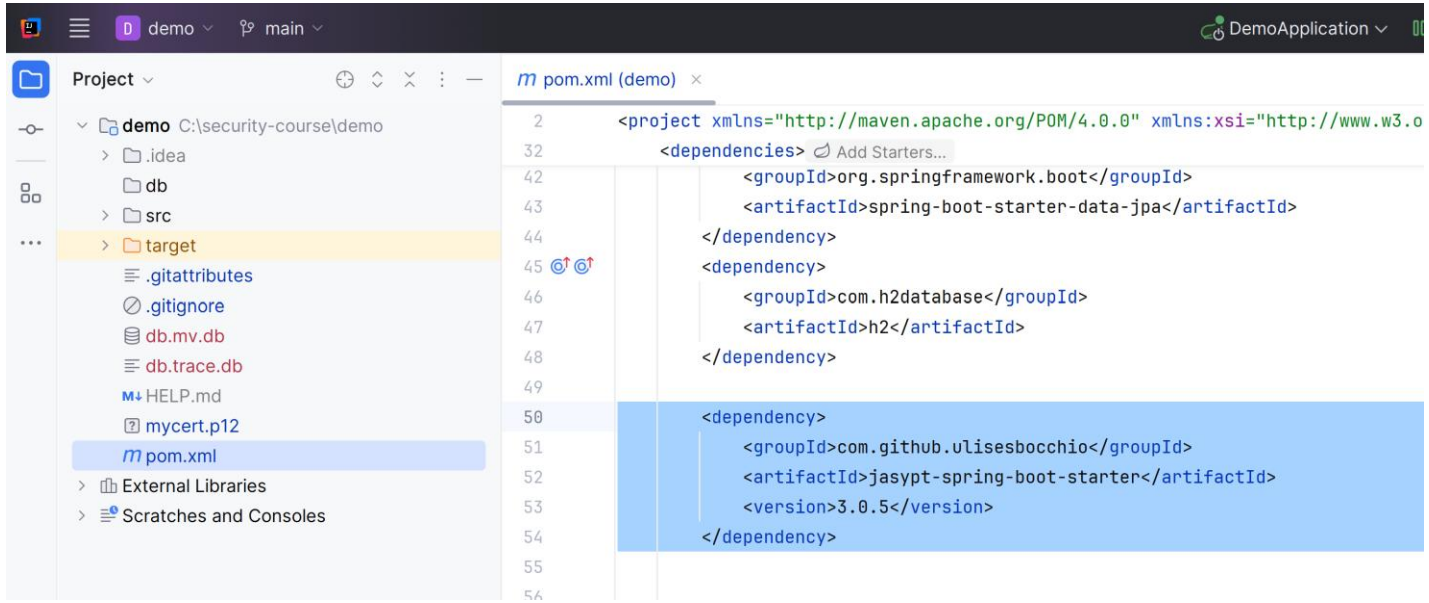
Security - Hands-On 3
springboot credential configuration (Jasypt, spring cloud, Vault)

Esilv 2025

arnaud.nauwynck@gmail.com

Using Jasypt springboot to encrypt configuration properties

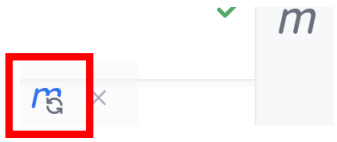
Jasypt [1/7] : adding maven pom.xml dependency



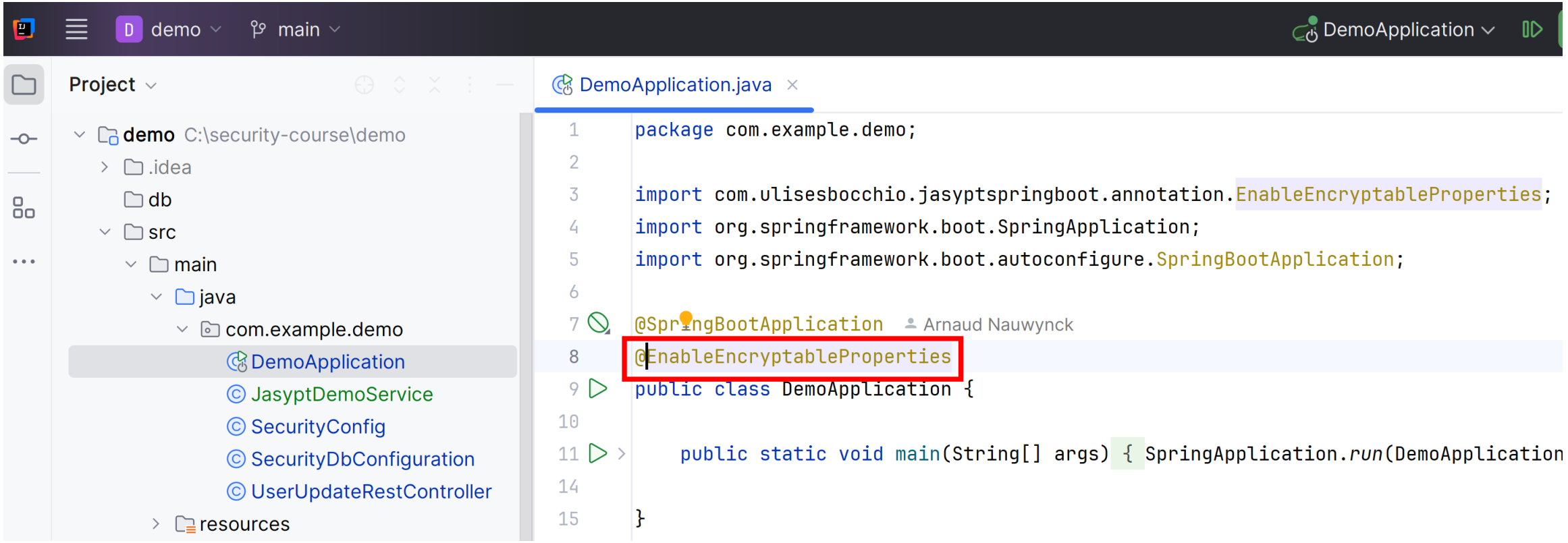
edit pom.xml, add in <dependencies>..

```
<dependency>
    <groupId>com.github.ulisesbocchio</groupId>
    <artifactId>jasypt-spring-boot-starter</artifactId>
    <version>3.0.5</version>
</dependency>
```

then click on Refresh maven

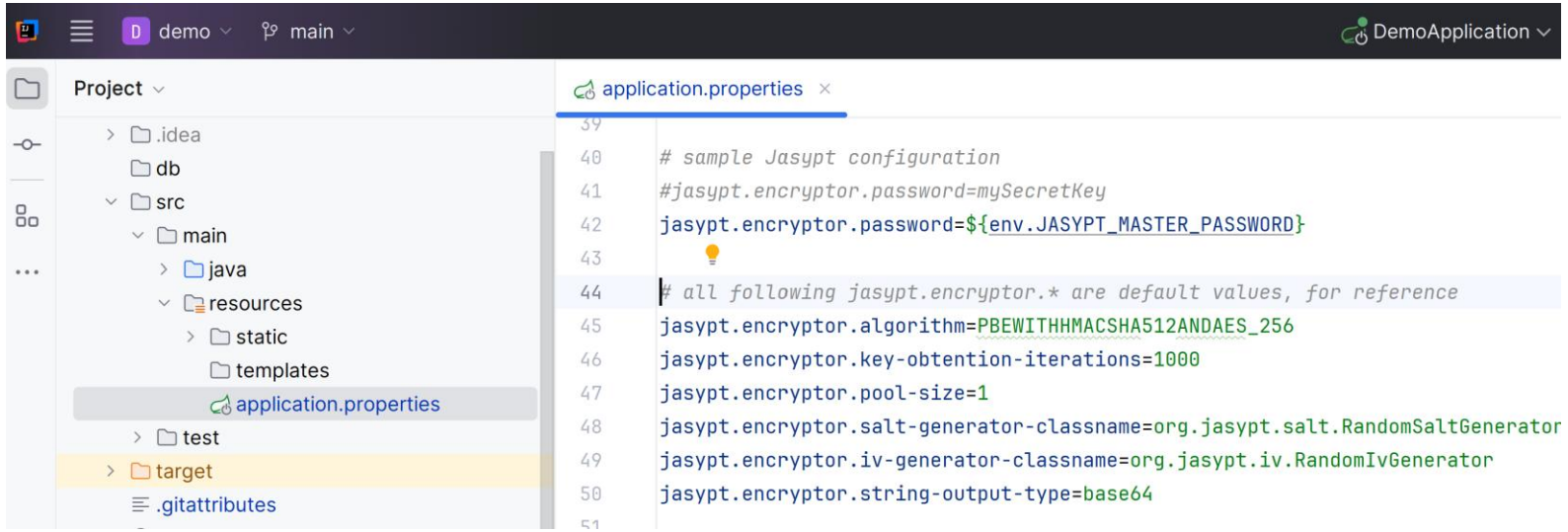


Jasypt [2/7] : Configure App to use EncryptableProperties



add
@EnableEncryptableProperties
to your app (on a the class main @SpringBootApplicatino or on any @Configuration class)

