Websocket Endpoint Analysis Report

Insecure WebSocket Implementations: Crawling Public Sites, Testing Endpoints for Vulnerabilities, and Reporting Impact Analysis

Report Generated on : June 23, 2025

Report Generated By – Puskar Mishra and Tejas MH
Under the guidance of Sushma E (CEH)

WebSocket Security Scan Report

Executive Summary

Real-time apps increasingly rely on WebSocket connections, but insecure implementations—such as missing origin checks or weak authentication—can allow hijacking or sensitive data exposure.

To address this, we developed an automated scanner that crawls public web applications, detects vulnerable WebSocket endpoints, and analyzes their real-world impact.

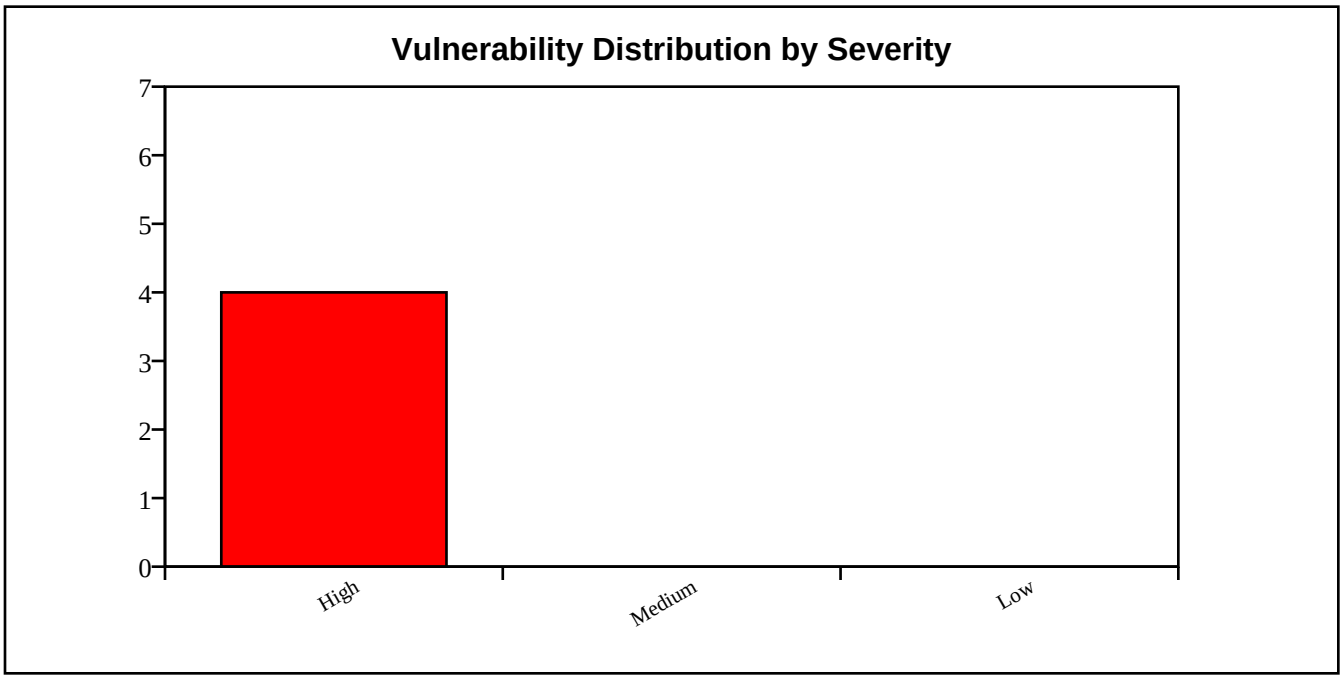
• Crawl and detect active WebSocket endpoints from public websites.
• Apply origin-header enforcement and protocol fuzzing tests to assess security gaps.
• Generate structured PDF reports summarizing detected vulnerabilities and severity.

Scan Start Time:	2025-06-23 20:53:10
Scan End Time:	2025-06-23 20:54:59
Total Scan Duration:	110.02 seconds
Total URLs Scanned:	1
High Severity Vulnerabilities:	4
Medium Severity Vulnerabilities:	0
Low Severity Vulnerabilities:	0

All Scanned Websites

This section lists all scanned websites and summarizes the overall vulnerability distribution by severity. The bar graph below visualizes the number of High, Medium, and Low severity vulnerabilities identified across all scanned sites.

