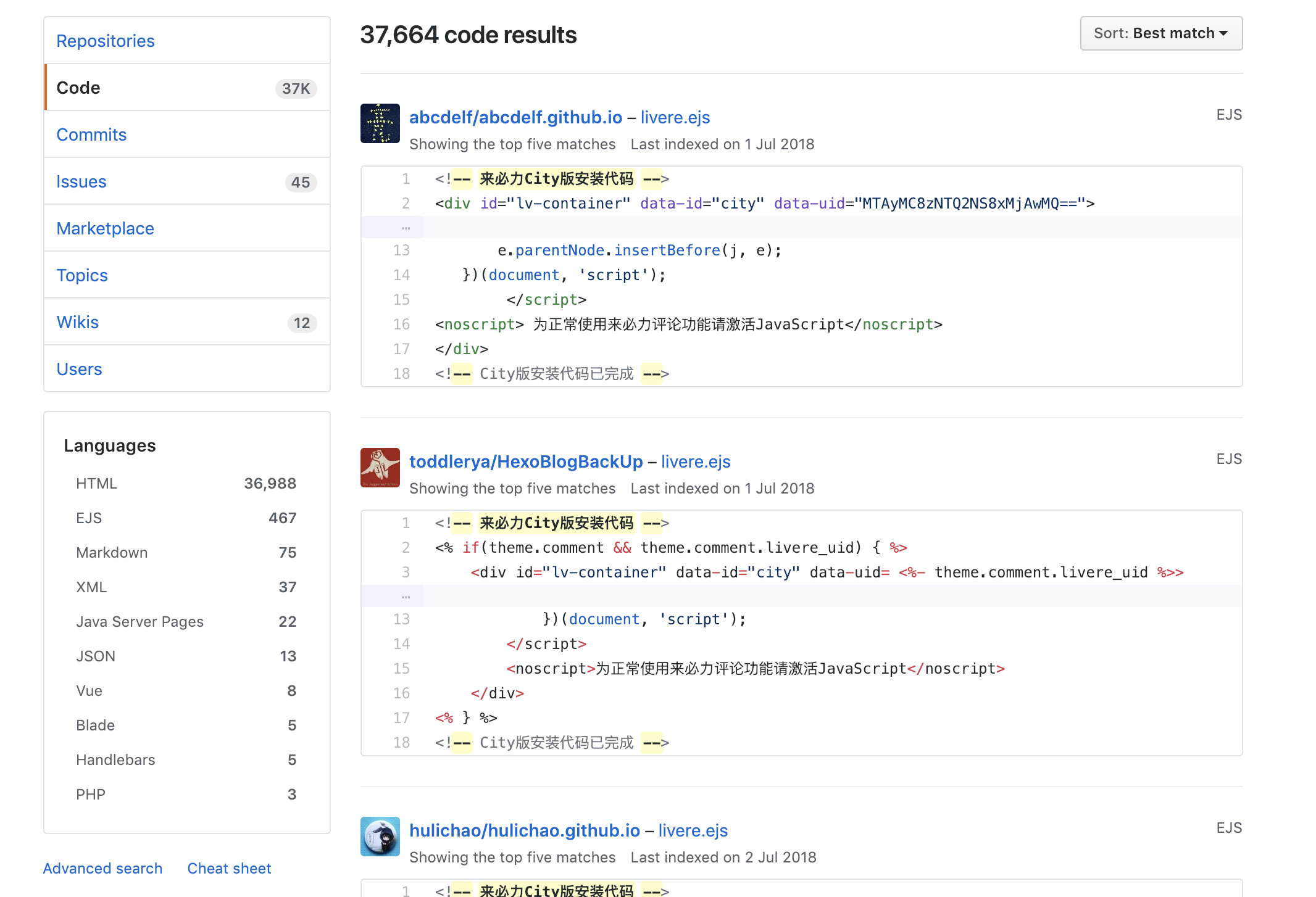
来必力评论插件存在存储xss 通用

官网：<https://www.livere.com/>

中文官网：https://www.livere.com/lvChangeLang?locale=zh

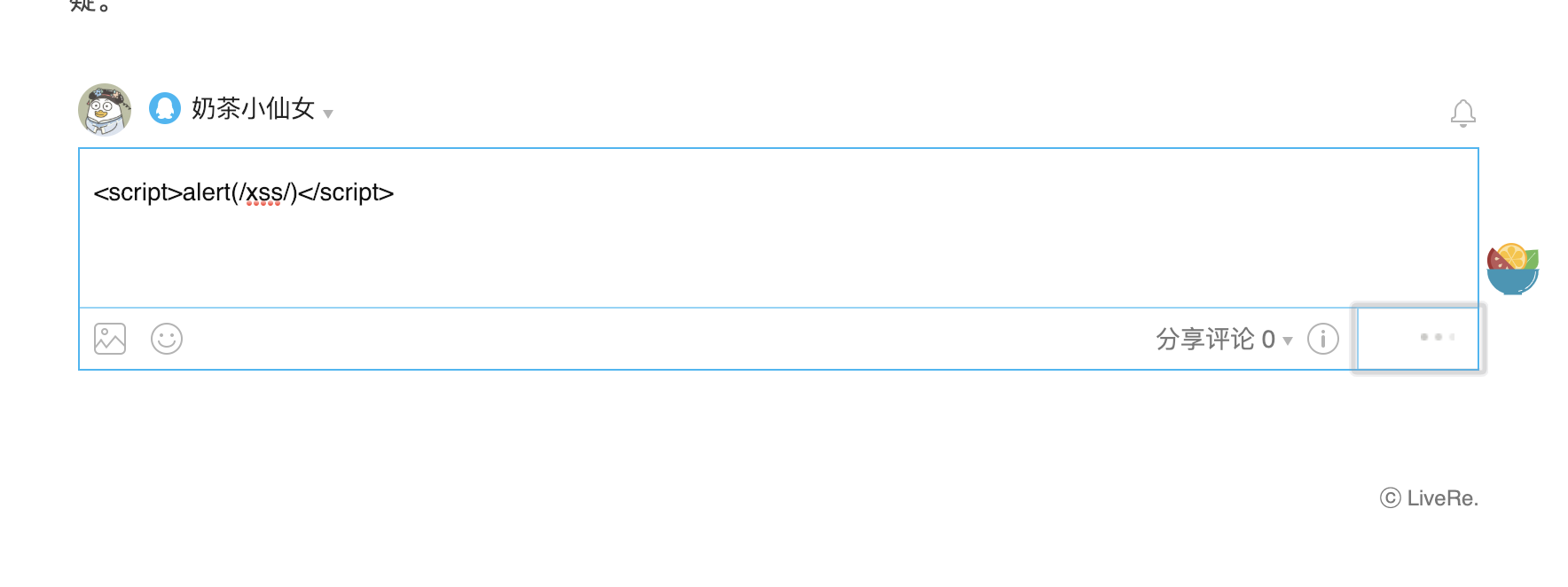
介绍:来必力插件使用社交网站账户登录，免去注册过程。提高用户的参与和沟通意愿。管理/删除我的评论内容。提供管理页面，管理网站文章及评论内容。



