Spring Boot Security – Enabling CSRF Protection

In a previous post we had implemented Spring Boot Security – Password Encoding Using Bcrypt.

But till now in all our examples we had disabled CSRF.

CSRF stands for Cross-Site Request Forgery.

It is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated.

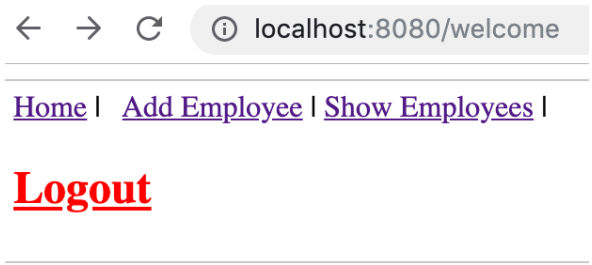
CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.

1. Continue with ***"boot-security-loginwith-users"***

2. RUN the APP

Visit ***http://localhost:8080/welcome***

3. Login as an ADMIN ROLE user



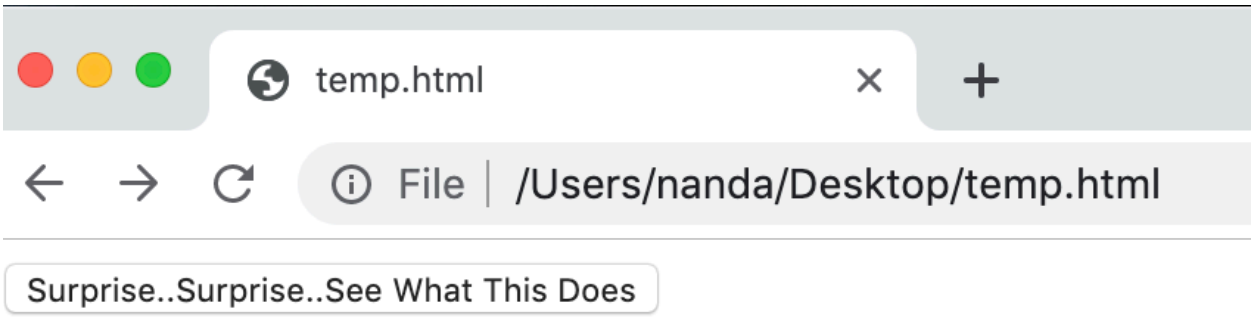
4. DO NOT close the browser

5. Create a HTML page and open it on the same browser

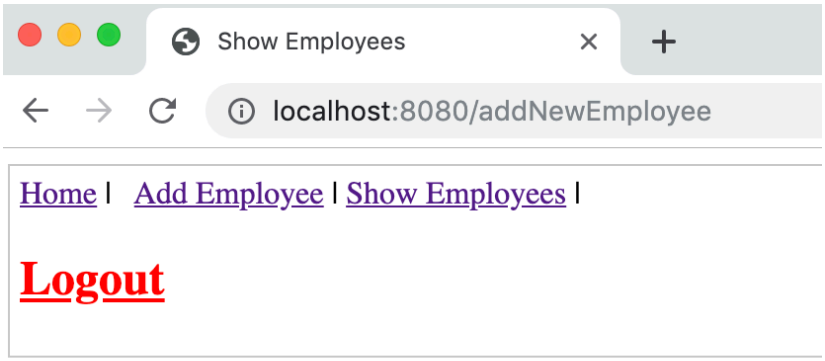
temp.html

```
<form method = "post" action="http://localhost:8080/
addNewEmployee">
<input id ="empId" type="hidden" name="empId" value="Hacker001"/
>
<input id ="empName" type="hidden" name="empName"
value="hacker"/>
<input type="SUBMIT" value="Surprise..Surprise..See What This
Does" />
</form>
```

