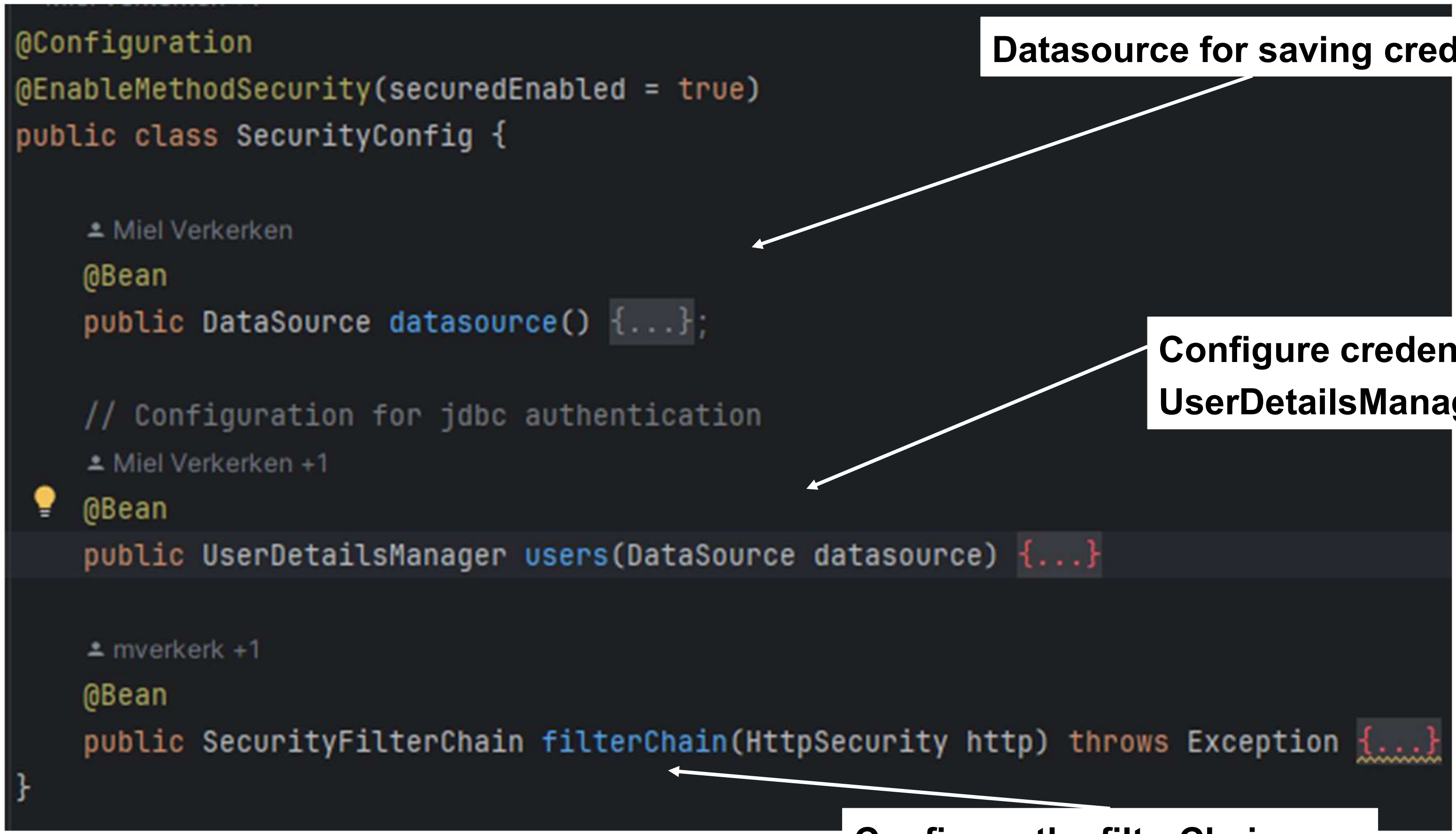
SECURITY CONFIGURATION



```
@Configuration
@EnableMethodSecurity(securedEnabled = true)
public class SecurityConfig {

    Miel Verkerken
    @Bean
    public DataSource datasource() {...};

    // Configuration for jdbc authentication
    Miel Verkerken +1
    @Bean
    public UserDetailsManager users(DataSource datasource) {...}

    mverkerk +1
    @Bean
    public SecurityFilterChain filterChain(HttpSecurity http) throws Exception {...}
}
```

