Electron Security

allowRunningInsecureContent

NOP Team

allowRunningInsecureContent

0x01 简介

大家好，今天和大家讨论的是 `allowRunningInsecureContent` 安全配置选项，这个选项非常容易理解，就是是/否允许在 `HTTPS` 的网站加载或执行 `HTTP` 协议的 `JavaScript`、`CSS`、插件等

从 `Electron 2.0.0` 开始默认为 `false`，即不允许在 `HTTPS` 网站中加载或执行 `HTTP` 协议的内容

当 `webSecurity` 被设置为 `false` 时，会自动将 `allowRunningInsecureContent` 设置为 `true`

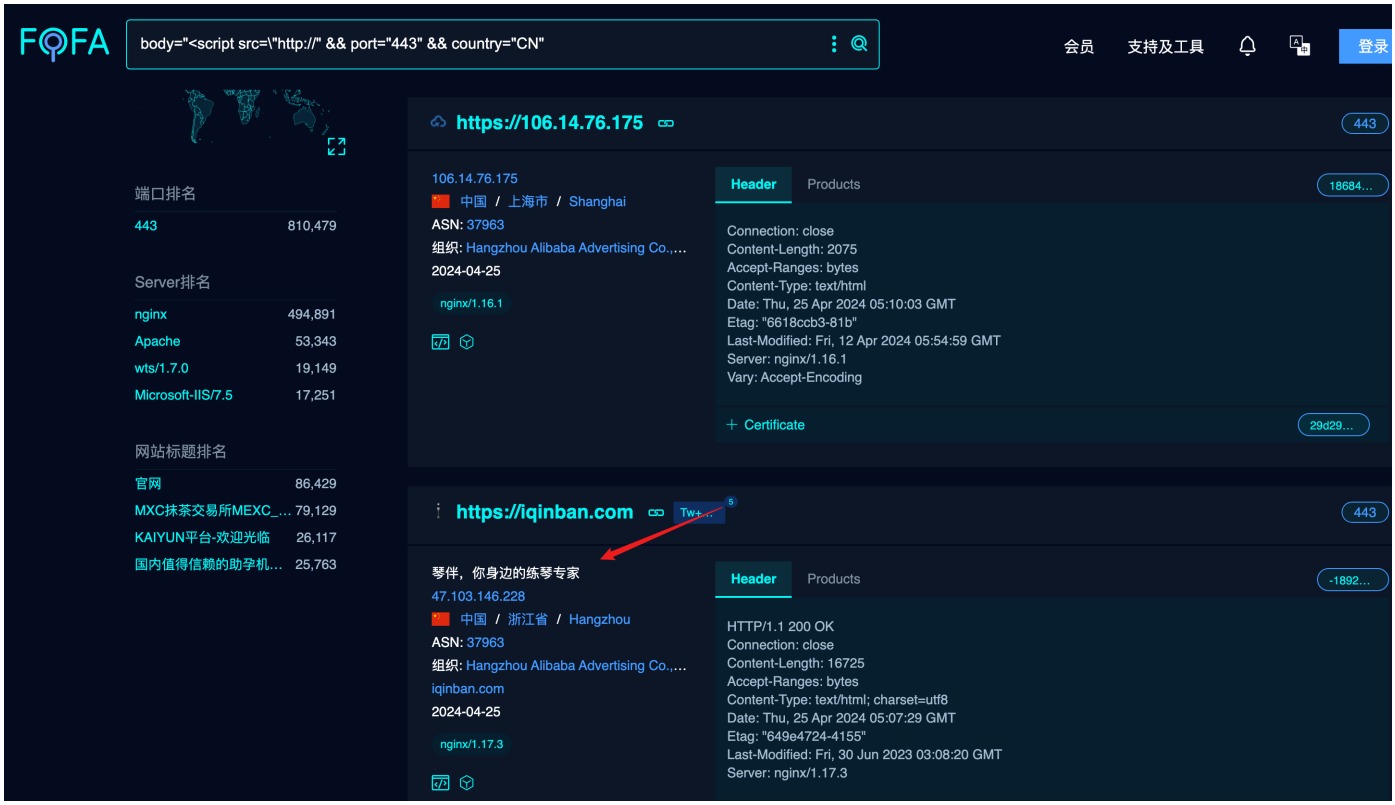
0x02 扩展探索

既然不允许 `HTTPS` 的网站加载 `HTTP` ，是否会允许 `loadFile` 加载本地文件创建窗口加载 `HTTP` 的资源呢?

1. 正常功能测试

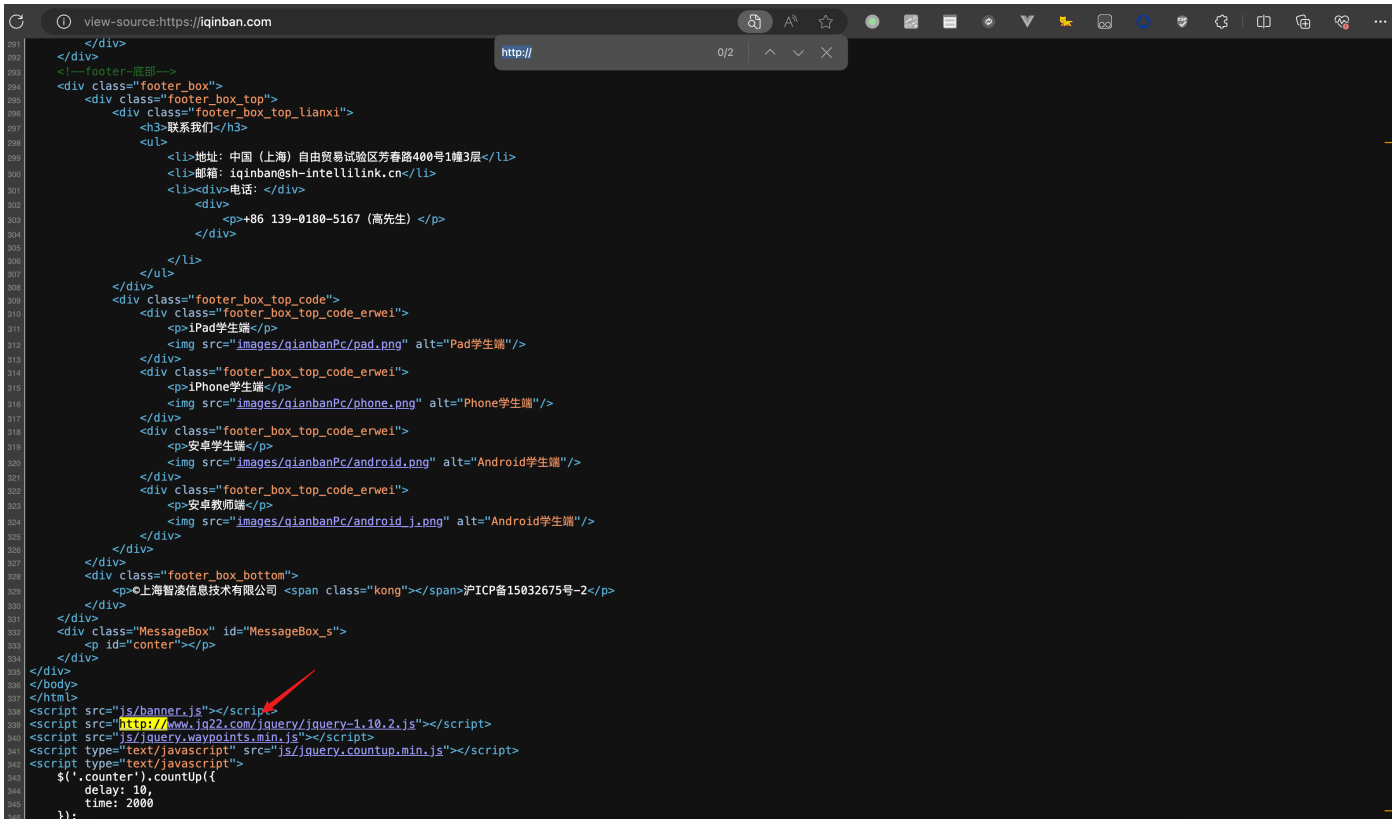
我们得找一个 `HTTPS` 的网站，并且还在网页内引用了 `HTTP` 的 `JavaScript` 等，搭建起来会比较麻烦，因为要有有效证书，还有配置同源策略等，我也不希望自签名证书通过自定义配置通过后再影响实验，因此通过 `fofa` 平台进行搜索

```
body="<script src=\"http://" && port="443" && country="CN"
```



选择这个 `琴伴` 作为案例

```
https://iqinban.com/
```



尝试默认情况下远程加载该网页创建窗口

在 `Electron 31.0.0.alpha.2` 中是会拦截的，设置 `allowRunningInsecureContent` 为 `true` 后，再次加载

这回就可以加载了，我们尝试在各个版本的 `Electron` 中进行尝试，在 `Electron 5.0、10.0、20.0、30.0` 版本中执行结果保持一致

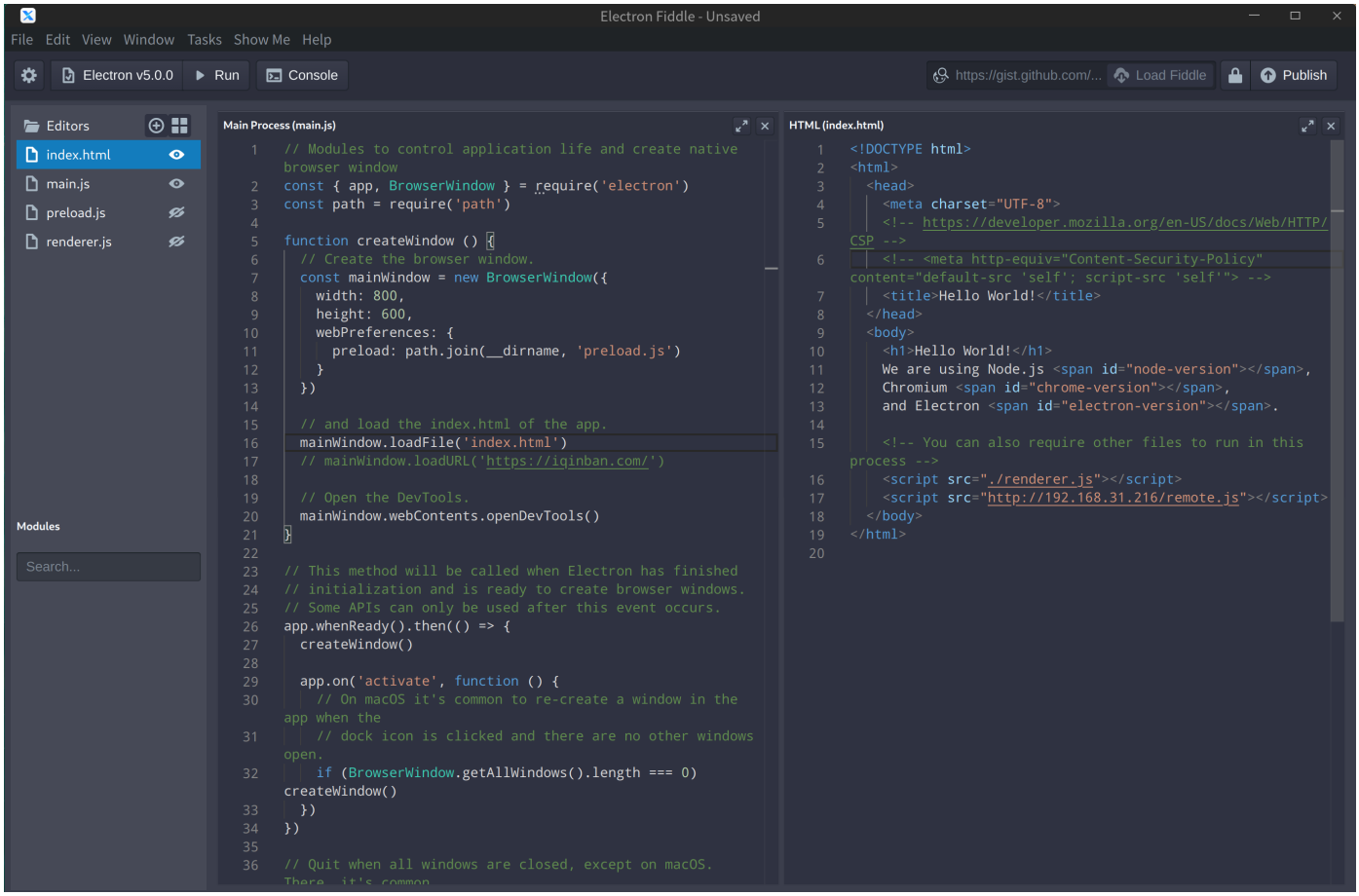
2. 本地加载文件测试

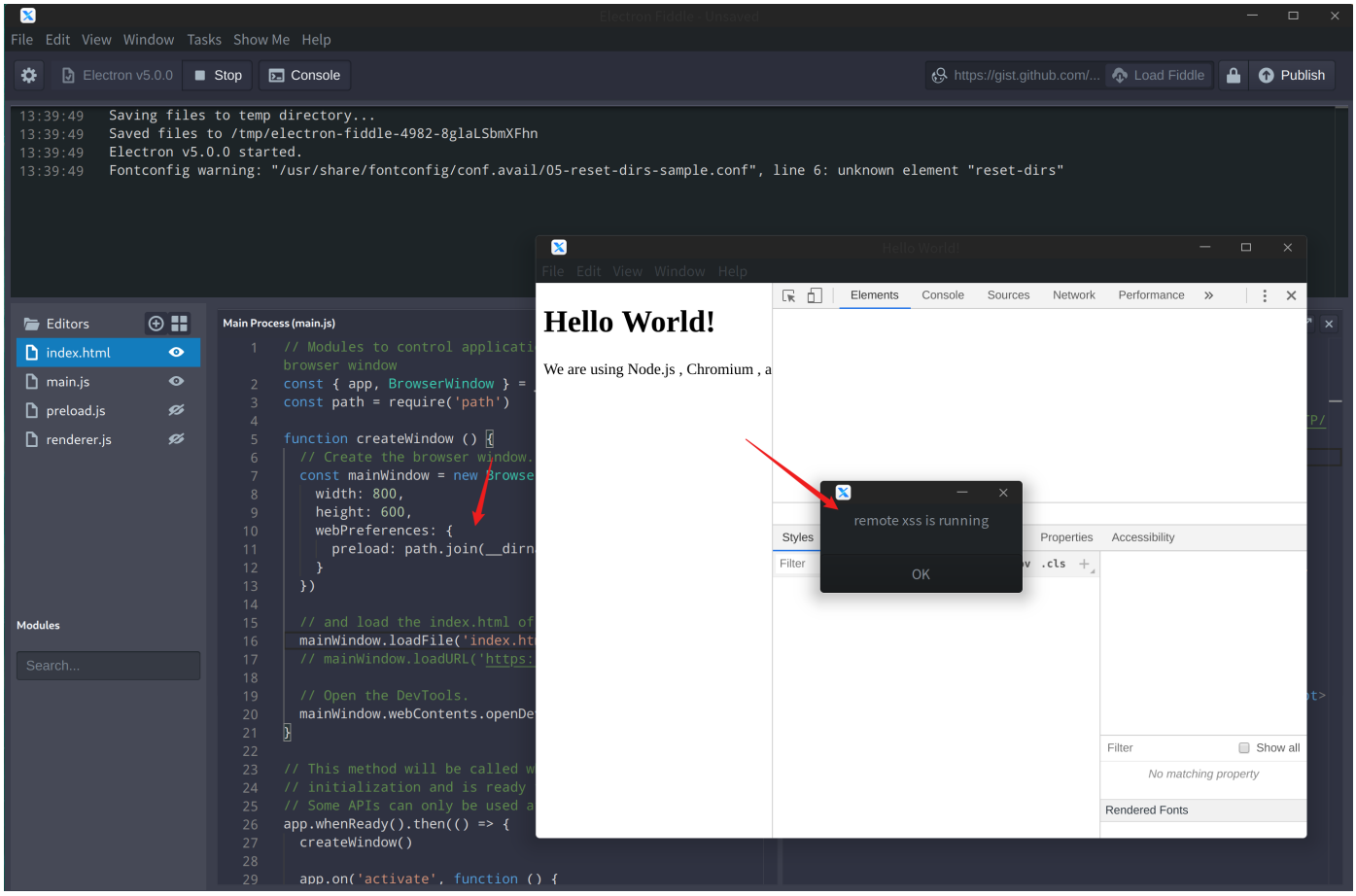
尝试在通过加载本地文件创建窗口情况下加载 `HTTP` 资源

搭建 `xss` 服务器

```
[~/D/t/21 ❯❯❯ cat remote.js
alert('remote xss is running')
[~/D/t/21 ❯❯❯ sudo python3 -m http.server 80
[Password:
Serving HTTP on :: port 80 (http://[::]:80/) ...
```

关闭 `CSP`，在 `index.html` 中远程加载 `remote.js`





发现即使在默认关闭了 `allowRunningInsecureContent` 的情况下，还是可以远程加载 `HTTP` 的 `JavaScript` 的

所以这方面还是得看 `CSP` 的， `CSP` 更牛一些

0x03 总结

`allowRunningInsecureContent` 仅在通过 `loadURL` 等远程加载网站创建窗口的时候有意义，对于通过 `loadFile` 加载本地文件的场景是没有作用的，同时 `Electron` 也没有变态到默认所有的远程加载内容（包括页面内 `img` 等元素的 `src` 属性指定的内容）必须都是 `HTTPS`