APIs WEB Segura

Como aplicar o spring-security corretamente

****

**Antonio Luis Reuter Andrade**

aandrade@avenuecode.com

Antonio Reuter é bacharel em Ciências da Computação pela Faculdade Ruy Barbosa. Trabalha com desenvolvimento de sistemas desde 2000, utilizando Java e JEE. Atualmente é consultor da AvenueCode trabalhando em projetos envolvendo Java/JEE e Ruby on Rails no e-commerce do Walmart.

Cenário

Nesse artigo iremos abordar como tornar uma API WEB segura, através do spring-security. Utilizaremos como base a API de uma loja virtual fictícia, demonstrando passo a passo como blindá-la da maioria dos tipos de ataque, além de apresentar os erros mais comuns ao tentar nesse caminho para torna-la impenetrável.

Introdução

*<< discutir sobre o problema que será tratado no artigo>>*

Neste artigo iremos abordar como tornar a API de uma loja virtual segura, uma vez que o dono da loja deseja expô-la na WEB para que seus parceiros comerciais consigam integrar em suas plataformas. Apresentaremos os erros mais comuns e como evita-los.

*<< descrever brevemente a solução comumente utilizada e que está inadequada >>*

A aplicação do nosso cliente já faz uso do spring-security, uma vez que a API em questão já vinha sendo utilizada internamente para permitir a integração com outros sistemas internos, contudo ao tentar disponibiliza-la na WEB algumas medidas precisam ser adotadas.

*<< descrever brevemente a solução que resolve o problema de uma forma mais adequada >>*

Para garantir que nossa API continue segura, e que os dados dos nossos clientes não fiquem expostos precisamos realizar alguns ajustes simples mas que farão toda a diferença, na tentativa de evitar que usuários maliciosos tentem acessar nossa aplicação.

*<<Cenário para analisar o problema e a solução>>*

Disponibilizando a API da Macaxeira Online na WEB

*<<descrever em detalhes o estudo de caso que será utilizado para analisar a “má prática” e a “boa prática”>>*

Os donos do Macaxeira Online resolveram expor sua API na WEB para alguns de seus parceiros comerciais. Eles reclamavam que desejavam acessar a API da loja virtual a fim de facilitar a integração nas suas plataformas.

O arquiteto do sistema avaliou a demanda e resolveu publicar a API de imediato para os parceiros comerciais, uma vez que a mesma já existia a já vinha sendo utilizada há algum tempo em integrações com outros sistemas internos da companhia.

A equipe de segurança, todavia, ainda precisava avaliar a aplicação, para garantir que a mesma estaria protegida de possíveis ataques. Ao final da análise um relatório deveria ser gerado informando os pontos de não conformidade e sugestões de melhorias.

*<<Estudo de caso considerando a má prática>>*

Relatório de Segurança

*<<descrever em detalhes o desenvolvimento do estudo de caso considerando a forma inadequada>>*

*<<deixar claro os problemas trazidos com o uso da má prática>>*

O time de segurança realizou uma análise detalhada do sistema e encontrou alguns pontos que precisavam ser corrigidos antes de disponibilizar para os usuários externos. O time de desenvolvimento foi chamado para entender melhor a questão.

O arquiteto não entendia como era possível a aplicação ainda apresentar brechas de segurança uma vez que eles estavam utilizando o *spring-security*. A API já vinha sendo consumida por outros sistemas internos havia pelo menos 1 ano.

No relatório foram reportados os seguintes tópicos:

1. problemas na autenticação;
2. problemas de autorização;
3. problemas de auditoria;
4. URL exposta;
5. dados sensíveis trafegando sem criptografia;
6. dados do usuário exposto de forma indevida.

O primeiro ponto levantado foi referente a forma como a autenticação estava sendo realizada. Eles encontraram um arquivo de texto dentro da aplicação contendo os dados do usuário e senha. Foi informado para o time de desenvolvimento que qualquer usuário mal intencionado que tivesse acesso ao arquivo obteria as credencias necessárias para se logar na aplicação.

**Listagem 1**. Arquivo de configuração da aplicação: application.properties

...

api.user=macaxeira

api.senha=1234

...

Além do fato do arquivo estar com os dados em um arquivo texto

**Estudo de caso considerando a boa prática**

* descrever em detalhes o desenvolvimento do estudo de caso considerando a forma adequada
* deixar claro as vantagens trazidas com o uso da boa prática

**Entendendo o porquê desta ser a melhor solução**

* comparar: boa prática VS má prática