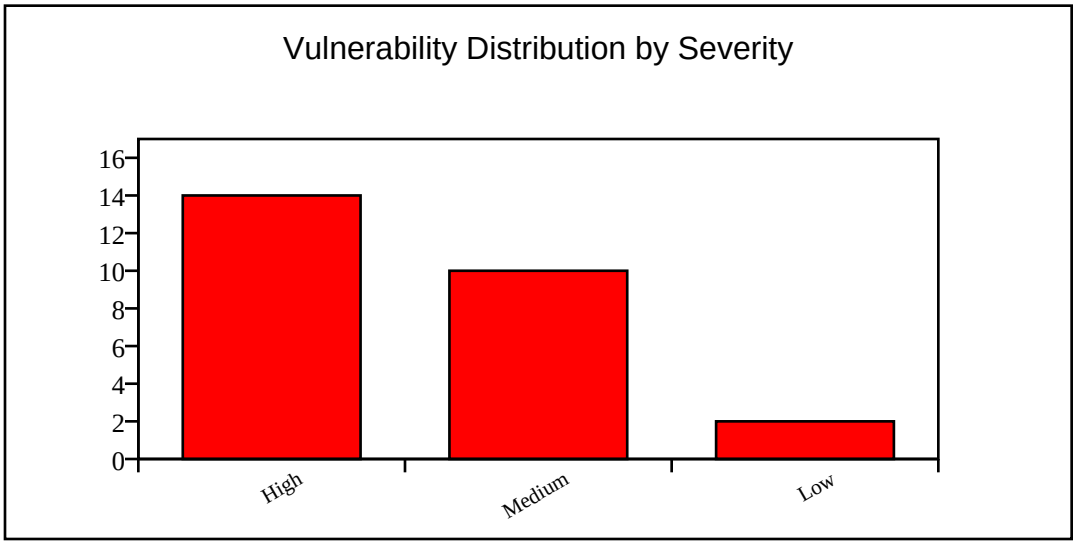
WebSocket Security Scan Report

Executive Summary

Scan Start Time:	2025-06-12 12:34:37
Scan End Time:	2025-06-12 12:36:59
Total Scan Duration:	142.57 seconds
Total URLs Scanned:	1
High Severity Vulnerabilities:	14
Medium Severity Vulnerabilities:	10
Low Severity Vulnerabilities:	2



Detailed Scan Results

Target URL: http://192.168.110.1:8080/

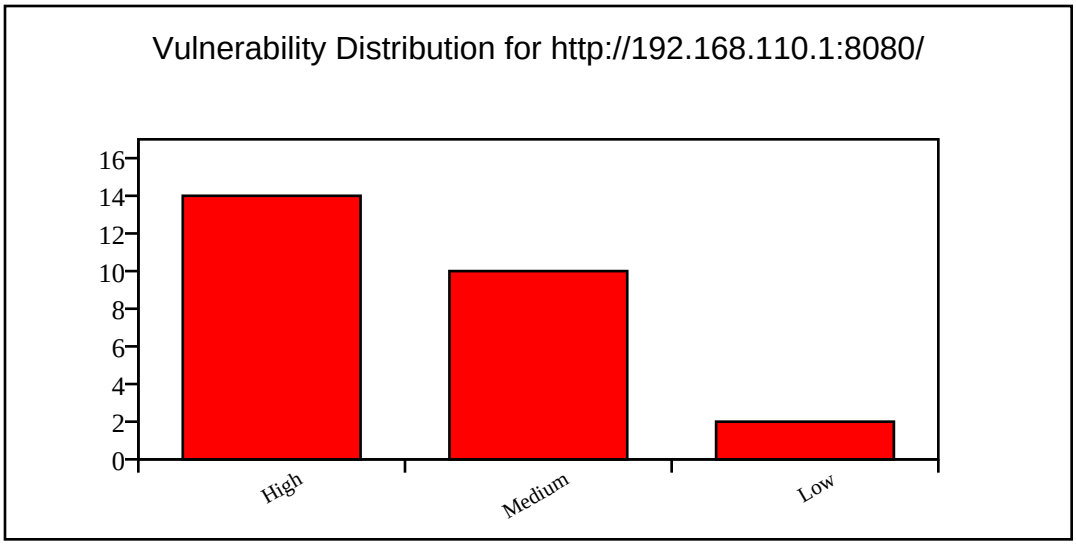
Scan Duration:	142.57 seconds
URLs Crawled:	1
WebSocket Endpoints Found:	2
Attack Performed:	True
Attack Type:	WebSocket Tests
High Severity Findings:	14
Medium Severity Findings:	10
Low Severity Findings:	2

WebSocket Endpoints:

#	URL
1	ws://localhost:8081
2	ws://localhost:8081/

Crawled URLs:

