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.

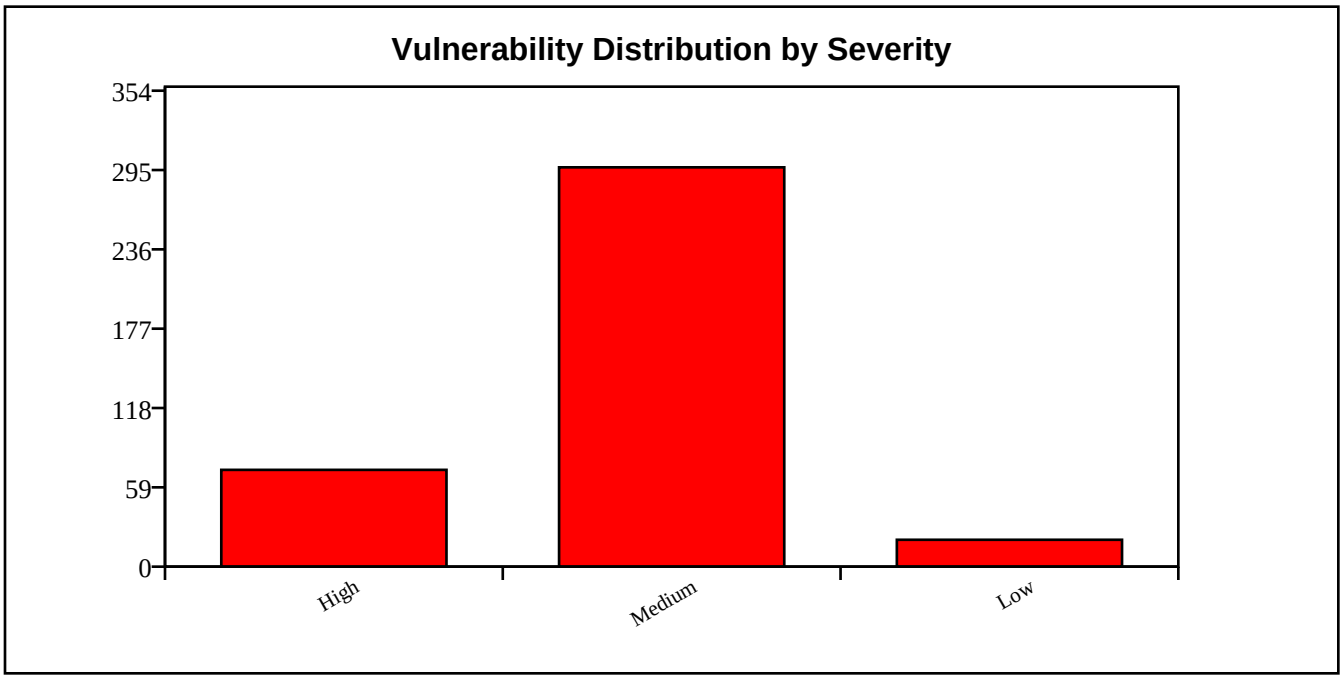
• Crawl and detect active WebSocket endpoints from public websites.
• Apply origin-header enforcement and protocol fuzzing tests to assess security gaps.
• Generate structured PDF reports summarizing detected vulnerabilities and severity.

Scan Start Time:	2025-06-24 14:09:59
Scan End Time:	2025-06-24 14:32:51
Total Scan Duration:	1376.62 seconds
Total URLs Scanned:	1
High Severity Vulnerabilities:	72
Medium Severity Vulnerabilities:	297
Low Severity Vulnerabilities:	20

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

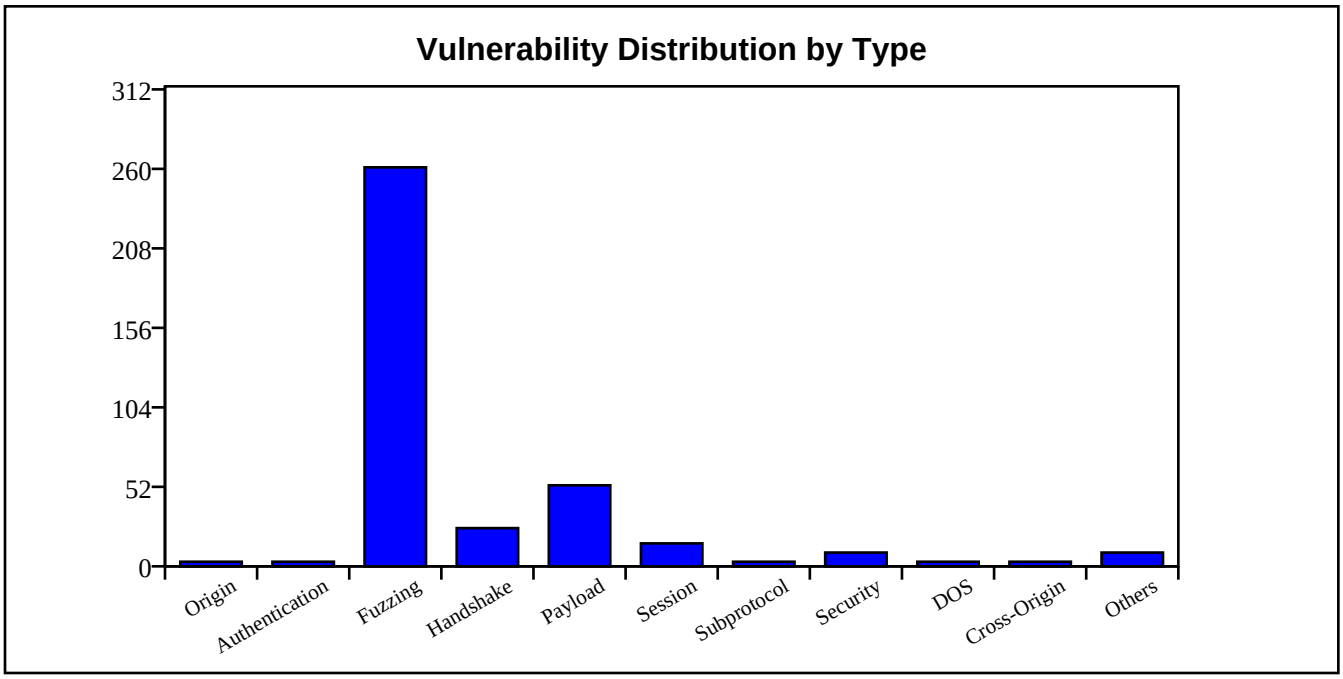


Vulnerability Summary by Type

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	3
Authentication	3
Fuzzing	261
Handshake	25
Payload	53
Session	15
Subprotocol	3
Security	9
DOS	3
Cross-Origin	3
Others	9


