Cross-Site Scripting(XSS)的类型

转载

weixin_30445169 于 2015-02-26 00:49:00 发布 40 收藏
文章标签： php javascript 数据库 ViewUI
原文链接：http://www.cnblogs.com/lightsong/p/4300466.html

本文源自：

https://www.owasp.org/index.php/Types_of_Cross-Site_Scripting

在原文理解上翻译为中文。

背景

本文描述多种不同类型的XSS攻击，和它们之间的相互关系。

最早，有两种类型的XSS攻击被定义，Stored 和 Reflected， 在二零零五年，Amit Klein定义了第三种攻击类型， DOM Based XSS攻击。

Stored 类型

见上一篇文章中的定义。 此外， 由于HTML5的降临， 和其它的浏览器技术， 攻击者的有效荷载可以持久地存储在受害者的浏览器中，例如HTML5数据库， 其不用被发送到服务器端。

Reflected 类型

见上一篇文章中的定义。

DOM Based类型

恶意数据流从源头到渗透，从未离开过浏览器， 例如源头可以是URL，或者是HTML元素。渗透是一些敏感的JS调用， 例如document.write。

XSS的类型

若干年来， 很多人认为三种XSS攻击类型是不同的，实际上三种攻击类型是可以重叠的。 一个攻击可能是Stored DOM Based XSS。这样造成概念很容易混淆，社区在二零一二年推荐使用新的术语，组织XSS攻击的分类：

1 Server XSS

2 Client XSS

Server XSS

Server XSS产生当不可信的用户提交数据被包含在服务器产生的响应中， 数据源可以来自请求， 也可以是来自存储位置。

因此， 会有两种叠加的XSS攻击：

Stored Server XSS

Reflected Server XSS

这种情况， 整个缺陷都在服务器端代码中，浏览器仅仅简单渲染服务器响应，并执行有效的内嵌脚本。

Client XSS

Client XSS发生当不可信的用户提交数据被用来更新DOM， 使用不安全的JS接口。

JS接口是不安全的， 如果其会引入有效的JS代码到DOM中。

数据源头可以来自DOM， 或者来自服务器端发送（via an AJAX call, or a page load）， 最终的来源可以来自请求， 或者来自服务器或者客户端的存储位置。

因此有两种重叠的攻击类型：Reflected Client XSS and Stored Client XSS

有了新的定义， DOM Based 类型的定义不变。DOM Based XSS仅仅是Client XSS的一个子集， 它的数据源头来自DOM的某处， 而不是来自服务器端。

考虑到 Server XSS and Client XSS 都可以是 Stored or Reflected 类型的， 新的术语产生了一个简单明了的 二乘二 矩阵， 一个轴是 Client & Server， 另外一个轴是 Stored and Reflected，如下图

Server-XSS vs Client-XSS Chart.jpg

推荐的Server XSS防御方法

Server XSS是由HTML中包含了不可信的数据导致。大多数情况下， 也是最早的最强大的防御方法是

- Context-sensitive server side output encoding （服务器端转码）

怎样执行转码，在如此链接中有详细描述 OWASP XSS (Cross Site Scripting) Prevention Cheat Sheet

输入校验 或者 数据清洗 也可以帮助预防此类攻击， 但是此法困难更加多很多， 比输出转码方法。

推荐的Client XSS预防方法

Client XSS攻击发生，由于不信任的数据被用来更新DOM，使用非安全的JS接口。

最早最强壮的防御方法：

Using safe JavaScript APIs（使用安全的JS接口）

但是，开发者往往不知道哪些接口是安全的，哪些不是，更不用说那些JS库的接口是安全的，哪些不是。

一些接口安全信息见 Unraveling some of the Mysteries around DOM Based XSS

如果你知道有个JS接口是不安全的，建议你使用安全的JS接口代替，如果不能代替， 在传送不信任的数据到JS接口前，

需要将数据执行浏览器端的转码。

OWASP指南关于如何实施转码工作见 DOM based XSS Prevention Cheat Sheet

此指南的适用性对所有类型的XSS攻击， 与数据实际从哪里来无关（Server DOM）。

References

[1] “DOM Based Cross Site Scripting or XSS of the Third Kind” (WASC writeup), Amit Klein, July 2005

http://www.webappsec.org/projects/articles/071105.shtml

Related OWASP Articles

- Cross-site Scripting (XSS)
- Stored XSS (AKA Persistent or Type I XSS)
- Reflected XSS (AKA Non-Persistent or Type II XSS)
- DOM Based XSS
- XSS (Cross Site Scripting) Prevention Cheat Sheet
- DOM based XSS Prevention Cheat Sheet

转载于:https://www.cnblogs.com/lightsong/p/4300466.html