Sri Lanka Institute of Information Technology

Web Security – IE2062

Topic: Bug Bounty Report 9

Y2S2.WE.CS

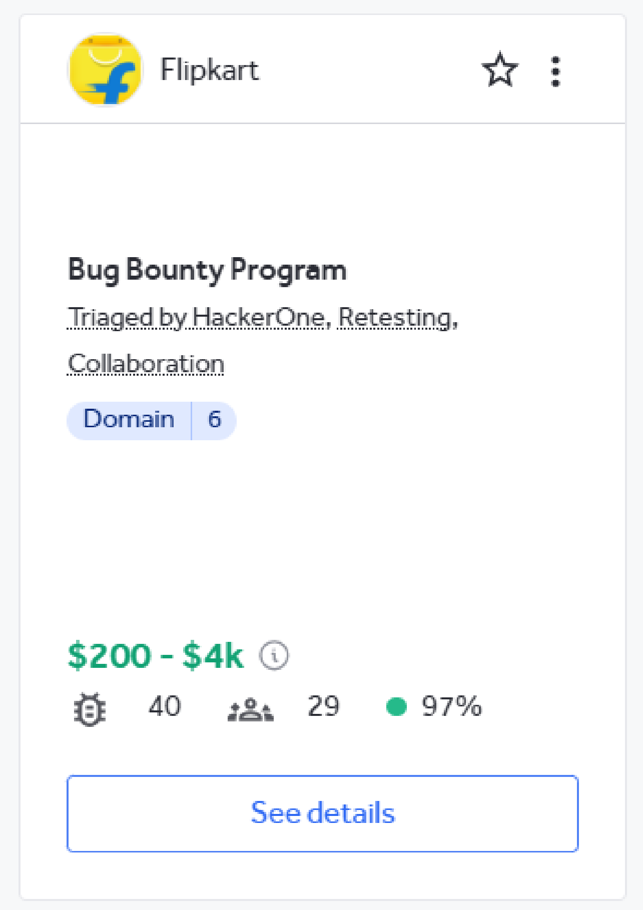
Name: S.D.W.Gunaratne

(IT23241978)

Table of Content

How I started?

1. Once I search from Hacker one, I saw a Flipkart bug bounty program.



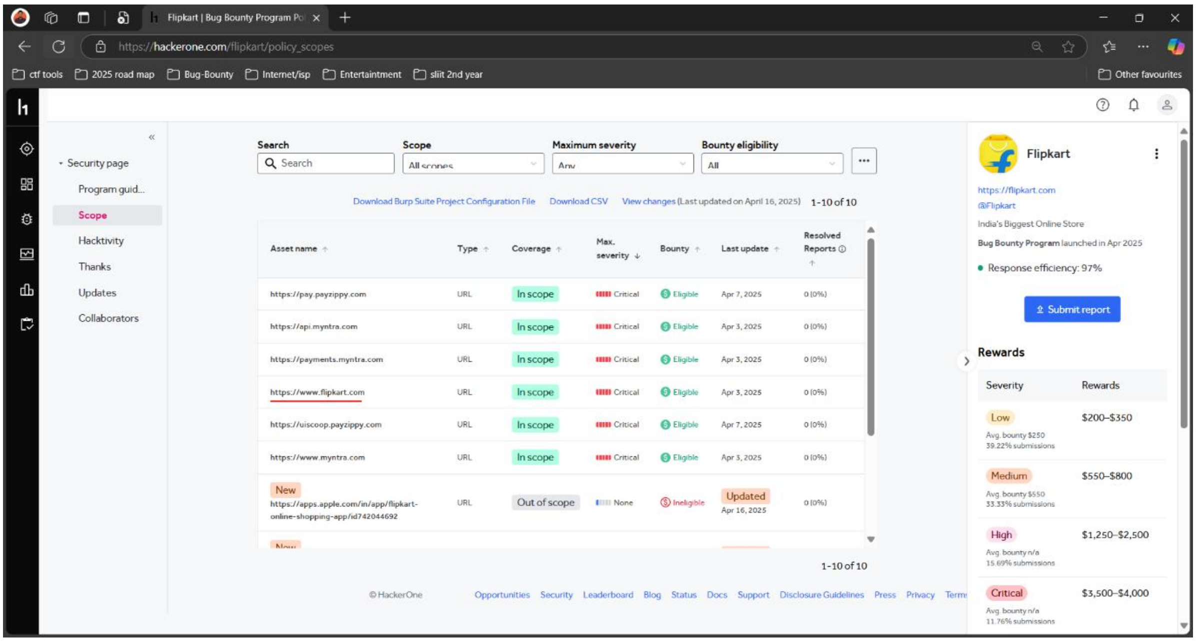
Flipkart

Bug Bounty Program

Triaged by HackerOne, Retesting, Collaboration

$200 - $4k

2. Then, I discovered full main domain allowed for scope, so that I choose https://flipkart.com .



Search: Search
Scope: All scopes
Maximum severity: Any
Bounty eligibility: All

Download Burp Suite Project Configuration File   Download CSV   View changes (Last updated on April 16, 2025)   1-10 of 10