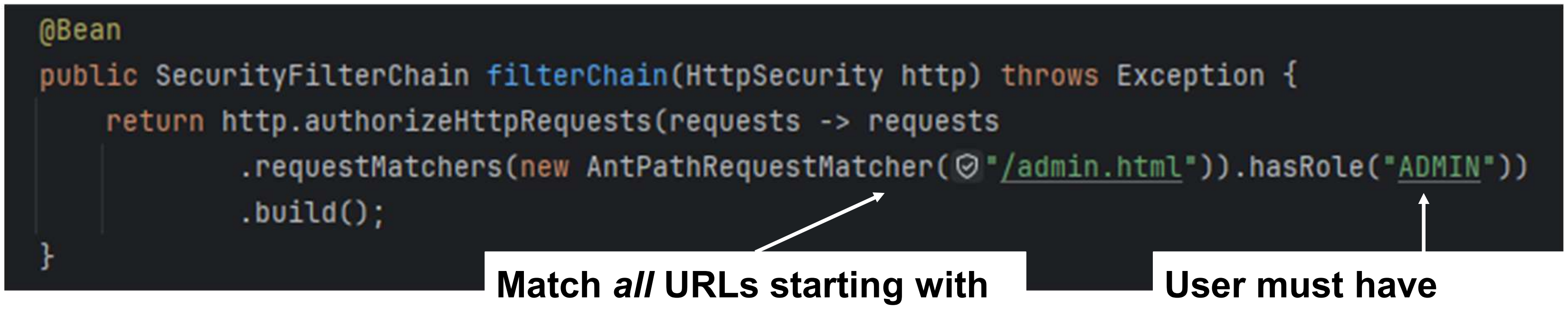
Datasource for saving credentials

Configure credentials using UserDetailsManager

Configure the filterChain

AUTHORIZING URL

- Define specific authorization restrictions for URLs
- Support “Ant-style” pattern matching
  - "/admin/*" only matches "/admin/xxx“
  - "/admin/**" matches any path under /admin
    - Such as "/admin/database/access-control“



```
@Bean
public SecurityFilterChain filterChain(HttpSecurity http) throws Exception {
    return http.authorizeHttpRequests(requests -> requests
            .requestMatchers(new AntPathRequestMatcher("/admin.html")).hasRole("ADMIN"))
            .build();
}
```

Match *all* URLs starting with *admin* (ANT-style path)