Vulnerability Distribution by Type
312
260
208
156
104
52
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:	1163.16 seconds
URLs Crawled:	100
WebSocket Endpoints Found:	144
Attack Performed:	True
Attack Type:	WebSocket Tests
High Severity Findings:	72
Medium Severity Findings:	297
Low Severity Findings:	20

WebSocket Endpoints:

#	URL
1	wss://bahamut-rpc.publicnode.com
2	wss://sei-evm-rpc.publicnode.com
3	wss://lava- rpc.publicnode.com:443/websocket
4	wss://evmos-testnet- rpc.publicnode.com:443/websocket
5	wss://optimism-sepolia- rpc.publicnode.com
6	wss://blast-rpc.publicnode.com
7	wss://opbnb-rpc.publicnode.com
8	wss://metis-rpc.publicnode.com:443
9	wss://comdex- rpc.publicnode.com:443/websocket
10	wss://scroll-rpc.publicnode.com
11	wss://fraxtal-holesky- rpc.publicnode.com:443
12	wss://moonbeam-rpc.publicnode.com

13	wss://babylon- rpc.publicnode.com:443/websocket
14	wss://nibiru-evm-rpc.publicnode.com
15	wss://rebus- rpc.publicnode.com:443/websocket
16	wss://omniflix- rpc.publicnode.com:443/websocket
17	wss://polygon-amoy-heimdall- rpc.publicnode.com:443/websocket
18	wss://xpla- rpc.publicnode.com:443/websocket
19	wss://celer- rpc.publicnode.com:443/websocket
20	wss://oraichain- rpc.publicnode.com:443/websocket
21	wss://evmos- rpc.publicnode.com:443/websocket
22	wss://dydx- rpc.publicnode.com:443/websocket
23	wss://gnosis-chiado-rpc.publicnode.com
24	wss://scroll-sepolia-rpc.publicnode.com
25	wss://elys- rpc.publicnode.com:443/websocket
26	wss://tenet-evm-rpc.publicnode.com

27	wss://celestia- rpc.publicnode.com:443/websocket
28	wss://neutron- rpc.publicnode.com:443/websocket
29	wss://stargaze- rpc.publicnode.com:443/websocket
30	wss://soneium-rpc.publicnode.com
31	wss://medibloc- rpc.publicnode.com:443/websocket
32	wss://evmos-evm-rpc.publicnode.com
33	wss://arbitrum-sepolia- rpc.publicnode.com
34	wss://fantom-rpc.publicnode.com
35	wss://ethereum-holesky- rpc.publicnode.com
36	wss://arbitrum-nova-rpc.publicnode.com
37	wss://berachain-rpc.publicnode.com
38	wss://avalanche-fuji-c-chain- rpc.publicnode.com
39	wss://dymension-evm-rpc.publicnode.com
40	wss://pulsechain-testnet- rpc.publicnode.com

41	wss://dymension- rpc.publicnode.com:443/websocket
42	wss://chiliz-spicy-rpc.publicnode.com
43	wss://ethereum-hoodi-rpc.publicnode.com
44	wss://unichain-sepolia- rpc.publicnode.com
45	wss://xpla-evm-rpc.publicnode.com
46	wss://teritori- rpc.publicnode.com:443/websocket
47	wss://taiko-rpc.publicnode.com
48	wss://syscoin-tanenbaum-evm- rpc.publicnode.com
49	wss://sifchain- rpc.publicnode.com:443/websocket
50	wss://polygon-bor-rpc.publicnode.com
51	wss://cosmos- rpc.publicnode.com:443/websocket
52	wss://mantle-rpc.publicnode.com
53	wss://base-rpc.publicnode.com
54	wss://analog-rpc.publicnode.com

55	wss://injective-testnet- rpc.publicnode.com:443/websocket
56	wss://solana-rpc.publicnode.com
57	wss://starknet-rpc.publicnode.com
58	wss://elys-testnet- rpc.publicnode.com:443/websocket
59	wss://terra-classic- rpc.publicnode.com:443/websocket
60	wss://celo-rpc.publicnode.com
61	wss://peaq-agung-rpc.publicnode.com
62	wss://cronos- rpc.publicnode.com:443/websocket
63	wss://mantra- rpc.publicnode.com:443/websocket
64	wss://manta-atlantic-rpc.publicnode.com
65	wss://coreum- rpc.publicnode.com:443/websocket
66	wss://fetch- rpc.publicnode.com:443/websocket
67	wss://haqq-evm-rpc.publicnode.com
68	wss://passage- rpc.publicnode.com:443/websocket

69	wss://starknet-sepolia- rpc.publicnode.com
70	wss://cronos-pos- rpc.publicnode.com:443/websocket
71	wss://bsc-testnet-rpc.publicnode.com
72	wss://celestia-mocha- rpc.publicnode.com:443/websocket
73	wss://axelar- rpc.publicnode.com:443/websocket
74	wss://evmos-testnet-evm- rpc.publicnode.com
75	wss://optimism-rpc.publicnode.com
76	wss://dora- rpc.publicnode.com:443/websocket
77	wss://quicksilver- rpc.publicnode.com:443/websocket
78	wss://sonic-rpc.publicnode.com:443
79	wss://bsc-rpc.publicnode.com
80	wss://gnosis-rpc.publicnode.com
81	wss://avail-rpc.publicnode.com
82	wss://polygon-heimdall- rpc.publicnode.com:443/websocket

83	wss://taiko-hekla-rpc.publicnode.com
84	wss://avalanche-c-chain- rpc.publicnode.com
85	wss://sui-testnet-rpc.publicnode.com
86	wss://sui-rpc.publicnode.com
87	wss://akash- rpc.publicnode.com:443/websocket
88	wss://unichain-rpc.publicnode.com
89	wss://sei- rpc.publicnode.com:443/websocket
90	wss://pulsechain-rpc.publicnode.com
91	wss://nibiru- rpc.publicnode.com:443/websocket
92	wss://regen- rpc.publicnode.com:443/websocket
93	wss://iris-evm-rpc.publicnode.com
94	wss://chihuahua- rpc.publicnode.com:443/websocket
95	wss://solana-testnet-rpc.publicnode.com
96	wss://linea-rpc.publicnode.com

