漏洞扫描报告

|  |  |  |
| --- | --- | --- |
| [&你的姓名&] | [&日期&] | 得分：[&得分&] |

域名：[&域名&]

## 得分分布

&图片&

## Playload

&playload&

## 修复建议

漏洞修复建议：

第一、控制脚本注入的语法要素。比如:JavaScript离不开:“<”、“>”、“(”、“）”、“;”...等等，我们只需要在输入或输出时对其进行字符过滤或转义处理就即可。一般我们会采用转义的方式来处理，转义字符是会使用到HTML的原始码，因为原始码是可以被浏览器直接识别的，所以使用起来非常方便。允许可输入的字符串长度限制也可以一定程度上控制脚本注入。

第二、所有的过滤、检测、限制等策略，建议在Web Server那一端去完成，而不是使用客户端的JavaScript或者VBScript去做简单的检查。因为真正的攻击者可以绕过你精心设计制作的客户端进行过滤、检测或限制手段。