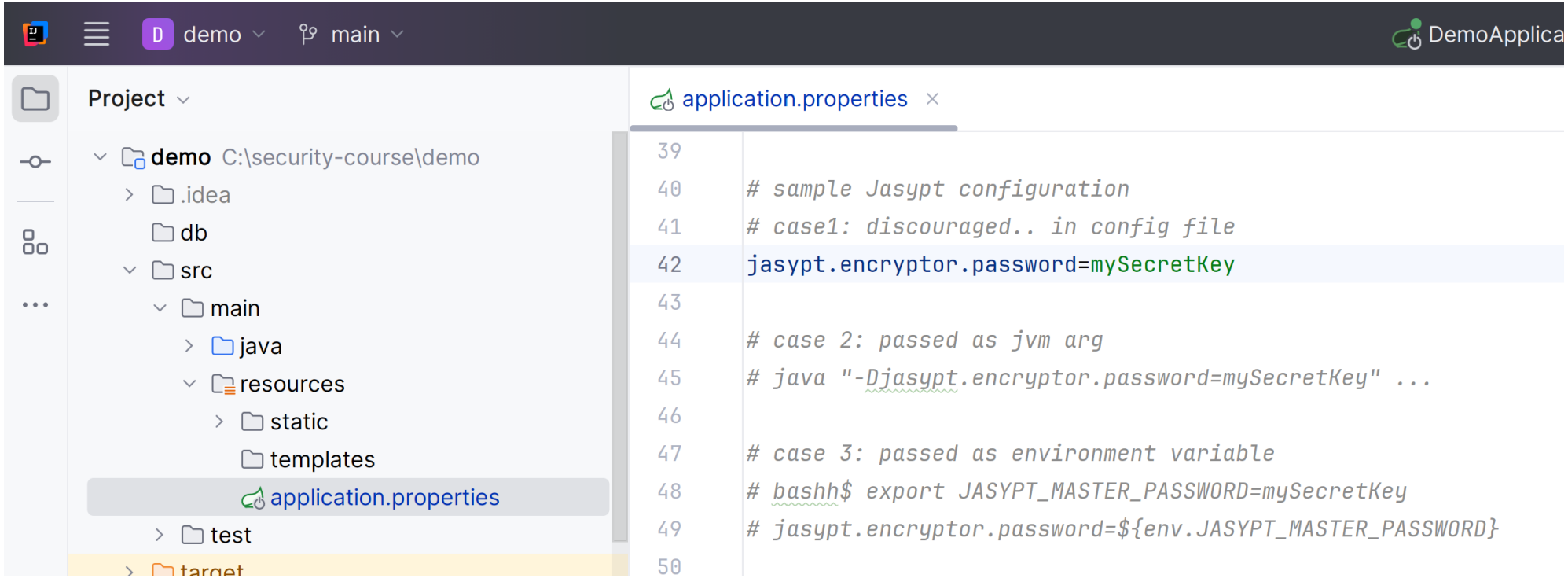
Jasypt [3/7] : default config of Jasypt Encryptor in application.properties



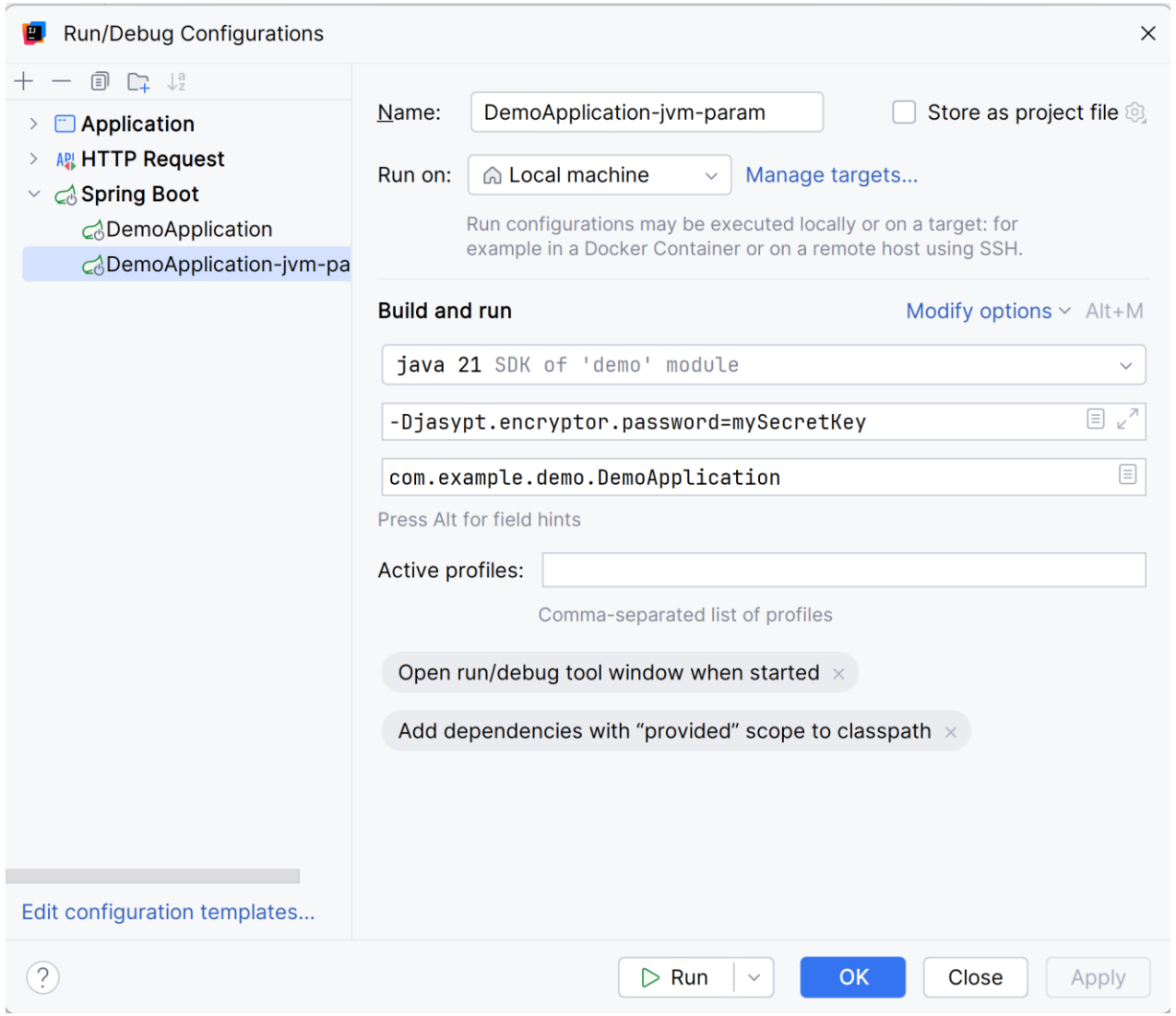
edit file
src/main/resources/application.properties

 # all following jasypt.encryptor.* are default values, for reference
jasypt.encryptor.algorithm=PBEWITHHMACSHA512ANDAES_256
jasypt.encryptor.key-obtention-iterations=1000
jasypt.encryptor.pool-size=1
jasypt.encryptor.salt-generator-classname=org.jasypt.salt.RandomSaltGenerator
jasypt.encryptor.iv-generator-classname=org.jasypt.iv.RandomIvGenerator
jasypt.encryptor.string-output-type=base64

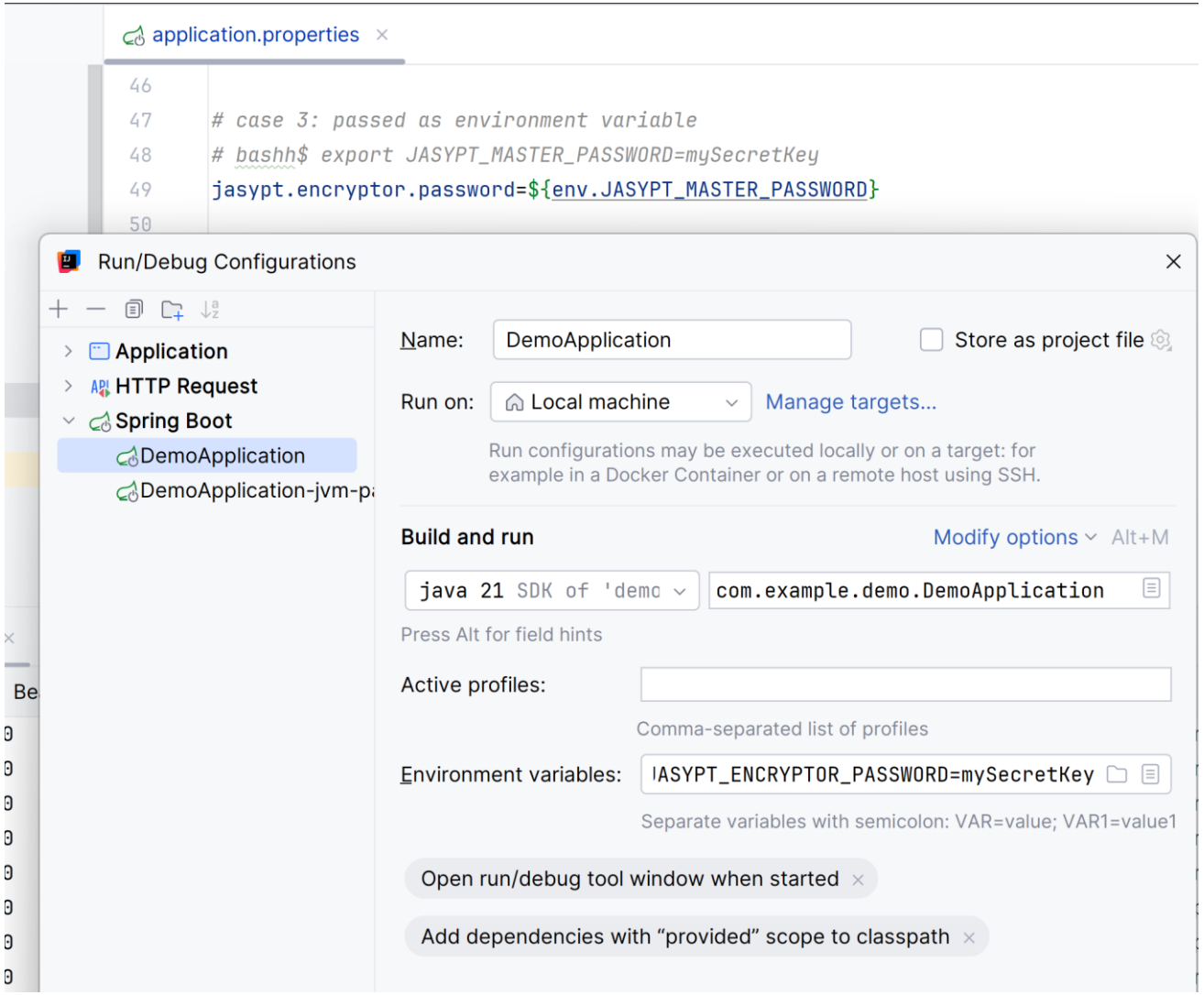
Jasypt [4/7] case 1: simpler (but not recommended) add jasypt encryptor password in configuration file



