

Graphical user interface, text, application, email

Description automatically generated

Changing the request method (right click on captured request in burp and select “change request method” ) can bypass CSRF validation in most situations.

Graphical user interface, text, application, email

Description automatically generated

Completely removing the CSRF parameter from the request can also bypass validation in some circumstances and enable CSRF.

We can test for CSRF by making 2 accounts and swapping CSRF values, if the request goes through with the CSRF token from a different account the page is likely vulnerable

Graphical user interface, text, application, email

Description automatically generated