#	Website
1	https://postman.com

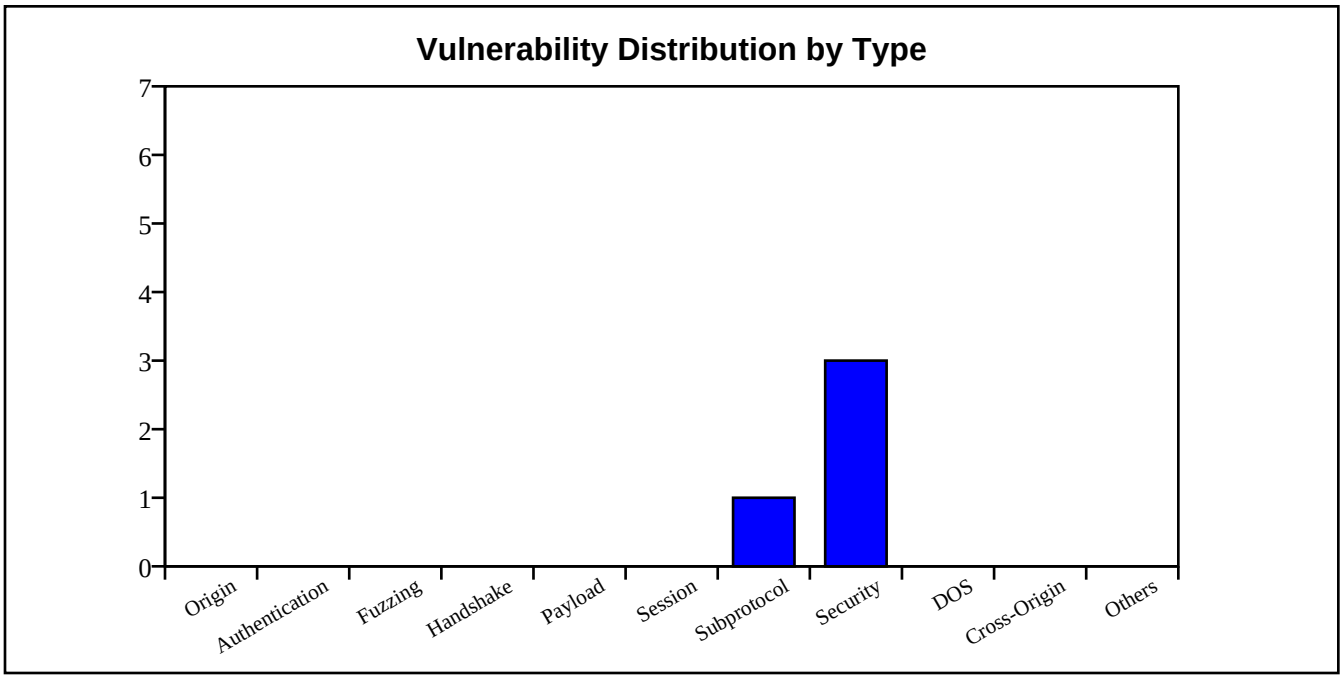


Vulnerability Summary by Type

This section summarizes key categories of vulnerabilities found during the scan. It groups issues like missing origin checks, weak authentication, insecure handshakes, and over 80 other attack for test to highlight common WebSocket flaws.

The bar chart below visualizes how many vulnerabilities were found in each category. This helps quickly identify the most common and critical problem areas across scanned applications.

Type	Count
Origin	0
Authentication	0
Fuzzing	0
Handshake	0
Payload	0
Session	0
Subprotocol	1
Security	3
DOS	0
Cross-Origin	0
Others	0


Vulnerability Distribution by Type
7
6
5
4
3
2
1
0
Origin
Authentication
Fuzzing
Handshake
Payload
Session
Subprotocol
Security
DOS
Cross-Origin
Others

Detailed Scan Results

This section provides an in-depth breakdown of each scanned target. For every URL, it lists the scan duration, number of URLs crawled during reconnaissance, and the WebSocket endpoints discovered. It helps identify how many potential communication channels were exposed for testing. Each target's vulnerability distribution is summarized by severity (High, Medium, Low) using a bar chart, followed by a detailed list of detected vulnerabilities. The section also documents the types of attacks performed and the exact WebSocket endpoints and internal URLs involved in the scan. This allows for a thorough understanding of the security posture and exposure of each target.

