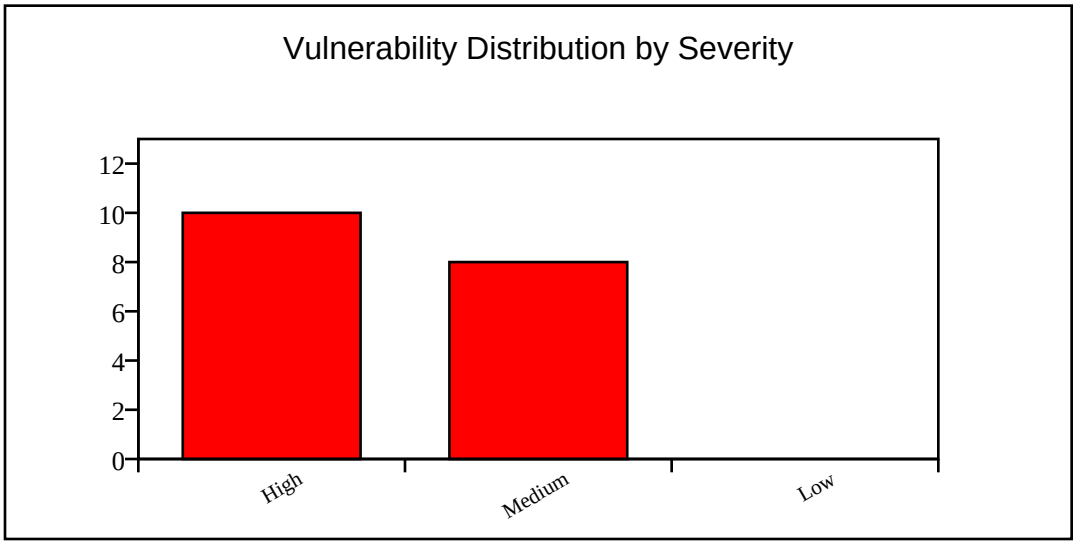
WebSocket Security Scan Report

Executive Summary

Scan Start Time:	2025-06-12 12:24:55
Scan End Time:	2025-06-12 12:25:16
Total Scan Duration:	20.93 seconds
Total URLs Scanned:	1
High Severity Vulnerabilities:	10
Medium Severity Vulnerabilities:	8
Low Severity Vulnerabilities:	0



Detailed Scan Results

Target URL: http://192.168.110.1:8080/

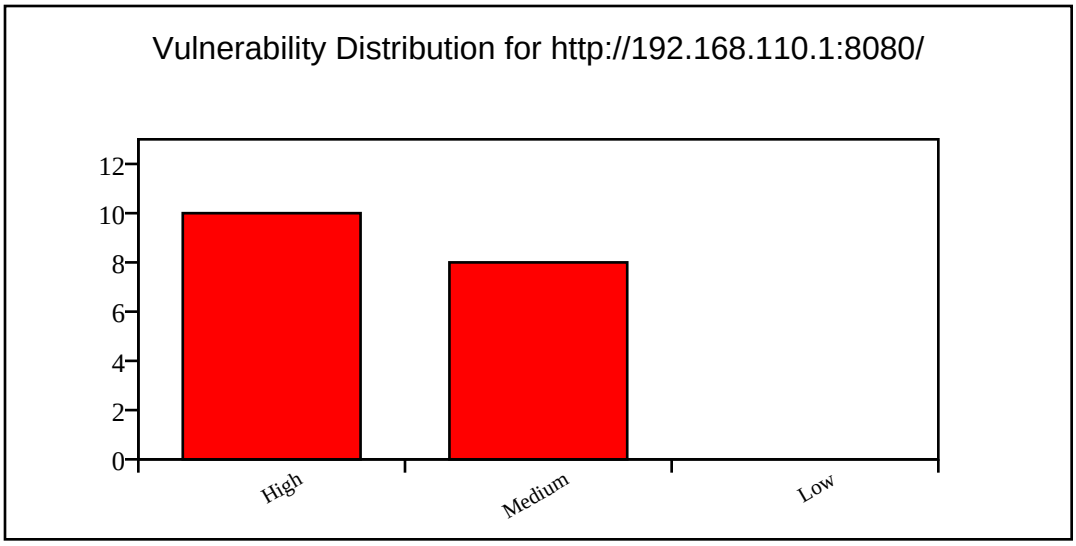
Scan Duration:	20.93 seconds
URLs Crawled:	1
WebSocket Endpoints Found:	2
Attack Performed:	True
Attack Type:	WebSocket Tests
High Severity Findings:	10
Medium Severity Findings:	8
Low Severity Findings:	0

