Websocket Endpoint Analysis Report

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

Report Generated on : June 24, 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.

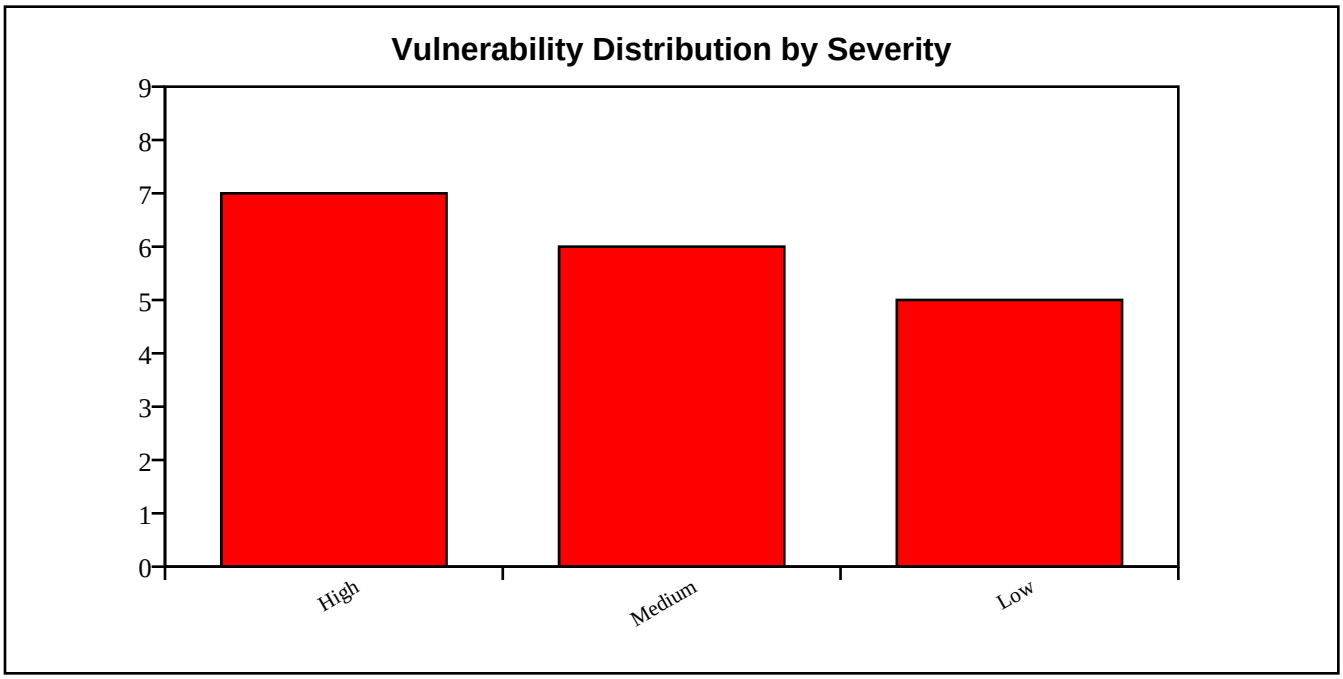
• Crawl and detect active WebSocket endpoints from public websites.
• Apply origin-header enforcement and protocol fuzzing tests to assess security gaps.
• Generate structured PDF reports summarizing detected vulnerabilities and severity.

Scan Start Time:	2025-06-24 09:35:16
Scan End Time:	2025-06-24 09:37:45
Total Scan Duration:	150.3 seconds
Total URLs Scanned:	1
High Severity Vulnerabilities:	7
Medium Severity Vulnerabilities:	6
Low Severity Vulnerabilities:	5

