Background:

A websocket is a socket initiated over HTTP and are typically long-lived. Messages can be sent in either direction at any time. They are useful where low-latency or server-initiated messages are required.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated

Graphical user interface, text, application

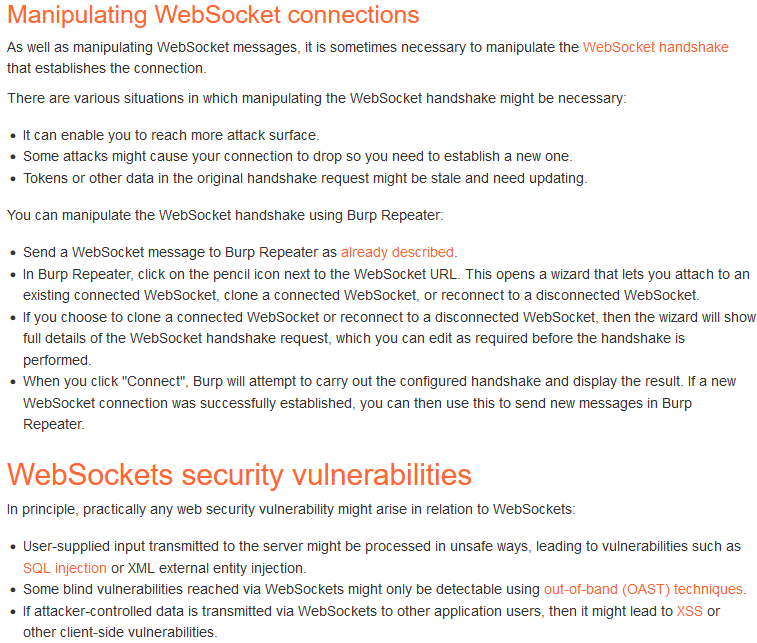
Description automatically generated

Graphical user interface, diagram

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Very cool, burp has its own tab in the proxy section dedicated to websockets. Simply do typical application mapping with burp and check this tab to see websocket requests/ responses.



This section details how to edit the websocket handshake, which can be used to initiate vulnerabilities

Timeline

Description automatically generated

Graphical user interface, text, application, email

Description automatically generatedMake sure to thoroughly look through all of the different websocket traffic and test all different parameters for a variety of vulnerabilities. If you see reflected input coming from a websocket message ofcourse make sure to test it for XSS! (test anything stored for SQLi, stored xss ………)

Graphical user interface, text, application, Word, email

Description automatically generated

Cross-site WebSocket Hijacking

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated