***Websockets vulnerability***

Ref:https://portswigger.net/web-security/websockets/what-are-websockets

### ***Websocket creation***

var ws = new WebSocket("wss://normal-website.com/chat"); # SSL

var ws = new WebSocket("ws://normal-website.com/chat"); # http

Request to open websocket

GET /chat HTTP/1.1

Host: normal-website.com

Sec-WebSocket-Version: 13

Sec-WebSocket-Key: wDqumtseNBJdhkihL6PW7w==

Connection: keep-alive, Upgrade

Cookie: session=KOsEJNuflw4Rd9BDNrVmvwBF9rEijeE2

Upgrade: websocket

Accepting the connection

HTTP/1.1 101 Switching Protocols

Connection: Upgrade

Upgrade: websocket

Sec-WebSocket-Accept: 0FFP+2nmNIf/h+4BP36k9uzrYGk=

Points to remember

1) The Connection and Upgrade headers in the request and response indicate that this is a WebSocket handshake

2) The Sec-WebSocket-Version request header specifies the WebSocket protocol version that the client wishes to use. This is typically 13.

3) The Sec-WebSocket-Key request header contains a Base64-encoded random value, which should be randomly generated in each handshake request.

4) The Sec-WebSocket-Accept response header contains a hash of the value submitted in the Sec-WebSocket-Key request header, concatenated with a specific string defined in the protocol specification. This is done to prevent misleading responses resulting from misconfigured servers or caching proxies.

Once the webscript is open then it lead to a lot of vulnerability like SQL Injection, XSS, Blind vulnerabilities.

In the Burp Proxy, there is websocket tab which keeps track of websocket connection. Check if reflective xss is there or not by passing html tags. The input might be encoded so you might need to send the connection to repeater and trigger the alert via `<img src=0 onerror='alert(1)'>`