XSCAN Security Report

Official Security Assessment for https://www.flipkart.com

Executive Summary

Severity	Findings Count
Critical	0
High	1
Medium	0
Low	4

Scan Metadata

Item	Detail
Scan ID	XSC-37
Target URL	https://www.flipkart.com
Lead Researcher	Ragnar
Generated On	2026-02-02 12:33:15
Scan Protocol	DEEP

Detailed Findings

1. Missing HSTS Header

HIGH

Description	HSTS header is missing. This may allow SSL stripping attacks.
Mitigation	Enable Strict-Transport-Security header.

2. Missing X-Frame-Options

LOW

Description	X-Frame-Options header is missing. Clickjacking possible.
Mitigation	Add X-Frame-Options SAMEORIGIN or DENY.

3. Robots.txt Found

LOW

Description	Robots.txt file found at https://www.flipkart.com/robots.txt. Check for sensitive paths.
Mitigation	Ensure no sensitive administrative paths are disclosed.

4. Server Header Disclosure

LOW

Description	Server header reveals: nginx
Mitigation	Configure server to suppress detailed version information.

5. Missing X-Content-Type-Options

LOW

Description	X-Content-Type-Options header is missing (nosniff).
Mitigation	Set X-Content-Type-Options to 'nosniff'.