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
https://pay.payzippy.com	URL	In scope	Critical	Eligible	Apr 7, 2025	0 (0%)
https://api.myntra.com	URL	In scope	Critical	Eligible	Apr 3, 2025	0 (0%)
https://payments.myntra.com	URL	In scope	Critical	Eligible	Apr 3, 2025	0 (0%)
https://www.flipkart.com	URL	In scope	Critical	Eligible	Apr 3, 2025	0 (0%)
https://uiscoop.payzippy.com	URL	In scope	Critical	Eligible	Apr 7, 2025	0 (0%)
https://www.myntra.com	URL	In scope	Critical	Eligible	Apr 3, 2025	0 (0%)
New https://apps.apple.com/in/app/flipkart-online-shopping-app/id742044692	URL	Out of scope	None	Ineligible	Updated Apr 16, 2025	0 (0%)

1-10 of 10

Flipkart

https://flipkart.com
@Flipkart
India's Biggest Online Store
Bug Bounty Program launched in Apr 2025

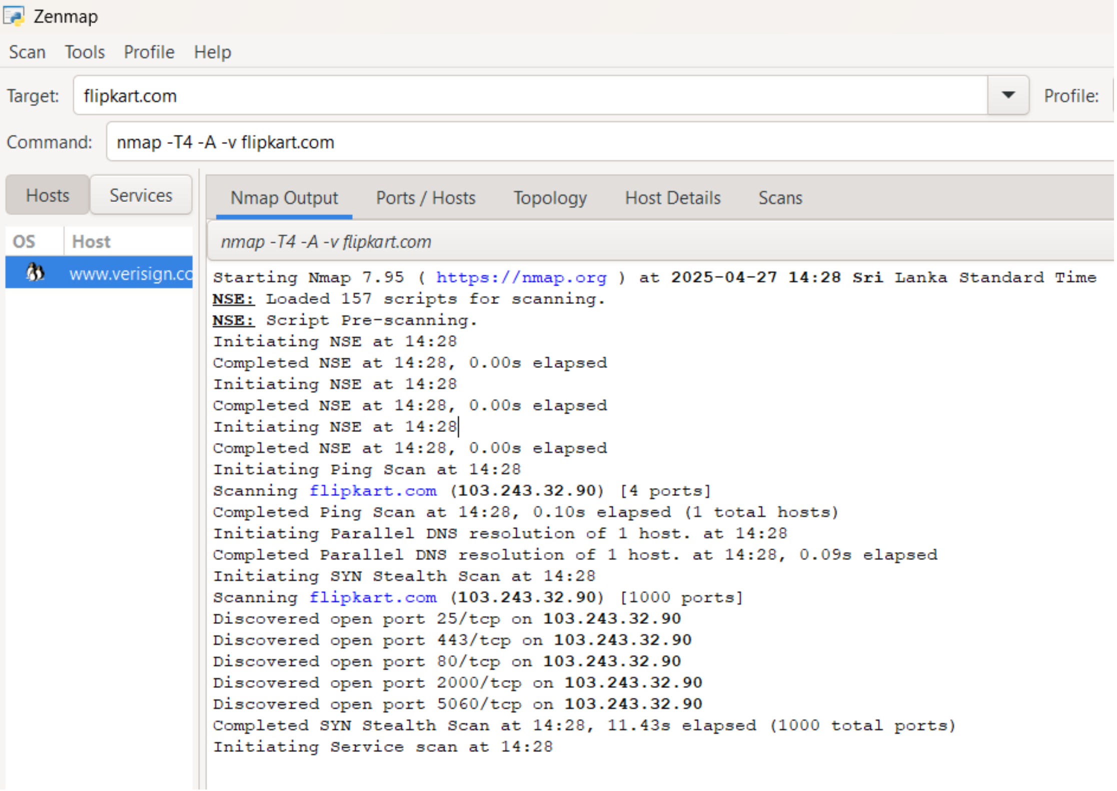
- Response efficiency: 97%

Rewards

Severity	Rewards
Low Avg. bounty $250 39.22% submissions	$200–$350
Medium Avg. bounty $550 33.33% submissions	$550–$800
High Avg. bounty n/a 15.69% submissions	$1,250–$2,500
Critical Avg. bounty n/a 11.76% submissions	$3,500–$4,000

