Contents

[Security Design Considerations 1](#_Toc81922594)

[Authentication 1](#_Toc81922595)

[Authorization 1](#_Toc81922596)

[Transport Protection 1](#_Toc81922597)

[Cross origin Resource sharing(CORS) 1](#_Toc81922598)

[Cross site request forgery(CSRF) 1](#_Toc81922599)

[Cross site Scripting(XSS) 1](#_Toc81922600)

# Security Design Considerations

## Authentication

## Authorization

## Transport Protection

Just use HTTPS from browser to backend service, or back to backend service calls

Uses SSL protocol – Secured Socket layer(Old)

New is TLS – Transport layer security

SSL Certificates are used

## Cross origin Resource sharing(CORS)

Browsers restrict client side code in being able to make http requests to any site other than site that client code came from

Headers – Access-Control-Allow-Origin

## Cross site request forgery(CSRF)

When using cookies

Forms authentication to secure sessions cookies

Token based protocols eliminate this

## Cross site Scripting(XSS)

Take direct input from user as string and inject it directly into DOM

If input contains expressions or script block, it will get executed or setup event handlers

Angular sanitizes inputs in data binding and escape script blocks

Securing on client side

RouteGuards

Filter data

Page navigation restrictions

Hide/Disable actions

Secure on server side to filter data

Control access to api’s

## OpenID Connect

Assumes you will use oauth for authorization

Same JWT token format

Standardizes flows for collecting credentials from client and issuing tokens

## Oauth2

Authorization

### Identity Provider

Authetication server

Authorization server

SSO Server

STS – security token service

### User Agent

Piece of software the user is interacting with, client app or OS

### Client

### Resource

### Scope

### JWT

# JavaScript

Use noscript tag if you want to show message to the non javascript supported browsers after script tag

If JS has to run on some event, include in head section

Include in body, if script needs to be run when the page loads, no functions

In an external file <script type = “text/javascript” src = filename< </script>

Scope of variables, global scope, local scope