IT & COMPUTER SOLUTIONS PRIVATE LIMITED

Make the World Around You Digitally Creative!

Web Application Security Audit Report

Target: kcit.com

Date: 15-03-2026

Prepared by: Kadambari

Contents

Executive Summary

This report presents the results of a web application security assessment conducted based on the OWASP Top 10 standard.

The objective of this assessment was to identify common security vulnerabilities that could be exploited by attackers. The testing was performed using a combination of manual techniques and automated tools.

Multiple vulnerabilities were identified during the assessment, including input validation issues and missing security controls. Some findings pose a significant risk and should be addressed on priority.

Overall Risk Level: Moderate to High

Scope & Methodology

Scope

- ☑ Target Application: https://kcit.com
- ☑ Testing Type: Black-box testing
- ☑ Testing Standard: OWASP Top 10 2025 (latest)

Methodology

The assessment was conducted using a structured approach covering key areas of web application security.

Testing included:

- Input validation testing
- Authentication and session management checks
- Security configuration review
- API endpoint testing (where applicable)

Tools used:

- Burp Suite
- OWASP ZAP
- Browser Developer Tools

Risk Summary

Risk Overview

Severity	Count
🔴 Critical	1
🟠 High	1
🟡 Medium	1
🟢 Low	0

Severity Classification

- **Critical:** Immediate exploitation possible with severe impact (data breach, full compromise)
- **High:** High likelihood of exploitation with significant impact
- **Medium:** Moderate risk requiring attention
- **Low:** Minor issue with limited impact

Detailed Findings

1. Cross-Site Scripting (XSS)

Severity: 🟠 High

Description:
The application does not properly sanitize user input in certain fields, allowing injection of malicious scripts.

Impact:
An attacker can execute arbitrary JavaScript in a user's browser, potentially leading to session hijacking, credential theft, or redirection to malicious sites.

Recommendation:

- Implement input validation
- Use output encoding
- Apply Content Security Policy (CSP)

2. Missing Security Headers

Severity: 🟡 Medium

Description:
The application response is missing important HTTP security headers such as Content-Security-Policy, X-Frame-Options, and X-Content-Type-Options.

Impact:
This increases the risk of clickjacking, MIME-type attacks, and other client-side exploits.

Recommendation:
Configure the following headers:

- Content-Security-Policy
- X-Frame-Options
- X-Content-Type-Options

Conclusion

The security assessment identified multiple vulnerabilities that could impact the confidentiality and integrity of the application.

Critical and high severity findings should be addressed immediately to reduce the risk of exploitation. Medium-level issues should be resolved in a timely manner as part of ongoing security improvements.

It is recommended to conduct regular security assessments and implement secure development practices.