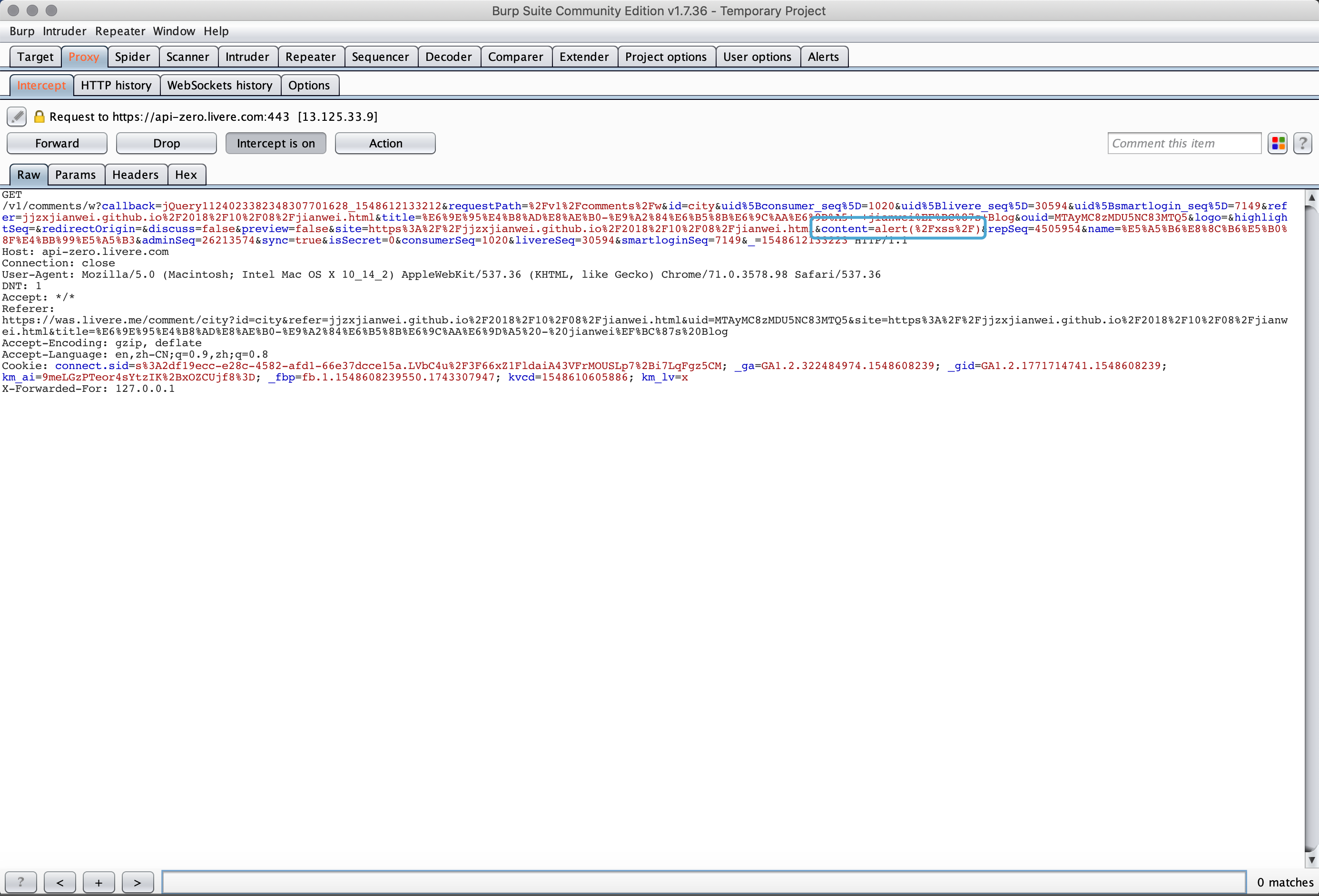
通过github查找，大概可以发现37k左右使用该插件的网站

复现过程：

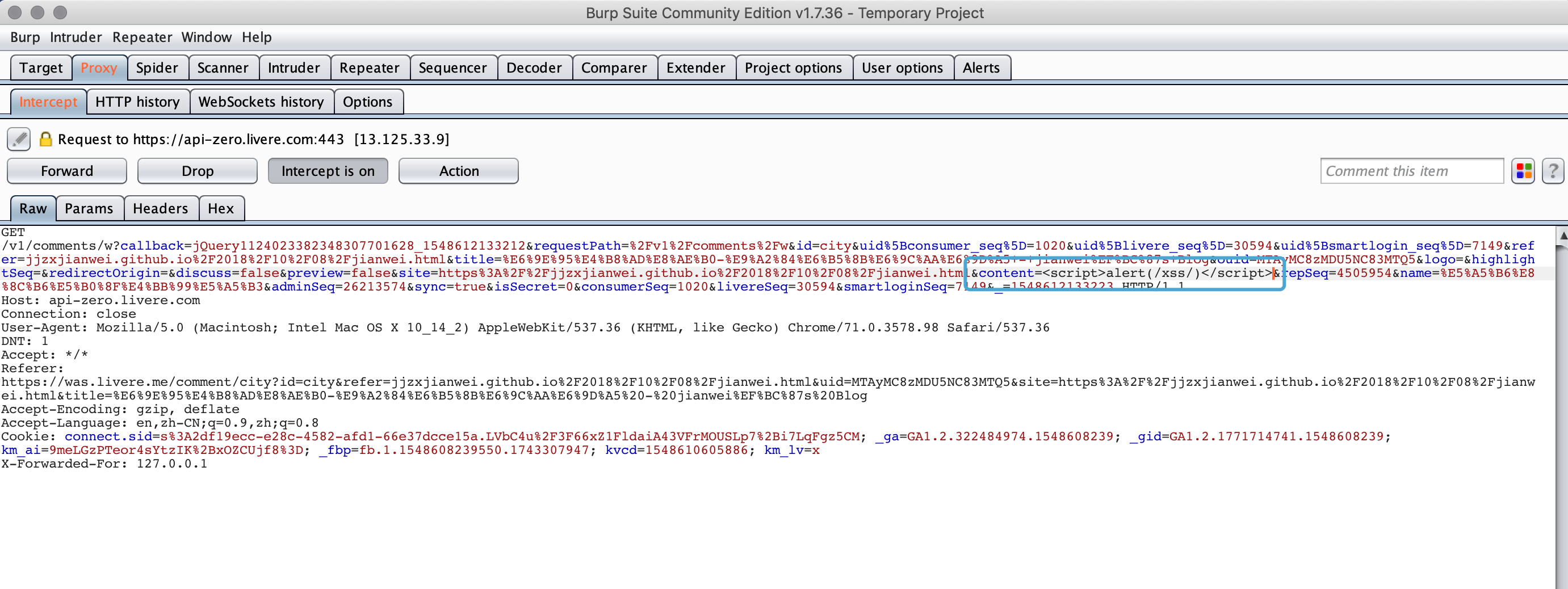
