XSS攻击原理：

恶意web用户将代码植入到提供给其它用户使用的页面中，如果程序没有经过过滤或者过滤敏感字符不严密就直接输出或者写入数据库。合法用户在访问这些页面的时候，程序将数据库里面的信息输出，这些恶意代码就会被执行

XSS攻击防范方法：

1. 过滤”<”和”>”标记XSS跨站攻击的最终目标是引入script代码在用户的浏览器中执行，所以最基本最简单的过滤方法，就是转换”<”和’>”标记。

2. HTML属性过滤。

3. 过滤特殊字符：&、回车和空格。