How to Handle a Possible CSRF Attack Message

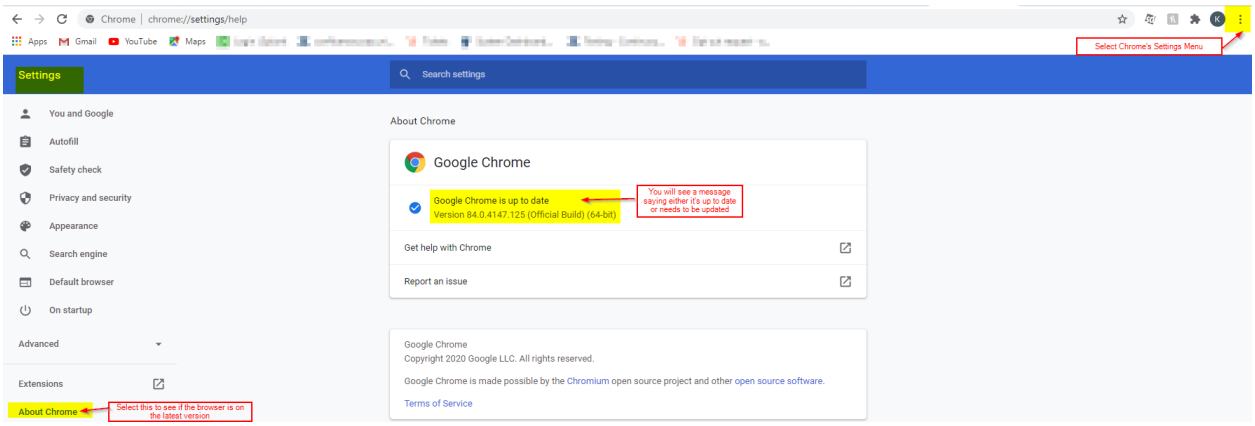
Cross-Site Request Forgery

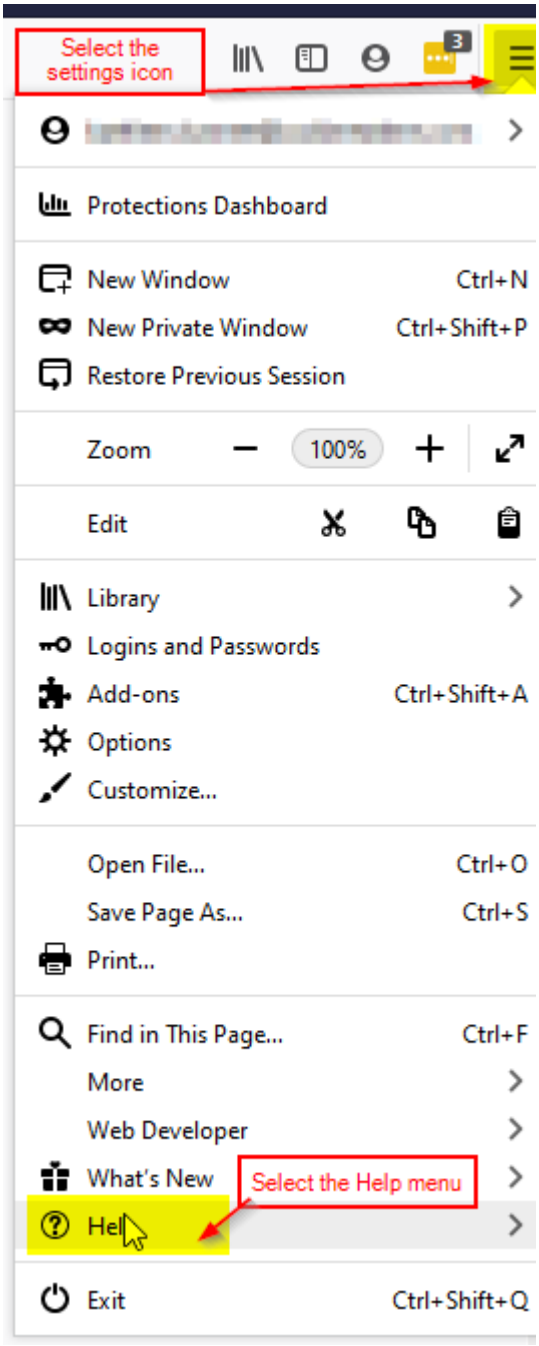
Cross-Site Request Forgery, which is abbreviated as CSRF, is flagged as a possible attack when a malicious website causes a user's web browser to perform an undesired action on the trusted site where the user is currently authenticated.

