ziyishen97 / CVE-2022-36254.md

Created 3 months ago

Public Reference for CVE-2022-36254

CVE-2022-36254.md

Product: Hotel Management System

Vendor: https://github.com/tramyardg

Affected Version(s): 1.0

CVE ID: CVE-2022-36254

Description: Multiple persistent cross-site scripting (XSS) vulnerabilities in index.php in tramyardg Hotel Management System 1.0 allow remote attackers to inject arbitrary web script or HTML via multiple parameters such as "fullname".

Vulnerability Type: Cross-Site Scripting (XSS)

Root Cause: Functions like insert(Customer $customer) in source file CustomerDAO.php do not have back-end input sanitization. And there is no sanitization on index.php as well.

Impact: An attacker is able to hijack authenticated users' sessions and act on behalf of them.

PoC:

1. Register a new account, then create a booking.
2. Submit the booking request, and ultilize Burpsuite to intercept the request.
3. Modify the value of a parameter such as requirement to <script>alert(1)</script>
4. Forward the request, and refresh index page. The payload will be triggered.