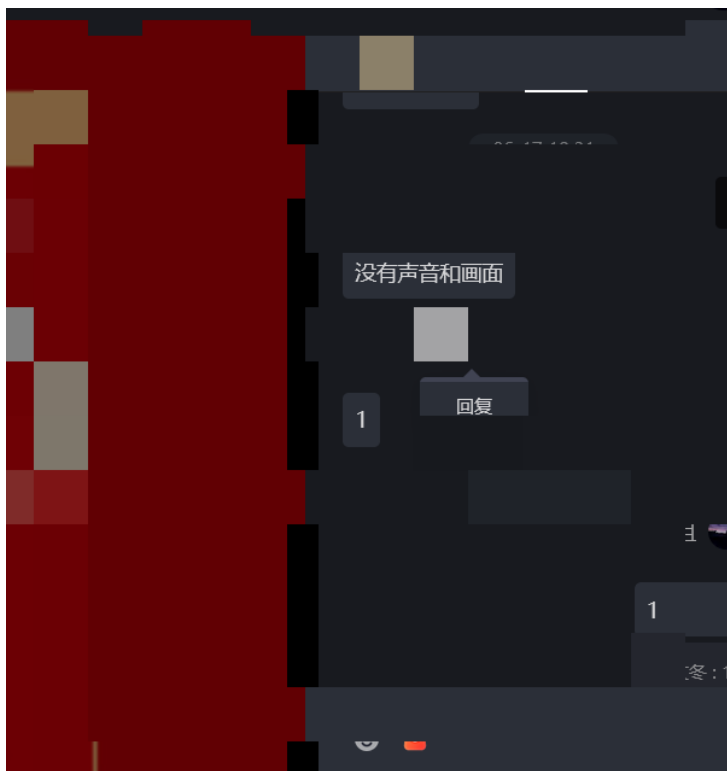
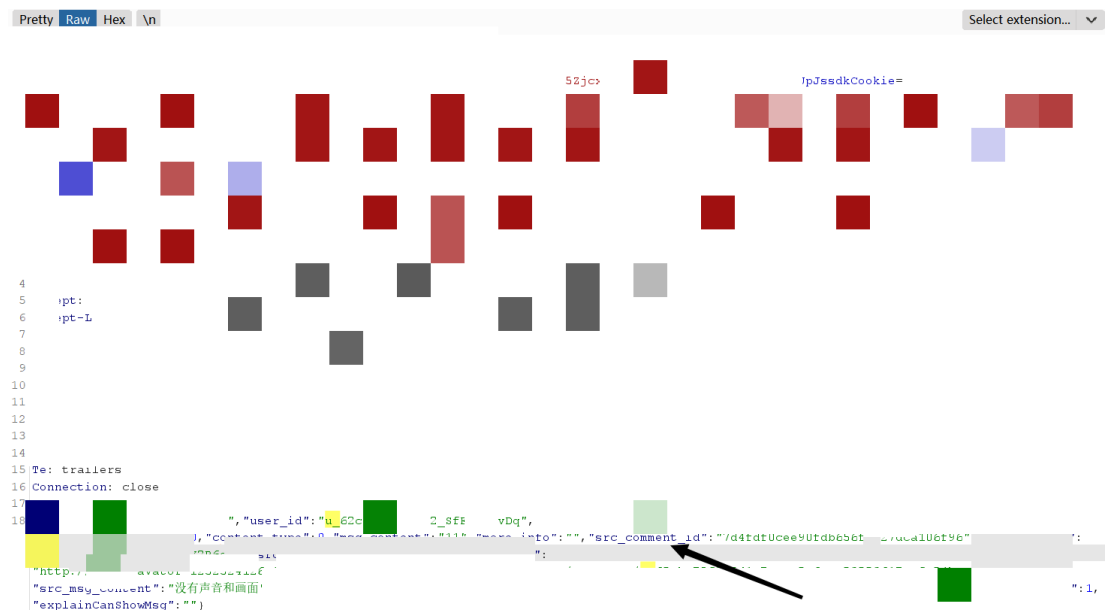