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://publicnode.com

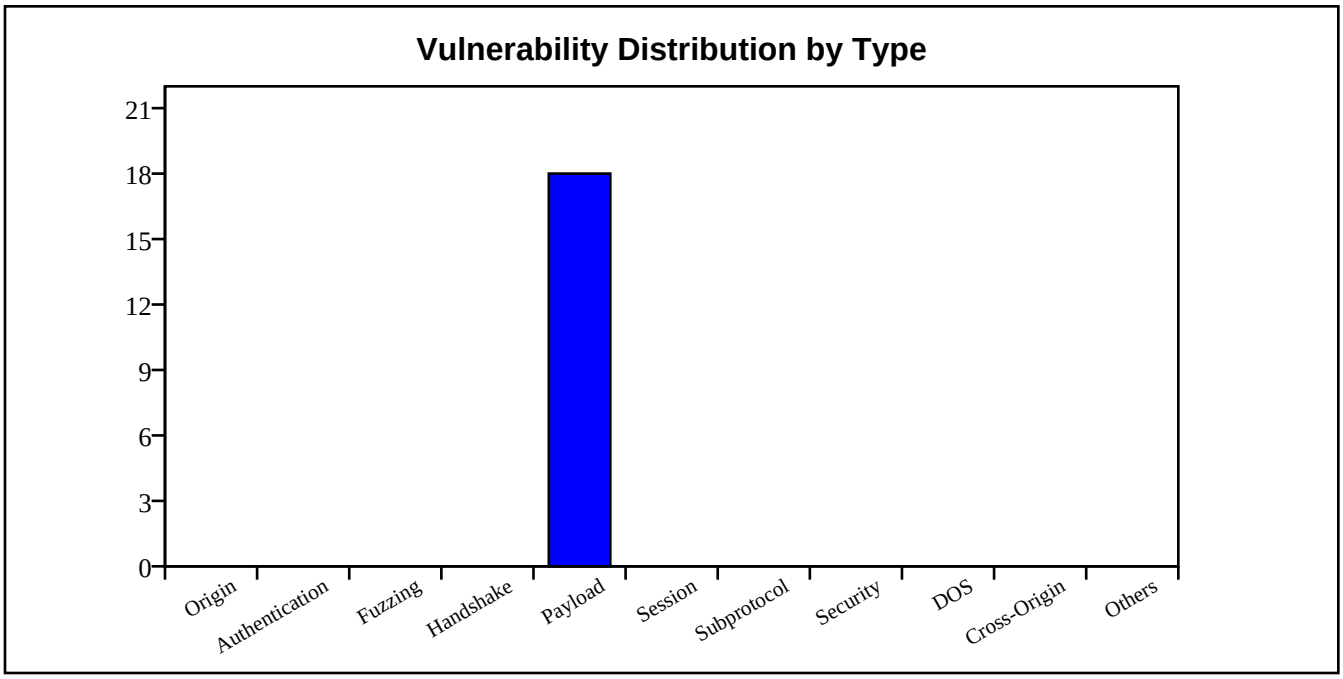


Vulnerability Summary by Type

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	18
Session	0
Subprotocol	0
Security	0
DOS	0
Cross-Origin	0
Others	0


Vulnerability Distribution by Type
21
18
15
12
9
6
3
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://publicnode.com

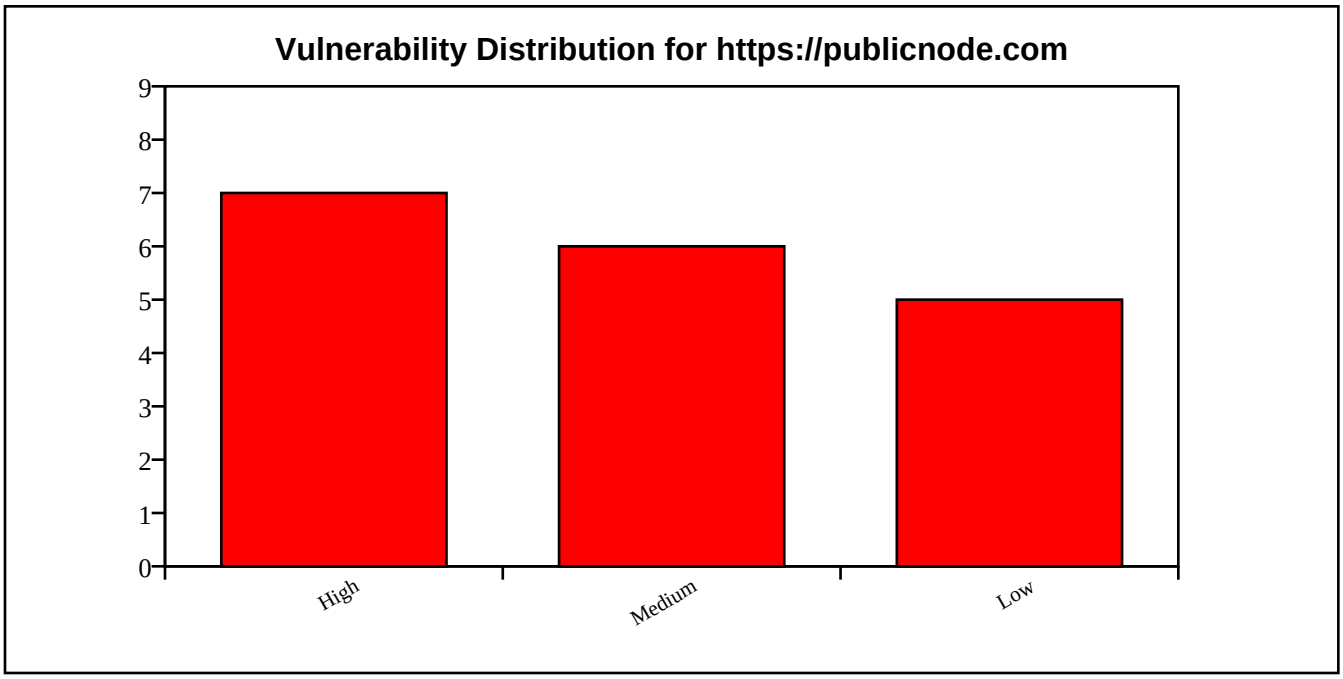
Scan Duration:	134.86 seconds
URLs Crawled:	100
WebSocket Endpoints Found:	1
Attack Performed:	True
Attack Type:	WebSocket Tests
High Severity Findings:	7
Medium Severity Findings:	6
Low Severity Findings:	5