3. I use several methods/tools to do penetration testing.

4. First, I used Nmap. It helps me to find what are the open ports, Identify the web technologies such as webservers.

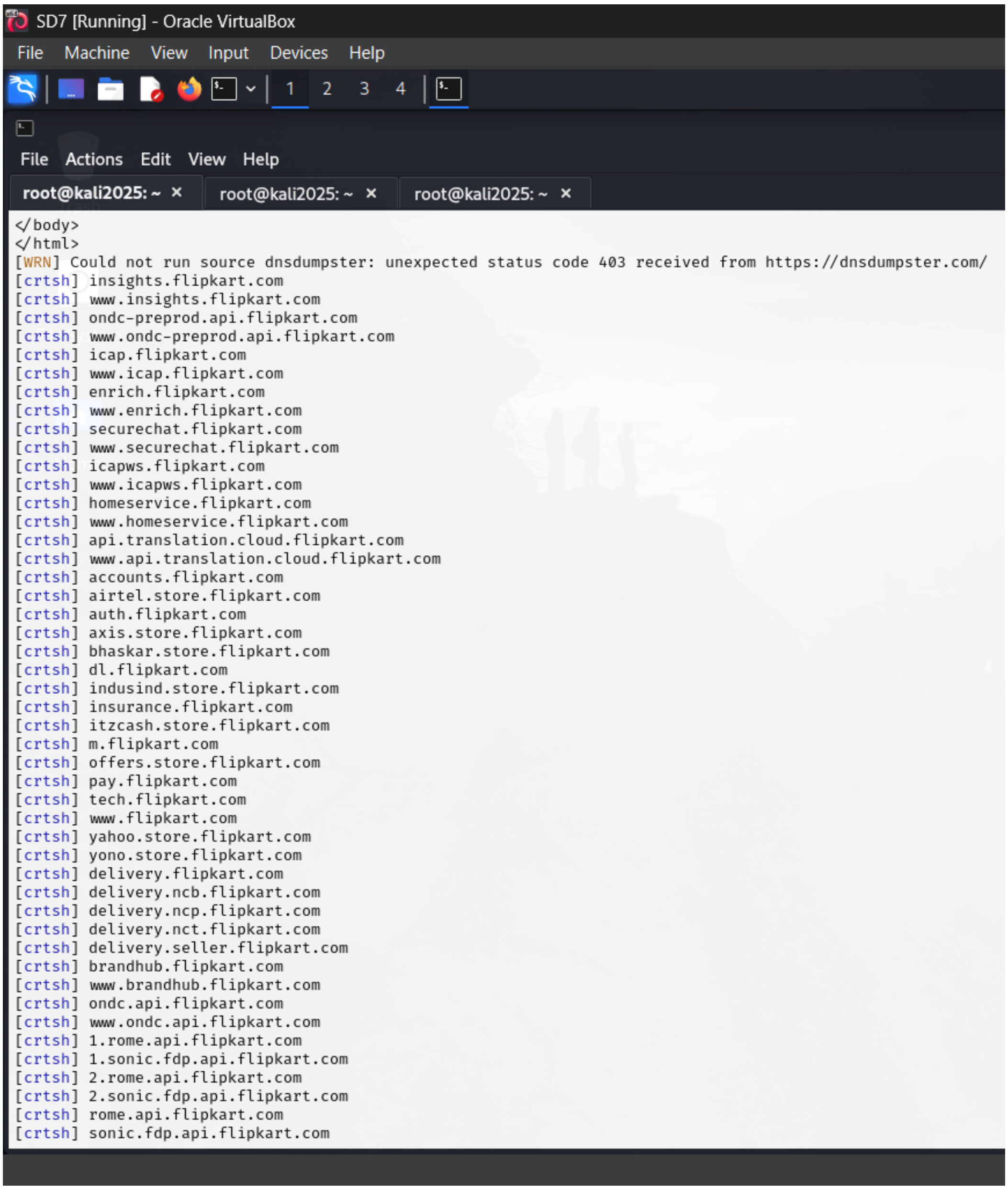


Target: flipkart.com

Command: nmap -T4 -A -v flipkart.com

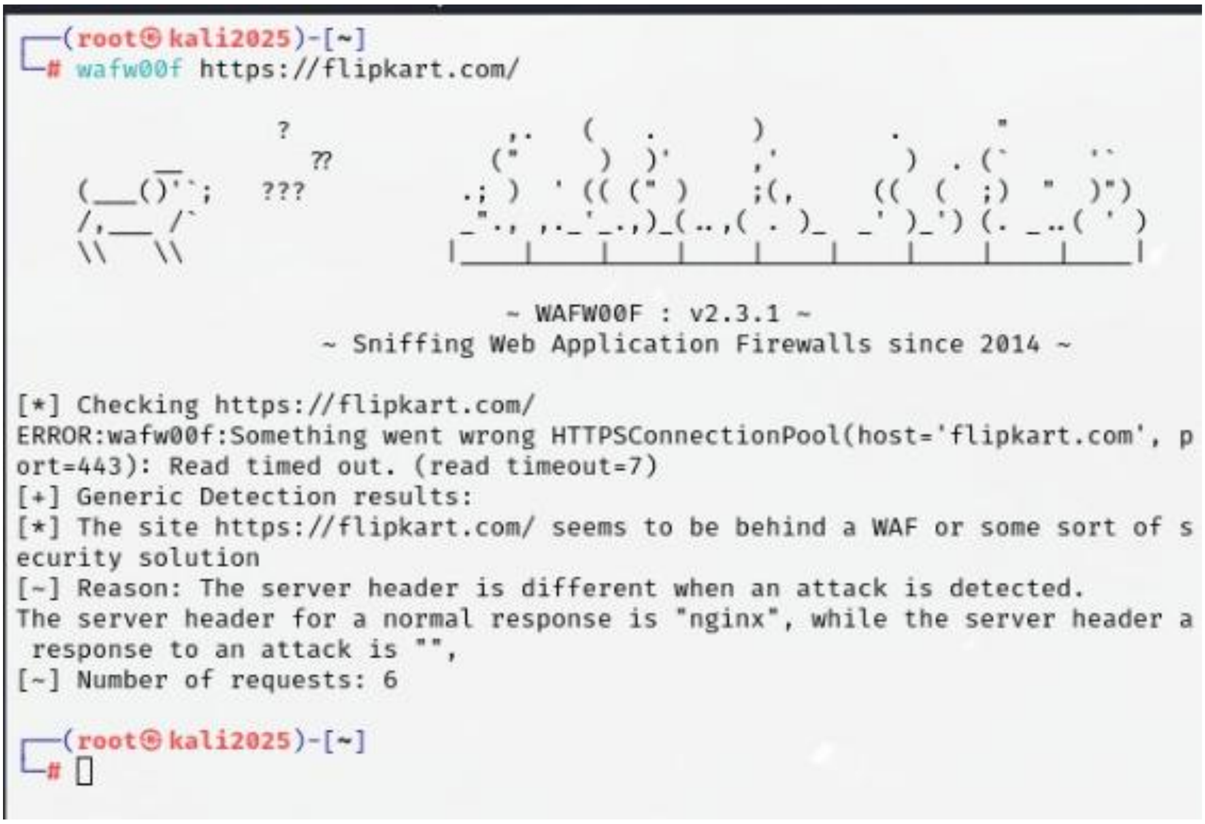
```
nmap -T4 -A -v flipkart.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 14:28 Sri Lanka Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 0.00s elapsed
Initiating Ping Scan at 14:28
Scanning flipkart.com (103.243.32.90) [4 ports]
Completed Ping Scan at 14:28, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:28
Completed Parallel DNS resolution of 1 host. at 14:28, 0.09s elapsed
Initiating SYN Stealth Scan at 14:28
Scanning flipkart.com (103.243.32.90) [1000 ports]
Discovered open port 25/tcp on 103.243.32.90
Discovered open port 443/tcp on 103.243.32.90
Discovered open port 80/tcp on 103.243.32.90
Discovered open port 2000/tcp on 103.243.32.90
Discovered open port 5060/tcp on 103.243.32.90
Completed SYN Stealth Scan at 14:28, 11.43s elapsed (1000 total ports)
Initiating Service scan at 14:28
```

5. Secondly, I used Subfider tool to find hidden or forgotten web asserts. Because hidden web assert can have poor security, unpatched vulnerabilities.


