# Same Site Strict

## In application.properties

### server.servlet.session.cookie.same-site=strict

Setting the **server.servlet.session.cookie.same-site** property to **"strict"** provides an important security benefit by enhancing protection against Cross-Site Request Forgery (CSRF) attacks.

When a cookie is set with the **"SameSite"** attribute set to **"strict"**, the browser will only include the cookie in a request if the request originated from the same site as the one that set the cookie. This helps prevent malicious websites from making requests to your server on behalf of the user, thereby reducing the risk of CSRF attacks.

By setting the **"SameSite"** attribute to **"strict"**, you're ensuring that cookies containing session information are only sent in requests that originate from your own site. This helps protect sensitive user data and prevents unauthorized access to user sessions. Overall, it strengthens the security posture of your web application.

**Rest Application: Most of time Stateless**

TELUSKO