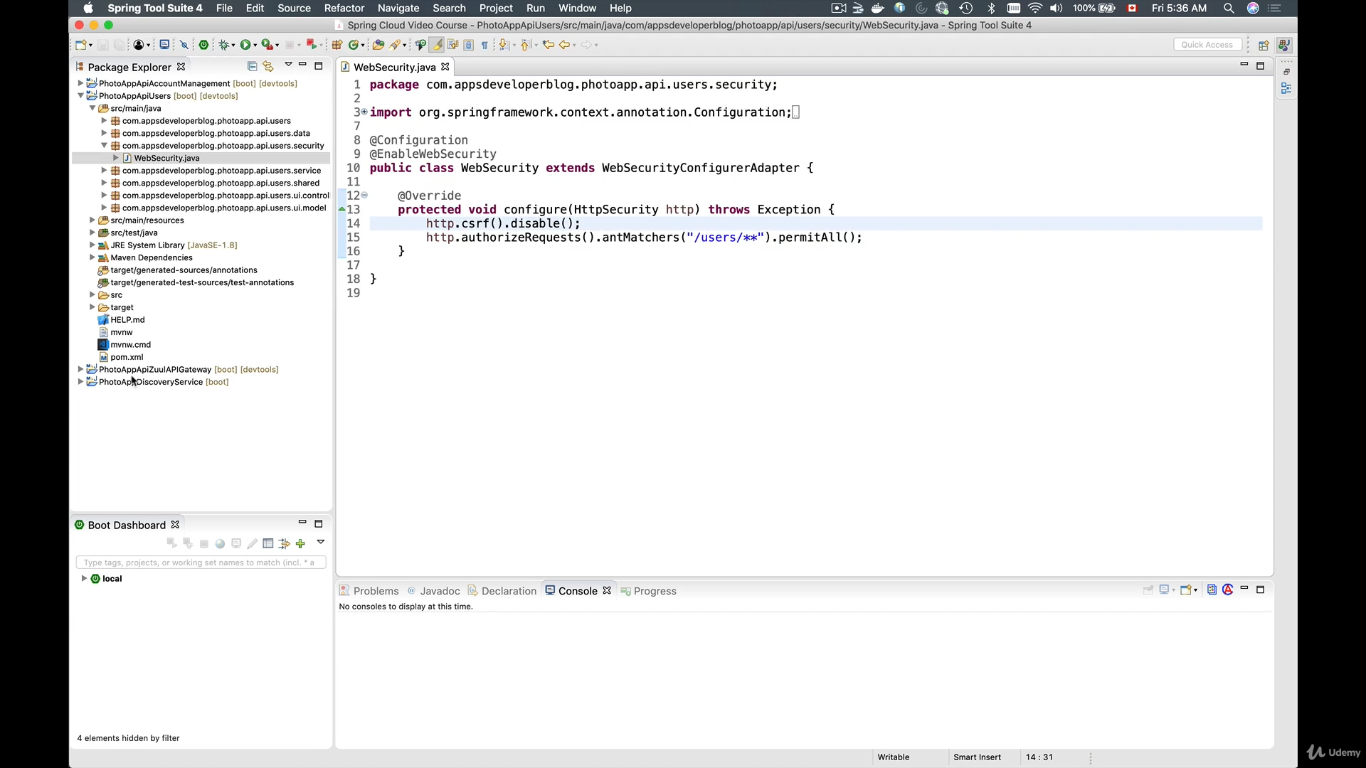
1. Create “User” model class.
2. Validate http request with hibernate validator
3. Create DTO’s

“UserModelRest”🡪”UserRestController”🡪”UserDto”🡪”UsersService”🡪”UserDto”🡪”UserEntity”🡪”UserRepository”🡪”DB”.

