登录

[基于DOM的XSS]不要过分的依赖Cloudflare

Agostop / 2018-11-21 07:30:00 / 浏览数 2795 安全技术 技术讨论 顶(1) 踩(0)

翻译自：https://medium.com/bugbountywriteup/dom-based-xss-or-why-you-should-not-rely-on-cloudflare-too-much-a1aa9f0ead7d
翻译人：Ago_stop

0x00 前言

我在一个漏洞赏金计划里又发现了一个XSS漏洞。

【redacted.com】这个网站受到Cloudflare WAF保护，所以很多payload都被过滤掉了，但是该网站的实现方式实在糟糕，以至于连Cloudflare也无法保护它。

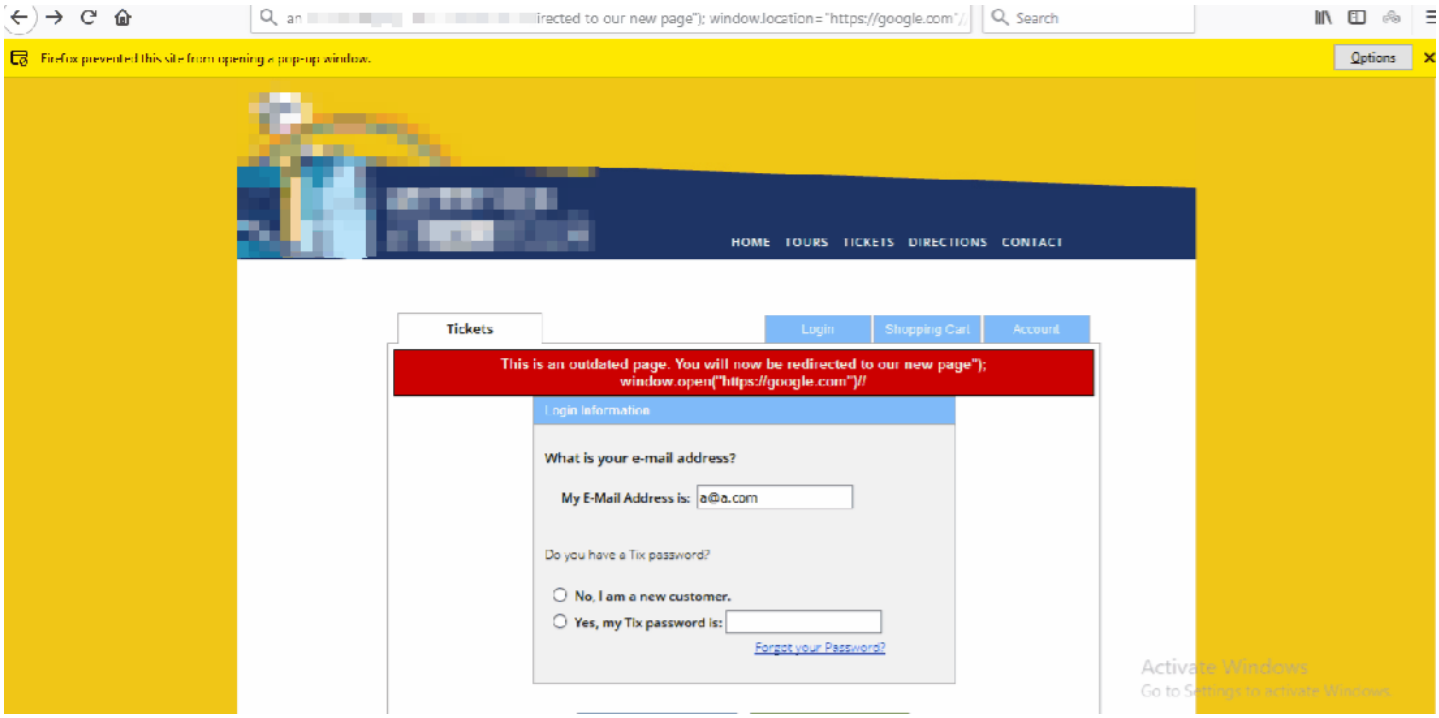
就在发现这个漏洞几天前的一个内部会议上，我还和我的同事说："不要过度的依赖防火墙和安全产品"，现在，我有了一个真实的案例可以分享了，LOL.