#	URL
1	http://192.168.110.1:8080/



Detected Vulnerabilities:

Name:	No Compression Negotiation
Risk Level:	Low
Description:	Server at localhost:8081 does not negotiate compression.
Solution:	Support permessage-deflate for efficient data transfer.
Affected URL:	localhost:8081

Name:	Connection Flood
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 accepts multiple connections without restriction.
Solution:	Implement connection rate limiting.
Affected URL:	ws://localhost:8081

Name:	Oversized Message
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 accepts oversized message (1MB).
Solution:	Enforce maximum message size limits.
Affected URL:	ws://localhost:8081

Name:	Max Connections
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 allows excessive connections (20).
Solution:	Set a maximum connection limit per client IP.
Affected URL:	ws://localhost:8081

Name:	Idle Timeout Abuse

Risk Level:	Medium
Description:	WebSocket at ws://localhost:8081 allows idle connection for 60 seconds.
Solution:	Implement idle timeout to close inactive connections.
Affected URL:	ws://localhost:8081

Name:	High Compression Ratio
Risk Level:	Medium
Description:	WebSocket at ws://localhost:8081 accepts highly compressible data (100KB).
Solution:	Limit compression ratios to prevent DoS.
Affected URL:	ws://localhost:8081

Name:	Resource Leak
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 handles rapid connection open/close.
Solution:	Ensure proper resource cleanup after connections.
Affected URL:	ws://localhost:8081

Name:	No Compression Negotiation

Risk Level:	Low
Description:	Server at localhost:8081 does not negotiate compression.
Solution:	Support permessage-deflate for efficient data transfer.
Affected URL:	localhost:8081

Name:	Connection Flood
Risk Level:	High
Description:	WebSocket at ws://localhost:8081/ accepts multiple connections without restriction.
Solution:	Implement connection rate limiting.
Affected URL:	ws://localhost:8081/

Name:	Oversized Message
Risk Level:	High
Description:	WebSocket at ws://localhost:8081/ accepts oversized message (1MB).
Solution:	Enforce maximum message size limits.
Affected URL:	ws://localhost:8081/

Name:	Max Connections
Risk Level:	High

Description:	WebSocket at ws://localhost:8081/ allows excessive connections (20).
Solution:	Set a maximum connection limit per client IP.
Affected URL:	ws://localhost:8081/

Name:	Idle Timeout Abuse
Risk Level:	Medium
Description:	WebSocket at ws://localhost:8081/ allows idle connection for 60 seconds.
Solution:	Implement idle timeout to close inactive connections.
Affected URL:	ws://localhost:8081/

Name:	High Compression Ratio
Risk Level:	Medium
Description:	WebSocket at ws://localhost:8081/ accepts highly compressible data (100KB).
Solution:	Limit compression ratios to prevent DoS.
Affected URL:	ws://localhost:8081/

Name:	Resource Leak
Risk Level:	High

Description:	WebSocket at ws://localhost:8081/ handles rapid connection open/close.
Solution:	Ensure proper resource cleanup after connections.
Affected URL:	ws://localhost:8081/

Name:	Missing CORS Headers
Risk Level:	Medium
Description:	Server at http://localhost:8081/ lacks CORS headers: Access-Control-Allow-Origin, Access- Control-Allow-Methods.
Solution:	Configure appropriate CORS headers.
Affected URL:	http://localhost:8081/

Name:	Cross-Origin Iframe
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 accepts cross- origin iframe connections.
Solution:	Validate Origin header; enforce X-Frame-Options: DENY.
Affected URL:	ws://localhost:8081

Name:	Spoofed URL
Risk Level:	High

Description:	WebSocket at ws://localhost:8081 accepts connections with spoofed URL ws://malicious.com.
Solution:	Validate WebSocket URLs and origins.
Affected URL:	ws://localhost:8081

Name:	Missing CORS Headers
Risk Level:	Medium
Description:	Server at http://localhost:8081/ lacks CORS headers: Access-Control-Allow-Origin, Access- Control-Allow-Methods.
Solution:	Configure appropriate CORS headers.
Affected URL:	http://localhost:8081/

Name:	Cross-Origin Iframe
Risk Level:	High
Description:	WebSocket at ws://localhost:8081/ accepts cross- origin iframe connections.
Solution:	Validate Origin header; enforce X-Frame-Options: DENY.
Affected URL:	ws://localhost:8081/

Name:	Spoofed URL
Risk Level:	High

Description:	WebSocket at ws://localhost:8081/ accepts connections with spoofed URL ws://malicious.com/.
Solution:	Validate WebSocket URLs and origins.
Affected URL:	ws://localhost:8081/

