Web Socket Abuse

Web Sockets are easy to ignore, which means they can be a fruitful place to test!

Ideas

Treat anything you see in a WebSockets message the same as you would if it were anyplace else.

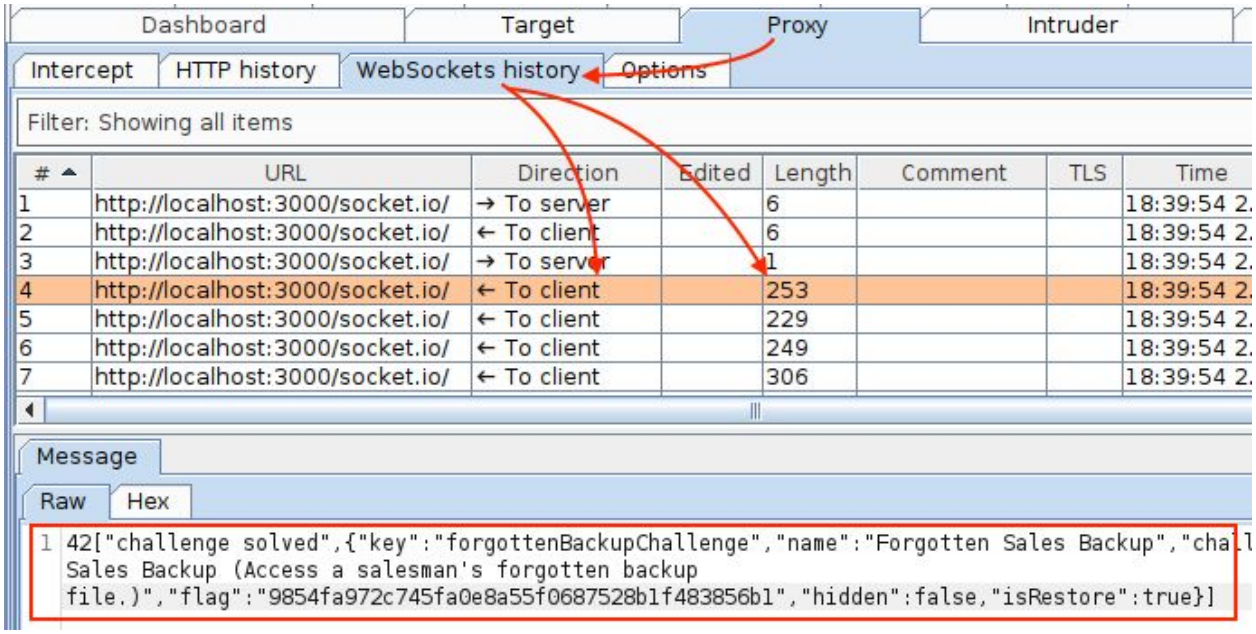
Walk-Thru

Make sure you have Firefox set to use your Burp Suite as a proxy, and that the Proxy > Intercept pane says "Intercept is off"

1. Think back to previous labs and remember that as soon as you solved any challenge, the browser immediately showed that green banner. This is done via Web Sockets.

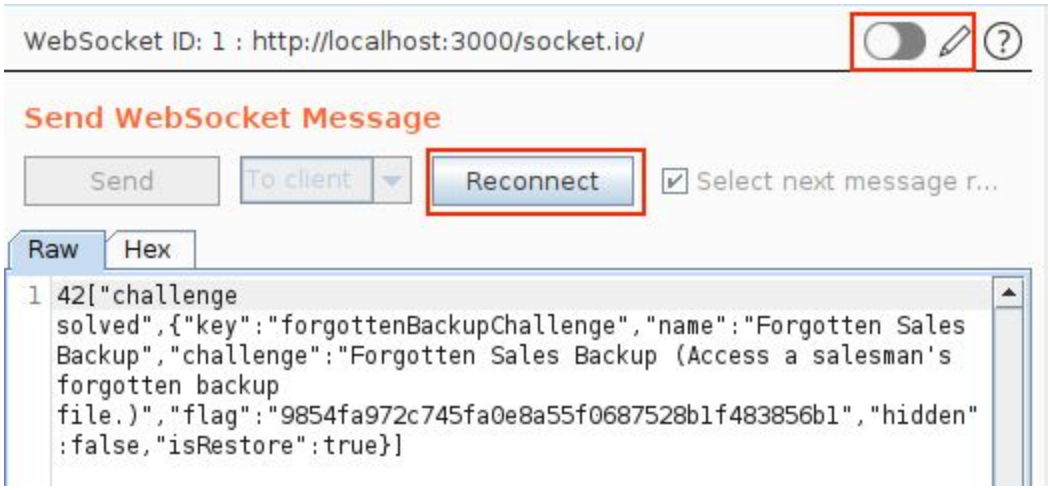
2. In Burp Suite, go to Proxy > WebSockets History

3. Find the item in the history that includes a message. To find them, look for larger numbers in the "Length" column, and "To client" in the "Direction" column.



