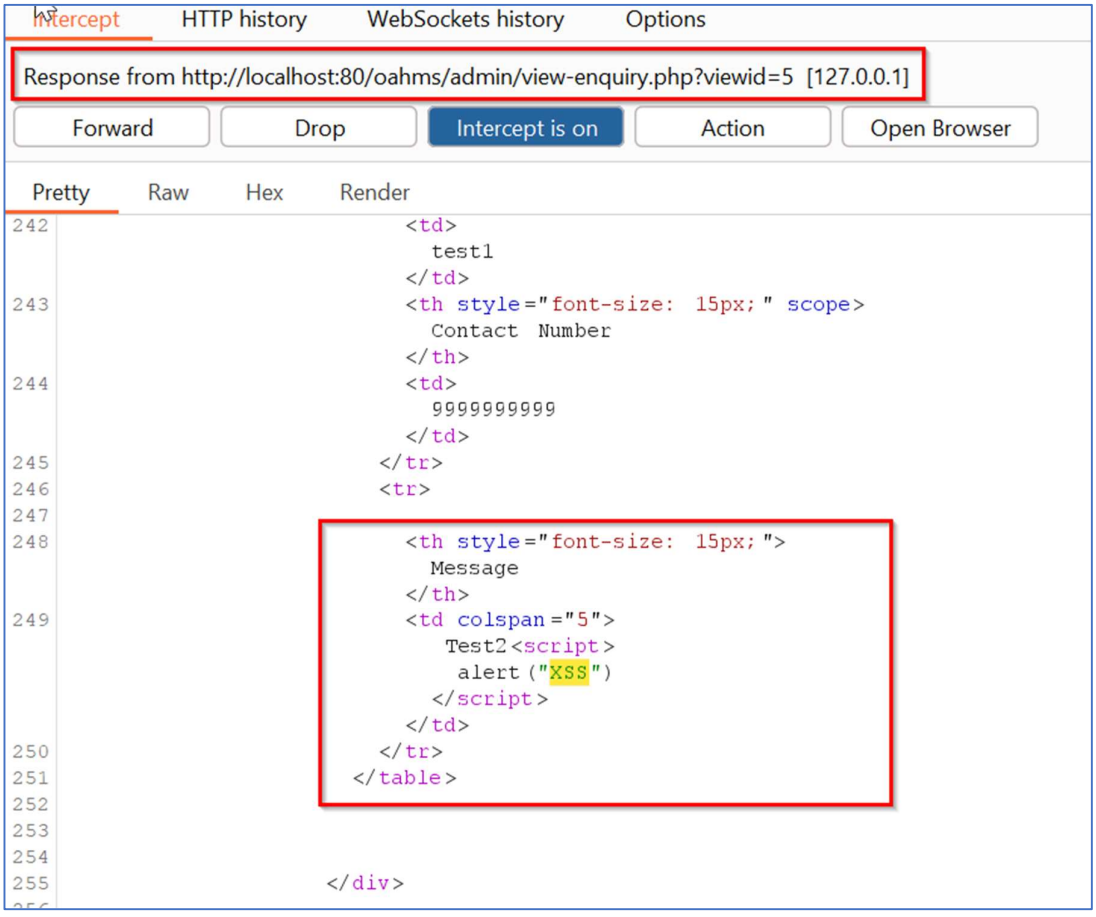
3. This will forward the “Contact Us” request with XSS script to server. The request gets accepted and the XSS script is stored in the application database.
4. Now login into the Admin panel of the Old Age Home Management System v1.0. URL: http://localhost/oahms/admin/
5. Access the menu “Enquiry” -> “Unread Enquiry”. URL: http://localhost/oahms/admin/unreadenq.php

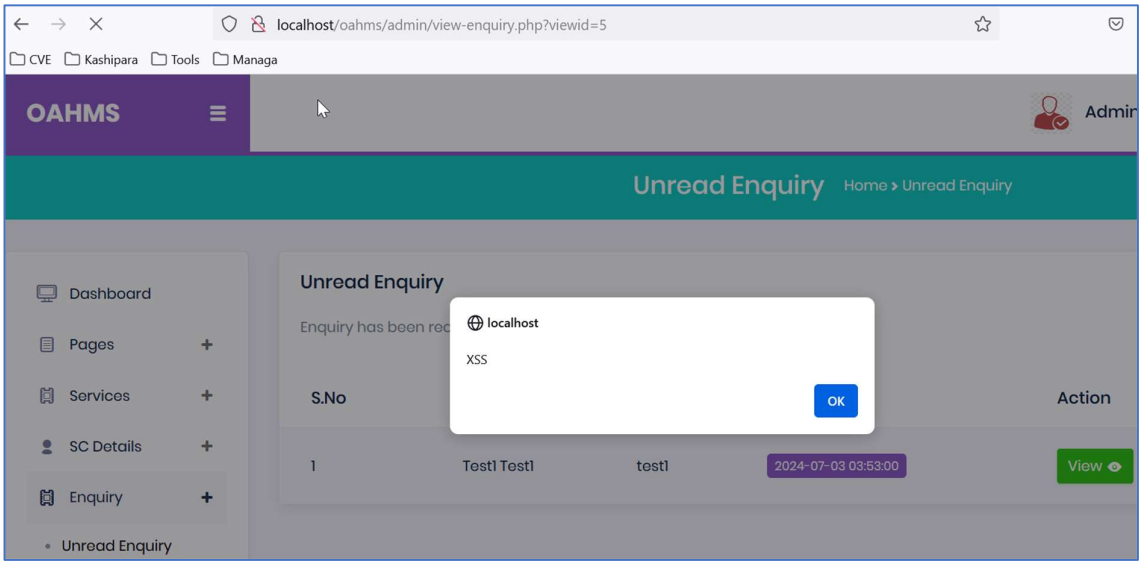


6. Click “View” to view the data.

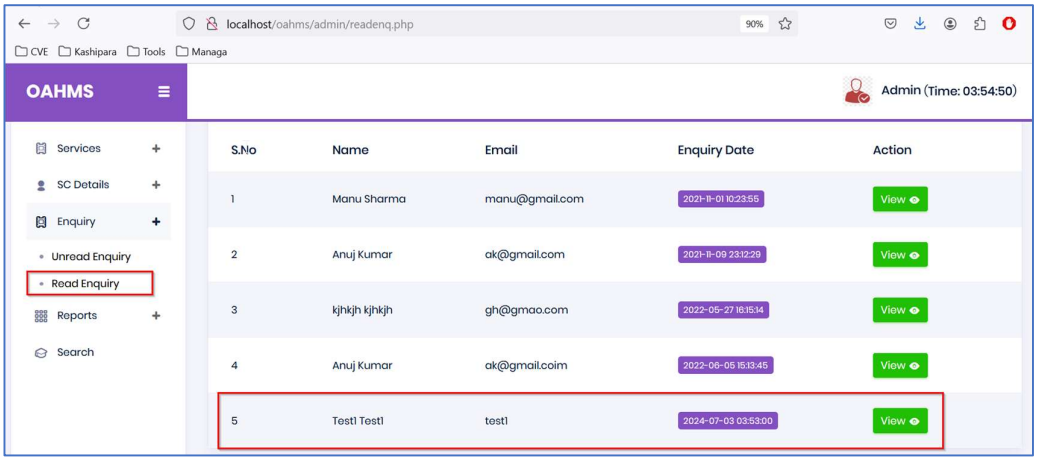
7. The XSS script we submitted in Step 2 is reflected back as it is back to the browser and the XSS script gets executed.

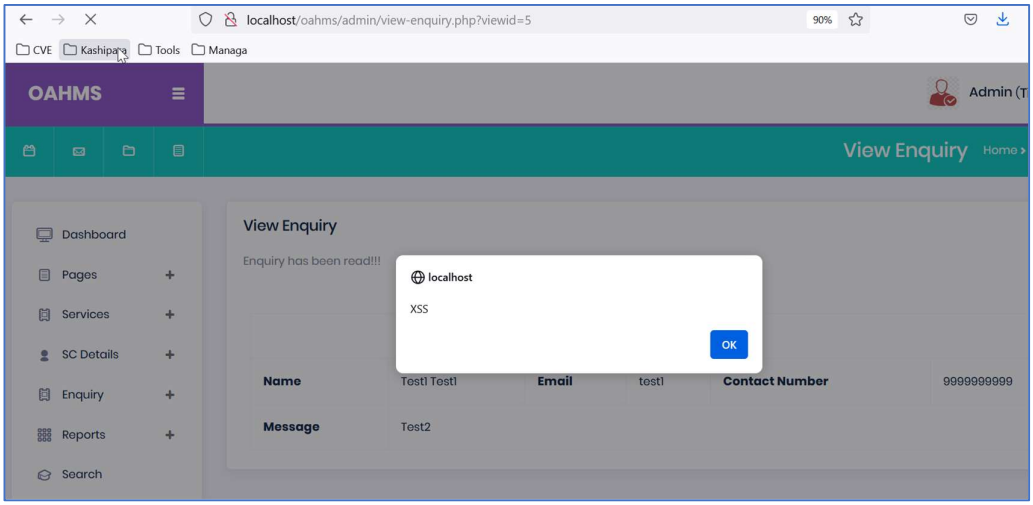






8. Now, every time we access this Enquiry entry (URL: http://localhost/oahms/admin/view-enquiry.php?viewid=5), the XSS script will get executed.





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