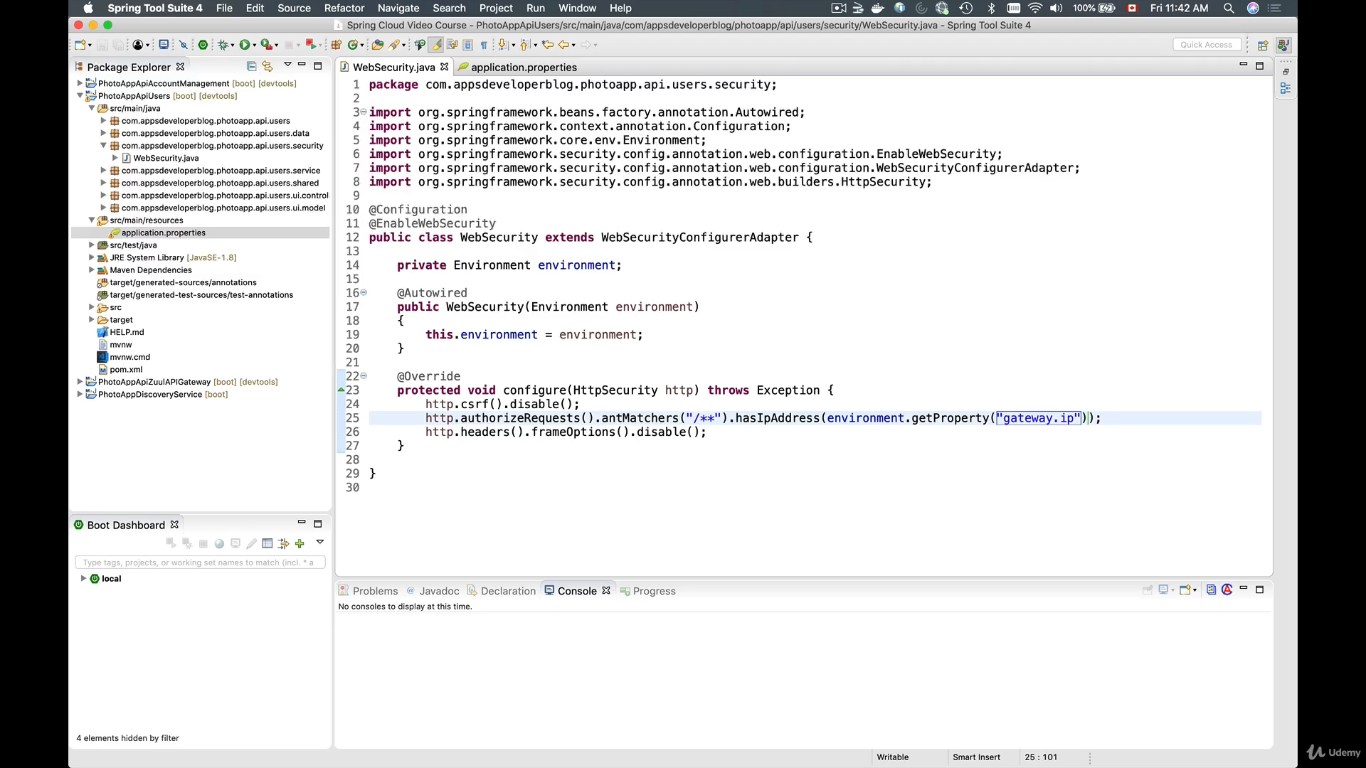
1. Every user we store in a DB should have a unique user id, so generate “UUID.Random().tostring”. We will use this id to pass and delete a user instead of DB id, as DB id is auto incremented and easy to guess.
2. Implement Service class
3. Create DataJpa repository
4. Create entity class
5. Return Http Status code.
6. Enable Security
7. Add spring security dependency
8. Add webSecurity Configuration



Since we are using jwt we are disabling csrf and with permit all we are a kind of disabling the security.

1. Inject the bcrypt dependency and encode the password.
2. Add the bcrypt bean in security config file.
3. Use the ModelMapper class to copy the dto class object to entity class.
4. Save to database(H2).
5. In order to allow only IP address of API Gateway, remove permitAll() method from configuration and add antMatcher(“/\*\*”)

hasIpAddress() method.



1. Add fasterxml.jackson.dataformat dependency to consume/produce the input/ output in xml and Json Format.
2. 