0x01 概述

当我触发了登录界面的一个错误时，一个名为Message的参数会反映在html主体和一个弹出框中，并没有被过滤掉。（即，Message的值被插入到JavaScript中，正好在ale

Payload:

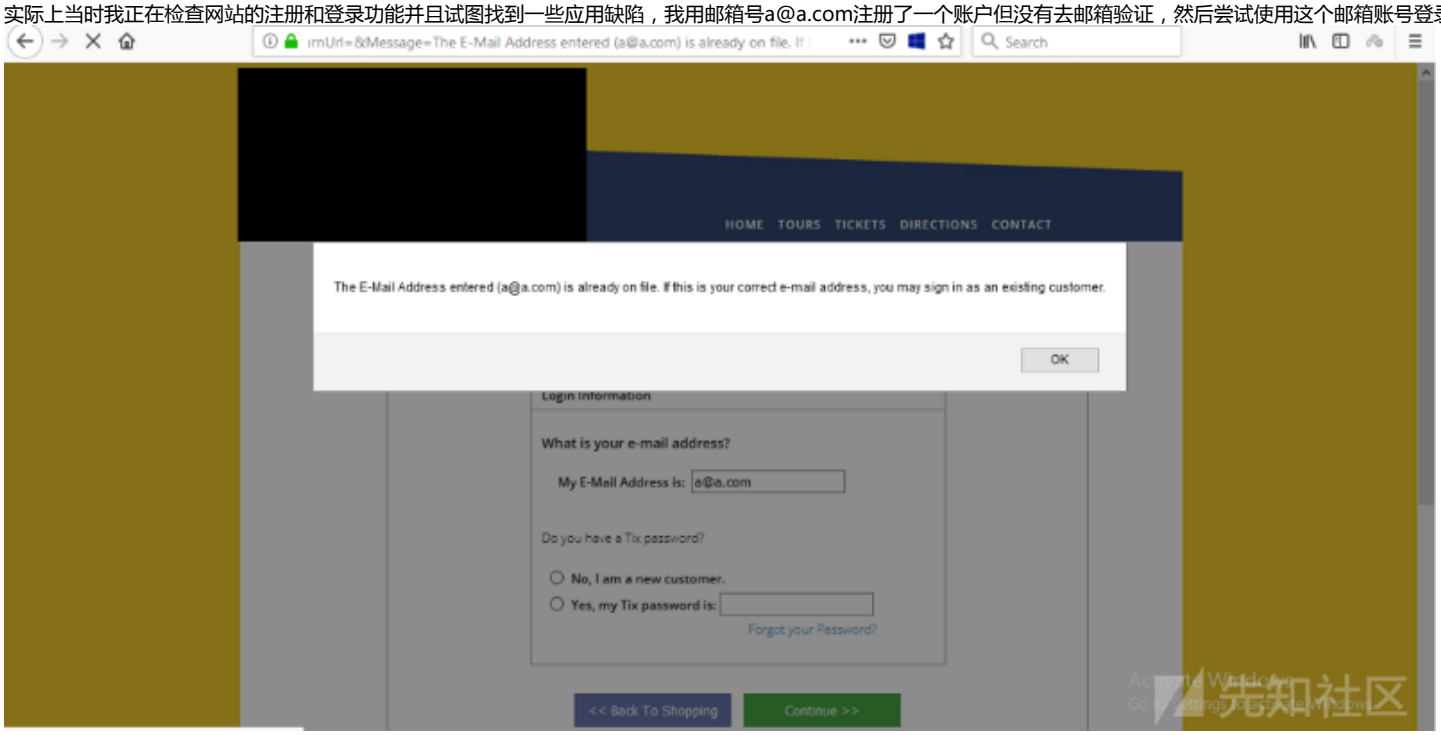
```
This is an outdated page. You will now be redirected to our new page"); window.location="https://google.com"//
```