Browser –> File –> Open –> temp.html



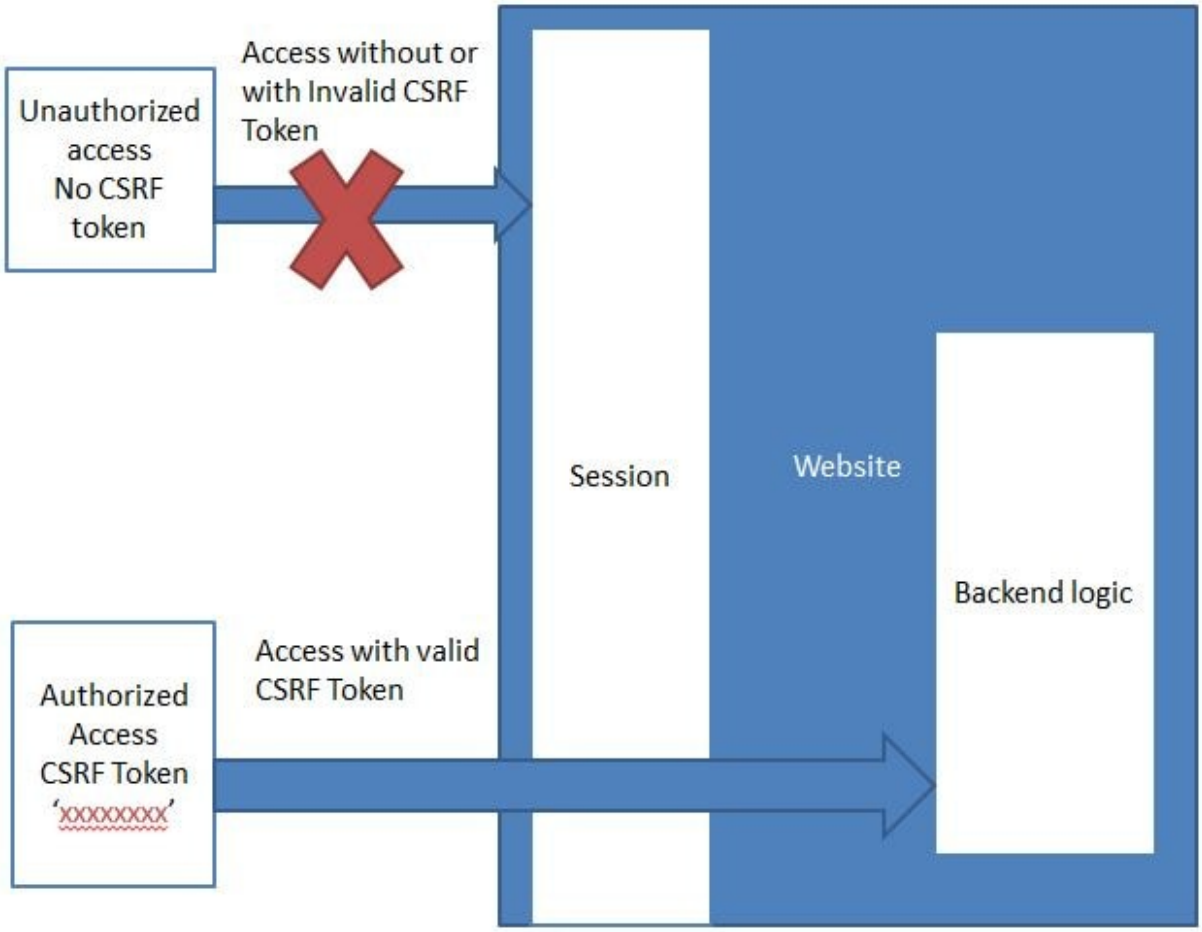
6. It adds a record into your database from an external HTML web page



Show All Employees

- Employee [empId=125, empName=Thomas]
- Employee [empId=175, empName=Joe]
- Employee [empId=Hacker001, empName=hacker]

Need to enable CSRF to avoid these unauthorized injections



7. Add a dependency for Spring Security Taglibs

pom.xml

```
<dependency>
                <groupId>org.springframework.security</groupId>
                <artifactId>spring-security-taglibs</artifactId>
          </dependency>
```

8. Next we modify the security configuration to enable CSRF by commenting the csrf disabled command .

EmployeeSecurityConfiguration.java

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

9. Next in all the jsp pages where you have a <FORM> tag, change them to use Spring Form Tag Library. So, you need the following in JSP's with forms:

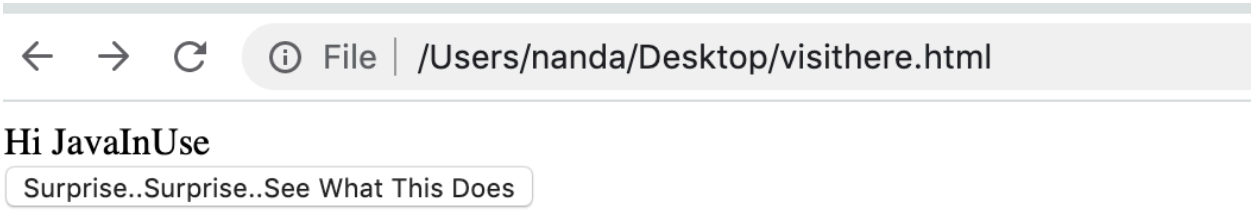
```
<%@ taglib prefix="form" uri="http://www.springframework.org/tags/form"%>

<form:form method="POST" action="/login" class="form-signin">
```

You can observe that Spring Form Tag adds a CSRF token automatically as a Hidden Form Field.

(This feature of Spring 5.0 onwards).

10.


File | /Users/nanda/Desktop/visithere.html
Hi JavaInUse
Surprise..Surprise..See What This Does

11.


localhost:8080/addNewEmployee
Whitelabel Error Page
This application has no explicit mapping for /error, so you are seeing this as a fallback.
Fri Jan 10 12:49:34 EST 2020
There was an unexpected error (type=Forbidden, status=403).
Invalid CSRF Token 'null' was found on the request parameter '_csrf' or header 'X-CSRF-TOKEN'.