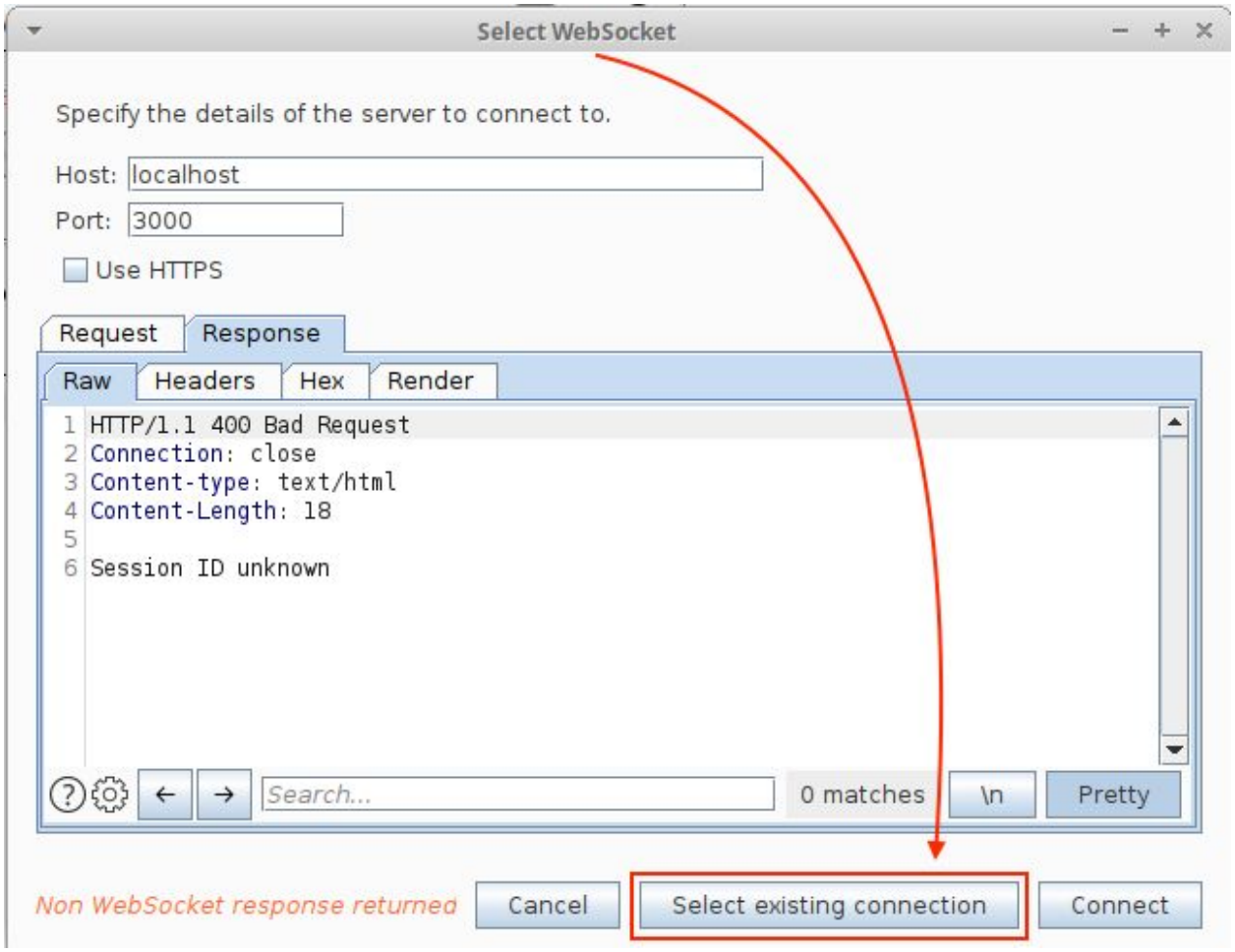
4. Right-click on the message and choose "Send to Repeater"

5. In Repeater, you may have a "Reconnect" button and a grayed out "write" slider, like in the image below.
If you don't have that button and the slider is green, skip to step 6.
If your window looks like the one below, click the "Reconnect" button or click on the slide switch above it.



