Stored Cross Site Scripting (XSS) vulnerability was found in "/admin/afeedback.php" in Kashipara Online Exam System v1.0 allows remote attackers to execute arbitrary code via "rname" and "email" POST parameter fields.

Affected Vendor: KASHIPARA (https://www.kashipara.com/)

Product Official Website URL: Online Exam System v1.0 (https://www.kashipara.com/project/php/3/online-exam-php-project-source-code-download)

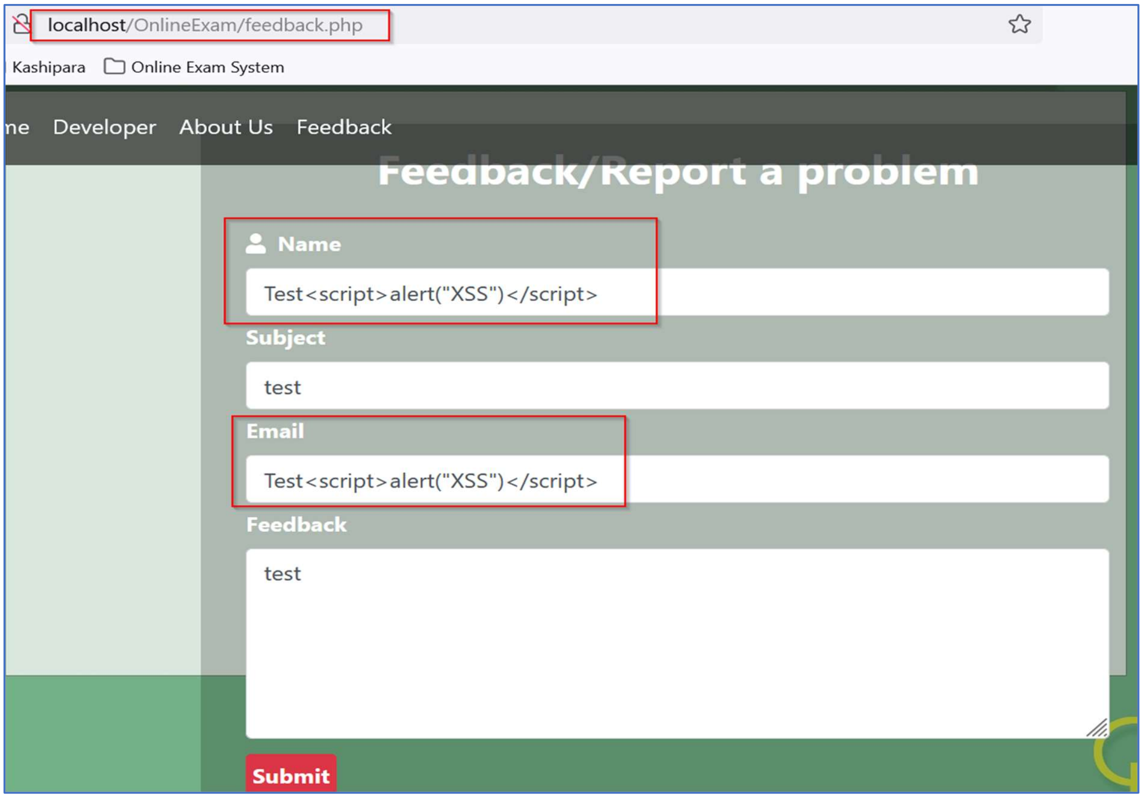
Version: 1.0

Affected Components:

- **Affected Code File:** /feedback.php & /admin/afeedback.php
- **Affected Parameter:** "rname" and "email" POST parameters
- **Application URL:** http://localhost/OnlineExam/admin/afeedback.php

Steps:

1. Access the Feedback page on the Online Exam System v1.0 (URL: http://localhost/OnlineExam/feedback.php)
2. Enter the XSS script in "Name" and "Email" input boxes: ***Test<script>alert("XSS")</script>***