WebSocket Endpoints:

#	URL
1	wss://evmos-testnet- rpc.publicnode.com:443/websocket

Crawled URLs:

#	URL
1	https://pivx-rpc.publicnode.com
2	https://www.publicnode.com/_next/static/ chunks/webpack-d17ebe0ea3c9d6aa.js
3	https://injective.publicnode.com
4	https://tron.publicnode.com
5	https://migaloo-rest.publicnode.com


Vulnerability Distribution for https://publicnode.com
9
8
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://evmos-testnet-rpc.publicnode.com:443/websocket

Name:	Undefined Opcode
Risk Level:	High
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted frame with undefined opcode 0x3.
Solution:	Reject frames with undefined opcodes.

Name:	Reserved Opcode
Risk Level:	High
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted frame with reserved opcode 0xB.
Solution:	Reject frames with reserved opcodes (0x3-0x7, 0xB-0xF).

Name:	Zero-Length Fragment
Risk Level:	Low
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted zero- length fragments and responded unexpectedly.
Solution:	Reject or limit incomplete fragmented messages.

Name:	Invalid Payload Length
Risk Level:	High
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted frame with declared payload length 10 but sent only 4 bytes.
Solution:	Validate payload length matches actual data.

Name:	Negative Payload Length
Risk Level:	High
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted forged extended payload length (0x8000000000000001).

Solution:	Validate payload length fields and reject extreme or invalid values.

Name:	Mismatched Payload
Risk Level:	Medium
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted frames with mismatched lengths.
Solution:	Ensure payload lengths match.

Name:	Invalid Masking Key
Risk Level:	High
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted a frame with invalid masking key pattern: All-zero.
Solution:	Enforce strict validation of client masking keys per RFC 6455.

Name:	Unmasked Client Frame
Risk Level:	High

Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted an unmasked client frame.
Solution:	Require masking for all client-to-server frames per RFC 6455.

Name:	Invalid RSV Bits
Risk Level:	Medium
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted a frame with invalid RSV1 bit set.
Solution:	Reject non-zero RSV bits unless explicitly negotiated via extension.

Name:	Oversized Control Frame
Risk Level:	Medium
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted a ping control frame with 126-byte payload.
Solution:	Reject control frames larger than 125 bytes as per RFC 6455.

Name:	Non-UTF-8 Text

Risk Level:	High
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted a text frame with invalid UTF-8 bytes.
Solution:	Ensure strict UTF-8 validation of text frames.

Name:	Null Bytes in Text
Risk Level:	Medium
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted a text frame containing null bytes.
Solution:	Validate and sanitize text frames for embedded nulls. Avoid C-style string truncation risks.

Name:	Binary as Text
Risk Level:	Low
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted a text frame with non-UTF-8 binary data.
Solution:	Validate UTF-8 compliance in all text frames as per RFC 6455.

Name:	Text as Binary
Risk Level:	Low
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted UTF-8 text sent in a binary frame.
Solution:	Handle binary and text frames with separate logic as per RFC 6455.

Name:	Invalid Close Code
Risk Level:	Medium
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted a close frame with invalid code 999.
Solution:	Close codes must conform to RFC 6455 (valid: 1000–1015, 3000–4999).

Name:	Early Close Frame
Risk Level:	Low
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted an early close frame before any data was exchanged.

Solution:	Gracefully handle close frames sent immediately after handshake.

Name:	No Close Frame
Risk Level:	Low
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket handled abrupt TCP closure and allowed clean reconnection.
Solution:	Ensure that server detects and cleans up on ungraceful disconnects.

Name:	Long Close Reason
Risk Level:	Medium
Description:	WebSocket at wss://evmos-testnet-rpc.publicnode.com:443/websocket accepted close frame with long reason (123 bytes).
Solution:	Enforce strict limits on close reason size (≤123 bytes).