SCENARIO

The application has a web-socket implemented live chat feature which are viewed by a support agent in real time but there exists a vulnerability of injecting JavaScript into it which will trigger an alert on the support agent’s browser.

**PROCEDURE**

1. Go to Live Chat option.
2. Start BurpSuite’s Interceptor.
3. Then type and send any special character into the chat box and we can see that the browser HTML encodes the message before sending.
4. Now, send another random text message and using BurpSuite’s Proxy’s Intercept modify the message with the given payload.
5. After injecting the payload there will be an alert on your side as well as the client’s side.

# PAYLOAD

<img src=1 onerror='alert(1)'>

**REMEDIATIONS**