风险等级：**高危**

漏洞说明：

存储型XSS是危害最大的一类XSS，攻击代码被直接存入数据库中，其他用户在客户端打开时就会自动执行这些攻击代码。

漏洞详情：

影响域名：

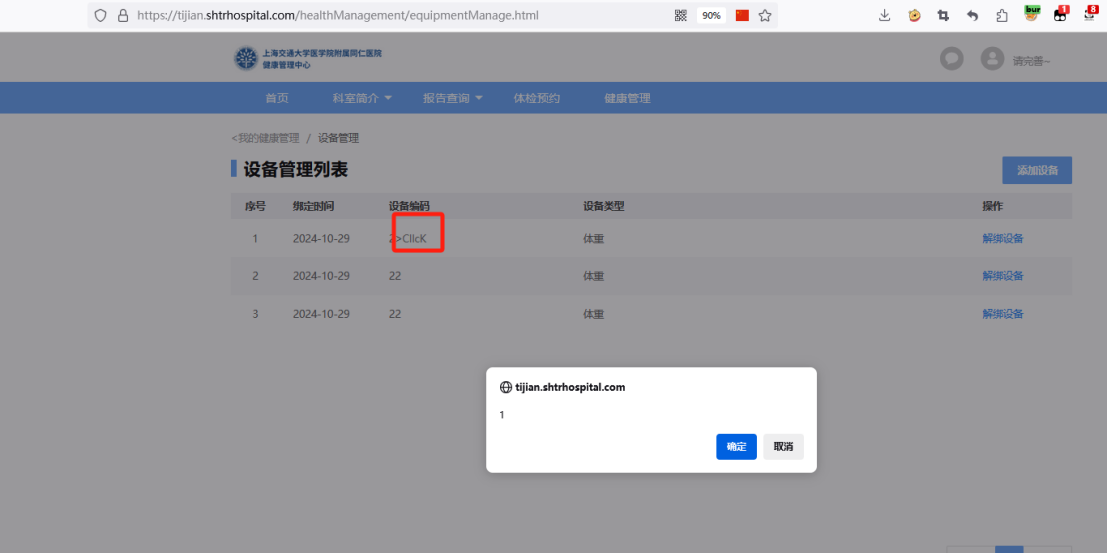
https://tijian.shtrhospital.com/healthManagement/myHealthManage.html

漏洞过程：

在健康数据添加设备



2.抓包插入payload：2>&lt;a HrEf=JaVaScRiPt:confirm`1`>CllcK&lt;/a> 完成后点击CllcK成功弹框



解决建议：

对产生漏洞模块的传入参数进行有效性检测，对如上存在漏洞页面当中的标签的传入允许值进行限定：

1.ID类型的只允许0-9的整型数字；

2.Name等字符类型的只允许a-z的英文字母；

3.当客户端输入限定值意外的字符后，立即转向自定义的错误页，而不能使用服务器默认的错误输出方式；

4.对客户端提交的字符进行过滤，禁止(‘、”、+、%、&、<、>、/、、（、）、;、script 、iframe 、src 、and、or、 onmouseover 、prompt等)特殊字符的传入。客户提交的方式包含get，post，cookie，user-agent，referrer，accept-language等；

5.对应用层防火墙配置策略进行审查，是否配置了过滤特殊字符。

6.禁止上传html、htm等可被浏览器解释为网页的文件，或使用下载的方式进行此类文件的传输；

7.使用html解析组件对富文本数据进行分析，禁止富文本元素中的任何script块、事件属性输入系统。