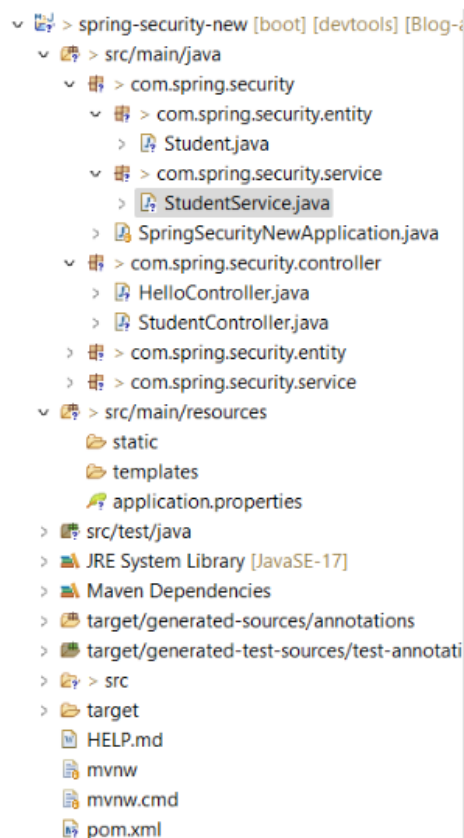


Error Without CSRF Token

- **Understanding CSRF (Cross-Site Request Forgery):** CSRF is a type of attack that tricks the user into executing unwanted actions on a web application where they are authenticated. CSRF tokens are used to prevent such attacks by adding an extra layer of verification.
- **Error Without CSRF Token:**
 - When trying to make a **POST**, **PUT**, **DELETE**, or any state-changing request without a CSRF token, the server may respond with a **403 Forbidden** error indicating a missing or invalid CSRF token.
 - This happens because CSRF protection is enabled by default in Spring Security for non-GET requests.

Project Structure:



```

  ▾ > spring-security-new [boot] [devtools] [Blog-
  ▾ > src/main/java
    ▾ > com.spring.security
      ▾ > com.spring.security.entity
        > Student.java
      ▾ > com.spring.security.service
        > StudentService.java
        > SpringSecurityNewApplication.java
    ▾ > com.spring.security.controller
      > HelloController.java
      > StudentController.java
    > com.spring.security.entity
    > com.spring.security.service
  ▾ > src/main/resources
    > static
    > templates
    > application.properties
  > src/test/java
  > JRE System Library [JavaSE-17]
  > Maven Dependencies
  > target/generated-sources/annotations
  > target/generated-test-sources/test-annotati
  > > src
  > target
  > HELP.md
  > mvnw
  > mvnw.cmd
  > pom.xml

```

login.html

login page :

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="description" content="">
    <meta name="author" content="">
    <title>Please sign in</title>
    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta/css/bootstrap.min.css"
      rel="stylesheet" integrity="sha384-
      /Y6pD6FV/Vv2HJnA6t+vslU6fwYXjCFtcEpHbNJ0lyAFsXTsjBbfaDjzALeQsN6M"
      crossorigin="anonymous">
    <link href="https://getbootstrap.com/docs/4.0/examples/signin/signin.css" rel="stylesheet"
      integrity="sha384-
      oOE/3m0LUMPub4kaC09mrdEhIc+e3exm4xOGxAmuFXhBNF4hcg/6MiAXAf5p0P5
      6" crossorigin="anonymous"/>
  </head>
  <body>
    <div class="container">
      <form class="form-signin" method="post" action="/login">
        <h2 class="form-signin-heading">Please sign in</h2>
        <div class="alert alert-success" role="alert">You have been signed out</div>
        <p>
          <label for="username" class="sr-only">Username</label>
          <input type="text" id="username" name="username" class="form-control"
            placeholder="Username" required autofocus>
        </p>
        <p>
          <label for="password" class="sr-only">Password</label>
          <input type="password" id="password" name="password" class="form-control"
            placeholder="Password" required>
        </p>
        <input name="_csrf" type="hidden"
          value="YxSzD99jndn06qhYNArI_UR0lYnZgdkkSZApPGiutUQZ9SdgUSXQPrtVq-
          zZ05hgDSf8ySJNuOu94-kJf_UeBV6ehXwpxhRV" />
        <button class="btn btn-lg btn-primary btn-block" type="submit">Sign in</button>
      </form>
    </div>
  </body>
</html>
```

logout.html

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="description" content="">
    <meta name="author" content="">
    <title>Confirm Log Out?</title>
    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta/css/bootstrap.min.css"
      rel="stylesheet" integrity="sha384-
      /Y6pD6FV/Vv2HJnA6t+vsIU6fwYXjCFtcEpHbNJ0lyAFsXTsjBbfaDjzALeQsN6M"
      crossorigin="anonymous">
    <link href="https://getbootstrap.com/docs/4.0/examples/signin/signin.css" rel="stylesheet"
      integrity="sha384-
      oOE/3m0LUMPub4kaC09mrdEhIc+e3exm4xOGxAmuFXhBNF4hcg/6MiAXAf5p0P5
      6" crossorigin="anonymous"/>
  </head>
  <body>
    <div class="container">
      <form class="form-signin" method="post" action="/logout">
        <h2 class="form-signin-heading">Are you sure you want to log out?</h2>
        <input name="_csrf" type="hidden" value="C-yWbXKOzTA1L-
          20Fnf48Gi4C4T0s9cHoVX-l-
          vTtY7s_uXjP9z1DhTs9QAYS97VJlrMw1jbJryV0LMqlzGYro21gb_bm9fQ" />
        <button class="btn btn-lg btn-primary btn-block" type="submit">Log Out</button>
      </form>
    </div>
  </body>
</html>
```