首先在输入框内输入XSS代码：



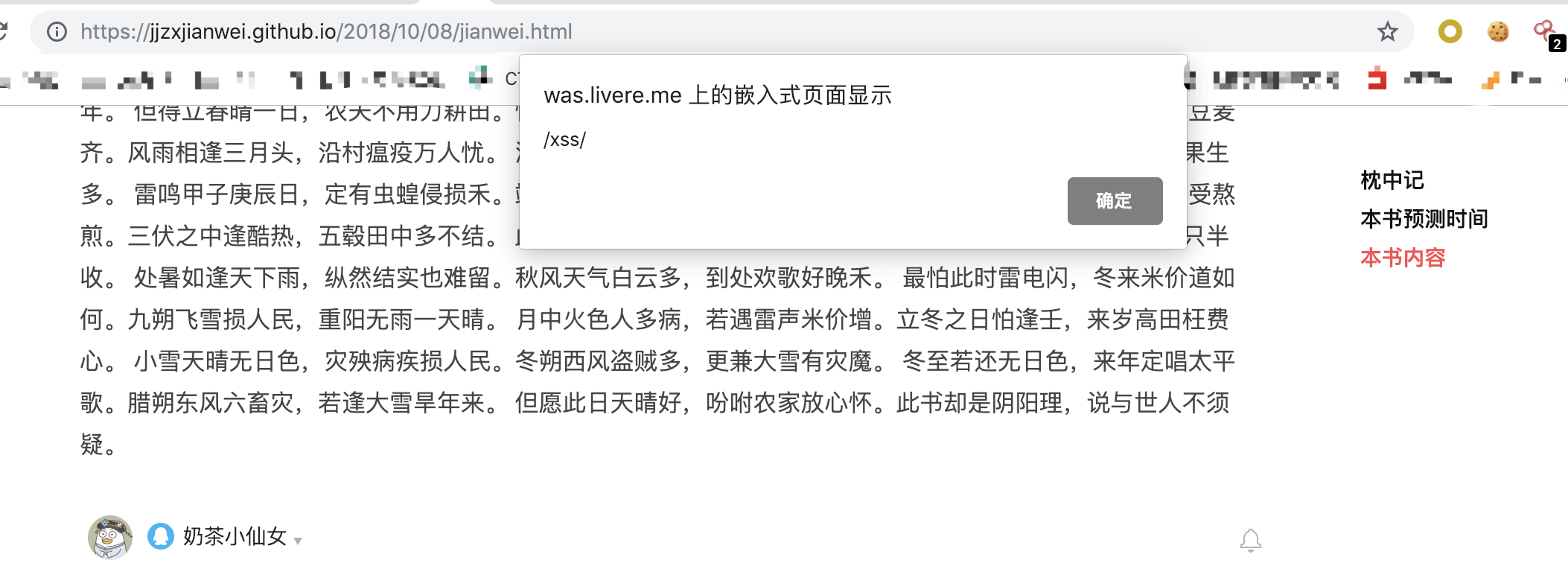
抓包：



发现前台已经将XSS过滤，修改数据包：



放行数据包后，刷新页面页面：