SD7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
root@kali2025: ~
root@kali2025: ~
root@kali2025: ~

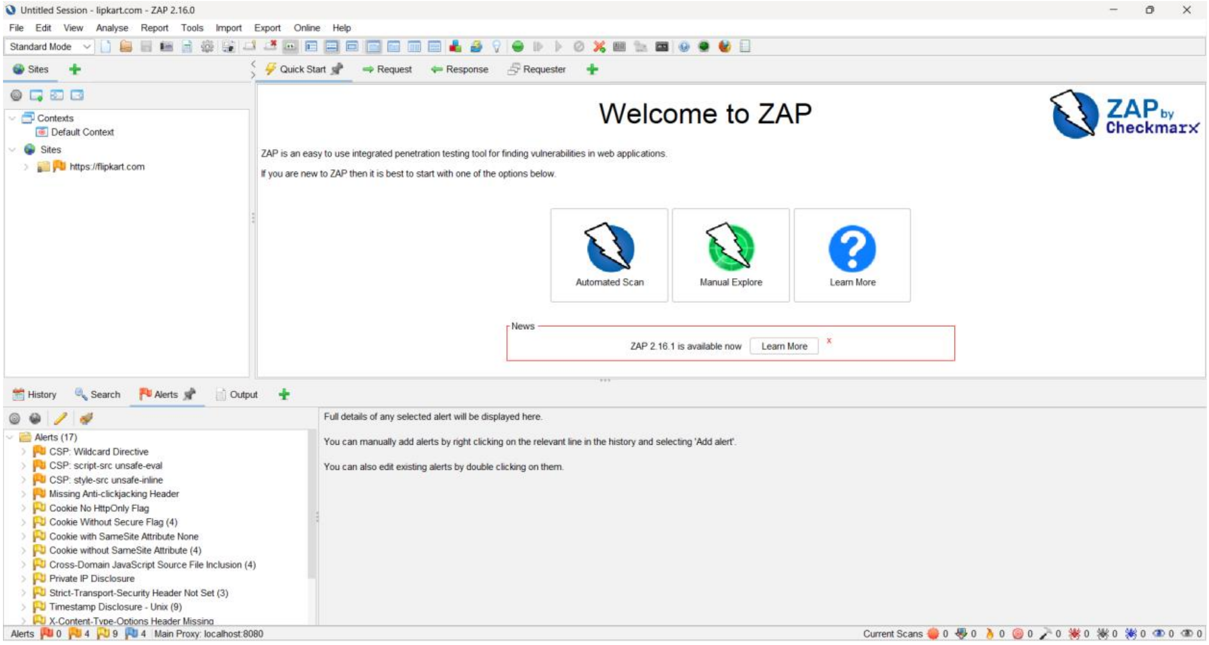
```
</body>
</html>
[WRN] Could not run source dnsdumpster: unexpected status code 403 received from https://dnsdumpster.com/
[crtsh] insights.flipkart.com
[crtsh] www.insights.flipkart.com
[crtsh] ondc-preprod.api.flipkart.com
[crtsh] www.ondc-preprod.api.flipkart.com
[crtsh] icap.flipkart.com
[crtsh] www.icap.flipkart.com
[crtsh] enrich.flipkart.com
[crtsh] www.enrich.flipkart.com
[crtsh] securechat.flipkart.com
[crtsh] www.securechat.flipkart.com
[crtsh] icapws.flipkart.com
[crtsh] www.icapws.flipkart.com
[crtsh] homeservice.flipkart.com
[crtsh] www.homeservice.flipkart.com
[crtsh] api.translation.cloud.flipkart.com
[crtsh] www.api.translation.cloud.flipkart.com
[crtsh] accounts.flipkart.com
[crtsh] airtel.store.flipkart.com
[crtsh] auth.flipkart.com
[crtsh] axis.store.flipkart.com
[crtsh] bhaskar.store.flipkart.com
[crtsh] dl.flipkart.com
[crtsh] indusind.store.flipkart.com
[crtsh] insurance.flipkart.com
[crtsh] itzcash.store.flipkart.com
[crtsh] m.flipkart.com
[crtsh] offers.store.flipkart.com
[crtsh] pay.flipkart.com
[crtsh] tech.flipkart.com
[crtsh] www.flipkart.com
[crtsh] yahoo.store.flipkart.com
[crtsh] yono.store.flipkart.com
[crtsh] delivery.flipkart.com
[crtsh] delivery.ncb.flipkart.com
[crtsh] delivery.ncp.flipkart.com
[crtsh] delivery.nct.flipkart.com
[crtsh] delivery.seller.flipkart.com
[crtsh] brandhub.flipkart.com
[crtsh] www.brandhub.flipkart.com
[crtsh] ondc.api.flipkart.com
[crtsh] www.ondc.api.flipkart.com
[crtsh] 1.rome.api.flipkart.com
[crtsh] 1.sonic.fdp.api.flipkart.com
[crtsh] 2.rome.api.flipkart.com
[crtsh] 2.sonic.fdp.api.flipkart.com
[crtsh] rome.api.flipkart.com
[crtsh] sonic.fdp.api.flipkart.com
```