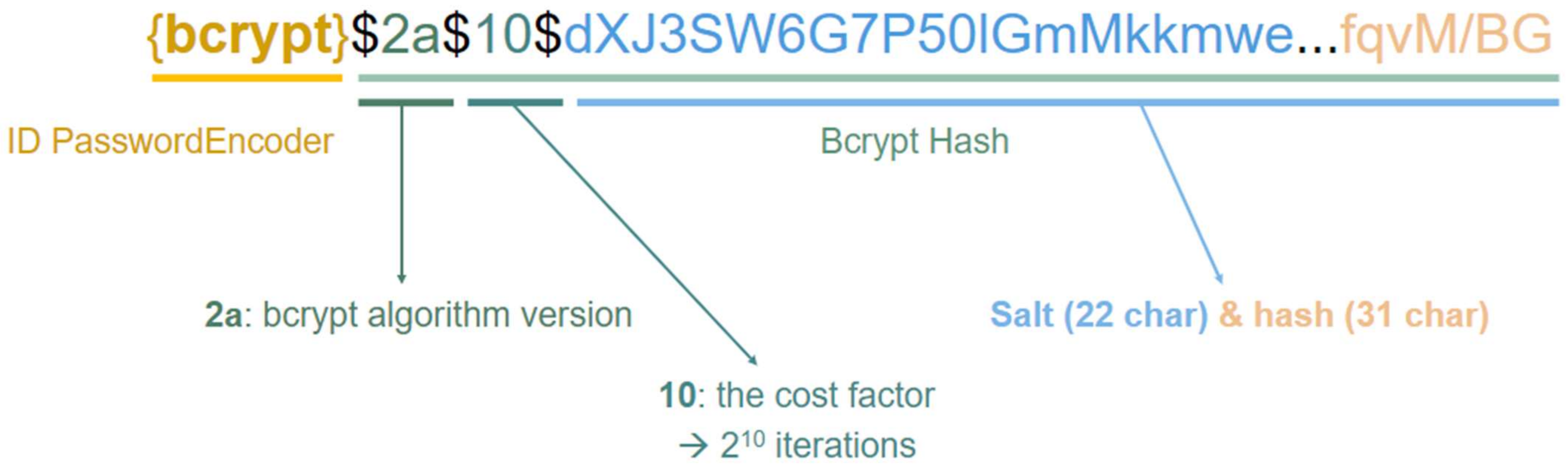
User must have ADMIN role

CHALLENGES PASSWORD ENCODING (1)

- Should be future proof
  - Secure today is not secure tomorrow
  - New encoding schemes emerge in the future
- Should accommodate old password formats
  - Co-exist new and old format passwords
- DelegatingPasswordEncoder
  - {id}encodedPassword
  - {**bcrypt**}$2a$10$dXJ3SW6G7P50lGmMkkmwe...fqvM/BG

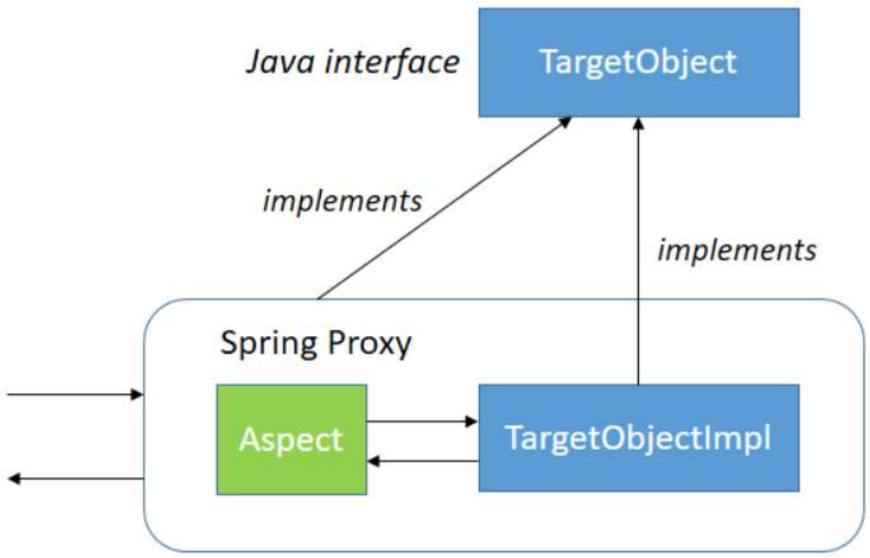
UNIVERSITEIT GENT

CHALLENGES PASSWORD ENCODING (2)


{bcrypt}$2a$10$dXJ3SW6G7P50lGmMkkmwe...fqvM/BG
ID PasswordEncoder
Bcrypt Hash
2a: bcrypt algorithm version
Salt (22 char) & hash (31 char)
10: the cost factor
→ 2^10 iterations