存储型XSS一枚。

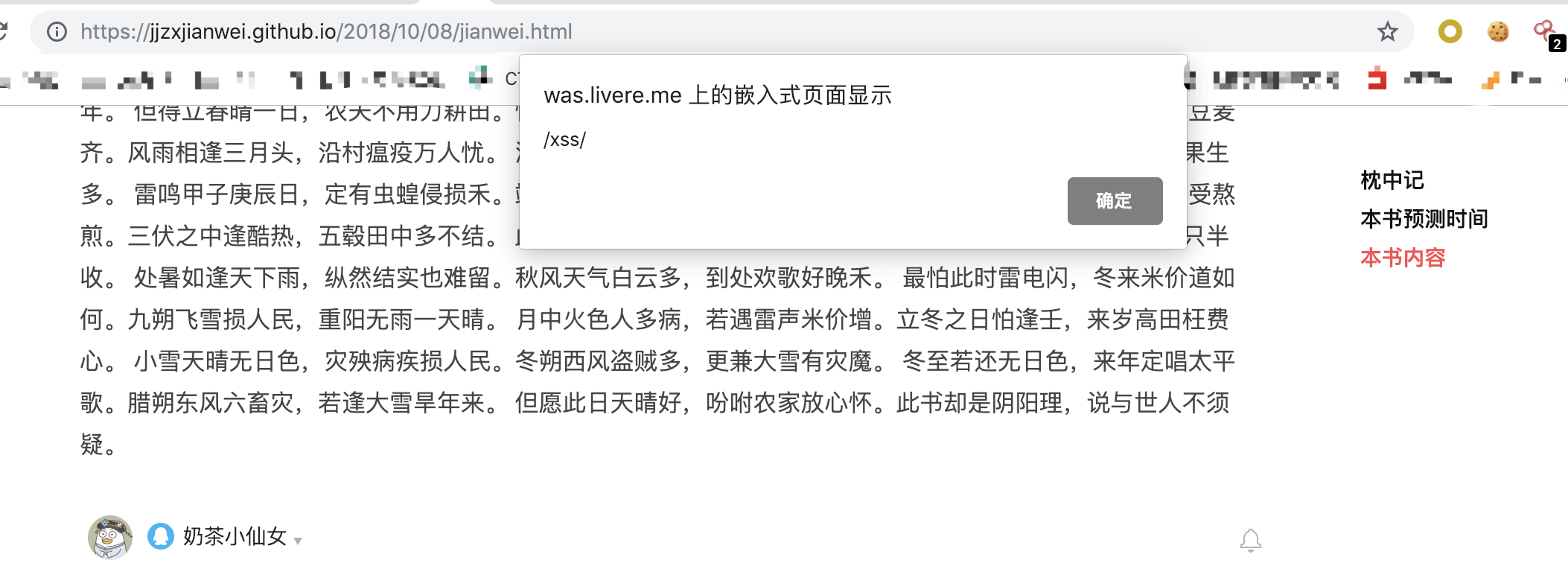
危害：

盗取用户信息

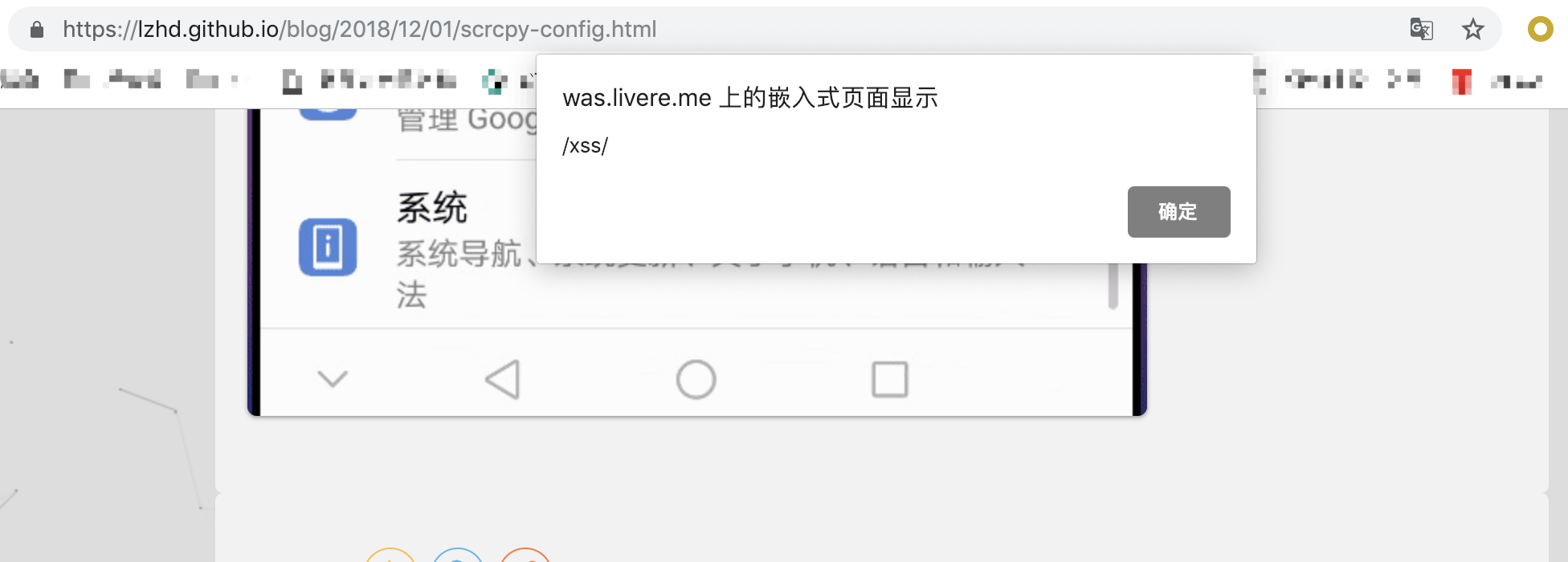
插入恶意脚本(比如挖矿)