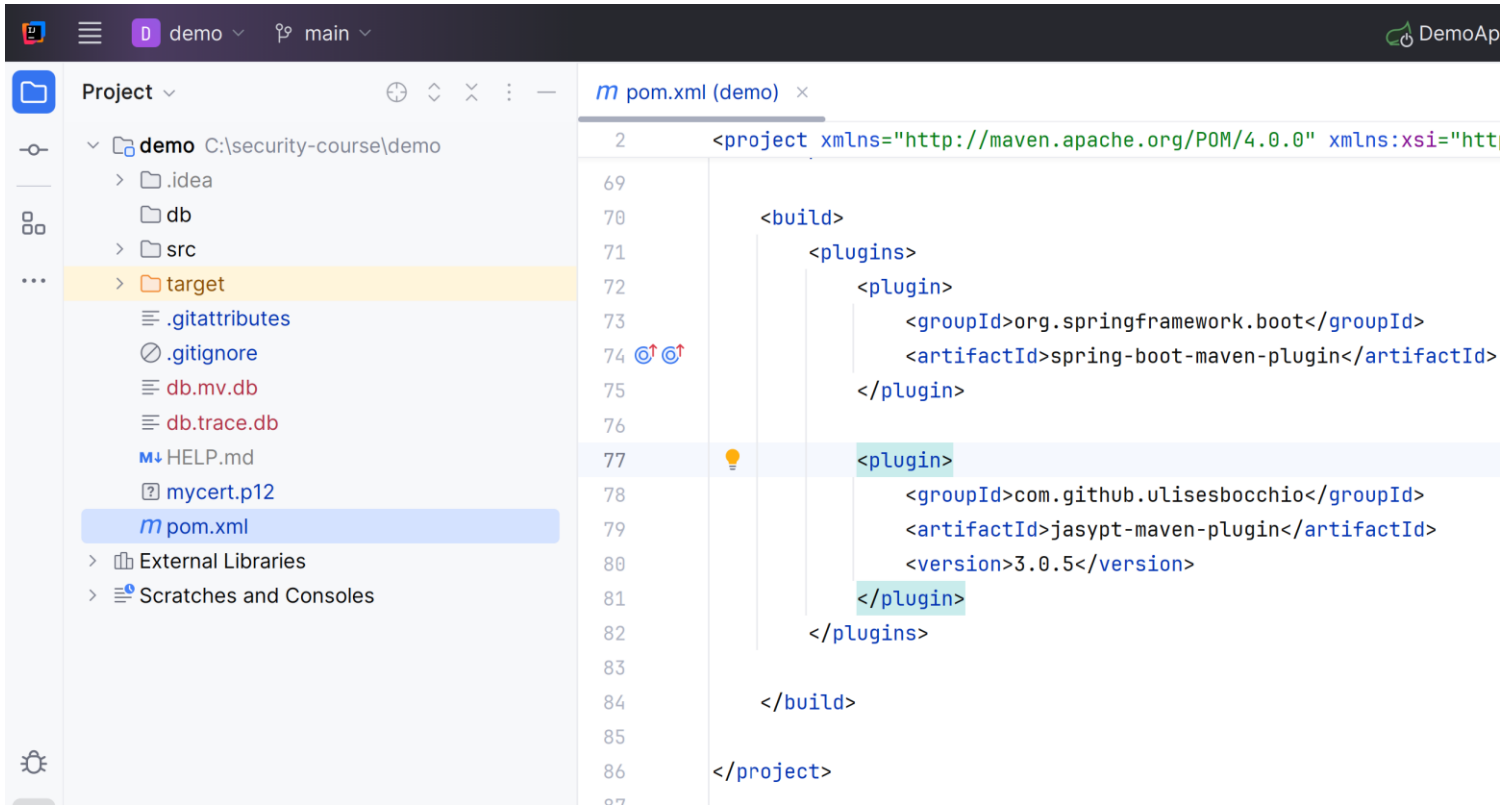
(Optionnal) Jasypt [4/7] case 2: with JVM param -Djasypt.encryptor.password=...



(Optionnal) Jasypt [4/7] case 3: with ENVIRONMENT variable + conf



Jasypt [6/7] : compute the encryption of a secret value



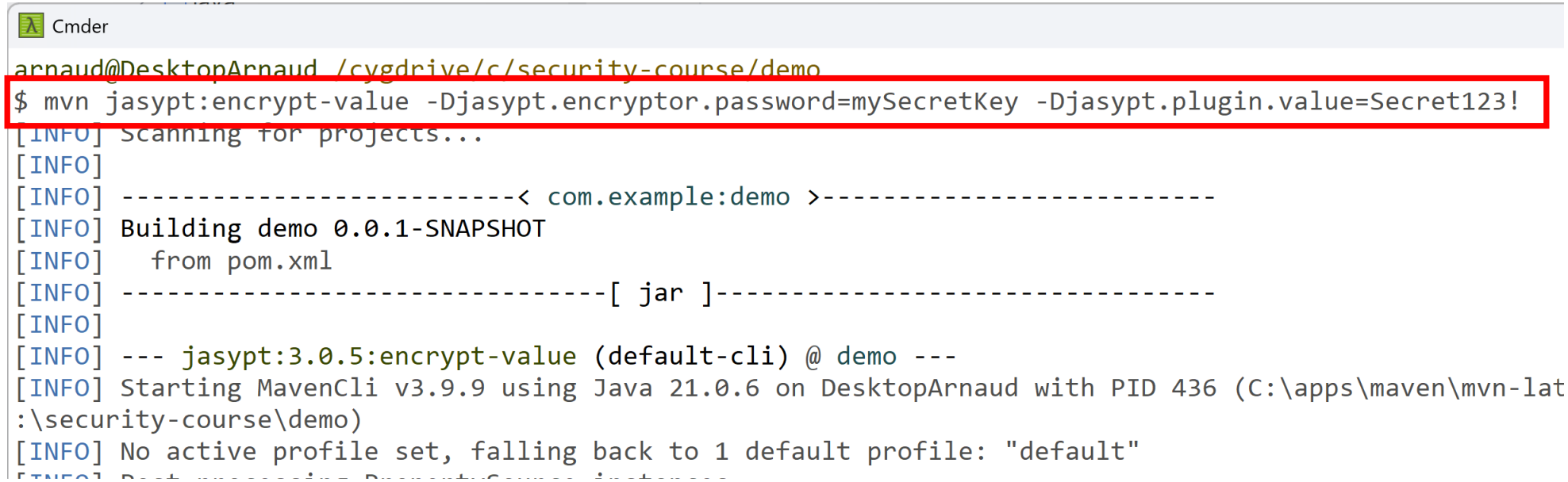
Could use directly "java -jar jasypt.jar .."
but would need to download manually
=> Simpler to use a maven plugin,
edit file pom.xml <build><plugins> ...

```
<plugin>
   <groupId>com.github.ulisesbocchio</groupId>
   <artifactId>jasypt-maven-plugin</artifactId>
   <version>3.0.5</version>
</plugin>
```

Jasypt [6/7] : compute the encryption of a secret value

open windows 'cmd' ... need to have maven downloaded and in %PATH% environment variable

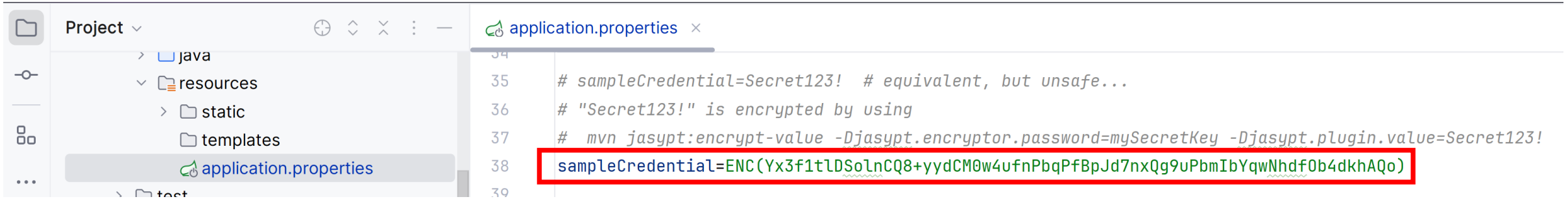
mvn jasypt:encrypt-value -Djasypt.encryptor.password=mySecretKey -Djasypt.plugin.value=Secret123!



