Self XSS到存储型XSS

mntn / 2019-01-28 08:06:00 / 浏览数 3396 技术文章 翻译文章 顶(0) 踩(1)

---

原文：Self XSS to Interesting Stored XSS
作者：rohan aggarwal@nahoragg

我在Hackerone的一个程序中找到了这个XSS。关于这个存储型XSS的有趣之事在于：它反映了我尝试通过某种办法升级self-xss，好运眷顾，我成功了。
此外，我不能透露这个程序的名字，因为他们要求不要，但是如果你发现了它，我并不感到惊讶。
那么让我们来看看这个网站，我们称之为`redacted.com`
我在`redacted.com`上耗费了几个小时，试图在上面得到一个xss漏洞，但即使我找到了一个，它也会因为网站正确编码了所有内容而变成一个self-xss。
这不是一个大型网站，在每个端点尝试了XSS后，我放弃了，继续查找其他漏洞。
第二天，我在HackerOne读到了一篇关于AngularJS的模板注入的文章，并且我所遇到的情况与其相似，我之前并不知道还有这种操作。回到`redacted.com`，它也运行An

所以我尝试了一个简单的表达式，如`{{4*4}}`

如果不进行编码就会显示16，最后找到一个不进行编码的地方。现在我可以使用这个payload来产生xss了

```
{{constructor.constructor('alert("XSS")')()}}
```

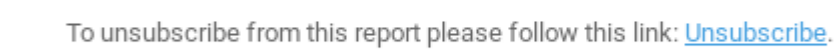
好极了！！！我发现了XSS，一分钟后我意识到。。。。DAMN，这是一个self-xss！

现在怎么办？？？

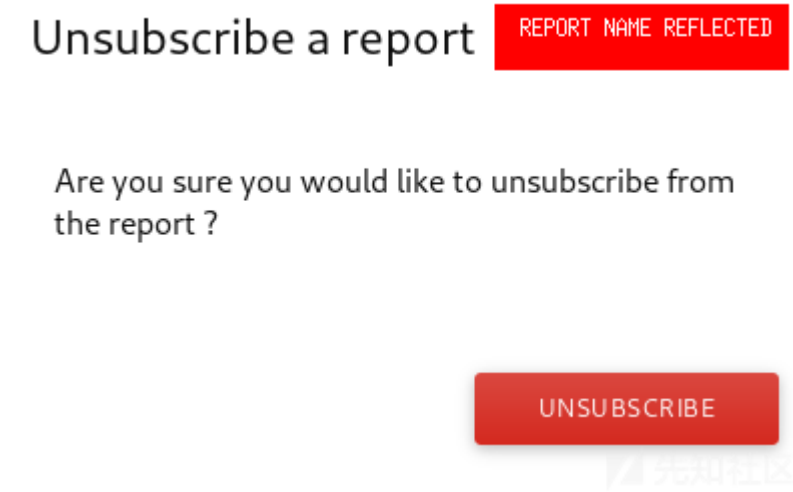
经过了几个小时的搜索之后，我找到了一个有趣的地方，它正在执行并且不需要任何的身份验证。

介绍下这个有趣的程序的背景：它有一个通过电子邮件发送报告的功能(无论这个网站在做什么)，我们可以给报告自定义敏子。这些报告是敏感的，只有能由经过身份验证的

我利用了这个功能，向我的邮箱发送了一个报告，发现一个小的取消订阅连接隐藏在角落里




打开链接，BOOM！它显示了报告的名字，没有经过任何身份验证！



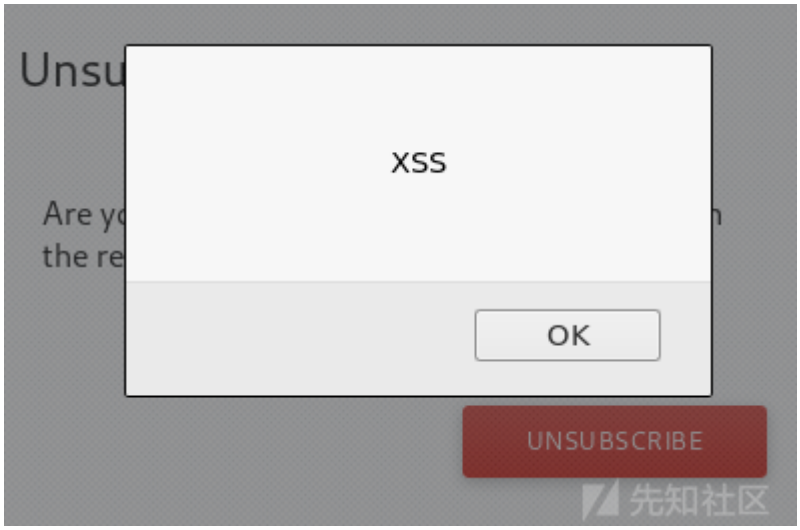

柳暗花明了！报告的名称可控并且存在xss，任何人都可以看到这个名称，那么它有可能从一个self-xss升级成存储型xss！

是时候测试它是否编码了大括号

回到发送报告功能，将报告名称命名为之前的payload：

```
{{constructor.constructor('alert("XSS")')()}}
```

并且保存发送，再次打开取消订阅的链接，BOOM！这是一个存储型XSS。




现在，任何人都可以打开取消订阅链接，xss将被执行。无论受害人是否经过身份验证，这适用于任何人。

Lesson Learned：

1. 查看应用程序上正在运行的技术并找到它们特定的漏洞
2. 在无聊时于都hackerone披露的报告
3. Try Harder On Everything In
   Application，我阅读了很多文章，但是从没有遇到过在电子邮件取消订阅链接中获得xss的经历，我本来可以报告self-xss，但是我花了更多时间，幸运的得到了更多。



上一篇：macOS/iOS漏洞之CVE-2... 下一篇：macOS/iOS漏洞之CVE-2...

1. 1 条回复

K0nJac 2019-01-29 00:19:08

很不认真的机翻

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