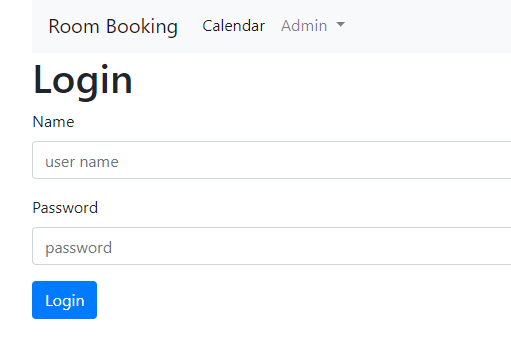
**Surviving a Refresh:**

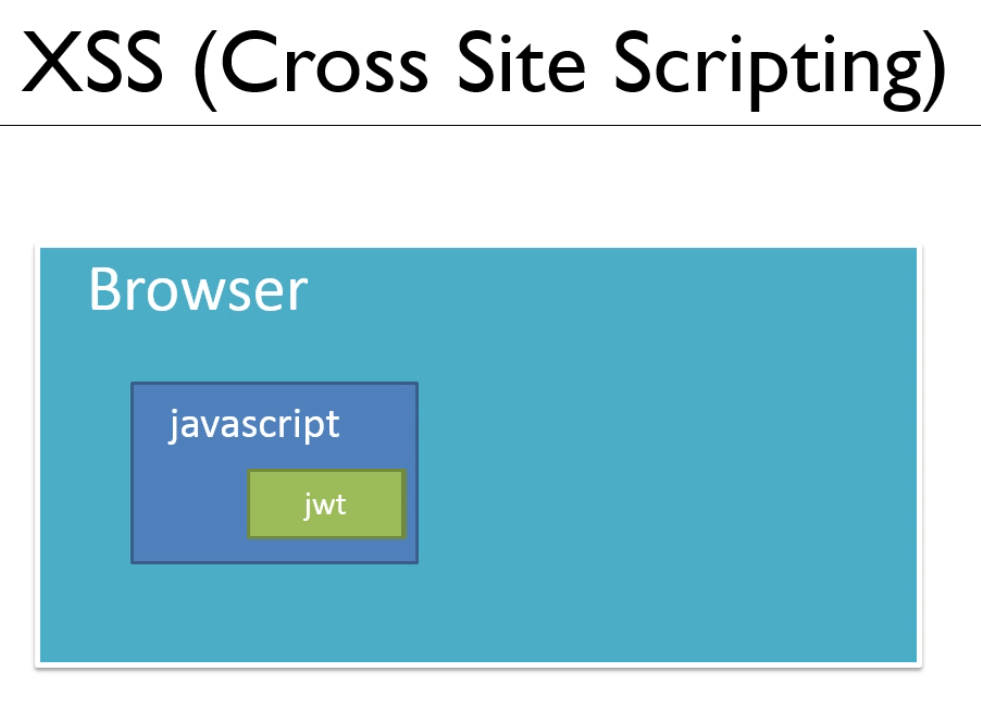
The risks of storing a JWT

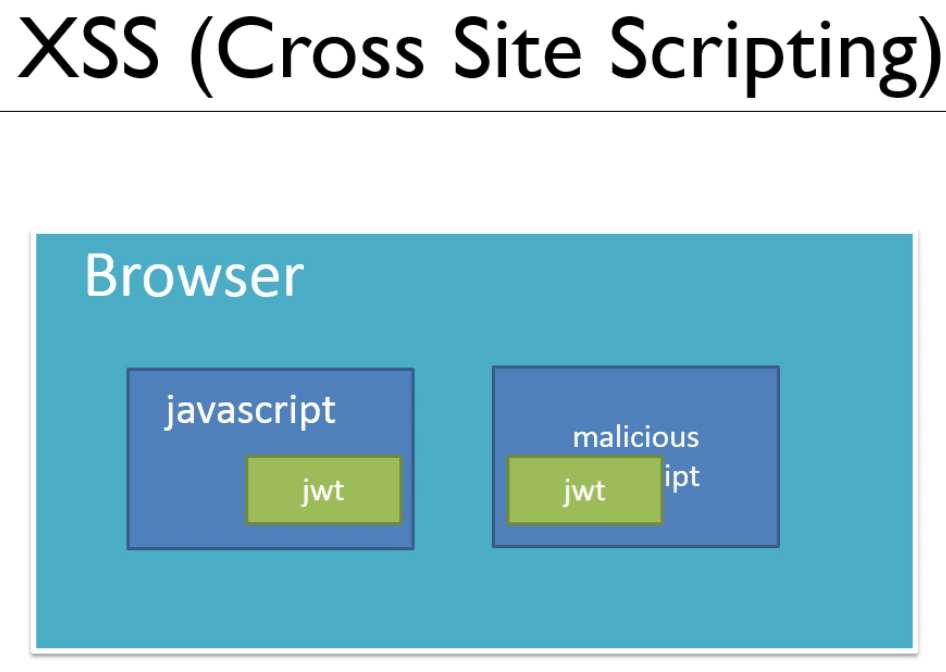
When we refresh the screen the user credentials are lost.