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 Session Cookie
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 accepts connections without a session cookie.
Solution:	Require valid session cookies for WebSocket connections.
Affected URL:	ws://localhost:8081

Name:	Expired Cookie
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 accepts connections with an expired session cookie.
Solution:	Validate cookie expiration on the server side.
Affected URL:	ws://localhost:8081

Name:	Fake Token
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 accepts connections with a fake authentication token.
Solution:	Implement robust token validation (e.g., JWT verification).
Affected URL:	ws://localhost:8081

Name:	Stale Session Reconnect
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 allows reconnection with a stale session.
Solution:	Invalidate stale sessions and require fresh authentication.
Affected URL:	ws://localhost:8081

Name:	Cross-Site Cookie Hijack
Risk Level:	High
Description:	WebSocket at ws://localhost:8081 accepts cookies from a different origin.
Solution:	Set SameSite=Strict on cookies and validate origin.
Affected URL:	ws://localhost:8081

Name:	No Session Cookie
Risk Level:	High
Description:	WebSocket at ws://localhost:8081/ accepts connections without a session cookie.
Solution:	Require valid session cookies for WebSocket connections.
Affected URL:	ws://localhost:8081/

Name:	Expired Cookie
Risk Level:	High
Description:	WebSocket at ws://localhost:8081/ accepts connections with an expired session cookie.
Solution:	Validate cookie expiration on the server side.
Affected URL:	ws://localhost:8081/

Name:	Fake Token
Risk Level:	High
Description:	WebSocket at ws://localhost:8081/ accepts connections with a fake authentication token.
Solution:	Implement robust token validation (e.g., JWT verification).
Affected URL:	ws://localhost:8081/

Name:	Stale Session Reconnect
Risk Level:	High
Description:	WebSocket at ws://localhost:8081/ allows reconnection with a stale session.
Solution:	Invalidate stale sessions and require fresh authentication.
Affected URL:	ws://localhost:8081/

Name:	Cross-Site Cookie Hijack
Risk Level:	High
Description:	WebSocket at ws://localhost:8081/ accepts cookies from a different origin.
Solution:	Set SameSite=Strict on cookies and validate origin.
Affected URL:	ws://localhost:8081/

Name:	Fake Extension
Risk Level:	Medium
Description:	Server at localhost:8081 accepted fake extension 'fake-extension'.
Solution:	Validate Sec-WebSocket-Extensions against supported extensions.
Affected URL:	localhost:8081

Name:	Conflicting Extensions
Risk Level:	Medium
Description:	Server at localhost:8081 accepted conflicting extensions.
Solution:	Reject requests with duplicate or conflicting extensions.
Affected URL:	localhost:8081

Name:	Invalid Subprotocol
Risk Level:	Medium
Description:	WebSocket at ws://localhost:8081 accepts invalid subprotocol 'invalid..protocol'.
Solution:	Validate subprotocol names against a whitelist.
Affected URL:	ws://localhost:8081

Name:	Unaccepted Subprotocol

Risk Level:	Medium
Description:	WebSocket at ws://localhost:8081 accepts unadvertised subprotocol 'unadvertised_protocol'.
Solution:	Only accept subprotocols advertised by the server.
Affected URL:	ws://localhost:8081