Target URL: https://postman.com

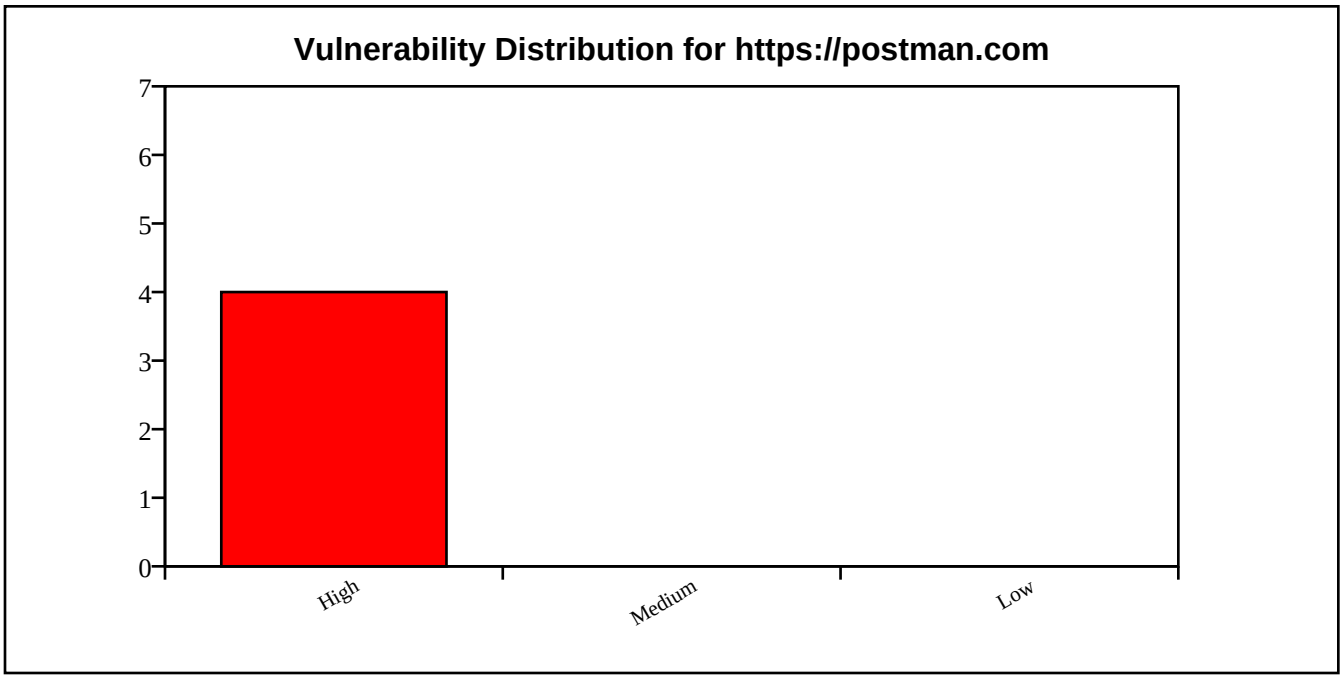
Scan Duration:	100.41 seconds
URLs Crawled:	100
WebSocket Endpoints Found:	1
Attack Performed:	True
Attack Type:	WebSocket Tests
High Severity Findings:	4
Medium Severity Findings:	0
Low Severity Findings:	0

WebSocket Endpoints:

#	URL
1	wss://ws2.qualified.com/cable?wv=9&token; =hhaW6HiVqGA5oJq1&vu;=c9d88a7e-c66c-47be- aa71-9d55967fad7f&wu;=904f04e4-f8e4-4165- 97f4-029fa2406d93&ca;=2025-06- 23T15%3A23%3A17.660Z&tz;=America%2FNew_Yo rk&bis;=5&referrer;=&pv;=1&fv;=2025-06-23- 416da42508&iml;=false&bl;=en-US■=true

Crawled URLs:

#	URL
1	https://voyager.postman.com/logo/externa l/travisci-logo.png
2	https://www.postman.com/product/tools
3	https://www.postman.com/product/integrat ions
4	https://voyager.postman.com/logo/externa l/dropbox-logo.svg
5	https://voyager.postman.com/logo/externa l/microsoft-logo-horizontal.svg


Vulnerability Distribution for https://postman.com
7
6
5
4
3
2
1
0
High
Medium
Low

Detected Vulnerabilities:

This section lists all vulnerabilities identified during the scan of the target. Each entry includes the vulnerability name, its severity (High, Medium, or Low), a description of the issue, recommended solutions, and the affected WebSocket URL or host. This detailed information helps prioritize fixes and understand the exact flaws present in the WebSocket implementation of each target.

Affected WebSocket Endpoint: wss://ws2.qualified.com/cable?wv=9&token;=hhaW6HiVqGA5oJq1&vu;=c9d88a7e-c66c-47be-aa71-9d55967fad7f&wu;=904f04e4-f8e4-4165-97f4-029fa2406d93&ca;=2025-06-23T15%3A23%3A17.660Z&tz;=America%2FNew_York&bis;=5&referrer;=&pv;=1&fv;=2025-06-23-416da42508&iml;=false&bl;=en-US■=true

Name:	Fake Extension
Risk Level:	High
Description:	Server at ws2.qualified.com:443 accepted spoofed extension.
Solution:	Validate Sec-WebSocket-Extensions header against supported values.

Name:	Spoofed Connection Header
Risk Level:	High
Description:	Server at ws2.qualified.com:443 accepted spoofed Connection header.
Solution:	Strictly validate Connection header to be exactly "Upgrade".

Name:	HTTP/1.0 Downgrade
Risk Level:	High
Description:	Server at ws2.qualified.com:443 accepted HTTP/1.0 WebSocket handshake.
Solution:	Only allow WebSocket upgrades over HTTP/1.1 or newer.

Name:	Insecure Cipher
Risk Level:	High
Description:	WebSocket at wss://ws2.qualified.com/cable?wv=9&to;ken=hhaW6HiVqGA5oJq1&vu;=c9d88a7e-c66c-47be-aa71-9d55967fad7f&wu;=904f04e4-f8e4-4165-97f4-029fa2406d93&ca;=2025-06-23T15%3A23%3A17.660Z&tz;=America%2FNew_York&bis;=5&r;eferrer=&pv;=1&fv;=2025-06-23-416da42508&iml;=false&bl;=en-US■=true accepts insecure TLS cipher: NULL-MD5.
Solution:	Disable weak ciphers like RC4, NULL, EXPORT, and DES-CBC-SHA. Use modern TLS ciphers only.