

Stored Cross Site Scripting (XSS) vulnerability was found in "`/admin/edit_room_controller.php`" of the Kashipara Hotel Management System v1.0 allows remote attackers to execute arbitrary code via "`room_name`" 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>)

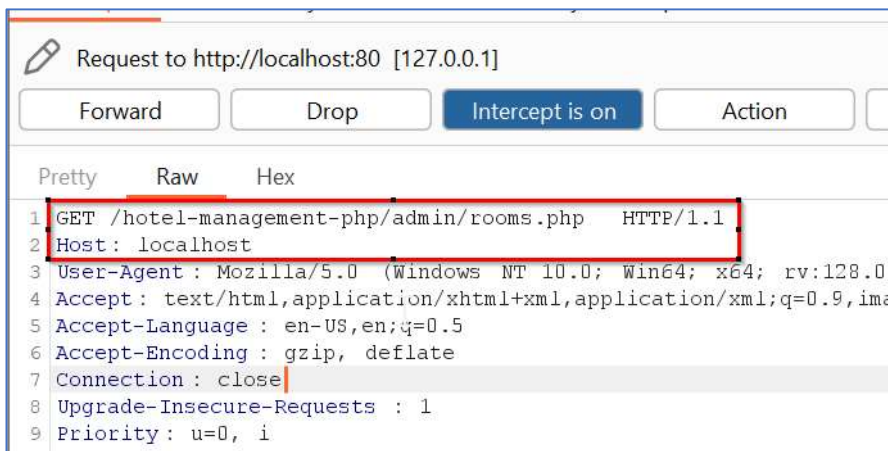
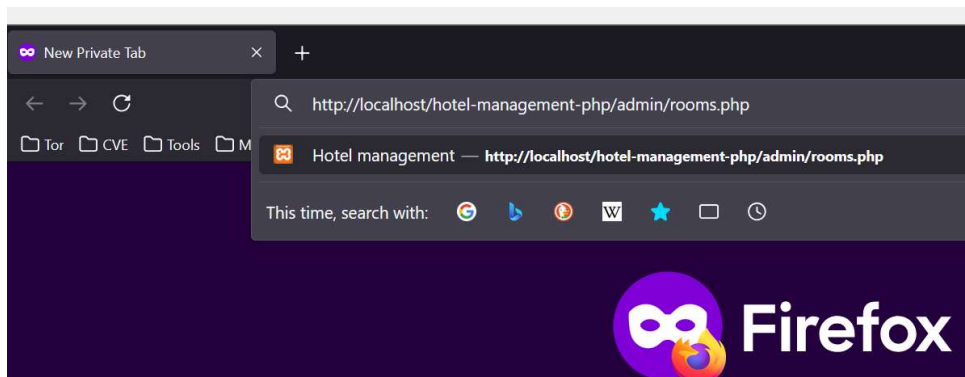
**Version:** 1.0

**Affected Components:**

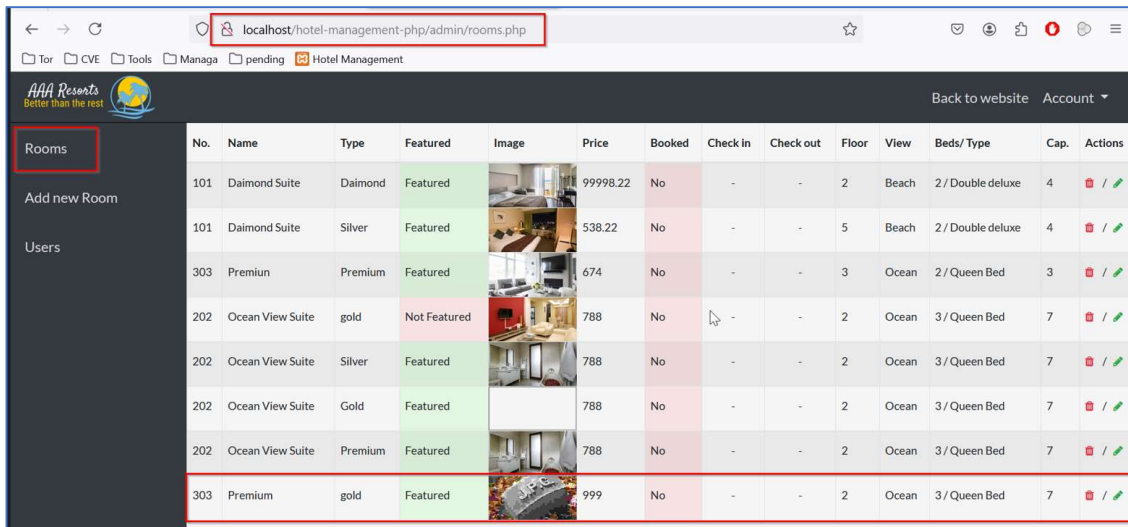
- **Affected Code File:** `/admin/edit_room_controller.php`
- **Affected Parameter:** "`room_name`" POST HTTP request parameter

