Iframe injection

1.简介

iframe是可用于在HTML页面中嵌入一些文件(如文档，视频等)的一项技术。对iframe最简单的解释就是“iframe是一个可以在当前页面中显示其它页面内容的技术”。

-----------------------------------------------------------------------------------------------------------------

Example 1:  
<iframesrc=”http:// [www.2cto.com](http://www.2cto.com/) ”></iframe>

该例说明在当前网页中显示其它站点。

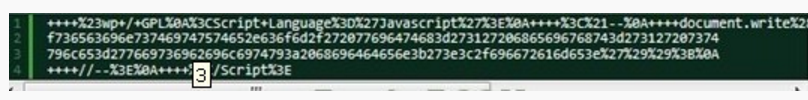
-----------------------------------------------------------------------------------------------------------------

Example 2:  
<iframesrc=’http:// [www.2cto.com](http://www.2cto.com/) /’ width=’500′ height=’600′ style=’visibility: hidden;’></iframe>

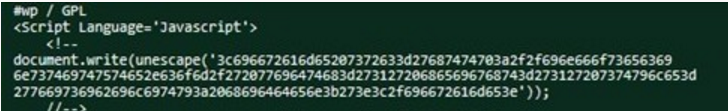
iframe中定义了宽度和高度，但是框架可见度被隐藏了，所以不能显示。由于这两个属性占用面积，一般情况下攻击者不使用它。现在，它完全可以从用户的视线中隐藏了，但是iframe仍然能够正常的运行

1. 混淆的iFrame注入攻击

混淆的iframe注入攻击是一个危险并棘手的攻击，因为它很难以被察觉，难以在网站上发现恶意的注射性代码。混淆是有隐藏交互的意思，因此难发现被注入的代码。这类攻击的目的是欺骗用户重定向到第三方网站并利用。如果使用iframe注入攻击控制了一个网站，那么很容易找到并定位注入的代码。但是使用混淆的iframe注入攻击，那么就不容易找到被注入的代码了。



这段代码看起来很正常，但是使用java解码后，如下：



这看起来像是一个合法的代码。但实际上是存在问题的。这些代码看起来似乎是十六进制，我们用十六进制解码器解码后如下：

实际结果是：  
<iframesrc=’http://freebuf.com/’ width=’1′ height=’1′ style=’visibility: hidden;’></iframe>

现在可以想象为何混淆的iframe注入攻击很难被发现了。