6. Thirdly, I used Wafwoof tool to find website is protected by a WAF (web application firewall). Because if WAF is active, so pen testers do their test without blocked, and they can do their testing with bypass WAF.



```
┌──(root㉿kali2025)-[~]
└─# wafw00f https://flipkart.com/

                ?              ,.   (   .      )        .      "
                  ??          ("     )  )'     ,'        )  . ("      ,.
   (___()'`;    ???         .; )  ' (( (" )    ;(,     ((  (  ;)  "  )")
   /,___ /`                 _".,  ,._'_.,)_(..,( . )_  _' )_') (. _..( ' )
   \\    \\                 |____|____|____|____|____|____|____|____|____|

                          ~ WAFW00F : v2.3.1 ~
              ~ Sniffing Web Application Firewalls since 2014 ~

[*] Checking https://flipkart.com/
ERROR:wafw00f:Something went wrong HTTPSConnectionPool(host='flipkart.com', p
ort=443): Read timed out. (read timeout=7)
[+] Generic Detection results:
[*] The site https://flipkart.com/ seems to be behind a WAF or some sort of s
ecurity solution
[~] Reason: The server header is different when an attack is detected.
The server header for a normal response is "nginx", while the server header a
 response to an attack is "",
[~] Number of requests: 6

┌──(root㉿kali2025)-[~]
└─# 
```

7.Finaly, I use OWASP zap to automatically find the vulnerabilities.



Untitled Session - lipkart.com - ZAP 2.16.0

Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.16.1 is available now

Alerts (17)
- CSP: Wildcard Directive
- CSP: script-src unsafe-eval
- CSP: style-src unsafe-inline
- Missing Anti-clickjacking Header
- Cookie No HttpOnly Flag
- Cookie Without Secure Flag (4)
- Cookie with SameSite Attribute None
- Cookie without SameSite Attribute (4)
- Cross-Domain JavaScript Source File Inclusion (4)
- Private IP Disclosure
- Strict-Transport-Security Header Not Set (3)
- Timestamp Disclosure - Unix (9)
- X-Content-Type-Options Header Missing

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Alerts 0 4 9 4 Main Proxy: localhost:8080

Current Scans 0 0 0 0 0 0 0 0 0 0 0

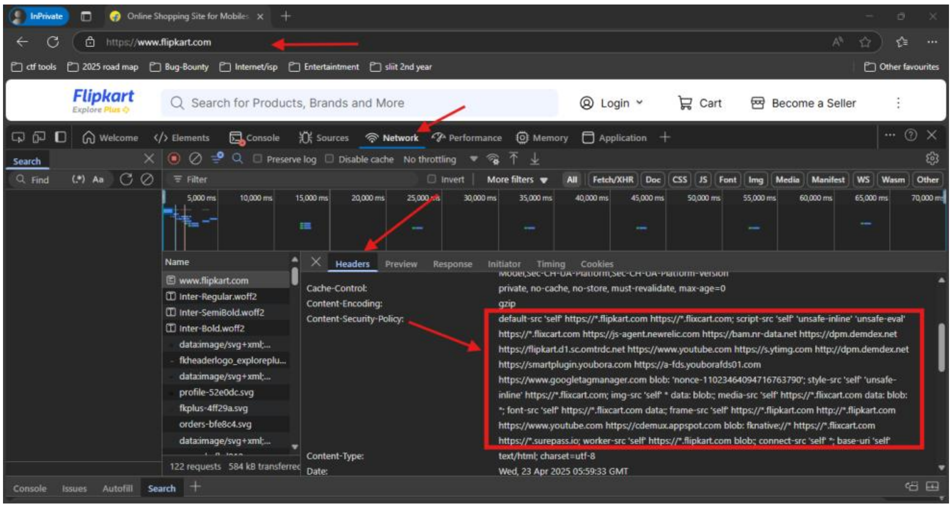
With getting these tool’s support, I found below details about vulnerability.

