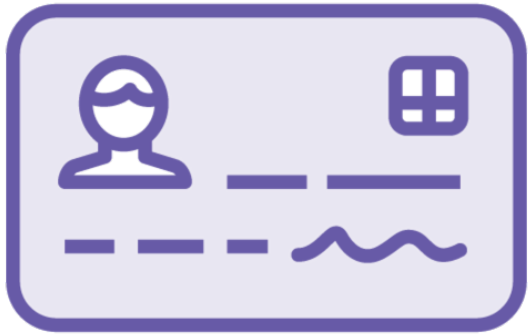
Enhancing with Customizations, Validation and Exception Handling

Oauth2

Open Authorization



OIDC

OpenID Connect

JWT

Jason Web Token

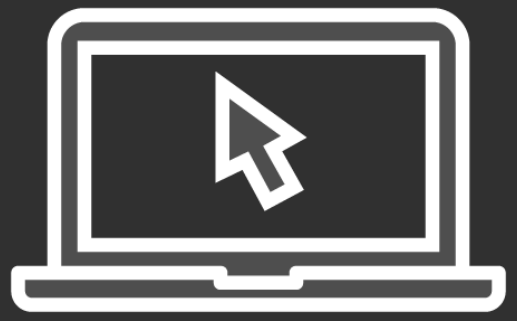
Overview

How to modify the authorization request to the authorization server using a custom: Oauth2AutherizationRequestResolver

Identify and address security vulnerabilities in our application

Why a valid token is not enough for authorization, and how to add additional token validation

Demo

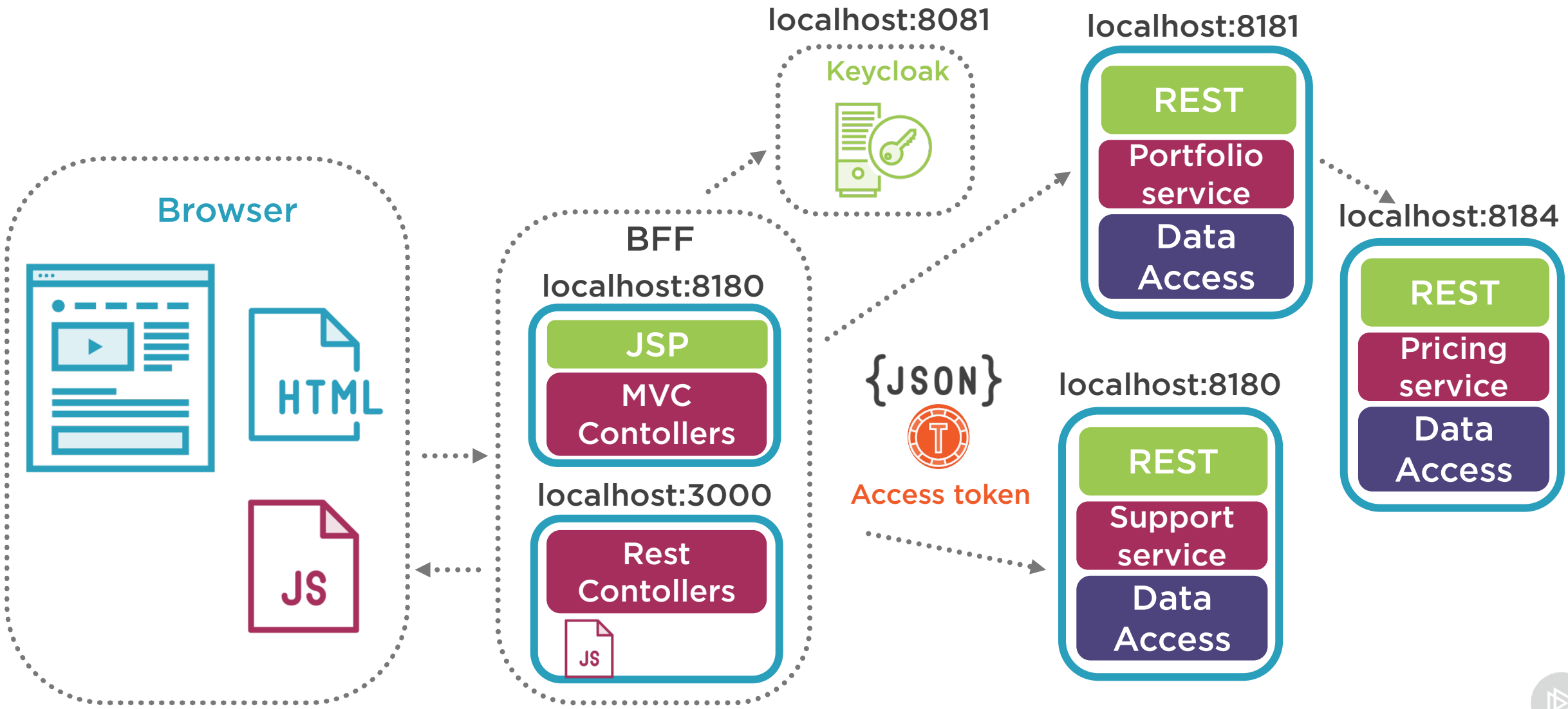


Resource Server

Actions to validate the token:

- Check the signature
- Check token is not expired
- Check if issuer URI was provided check issuer matches

Security Architecture



Module Complete

For authorization, it is not adequate to solely rely on the validity of the access token

Distributed applications are as strong as their weakest link

In addition to the authorization endpoint you can also customize the token endpoint

Use the audience attribute to ensure the token is used in the proper context.

It's important not to get to granular with your audience validation, it should be for who can receive and process the token.