Web Security Assessment Report

Target Information

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

Scan Date: 2025-07-31 19:01:13

Total Alerts: 13

URLs Scanned: 0

Risk Summary

Risk Level	Count
High	1
Medium	5
Low	7
Informational	0

Executive Summary

The security assessment identified 13 potential security issues. Among these, 1 are classified as high risk and require immediate attention. 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

Critical Issues Found:

• PII Disclosure

Vulnerability Details

High Risk Vulnerabilities

1. PII Disclosure

Description: The response contains Personally Identifiable Information, such as CC number, SSN and s

Risk Level: High

Confidence: Medium

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

Parameter:

Recommended Solution:

Ensure that PII is properly protected and not disclosed in responses.

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. Cross-Domain Misconfiguration

Description:	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (COR
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Ensure that the CORS configuration is secure and does not allow unauthorized cross-origin requests.

4. Secure Pages Include Mixed Content

Description:	The page includes mixed content, that is content accessed via both HTTP and HTTPS.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS.

5. Insecure JSF ViewState

Description:	The response contains ViewState value of a JSF (JavaServer Faces) and it is not encrypte
Risk Level:	Medium
Confidence:	High
URL:	https://raceprod.mjunction.in/jsf-page
Parameter:	javax.faces.ViewState

Recommended Solution:

Secure JSF ViewState with encryption and/or MAC.

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.

2. 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".

3. 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.

4. 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/login
Parameter:	JSESSIONID

Recommended Solution:

Ensure that the HttpOnly flag is set for all cookies.

5. 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.

6. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description:	The web/application server is leaking information via one or more "X-Powered-By" HTTP re
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 suppress "X-Powered-By" headers.

7. Timestamp Disclosure

Description:	A timestamp was disclosed by the application/web server.
Risk Level:	Low
Confidence:	Low

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

Parameter:

Recommended Solution:

Remove unnecessary timestamp information from responses.

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:

• Set Secure flag on all cookies over HTTPS
• Address the identified Permissions Policy Header Not Set vulnerability according to security best practices
• Address the identified Insecure JSF ViewState vulnerability according to security best practices
• Address the identified X-Content-Type-Options Header Missing vulnerability according to security best practices
• Address the identified Content Security Policy (CSP) Header Not Set vulnerability according to security best practices
• Remove sensitive information from error messages and headers
• Address the identified Cookie Without HttpOnly Flag vulnerability according to security best practices
• Address the identified Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) vulnerability according to security best practices
• Address the identified Timestamp Disclosure vulnerability according to security best practices
• Address the identified Cross-Domain JavaScript Source File Inclusion vulnerability according to security best practices