Atividade prática ATVIV

Professor Dr. Eng. Gerson Penha

Softwares sugeridos:

- Eclipse IDE.
- Linguagem Java.
- Spring framework.

Contextualização:

Segurança pode ser definida como ação ou efeito de tornar algo ou a si mesmo seguro, com estabilidade ou firmeza. Também pode-se imputar o significado de estado, qualidade ou condição de quem ou do que está livre de perigos, incertezas, assegurado de danos e riscos eventuais; situação em que nada há a temer.

Quando transportado para o ambiente da computação e sistema de informação o significado de segurança torna-se mais específico, partindo do conceito de segurança da informação.

A segurança da informação está diretamente relacionada com a proteção de um conjunto de informações, dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. Portanto, a segurança da informação é o conceito por trás da defesa dos dados, detalhes e afins para assegurar que eles estejam acessíveis somente aos seus responsáveis de direito ou as pessoas às quais foram enviados. Para isto, seguem-se os seguintes pilares: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Cada pilar descreve um aspecto, que se desdobra em uma junção de partes que vão desde a concepção, chegando ao desenvolvimento e por fim na implantação e disponibilização de um sistema ou aplicação. Dentre estas partes destacam-se dois conceitos denominados de autorização e autenticação.

Autenticação e autorização são dois termos, que correspondem a duas técnicas de aplicação comuns para a maioria dos sistemas de informação e aplicações. Com estas técnicas garante-se mais segurança aos recursos, informações ou dados, que devem ser protegidos.

A autenticação verifica a identidade digital do usuário, ou seja, processo de verificação de uma identidade. Em termos mais simples, é quando o usuário prova de fato quem ele é. Sendo que, para sistemas e aplicações, usuários podem ser pessoas, outras máquinas ou softwares que solicitem comunicação e/ou conexão.

A autorização é o processo que ocorre após validação da autenticação. Diz respeito aos privilégios, que são concedidos a determinado usuário ao utilizar uma aplicação ou sistema. Serve para verificar se determinado usuário terá permissão para acessar, incluir ou modificar alguma informação/dado. Também, defini quais ações o usuário pode executar, o que é de fundamental importância dentro de uma aplicação ou sistema.

Quando se entra na ceara de micro-serviços percebe-se mais de uma forma de implementar autenticação e autorização, mas, uma comum é conhecida como Json Web Token (JWT). O JWT é um padrão da Internet para a criação de dados com assinatura opcional e/ou criptografia cujo carga contém o JSON, que armazena um determinado número de informações. Este JSON é transmitido no cabeçalho das requisições como um token, uma cadeia de caracteres criptografada. Os tokens são assinados usando um segredo privado ou uma chave pública/privada.

Atividade:

Dado que a “atualização base” foi concluída, o próximo passo é implementar a “atualização segurança”, que consiste em incluir no sistema o processo de autenticação e autorização via Json Web Token (JWT).

A implementação da “atualização segurança” é fundamental, lembre-se que os investidores são dois grupos empresariais com exigências de nível internacional. Sem adição de segurança o possível aporte dos investidores será cancelado.

Os investidores sugeriram um padrão para os perfis de usuários e suas autorizações. Este padrão é o utilizado no sistema atual da maioria das lojas da Toyota. Os perfis e suas autorizações são descritos na Tabela 1.

Tabela 1. Perfis de usuários.

Perfil	Autorizações
Administrador	Autorização para fazer todas as operações de CRUD na aplicação, incluindo adicionar ou remover usuários administradores.
Gerente	Autorização para fazer todas as operações de CRUD sobre usuários dos perfis gerente, vendedor e cliente. Autorização para fazer todas as operações de CRUD sobre serviços, vendas e mercadorias.
Vendedor	Autorização para fazer todas as operações de CRUD sobre usuários do perfil cliente. Autorização para ler informações sobre serviços e mercadorias. Autorização para criar vendas feitas por si mesmo e ler suas informações.
Cliente	Autorização para ler informações sobre o seu próprio cadastro. Autorização para ler informações de vendas das quais o usuário foi consumidor.

Para auxiliar na implementação a equipe de engenharia de software da Toyota disponibilizou um modelo de projeto, que está incompleto, mas pode auxiliar no desenvolvimento. O modelo de projeto foi disponibilizado em um repositório remoto, que está disponível pelo endereço: https://github.com/gerson-pn/atviv-autobots-microservico-spring ou pela Figura 1.

Figura 1. Modelo de projeto, com implementação de autenticação e autorização