**XSS攻击防范**

XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，但实际上也可以包括Java、 VBScript、ActiveX、 Flash 或者甚至是普通的HTML。攻击成功后，攻击者可能得到包括但不限于更高的权限（如执行一些操作）、私密网页内容、会话和cookie等各种内容。

**什么是XSS攻击**

XSS跨站脚本攻击:黑客想尽一切方法 将一段脚本内容放到目标网站的目标浏览器上解释执行!!

## XSS防御方案

通过以上实验 我们得出防御XSS攻击的有效方式是对输入进行过滤!!!  
有效方式有如下:  
1. 部署WAF Web 应用层防火墙  
2. 过滤所有HTTML JS CSS标签  
3. 过滤异常字符编码

## XSS 过滤

CodeIgniter 自带有一个 XSS 过滤器，这个过滤器可以查找一些 XSS 的常用技术， 例如向你的数据中嵌入恶意的 JavaScript 脚本，劫持 cookie 信息或其他一些技术。 XSS 过滤器在 [这里](https://codeigniter.org.cn/userguide3/libraries/security.html) 有更详细的描述。

**注解**

XSS 过滤 只应该在输出数据时使用 。 对输入的数据进行过滤可能会 在无意中对数据造成修改，例如过滤密码中的特殊字符，这样会降低安全性， 而不是提高安全性。