Web Security Assessment Report

Target Information

Target URL: https://tsit.mjunction.in/tauc/security/getLogin

Scan Date: 2025-07-31 17:57:36

Total Alerts: 2

URLs Scanned: 3

Risk Summary

Risk Level	Count
High	2
Medium	0
Low	0
Informational	0

Executive Summary

The security assessment identified 2 potential security issues. Among these, 2 are classified as high risk and require immediate attention. This report provides detailed information about each finding along with recommended remediation steps.

Key Findings

Critical Issues Found:

- Cross Site Scripting (Reflected)
- SQL Injection

Vulnerability Details

High Risk Vulnerabilities

1. Cross Site Scripting (Reflected)

Description:	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied c
Risk Level:	High
Confidence:	Medium
URL:	http://example.com/search
Parameter:	q

Recommended Solution:

Validate all input and encode output to prevent XSS attacks.

2. SQL Injection

Description:	SQL injection may be possible.
Risk Level:	High
Confidence:	High
URL:	http://example.com/login
Parameter:	username

Recommended Solution:

Use parameterized queries to prevent SQL injection.

Security Recommendations

General Security Best Practices:

• Implement proper input validation and sanitization
• Use HTTPS for all communications
• Implement Content Security Policy (CSP) headers
• Regular security updates and patches
• Implement proper authentication and authorization
• Use secure coding practices
• Regular security assessments and penetration testing
• Implement proper logging and monitoring

Specific Recommendations Based on Findings:

• Implement proper input validation and output encoding
• Use parameterized queries and stored procedures