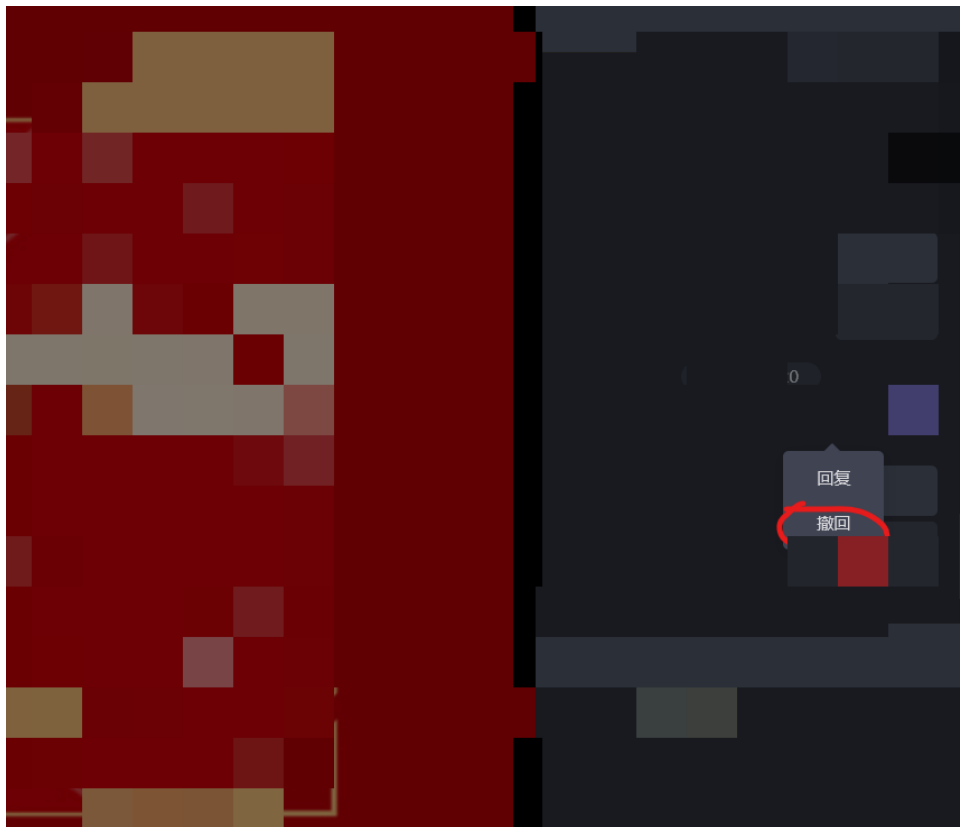
1. 在这里我们可以看到，在评论这里，有自己的发言，和别人的评论。我们点击回复，随便输入，然后点击发送，抓包，就可以看到别人的 `comment_id`:



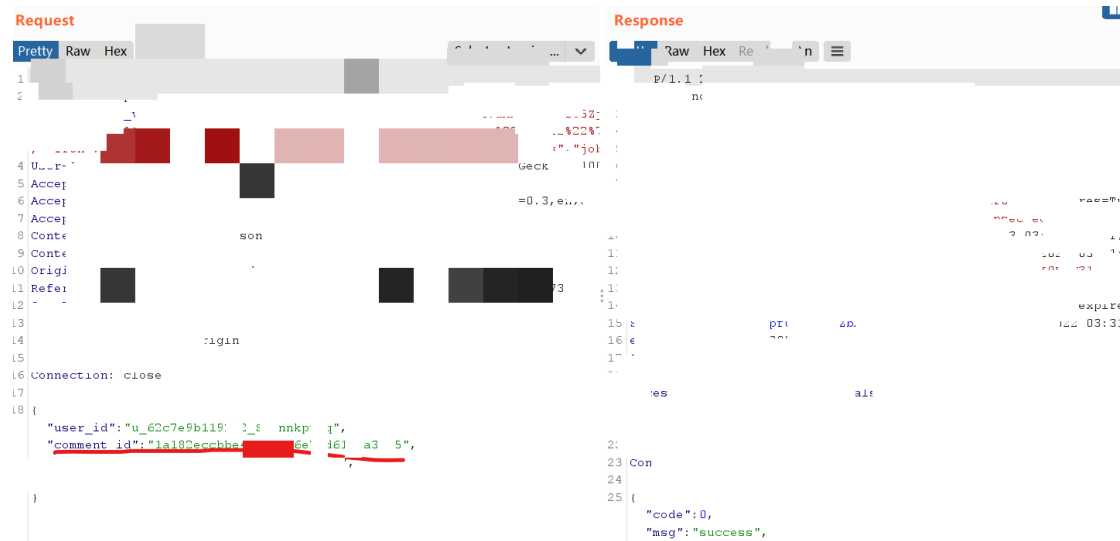
- 2.



3. 越权撤回评论，我们在回复的时候上面还携带了：
 "comment_id":"7d4fdf0cee90fdb65xxxxxxx",这个就是别人的内容 id。
 我们点击自己的评论，点击撤回，抓包



4. 我们只需要把这里的 comment_id，替换成别人的内容 id，就可以造成越权撤回任意评论内容。



5. 替换成别人的 id:发包，成功

6. 漏洞验证：可以看到，这里的那条评论已经撤回了。