Name:	Fake Extension
Risk Level:	Medium
Description:	Server at localhost:8081 accepted fake extension 'fake-extension'.
Solution:	Validate Sec-WebSocket-Extensions against supported extensions.
Affected URL:	localhost:8081

Name:	Conflicting Extensions
Risk Level:	Medium
Description:	Server at localhost:8081 accepted conflicting extensions.
Solution:	Reject requests with duplicate or conflicting extensions.
Affected URL:	localhost:8081

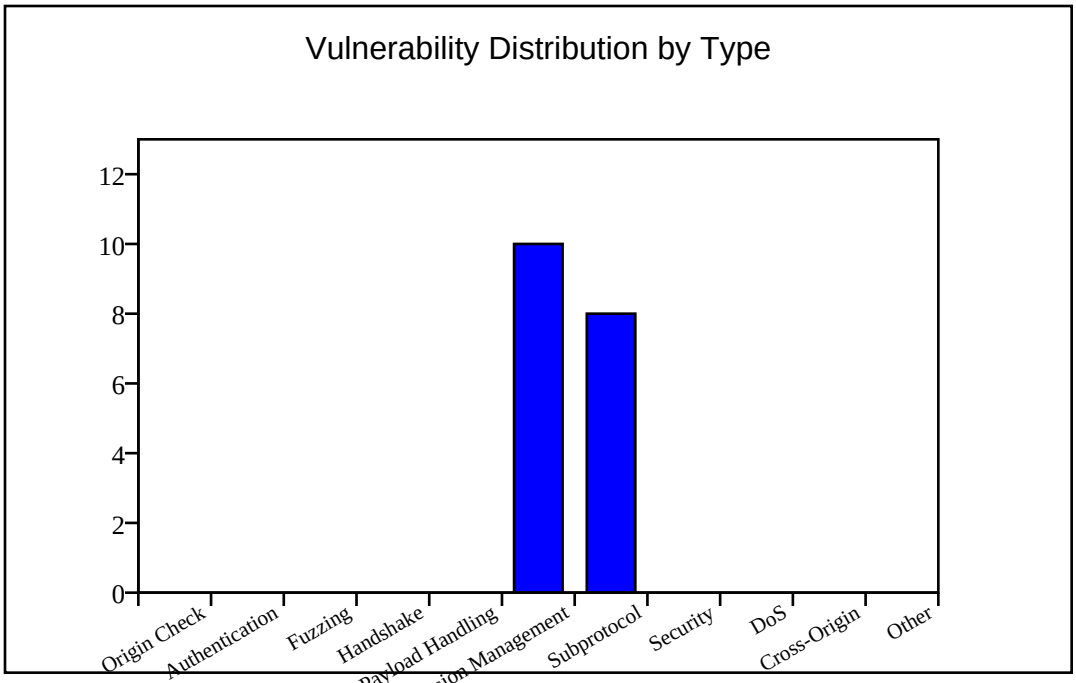
Name:	Invalid Subprotocol
Risk Level:	Medium

Description:	WebSocket at ws://localhost:8081/ accepts invalid subprotocol 'invalid..protocol'.
Solution:	Validate subprotocol names against a whitelist.
Affected URL:	ws://localhost:8081/

Name:	Unaccepted Subprotocol
Risk Level:	Medium
Description:	WebSocket at ws://localhost:8081/ accepts unadvertised subprotocol 'unadvertised_protocol'.
Solution:	Only accept subprotocols advertised by the server.
Affected URL:	ws://localhost:8081/

Vulnerability Summary by Type

Type	Count
Origin Check	0
Authentication	0
Fuzzing	0
Handshake	0
Payload Handling	0
Session Management	10
Subprotocol	8
Security	0
DoS	0
Cross-Origin	0
Other	0


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