因此，我们可以欺骗用户使其认为他们要定向到一个更新的网页，并且需要重新登录（这里重定向到google来做演示）

0x02 漏洞发现

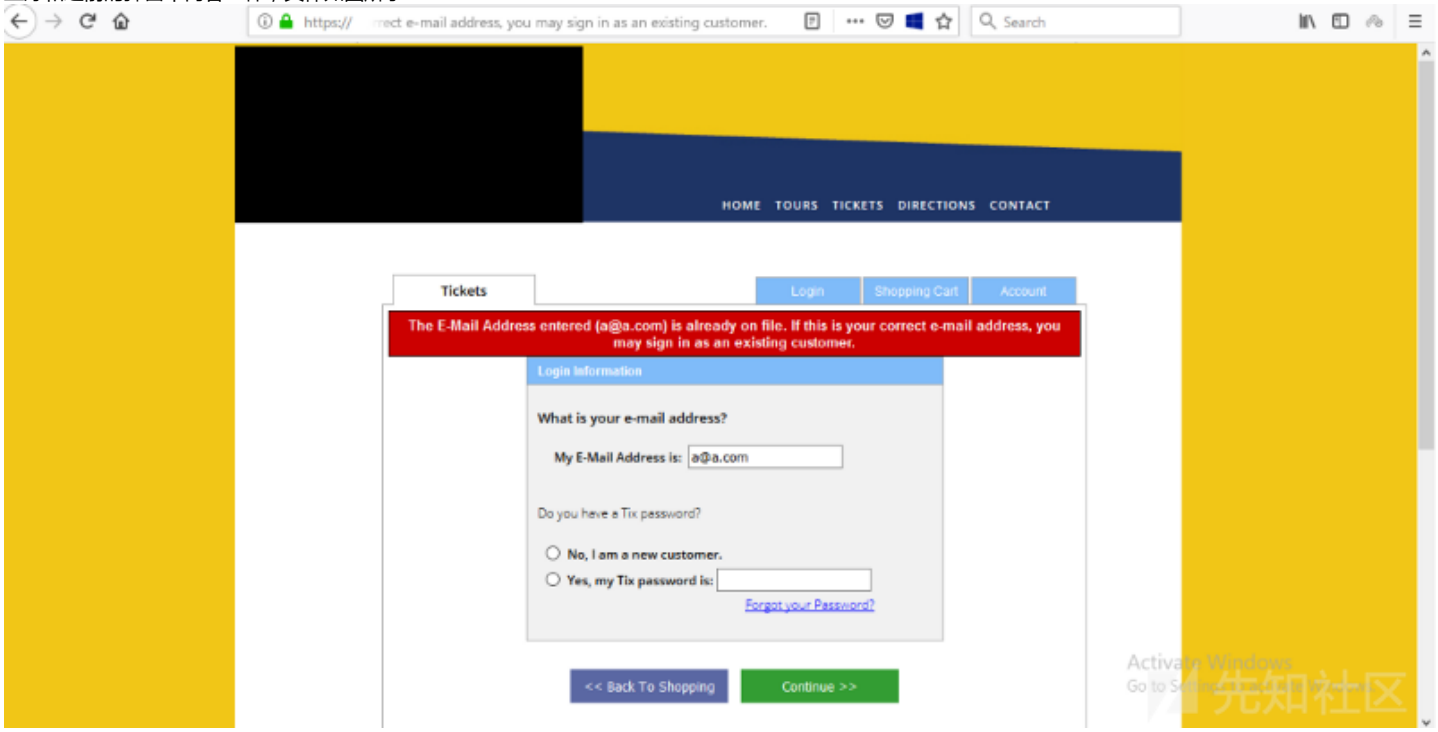
实际上当时我正在检查网站的注册和登录功能并且试图找到一些应用缺陷，我用邮箱号a@a.com注册了一个账户但没有去邮箱验证，然后尝试使用这个邮箱账号登录，发现