**Steps:**

1. Access the "Admin -> Rooms" menu directly without any authentication (URL: <http://localhost/hotel-management-php/admin/rooms.php>)



- It was observed that the valid hotel room entries in the “Admin -> Rooms” menu page are directly accessible without authentication.



localhost/hotel-management-php/admin/rooms.php

AAA Resorts  
Better than the rest

Back to website Account

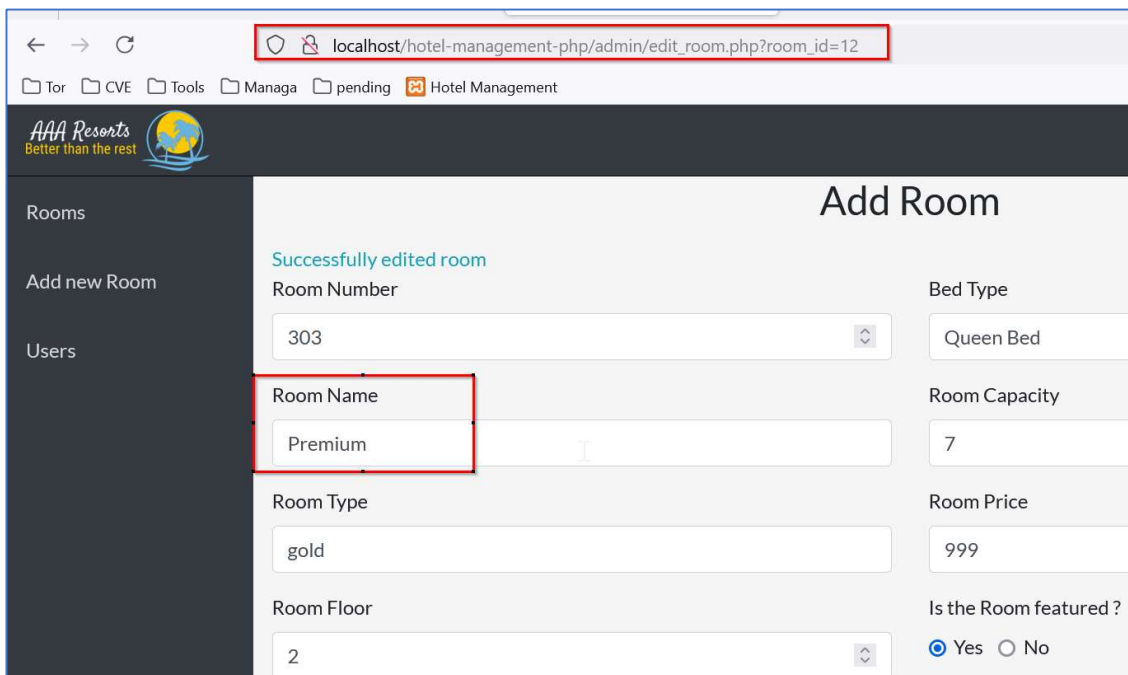
Rooms

Add new Room

Users

No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/Type	Cap.	Actions
101	Diamond Suite	Diamond	Featured		99998.22	No	-	-	2	Beach	2 / Double deluxe	4	
101	Diamond Suite	Silver	Featured		538.22	No	-	-	5	Beach	2 / Double deluxe	4	
303	Premium	Premium	Featured		674	No	-	-	3	Ocean	2 / Queen Bed	3	
202	Ocean View Suite	gold	Not Featured		788	No	-	-	2	Ocean	3 / Queen Bed	7	
202	Ocean View Suite	Silver	Featured		788	No	-	-	2	Ocean	3 / Queen Bed	7	
202	Ocean View Suite	Gold	Featured		788	No	-	-	2	Ocean	3 / Queen Bed	7	