案例地址：

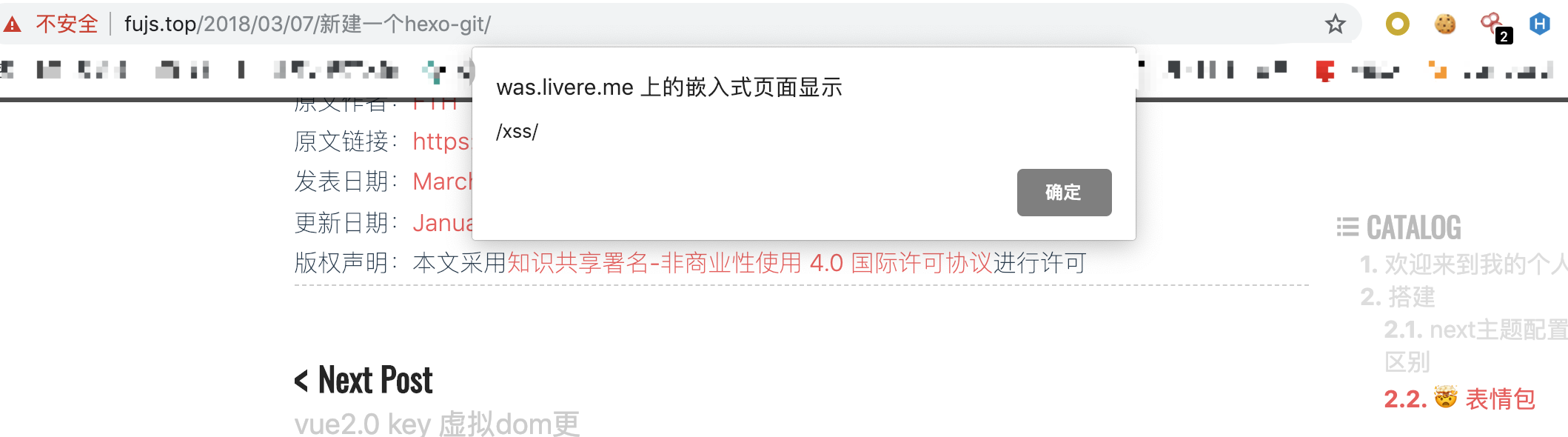
1. <https://jjzxjianwei.github.io/2018/10/08/jianwei.html>