StudentController.java

```
@RestController
public class StudentController {

    @Autowired
    private StudentService studentService;

    @GetMapping("/students")
    public ResponseEntity<List<Student>> getStudents(){

        return ResponseEntity.ok(studentService.getStudents());

    }

    @PostMapping("/students")
    public ResponseEntity<Student> addStudent(@RequestBody Student student ){
        if(studentService.addStudent(student)) {
            return ResponseEntity.ok(student);
        }else {
            return ResponseEntity.internalServerError().build();
        }
    }
}
```

StudentService.java

```
@Service
public class StudentService {

    private static List<Student> students=new ArrayList<>(List.of(
        new Student(1,"Shiva","Java"),
        new Student(2,"Muskan","Python")
    ));

    public List<Student> getStudents(){
        return students;
    }

    public boolean addStudent(Student student) {
        return students.add(student);
    }
}
```

Student.java

```
package com.spring.security.entity;

import lombok.AllArgsConstructor;
import lombok.Data;
import lombok.NoArgsConstructor;

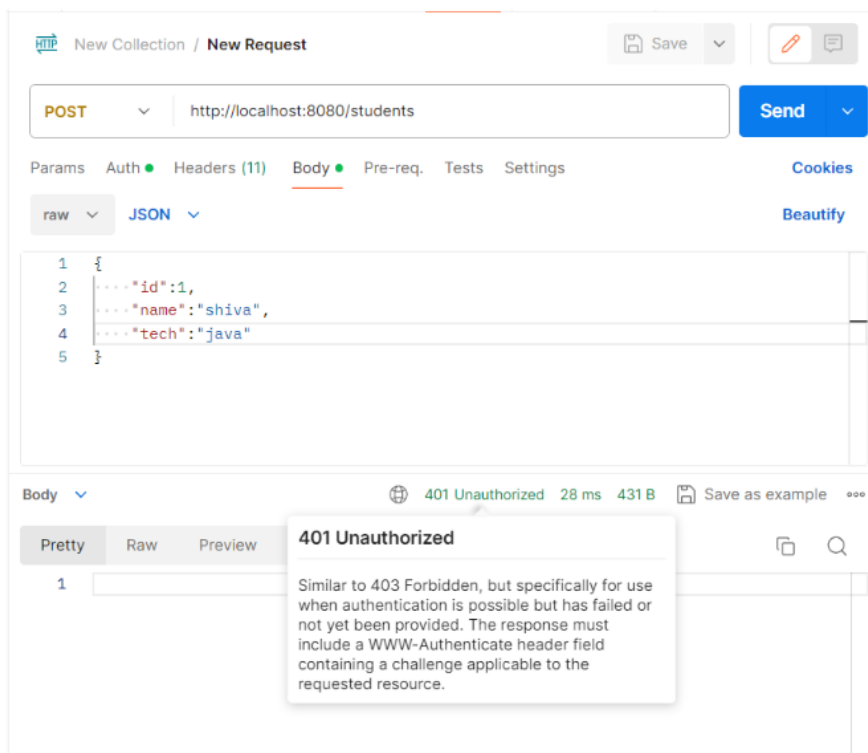
@Data
@NoArgsConstructor
@AllArgsConstructor
public class Student {

    private int id;
    private String name;
    private String tech;

}
```

Without token:

For POST method:



For GET method:



Browser