97	wss://ethereum-rpc.publicnode.com
98	wss://juno- rpc.publicnode.com:443/websocket
99	wss://dymension-testnet- rpc.publicnode.com:443/websocket
100	wss://shentu- rpc.publicnode.com:443/websocket
101	wss://base-sepolia-rpc.publicnode.com
102	wss://linea-sepolia-rpc.publicnode.com
103	wss://arbitrum-one-rpc.publicnode.com
104	wss://avail-turing-rpc.publicnode.com
105	wss://haqq- rpc.publicnode.com:443/websocket
106	wss://soneium-minato-rpc.publicnode.com
107	wss://asset-mantle- rpc.publicnode.com:443/websocket
108	wss://berachain-bepolia- rpc.publicnode.com
109	wss://kava- rpc.publicnode.com:443/websocket
110	wss://polkadot-rpc.publicnode.com

111	wss://fraxtal-rpc.publicnode.com:443
112	wss://syscoin-evm-rpc.publicnode.com
113	wss://osmosis- rpc.publicnode.com:443/websocket
114	wss://cheqd- rpc.publicnode.com:443/websocket
115	wss://bitcanna- rpc.publicnode.com:443/websocket
116	wss://mantra-testnet- rpc.publicnode.com:443/websocket
117	wss://nolus- rpc.publicnode.com:443/websocket
118	wss://migaloo- rpc.publicnode.com:443/websocket
119	wss://sonic-blaze-rpc.publicnode.com:443
120	wss://persistence- rpc.publicnode.com:443/websocket
121	wss://rizon- rpc.publicnode.com:443/websocket
122	wss://side- rpc.publicnode.com:443/websocket
123	wss://polygon-amoy-bor- rpc.publicnode.com
124	wss://kava-evm-rpc.publicnode.com

125	wss://chiliz-rpc.publicnode.com
126	wss://cronos-evm-rpc.publicnode.com
127	wss://moonriver-rpc.publicnode.com
128	wss://iris- rpc.publicnode.com:443/websocket
129	wss://saga- rpc.publicnode.com:443/websocket
130	wss://kusama-rpc.publicnode.com
131	wss://metis-sepolia- rpc.publicnode.com:443
132	wss://aurora-rpc.publicnode.com
133	wss://sentinel- rpc.publicnode.com:443/websocket
134	wss://dymension-testnet-evm- rpc.publicnode.com
135	wss://opbnb-testnet-rpc.publicnode.com
136	wss://terra- rpc.publicnode.com:443/websocket
137	wss://tenet- rpc.publicnode.com:443/websocket
138	wss://stride- rpc.publicnode.com:443/websocket

139	wss://injective- rpc.publicnode.com:443/websocket
140	wss://fantom-testnet-rpc.publicnode.com
141	wss://kujira- rpc.publicnode.com:443/websocket
142	wss://peaq-rpc.publicnode.com
143	wss://ethereum-sepolia- rpc.publicnode.com
144	wss://atomone- rpc.publicnode.com:443/websocket

Crawled URLs:

#	URL
1	https://pulsechain-beacon- api.publicnode.com
2	https://omniflix.publicnode.com
3	https://axelar-grpc-web.publicnode.com
4	https://dymension-testnet- rest.publicnode.com
5	https://dora.publicnode.com

6	https://www.publicnode.com/_next/static/ CawY8Ql4hEXlTj-05WlRf/_ssgManifest.js
7	https://celo-rpc.publicnode.com
8	https://sui.publicnode.com
9	https://linea-sepolia-rpc.publicnode.com
10	https://firo-rpc.publicnode.com
11	https://celer-rest.publicnode.com
12	https://quicksilver-rest.publicnode.com
13	https://sei.publicnode.com
14	https://sifchain-rest.publicnode.com
15	https://coreum-rest.publicnode.com
16	https://sifchain-grpc-web.publicnode.com
17	https://kujira-grpc-web.publicnode.com
18	https://sentinel-rest.publicnode.com
19	https://akash.publicnode.com

20	https://bitcoin-testnet- rpc.publicnode.com
21	https://ethereum-beacon- api.publicnode.com
22	https://arbitrum-one-rpc.publicnode.com
23	https://bitcanna-rest.publicnode.com
24	https://tenet.publicnode.com
25	https://analog-rpc.publicnode.com
26	https://bitcoin.publicnode.com
27	https://asset-mantle-grpc- web.publicnode.com
28	https://elys-grpc-web.publicnode.com
29	https://tron-evm-rpc.publicnode.com
30	https://www.publicnode.com/_next/static/ chunks/pages/index-50378be0ac16ad19.js
31	https://taiko-hekla-rpc.publicnode.com
32	https://publicnode.com/snapshots
33	https://avail-rpc.publicnode.com