The logon screen is redisplayed.



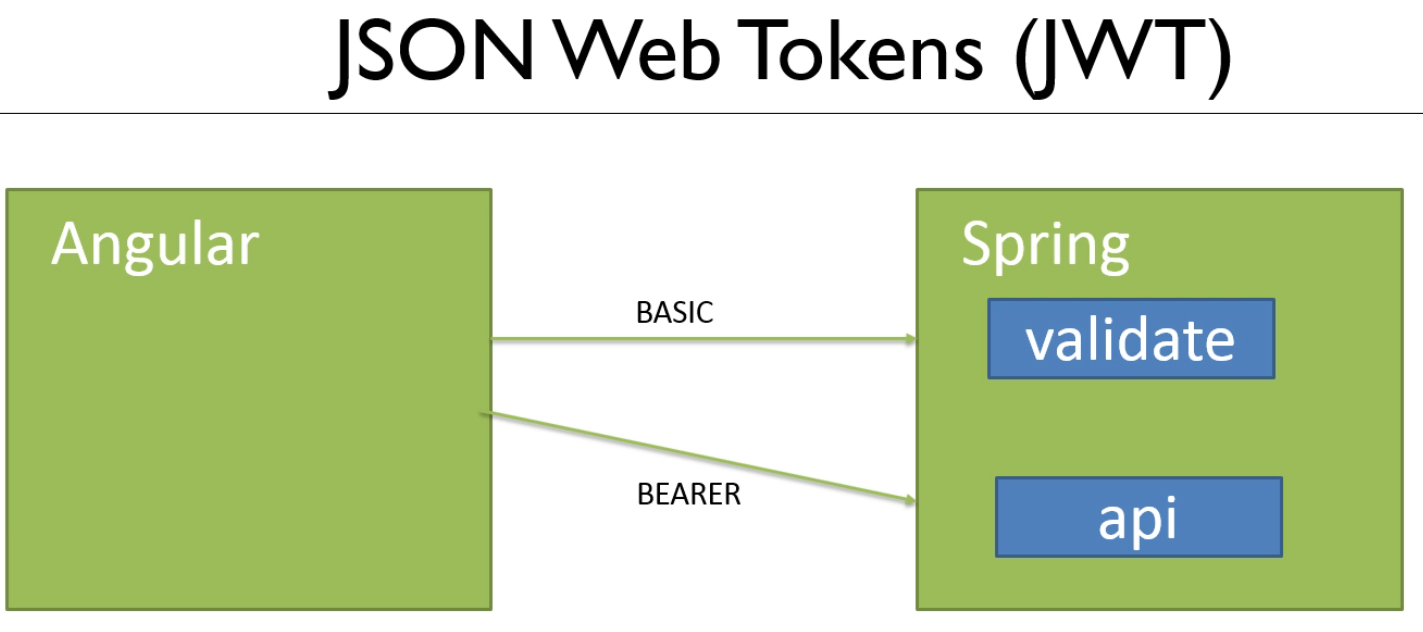
The isAuthenticated is reset to false, and the jwtToken is reset to null.

