跨站脚本攻击防御

跨站脚本攻击防御

跨站脚本攻击（cross-site scripting，XSS）是 Web 开发人员面对的严重安全问题。这种攻击允许恶意网站操作人员滥用 Web 用户对不相关的第三方网站的信任，在终端用户系统上执行任意脚本。XSS 攻击发生时，恶意人士在其他用户的浏览器中运行恶意浏览器脚本。本专题将介绍跨站脚本攻击（XSS）以及如何进行防御。

跨站脚本攻击简介

跨站脚本攻击（cross-site scripting，XSS）允许恶意网站操作人员滥用 Web 用户对不相关的第三方网站的信任，在终端用户系统上执行任意脚本。XSS 攻击发生时，恶意人士在其他用户的浏览器中运行恶意浏览器脚本。本部分将会介绍跨站脚本攻击（Cross-site scripting，XSS）的攻击原理。

- 跨站脚本攻击解析
- XSS——你会受到攻击吗？
- 跨站脚本攻击（XSS）进化了吗？

跨站脚本攻击漏洞

微软和 Mozilla 的浏览器中都曾经出现过跨站脚本攻击（XSS）漏洞，并发布了修复补丁，在本部分中介绍微软和 Mozilla 的漏洞修复补丁外，还将介绍发现跨站脚本攻击漏洞的 Fuzzing 技术。

- 微软解决 IE 跨站脚本攻击
- Mozilla 修复跨站脚本漏洞
- Fuzzing 可以有效地挖掘跨站点脚本的漏洞吗？

跨站脚本攻击防御

跨站脚本攻击（XSS）包括一个收集用户输入信息，并且不经过任何过滤逐字向用户显示的网站（例如一个银行或者电子商务网站）。攻击者可以创建 Web 内容来访问这样的网站，提供包括浏览器脚本的用户输入信息，那么应该如何防御跨站脚本攻击呢？限制特殊字符的使用，可以帮助防范的 XSS 漏洞的出现吗？

- 如何防御跨站脚本攻击
- 防御跨站点脚本攻击的新策略
- 防御跨站脚本攻击 拒绝特殊字符

跨站脚本攻击解析

跨站脚本攻击（cross-site scripting，XSS）是 Web 开发人员面对的严重安全问题。这种攻击允许恶意网站操作人员滥用 Web 用户对不相关的第三方网站的信任，在终端用户系统上执行任意脚本。

描述跨站脚本攻击最简单地方法是使用案例。假如恶意网站 www.malicious.com 的操作员 Mal 决定利用来自 Acme Widgets 的影响用户的漏洞。Mal 知道 Acme 操作企业内部互联网站，而网站上含有 www.feedback.acme/form.htm 的反馈形式。这种形式可以处理用于的反馈并显示确认页面，感谢用户提交并显示输入到页面的数据。Mal 还知道 Acme 的用于把 www.feedback.acme 网站列为了受信网站，而他的网站 www.malicious.com 是不受信任的网站。

为了进行攻击，Mal 在网站中加了超级链接，写上“免费啤酒，点击这里！”（或者其他的），并编写代码向 Web 网页提交数据，处理来自 www.feedback.acme/form.htm 的输入信息。在反馈中，他输入“谢谢”信息。

当用户点击“免费啤酒，点击这里！”的链接，他或她就会无意间向受信网站提交格式，然后他们的浏览器显示感谢他们输入的信息。但是，当浏览器在标签中遇到页面的一部分的时候，它就会执行 Web 脚本代码。

现在，你可能会问把用户从 Mal 的网站导向 Acme 的网站有什么好处啊。它存在于收信任的关系中。当然，Mal 可以简单地把脚本放在自己的网站上，绕过这种情况中跨站的部分。但是，在这种情况下，Mal 的代码可以通过浏览器队不受信任网站的规则处理掉。通过使用跨站脚本攻击，他可以有效地劫持 Acme 用户和 Acme 企业内网之间的受信关系，并根据浏览器对受信网站的规则执行他的代码是最好的解决方案。

