**Sobre o Spring Security, julgue a alternativa correta:**

* Para adicionarmos um nível de segurança em uma aplicação Spring Boot é necessário apenas importar o Starter do Spring Security.
* O starter é:   
  <dependency>  
   <groupId>org.spring.boot</groupId>  
  <artifactId>spring-boot-starter-security</artifactId>   
  </dependency>
* Para criar mais de um usuário e perfis de acesso em memória, não é necessário criar uma classe que estenda WebSecurityConfigurerAdapter.
* {bcrypt} BCryptPasswordEnconder é a única implementação de criptografia realmente segura.
* Nenhuma das alternativas.

**Sobre o Spring Security, julgue a ALTERNATIVA INCORRETA:**

* Default o Spring Security não possui um usuário padrão chamado User e toda vez que sua aplicação é iniciada ele gera uma senha aleatória no console.
* Função refere-se a um grupo de permissões do usuário autenticado
* Em um projeto Spring Boot Web você precisa somente incluir a dependência no pom.xml.
* Autoridade concedida refere-se à permissão do usuário autenticado.
* Nenhuma das Alternativas.

**Dentre as alternativas abaixo, qual delas traz a definição da “JWT”?**

* É basicamente um formato leve de troca de informações/dados entre sistemas.
* Nenhuma das alternativas.
* É muito útil para lidar com exceções quando você tem vários controladores REST API fazendo muitos trabalhos diferentes.
* É um esquema de gerenciamento de memória pelo qual um computador armazena e recupera dados de um armazenamento secundário para uso na memória principal.
* É uma estratégia para realizar autenticação entre duas partes por meio de um token assinado que autentica uma requisição Web. Além disso, um token JWT também pode conter informações relacionadas à autorização.

**Qual das alternativas abaixo contém o Starter correto para importarmos a dependência referente ao Spring Security?**

* Nenhuma das alternativas.
* <dependency>  
   <groupId>org.springframework.boot</groupId>   
   <artifactId>spring-boot-starter-security</artifactId>  
   </dependency>
* <dependency>   
   <groupId>org.springboot.framework</groupId>  
   <artifactId>spring-boot-starter-security</artifactId>  
  </dependency>
* <dependency>  
   <groupId>org.springframework.boot</groupId>  
   <artifactId>spring-boot-test-security</artifactId>  
   </dependency>
* <dependency>  
   <groupId>org.spring.boot</groupId>   
   <artifactId>spring-boot-starter-security</artifactId>   
  </dependency>

**I. Refere ao processo de verificação da identidade de um usuário, com base nas credenciais fornecidas. II. Refere ao processo de determinar se um usuário tem permissão adequada para executar uma ação específica ou ler dados específicos Sobre as terminologias do Spring Security, estamos falando respectivamente de:**

* Nenhuma das alternativas.
* Autenticação e Autorização.
* Princípio e Autoridade concedida.
* Autorização e Autenticação.
* Função e Permissão.

**Qual das alternativas abaixo contém o Starter correto para importarmos a dependência referente ao JWT?**

* <dependency>   
  <groupId>io.jsonwebtoken</groupId>   
  <artifactId>Spring-boot-starter-security</artifactId>   
  <version>0.7.0</version>   
  </dependency>
* <dependency>   
  <groupId>io.jsonwebtoken</groupId>  
   <artifactId>spring-boot-starter-security</artifactId>   
  </dependency>
* Nenhuma das Alternativas.
* <dependency>   
  <groupId>io.jsonwebtoken</groupId>   
  <artifactId>jjwt</artifactId>   
  <version>0.7.0</version>   
  </dependency>
* <dependency>   
  <groupId>io.springframework.jsonwebtoken</groupId>   
  <artifactId>jjwt</artifactId>   
  <version>0.7.0</version>   
  </dependency>

**Para que serve a anotação @PreAuthorize?**

* Fornece controle de acesso baseado em expressão. Verifica a expressão fornecida depois de inserir o método.
* É usado para especificar uma lista de funções em um método.
* Fornece controle de acesso baseado em expressão. Verifica a expressão fornecida antes de inserir o método.
* Nenhuma das alternativas.
* Filtrar um argumento de coleção antes de executar o método.

**Qual o tipo de autorização devemos utilizar quando queremos fazer uma autenticação básica de um usuário?**

* OAuth2
* Basic Auth
* Nenhuma das alternativas.
* Bearer Token
* API key

**A interface \_\_\_\_\_\_\_\_\_\_\_\_ é usada para recuperar dados relacionados ao usuário. Estamos falando de qual interface?**

* CrudRepository
* UserDetailsService
* PagingAndSortingRepository
* JpaRepository
* Nenhuma das Alternativas.

**Para obter os dados do usuário em memória, devemos sobrescrever o método “configure” estendida da classe WebSecurityConfigurerAdapter. Para tal, qual argumento este método recebe?**

* Nenhuma das alternativas.
* AuthenticationManagerBuilder auth
* HttpServletRequest request
* HttpSecurity http
* WebSecurity web