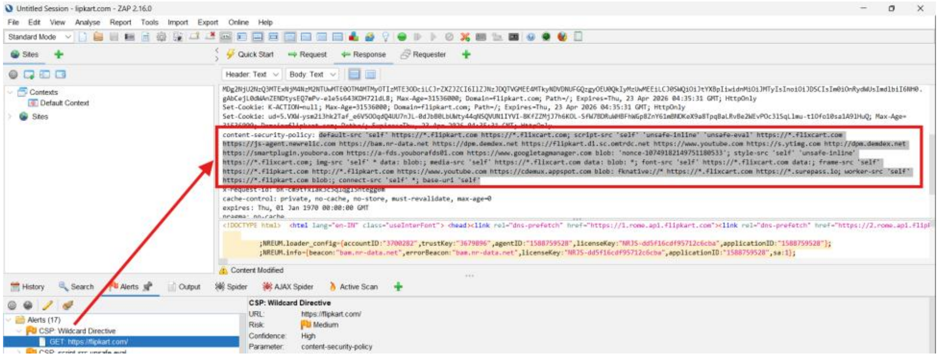
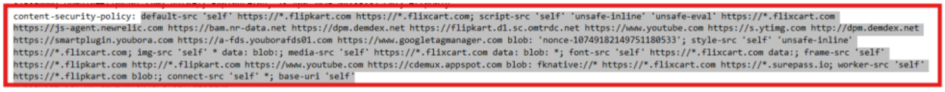
2) Introduction

1.1 Domain	https://flipkart.com/
1.2 Severity	• **Medium**

3) Vulnerability

3.1 Vulnerability title	CSP: Wildcard Directive CWE-693 OWASP_2021_A05
3.2 Vulnerability description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
3.3 Affected components	In this website we can see CSP header implemented, but it is misconfigured. There are some directives are missing or give more permissions. Full access • Media-src:allow * • Img-src: allow * • Connect-src: allow * Missing • Frame-ancestors: • Form-action: These impact how external media like scripts, media, and images handle are with, adding the risk of exploitation.

3.4 Impact assessment	When there is wildcard, we can see that give permission to any (*) script, image or media to load on our websites. So this is really bad because this is vulnerable to XXS (cross site scripting attack) Data leakage due to malicious 3rd party links. Without strict directives, attackers can inject malicious scripts or forward victims to phishing web sites, which can compromise critical data and trust.
3.5 Steps to reproduce	Below mention are the steps: 1. Go browser and search “ https://flipkart.com/ ” 2. Go to developer tools by using f12. 3. Then go to network tab and refresh it. 4. Then find the main page and go to header tab 5. Find the CSP header 6. Then check wildcard (*) and missing ones.  Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Content-Encoding: gzip Content-Security-Policy: default-src 'self' https://*.flipkart.com https://*.flixcart.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://*.flixcart.com https://js-agent.newrelic.com https://bam.nr-data.net https://dpm.demdex.net https://flipkart.d1.sc.omtrdc.net https://www.youtube.com https://s.ytimg.com http://dpm.demdex.net https://smartplugin.youbora.com https://a-fds.youborafds01.com https://www.googletagmanager.com blob: 'nonce-11023464094716763790'; style-src 'self' 'unsafe-inline' https://*.flixcart.com; img-src 'self' * data: blob:; media-src 'self' https://*.flixcart.com data: blob: *; font-src 'self' https://*.flixcart.com data:; frame-src 'self' https://*.flipkart.com http://*.flipkart.com https://www.youtube.com https://cdemux.appspot.com blob: fknative://* https://*.flixcart.com https://*.surepass.io; worker-src 'self' https://*.flipkart.com blob:; connect-src 'self' *; base-uri 'self' Content-Type: text/html; charset=utf-8 Date: Wed, 23 Apr 2025 05:59:33 GMT InPrivate Online Shopping Site for Mobile: https://www.flipkart.com ctf tools 2025 road map Bug-Bounty Internet/isp Entertainment sliit 2nd year Other favourites Flipkart Explore Plus Search for Products, Brands and More Login Cart Become a Seller Welcome Elements Console Sources Network Performance Memory Application Search Preserve log Disable cache No throttling Filter Invert More filters All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other Name www.flipkart.com Inter-Regular.woff2 Inter-SemiBold.woff2 Inter-Bold.woff2 fkheaderlogo_exploreplu... profile-52e0dc.svg fkplus-4ff29a.svg orders-bfe8c4.svg 122 requests 584 kB transferred Headers Preview Response Initiator Timing Cookies Console Issues Autofill Search