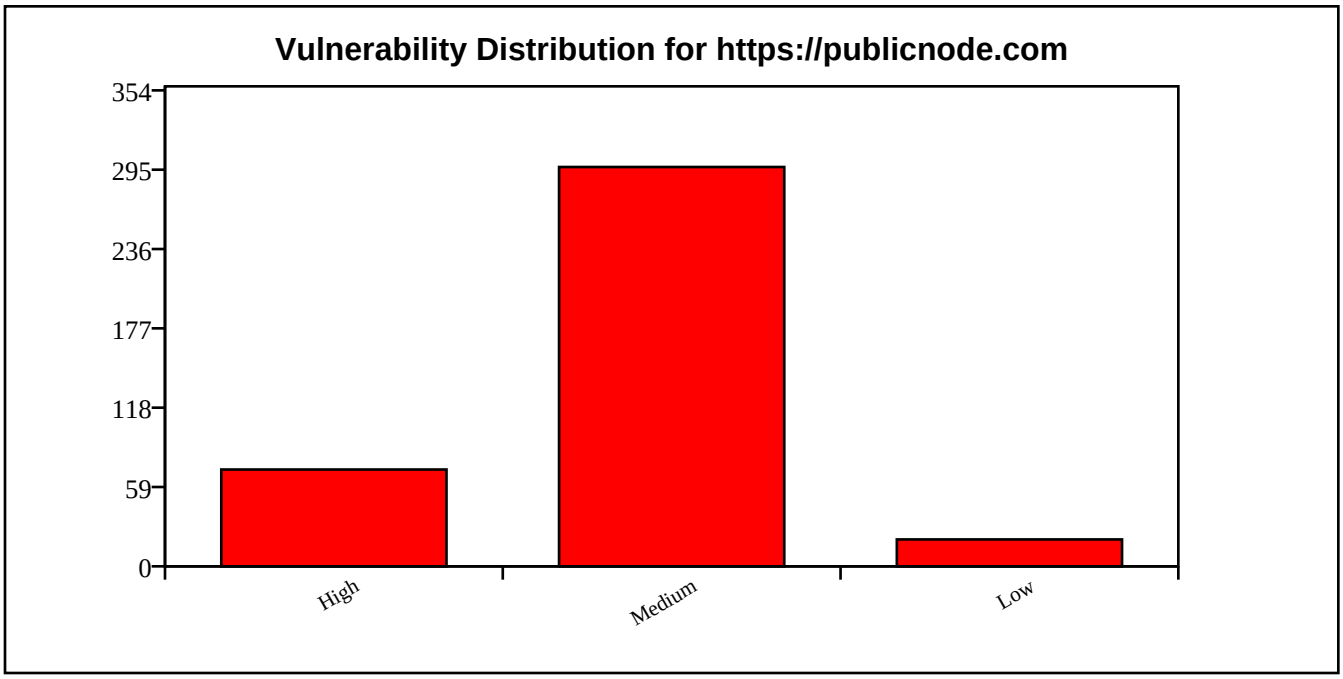
34	https://elys-rest.publicnode.com
35	https://www.publicnode.com/_next/static/ chunks/webpack-d17ebe0ea3c9d6aa.js
36	https://cosmos-rest.publicnode.com
37	https://sei-grpc-web.publicnode.com
38	https://fetch-grpc-web.publicnode.com
39	https://iris-rest.publicnode.com
40	https://shentu-grpc-web.publicnode.com
41	https://sei-rest.publicnode.com
42	https://kava.publicnode.com
43	https://cronos-evm-rpc.publicnode.com
44	https://berachain-bepolia-beacon- rpc.publicnode.com
45	https://avalanche-p-chain- rpc.publicnode.com
46	https://publicnode.com
47	https://www.publicnode.com/_next/static/ chunks/346-5062da986821e93a.js

48	https://pulsechain-testnet-beacon- api.publicnode.com
49	https://www.publicnode.com/_next/static/ CawY8Ql4hEXlTj-05WlRf/_buildManifest.js
50	https://haqq-grpc-web.publicnode.com
51	https://teritori.publicnode.com
52	https://www.publicnode.com/_next/static/ chunks/290-ae0f63b140493652.js
53	https://lava-rest.publicnode.com
54	https://nibiru-evm-rpc.publicnode.com
55	https://moonbeam-rpc.publicnode.com
56	https://evmos-testnet-evm- rpc.publicnode.com
57	https://nolus-rest.publicnode.com
58	https://firo.publicnode.com
59	https://dymension.publicnode.com
60	https://injective-testnet- rest.publicnode.com
61	https://soneium-rpc.publicnode.com

62	https://passage.publicnode.com
63	https://starknet-sepolia- rpc.publicnode.com
64	https://shentu-rest.publicnode.com
65	https://fantom-testnet- rpc.publicnode.com
66	https://aurora.publicnode.com
67	https://ethereum-hoodi- rpc.publicnode.com
68	https://atomone-grpc-web.publicnode.com
69	https://avail.publicnode.com
70	https://berachain-rpc.publicnode.com
71	https://publicnode.com/_next/static/chun ks/290-ae0f63b140493652.js
72	https://fetch.publicnode.com
73	https://shentu.publicnode.com
74	https://mantra-testnet- rest.publicnode.com
75	https://asset-mantle-rest.publicnode.com

76	https://migaloo.publicnode.com
77	https://optimism-rpc.publicnode.com
78	https://xpla-evm-rpc.publicnode.com
79	https://coreum-grpc-web.publicnode.com
80	https://syscoin-evm-rpc.publicnode.com
81	https://sentinel.publicnode.com
82	https://solana-rpc.publicnode.com
83	https://polygon-amoy-bor- rpc.publicnode.com
84	https://nolus.publicnode.com
85	https://aurora-rpc.publicnode.com
86	https://dydx.publicnode.com
87	https://taiko.publicnode.com
88	https://oraichain.publicnode.com
89	https://www.publicnode.com/privacy

90	https://scroll-rpc.publicnode.com
91	https://www.publicnode.com/cookies
92	https://unichain.publicnode.com
93	https://chiliz.publicnode.com
94	https://mantra-grpc-web.publicnode.com
95	https://akash-grpc-web.publicnode.com
96	https://cosmos.publicnode.com
97	https://coreum.publicnode.com
98	https://tenet-evm-rpc.publicnode.com
99	https://publicnode.com/_next/static/chun ks/902-fc4c86e9cf75fdc1.js
100	https://iris-grpc-web.publicnode.com


Vulnerability Distribution for https://publicnode.com
354
295
236
177
118
59
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://bahamut-rpc.publicnode.com

Name:	Missing Origin Check
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com accepts connections from unauthorized origin 'http://malicious-site.com'.
Solution:	Implement strict Origin header validation (whitelist allowed domains).