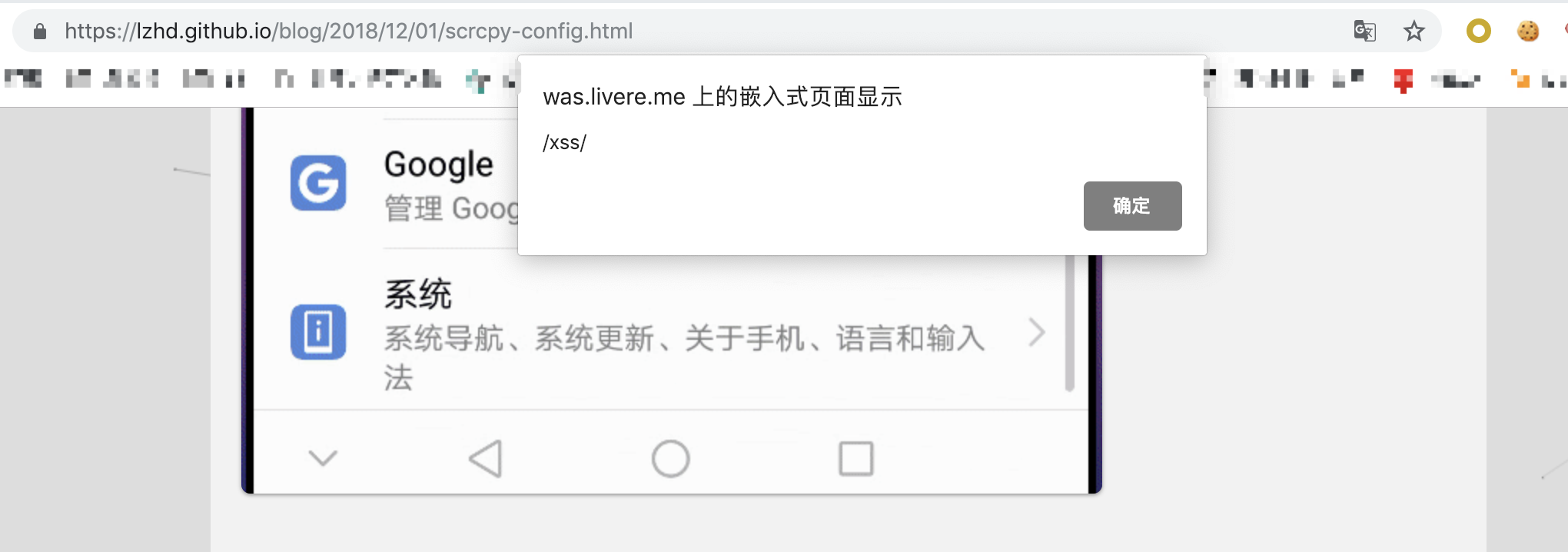
1. <https://lzhd.github.io/blog/2018/12/01/scrcpy-config.html>



1. <http://fujs.top/2018/03/07/%E6%96%B0%E5%BB%BA%E4%B8%80%E4%B8%AAhexo-git/>



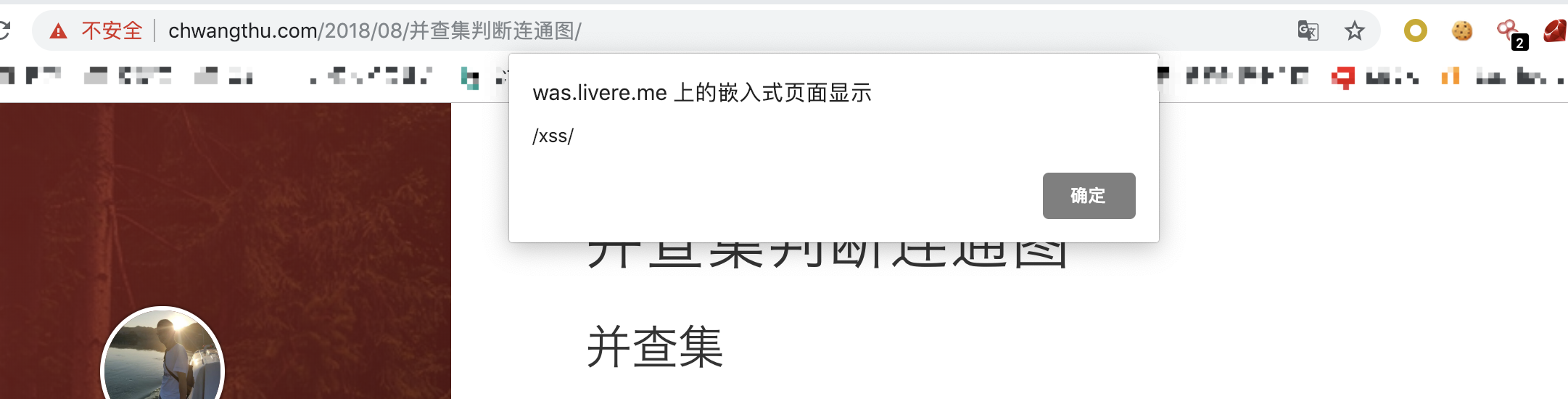
1. <https://ddqszcxy.github.io/005>



1. <https://rjli.github.io/2018/08/17/minipogram/%E5%B0%8F%E7%A8%8B%E5%BA%8F%E8%87%AA%E5%AE%9A%E4%B9%89%E7%BB%84%E4%BB%B6/>