不幸的是，跨站脚本漏洞没有简单的修复补丁。Web 开发人员必须在用户浏览器上显示之前，认真过滤掉需要处理数据的标签和其他任何敏感 HTML 元素。和很多 Web 安全问题一样，由注重安全意识的开发人员警惕注意安全项目。

(作者：Mike Chapple　译者：Tina Guo 来源：TechTarget 中国)

XSS——你会受到攻击吗？

跨站脚本攻击（Cross-site scripting，XSS）使攻击者可以向网站发送自定义请求，造成被修改的 Web 或者邮件代码被发送给其它用户。也就是说，它允许攻击者利用 Internet 服务器中的漏洞或者弱点向其它用户发送恶意代码。XSS 攻击被用于利用受害者系统上的漏洞发送恶意代码而不是攻击系统本身。

服务器的最严重的问题，它仍然很重要，需要严肃对待。通过 XSS 攻击发送给用户脚本或者代码可以在受害系统中的浏览器或者邮件查看其的安全环境中运行。在很多情况下，这可以允许对用户的所有个人数据资料以及系统本身相当大部分的全面读写访问权，例如驱动文件和配置设置。

在 Microsoft Internet Security and Acceleration (ISA) Server 2000 中曾经出现的漏洞就可以允许 XSS。攻击者可以改变不成功页面请求中的错误页面或者从 ISA 向客户端发送的无效数据提交。错误页面可以更改，这样他们就可以把受害者导向下在恶意代码或者访问恶意网站。受到攻击的错误页面还可以在受害系统上强制自动下载或者进行 URL 活动。

上面提到的 ISA 中的漏洞可以通过简单的补丁修复。

（作者：James Michael Stewart　译者：Tina Guo 来源：TechTarget 中国）

跨站脚本攻击（XSS）进化了吗？

问：跨站脚本有没有新的变化？它还是十几年前的旧式攻击吗？为什么所有的混乱中都有它？

答：目前的跨站脚本攻击（cross-site scripting，XSS）策略与上个世纪末的攻击已经大不一样了。当时黑客的手段是突然出现的对话框和窃取浏览器中的电子商务cookie。虽然这些早期的攻击依然存在，但是攻击已经变得更加严重了。随着Asynchronous JavaScript 和 XML (AJAX)等新开发方式的出现，网站推到浏览器的脚本的能力比以前的更强了。

为了了解发生了什么，考虑这种攻击的情况：你发现自己正在属于攻击者的网站上浏览，或者甚至是在即使是在含有从其他用户获取的清白的网站，例如社交网站、拍卖网站或者 Web 邮件网站。（如果没有恰当的消除用户的输入过滤浏览脚本，清白的网站可能会产生 XSS 漏洞。）一旦出现这种情况，恶意脚本程序都会忠实的传送到你的浏览器上。浏览器然后运行脚本，并把它们作为网站传送来的内容解读。

“然后呢？”你会问。原罪就要发生了。在浏览器上运行的脚本，可以在网站上做任何你可以做的事情：出价拍卖、购买物品或者在好友列表中增加讨厌的人。但是会变得更糟糕。这些脚本可以查看你的浏览器历史，观察你是否访问了什么不好的网站，并依次向攻击者返回信息。脚本还可以使用浏览器开始扫面其它网站服务器，即使是你的企业防火墙内部的服务器。

目前浏览器脚本可以做的事情令人震惊。而且，所有的一切都可能发生，因为你是在攻击者的网站上冲浪的，或者是在第三方的位置上查看的攻击者的内容。

简而言之，攻击者可以使用浏览器脚本支配受害计算机的网络控制。当然，对于脚本可以在浏览器上进行的活动也有一些限制。例如，它们不能直接访问文件系统中的任何文

件或者在计算机上运行任意程序，但是灵活的研究人员正在寻找躲避这些限制或者在内部生存并完成强大控制的方法。

怎么防御呢？在高度敏感的计算机上，可以完全用浏览器脚本。此外，确保杀毒软件的更新。还要认真观察这种趋势。可以确定的是，在这个领域有很多资料。

(作者：Ed Skoudis 译者：Tina Guo 来源：TechTarget 中国)

