Vulnerability Assessment Report: flipkart.com

SECURITY SCORE: 80/100

OVERALL RISK LEVEL: MEDIUM

1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http		open
443	https		open

2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP: 163.53.76.86
+ Target Hostname: flipkart.com
+ Target Port: 80
+ Start Time: 2026-02-13 17:31:10 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://flipkart.com:443/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /cfappman/index.cfm - Redirects (301) to https://flipkart.com:443/cfappman/index.cfm
, susceptible to ODBC/pipe-style exploit; see RFP9901
http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /cfdocs/examples/cvbeans/beaninfo.cfm - Redirects (301) to
https://flipkart.com:443/cfdocs/examples/cvbeans/beaninfo.cfm , susceptible to our ODBC
exploit; see RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /cfdocs/examples/parks/detail.cfm - Redirects (301) to
https://flipkart.com:443/cfdocs/examples/parks/detail.cfm , susceptible to our ODBC
exploit; see RFP9901 http://www.wiretrip.net/rfp/p/doc.asp/i2/d3.htm
+ /kboard/ - Redirects (301) to https://flipkart.com:443/kboard/ , KBoard Forum 0.3.0
and prior have a security problem in forum_edit_post.php, forum_post.php and
forum_reply.php
+ /lists/admin/ - Redirects (301) to https://flipkart.com:443/lists/admin/ , PHPList
pre 2.6.4 contains a number of vulnerabilities including remote administrative access,
harvesting user info and more. Default login to admin interface is admin/phplist
+ /splashAdmin.php - Redirects (301) to https://flipkart.com:443/splashAdmin.php ,
Cobalt Qube 3 admin is running. This may have multiple security problems as described by
www.scan-associates.net. These could not be tested remotely.
+ /ssdefs/ - Redirects (301) to https://flipkart.com:443/ssdefs/ , Siteseed pre 1.4.2
has 'major' security problems.
+ /sshome/ - Redirects (301) to https://flipkart.com:443/sshome/ , Siteseed pre 1.4.2
has 'major' security problems.
+ /tiki/ - Redirects (301) to https://flipkart.com:443/tiki/ , Tiki 1.7.2 and previous
allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could
be admin/admin
+ /tiki/tiki-install.php - Redirects (301) to
https://flipkart.com:443/tiki/tiki-install.php , Tiki 1.7.2 and previous allowed
restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be
admin/admin
+ /scripts/samples/details.idc - Redirects (301) to
https://flipkart.com:443/scripts/samples/details.idc , See RFP 9901; www.wiretrip.net
+ /includes/conexion.inc - Redirects (301) to
```

```
https://flipkart.com:443/includes/conexion.inc , Database connection file found.
+ /.svn/entries - Redirects (301) to https://flipkart.com:443/.svn/entries , Subversion
Entries file may contain directory listing information.
+ /.svn/wc.db - Redirects (301) to https://flipkart.com:443/.svn/wc.db , Subversion
SQLite DB file may contain directory listing information.
+ /.git/index - Redirects (301) to https://flipkart.com:443/.git/index , Git Index file
may contain directory listing information.
+ /.hg/dirstate - Redirects (301) to https://flipkart.com:443/.hg/dirstate , Mercurial
DirState file may contain directory listing information.
+ 26 items checked: 8 error(s) and 1 item(s) reported on remote host
+ End Time: 2026-02-13 17:33:54 (GMT0) (164 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Crawled Website Endpoints

- https://www.flipkart.com/communication-preferences/push?t=all
- https://www.flipkart.com/flipkart-minutes-store?marketplace=HYPERLOCAL
- https://www.flipkart.com/wishlist?link=home_wishlist
- https://www.flipkart.com/helpcentre
- https://www.flipkart.com/plus
- https://www.flipkart.com/account/login?ret=/
- [FORM] https://www.flipkart.com/search
- https://www.flipkart.com/grocery-supermart-store?marketplace=GROCERY
- https://www.flipkart.com/the-gift-card-store?link=home_giftcard
- https://www.flipkart.com/searchsuggestion
- https://www.flipkart.com/account/login?signup=true&ret;=/
- https://www.flipkart.com/account/?rd=0&link;=home_account
- https://www.flipkart.com/account/rewards?link=home_rewards
- https://www.flipkart.com/travel/flights
- https://www.flipkart.com/account/orders?link=home_orders
- https://www.flipkart.com/

4. Vulnerabilities Detected

- Missing Security Headers
- Information Disclosure

5. Vulnerability Intelligence (CVE Mapping)

Legacy Vulnerability Intelligence
- ■■ NOTICE: Our engine identified 10 additional legacy vulnerabilities (pre-2016).

6. Attack Possibilities & Mitigation

Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.

Attack: Data Leaks / Reconnaissance

Mitigation: Restrict access to sensitive directories (like .git or /admin) and disable directory listing.