Jasypt [6/7] : compute the encryption of a secret value

```
[INFO] Started MavenCli in 1.201 seconds (JVM running for 3.729)
[INFO] Active Profiles: Default
[INFO] Encrypting value Secret123!
[INFO] String Encryptor custom Bean not found with name 'jasyptStringEncryptor'. Initializing Default String Encryptor
[INFO] Encryptor config not found for property jasypt.encryptor.algorithm, using default value: PBEWITHHMACSHA512ANDAES_256
[INFO] Encryptor config not found for property jasypt.encryptor.key-obtention-iterations, using default value: 1000
[INFO] Encryptor config not found for property jasypt.encryptor.pool-size, using default value: 1
[INFO] Encryptor config not found for property jasypt.encryptor.provider-name, using default value: null
[INFO] Encryptor config not found for property jasypt.encryptor.provider-class-name, using default value: null
[INFO] Encryptor config not found for property jasypt.encryptor.salt-generator-classname, using default value: org.jasypt.salt.RandomSaltGenerator
[INFO] Encryptor config not found for property jasypt.encryptor.iv-generator-classname, using default value: org.jasypt.iv.RandomIvGenerator
[INFO] Encryptor config not found for property jasypt.encryptor.string-output-type, using default value: base64
[INFO]
ENC(Yx3f1tlDSolnCQ8+yydCM0w4ufnPbqPfBpJd7nxQg9uPbmIbYqwNhdfOb4dkhAQo)
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  2.427 s
[INFO] Finished at: 2025-03-07T21:13:19+01:00
[INFO] ------------------------------------------------------------------------
```

Jasypt [6/7] : add encrypted value in application.properties

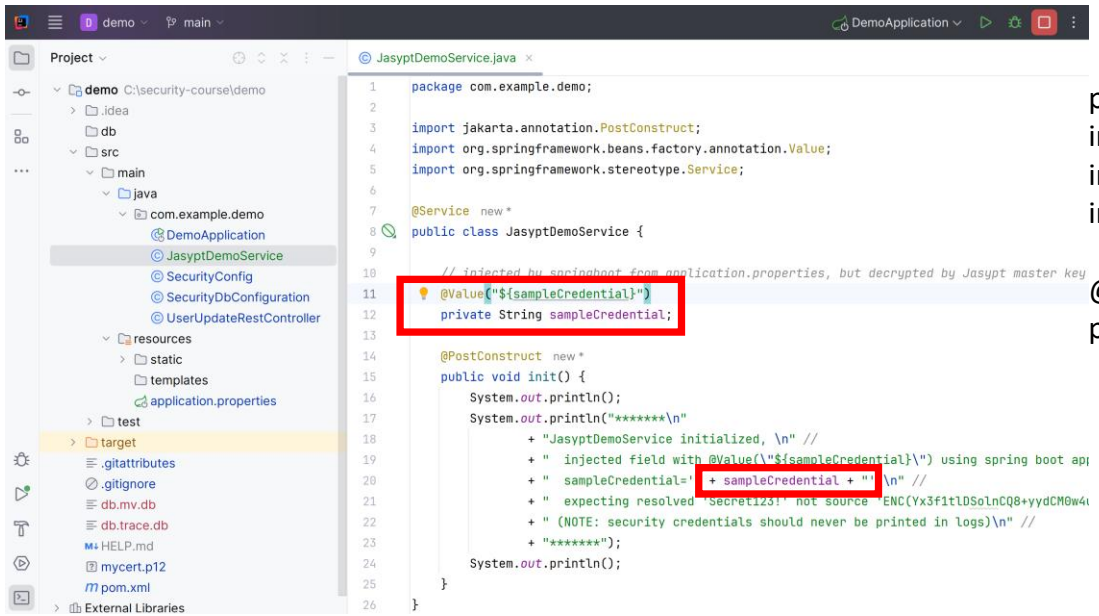


edit src/main/resources/application.properties

sampleCredential=ENC(Yx3f1tlDSolnCQ8+yydCM0w4ufnPbqPfBpJd7nxQg9uPbmIbYqwNhdfOb4dkhAQo)

NOTICE: because of random Salting, every re-generation will get a different value

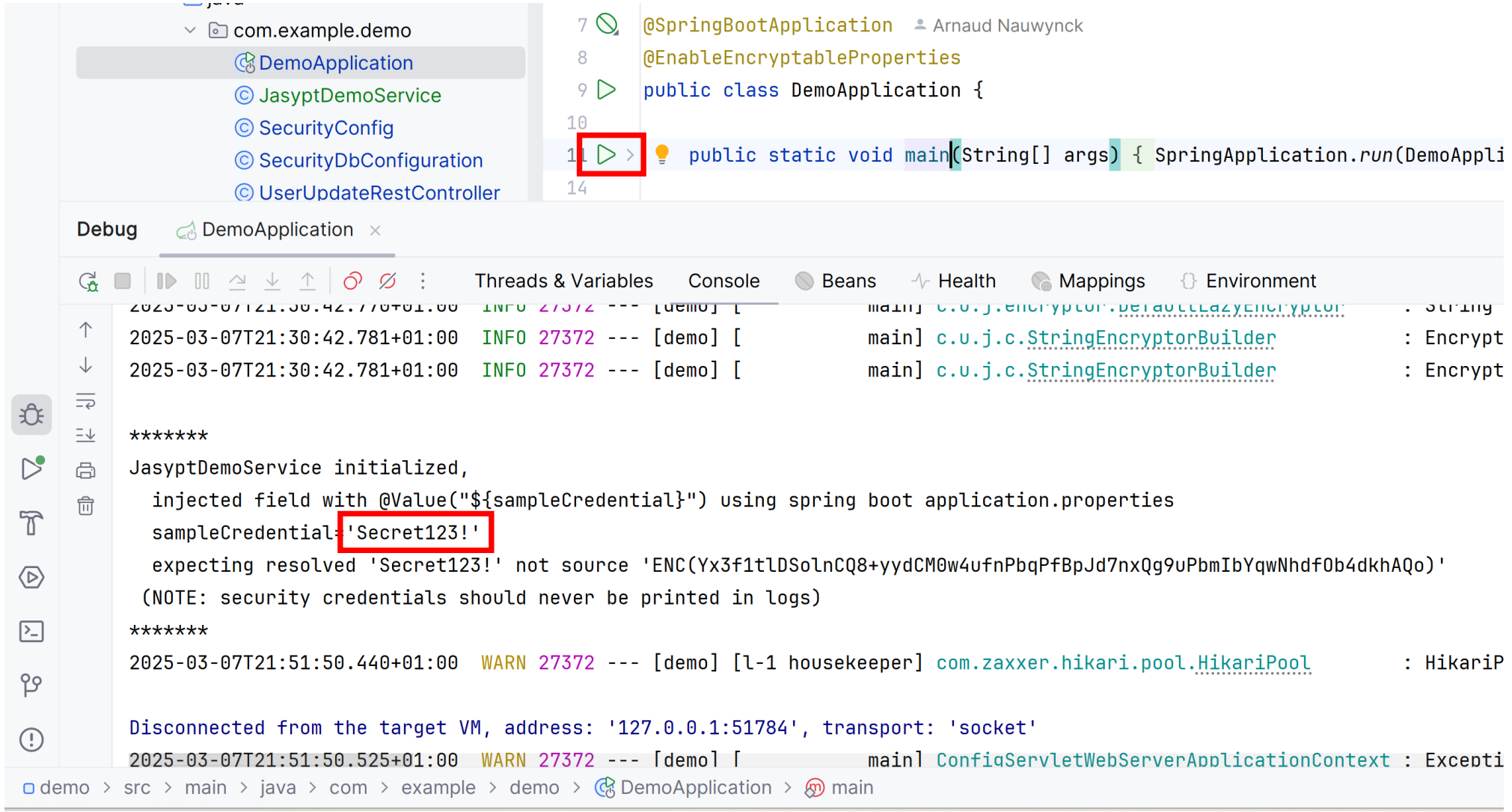
Jasypt [7/7] :use injected value in java code



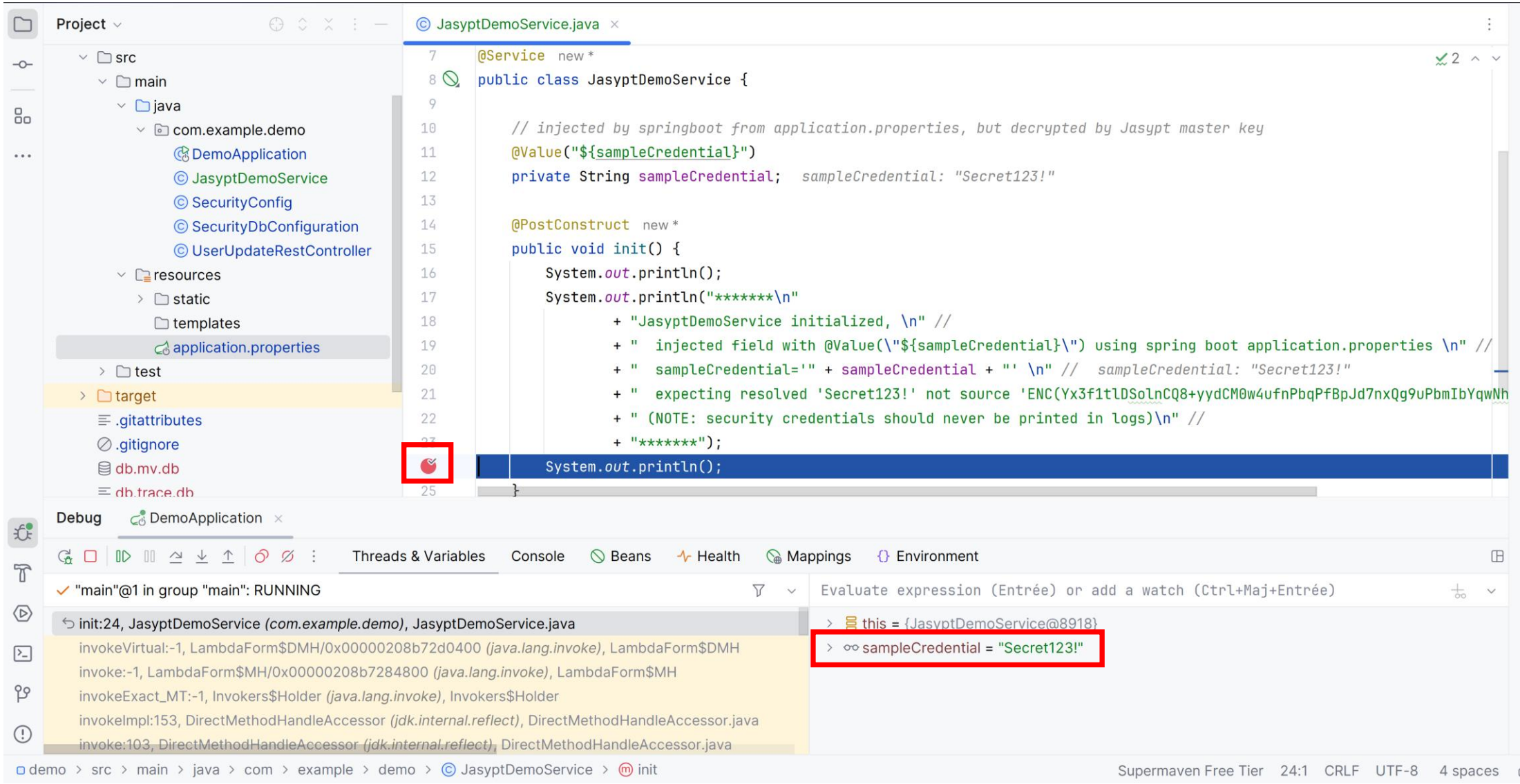
add new java class JasyptDemoService

```
package com.example.demo;
import jakarta.annotation.PostConstruct;
import org.springframework.beans.factory.annotation.Value;
import org.springframework.stereotype.Service;

@Service
public class JasyptDemoService {

   // injected by springboot from application.properties, but decrypted by Jasypt master key
   @Value("${sampleCredential}")
   private String sampleCredential;

   @PostConstruct
   public void init() {
      System.out.println();
      System.out.println("*******\n"
         + "JasyptDemoService initialized, \n" //
         + "  injected field with @Value(\"${sampleCredential}\") using spring boot application.properties \n" //
         + "  sampleCredential='" + sampleCredential + "' \n" //
         + "  expecting resolved 'Secret123!' not source
'ENC(Yx3f1tlDSolnCQ8+yydCM0w4ufnPbqPfBpJd7nxQg9uPbmIbYqwNhdfOb4dkhAQo)' \n" //
         + " (NOTE: security credentials should never be printed in logs)\n" //
         + "*******");
      System.out.println();
   }
}
```

Jasypt [7/7]: Run see startup logs



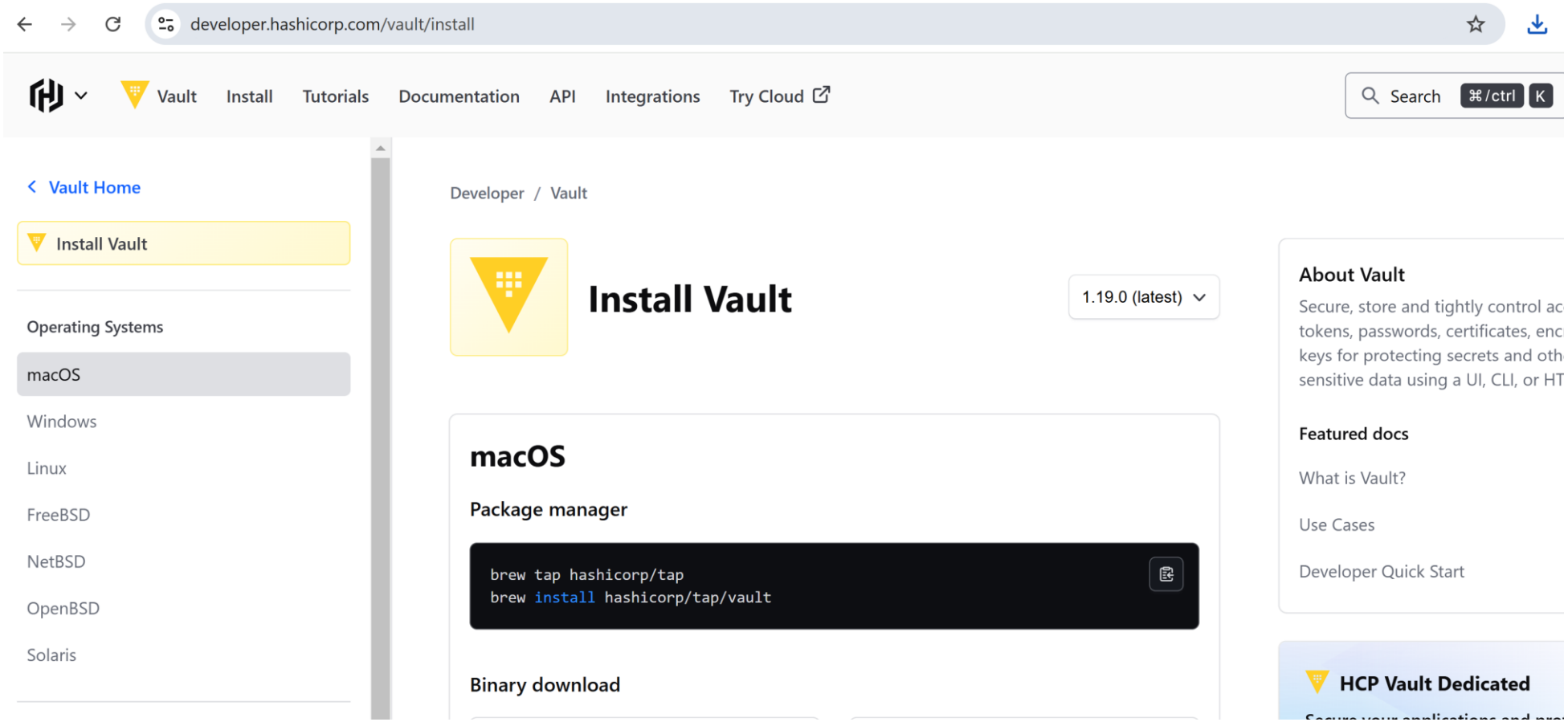
Jasypt [7/7]: Debug with Breakpoint (debug as you should never print credential in logs!)



Using Hashicorp Vault

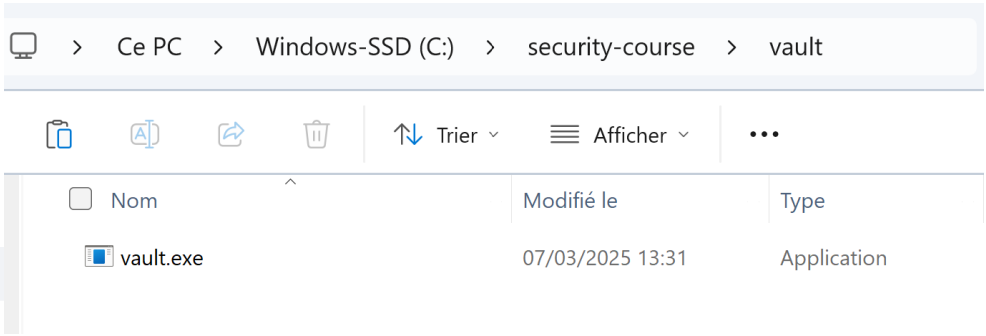
Download + Unzip Hashicorp Vault

https://developer.hashicorp.com/vault/install



Run in "-dev " mode

C:\security-course\vault> **vault.exe server -dev**

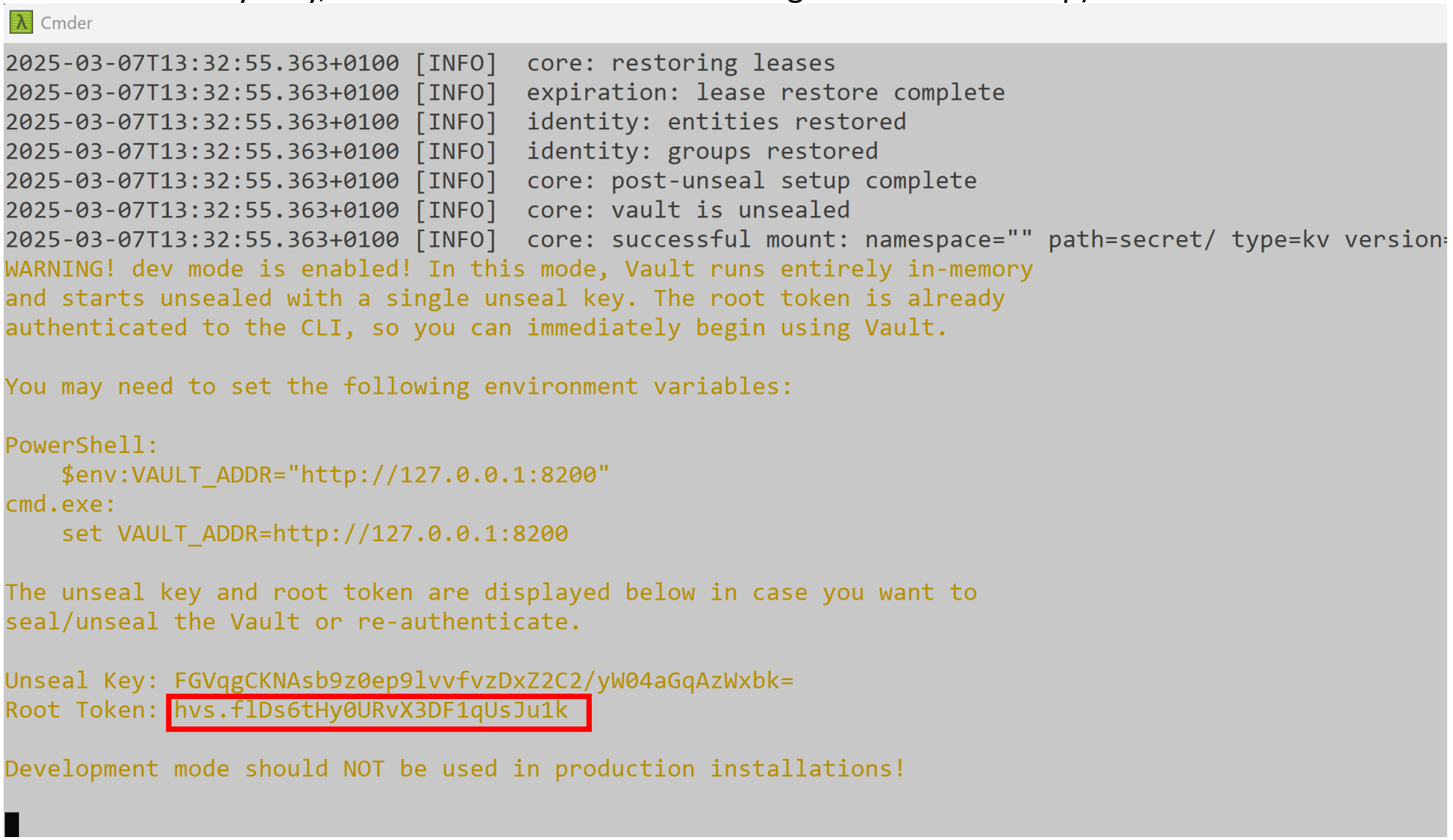


Cmder

```
arnaud@DesktopArnaud /cygdrive/c/security-course/vault
$ ./vault.exe server -dev
==> Vault server configuration:

Administrative Namespace:
             Api Address: http://127.0.0.1:8200
                     Cgo: disabled
         Cluster Address: https://127.0.0.1:8201
   Environment Variables: , ALLUSERSPROFILE, ANSICON, ANSICON_DEF, APPDATA, CMDER_ROOT, C
ommonProgramW6432, ConEmuANSI, ConEmuArgs, ConEmuBackHWND, ConEmuBaseDir, ConEmuBaseDirSh
ve, ConEmuHWND, ConEmuHooks, ConEmuPID, ConEmuPalette, ConEmuServerPID, ConEmuTask, ConEm
WSER_APP_PROFILE_STRING, FPS_BROWSER_USER_PROFILE_STRING, GRADLE_HOME, HADOOP_HOME, HOME,
ATA, LOGONSERVER, M2_HOME, MAVEN_OPTS, NODE_HOME, NODE_OPTIONS, NUMBER_OF_PROCESSORS, OLD
ARCHITECTURE, PROCESSOR_ARCHITEW6432, PROCESSOR_IDENTIFIER, PROCESSOR_LEVEL, PROCESSOR_RE
YSPARK_PYTHON, ProgramData, ProgramFiles(x86), ProgramW6432, SBT_HOME, SESSIONNAME, SHELL
SER, USERDOMAIN, USERDOMAIN_ROAMINGPROFILE, USERNAME, USERPROFILE, VBOX_MSI_INSTALL_PATH,
              Go Version: go1.23.6
              Listener 1: tcp (addr: "127.0.0.1:8200", cluster address: "127.0.0.1:8201",
x_request_size: "33554432", tls: "disabled")
               Log Level:
                   Mlock: supported: false, enabled: false
```

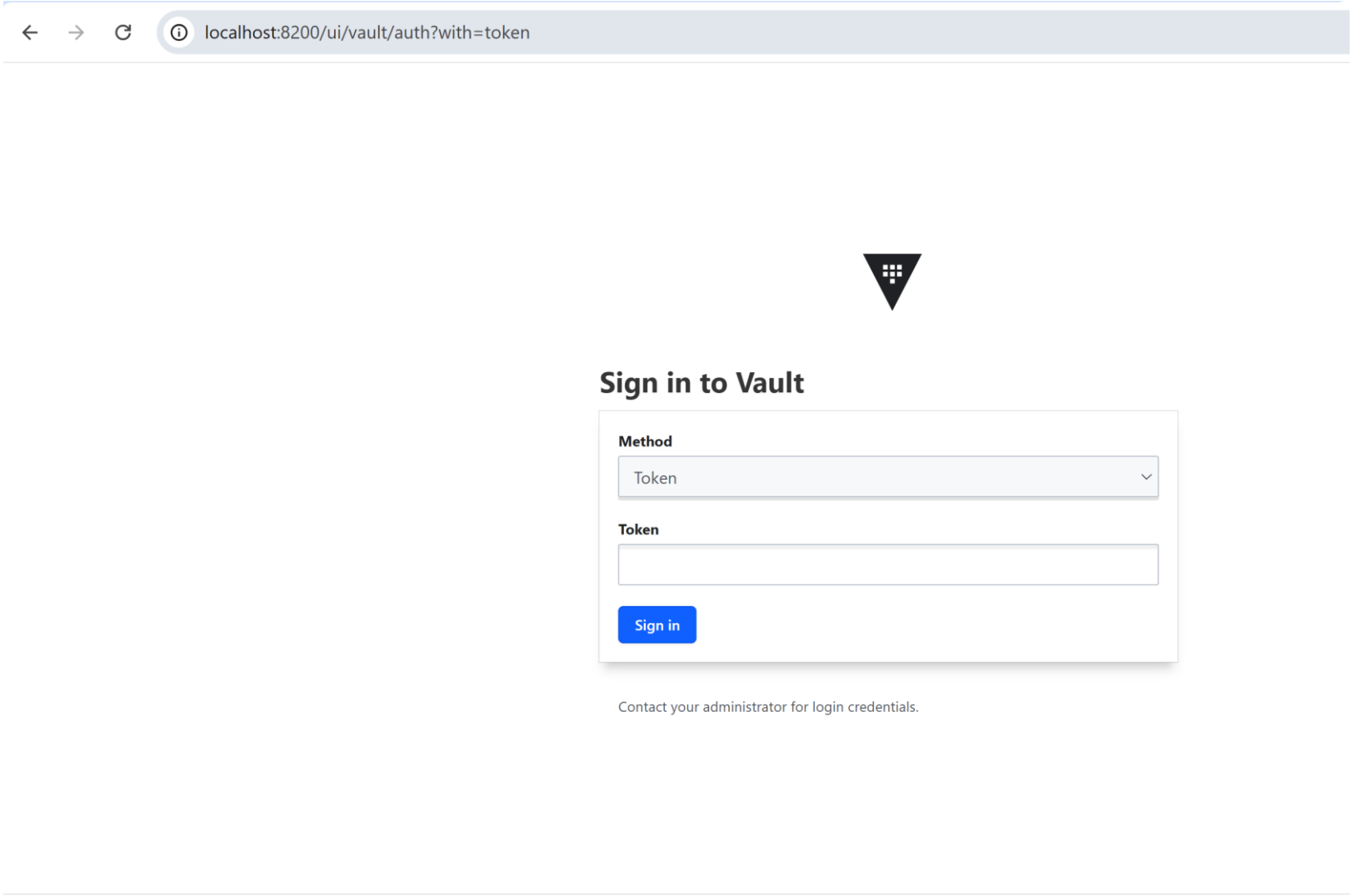
See console log root "token"

(NOTICE: "-dev" = in-memory only, no secrets saved... and token regenerated at startup)

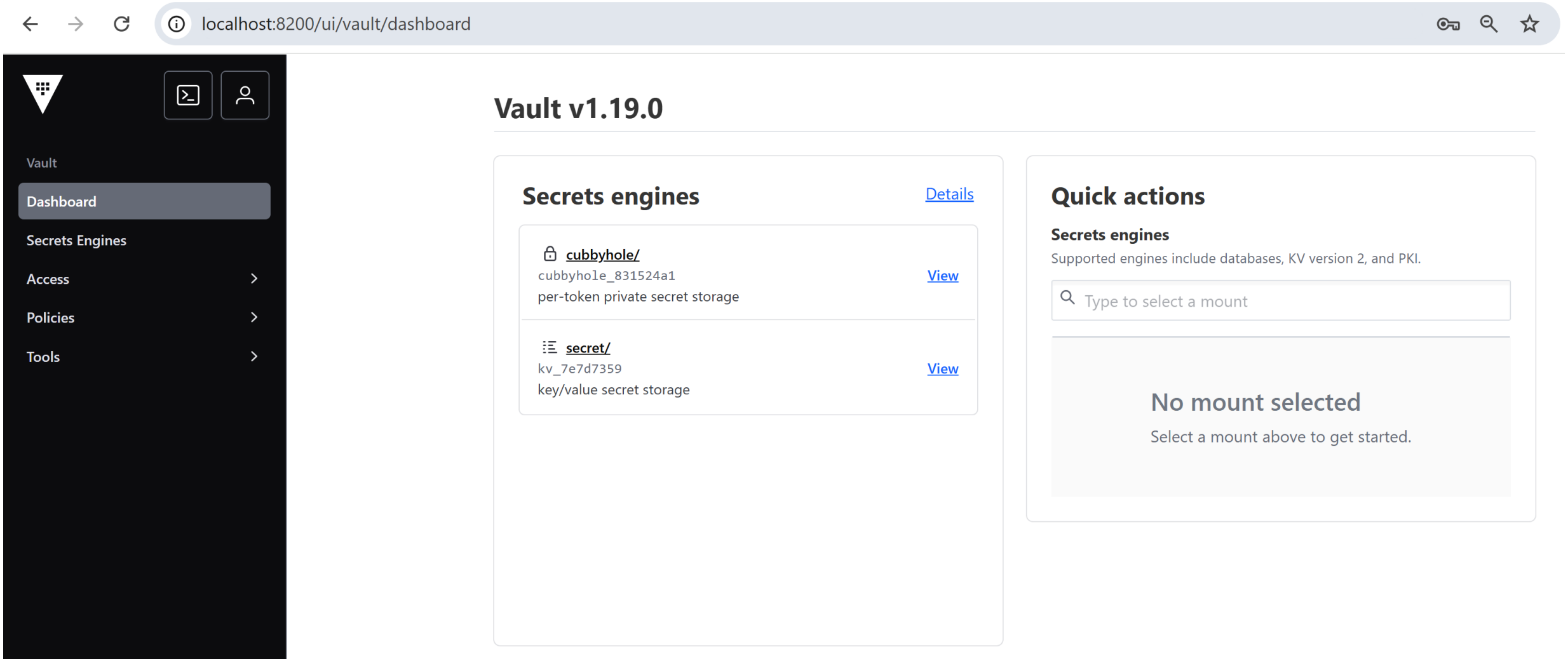


Open Vault Http UI

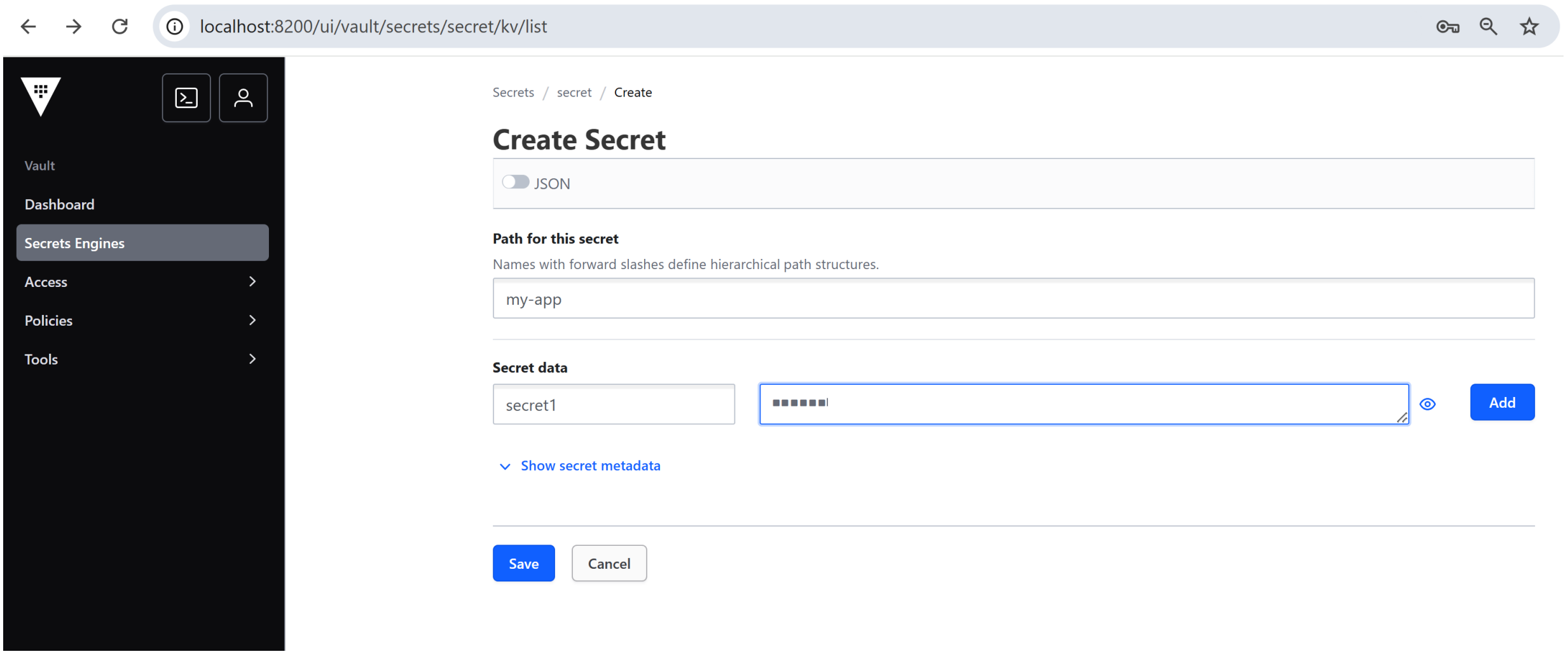
http://localhost:8200



Login... UI Home Page



Create a Secret



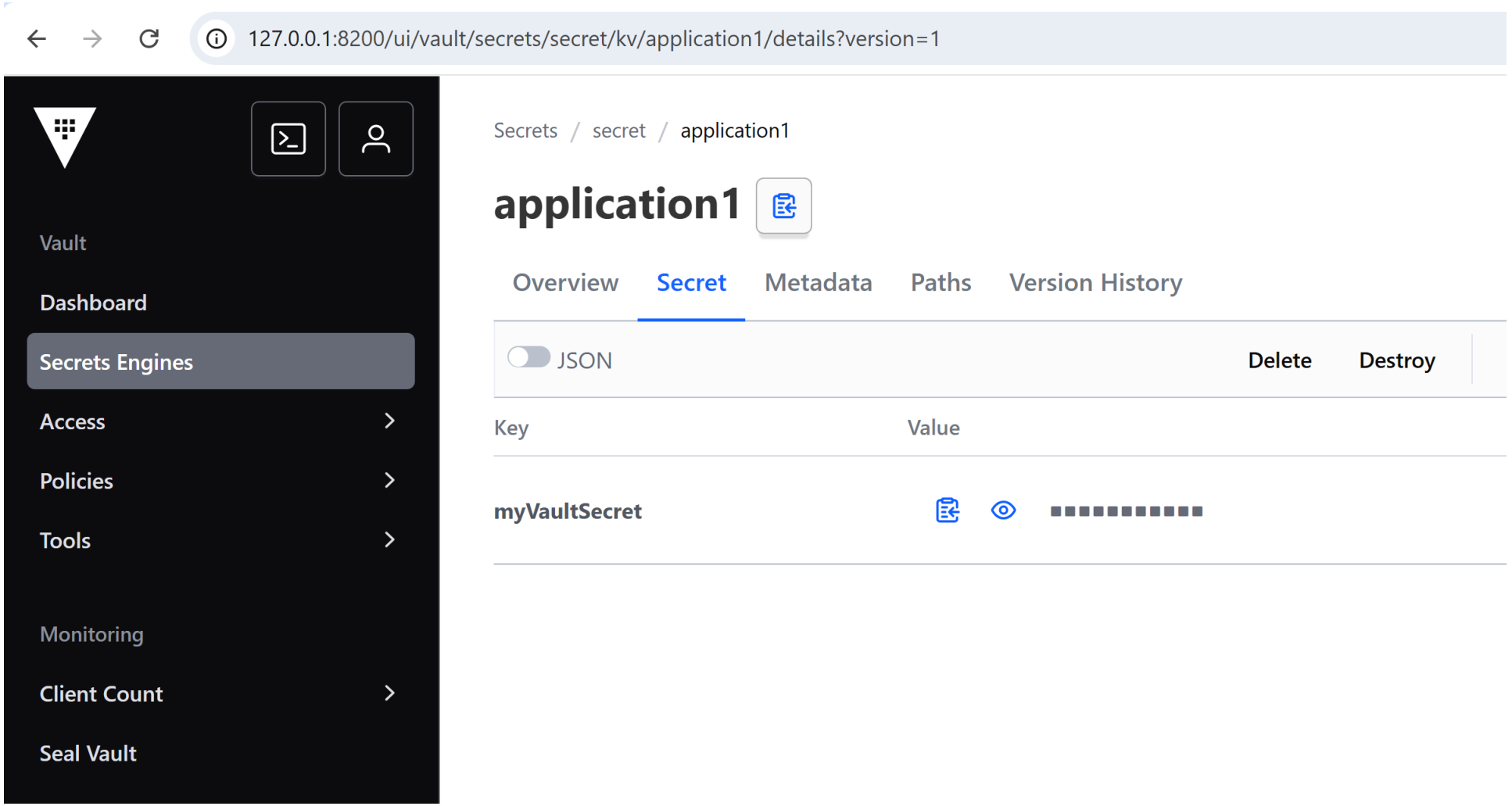
(Optionnal) Creating secret with cmd

./vault kv put secret/application1 "myVaultSecret=Secret123"

```
$ ./vault kv put secret/application1 "myVaultSecret=Secret123"
====== Secret Path ======
secret/data/application1

======= Metadata =======
Key                Value
---                -----
created_time       2025-03-07T23:04:16.9254565Z
custom_metadata    <nil>
deletion_time      n/a
destroyed          false
version            3
```

Configured Secret in Vault

path=application1
secretName=myVaultSecret (secretValue=Secret123)



Use springboot cloud + Hashicorp Vault

to resolve secrets in config

add pom.xml dependency spring-cloud-starter-vault-config

edit pom.xml, add <dependencies>...

```
<dependency>
    <groupId>org.springframework.cloud</groupId>
    <artifactId>spring-cloud-starter-vault-config</artifactId>
    <version>4.1.2</version>
</dependency>
```

Configure springboot - Vault

application.properties

```
62
63  # Spring Cloud HashiCorp Vault configuration
64
65  #spring.cloud.vault.enabled=true
66  spring.cloud.vault.uri=http://localhost:8200
67  spring.cloud.vault.token=hvs.6qzL7qdKN2EjtbieAzhXqqTZ
68  spring.cloud.vault.kv.backend=secret
69  spring.cloud.vault.kv.default-context=application1
70
