**MODULE 4**

**AUTHENICATION & AUTHORIZATION**

TASK 1 (pp. 1 - 3)

Create a simple Spring Web application with endpoint /study/v1/info with returns simple text:

A screenshot of a computer

Description automatically generated

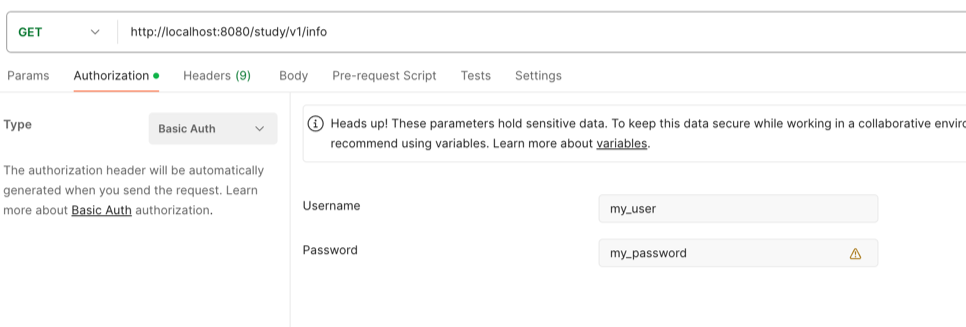
After added spring security dependency and configuration of web security context:

A screenshot of a computer

Description automatically generated

Endpoint stopped being available without authorization.

After adding authorization header with correspondent data:



Endpoint started being available back:

A screenshot of a computer

Description automatically generated

TAKS 2 (pp. 4-6)

In-Memory auth does not work anymore:

A screenshot of a computer

Description automatically generated

Havin provided correct credentials we get access to endpoint:

A screenshot of a computer

Description automatically generated

Now let’s try to login under admin user with incorrect password:

A screenshot of a computer

Description automatically generated

And providing correct password we get access to the endpoint under admin user:

A screenshot of a computer

Description automatically generated

BUT, still the password is used as plain text what’s insecure.

A screenshot of a computer

Description automatically generated

Having installed Spring CLI and executed password encode commands:

A screenshot of a computer program

Description automatically generated

So, now we can store the password in encoded format as bcrypt. Let’s update Liquibase script to replace password field.

Database table with users looks as follows:

A screenshot of a computer

Description automatically generated

Testing endpoint. With correct credentials for ADMIN user:

A screenshot of a computer

Description automatically generated

With incorrect credentials:

SA user

A screenshot of a computer

Description automatically generated

Admin user:

A screenshot of a computer

Description automatically generated

And with correct credentials for SA user:

A screenshot of a computer

Description automatically generated

Introducing new endpoint /study/v1/about with non-authenticated access:

A screenshot of a computer

Description automatically generated

Trying to call /study/v1/info in non-authenticated mode:

A screenshot of a computer

Description automatically generated

DENIED!

Setting up authentication mode ad providing credentials:

A screenshot of a computer

Description automatically generated

TASK 3 (pp. 7-11)

Arranged endpoints with the following authorizations:

/study/v1/about – non-authenticated mode

/study/v1/info – authenticated mode + requires role VIEW\_INFO

/study/v1/admin – authenticated mode + requires role VIEW\_ADMIN

The following users are pre-created and stand for verifications:

‘user\_view’ has role VIEW\_INFO

‘user\_admin’ has role VIEW\_ADMIN

‘user\_view\_admin’ has roles VIEW\_INFO + VIEW\_ADMIN

1. Endpoint ‘about’ does not require authentication:

A screenshot of a computer

Description automatically generated

1. Endpoint ‘info’ requires authentication and role VIEW\_INFO:

Users ‘user\_view’ and ‘user\_view\_admin’ can access it:

‘user\_view’ accesses:

A screenshot of a computer

Description automatically generated

‘user\_admin’ can’t access:

A screenshot of a computer

Description automatically generated

‘user\_view\_admin’ accesses:

A screenshot of a computer

Description automatically generated

1. Endpoint ‘admin’ requires authentication and role VIEW\_INFO:

Users ‘user\_admin’ and ‘user\_view\_admin’ can access it:

‘user\_view’ can’t access:

A screenshot of a computer

Description automatically generated

‘user\_admin; accesses:

A screenshot of a computer

Description automatically generated

‘user\_view\_admin’ accesses:

A screenshot of a computer

Description automatically generated

Having created Login form and configured Web Security to handle it for login and logout actions:

A screenshot of a computer

Description automatically generated

Providing incorrect credentials get error:

A screenshot of a computer

Description automatically generated

Populating with correct credentials:

A screenshot of a computer

Description automatically generated

We are redirected to page under authorization:

A computer screen shot of a computer

Description automatically generated

Logout will get us back to login page:

A screenshot of a computer

Description automatically generated

Demonstrating brute force protector.

Application property has setting of maximum login failure attempts as 3 times.

A screenshot of a computer

Description automatically generated

After 2 attempts of login with incorrect password user is not in blocked list:

A screenshot of a computer

Description automatically generated

Having made only at least 3 attempts for user ‘admin’ to enter password incorrectly we got that ‘admin’ is blocked.

A screenshot of a computer

Description automatically generated

Blocking is limited with 5 minutes.

It’s set in application properties:

A screenshot of a computer

Description automatically generated

So, at 15:39:17 user admin is activated again and goes from blocked list.

A screenshot of a computer

Description automatically generated

Still here as time has not passed.

A screenshot of a computer

Description automatically generated

Still blocked as time has not come yet.

And at expected time user admin goes unlocked.

A screenshot of a computer

Description automatically generated