Web Security Assessment Report

Target Information

Target URL: https://www.flipkart.com/

Scan Date: 2025-07-31 18:09:38

Total Alerts: 8

URLs Scanned: 20

Risk Summary

Risk Level	Count
High	2
Medium	4
Low	2
Informational	0

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:

- Cross Site Scripting (Reflected)
- SQL Injection

Vulnerability Details

High Risk Vulnerabilities

1. 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://www.flipkart.com/login
Parameter:	username

Recommended Solution:

Validate all input and encode output to prevent XSS attacks.

2. SQL Injection

Description:	SQL injection may be possible through user input fields.
Risk Level:	High
Confidence:	High
URL:	https://www.flipkart.com/login
Parameter:	password

Recommended Solution:

Use parameterized queries to prevent SQL injection.

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://www.flipkart.com/profile
Parameter:	form

Recommended Solution:

Implement CSRF protection tokens in all forms.

2. Information Disclosure - Sensitive Information in URL

Description:	The request appears to contain sensitive information leaked in the URL.
Risk Level:	Medium
Confidence:	High
URL:	https://www.flipkart.com/api/users
Parameter:	api_key

Recommended Solution:

Never pass sensitive data via URL parameters.

3. Directory Browsing

Description:	It is possible to view a listing of the directory contents.
Risk Level:	Medium
Confidence:	High
URL:	https://www.flipkart.com/assets/
Parameter:	

Recommended Solution:

Disable directory browsing on the web server.

4. X-Frame-Options Header Not Set

Description:	X-Frame-Options header is not included in the HTTP response to protect against clickjacki
Risk Level:	Medium
Confidence:	Medium
URL:	https://www.flipkart.com/dashboard
Parameter:	

Recommended Solution:

Set X-Frame-Options header to DENY or SAMEORIGIN.

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://www.flipkart.com/assets/css/style.css
Parameter:	

Recommended Solution:

Set X-Content-Type-Options header to nosniff.

2. Server Leaks Information via X-Powered-By HTTP Response Header

Description:	The web/application server is leaking information via one or more X-Powered-By HTTP res
Risk Level:	Low
Confidence:	High
URL:	https://www.flipkart.com/
Parameter:	

Recommended Solution:

Remove or customize the X-Powered-By header.

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 Server Leaks Information via X-Powered-By HTTP Response Header vulnerability according to security best practices
• Address the identified X-Frame-Options Header Not Set vulnerability according to security best practices
• Address the identified Missing Anti-CSRF Tokens vulnerability according to security best practices
• Implement proper input validation and output encoding
• Address the identified Directory Browsing vulnerability according to security best practices
• Remove sensitive information from error messages and headers
• Use parameterized queries and stored procedures
• Address the identified Content Type Options Not Set vulnerability according to security best practices