

[登录](#)

Hangouts Chat漏洞分析：从开放式重定向到代码执行

[mss****](#) / 2018-08-26 17:06:16 / 浏览数 2843 [技术文章](#) [技术文章](#) [顶\(0\)](#) [踩\(0\)](#)

原文：<https://blog.bentkowski.info/2018/07/vulnerability-in-hangouts-chat-aka-how.html>

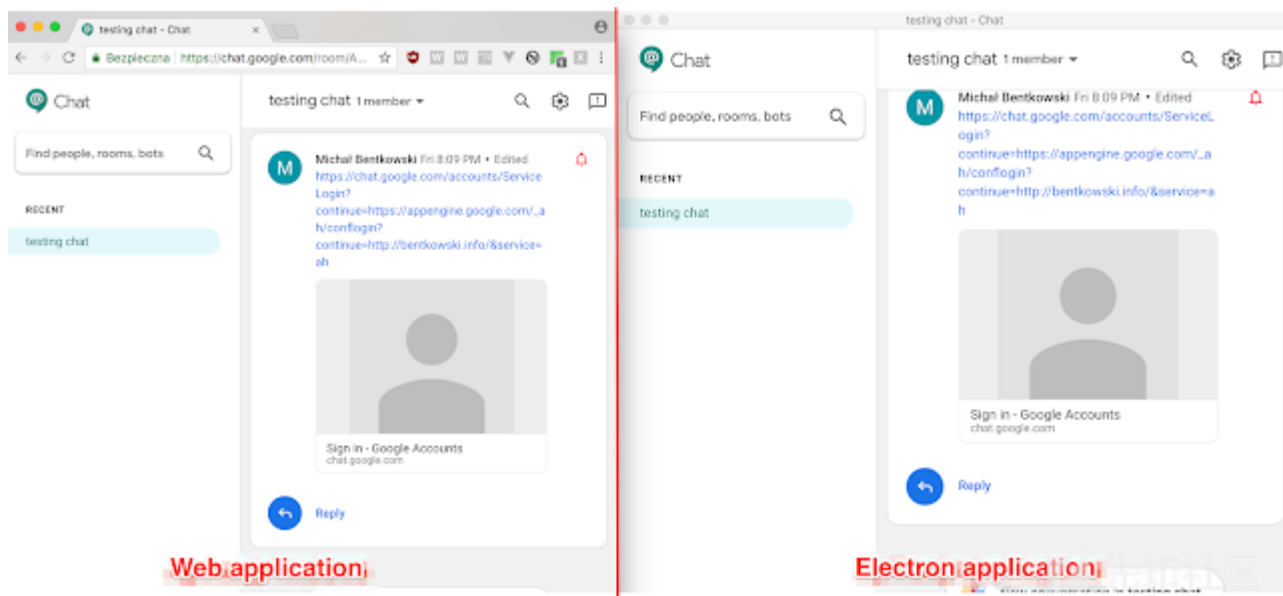
几个月前，谷歌发布了一个新产品：[Hangouts Chat](#)应用程序，这无疑是对[Slack](#)的一个回应。Hangouts Chat不仅提供了[浏览器版本](#)（要求具有G Suite帐户），同时，也提供了桌面版或移动版应用程序，对于后者，读者可从[这里](#)下载相应的程序。

与此同时，几个月前，我正好获得了一笔用于分析应用程序安全性的[研究经费](#)，于是，我决定专注于考察桌面应用程序的安全漏洞。

Hangouts Chat——桌面应用

安装后，该桌面应用程序实际上就是一个[Electron](#)

