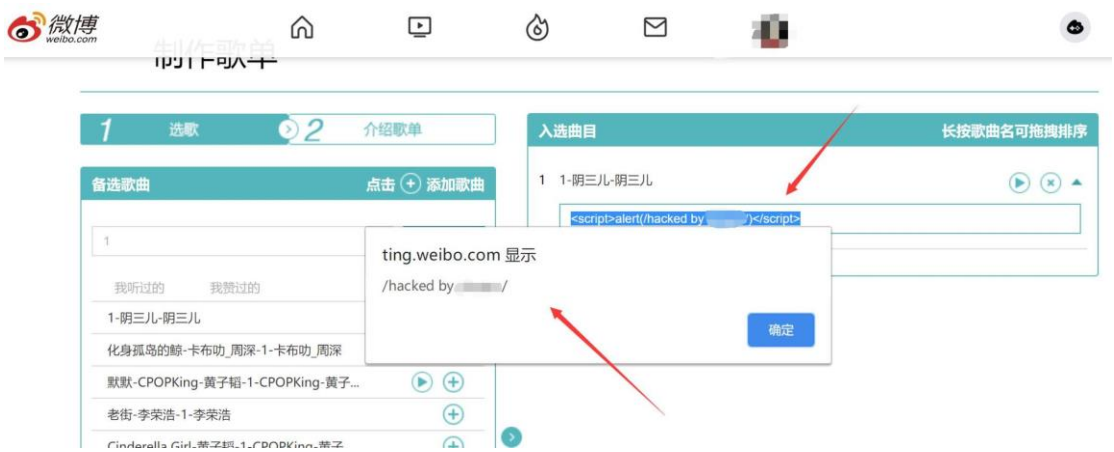
案例 1

子域名爆破+dirsearch 得到：https://ting.weibo.com/list

直接放上 payload



这里其实还有个保存歌单功能，但已经失效了，如果尝试绕过成功的话，此处反射型 xss 即可变成存储型 xss。

案例 2

微博首页广告处，审查元素可以看到一个 ad-data url

把 url 复制下来进行解码，将 adurl 参数后面的内容删掉，则不会继续跳转到广告页面，经测试 adid 会在此接口回显出来，所以直接放 payload 即可。

https://wapwbclick.uve.weibo.com/adfront/click_deliver.php?posid=pos525904036078b&adid=<script>alert(/xss/)</script>&uid=xxxxx&size=600x80&platform=web&wm=&from=&cip=xxx.xxx.xxx.xxx&adurl=https://s.weibo.com/weibo/%2523%25E7%2594%25B5%25E5%25BD%25B1%25E7%25A9%25BF%25E8%25BF%2587%25E5%25AF%2592%25E5%2586%25AC%25E6%258B%25A5%25E6%258A%25B1%25E4%25BD%25A0%2523?topnav=1&wvr=6&b=1&wb_behavior=9&wb_stat=0

EST URL!