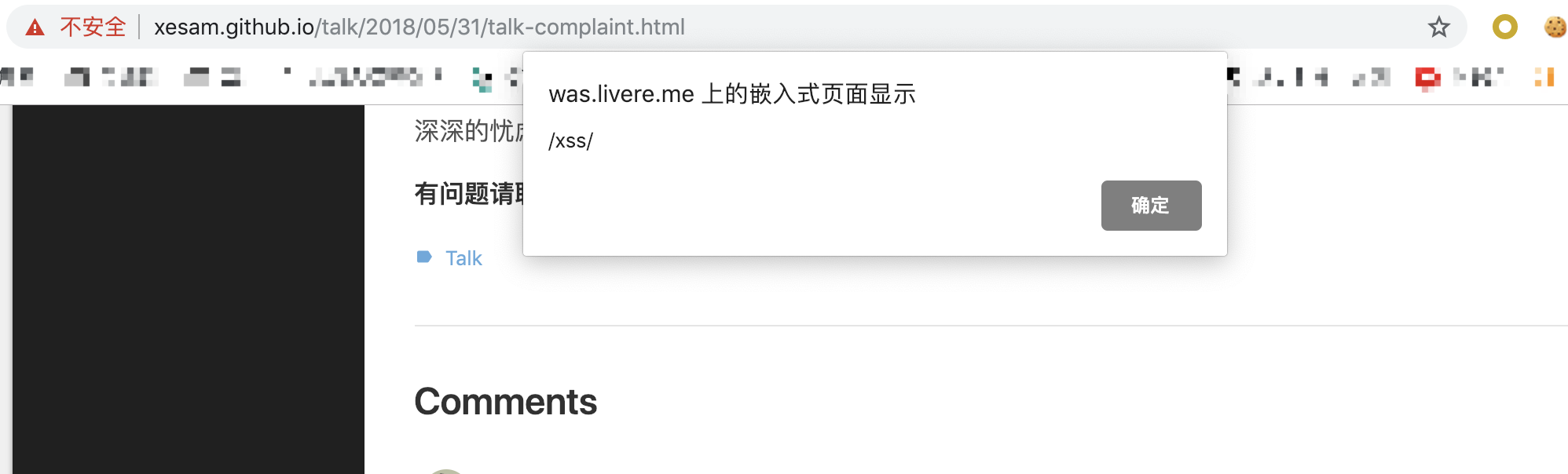
1. http://chwangthu.com/2018/08/%E5%B9%B6%E6%9F%A5%E9%9B%86%E5%88%A4%E6%96%AD%E8%BF%9E%E9%80%9A%E5%9B%BE/



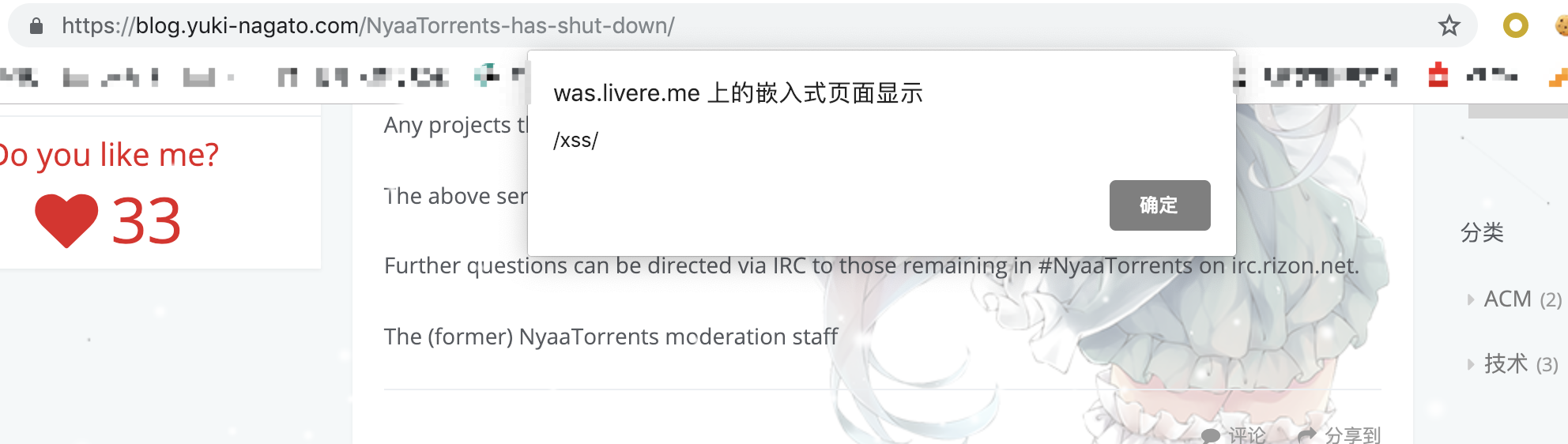
1. <https://xls-github.github.io/2017/04/%E4%BD%BF%E7%94%A8github%E5%85%8D%E8%B4%B9%E6%90%AD%E5%BB%BA%E4%B8%AA%E4%BA%BA%E5%8D%9A%E5%AE%A2%E5%90%8E%E7%9A%84%E4%B8%8A%E4%BC%A0%E6%96%B9%E6%B3%95/>



