WebSocket Insecurities Report

What is websocket

References

RFC 6455

OWASP WS Cheat sheet

What are vulnerabilities

Types of vulnerabilities:

**1️⃣ Handshake & HTTP Request Tests**

[**https://core.ac.uk/download/pdf/45601062.pdf**](https://core.ac.uk/download/pdf/45601062.pdf)

**2️⃣ Payload Handling & Fragmentation**

[**https://www.openmymind.net/WebSocket-Framing-Masking-Fragmentation-and-More/?utm\_source=chatgpt.com**](https://www.openmymind.net/WebSocket-Framing-Masking-Fragmentation-and-More/?utm_source=chatgpt.com)

**3️⃣ Authentication & Session Management**

[**https://arxiv.org/pdf/2104.05324**](https://arxiv.org/pdf/2104.05324)

**4️⃣ Subprotocol & Extension Handling**

[**https://www.cyberchief.ai/2025/05/securing-websockets.html**](https://www.cyberchief.ai/2025/05/securing-websockets.html?utm_source=chatgpt.com)

**5️⃣ Security & Encryption**

[**https://www.ijnrd.org/papers/IJNRD2407274.pdf**](https://www.ijnrd.org/papers/IJNRD2407274.pdf)

**6️⃣ Denial of Service (DoS) & Resource Management**

[**https://cqr.company/web-vulnerabilities/denial-of-service-dos-via-websockets/**](https://cqr.company/web-vulnerabilities/denial-of-service-dos-via-websockets/)

**7️⃣ Cross-Origin & Mixed Content**

**8️⃣ Other Server Vulnerabilities**

[**https://arxiv.org/abs/1409.3367**](https://arxiv.org/abs/1409.3367)

**Papers used at the start**

[**https://www.researchgate.net/publication/384105299\_Review\_Analysis\_of\_Web\_Socket\_Security\_Case\_Study**](https://www.researchgate.net/publication/384105299_Review_Analysis_of_Web_Socket_Security_Case_Study)

[**https://juerkkil.iki.fi/files/websocket2012.pdf**](https://juerkkil.iki.fi/files/websocket2012.pdf)

[**https://oulurepo.oulu.fi/bitstream/handle/10024/6116/nbnfioulu-201603081281.pdf?sequence=1&utm\_source=chatgpt.com**](https://oulurepo.oulu.fi/bitstream/handle/10024/6116/nbnfioulu-201603081281.pdf?sequence=1&utm_source=chatgpt.com)

[**https://www.ijsr.net/getabstract.php?paperid=SUB152856**](https://www.ijsr.net/getabstract.php?paperid=SUB152856)

[**https://www.praetorian.com/blog/meshcentral-cross-site-websocket-hijacking-vulnerability/**](https://www.praetorian.com/blog/meshcentral-cross-site-websocket-hijacking-vulnerability/)