微软解决 IE 跨站脚本攻击

微软计划在 IE 浏览器的下一个版本中增加新的安全功能，包括防御跨站脚本攻击的功能。

IE 8 的 beta 版本将在 8 月发布。它带有 XSS（跨站脚本攻击）过滤器，此外还提供了更好防御网络钓鱼攻击的过滤器。这些功能使开发人员工容易地跨域申请资源并分享信息，更容易的改变浏览器解决 ActiveX 控件的方法。特别是，开发人员将可以编写一些控件，而这些控件只有下载的用户才可以使用。

IE 8 新功能的宣布是在 Firefox 3 发布一周后，而 Firefox 3 是在浏览器世界中 IE 的主要竞争对手的最新版本。Firefox 3 也包括了更新反恶意软件和反网络钓鱼的功能，此外还有一些其它的安全更新。自从 Firefox 最初版本的发布以来，微软已经为 IE 的安全声誉奋斗可好几年了。Mozilla Foundation 把 Firefox 定位为更安全的 IE 替代品。

但是在这种普遍使用的 IE 的最近版本中，微软在安全方面稳步前进，并且 IE 8 在这个方面更进一步。这个新的浏览器的最有魅力的、最有潜在用处的功能就是 XSS（跨站脚本攻击）过滤器。它是为了防御 Type-1 XSS 攻击。这种攻击事目前比较常见的在线攻击。很多非技术用户甚至都不知道它的存在，更不用提如何解决了。IE 8 中的 XSS 过滤器监控浏览器的所有请求和回应，并在发现 XSS 的时候，自动防御。用户将要看到请求页面的改良版本，可以看到攻击被阻止。

微软的安全软件工程师 David Ross 在宣布新功能地时候写道：“最终，我们采用了非常实用的方法——我们选择不用危及网站兼容性的方法创建过滤器。所以 XSS 过滤器可以防御最常见的 XSS 攻击，但是它不是，也不会是 XSS 万能药。这和 ASP.NET 请求确认使用的使用方法类似，但是 XSS 过滤器的功能要比 ASP.NET 功能更主动。”

此外，在 IE 的新版本中，数据执行保护（DEP， Data execution Protection）功能将在运行 Vista SP1 或 XP SP3 的电脑上默认激活。DEP 是为了阻止恶意代码写入可设定地址的内存空间。IE 的前一个版本就有这个功能，但是因为兼容性问题和其他考虑没有默认激活。

（作者：Dennis Fisher 译者：Tina Guo 来源：TechTarget 中国）

Mozilla 修复跨站脚本漏洞

Mozilla 发布了一个更新，修复几个危险的跨站脚本（XSS）漏洞。这些漏洞可以允许攻击者运行恶意代码并获得对关键系统文件的访问。

这些漏洞是在 Firefox 浏览器的版本 2 和版本 3 上发现的。Firefox3.0.5 在 SessionStore 中修复了一个 XSS 漏洞，SessionStore 是一个对话恢复功能，它包含的一个错误可以被用于在浏览器中注入恶意代码。

Mozilla 在公告中说，还修复了一个严重的 JavaScript 权限提升漏洞，包括一个 JavaScript 语句错误，这个错误可以被恶意网站用于盗取用户隐私数据，而这个用户拥有改变网站导向的权利。

Danish vulnerability clearinghouse Secunia 给漏洞的级别是高度严重。在公告中，Secunia 说有些 Mozilla 修复的错误允许攻击者绕过 cookie 设置并在浏览器对话中认证具体用户。

