Web Security Assessment Report

Target Information

Target URL:	https://tsit.mjunction.in/tauc/security/getLogin
Scan Date:	2025-07-31 21:00:54
Total Alerts:	4
URLs Scanned:	0

Risk Summary

Risk Level	Count
High	1
Medium	2
Low	1
Informational	0

Executive Summary

The security assessment identified 4 potential security issues. Among these, 1 are classified as high risk and require immediate attention. Additionally, 2 medium-risk vulnerabilities were found that should be addressed in the near term. This report provides detailed information about each finding along with recommended remediation steps.

Key Findings

Critical Issues Found:

- Network Connectivity Issues

Vulnerability Details

High Risk Vulnerabilities

1. Network Connectivity Issues

Description:	Target URL is not accessible or responding slowly
Risk Level:	High
Confidence:	High
URL:	https://tsit.mjunction.in/tauc/security/getLogin
Parameter:	

Recommended Solution:

Check network connectivity and server availability

Medium Risk Vulnerabilities

1. Missing Anti-CSRF Tokens

Description:	No Anti-CSRF tokens were found in a HTML submission form.
Risk Level:	Medium
Confidence:	Medium
URL:	https://tsit.mjunction.in/profile
Parameter:	form

Recommended Solution:

Implement CSRF protection tokens in all forms.

2. Directory Browsing

Description:	It is possible to view a listing of the directory contents.
Risk Level:	Medium
Confidence:	High
URL:	https://tsit.mjunction.in/assets/
Parameter:	

Recommended Solution:

Disable directory browsing on the web server.

Low Risk Vulnerabilities

1. Content Type Options Not Set

Description:	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to nosniff.
Risk Level:	Low
Confidence:	Medium
URL:	https://tsit.mjunction.in/assets/css/style.css
Parameter:	

Recommended Solution:

Set X-Content-Type-Options header to nosniff.

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:

- Address the identified Network Connectivity Issues vulnerability according to security best practices
- Address the identified Content Type Options Not Set vulnerability according to security best practices
- Address the identified Directory Browsing vulnerability according to security best practices
- Address the identified Missing Anti-CSRF Tokens vulnerability according to security best practices