

Web Security Assessment Report

Target Information

Target URL: https://raceprod.mjunction.in/
Scan Date: 2025-07-31 21:03:32
Total Alerts: 94
URLs Scanned: 0

Risk Summary

Risk Level	Count
High	4
Medium	50
Low	24
Informational	16

Executive Summary

The security assessment identified 94 potential security issues. Among these, 4 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:

- Path Traversal
- Remote File Inclusion
- Heartbleed OpenSSL Vulnerability
- LDAP Injection

Vulnerability Details

High Risk Vulnerabilities

1. Path Traversal

Description:	The Path Traversal attack technique allows an attacker access to files, directories, and con
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/../../../../etc/passwd
Parameter:	file

Recommended Solution:

Assume all input is malicious. Use an "accept known good" input validation strategy.

2. Remote File Inclusion

Description:	Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mec
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	include

Recommended Solution:

Update to the latest version. Apply the latest patches. Use indirect object references.

3. Heartbleed OpenSSL Vulnerability

Description:	The TLS implementation in OpenSSL 1.0.1 before 1.0.1g does not properly handle TLS/D
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Update to OpenSSL 1.0.1g or later.

4. LDAP Injection

Description:	LDAP Injection may be possible.
Risk Level:	High
Confidence:	Medium
URL:	https://raceprod.mjunction.in//search
Parameter:	username

Recommended Solution:

Validate and/or escape all user input before using it to create an LDAP query.

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 mitigate some types of attacks, including Cross Site Scripting (XSS) and data injection attacks.
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 'ClickJacking' attacks.
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.

6. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like t
Risk Level: Medium
Confidence: Medium
URL: https://raceprod.mjunction.in/
Parameter:

Recommended Solution:

Review the source code of this page. Implement custom error pages.

7. Backup File Disclosure

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

Recommended Solution:

Do not edit files in-situ on the web server, and ensure that un-necessary files (including backup files) are removed from the web server.

8. Directory Browsing

Description:	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in//admin/
Parameter:	

Recommended Solution:

Configure the web server to disable directory browsing.

9. Source Code Disclosure - SVN

Description:	The source code repository SVN metadata was disclosed by the web/application server.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in//.svn/
Parameter:	

Recommended Solution:

Ensure that SVN metadata files are not deployed to the web server or application server, or are otherwise made accessible to browsers.

10. Source Code Disclosure - Git

Description:	The source code repository Git metadata was disclosed by the web/application server.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/.git/
Parameter:	

Recommended Solution:

Ensure that Git metadata files are not deployed to the web server or application server.

11. Weak Authentication Method

Description:	HTTP BASIC authentication was used over an unsecured connection.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/admin
Parameter:	Authorization

Recommended Solution:

Protect the connection using HTTPS or use a stronger authentication mechanism.

12. Session ID in URL Rewrite

Description:	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site scripting.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/;jsessionid=123
Parameter:	jsessionid

Recommended Solution:

For secure content, put session ID in a cookie.

13. Session Fixation

Description:	The application may be vulnerable to session fixation attacks.
Risk Level:	Medium
Confidence:	Medium

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

Recommended Solution:

Generate a new session ID for each authenticated session.

14. Absence of Anti-CSRF Tokens

Description: No Anti-CSRF tokens were found in a HTML submission form.
Risk Level: Medium
Confidence: Low
URL: https://raceprod.mjunction.in//form
Parameter:

Recommended Solution:

Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur.

15. Cross-Domain Misconfiguration

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration.
Risk Level: Medium
Confidence: Medium
URL: https://raceprod.mjunction.in/
Parameter: Access-Control-Allow-Origin

Recommended Solution:

Ensure that sensitive data is not available in an unauthenticated manner.

16. HTTP Only Site

Description: The site is only served under HTTP and not HTTPS.
Risk Level: Medium
Confidence: Medium
URL: https://raceprod.mjunction.in/
Parameter:

Recommended Solution:

Configure your web or application server to use SSL (https).