另外，Mizilla 宣布将减少对 FireFox 2 的支持。最新的安全更新将是这个旧版浏览器的恶最后一个更新。钓鱼保护是和 Google 通讯确认可能的钓鱼网站的功能，也在 Firefox 2 中减少了支持。Mozilla 敦促用户更新到最新版本。

(作者：SearchSecurity.com Staff 译者：Tina Guo 来源：TechTarget 中国)

Fuzzing 可以有效地挖掘跨站点脚本的漏洞吗？

问:Fuzzing 可以有效地挖掘跨站点脚本的漏洞吗？

答:简而言之，可以。在初学者看来，Fuzzing （ 模糊测试)是一个通过向软件重复发送不同输入值来挖掘该软件漏洞的过程，试图使目标程序中断或崩溃。多年来，研究人员一直使用 Fuzzer 工具软件有效地找到缓冲区溢出漏洞。在这些分析中，研究人员可以使用的工具软件有免费的通用 fuzzer，或商业性 Mu- 4000 模糊应用。为了找到一个难以确定的漏洞， fuzzer 可能花几个星期，向发送数十亿个用户输入参数，让分析过程自动进行。现在有大量免费的 fuzzers 可以提供这样的功能。

对于跨站点脚本(XSS)，一个 fuzzer 可以将不同的浏览器脚本输入到目标网站里，组合不同的字符串、功能性、编码、大小和用户输入的其它方面，来判断目标网站应用程序是将输入值反射，还是保存，并不经过任何过滤反馈回研究人员。如果 Fuzzer 的危险脚本的确畅通地返回，就表明目标应用程序很容易受到 XSS 攻击。黑客可以将脚本输入到应用程序中，并使用者的浏览器上运行。

2007 年 7 月，Google 公开宣布正在开发一个供自己内部使用的 XSS fuzzer。这个命名为 Lemon(柠檬)的项目表明 Google 已经意识到跨站点脚本的威胁，而且 fuzzer 可以帮助找到这些漏洞。在过去的一年里，Google 的应用程序已经发现一些 XSS 漏洞。设计 Lemon 的目的是为了在黑客攻击这些漏洞前，就找出漏洞，并由 Google 及时修补。目前，Lemon 仅限于 Google 内部使用，不过 Google 的员工已经在公开场合谈论这项工具。

其他免费的、公开的源代码工具也已经开始处理 XSS 模糊问题了，例如，“公开网络应用安全项目(OWASP)”的 WebScarab 扫描工具。该项目详细描述了 WebScarab 作为 XSS fuzzer 工具软件的使用方法。

Fuzzing 是有用的，但测试过程并不能找出所有的漏洞。Fuzzing 软件通常都是非智能型的;它只是向目标发出一大堆垃圾（精心挑选的垃圾，但不是真正的垃圾），旨在找到一些怪异的反应。然而，这些怪异的反应可能过于微小以至 Fuzzer 难以检测到。同样，Fuzzer 发送出的输入值可能无法包括所有的必须的技术组合，来检测目标软件的漏洞。因此，Fuzzing 本身并不能充分确保一个程序是否安全的。 一套综合的软件测 试方法会包括包括构架审查、代码审查与详细测试，Fuzzing 应该是包括在其中的一部分。

（作者：Ed Skoudis 译者：Shirley 来源：TechTarget 中国）

如何防御跨站脚本攻击

问：跨站脚本攻击可以做什么？我们如何保护我们的网站/应用？

答：跨站脚本攻击（XSS）包括一个收集用户输入信息，并且不经过任何过滤逐字向用户显示的网站（例如一个银行或者电子商务网站）。攻击者可以创建 Web 内容来访问这样的网站，提供包括浏览器脚本的用户输入信息，然后欺骗用户浏览带有这些内容的网站。例如，攻击者可以向受害者发送带有合法 URL 的电子邮件，这个 URL 会指向这个网站并作为输入信息提供浏览器脚本。攻击者也可以在新闻组或者第三方网站中加入一个链接或者在允许第三方上传内容的网站增加内容，送例如社会网络网站、Web 邮件提供者、博客网站等等。当一个受害的用户来到这个网站，那些恶意内容，包括脚本，就回到了浏览器并在那里运行。浏览器不知道这个脚本是恶意的，就运行了这个程序，而且不注意地就允许了攻击者的脚本访问这个网站的所有功能。它可以窃取 cookie 并把它们发送给攻击，或者受害用户参与到传送中。所以，不过滤用户输入信息来移除和浏览器脚本相关的潜在危险字符的电子商务网站很容易受到跨站脚本攻击。

