登录

postMessage跨域

bywalks / 2018-05-07 21:12:02 / 浏览数 1969 安全技术 技术讨论 顶(0) 踩(0)

前言：

postMessage是HTML5衍生出来的，用来规范跨域的问题。但由于使用者不注意一些安全性，可能会产生一些漏洞，这篇文章介绍可能产生的问题。

目录：

0x01：如何工作

0x02：可能的三个漏洞

0x03：正确代码

如何工作

为了跨域去发送一些数据，应用会用如下的语句去发送

```
targetWindow.postMessage(data, "*");
data■■■■"*"■■■■
```

-
为了去接受一些数据，接收端会添加一个事件监听器用来接受跨域传输过来的数据

```
window.addEventListener("message", function(message){console.log(message.data)});
```

-

-
可能的三个问题

Issue One:

```
targetWindow.postMessage(data, "*");
```

如上代码，第一个问题就产生在这里，当postMessage的第二个参数为"*"时，也就意味着数据可以被跨域传送到任何地方，如果这个数据为个人数据或者其他隐私呢？结果

-

Issue Two:

```
//Listener on
window.addEventListener("message", function(message){
   if(/^http://www.bywalks.com$/.test(message.origin)){
        console.log(message.data);
  }});
```

如上代码，这是产生在接收端的问题。上面的代码通过正则来规范传输端，这里我们要着重关注"."，你看出问题了么？origin可以是http://www.bywalks.com
同时也可以是http://wwwabywalks.com
因为在正则里面，"."匹配\r之外的任意单字符。

-

Issue Three:

```
//Listener on
window.addEventListener("message", function(message){
  if(/^http://www\.bywalks\.com$/.test(message.origin)){
     document.getElementById("message").innerHTML = message.data;
  }});
```

这是一个基于DOM的XSS，如上代码，id=message的事件文本内容为跨域传送来的data，这里规范了origin为http://www.bywalks.com

那么是否我们可以在http://www.bywalks.com（传输端）上面找到一个XSS漏洞，也就意味着在接收端找到一个XSS漏洞呢？要知道，在网站上载入第三方JS是一个很常见

正确代码

```
var data = JSON.parse(decodeURIComponent(document.getElementById('data').value));

// cross browser origin determination
var origin = (window.location.protocol + '//' + window.location.hostname
 + (window.location.port ? ':' + window.location.port : ''));

if (window.opener) {
 window.opener.postMessage(data, origin);
} else {
 // attempt to redirect back to the origin
 window.location = origin;
}
```

如上代码，这里就规范了origin，避免产生把data发送到其他网站的信息泄露事件
与此同时，接收端也应该做出限制。

上一篇：【Struts2-命令-代码执行漏... 下一篇：CVE-2017-9841到root提权

1. 0 条回复
   - 动动手指，沙发就是你的了！