"Electron")应用程序。从本质上说，该桌面应用程序只是用于显示"<https://chat.google.com>"上托管的Web应用程序的内容而已。



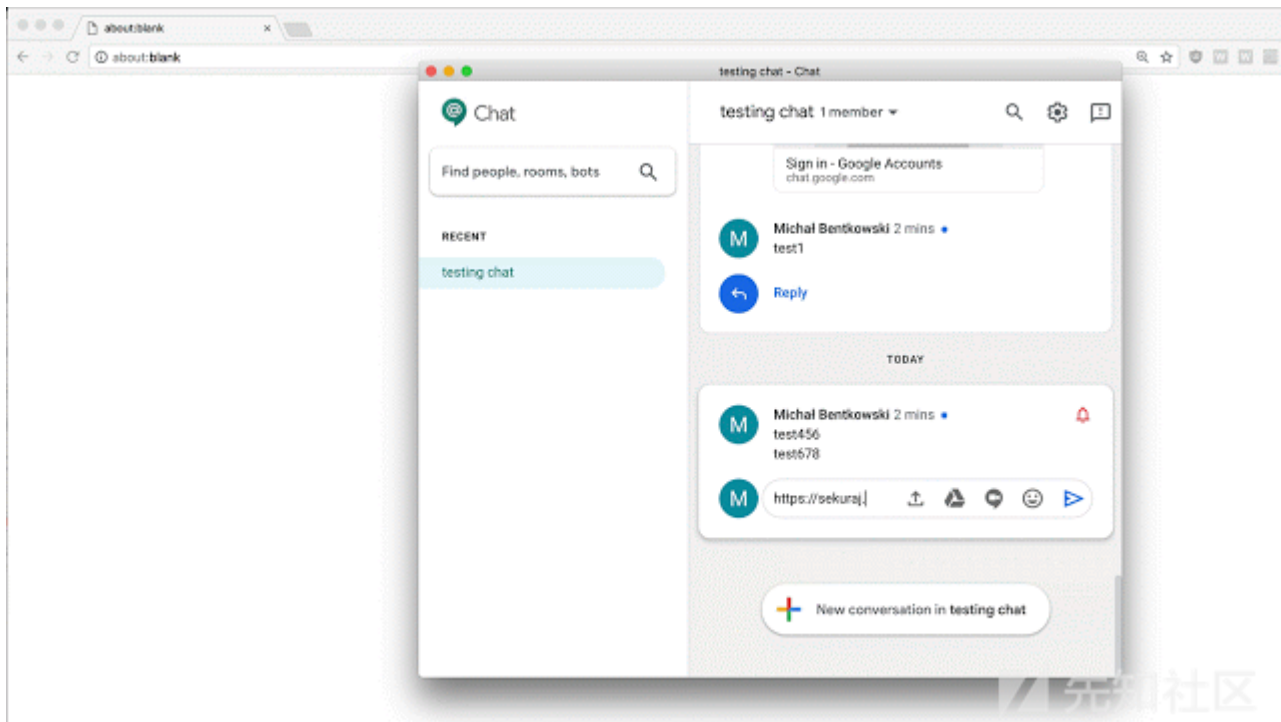
因此，对于这款Electron应用程序来说，查找其安全漏洞，与查找其Web版本的安全漏洞并没有什么多大区别。不过，有一点需要注意，即该应用的Web版本在浏览器中显示。Zalewski在Tangled Web中所言：

URL

但是，在Electron应用程序中，却没有提供地址栏。这意味着，用户必须相信应用程序本身提供的、来自“<https://chat.google.com>”的内容，但并没有可靠的指标对其进行