Name:	Missing Authentication
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com allows unauthenticated connections and responds with data.
Solution:	Require authentication (e.g., JWT, API keys) for WebSocket connections.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Malformed JSON to test parsing errors...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: "type": "invalid_json",...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: "data": "unclosed bracket...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # XSS attempt to check for reflected scripts...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: alert('XSS')...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Large payload to test buffer overflow or DoS...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"type": "large_payload", "data": "A" * 1000000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid WebSocket frame (binary data)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x00\xFF\xFE\xFD...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Command injection attempt...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"command": "whoami; ls"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # SQL injection attempt...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"query": "SELECT * FROM users WHERE id = '1' OR '...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Expression evaluation attempt...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: ${{7*7}}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Null bytes to test input sanitization...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"data": "\0\0\0"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Oversized header- like input...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"headers": "X" * 5000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid UTF-8 sequence...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"data": "\xFF\xFE\xFD"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Empty message...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Malformed protocol message...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: GET / HTTP/1.1...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Host: example.com...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Upgrade: websocket...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Connection: Upgrade...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Unicode payload to test encoding issues (Vuln #1...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"data": "■■■"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Oversized message for DoS (Vuln #58)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"message": "B" * 2000000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid opcode frame (Vuln #23) - Protocol Fuzzi...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x83\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Reserved opcode frame (Vuln #24) - Protocol Fuzz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x8B\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Zero-length fragment (Vuln #25) - Protocol Fuzzi...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x01\x00...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid payload length (Vuln #26) - Protocol Fuz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\x0Atest...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Negative payload length (Vuln #27) - Protocol Fu...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\xFFtest...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Mismatched payload (Vuln #28) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\x04testtest...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid masking key (Vuln #29) - Protocol Fuzzin...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\x84\x00\x00\x00\x00test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Unmasked client frame (Vuln #30) - Protocol Fuzz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid RSV bits (Vuln #31) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \xC1\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Oversized control frame (Vuln #32) - Protocol Fu...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x89\x7E\x00\x7EAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Non-UTF-8 text (Vuln #33) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\x02\xFF\xFF...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Null bytes in text (Vuln #34) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\x05te\x00st...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Binary as text (Vuln #35) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\x04\x00\xFF\x00\xFF...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Text as binary (Vuln #36) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x82\x04text...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid close code (Vuln #37) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x88\x04\x03\xE7OK...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Long close reason (Vuln #40) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x88\x7D\x03\xE8AAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Path traversal attempt (Vuln #74)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"path": "/../../etc/passwd"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Query parameter flood (Vuln #75)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"query": "param=" + "X" * 1000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # PostMessage abuse attempt (Vuln #68)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: {"message": "window.postMessage('malicious','*')"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Spoofed Origin header for origin check (Vuln #65...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Origin: http://malicious.com...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Missing Origin header for origin check (Vuln #65...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Origin:...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid Origin header for origin check (Vuln #65...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Origin: null...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Missing authentication cookie (Vuln #41)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Cookie:...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Invalid authentication token (Vuln #43)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Authorization: Bearer invalid-token...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Expired authentication token (Vuln #42)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Malformed WebSocket frame with invalid opcode se...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \xFF\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: # Oversized WebSocket frame (Protocol Fuzzing)...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com responds to malformed payload: \x81\x7F\x00\x00\x00\x00\x00\x10\x00\x00{"data": "...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Non-Base64 Sec-WebSocket-Key
Risk Level:	Medium
Description:	Server at bahamut-rpc.publicnode.com:443 accepted non-base64 Sec-WebSocket-Key.
Solution:	Validate Sec-WebSocket-Key as base64-encoded.

Name:	Oversized Sec-WebSocket-Key
Risk Level:	Medium
Description:	Server at bahamut-rpc.publicnode.com:443 accepted oversized Sec-WebSocket-Key (1KB).

Solution:	Limit Sec-WebSocket-Key size to prevent resource exhaustion.

Name:	Duplicate Sec-WebSocket-Key
Risk Level:	Medium
Description:	Server at bahamut-rpc.publicnode.com:443 accepted duplicate Sec-WebSocket-Key headers.
Solution:	Reject requests with multiple Sec-WebSocket-Key headers.

Name:	Missing Sec-WebSocket-Version
Risk Level:	High
Description:	Server at bahamut-rpc.publicnode.com:443 accepted handshake without Sec-WebSocket-Version.
Solution:	Require Sec-WebSocket-Version header for WebSocket handshake.

Name:	Invalid Sec-WebSocket-Version
Risk Level:	High
Description:	Server at bahamut-rpc.publicnode.com:443 accepted invalid Sec-WebSocket-Version.

Solution:	Validate Sec-WebSocket-Version (e.g., 13) for WebSocket handshake.

Name:	Conflicting Sec-WebSocket-Version
Risk Level:	High
Description:	Server at bahamut-rpc.publicnode.com:443 accepted conflicting Sec-WebSocket-Version headers.
Solution:	Reject requests with multiple Sec-WebSocket- Version headers.

Name:	Missing Connection Header
Risk Level:	High
Description:	Server at bahamut-rpc.publicnode.com:443 accepted handshake without Connection header.
Solution:	Require Connection: Upgrade header for security.

Name:	Case-Sensitive Headers
Risk Level:	Low
Description:	Server at bahamut-rpc.publicnode.com:443 accepted case-sensitive headers.

Solution:	Ensure case-insensitive header parsing as per RFC.

Name:	Oversized Headers
Risk Level:	Medium
Description:	Server at bahamut-rpc.publicnode.com:443 accepted handshake with oversized headers.
Solution:	Set limits for header size to prevent resource exhaustion.

Name:	Long URL Path
Risk Level:	Low
Description:	Server at bahamut-rpc.publicnode.com:443 accepted handshake with long URL path (2KB).
Solution:	Limit URL path length to prevent resource exhaustion.

Name:	Undefined Opcode
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com accepted frame with undefined opcode 0x3.

Solution:	Reject frames with undefined opcodes.

Name:	Reserved Opcode
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com accepted frames with mismatched lengths.
Solution:	Ensure payload lengths match.

Name:	Invalid Masking Key
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com 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://bahamut-rpc.publicnode.com accepted close frame with long reason (123 bytes).
Solution:	Enforce strict limits on close reason size (≤123 bytes).

Name:	No Session Cookie
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com accepts connections without a session cookie.

Solution:	Require valid session cookies (or tokens) to authenticate WebSocket clients.

Name:	Expired Cookie
Risk Level:	Medium
Description:	WebSocket at wss://bahamut-rpc.publicnode.com accepts connections with an expired session cookie.
Solution:	Validate cookie expiration on the server side and reject expired tokens.

Name:	Fake Token
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com accepts connections with a fake authentication token.
Solution:	Implement robust token validation (e.g., JWT signature verification, token expiry check, audience validation).

Name:	Stale Session Reconnect
Risk Level:	High

Description:	WebSocket at wss://bahamut-rpc.publicnode.com allows reconnection with same stale session cookie.
Solution:	Invalidate old session IDs on WebSocket reconnect. Require fresh authentication or refresh token.

Name:	Cross-Site Cookie Hijack
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com accepted cross-origin cookies and origin header.
Solution:	Set SameSite=Strict on cookies and validate the Origin header server-side.