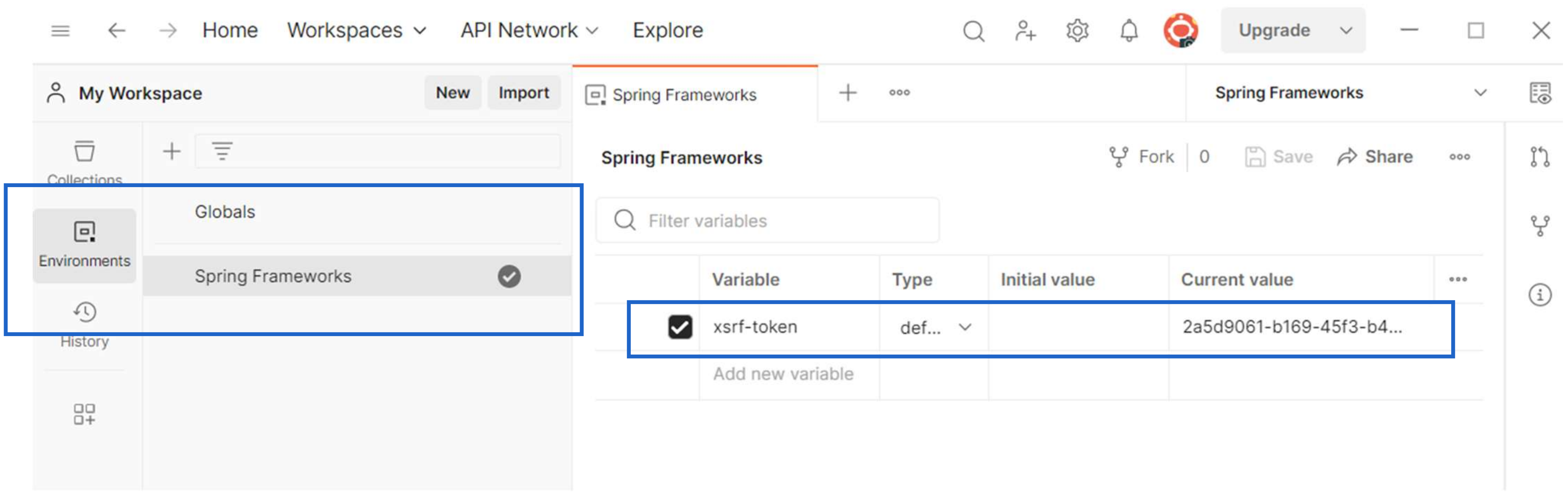
METHOD SECURITY

- Spring Security uses AOP for method-level security
  - Annotations: either Spring's own or JSR-250
- Spring uses a AOP Proxy



UNIVERSITEIT GENT

CSRF TOKEN IN POSTMAN (1)