Name:	Invalid Content-Type
Risk Level:	Medium
Description:	Server at localhost:8081 accepted handshake with invalid Content-Type.
Solution:	Ignore or validate Content-Type headers for WebSocket handshakes.
Affected URL:	localhost:8081

Name:	Missing Security Headers
Risk Level:	Medium
Description:	Server at localhost:8081 lacks security headers: Content-Security-Policy, X-Content-Type-Options, X-XSS-Protection.
Solution:	Implement security headers like CSP, X-Content- Type-Options, and X-XSS-Protection.
Affected URL:	localhost:8081

Name:	URL Path Traversal
Risk Level:	High

Description:	WebSocket at ws://localhost:8081 is vulnerable to path traversal with path /../../etc/passwd.
Solution:	Sanitize and validate URL paths to prevent directory traversal.
Affected URL:	ws://localhost:8081

Name:	Invalid Content-Type
Risk Level:	Medium
Description:	Server at localhost:8081 accepted handshake with invalid Content-Type.
Solution:	Ignore or validate Content-Type headers for WebSocket handshakes.
Affected URL:	localhost:8081

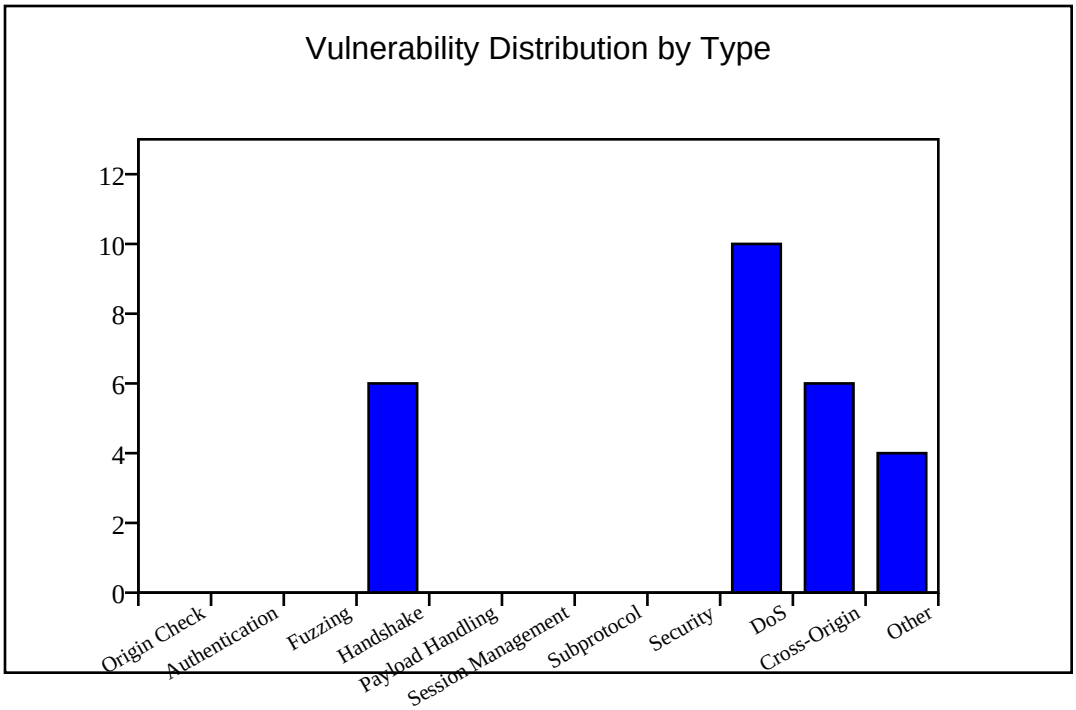
Name:	Missing Security Headers
Risk Level:	Medium
Description:	Server at localhost:8081 lacks security headers: Content-Security-Policy, X-Content-Type-Options, X-XSS-Protection.
Solution:	Implement security headers like CSP, X-Content- Type-Options, and X-XSS-Protection.
Affected URL:	localhost:8081

Name:	URL Path Traversal
Risk Level:	High

Description:	WebSocket at ws://localhost:8081/ is vulnerable to path traversal with path /../../etc/passwd.
Solution:	Sanitize and validate URL paths to prevent directory traversal.
Affected URL:	ws://localhost:8081/

Vulnerability Summary by Type

Type	Count
Origin Check	0
Authentication	0
Fuzzing	0
Handshake	6
Payload Handling	0
Session Management	0
Subprotocol	0
Security	0
DoS	10
Cross-Origin	6
Other	4


Vulnerability Distribution by Type
12
10
8
6
4
2
0
Origin Check
Authentication
Fuzzing
Handshake
Payload Handling
Session Management
Subprotocol
Security
DoS
Cross-Origin
Other