3.6 Proof of concept	 Untitled Session - lipkart.com - ZAP 2.16.0
	File Edit View Analyse Report Tools Import Export Online Help
	Standard Mode
	Sites
	Quick Start
	Request
	Response
	Requester
	Header: Text
	Body: Text
	Contexts
	Default Context
	Sites
	Content Modified
	History
	Search
	Alerts
	Output
	Spider
	AJAX Spider
	Active Scan
	Alerts (17)
	CSP: Wildcard Directive
	GET: https://flipkart.com/
	`MDg2NjU2NzQ3MTExNjM4NzM2NTUwMTE0OTM4MTMyOTIzMTE3ODciLCJrZXZJZCI6I1ZJNzJDQTVGMEE4MTkyNDVDNUFGQzgyOEU0QkIyMzUwMEEiLCJ0SWQiOiJtYXBpIiwidnMiOiJMTyIsInoiOiJDSCIsIm0iOnRydWUsImdlbiI6NH0.`
	`gAbCejL0dWAnZENDtysEQ7mPv-ele5s643KDH721dL8; Max-Age=31536000; Domain=flipkart.com; Path=/; Expires=Thu, 23 Apr 2026 04:35:31 GMT; HttpOnly`
	`Set-Cookie: K-ACTION=null; Max-Age=31536000; Domain=flipkart.com; Path=/; Expires=Thu, 23 Apr 2026 04:35:31 GMT; HttpOnly`
	`Set-Cookie: ud=5.VXW-ysm2i3hk2Taf_e6V5O0qdQ4UU7nJL-0dJbB0LbUWty44qNSQVUN1IYVI-8KfZ2Mj7h6KOL-SfW7BDRuWHBFhWGp8ZnY61mBNDKeX9a8TpqBaLRvBe2WEvPOc31SqLlmu-t10fo10sa1A91HuQ; Max-Age=`
	`content-security-policy: default-src 'self' https://*.flipkart.com https://*.flixcart.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://*.flixcart.com https://js-agent.newrelic.com https://bam.nr-data.net https://dpm.demdex.net https://flipkart.d1.sc.omtrdc.net https://www.youtube.com https://s.ytimg.com http://dpm.demdex.net https://smartplugin.youbora.com https://a-fds.youborafds01.com https://www.googletagmanager.com blob: 'nonce-10749182149751180533'; style-src 'self' 'unsafe-inline' https://*.flixcart.com; img-src 'self' * data: blob:; media-src 'self' https://*.flixcart.com data: blob: *; font-src 'self' https://*.flixcart.com data:; frame-src 'self' https://*.flipkart.com http://*.flipkart.com https://www.youtube.com https://cdemux.appspot.com blob: fknative://* https://*.flixcart.com https://*.surepass.io; worker-src 'self' https://*.flipkart.com blob:; connect-src 'self' *; base-uri 'self'`
	`cache-control: private, no-cache, no-store, must-revalidate, max-age=0`
	`expires: Thu, 01 Jan 1970 00:00:00 GMT`
	`<!DOCTYPE html> <html lang="en-IN" class="useInterFont"> <head><link rel="dns-prefetch" href="https://1.rome.api.flipkart.com"><link rel="dns-prefetch" href="https://2.rome.api.flipl`
	`;NREUM.loader_config={accountID:"3700282",trustKey:"3679896",agentID:"1588759528",licenseKey:"NRJS-dd5f16cdf95712c6cba",applicationID:"1588759528"};`
	`;NREUM.info={beacon:"bam.nr-data.net",errorBeacon:"bam.nr-data.net",licenseKey:"NRJS-dd5f16cdf95712c6cba",applicationID:"1588759528",sa:1};`
	CSP: Wildcard Directive
	URL: https://flipkart.com/
	Risk: Medium
	Confidence: High
	Parameter: content-security-policy
	CSP header respond
	
	`content-security-policy: default-src 'self' https://*.flipkart.com https://*.flixcart.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://*.flixcart.com https://js-agent.newrelic.com https://bam.nr-data.net https://dpm.demdex.net https://flipkart.d1.sc.omtrdc.net https://www.youtube.com https://s.ytimg.com http://dpm.demdex.net https://smartplugin.youbora.com https://a-fds.youborafds01.com https://www.googletagmanager.com blob: 'nonce-10749182149751180533'; style-src 'self' 'unsafe-inline' https://*.flixcart.com; img-src 'self' * data: blob:; media-src 'self' https://*.flixcart.com data: blob: *; font-src 'self' https://*.flixcart.com data:; frame-src 'self' https://*.flipkart.com http://*.flipkart.com https://www.youtube.com https://cdemux.appspot.com blob: fknative://* https://*.flixcart.com https://*.surepass.io; worker-src 'self' https://*.flipkart.com blob:; connect-src 'self' *; base-uri 'self'`

3.7 Proposed mitigation or fix	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header. Best solution for this is, without using wild card (*), we can specify the trusted sources and allow them only.