COMMUNITY CONTENT

Home › Submit › 786325

Submit #786325: code-projects Online Hotel Booking IN PHP 1.0 Cross Site Scripting

Title	code-projects Online Hotel Booking IN PHP 1.0 Cross Site Scripting
Description	A Reflected Cross-Site Scripting (XSS) vulnerability exists in the Online Hotel Booking System in PHP within the booking functionality. The vulnerability occurs in the following endpoint: /hotel booking/booknow.php The application processes user-controlled input through the roomname parameter supplied via the HTTP GET request. The value of this parameter is reflected in the application response without proper validation or output encoding. Because the application directly includes the user-supplied value in the HTML output, malicious HTML or JavaScript code can be injected and executed in the browser of users who access a specially crafted URL. During testing, it was observed that injecting JavaScript code into the roomname parameter results in script execution when the page is rendered. injected value: Duplexerwat<script>alert(1)</script>d494k This indicates that the application fails to properly sanitize or encode user input before rendering it in the browser.
Source	⚠ https://github.com/ahmadmarz10-hub/CVEsMarz/blob/main/Reflected%20Cross-Site%20Scripting%20(XSS)%20in%20Online%20Hotel%20Booking%20System%20roomname%20Parameter.md
User	AhmadMarzouk (UID 95993)
Submission	03/23/2026 07:12 PM (14 days ago)
Moderation	04/06/2026 04:17 PM (14 days later)
Status	Accepted
VulDB entry	359421 [code-projects Online Hotel Booking 1.0 Booking Endpoint /booknow.php roomname cross site scripting]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling