Filter

בקשה יכולה לעבור דרך הרבה פילטרים עד שהיא תגיע אלינו

לדוגמא אנחנו הרחבנו פילטר של ספרינט

```
public class JwtUsernameAndPasswordAuthenticationFilter extends UsernamePasswordAuthenticationFilter {
```

עכשיו כדי לשהתמש בפילטר הזה נוסיף אותו בקונפיגרציה שלנו

אז דבר ראשון מחקנו את כל מה שעשינו שקשור להתחברות קודם

```
//                  .and()
//                  .formLogin()
//                  .loginPage("/login")
//                  .defaultSuccessUrl("/courses")
//                  .and()
//                  .rememberMe()
//                  .tokenValiditySeconds((int) TimeUnit.DAYS.toSeconds(21)) //default to 2 weeks
//                  .key("something_very_secured")
//                  .and()
//                  .logout()
//                      .logoutUrl("/logout") // באיזה נתיב מתנקים
//                      .clearAuthentication(true) //
//                      .invalidateHttpSession(true) //
//                      .deleteCookies("JSESSIONID", "remember-me") // איזה עוגיות למחוק
//                      .logoutSuccessUrl("/login"); // מה קורה כשמסיימים את הlogout
```

ונוסיף את הפילטר

והוספנו פה גם את העניין שJWT הוא stateless

```
@Override
protected void configure(HttpSecurity http) throws Exception {
    http
..
            .csrf().disable() // אם נרצה לבטל את ה csrf
            .sessionManagement().sessionCreationPolicy(SessionCreationPolicy.STATELESS)
            .and()
            .addFilter(new JwtUsernameAndPasswordAuthenticationFilter(authenticationManager()))
            .authorizeRequests()// אנחנו רוצים לאמת בקשות
```

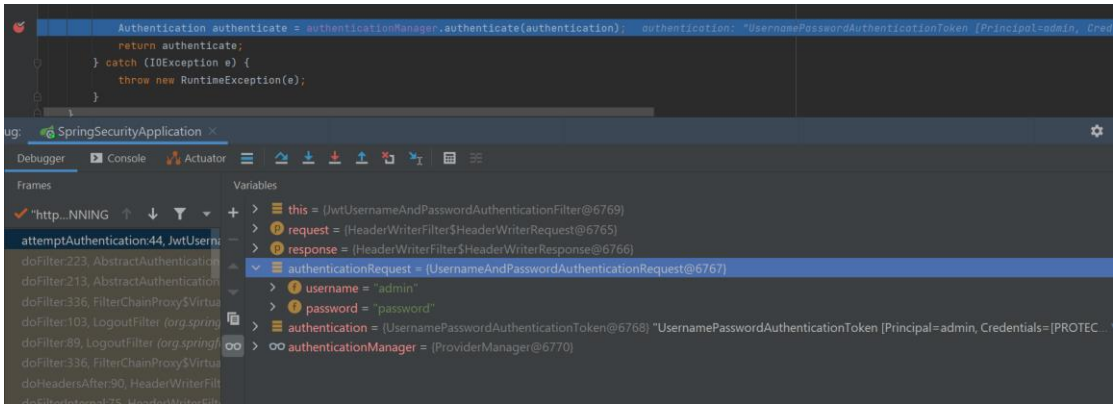
עכשיו נשלח בקשה ונפעיל דיבאגר

POST http://localhost:8080/login

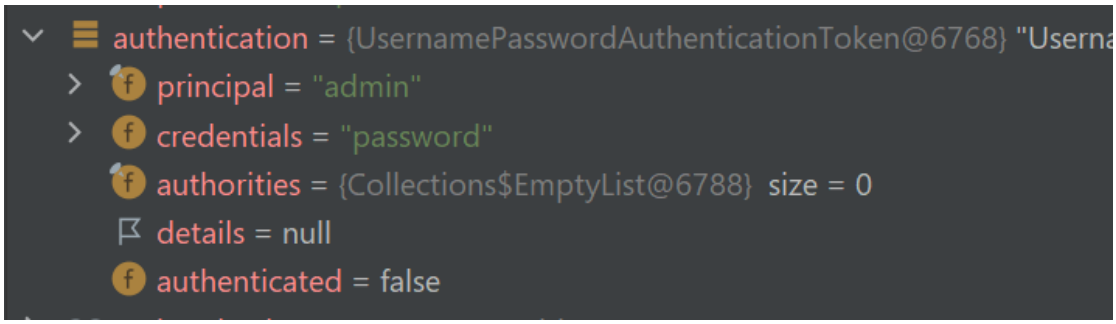
Params Authorization Headers (10) Body Pre-re

none form-data x-www-form-urlencoded raw

```
1 {
2     "username": "admin",
3     "password":"password"
4 }
```



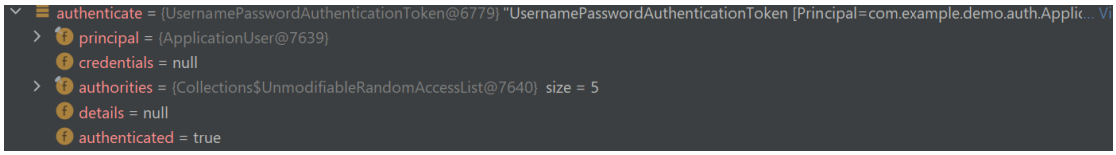
הבקשה לפני האימות

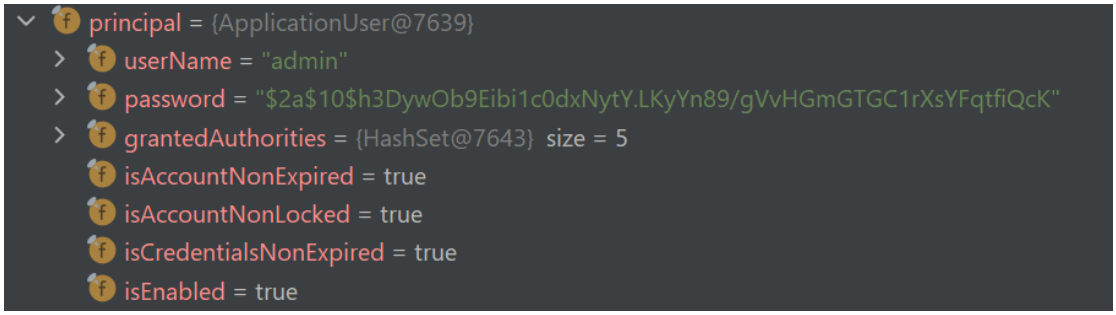


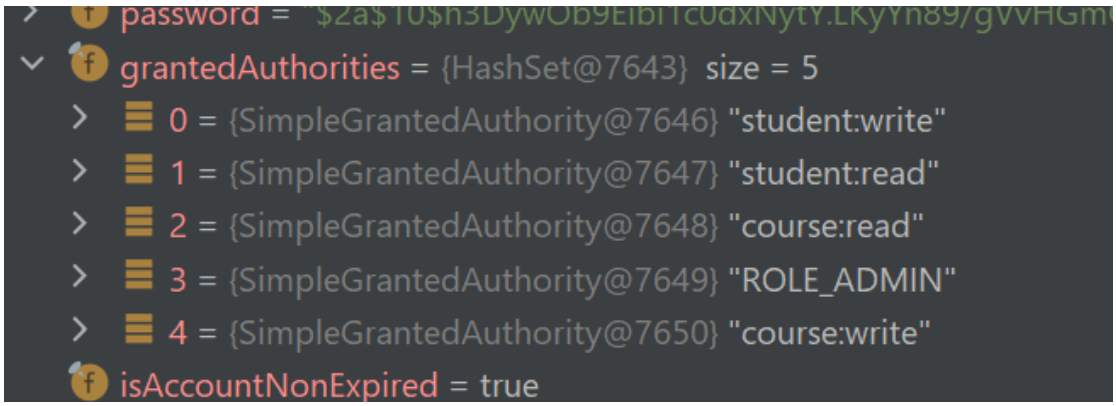
אחרי

אפשר לראות כמה הבדלים :

- הprincipal התמלא בכל המידע שאנחנו צריכים על היוזר: שם משתמש, סיסמא, ההרשאות שלו, וכל המשתנים הבוליאנים
- ה credentials הפך ל null מהסיסמא הלא מוצפנת
- הauthories שלו המתלאו (כמו בprincipal)
- השדה של authenticated הפך לture







```
authorities = {Collections$UnmodifiableRandomAccessList@7640} size = 5
  0 = {SimpleGrantedAuthority@7646} "student:write"
  1 = {SimpleGrantedAuthority@7647} "student:read"
  2 = {SimpleGrantedAuthority@7648} "course:read"
  3 = {SimpleGrantedAuthority@7649} "ROLE_ADMIN"
  4 = {SimpleGrantedAuthority@7650} "course:write"
details = null
```

אפשר לראות איזה טוקן ארוך נוצר עכשיו

נשים עוד עצירה ב

```
response.addHeader( s: "Authorization", s1: "Bearer " + token);
```

וזה הטוקן שנוצר לנו

```
eyJhbGciOiJIUzI1NiJ9.
.eyJzdWIiOiJhZG1pbiIsImF1dGhvcml0aWVzIjpbeyJhdXRob3JpdHkiOiJzdHVkZW50OndyaXRlIn0seyJhdXRob3Jpd
HkiOiJzdHVkZW50OnJlYWQifSx7ImF1dGhvcml0eSI6ImNvdXJzZTpyZWFkIn0seyJhdXRob3JpdHkiOiJST0xFX0FETUl
OIn0seyJhdXRob3JpdHkiOiJjb3Vyc2U6d3JpdGUifV0sImlhdCI6MTY1MDQ3MTc0MywiZXhwIjoxNjUxNjExNjAwfQ.
.wdOWtk_3N-IxmW89q8iMC2cKVXYB8EgPO9vQqR6skz0
```

```
Variables
  ((UsernamePasswordAuthenticationTok
  this = {JwtUsernameAndPasswordAuth
  request = {HeaderWriterFilter$HeaderV
  response = {HeaderWriterFilter$Heade
  chain = {FilterChainProxy$VirtualFilterC
  authResult = {UsernamePasswordAuthe
  key = "secure_secure_secure_secure_sec
  token = "eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJhZG1pbiIsImF1dGhvcml0aWVzIjpbeyJhdXRob3JpdHkiOiJzdHVkZW50OndyaXRlIn0seyJhdXRob3JpdHkiO...
```

ואם ניכנס לheaders של הבקשה נוכל לראות את מה ששמנו

Body Cookies Headers (11) Test Results Status: 200 OK Time: 4.25 s Size: 693 B Save Response

KEY	VALUE
Authorization	Bearer eyJhbGciOiJIUzM4NCJ9.eyJzdWIiOiJhZG1pbiIsImF1dGhvcml0aWVzIjpbeyJhdXRob3JpdHkiOiJzdHVkZW50OndyaXRlIn0seyJhdXRob3JpdHkiOiJzdHVkZW50OnJlYWQifSx7ImF1dGhvcml0eSI6ImNvdXJzZTpyZWFkIn0seyJhdXRob3JpdHkiOiJST0xFX0FETUlOIn0seyJhdXRob3JpdHkiOiJjb3Vyc2U6d3JpdGUifV0sImlhdCI6MTY1MDQ3MTg2MCwiZXhwIjoxNjUxNjExNjAwfQ.MDGicWv2usyyZl2JdkuEGHBYcHFm5QzDNIvlNca4v7CXfNrcTTln6raxFusLsKtk
X-Content-Type-Options	
X-XSS-Protection	
Cache-Control	no-cache, no-store, max-age=0, must-revalidate

ואם נכנס ל https://jwt.io/

נוכל לעשות Decoded

ונראה את הכל המידע

- Sub – השם משתמש
- ואז את ההרשאות שיש לה
- את היצירה
- את התאריך תפוגה

eyJhbGciOiJIUzM4NCJ9.eyJzdWIiOiJhZG1pbiIsImF1dGhvcml0aWVzIjpbeyJhdXRob3JpdHkiOiJzdHVkZW50OndyaXRlIn0seyJhdXRob3JpdHkiOiJzdHVkZW50OnJlYWQifSx7ImF1dGhvcml0eSI6ImNvdXJzZTpyZWFkIn0seyJhdXRob3JpdHkiOiJST0xFX0FETUlOIn0seyJhdXRob3JpdHkiOiJjb3Vyc2U6d3JpdGUifV0sImlhdCI6MTY1MDQ3MTg2MCwiZXhwIjoxNjUxNjExNjAwfQ.MDGicWv2usyyZl2JdkuEGHBYcHFm5QzDNIvlNca4v7CXfNrcTTln6raxFusLsKtk

Subject (whom the token refers to)

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS384"
}
```

PAYLOAD: DATA

```
{
  "sub": "admin",
  "authorities": [
    {
      "authority": "student:write"
    },
    {
      "authority": "student:read"
    },
    {
      "authority": "course:read"
    },
    {
      "authority": "ROLE_ADMIN"
    },
    {
      "authority": "course:write"
    }
  ],
  "iat": 1650471860,
  "exp": 1651611600
}
```

VERIFY SIGNATURE

```
HMACSHA384(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```