Need for securing RestFul services arises when the authorized entities alone have to access to the end points

We can secure Spring REST endpoints using ,

1st : Basic Authentication 2nd : OAUTh2 authentication

Basic Authentication : When client requests for a protected resource , server demands the client to supply the authentication credentials . client will get the requested resource only when the credentials pass authentication at server side .

Like wise when we do it from postman , we need to give basic auth like username and password

Steps :

1st : client request a protected resource = > 2nd : Server requests UserName and password = > 3rd : client sends username and password = > 4th : server returns requested resource

With Basic Authentication in place , clients send their Base64 encoded credentials with each request Using HTTP Authorization header .

This type of authentication does not mandate us to have any loging page which is the very standard way of authenticating the client request in any web application . In addition , there is no need to store credentials or any related info in the session .

Dependency : spring-boot-starter-security : this is used to apply spring security in RestApi .

**Steps : how to apply basic authentication in web application or RESTful API**

**1st : we need to make a configuration class with @Configuration annotation 2nd:**