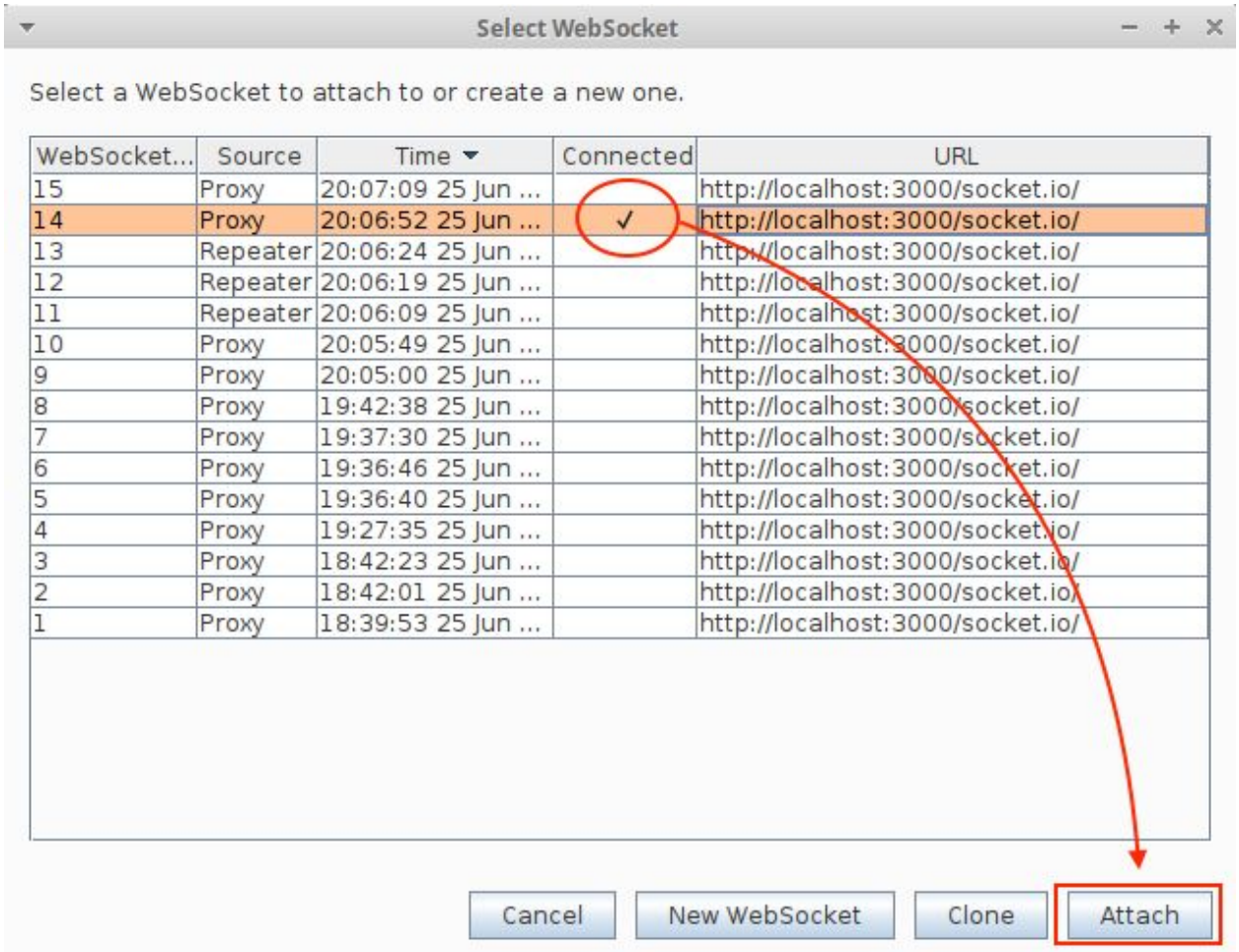
Repeater Looks Different for WebSockets

5A. In the "Select WebSocket" window that opens, click "Select existing connection"



Attach to An Existing WebSocket

5B. Select a row with a checkmark in the "Connected" column, then click "Attach"



