Web Security Assessment Report

Target Information

Target URL: https://raceprod.mjunction.in/

Scan Date: 2025-07-31 20:42:18

Total Alerts: 7

URLs Scanned: 0

Risk Summary

Risk Level	Count
High	0
Medium	3
Low	2
Informational	2

Executive Summary

The security assessment identified 7 potential security issues. Additionally, 3 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

No critical security issues found.

Vulnerability Details

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://raceprod.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://raceprod.mjunction.in/assets/
Parameter:	

Recommended Solution:

Disable directory browsing on the web server.

3. Missing Security Headers

Description:	The following security headers are missing: X-Content-Type-Options, X-XSS-Protection
Risk Level:	Medium
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Configure web server to include proper security headers

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://raceprod.mjunction.in/assets/css/style.css
Parameter:	

Recommended Solution:

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

2. Server Information Disclosure

Description:	Server header reveals technology: Apache/2.4.62 ()
Risk Level:	Low
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Configure server to hide version information

Informational Risk Vulnerabilities

1. SSL/TLS Configuration Review

Description:	SSL/TLS configuration should be reviewed for best practices
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Use SSL Labs test to verify cipher suites and protocol versions

2. Security Best Practices Review

Description:	Regular security assessments recommended for web applications
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Implement regular security testing and code reviews

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 Missing Security Headers vulnerability according to security best practices
• Address the identified Security Best Practices Review vulnerability according to security best practices
• Address the identified Missing Anti-CSRF Tokens vulnerability according to security best practices
• Address the identified SSL/TLS Configuration Review vulnerability according to security best practices
• Address the identified Directory Browsing vulnerability according to security best practices
• Address the identified Content Type Options Not Set vulnerability according to security best practices
• Remove sensitive information from error messages and headers