71  spring.config.import=vault://
```

edit file
src/main/resources/
application.properties

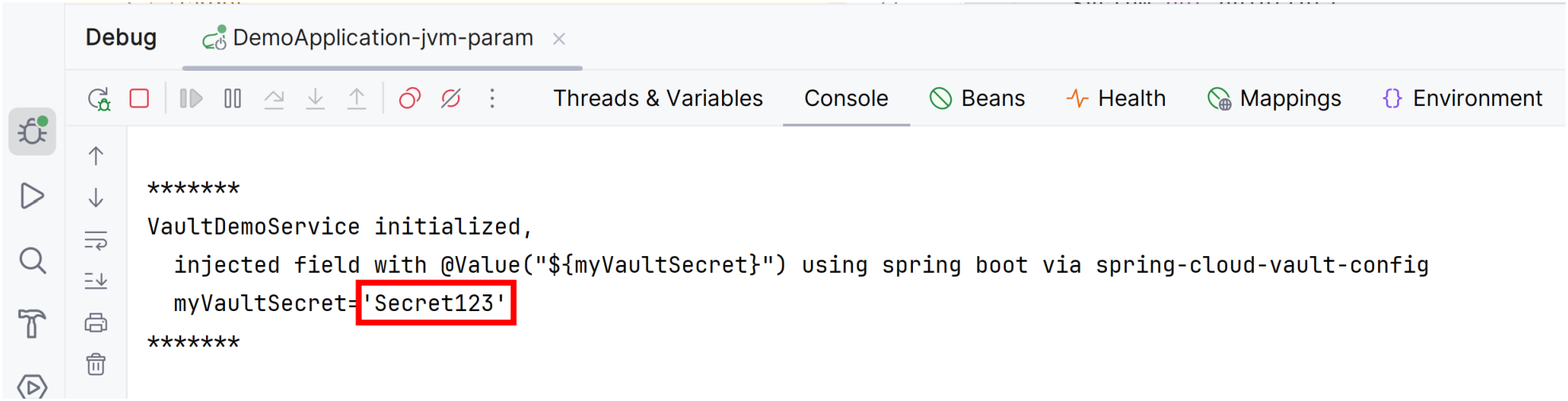
```
# Spring Cloud HashiCorp Vault configuration
spring.cloud.vault.uri=http://localhost:8200
spring.cloud.vault.token=**************your token
spring.cloud.vault.kv.backend=secret
spring.cloud.vault.kv.default-context=application1

spring.config.import=vault://

# myVaultSecret=.. cf overriden injected from Vault 'application1/secret/myVaultSecret'
```

Add Java code to use injected value

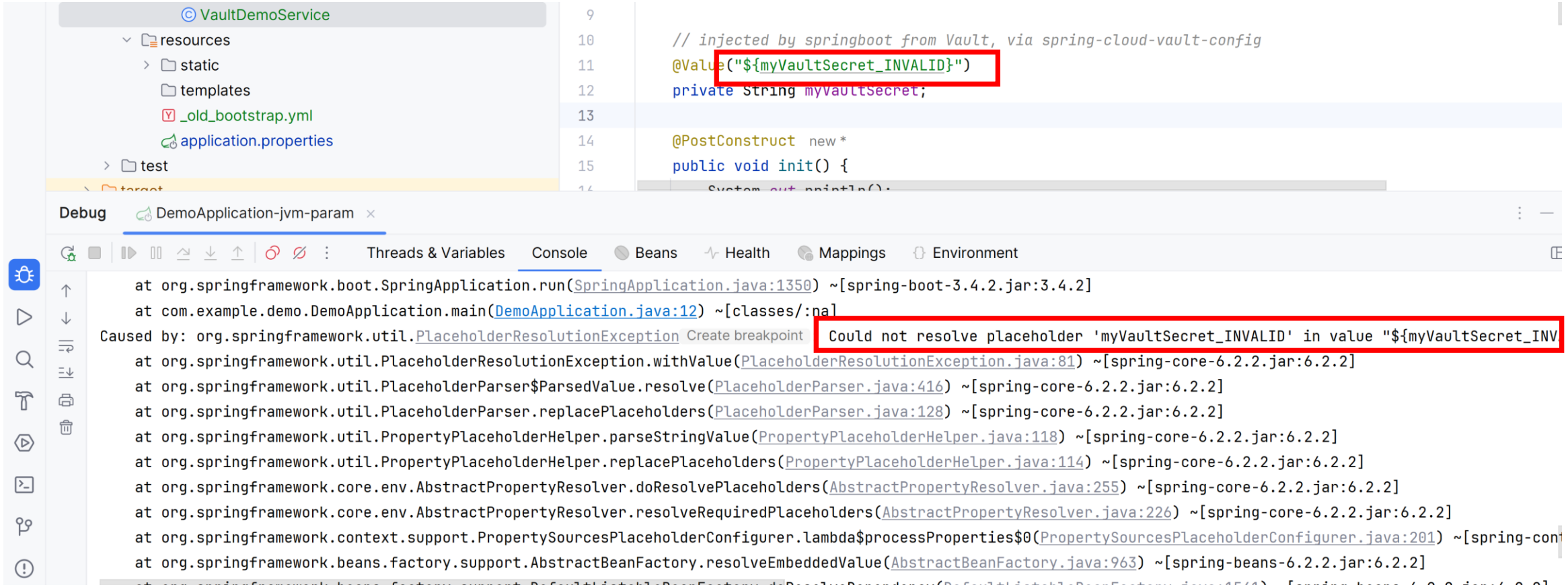
edit new java class
VaultDemoService

```
@Service
public class VaultDemoService {

   // injected by springboot from Vault, via spring-cloud-vault-
config
   @Value("${myVaultSecret}")
   private String myVaultSecret;

   @PostConstruct
   public void init() {
      System.out.println();
      System.out.println("*******\n"
            + "VaultDemoService initialized, \n" //
            + "  injected field with @Value(\"${myVaultSecret}\")
using spring boot via spring-cloud-vault-config \n" //
            + "  myVaultSecret='" + myVaultSecret + "' \n" //
            + "*******");
      System.out.println();
   }
}
```

Run/Debug


Debug
DemoApplication-jvm-param
Threads & Variables
Console
Beans
Health
Mappings
Environment
****
VaultDemoService initialized,
injected field with @Value("${myVaultSecret}") using spring boot via spring-cloud-vault-config
myVaultSecret='Secret123'
****

NOTICE... if property (Secret) not found
=> Error at startup



Questions ?