Web Security Assessment Report

Target Information

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

Scan Date: 2025-07-31 20:49:43

Total Alerts: 27

URLs Scanned: 0

Risk Summary

Risk Level	Count
High	0
Medium	5
Low	10
Informational	12

Executive Summary

The security assessment identified 27 potential security issues. Additionally, 5 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

4. 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.

5. 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. 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

3. Permissions Policy Header Not Set

Description:	Permissions Policy Header is an added layer of security that helps to restrict from unautho
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

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

4. Server Leaks Information via "Server" HTTP Response Header Field

Description:	The web/application server is leaking information via the "Server" HTTP response header.
Risk Level:	Low
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	Server

Recommended Solution:

Ensure that your web server, application server, load balancer, etc. is configured to suppress "Server" header.

5. X-Content-Type-Options Header Missing

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/

Parameter:

Recommended Solution:

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff'.

6. Cookie No SameSite Attribute

Description: A cookie has been set without the SameSite attribute, which means that the cookie can be

Risk Level: Low

Confidence: Medium

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

Parameter: Set-Cookie

Recommended Solution:

Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

7. Cookie Without HttpOnly Flag

Description: A cookie has been set without the HttpOnly flag, which means that the cookie can be acce

Risk Level: Low

Confidence: Medium

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

Parameter: Set-Cookie

Recommended Solution:

Ensure that the HttpOnly flag is set for all cookies.

8. 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/

Parameter: Set-Cookie

Recommended Solution:

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

9. Cross-Domain JavaScript Source File Inclusion

Description:	The page includes one or more script files from a third-party domain.
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Ensure JavaScript source files are loaded from only trusted sources, and the sources cannot be controlled by end users of the application.

10. Strict-Transport-Security Header Not Set

Description:	HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps to pr
Risk Level:	Low
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 Strict-Transport-Security header.

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. Referrer Policy Header Not Set

Description: This response did not specify a Referrer Policy header, which dictates how much referrer i

Risk Level: Informational

Confidence: Medium

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

Parameter:

Recommended Solution:

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

3. Base64 Disclosure

Description: Base64 encoded data was disclosed by the application/web server.

Risk Level: Informational

Confidence: Medium

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

Parameter:

Recommended Solution:

Manually confirm that the Base64 data does not leak sensitive information, and that the data cannot be aggregated/used to exploit other vulnerabilities.

4. Information Disclosure - Suspicious Comments

Description: The response appears to contain suspicious comments which may help an attacker.

Risk Level: Informational

Confidence: Low

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

Parameter:

Recommended Solution:

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

5. Modern Web Application

Description: The application appears to be a modern web application. If you need to explore it automati

Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

This is an informational alert and so no changes are required.

6. Storable and Cacheable Content

Description:	The response contents are storable by caching components such as proxy servers, and ma
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Validate that the response does not contain sensitive, personal or user-specific information.

7. Timestamp Disclosure - Unix

Description:	A timestamp was disclosed by the application/web server - Unix
Risk Level:	Informational
Confidence:	Low
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

8. Hash Disclosure

Description:	A hash was disclosed by the web server.
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Ensure that hashes that are used to protect credentials or other resources are not leaked by the web server or database.

9. Incomplete or No Cache-control Header Set

Description:	The cache-control header has not been set properly or is missing, allowing the browser an
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	Cache-Control

Recommended Solution:

Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate.

10. Retrieved from Cache

Description:	The content was retrieved from a shared cache. If the response data is sensitive, personal
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Validate that the response does not contain sensitive, personal or user-specific information.

11. Re-examine Cache-control Directives

Description:	The cache-control header has not been set properly or is missing, allowing the browser an
Risk Level:	Informational
Confidence:	Low
URL:	https://raceprod.mjunction.in/
Parameter:	Cache-Control

Recommended Solution:

For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate".

12. 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:

• Remove sensitive information from error messages and headers
• Address the identified Incomplete or No Cache-control Header Set vulnerability according to security best practices
• Address the identified Permissions Policy Header Not Set vulnerability according to security best practices
• Address the identified Missing Anti-CSRF Tokens vulnerability according to security best practices
• Address the identified Server Leaks Information via "Server" HTTP Response Header Field vulnerability according to security best practices
• Address the identified X-Frame-Options Header Not Set vulnerability according to security best practices
• Address the identified Base64 Disclosure vulnerability according to security best practices
• Address the identified Retrieved from Cache vulnerability according to security best practices
• Address the identified SSL/TLS Configuration Review vulnerability according to security best practices
• Address the identified X-Content-Type-Options Header Missing vulnerability according to security best practices