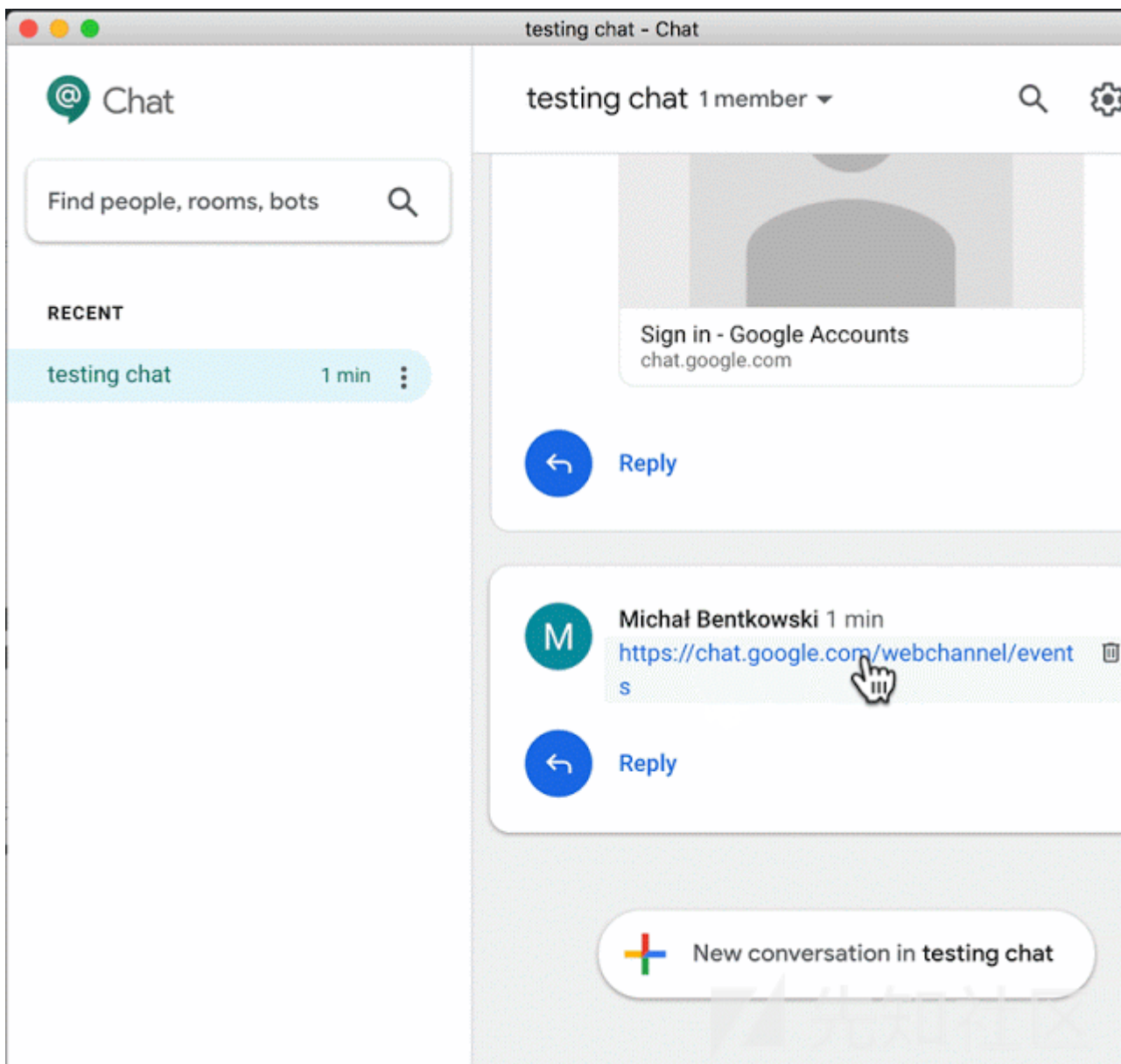
于是我想，也许可以找到一种方法将应用程序重定向到外部域（即chat.google之外的域），这样的话，就可以非常可靠地进行网络钓鱼了。为此，可以用户将重定向到攻击寻找重定向

于是，我就从最简单的想法开始下手：将用户重定向到另一个域。为此，我们只要在该聊天软件中添加一个指向外部域的链接即可。这样的话，只要用户点击了该链接，就会打开外部域。然而，这显然是行不通的，因为外部链接将会在默认浏览器中打开。

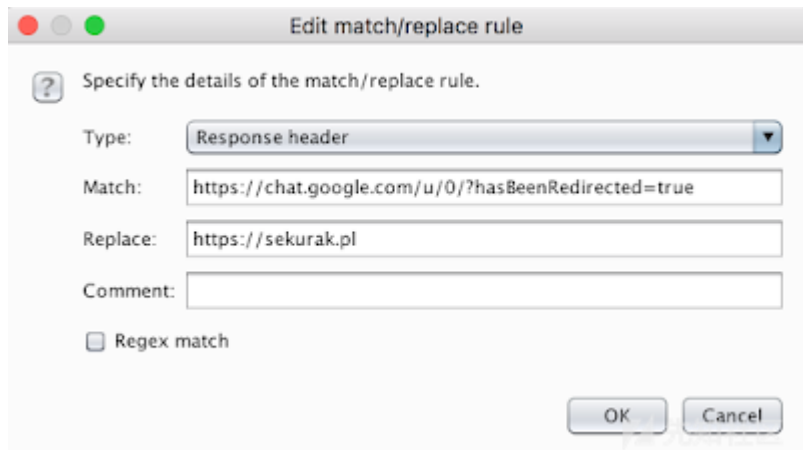


但是，我们也不用灰心，继续探索。

经过进一步研究，我注意到chat.google.com的链接是直接Electron应用程序中打开的。顺便说一下，当用户点击的链接返回200以外的代码时（例如：“<https://chat.google.com/webchannel/event>”



要想绕过URL访问规则，一种非常常见的方法便是滥用重定向（响应代码为3xx）。研究发现，当导航到不存在的网址（例如“<https://chat.google.com/test123>”）时，“chat.google.com”返回的响应头包含“hasBeenRedirected=true”URL重写为sekurak.pl，来看看会发生什么情况。