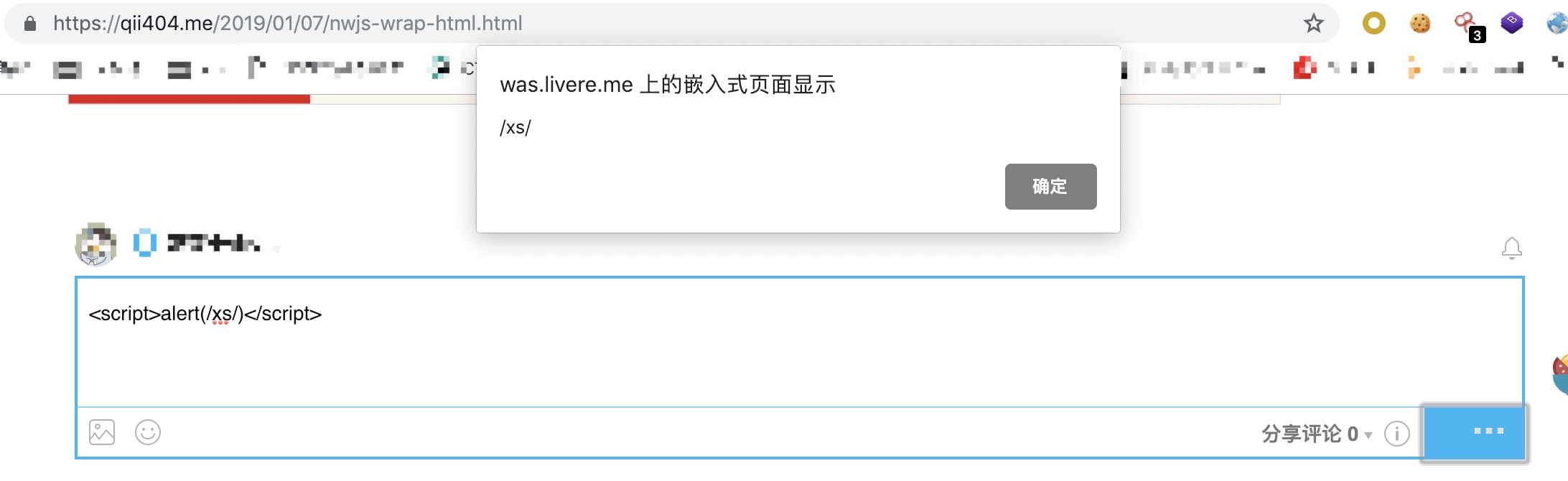
1. <http://xesam.github.io/talk/2018/05/31/talk-complaint.html>



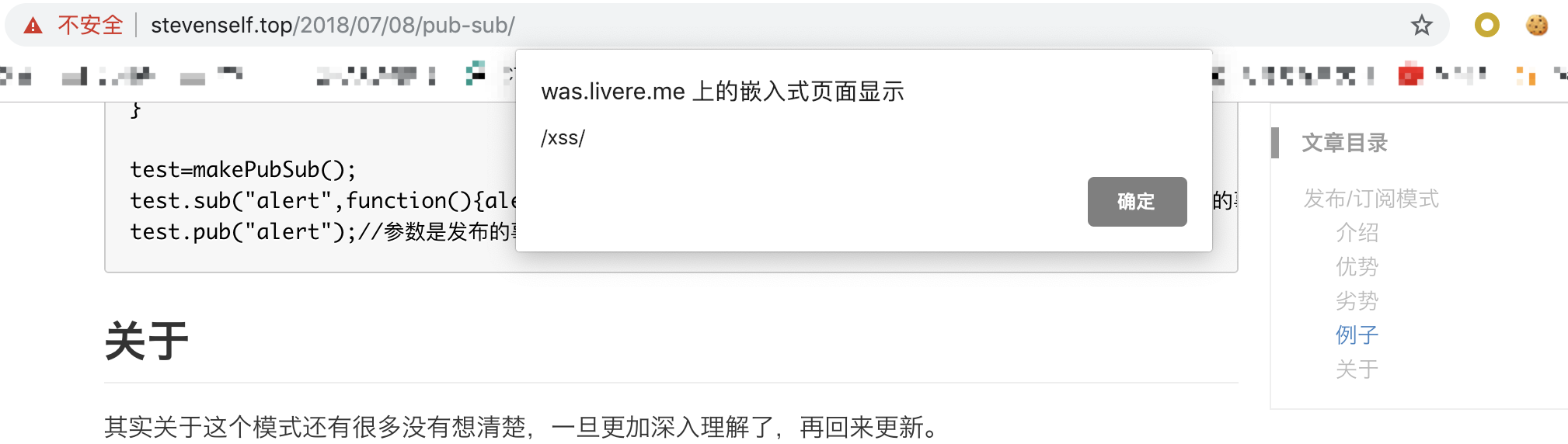
1. <https://blog.yuki-nagato.com/NyaaTorrents-has-shut-down/>



1. <https://qii404.me/2019/01/07/nwjs-wrap-html.html>



1. <http://stevenself.top/2018/07/08/pub-sub/>



1. <https://mryousing.github.io/2019/01/27/my-development-log-0010.html>
2. <https://shanks07.github.io/2018/03/javaLearn2/>
3. <http://oxffff.com/2018/04/25/Java8-Stream-API/>
4. <http://carolineliao.cn/2018/05/10/%E4%BA%8EsetTimeout/>
5. <https://psiace.me/>
6. <http://derek520.com/2018/11/04/Docker%E6%93%8D%E4%BD%9C%E5%91%BD%E4%BB%A4/>

修复建议：服务器端过滤