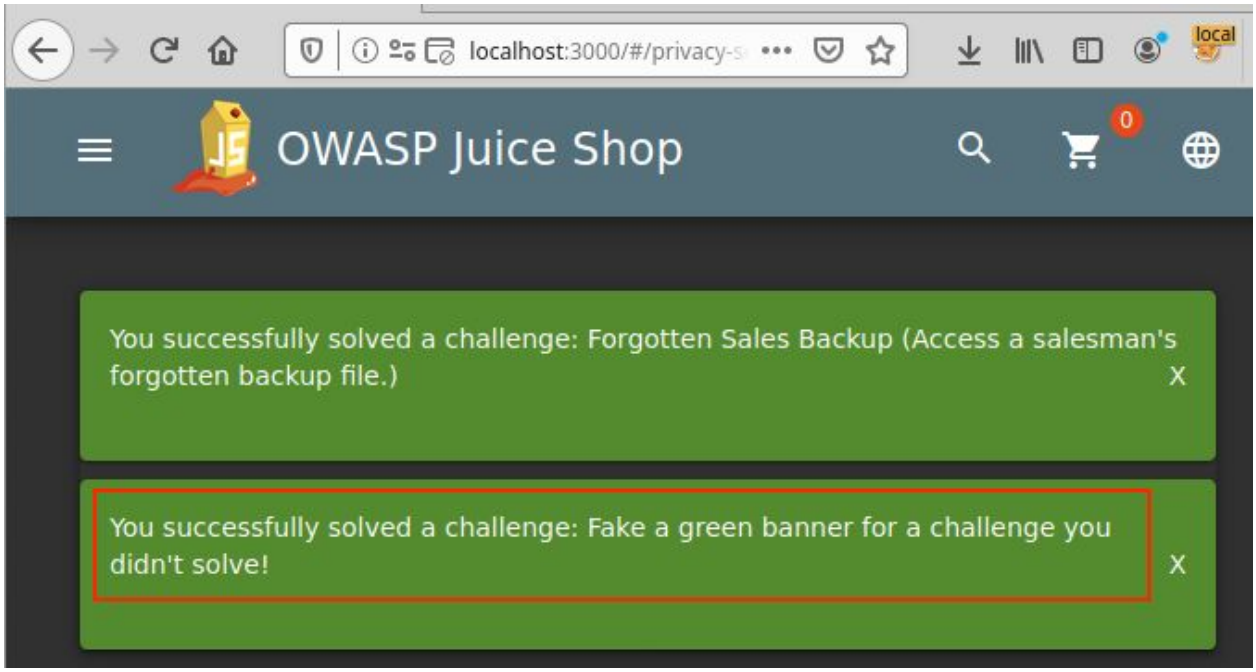
Choose a "Connected" Item from the List

6. Now that you've reconnected to a socket, go to the "Send Websocket Message" pane and edit the "challenge" parameter's value to be whatever you want it to be.

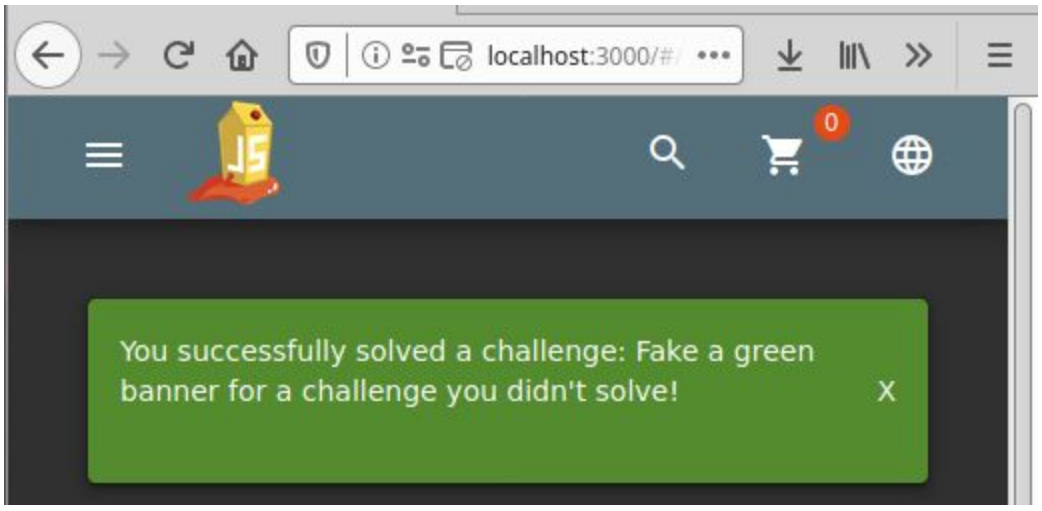
Make Your Attack Here

7. Make sure the "Direction" dropdown says, "To client" and then click "Send"

8. Go back to your browser to see your forged message right below the legitimate one (if the legitimate one was still there)



or



11. This is not one of the defined challenges in Juice Shop, so you don't get a real banner to go along with your fake banner. If you are sad about that, console yourself with more fake banners.