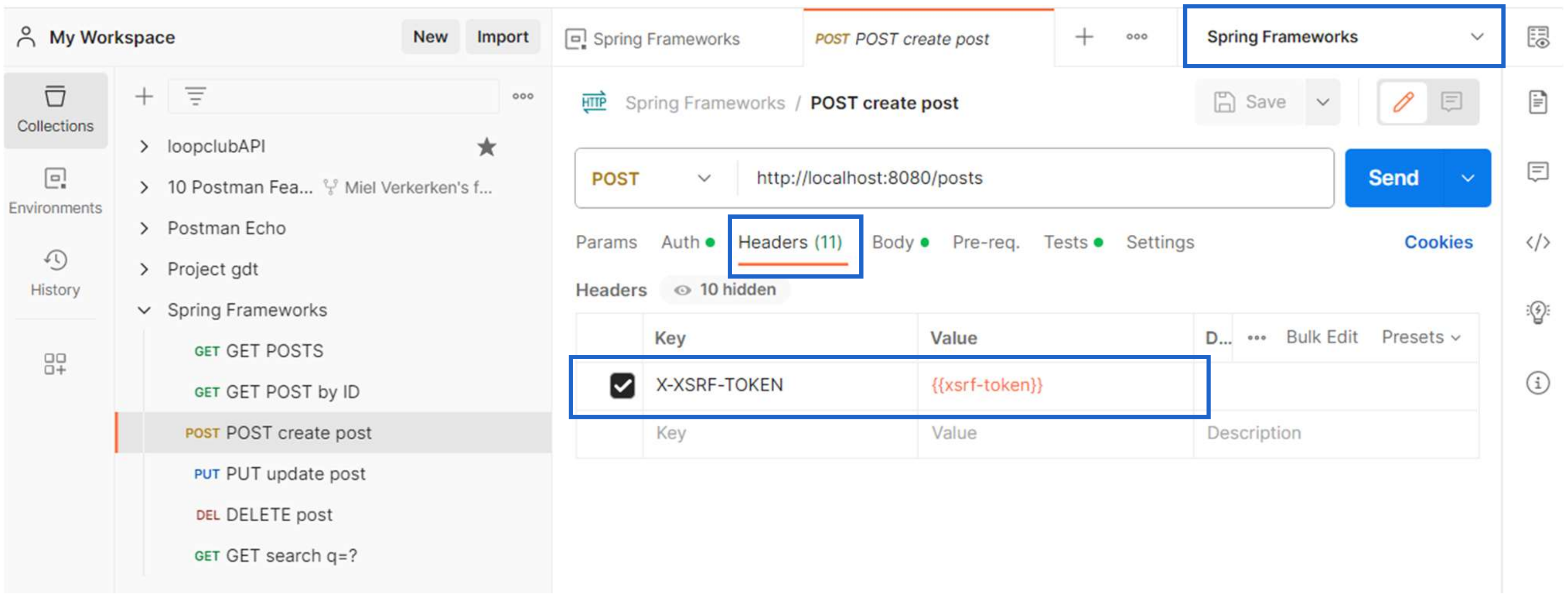


Spring Frameworks

	Variable	Type	Initial value	Current value
✓	xsrf-token	def...		2a5d9061-b169-45f3-b4...

UNIVERSITEIT GENT

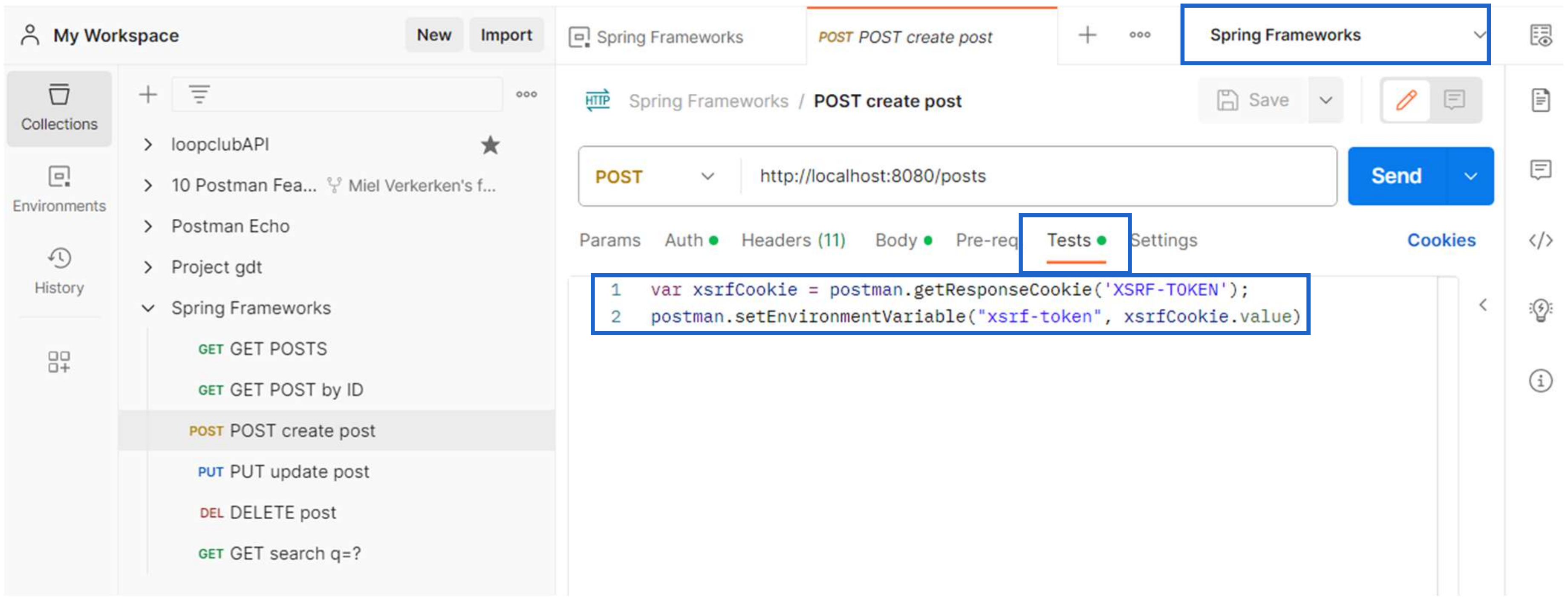
CSRF TOKEN IN POSTMAN (2)