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

Name:	Spoofed Connection Header

Risk Level:	High
Description:	Server at bahamut-rpc.publicnode.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 bahamut-rpc.publicnode.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://bahamut-rpc.publicnode.com accepts insecure TLS cipher: NULL-MD5.
Solution:	Disable weak ciphers like RC4, NULL, EXPORT, and DES-CBC-SHA. Use modern TLS ciphers only.

Name:	Resource Leak - Message Flood

Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com accepted repeated large messages without closing.
Solution:	Set server-side limits for message size and rate. Monitor memory usage.

Name:	Resource Leak - Hanging Sockets
Risk Level:	High
Description:	WebSocket at wss://bahamut-rpc.publicnode.com accepted hanging TCP connections without timeout.
Solution:	Use TCP keep-alive and server-side timeout policies.

Name:	Missing CORS Headers
Risk Level:	High
Description:	WebSocket endpoint wss://bahamut- rpc.publicnode.com (HTTP equivalent) lacks proper CORS headers.
Solution:	Implement proper CORS headers to restrict cross- origin access.

Name:	Invalid Content-Type

Risk Level:	Medium
Description:	WebSocket endpoint wss://bahamut- rpc.publicnode.com (HTTP equivalent) serves invalid Content-Type: text/html; charset=utf-8.
Solution:	Ensure WebSocket endpoints return appropriate Content-Type or upgrade headers.

Name:	Missing Security Headers
Risk Level:	Medium
Description:	WebSocket endpoint wss://bahamut- rpc.publicnode.com (HTTP equivalent) lacks the following headers: Content-Security-Policy.
Solution:	Add missing security headers such as Content- Security-Policy, X-Frame-Options, and Strict- Transport-Security.

Name:	Query Parameter Flood
Risk Level:	High
Description:	WebSocket endpoint wss://bahamut- rpc.publicnode.com?[1000 params] accepts 1000 query parameters.
Solution:	Limit query parameters and implement strict validation.

Affected WebSocket Endpoint: wss://sei-evm-rpc.publicnode.com

Name:	Missing Origin Check
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com accepts connections from unauthorized origin 'http://malicious-site.com'.
Solution:	Implement strict Origin header validation (whitelist allowed domains).

Name:	Missing Authentication
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com allows unauthenticated connections and responds with data.
Solution:	Require authentication (e.g., JWT, API keys) for WebSocket connections.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Malformed JSON to test parsing errors...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: "type": "invalid_json",...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: "data": "unclosed bracket...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # XSS attempt to check for reflected scripts...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: alert('XSS')...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Large payload to test buffer overflow or DoS...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"type": "large_payload", "data": "A" * 1000000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid WebSocket frame (binary data)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x00\xFF\xFE\xFD...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Command injection attempt...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"command": "whoami; ls"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # SQL injection attempt...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"query": "SELECT * FROM users WHERE id = '1' OR '...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Expression evaluation attempt...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: ${{7*7}}...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Null bytes to test input sanitization...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"data": "\0\0\0"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Oversized header- like input...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"headers": "X" * 5000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid UTF-8 sequence...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"data": "\xFF\xFE\xFD"}...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Empty message...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Malformed protocol message...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: GET / HTTP/1.1...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Host: example.com...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Upgrade: websocket...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Connection: Upgrade...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Unicode payload to test encoding issues (Vuln #1...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"data": "■■■"}...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Oversized message for DoS (Vuln #58)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"message": "B" * 2000000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid opcode frame (Vuln #23) - Protocol Fuzzi...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x83\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Reserved opcode frame (Vuln #24) - Protocol Fuzz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x8B\x04test...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Zero-length fragment (Vuln #25) - Protocol Fuzzi...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x01\x00...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid payload length (Vuln #26) - Protocol Fuz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\x0Atest...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Negative payload length (Vuln #27) - Protocol Fu...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\xFFtest...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Mismatched payload (Vuln #28) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\x04testtest...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid masking key (Vuln #29) - Protocol Fuzzin...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\x84\x00\x00\x00\x00test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Unmasked client frame (Vuln #30) - Protocol Fuzz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid RSV bits (Vuln #31) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \xC1\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Oversized control frame (Vuln #32) - Protocol Fu...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x89\x7E\x00\x7EAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Non-UTF-8 text (Vuln #33) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\x02\xFF\xFF...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Null bytes in text (Vuln #34) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\x05te\x00st...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Binary as text (Vuln #35) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\x04\x00\xFF\x00\xFF...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Text as binary (Vuln #36) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x82\x04text...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid close code (Vuln #37) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x88\x04\x03\xE7OK...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Long close reason (Vuln #40) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x88\x7D\x03\xE8AAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Path traversal attempt (Vuln #74)...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"path": "/../../etc/passwd"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Query parameter flood (Vuln #75)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"query": "param=" + "X" * 1000}...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # PostMessage abuse attempt (Vuln #68)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: {"message": "window.postMessage('malicious','*')"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Spoofed Origin header for origin check (Vuln #65...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Origin: http://malicious.com...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Missing Origin header for origin check (Vuln #65...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Origin:...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid Origin header for origin check (Vuln #65...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Origin: null...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Missing authentication cookie (Vuln #41)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Cookie:...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Invalid authentication token (Vuln #43)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Authorization: Bearer invalid-token...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Expired authentication token (Vuln #42)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Malformed WebSocket frame with invalid opcode se...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \xFF\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: # Oversized WebSocket frame (Protocol Fuzzing)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com responds to malformed payload: \x81\x7F\x00\x00\x00\x00\x00\x10\x00\x00{"data": "...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Non-Base64 Sec-WebSocket-Key
Risk Level:	Medium
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted non-base64 Sec-WebSocket-Key.
Solution:	Validate Sec-WebSocket-Key as base64-encoded.

Name:	Oversized Sec-WebSocket-Key
Risk Level:	Medium
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted oversized Sec-WebSocket-Key (1KB).
Solution:	Limit Sec-WebSocket-Key size to prevent resource exhaustion.

Name:	Duplicate Sec-WebSocket-Key
Risk Level:	Medium
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted duplicate Sec-WebSocket-Key headers.
Solution:	Reject requests with multiple Sec-WebSocket-Key headers.

Name:	Missing Sec-WebSocket-Version
Risk Level:	High
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted handshake without Sec-WebSocket-Version.
Solution:	Require Sec-WebSocket-Version header for WebSocket handshake.

Name:	Invalid Sec-WebSocket-Version
Risk Level:	High
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted invalid Sec-WebSocket-Version.
Solution:	Validate Sec-WebSocket-Version (e.g., 13) for WebSocket handshake.