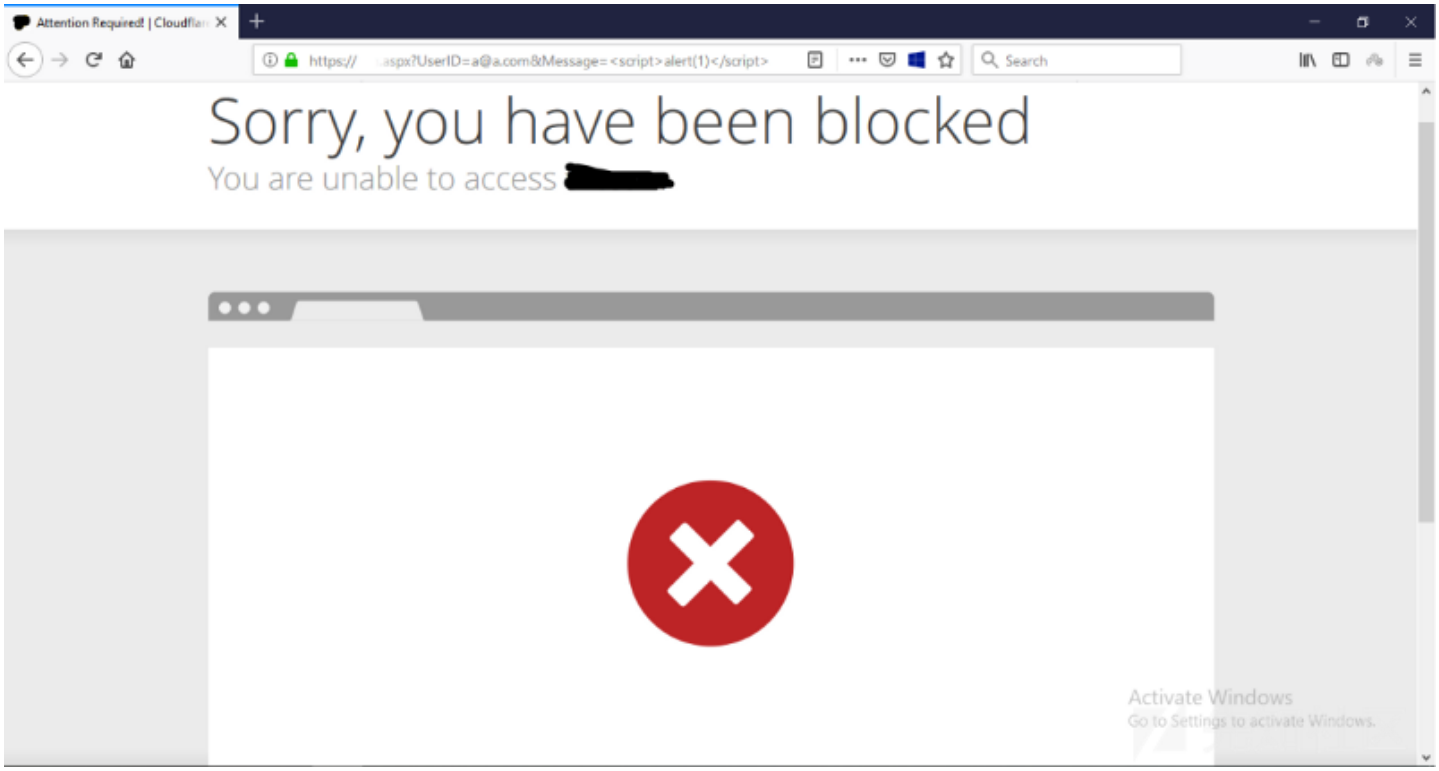
并且我发现URL变成了：

```
https://redacted.com/Secure/Login.aspx?UserID=a@a.com&ReturnUrl=&Message=The E-Mail Address entered (a@a.com) is already on fi
```

