

2、Spring Security中的CSRF

从 Spring Security4开始CSRF防护默认开启。默认会拦截请求。进行CSRF处理。CSRF为了保证不是其他第三方网站访问，要求访问时携带参数名为 `_csrf` 值为token(token 在服务端产生)的内容，如果token和服务端的token匹配成功，则正常访问。

2.1、编写控制器方法

编写控制器方法，跳转到 templates 中 login.html 页面。

```
@RequestMapping("/showLogin")
public String showLogin(){
    return "login";
}
```

2.2、新建login.html

红色部分是必须存在的否则无法正常登录。

```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml"
      xmlns:th="http://www.thymeleaf.org"
>
<head>
    <meta charset="UTF-8">
    <title>Title</title>
</head>
<body>
<form action="/login" method="post">
    <input type="hidden" th:value="${_csrf.token}" name="_csrf" th:if="${_csrf}"/>
    用户名: <input type="text" name="username" /><br/>
    密码: <input type="password" name="password" /><br/>
    <input type="submit" value="登录" />
</form>
</body>
</html>
```

修改配置类

在配置类中注释掉 CSRF 防护失效

```
//关闭csrf防护
// http.csrf().disable();
```