17. Insecure JSF ViewState

Description:	The application is using JSF viewstate but it is not properly protected.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	javax.faces.ViewState

Recommended Solution:

Secure the JSF ViewState by encrypting it.

18. Sensitive Directory - /admin

Description:	A potentially sensitive directory was identified at /admin.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in//admin
Parameter:	

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

19. Sensitive Directory - /api

Description:	A potentially sensitive directory was identified at /api.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in//api
Parameter:	

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

20. Sensitive Directory - /login

Description:	A potentially sensitive directory was identified at /login.
---------------------	---

Risk Level: Medium
Confidence: Low
URL: <https://raceprod.mjunction.in//login>
Parameter:

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

21. Sensitive Directory - /register

Description: A potentially sensitive directory was identified at /register.
Risk Level: Medium
Confidence: Low
URL: <https://raceprod.mjunction.in//register>
Parameter:

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

22. Sensitive Directory - /upload

Description: A potentially sensitive directory was identified at /upload.
Risk Level: Medium
Confidence: Low
URL: <https://raceprod.mjunction.in//upload>
Parameter:

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

23. Sensitive Directory - /download

Description: A potentially sensitive directory was identified at /download.
Risk Level: Medium
Confidence: Low
URL: <https://raceprod.mjunction.in//download>
Parameter:

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

24. Sensitive Directory - /search

Description:	A potentially sensitive directory was identified at /search.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in//search
Parameter:	

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

25. Sensitive Directory - /config

Description:	A potentially sensitive directory was identified at /config.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in//config
Parameter:	

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

26. Sensitive Directory - /backup

Description:	A potentially sensitive directory was identified at /backup.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in//backup
Parameter:	

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

27. Sensitive Directory - /test

Description: A potentially sensitive directory was identified at /test.
Risk Level: Medium
Confidence: Low
URL: https://raceprod.mjunction.in//test
Parameter:

Recommended Solution:

Restrict access to sensitive directories or remove them if not needed.

28. Parameter Pollution - id

Description: HTTP Parameter Pollution was identified for parameter id.
Risk Level: Medium
Confidence: Low
URL: https://raceprod.mjunction.in/?id=test&id=test2
Parameter: id

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

29. Open Redirect - id

Description: Open redirect vulnerability found via id parameter.
Risk Level: Medium
Confidence: Medium
URL: https://raceprod.mjunction.in/?id=http://evil.com
Parameter: id

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

30. Parameter Pollution - user

Description: HTTP Parameter Pollution was identified for parameter user.
Risk Level: Medium
Confidence: Low
URL: https://raceprod.mjunction.in/?user=test&user=test2

Parameter: user

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

31. Open Redirect - user

Description: Open redirect vulnerability found via user parameter.
Risk Level: Medium
Confidence: Medium
URL: <https://raceprod.mjunction.in/?user=http://evil.com>
Parameter: user

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

32. Parameter Pollution - file

Description: HTTP Parameter Pollution was identified for parameter file.
Risk Level: Medium
Confidence: Low
URL: <https://raceprod.mjunction.in/?file=test&file=test2>
Parameter: file

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

33. Open Redirect - file

Description: Open redirect vulnerability found via file parameter.
Risk Level: Medium
Confidence: Medium
URL: <https://raceprod.mjunction.in/?file=http://evil.com>
Parameter: file

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

34. Parameter Pollution - page

Description:	HTTP Parameter Pollution was identified for parameter page.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/?page=test&page=test2
Parameter:	page

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

35. Open Redirect - page

Description:	Open redirect vulnerability found via page parameter.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/?page=http://evil.com
Parameter:	page

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

36. Parameter Pollution - redirect

Description:	HTTP Parameter Pollution was identified for parameter redirect.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/?redirect=test&redirect=test2
Parameter:	redirect

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

37. Open Redirect - redirect

Description:	Open redirect vulnerability found via redirect parameter.
Risk Level:	Medium
Confidence:	Medium