202	Ocean View Suite	Premium	Featured		788	No	-	-	2	Ocean	3 / Queen Bed	7	
303	Premium	gold	Featured		999	No	-	-	2	Ocean	3 / Queen Bed	7	

- Select & edit any one of the hotel room entries. I have selected last hotel room entry with room name “Premium”. Click on the edit icon on right hand side.
- I am redirected to Add Room page. URL: [http://localhost/hotel-management-php/admin/edit\\_room.php?room\\_id=12](http://localhost/hotel-management-php/admin/edit_room.php?room_id=12)



localhost/hotel-management-php/admin/edit\_room.php?room\_id=12

AAA Resorts  
Better than the rest

Rooms

Add new Room

Users

## Add Room

Successfully edited room

Room Number

303

Bed Type

Queen Bed

Room Name

Premium

Room Capacity

7

Room Type

gold

Room Price

999

Room Floor

2

Is the Room featured ?

☒ Yes ☐ No

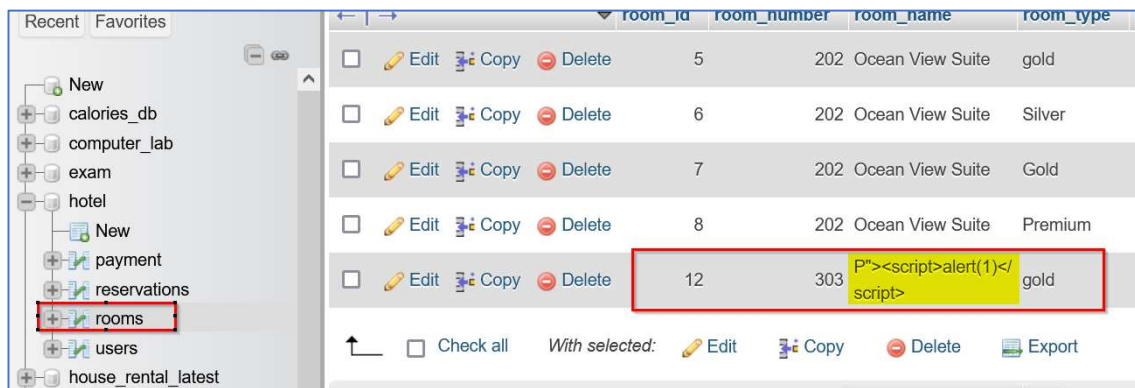
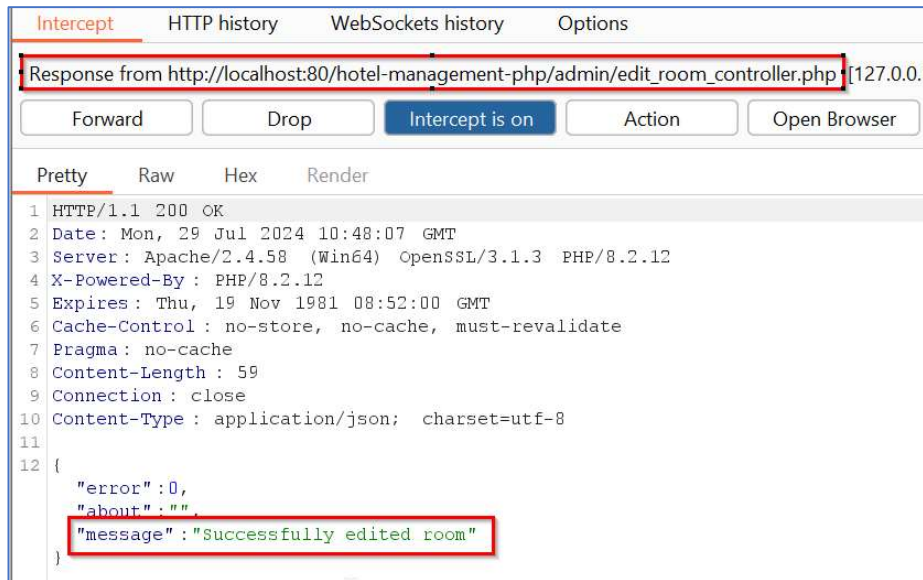
5. Now insert the XSS script `"><script>alert(1)</script>"` in the "Room Name" textbox. Enter any random value in other textboxes and click "Edit Room" button.

