# 跨站脚本漏洞

### 风险分析

攻击者可以通过构造URL注入JavaScript、VBScript、ActiveX、HTML或者Flash的手段，利用跨站脚本漏洞欺骗用户，收集Cookie等相关数据并冒充其他用户。通过精心构造的恶意代码，可以让访问者访问非法网站或下载恶意木马，如果再结合其他攻击手段（如社会工程学、提权等），甚至可以获取系统的管理权限。

### 测试详情

下面是测试截图：



### 风险等级

高危

### 修复建议

对用户输入的数据进行全面安全检查或过滤，尤其注意检查是否包含HTML特殊字符。这些检查或过滤必须在服务器端完成，建议过滤的常见危险字符如下：