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

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

38. Parameter Pollution - url

Description: HTTP Parameter Pollution was identified for parameter url.
Risk Level: Medium
Confidence: Low
URL: https://raceprod.mjunction.in/?url=test&url=test2
Parameter: url

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

39. Open Redirect - url

Description: Open redirect vulnerability found via url parameter.
Risk Level: Medium
Confidence: Medium
URL: https://raceprod.mjunction.in/?url=http://evil.com
Parameter: url

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

40. Parameter Pollution - callback

Description: HTTP Parameter Pollution was identified for parameter callback.
Risk Level: Medium
Confidence: Low
URL: https://raceprod.mjunction.in/?callback=test&callback=test2
Parameter: callback

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

41. Open Redirect - callback

Description:	Open redirect vulnerability found via callback parameter.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/?callback=http://evil.com
Parameter:	callback

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

42. Parameter Pollution - return

Description:	HTTP Parameter Pollution was identified for parameter return.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/?return=test&return=test2
Parameter:	return

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

43. Open Redirect - return

Description:	Open redirect vulnerability found via return parameter.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/?return=http://evil.com
Parameter:	return

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

44. Parameter Pollution - next

Description:	HTTP Parameter Pollution was identified for parameter next.
Risk Level:	Medium

Confidence: Low
URL: https://raceprod.mjunction.in/?next=test&next=test2
Parameter: next

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

45. Open Redirect - next

Description: Open redirect vulnerability found via next parameter.
Risk Level: Medium
Confidence: Medium
URL: https://raceprod.mjunction.in/?next=http://evil.com
Parameter: next

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

46. Parameter Pollution - search

Description: HTTP Parameter Pollution was identified for parameter search.
Risk Level: Medium
Confidence: Low
URL: https://raceprod.mjunction.in/?search=test&search=test2
Parameter: search

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

47. Open Redirect - search

Description: Open redirect vulnerability found via search parameter.
Risk Level: Medium
Confidence: Medium
URL: https://raceprod.mjunction.in/?search=http://evil.com
Parameter: search

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

48. Parameter Pollution - q

Description:	HTTP Parameter Pollution was identified for parameter q.
Risk Level:	Medium
Confidence:	Low
URL:	https://raceprod.mjunction.in/?q=test&q=test2
Parameter:	q

Recommended Solution:

Identify the intended parameter and remove or ignore the duplicate.

49. Open Redirect - q

Description:	Open redirect vulnerability found via q parameter.
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/?q=http://evil.com
Parameter:	q

Recommended Solution:

Validate all input and use a whitelist of allowed redirect targets.

50. ASP.NET ViewState Without MAC

Description:	ASP.NET ViewState is not protected with a MAC (Message Authentication Code).
Risk Level:	Medium
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	__VIEWSTATE

Recommended Solution:

Enable ViewState MAC protection in web.config.

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 unauthorized access to certain features of the browser.
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 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 acces
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 accessed over an unencrypted channel.

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 protect websites from "man-in-the-middle" attacks by enforcing secure connections.

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.

11. 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:

Remove the private IP address from the HTTP response body.

12. Big Redirect Detected (Potential Sensitive Information Leak)

Description:	The server has responded with a redirect that seems to provide a large response.
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in//redirect
Parameter:	

Recommended Solution:

Ensure that the response body is empty for 3xx status codes.

13. Information Disclosure - /admin

Description:	The /admin endpoint may disclose sensitive information.
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in//admin
Parameter:	

Recommended Solution:

Review the information disclosed by this endpoint.

14. Information Disclosure - /api

Description: The /api endpoint may disclose sensitive information.

Risk Level: Low

Confidence: Medium

URL: <https://raceprod.mjunction.in//api>

Parameter:

Recommended Solution:

Review the information disclosed by this endpoint.

15. Information Disclosure - /login

Description: The /login endpoint may disclose sensitive information.