正好和之前的弹窗中内容一样，具体如图所示：

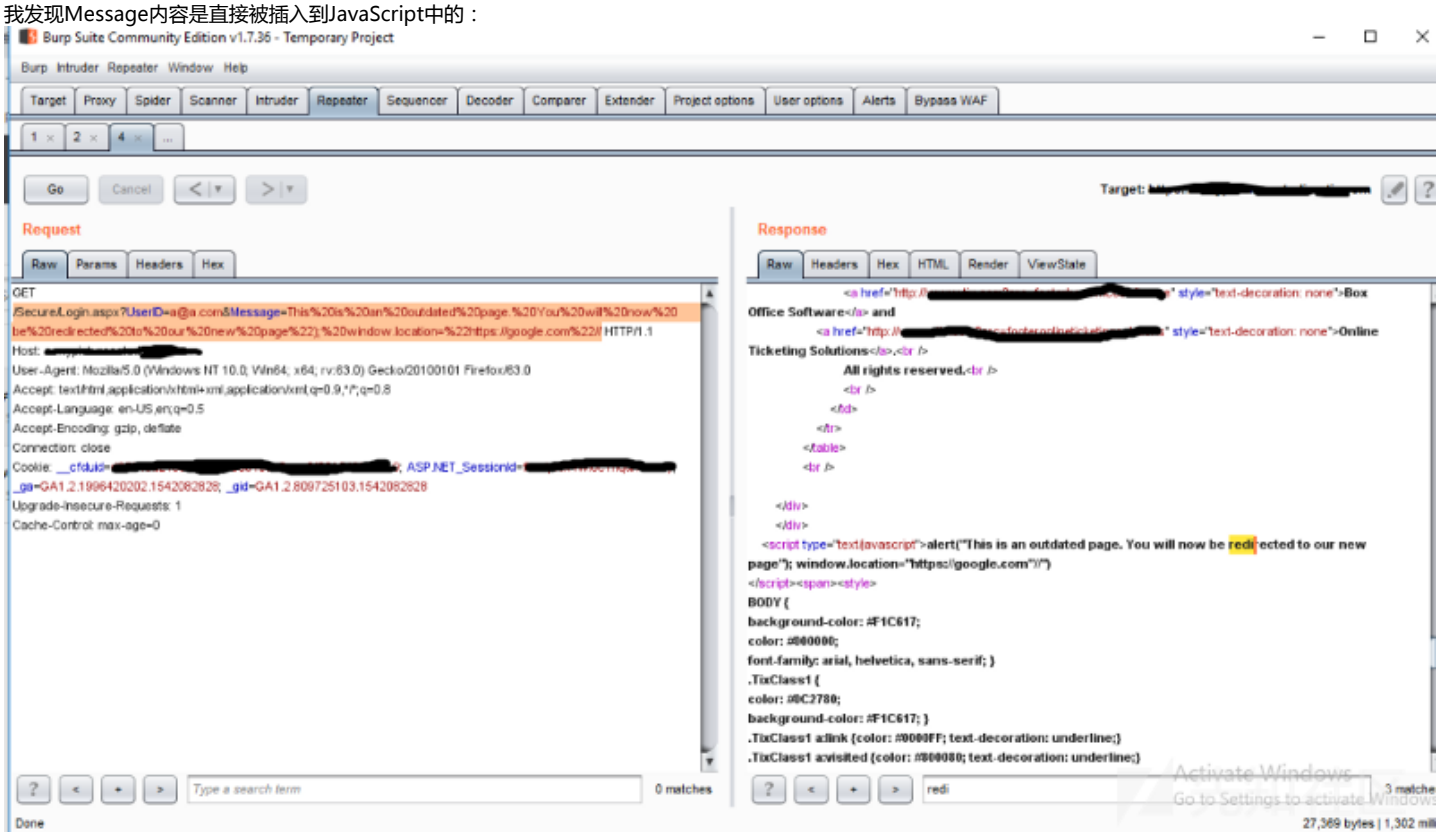


因此Message的内容可能能够反映在HTML内容中，我直接用这个payload（ <script>alert(1)</script> ）尝试了一下，得到了下面的结果：



哎呀，Cloudflare,不过没关系，在意料之中，这个payload用的是假用户账号。

我发现Message内容是直接被插入到JavaScript中的：



所以，我们能做的就是闭合双引号和括号之类的符号，例如：

```
alert("something_here");evil_script_here// ")
```

这样，我们就可以为所欲为了！

总结，再好的防火墙也保护不了糟糕的代码，感谢您的阅读。

上一篇：浅析IO_FILE结构及利用 下一篇：java代码审计手书(一）

1. 0 条回复

- 动动手指，沙发就是你的了！

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