Web Security Assessment Report

Target Information

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

Scan Date: 2025-07-31 18:54:38

Total Alerts: 8

URLs Scanned: 0

Risk Summary

Risk Level	Count
High	2
Medium	4
Low	1
Informational	1

Executive Summary

The security assessment identified 8 potential security issues. Among these, 2 are classified as high risk and require immediate attention. Additionally, 4 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:

- SQL Injection
- Cross Site Scripting (Reflected)

Vulnerability Details

High Risk Vulnerabilities

1. SQL Injection

Description:	SQL injection may be possible. The application may be vulnerable to SQL injection attacks
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/search?q=test
Parameter:	q

Recommended Solution:

Use prepared statements and parameterized queries to prevent SQL injection.

2. 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:	https://raceprod.mjunction.in/search?query=<script>alert(1)</script>
Parameter:	query

Recommended Solution:

Validate all input and encode all output to prevent XSS.

Medium Risk Vulnerabilities

1. Information Disclosure - Sensitive Information in URL

Description:	The request appears to contain sensitive information leaked in the URL. This can violate P
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/login?redirect=/admin
Parameter:	redirect

Recommended Solution:

Do not pass sensitive information in URLs.

2. Content Security Policy (CSP) Header Not Set

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigat
Risk Level:	Medium
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

3. Absence of 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/contact
Parameter:	

Recommended Solution:

Use anti-CSRF tokens in all state-changing forms.

4. X-Frame-Options Header Not Set

Description:	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJac
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site.

Low Risk Vulnerabilities

1. Cookie Without Secure Flag

Description:	A cookie has been set without the secure flag, which means that the cookie can be access
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in/login
Parameter:	sessionid

Recommended Solution:

Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel.

Informational Risk Vulnerabilities

1. Modern Web Application

Description:	The application appears to be a modern web application. This is not necessarily a vulnerab
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Ensure the application follows modern security practices and implements appropriate security headers.

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 Absence of Anti-CSRF Tokens vulnerability according to security best practices
• Use parameterized queries and stored procedures
• Address the identified X-Frame-Options Header Not Set vulnerability according to security best practices
• Set Secure flag on all cookies over HTTPS
• Remove sensitive information from error messages and headers
• Implement proper input validation and output encoding
• Address the identified Content Security Policy (CSP) Header Not Set vulnerability according to security best practices
• Address the identified Modern Web Application vulnerability according to security best practices