这就是该应用程序的反应：



太棒了！它实际上证实了302重定向能被用来在Hangouts Chat窗口中显示任意网站。

接下来，只要对“<https://chat.google.com>”进行实际的重定向就行了。

开放式重定向漏洞

开放式重定向的确是一种安全漏洞，但是在我看来，其威胁程度往往被高估。下面内容摘自谷歌的[漏洞赏金大学](#)页面：

开放式重定向器会将您从Google

URL转到由构建该链接的人指定的另一个网站。安全社区的一些成员认为，这种重定向器会成为网络钓鱼的帮凶，因为用户可能倾向于信任链接上的鼠标悬停工具提示，然而

对于这种观点我是赞同的。通常情况下，用户应该将地址栏作为唯一可靠的安全指标。但是，在Electron中，情况就变了——在Electron应用程序中，并没有地址栏，因此，

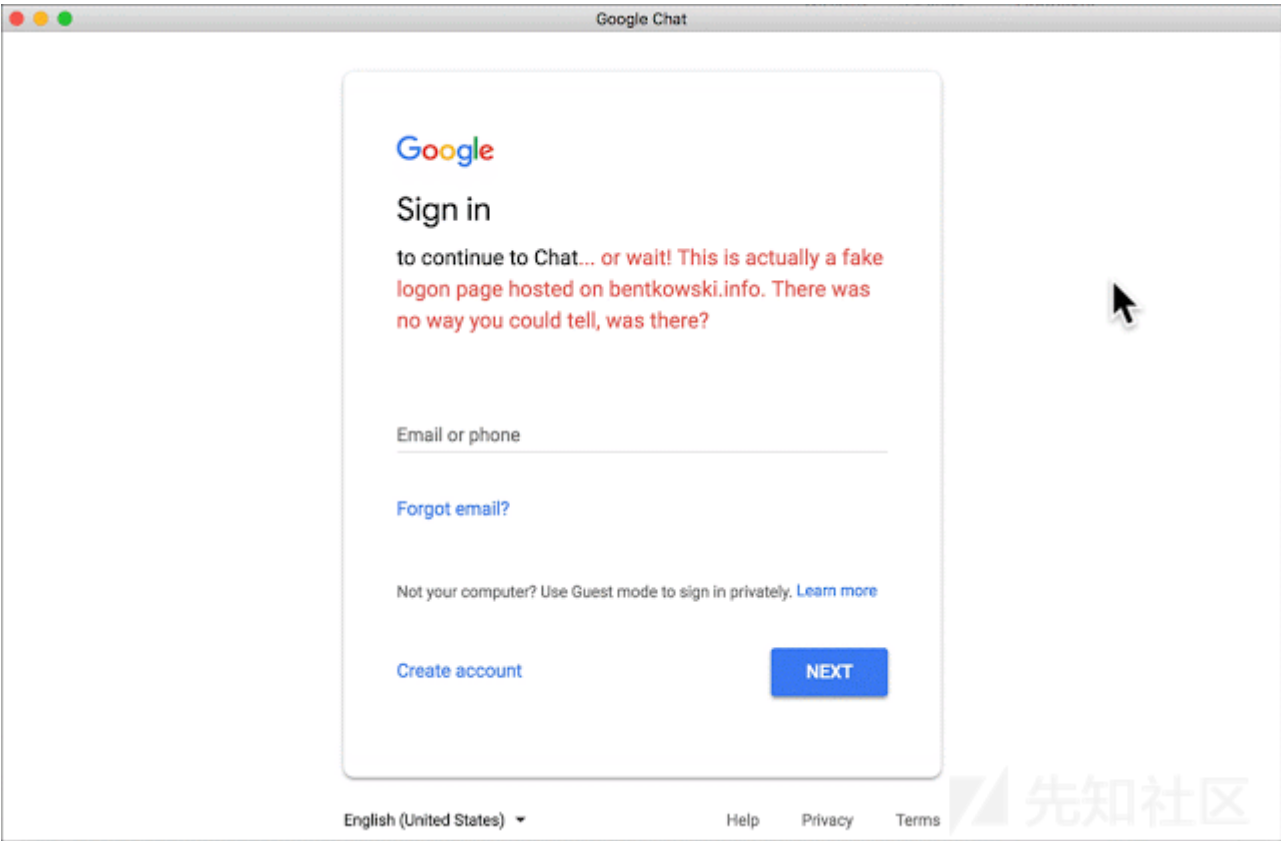
事实表明，在“<https://chat.google.com>”中搜索开放式重定向漏洞，比我最初想象的要容易得多。因为在“<https://chat.google.com/accounts>”域下的任何网址都会被重定向

不过，重定向到“accounts.google.com”只是攻击过程的第一步。实际上，最重要的事实是，在“accounts.google.com”上存在一个已经公开披露的著名开放式重定向漏洞URL上即可。

最终，用于chat.google.com的开放式重定向代码如下所示：

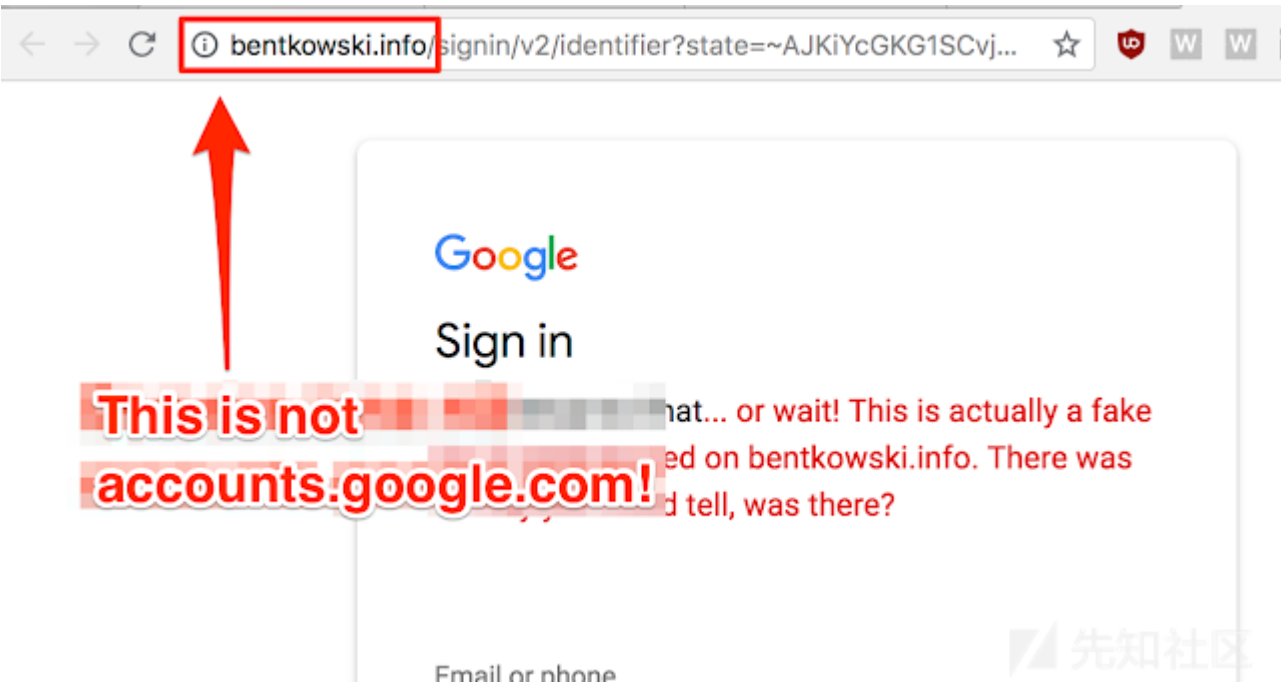
https://chat.google.com/accounts/ServiceLogin?continue=https://appengine.google.com/_ah/conflogin?continue=http://bentkowski.i

然后，我又仿造了一个类似于谷歌的登录页面——现在，我们终于搞定了—一个非常可靠的网络钓鱼页面:)



如上面的gif所示，用户根本无从得知自己位于假冒的页面上，因为这里压根就没有地址栏呀。

不过，上面介绍的攻击方法对该软件的Web应用程序版本是不起作用的：



小结

正如您所看到的，由于Electron应用程序没有提供地址栏，所以才使开放式重定向漏洞有了可乘之机。因此，当您开发Electron应用程序的时候，请确保无法将主窗口重定向

如果您正在使用Google Hangouts Chat，请务必进行更新，因为谷歌已经在几天前就发布了相应的安全补丁。

有趣的是，谷歌对该漏洞的赏金非常慷慨，支付了7,500美元。需要说明的是，该赏金实际上针对代码执行漏洞的。虽然我仍然无法将其升级为代码执行漏洞，但Matt Austin (@mattaustin) 在推文中已经指出，这种漏洞升级是完全可行的。谢谢您的出色工作，Matt！

顺便说一下，对于谷歌提供的研究经费表示衷心感谢！否则的话，到现在我可能也不会接触该应用程序。

点击收藏 | 0 关注 | 1

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](#)