POST http://localhost:8080/posts

Key	Value	Description
X-XSRF-TOKEN	{{xsrf-token}}	

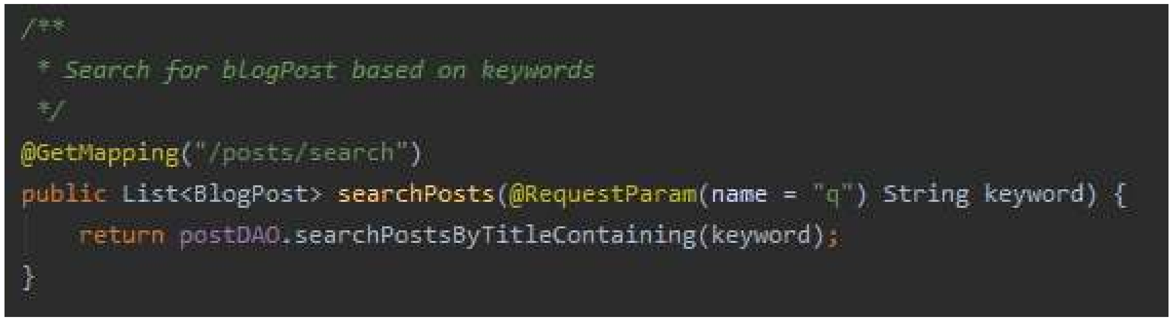
CSRF TOKEN IN POSTMAN (3)



```
var xsrfCookie = postman.getResponseCookie('XSRF-TOKEN');
postman.setEnvironmentVariable("xsrf-token", xsrfCookie.value)
```

UNIVERSITEIT GENT

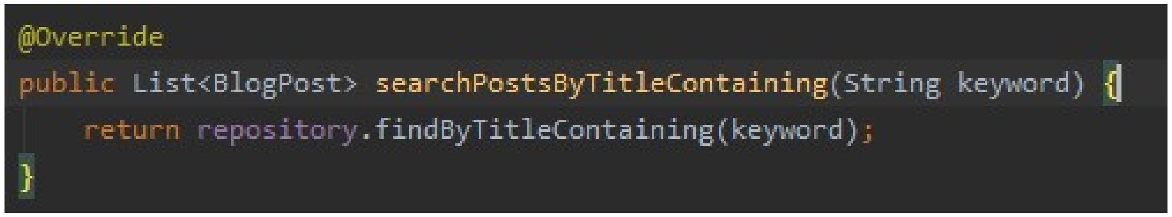
ZOEK FUNCTIONALITEIT



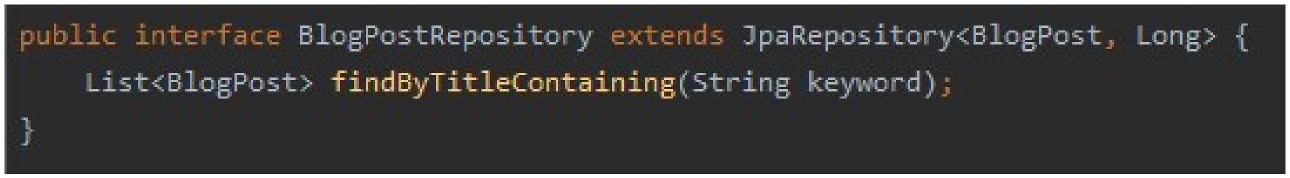
```java
/**
 * Search for blogPost based on keywords
 */
@GetMapping("/posts/search")
public List<BlogPost> searchPosts(@RequestParam(name = "q") String keyword) {
    return postDAO.searchPostsByTitleContaining(keyword);
}
```

Controller

DAO



```java
@Override
public List<BlogPost> searchPostsByTitleContaining(String keyword) {
    return repository.findByTitleContaining(keyword);
}
```



```java
public interface BlogPostRepository extends JpaRepository<BlogPost, Long> {
    List<BlogPost> findByTitleContaining(String keyword);
}
```

Repository

UNIVERSITEIT GENT