ES6中的模板字符串和新XSS Payload

阿里聚安全 / 2016-11-11 07:55:27 / 浏览数 4123 安全技术 漏洞分析 顶(0) 踩(0)

ES6中的模板字符串和新XSS Payload

众所周知，在XSS的实战对抗中，由于防守方经常会采用各种各样严格的过滤手段来过滤输入，所以我们使用的XSS Payload也会根据实际情况作出各种各样的调整，最常见的如避免括号，避免引号，避免关键字等，以绕开过滤函数的检查，从而成功将代码注入到网页中运行。
在传统的XSS Payload变形中，常用的无非有以下几种：

1. 使用String.fromCharCode来避免关键字，如String.fromCharCode(97,108,101,114,116,40,49,41);
2. 使用URL编码来避免括号的识别，如location='alert%281%29';
   3.使用正则对象的特点来避开引号，如alert(/1/);
   在多年的研究中基本上传统的变形手段都被研究的差不多了，很难找到创新的绕开手段。
   然而，近几年ECMAScript新版本的不断发展和推行，在带来了各种激动人心的语言特性的同时，也不可避免地带来了一些新的安全挑战。本文中所说的模板字符串，便是
   6草案中的一种新特性。
   如MDN 中所述，模板字符串（Template literals）允许嵌入表达式，并且支持多行字符串和字符串插补特性。基本语法为以下几种：

其中第一行为最基本用法，即使用反引号 (`) 来代替普通字符串中的用双引号和单引号。
第二行为多行字符串用法，即反引号中文本可以直接接受换行而不必使用\n换行符来强制换行。
第三行则为模板字符串的最核心用法，即反引号中的${expression}占位符中expression可以为任意的JavaScript表达式，甚至为模板字符串。
第四行则为使模板字符串变强大的最主要原因，如果一个模板字符串由表达式开头，则该字符串被称为带标签的模板字符串，该表达式通常是一个函数，它会在模板字符串处
第三行的用法我们称之为"表达式插补"，在普通字符串中嵌入表达式时，必须使用如下语法：

现在通过模板字符串，我们可以使用一种更优雅的方式来表示：

第四行的用法我们称之为"带标签的模板字符串"，模板字符串的一种更高级的形式称为带标签的模板字符串。它允许您通过标签函数修改模板字符串的输出。标签函数的第一
最后，标签函数返回处理好的字符串。在后面的示例中，标签函数的名称可以为任意的合法标示符。

在了解了以上知识后，我们不难发现，对于一个最简单的XSS Payload：alert('A')来说，我们可以利用上述例子第一行的知识，使用""■■■■■■■■■■alert(A)■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■alert■■■■■■■■ alertA■■■■■■■ECMAScript 6■■■■■■■■■ ■code point■■■■■Unicode■■■■■■■■■"■■■■+u+■■"■■■■■■■alert■■■■■■■■■■■■■■■Unicode■■■■■■alert■■■■■■■payload■■\u0061\u006c\
此时最终的payload已经完全见不到alert关键字，括号，以及引号了。测试结果如下：

如果需要将这个payload当做字符串作为函数参数，则可以按照表达式插补的写法，直接在外层套一个${}即可，例如：${alertA} 或 ${\u0061\u006c\u0065\u0072\u0074A} 。则console.log(${alertA})也可以弹出。
以上的方法经测试，在最新版本的Chrome，Firefox以及Edge浏览器中均可以执行。我们可以看出，ES6的新方法给我们带来便利的同时，也给XSS字符的安全监测带来了新

作者：负羽，更多安全类文章，请访问阿里聚安全博客

上一篇：【独家连载】mysql注入天书（一... 下一篇：【独家】闲聊阿里加固（一）

1. 5 条回复

px1624 2016-11-22 02:30:40

这文章不错啊，竟然没人评论，赞一个！

0 回复Ta

 紫霞仙子 2016-11-22 02:32:59

666666666666

0 回复Ta

 monika 2017-11-08 10:58:03

<ImG/src=1 OnErRoR=${\u0061\u006c\u0065\u0072\u0074A}>

<script>`${\u0061\u006c\u0065\u0072\u0074`A`}`</script> <svg><script>`${\u0061\u006c\u0065\u0072\u0074`1`}`</script>

0 回复Ta

 monika 2017-11-08 11:00:06

0 回复Ta

monika 2017-11-08 11:01:37

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板