**跨站脚本攻击**

1）跨站脚本攻击(Cross Site Scripting)，为不和层叠样式表(Cascading Style Sheets, CSS)的缩写混淆。故将跨站脚本攻击缩写为XSS。

2）XSS工作原理

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。

3）XSS漏洞的分类

1.本地利用漏洞，这种漏洞存在于页面中客户端脚本自身；

2.反射式漏洞，这种漏洞和类型A有些类似，不同的是Web客户端使用Server端脚本生成页面为用户提供数据时，如果未经验证的用户数据被包含在页面中而未经HTML实体编码，客户端代码便能够注入到动态页面中；

3.存储式漏洞，该类型是应用最为广泛而且有可能影响到Web服务器自身安全的漏洞，攻击者将攻击脚本上传到Web服务器上，使得所有访问该页面的用户都面临信息泄漏的可能，其中也包括了Web服务器的管理员。

4）XSS攻击的危害

1.盗取用户cookie；

2.盗取各类用户帐号，如机器登录帐号、用户网银帐号、各类管理员帐号；

3.控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力；

4.盗窃企业重要的具有商业价值的资料；

5.强制发送电子邮件；

6.网站挂马；

存储式跨站脚本漏洞检测：

一般留言系统可能存在该漏洞：

在留言框中输入：<script>alert(“xss test”)</script>

刷新留言板，若有JS脚本弹框，则说明存在该漏洞。

<iframe src="http://www.xxxx.com"></iframe>//将恶意网址插入到留言系统中

<iframe src="http://www.xxxx.com" width=”0” height=”0”></iframe>// 将而已网址隐藏起来

<script>document.write(document.cookie)</script>//利用存储式漏洞盗取用户cookie