Name:	Conflicting Sec-WebSocket-Version
Risk Level:	High
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted conflicting Sec-WebSocket-Version headers.
Solution:	Reject requests with multiple Sec-WebSocket- Version headers.

Name:	Missing Connection Header
Risk Level:	High
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted handshake without Connection header.
Solution:	Require Connection: Upgrade header for security.

Name:	Case-Sensitive Headers
Risk Level:	Low
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted case-sensitive headers.
Solution:	Ensure case-insensitive header parsing as per RFC.

Name:	Oversized Headers
Risk Level:	Medium
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted handshake with oversized headers.
Solution:	Set limits for header size to prevent resource exhaustion.

Name:	Long URL Path
Risk Level:	Low
Description:	Server at sei-evm-rpc.publicnode.com:443 accepted handshake with long URL path (2KB).
Solution:	Limit URL path length to prevent resource exhaustion.

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

Name:	Reserved Opcode
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com accepted frames with mismatched lengths.
Solution:	Ensure payload lengths match.

Name:	Invalid Masking Key
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com 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://sei-evm-rpc.publicnode.com accepted close frame with long reason (123 bytes).
Solution:	Enforce strict limits on close reason size (≤123 bytes).

Name:	No Session Cookie
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com accepts connections without a session cookie.
Solution:	Require valid session cookies (or tokens) to authenticate WebSocket clients.

Name:	Expired Cookie
Risk Level:	Medium
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com accepts connections with an expired session cookie.
Solution:	Validate cookie expiration on the server side and reject expired tokens.

Name:	Fake Token
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com accepts connections with a fake authentication token.
Solution:	Implement robust token validation (e.g., JWT signature verification, token expiry check, audience validation).

Name:	Stale Session Reconnect
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com allows reconnection with same stale session cookie.

Solution:	Invalidate old session IDs on WebSocket reconnect. Require fresh authentication or refresh token.

Name:	Cross-Site Cookie Hijack
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com accepted cross-origin cookies and origin header.
Solution:	Set SameSite=Strict on cookies and validate the Origin header server-side.

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

Name:	Spoofed Connection Header
Risk Level:	High

Description:	Server at sei-evm-rpc.publicnode.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 sei-evm-rpc.publicnode.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://sei-evm-rpc.publicnode.com accepts insecure TLS cipher: NULL-MD5.
Solution:	Disable weak ciphers like RC4, NULL, EXPORT, and DES-CBC-SHA. Use modern TLS ciphers only.

Name:	Resource Leak - Message Flood
Risk Level:	High

Description:	WebSocket at wss://sei-evm-rpc.publicnode.com accepted repeated large messages without closing.
Solution:	Set server-side limits for message size and rate. Monitor memory usage.

Name:	Resource Leak - Hanging Sockets
Risk Level:	High
Description:	WebSocket at wss://sei-evm-rpc.publicnode.com accepted hanging TCP connections without timeout.
Solution:	Use TCP keep-alive and server-side timeout policies.

Name:	Missing CORS Headers
Risk Level:	High
Description:	WebSocket endpoint wss://sei-evm- rpc.publicnode.com (HTTP equivalent) lacks proper CORS headers.
Solution:	Implement proper CORS headers to restrict cross- origin access.

Name:	Invalid Content-Type
Risk Level:	Medium

Description:	WebSocket endpoint wss://sei-evm- rpc.publicnode.com (HTTP equivalent) serves invalid Content-Type: text/html; charset=utf-8.
Solution:	Ensure WebSocket endpoints return appropriate Content-Type or upgrade headers.

Name:	Missing Security Headers
Risk Level:	Medium
Description:	WebSocket endpoint wss://sei-evm- rpc.publicnode.com (HTTP equivalent) lacks the following headers: Content-Security-Policy.
Solution:	Add missing security headers such as Content- Security-Policy, X-Frame-Options, and Strict- Transport-Security.

Name:	Query Parameter Flood
Risk Level:	High
Description:	WebSocket endpoint wss://sei-evm- rpc.publicnode.com?[1000 params] accepts 1000 query parameters.
Solution:	Limit query parameters and implement strict validation.

Affected WebSocket Endpoint: wss://lava-rpc.publicnode.com:443/websocket

Name:	Missing Origin Check
Risk Level:	High
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket accepts connections from unauthorized origin 'http://malicious-site.com'.
Solution:	Implement strict Origin header validation (whitelist allowed domains).

Name:	Missing Authentication
Risk Level:	High
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket allows unauthenticated connections and responds with data.
Solution:	Require authentication (e.g., JWT, API keys) for WebSocket connections.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Malformed JSON to test parsing errors...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: "type": "invalid_json",...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: "data": "unclosed bracket...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # XSS attempt to check for reflected scripts...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: alert('XSS')...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Large payload to test buffer overflow or DoS...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"type": "large_payload", "data": "A" * 1000000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid WebSocket frame (binary data)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x00\xFF\xFE\xFD...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Command injection attempt...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"command": "whoami; ls"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # SQL injection attempt...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"query": "SELECT * FROM users WHERE id = '1' OR '...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Expression evaluation attempt...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: ${{7*7}}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Null bytes to test input sanitization...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"data": "\0\0\0"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Oversized header-like input...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"headers": "X" * 5000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid UTF-8 sequence...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"data": "\xFF\xFE\xFD"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Empty message...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Malformed protocol message...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: GET / HTTP/1.1...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Host: example.com...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Upgrade: websocket...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Connection: Upgrade...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Unicode payload to test encoding issues (Vuln #1...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"data": "■■■"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Oversized message for DoS (Vuln #58)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"message": "B" * 2000000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid opcode frame (Vuln #23) - Protocol Fuzzi...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x83\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Reserved opcode frame (Vuln #24) - Protocol Fuzz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x8B\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Zero-length fragment (Vuln #25) - Protocol Fuzzi...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x01\x00...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid payload length (Vuln #26) - Protocol Fuz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\x0Atest...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Negative payload length (Vuln #27) - Protocol Fu...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\xFFtest...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Mismatched payload (Vuln #28) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\x04testtest...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid masking key (Vuln #29) - Protocol Fuzzin...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\x84\x00\x00\x00\x00test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Unmasked client frame (Vuln #30) - Protocol Fuzz...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid RSV bits (Vuln #31) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \xC1\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Oversized control frame (Vuln #32) - Protocol Fu...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x89\x7E\x00\x7EAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAA...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Non-UTF-8 text (Vuln #33) - Protocol Fuzzing...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\x02\xFF\xFF...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Null bytes in text (Vuln #34) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\x05te\x00st...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Binary as text (Vuln #35) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\x04\x00\xFF\x00\xFF...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Text as binary (Vuln #36) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x82\x04text...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid close code (Vuln #37) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x88\x04\x03\xE7OK...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Long close reason (Vuln #40) - Protocol Fuzzing...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x88\x7D\x03\xE8AAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAA...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Path traversal attempt (Vuln #74)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"path": "/../../etc/passwd"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Query parameter flood (Vuln #75)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"query": "param=" + "X" * 1000}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # PostMessage abuse attempt (Vuln #68)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: {"message": "window.postMessage('malicious','*')"}...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Spoofed Origin header for origin check (Vuln #65...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Origin: http://malicious.com...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Missing Origin header for origin check (Vuln #65...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Origin:...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid Origin header for origin check (Vuln #65...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Origin: null...

Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Missing authentication cookie (Vuln #41)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Cookie:...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Invalid authentication token (Vuln #43)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Authorization: Bearer invalid- token...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Expired authentication token (Vuln #42)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability

Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Malformed WebSocket frame with invalid opcode se...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \xFF\x04test...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: # Oversized WebSocket frame (Protocol Fuzzing)...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Protocol Fuzzing Vulnerability
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket responds to malformed payload: \x81\x7F\x00\x00\x00\x00\x00\x10\x00\x00{"data": "...
Solution:	Implement robust input validation and reject malformed messages.

Name:	Invalid Sec-WebSocket-Version
Risk Level:	High
Description:	Server at lava-rpc.publicnode.com:443 accepted invalid Sec-WebSocket-Version.

Solution:	Validate Sec-WebSocket-Version (e.g., 13) for WebSocket handshake.

Name:	Conflicting Sec-WebSocket-Version
Risk Level:	High
Description:	Server at lava-rpc.publicnode.com:443 accepted conflicting Sec-WebSocket-Version headers.
Solution:	Reject requests with multiple Sec-WebSocket- Version headers.

Name:	Missing Connection Header
Risk Level:	High
Description:	Server at lava-rpc.publicnode.com:443 accepted handshake without Connection header.
Solution:	Require Connection: Upgrade header for security.

Name:	Case-Sensitive Headers
Risk Level:	Low
Description:	Server at lava-rpc.publicnode.com:443 accepted case-sensitive headers.

Solution:	Ensure case-insensitive header parsing as per RFC.

Name:	Oversized Headers
Risk Level:	Medium
Description:	Server at lava-rpc.publicnode.com:443 accepted handshake with oversized headers.
Solution:	Set limits for header size to prevent resource exhaustion.

Name:	Undefined Opcode
Risk Level:	High
Description:	WebSocket at wss://lava- 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://lava- 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://lava- 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://lava- 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://lava- 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://lava- 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://lava- 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://lava- 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://lava- 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://lava- 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:	Null Bytes in Text
Risk Level:	Medium
Description:	WebSocket at wss://lava- 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://lava- 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://lava- 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://lava- 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://lava- 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://lava- 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://lava- rpc.publicnode.com:443/websocket accepted close frame with long reason (123 bytes).

Solution:	Enforce strict limits on close reason size (≤123 bytes).

Name:	No Session Cookie
Risk Level:	High
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket accepts connections without a session cookie.
Solution:	Require valid session cookies (or tokens) to authenticate WebSocket clients.

Name:	Expired Cookie
Risk Level:	Medium
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket accepts connections with an expired session cookie.
Solution:	Validate cookie expiration on the server side and reject expired tokens.

Name:	Fake Token
Risk Level:	High

Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket accepts connections with a fake authentication token.
Solution:	Implement robust token validation (e.g., JWT signature verification, token expiry check, audience validation).

Name:	Stale Session Reconnect
Risk Level:	High
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket allows reconnection with same stale session cookie.
Solution:	Invalidate old session IDs on WebSocket reconnect. Require fresh authentication or refresh token.

Name:	Cross-Site Cookie Hijack
Risk Level:	High
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket accepted cross- origin cookies and origin header.
Solution:	Set SameSite=Strict on cookies and validate the Origin header server-side.

Name:	Fake Extension

Risk Level:	High
Description:	Server at lava-rpc.publicnode.com:443 accepted spoofed extension.
Solution:	Validate Sec-WebSocket-Extensions header against supported values.

Name:	Spoofed Connection Header
Risk Level:	High
Description:	Server at lava-rpc.publicnode.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 lava-rpc.publicnode.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://lava- rpc.publicnode.com:443/websocket accepts insecure TLS cipher: NULL-MD5.
Solution:	Disable weak ciphers like RC4, NULL, EXPORT, and DES-CBC-SHA. Use modern TLS ciphers only.

Name:	Resource Leak - Hanging Sockets
Risk Level:	High
Description:	WebSocket at wss://lava- rpc.publicnode.com:443/websocket accepted hanging TCP connections without timeout.
Solution:	Use TCP keep-alive and server-side timeout policies.

Name:	Missing CORS Headers
Risk Level:	High
Description:	WebSocket endpoint wss://lava- rpc.publicnode.com:443/websocket (HTTP equivalent) lacks proper CORS headers.
Solution:	Implement proper CORS headers to restrict cross- origin access.

Name:	Invalid Content-Type

Risk Level:	Medium
Description:	WebSocket endpoint wss://lava- rpc.publicnode.com:443/websocket (HTTP equivalent) serves invalid Content-Type: text/html; charset=utf-8.
Solution:	Ensure WebSocket endpoints return appropriate Content-Type or upgrade headers.

Name:	Missing Security Headers
Risk Level:	Medium
Description:	WebSocket endpoint wss://lava- rpc.publicnode.com:443/websocket (HTTP equivalent) lacks the following headers: Content-Security-Policy, X-Frame-Options.
Solution:	Add missing security headers such as Content- Security-Policy, X-Frame-Options, and Strict- Transport-Security.

Name:	Query Parameter Flood
Risk Level:	High
Description:	WebSocket endpoint wss://lava-rpc.publicnode.com:443/websocket?[1000 params] accepts 1000 query parameters.
Solution:	Limit query parameters and implement strict validation.