Risk Level: Low

Confidence: Medium

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

Parameter:

Recommended Solution:

Review the information disclosed by this endpoint.

16. Information Disclosure - /register

Description: The /register endpoint may disclose sensitive information.

Risk Level: Low

Confidence: Medium

URL: <https://raceprod.mjunction.in//register>

Parameter:

Recommended Solution:

Review the information disclosed by this endpoint.

17. Information Disclosure - /upload

Description: The /upload endpoint may disclose sensitive information.

Risk Level: Low

Confidence: Medium

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

Parameter:

Recommended Solution:

Review the information disclosed by this endpoint.

18. Information Disclosure - /download

Description: The /download endpoint may disclose sensitive information.

Risk Level: Low

Confidence: Medium

URL: <https://raceprod.mjunction.in//download>

Parameter:

Recommended Solution:

Review the information disclosed by this endpoint.

19. Information Disclosure - /search

Description: The /search endpoint may disclose sensitive information.

Risk Level: Low

Confidence: Medium

URL: <https://raceprod.mjunction.in//search>

Parameter:

Recommended Solution:

Review the information disclosed by this endpoint.

20. Information Disclosure - /config

Description: The /config endpoint may disclose sensitive information.

Risk Level: Low

Confidence: Medium

URL: <https://raceprod.mjunction.in//config>

Parameter:

Recommended Solution:

Review the information disclosed by this endpoint.

21. Information Disclosure - /backup

Description:	The /backup endpoint may disclose sensitive information.
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in//backup
Parameter:	

Recommended Solution:

Review the information disclosed by this endpoint.

22. Information Disclosure - /test

Description:	The /test endpoint may disclose sensitive information.
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in//test
Parameter:	

Recommended Solution:

Review the information disclosed by this endpoint.

23. Apache Server Info Disclosure

Description:	Apache server information was disclosed.
Risk Level:	Low
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	Server

Recommended Solution:

Configure Apache to suppress version information.

24. PHP Version Disclosure

Description:	PHP version information was disclosed.
Risk Level:	Low
Confidence:	Medium

URL: https://raceprod.mjunction.in/
Parameter: X-Powered-By

Recommended Solution:

Configure PHP to suppress 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. Referrer Policy Header Not Set

Description: This response did not specify a Referrer Policy header, which dictates how much referrer information is passed to the destination.
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 m
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 and
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 and other clients to cache the response.
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. Username Hash Found

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

Recommended Solution:

Ensure that usernames are not disclosed in an encoded fashion.

13. Cookie Loosely Scoped to Domain

Description: Cookies can be scoped by domain or path. This check is only concerned with domain scope.
Risk Level: Informational
Confidence: Low
URL: https://raceprod.mjunction.in/
Parameter: Set-Cookie

Recommended Solution:

Always scope cookies to a FQDN (Fully Qualified Domain Name).

14. jQuery Version Disclosure

Description:	jQuery version information was disclosed.
Risk Level:	Informational
Confidence:	High
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Update to the latest version of jQuery.

15. Bootstrap Version Disclosure

Description:	Bootstrap framework version was disclosed.
Risk Level:	Informational
Confidence:	Medium
URL:	https://raceprod.mjunction.in/
Parameter:	

Recommended Solution:

Update to the latest version of Bootstrap.

16. 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 Retrieved from Cache vulnerability according to security best practices
- Address the identified Open Redirect - q vulnerability according to security best practices
- Address the identified jQuery Version Disclosure vulnerability according to security best practices
- Address the identified Permissions Policy Header Not Set vulnerability according to security best practices
- Address the identified Source Code Disclosure - SVN vulnerability according to security best practices
- Address the identified Apache Server Info Disclosure vulnerability according to security best practices
- Address the identified Application Error Disclosure vulnerability according to security best practices
- Address the identified Open Redirect - page vulnerability according to security best practices
- Address the identified Sensitive Directory - /upload vulnerability according to security best practices
- Address the identified X-Content-Type-Options Header Missing vulnerability according to security best practices