那么 Web 网站应该如何防御跨站脚本攻击呢？Web 开发人员可以向所有用户的输入信息执行过滤代码，移除可能有害的代码，或者内把他们转成浏览器不能运行的信息（例如，>和<可以相应的转为>和<）。CodeIgniter 包括免费的 PHp 过滤代码，防御跨站脚本攻击和其他类型的攻击。了解更多 CodeIgniter 的信息可以访问 http://www.codeigniter.com。

（作者：Ed Skoudis 译者：Tina Guo 来源：TechTarget 中国）

防御跨站点脚本攻击的新策略

问：我听说的跨站点脚本攻击（XSS ）是目前最高等级的安全风险。是否有企业安全专业人员可以使用的新的策略来防御它呢？

答：跨站点脚本攻击（简称 XSS，这样我们就不会混淆它们与层叠样式表）是目前的主要攻击媒介。它们攻击从用户那里得到信息的脆弱网站，而这些网站把这些数据返回到浏览器。XSS 攻击发生时，恶意人士在其他用户的浏览器中运行一个恶意的浏览器脚本。然后，攻击者可以窃取的 cookies -或者甚至使用脆弱的电子商务网站-使浏览器忙于处理问题，使它像是受害者的浏览器。我们在 Intelguardians 的渗透测试工作中，所测试的 Web 应用大约有 80%含有 XSS 漏洞。

企业可以通过仔细过滤用户输入和输出，消除和脚本相关的=<>’″();&等字符，防范的 XSS 漏洞。在过去，大多数机构的重点是控制和过滤输入信息。当然这是一个好主意。攻击者仍然通过不受保护的输入信息流渗透到应用中。一些诱人的目标，包括磁条纹、电子数据交换的资料和纸质邮件，通过光学字符识别获得扫描和转换。如果 Web 应用开始发送攻击者的恶意浏览器脚本，用户就处于危险之中。为避免这种情况，需要过滤应用输出流量中的恶意脚本。当然，你也应该过滤合法的浏览器脚本，这些浏览器可以被用于并允许他们送到浏览器。但是，特定的数据牵引功能绝不能有浏览器脚本。在这些情况下，过滤器应该在最终页面制作并返回到浏览器之前配置。

（作者：Ed Skoudis 译者：梁冬晨 来源：TechTarget 中国）

防御跨站脚本攻击 拒绝特殊字符

问：我对防御跨站脚本攻击（XSS） 很有兴趣。如果我拒绝使用<、 >、脚本——以及容易导致恶意攻击的同等实体参数——这样的字符和词语，那么就会增加应用开发的成本。你会推荐这种“作战”方式吗？

答：不，相反，我推荐开发人员在他们的应用代码中只允许适应应用功能所必需的规定字符。这是应用开发的最佳做法。

很多企业都把安全代码作为在开发过程的最后才会发生的事情。但是，如果在开发周期的最后阶段测试应用的人说应用需要记录来保证安全性，那么应用就需要重写并重新测试，与之相结合的其他应用也是如此。这种持续的矛盾比在安全开发周期中进行的不断地安全过程成本高得多。

如果有一种领域称为“稳定”，例如，就没有理由允许<、>、;、*、--或者:作为可能参数。如果应用开发人员写的代码只允许接受已知的良好参数，就会通过减少质量担保和认证以及信赖测试的成本降低应用开发的整体成本。

(作者：John Strand 译者：Tina Guo 来源：TechTarget 中国)