The screenshot shows a web application interface for editing a room. The form includes fields for Room Name, Room Capacity, Room Type, Room Price, Room Floor, Room View, and Room Amenities. The Room Name field is highlighted with a red box and contains the XSS payload `"><script>alert(1)</script>"`. The Room Capacity is 7, Room Price is 999, Room Floor is 2, Room View is Ocean, and Room Amenities is Ocean View, Wifi, Double bathroom. The Editing room... button is also highlighted with a red box.

6. This will forward the request with XSS script to server in the "room\_name" HTTP POST request parameter.

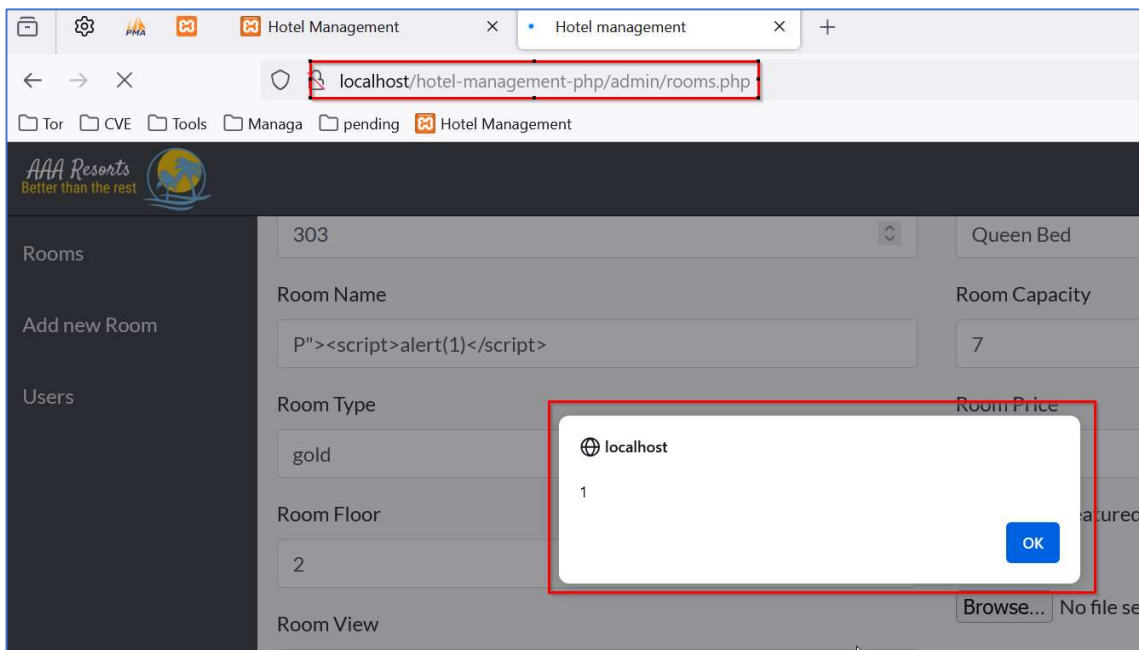
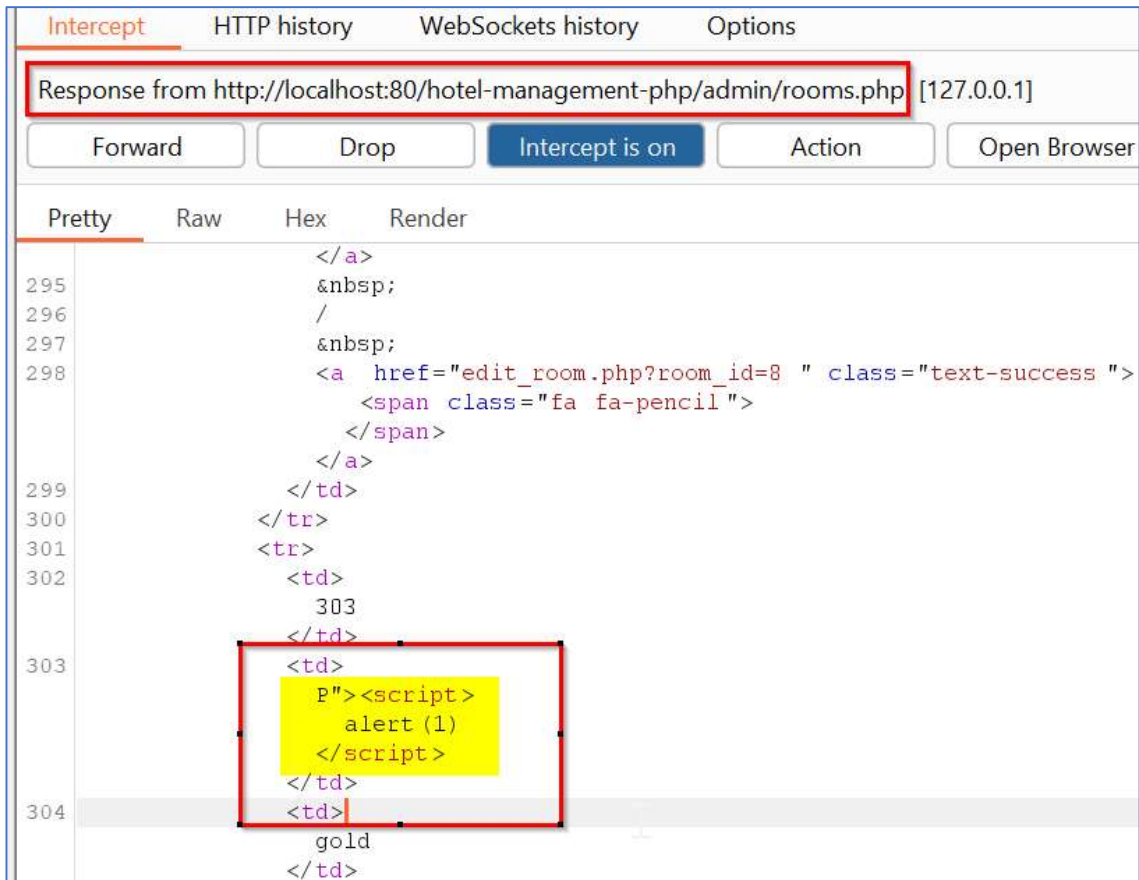


7. The request gets accepted and the hotel room name entry with XSS script is stored in the application database.



8. Let us try to view the "Admin -> Rooms" menu again. URL: <http://localhost/hotel-management-php/admin/rooms.php>.

9. The XSS script we submitted in the Step 5, gets reflected back as it is in the response and it gets executed in the browser.



**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](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)