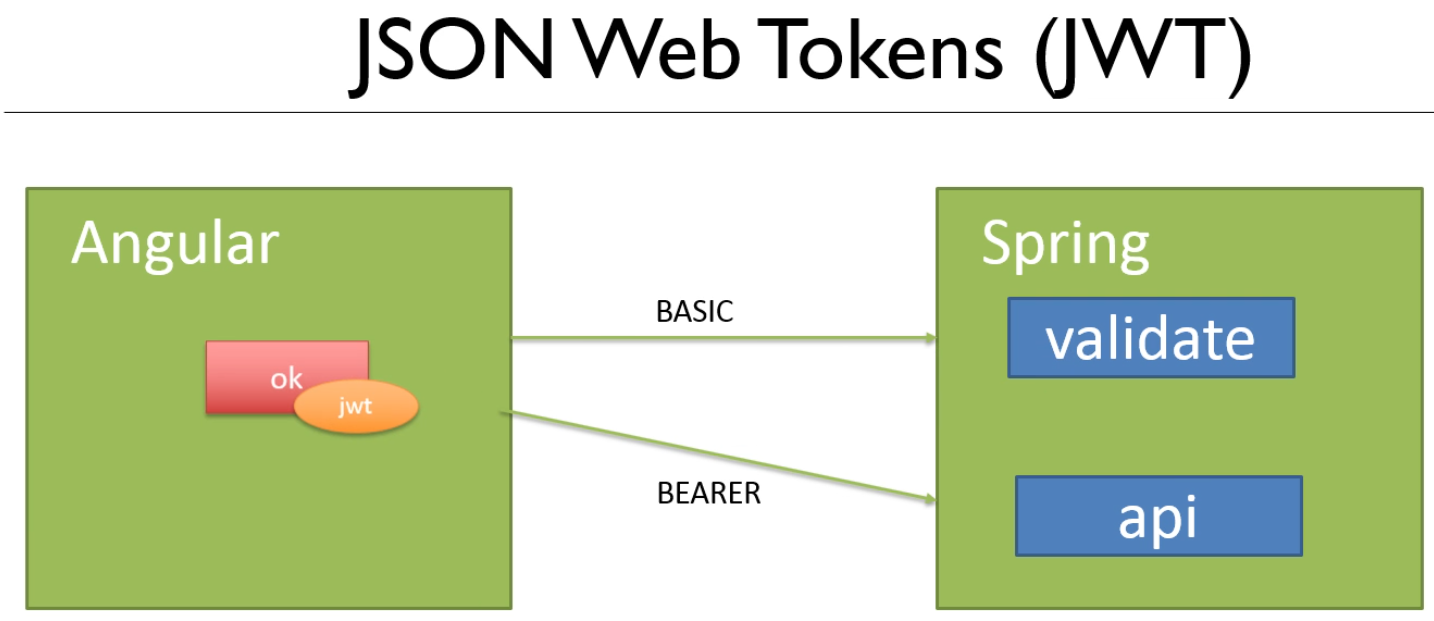




A hacker using a malicious script could capture the jwt and then decode it. XSS Problem

Storing the JWT as a cookie removes the access of javascript.

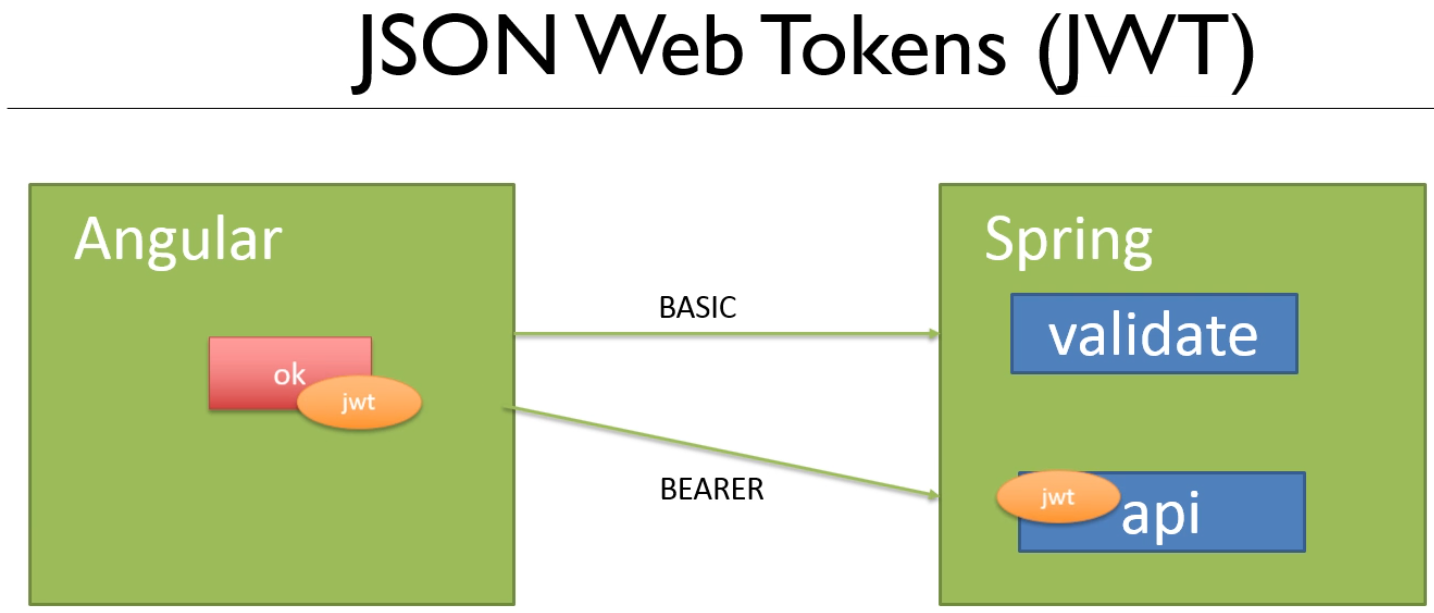




The response ‘ok’ and jwt as a cookie are sent by the server.

This is an HTTPonly cookie, no javascript is sent by the server.

The cookie sends the jwt back to the server automatically.



The cookie is unaffected by refresh

This is the production standard for JWT