localhost/OnlineExam/feedback.php

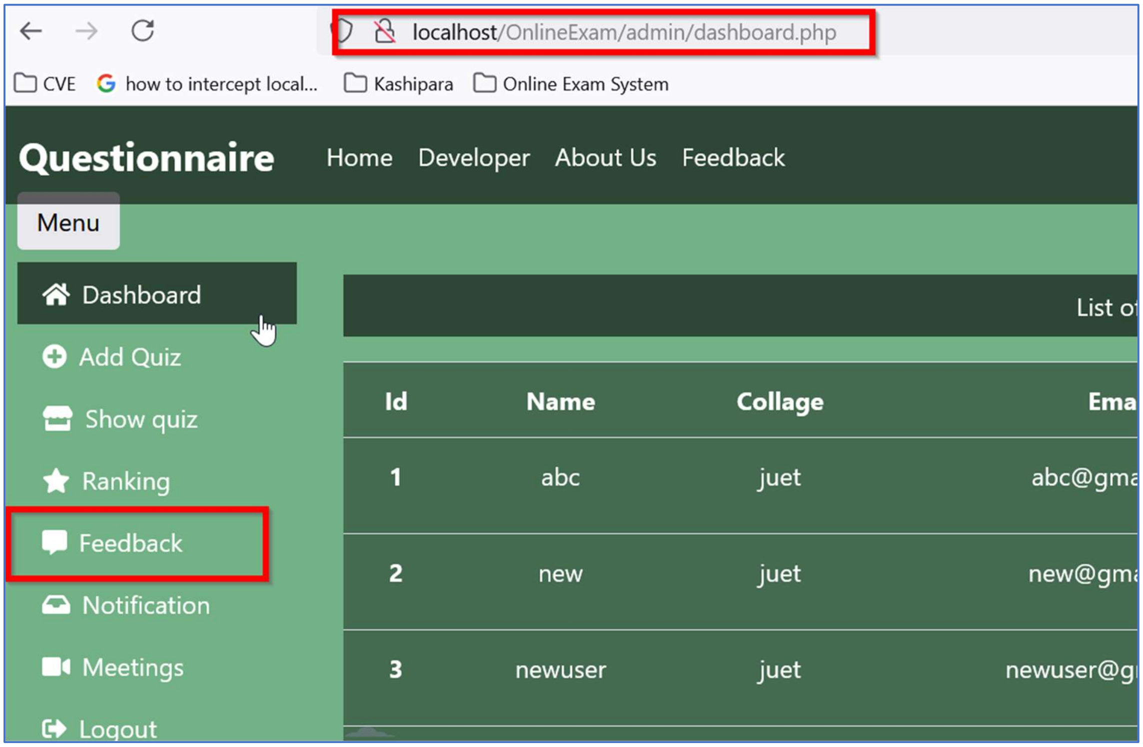
Name: Test<script>alert("XSS")</script>

Subject: test

Email: Test<script>alert("XSS")</script>

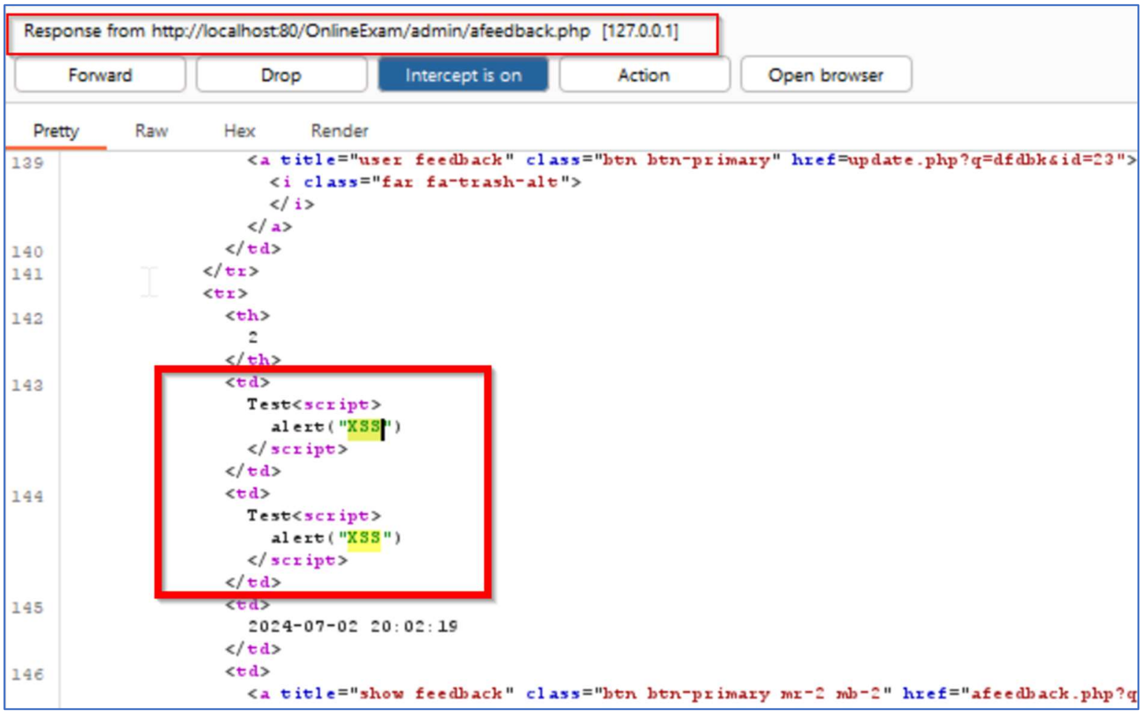
Feedback: test

3. Submit the feedback request by clicking on “Submit” button.
4. The XSS scripts gets stored in the database.
5. Login into the Admin module. URL: http://localhost/OnlineExam/admin/adminlogin.php
6. Access the “Feedback” section. URL: http://localhost/OnlineExam/admin/afeedback.php



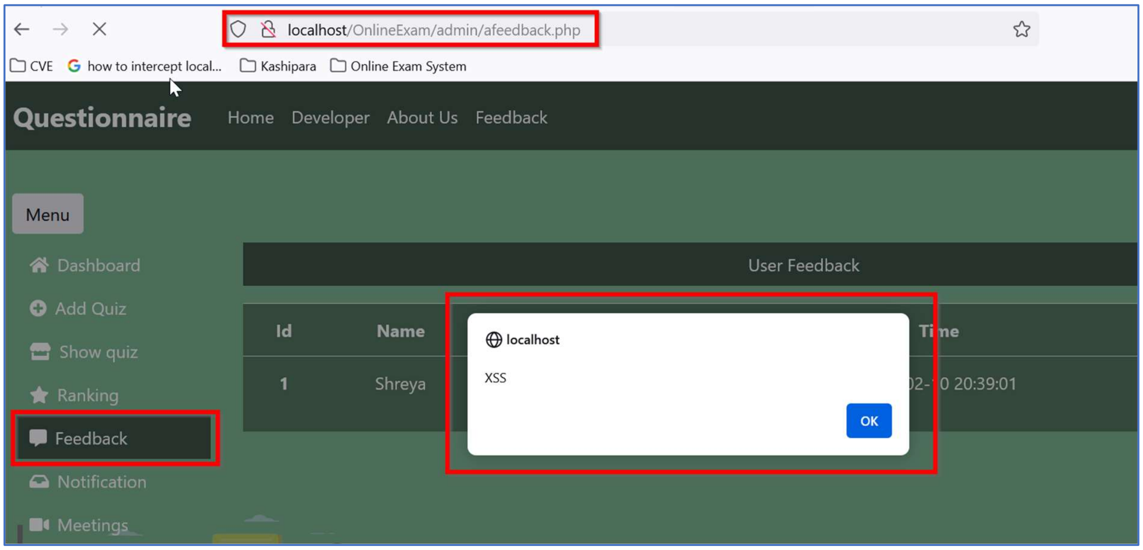
Id	Name	Collage	Ema
1	abc	juet	abc@gma
2	new	juet	new@gma
3	newuser	juet	newuser@g

7. The XSS scripts we entered in Step 2 are now displayed back as it is on the browser. This results in script execution and the Alert popup is displayed on the browser.


Response from http://localhost:80/OnlineExam/admin/afeedback.php [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
Render

```
          <a title="user feedback" class="btn btn-primary" href=update.php?q=dfdbk&id=23">
            <i class="far fa-trash-alt">
            </i>
          </a>
        </td>
      </tr>
      <tr>
        <th>
          2
        </th>
        <td>
          Test<script>
            alert("XSS")
          </script>
        </td>
        <td>
          Test<script>
            alert("XSS")
          </script>
        </td>
        <td>
          2024-07-02 20:02:19
        </td>
        <td>
          <a title="show feedback" class="btn btn-primary mr-2 mb-2" href="afeedback.php?q
```

8. This XSS script is stored in browser so every time the Feedback page is accessed; the script will get executed.



User Feedback

Id	Name	Time
1	Shreya	02-0 20:39:01

localhost

XSS

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