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 para alguns 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.

Dentre os pontos levantados como restrição para liberar o acesso para terceiros alguns pontos foram levantados, dentre eles a questão da segurança. O arquiteto argumentou que eles já utilizavam o spring-security, portanto a API já estava segura, não sendo portanto um empecilho para o lançamento.

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

1, 2, 3... No ar

*<<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 responsável pela API enfim publicou na data acordada; afinal de contas, não foi necessário grandes ajustes. Os parceiros comerciais começaram a usar a aplicação e integrar em suas plataformas.

Depois de alguns meses de funcionamento a equipe verificou que informações confidencias dos clientes estavam vazando, além de estarem sofrendo alguns ataques (especificar possíveis tipos de ataques). Além disso, um DBA que havia sido demitido recentemente havia recuperado o acesso de alguns dos usuários da API antes de deixar a empresa, com a intenção de sabotar futuramente companhia.

Ora se a aplicação já utilizava o spring-security não haviam motivos para preocupação, afinal de contas ela já estava segura!

Uma empresa especializada em segurança foi então contratada para realizar uma análise do que poderia estar acontecendo na Macaxeira Online. Eles começaram então a realizar um raio-x da aplicação em busca de possíveis brechas, a fim de poder gerar um relatório com um plano de ação para sanar os problemas.

Eles constataram que ao implantarem o spring-security na API, quando o seu uso era apenas de caráter corporativo, alguns pontos na sua configuração passaram desapercebidos. Contudo, até aquele momento aquilo não chegava a representar um problema iminente, uma vez que ela só vinha consumida dentro da própria empresa, sendo acessada apenas por alguns sistemas internos, além do fato de rodar atrás de um firewall.

**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