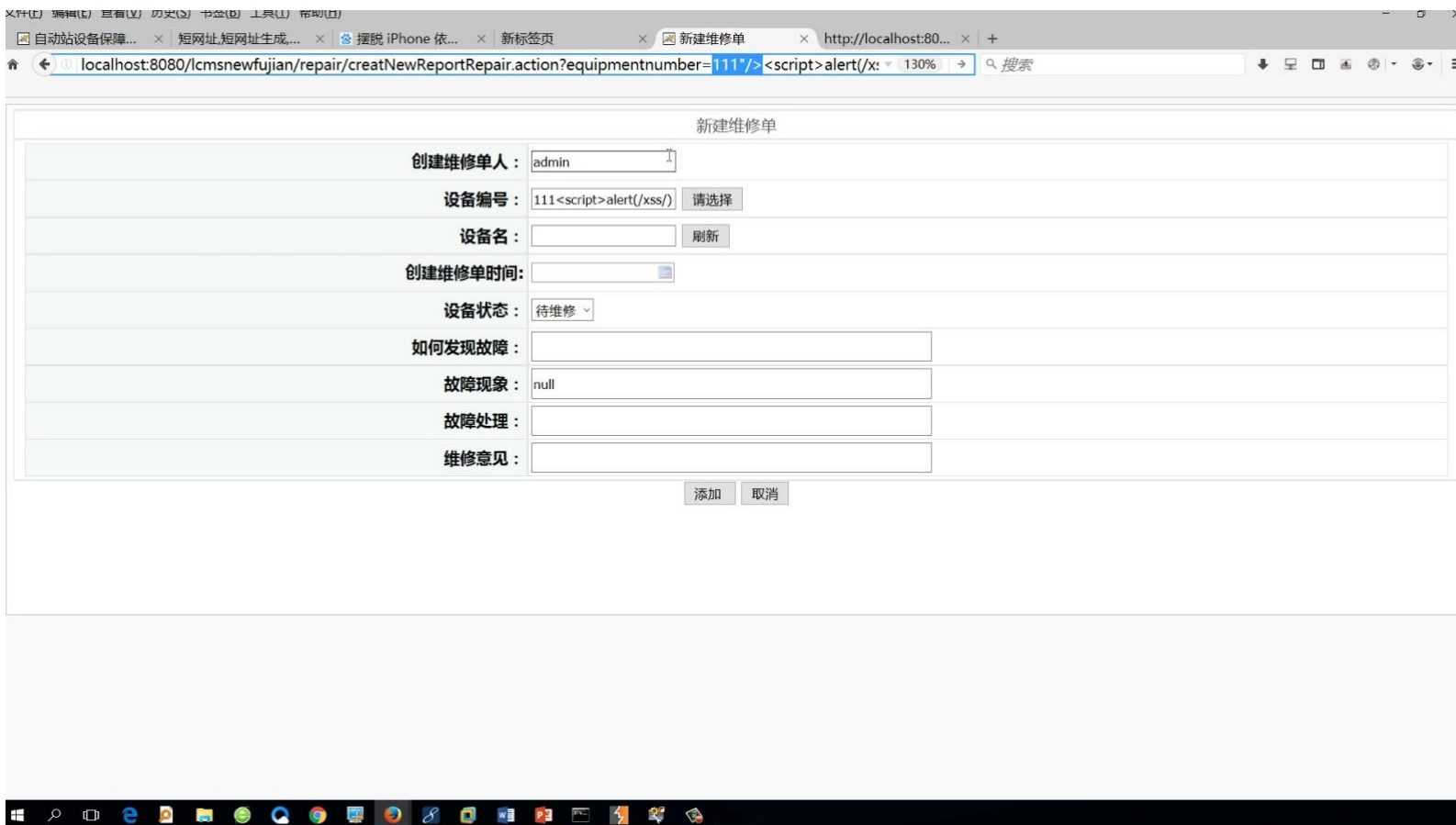


java代码审计 深度解析

第七课 反射型XSS黑盒验证



```
文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)
自动站设备保障... 短网址,短网址生成... 摆脱 iPhone 依... 新标签页 新建维修单 http://localhost:80...
view-source:http://localhost:8080/lcmsnewfujian/repair/creatNewReportRepair.action?equipmentnumber=111 130% 搜索
68
69
70
71 <td class="left_title_2" style="padding-left:100px" >
72     创建维修单人:
73 </td>
74 <td class="tdEditContent">
75     <input name="domaintanpeople" id="domaintanpeople" value="admin"/>
76 </td>
77 </tr>
78
79 <tr>
80 <td class="left_title_1" style="padding-left:100px">
81     设备编号:
82 </td>
83
84 <td class="tdEditContent" >
85
86     <input name="place" id="place" readonly="readonly" value="111<script>alert(/xss/)</script>"/>
87 <input type="button" onclick="openWin('findEquipmentNumber.action','请选择',780,500,0);" value="请选择" class="seLect"/>
88
89 </td>
90 </tr>
91
92 <tr>
93 <td class="left_title_2" style="padding-left:100px">
94     设备名:
95 </td>
96
97 <td class="tdEditContent">
98
99
100 <input name="stationname" id="stationname" readonly="readonly" value="" />
101 <!-- <input name="stationname" id="stationname" readonly="readonly" value="" /-->
102
103 <input type="button" onclick="selectStation()" value="刷新" class="seLect"/>
104
alert
```





谢谢观赏