SCENARIO

The application has an aggressive but flawed XSS filter in the live chat functionality as it blocks an IP if it detects any JavaScript code being injected at a wrong place. We will try to exploit the vulnerability to generate an alert on the client’s browser.

# PROCEDURE

1. Go to live chat option.
2. Start BurpSuite’s Interceptor.
3. Then send a message to the support agent, then we will go to the BurpSuite’s Proxy’s WebSocket History and send that request to our BurpSuite’s Repeater.
4. We noticed that if we replay the same request with the payload then our IP gets blocked.
5. So, we will bypass that by using X-Forwarded-For header in order to spoof our IP address.
6. Then we will send the request again and it will be successful.

# PAYLOAD

1. <img src=1 oNeRrOr=alert`1`>
2. X-Forwarded-For: 1.1.1.1

# REMEDIATION