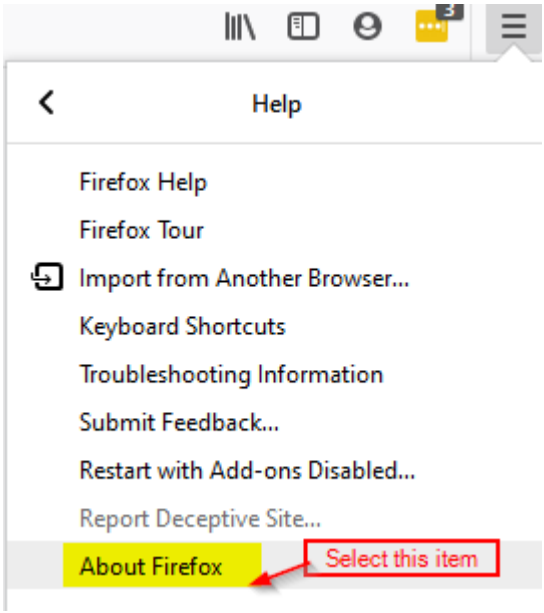
CSRF prevents users from using the same tokens to make a request from outside of their own session on a website. When this error occurs, it is because the request is detected as a malicious request.

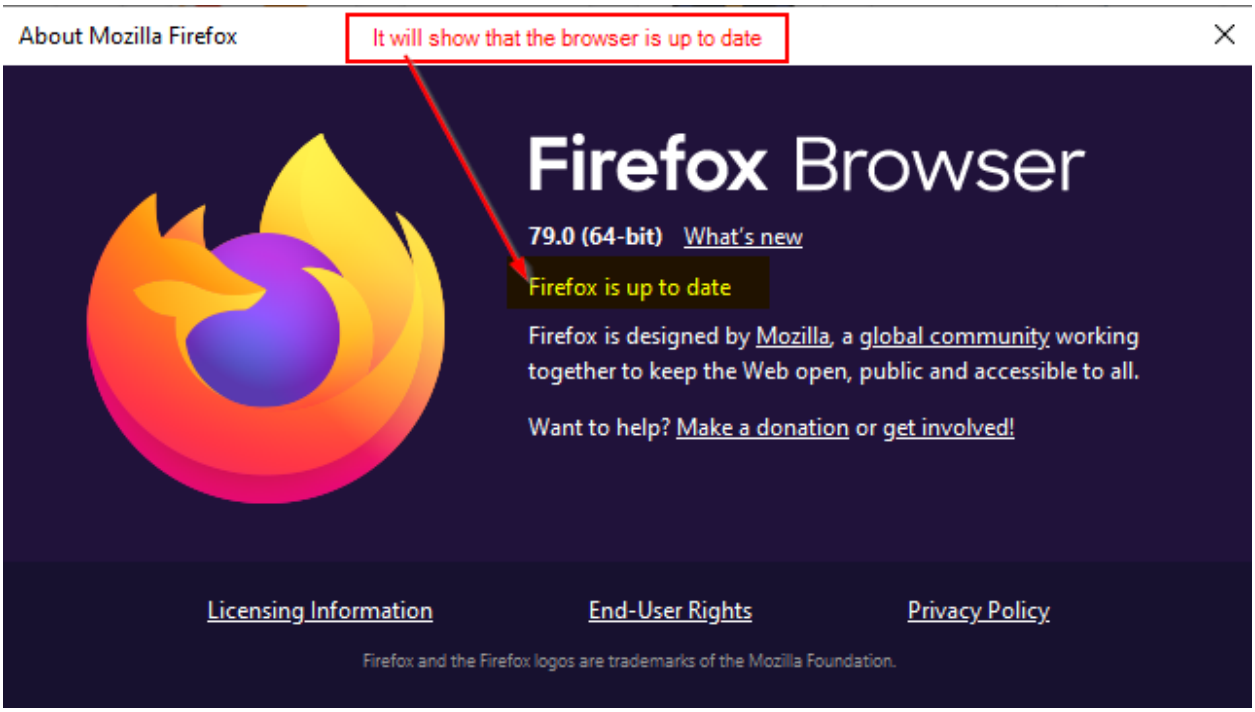
Steps to Fix This Error:

1. Make sure you are using an up-to-date browser.









2. Make sure your browser accepts cookies. Depending on your browser settings, you may have to enable them explicitly.
3. Clear your cache and remove all cookies from your browser.
4. Refresh the page.