不安全对象直接调用

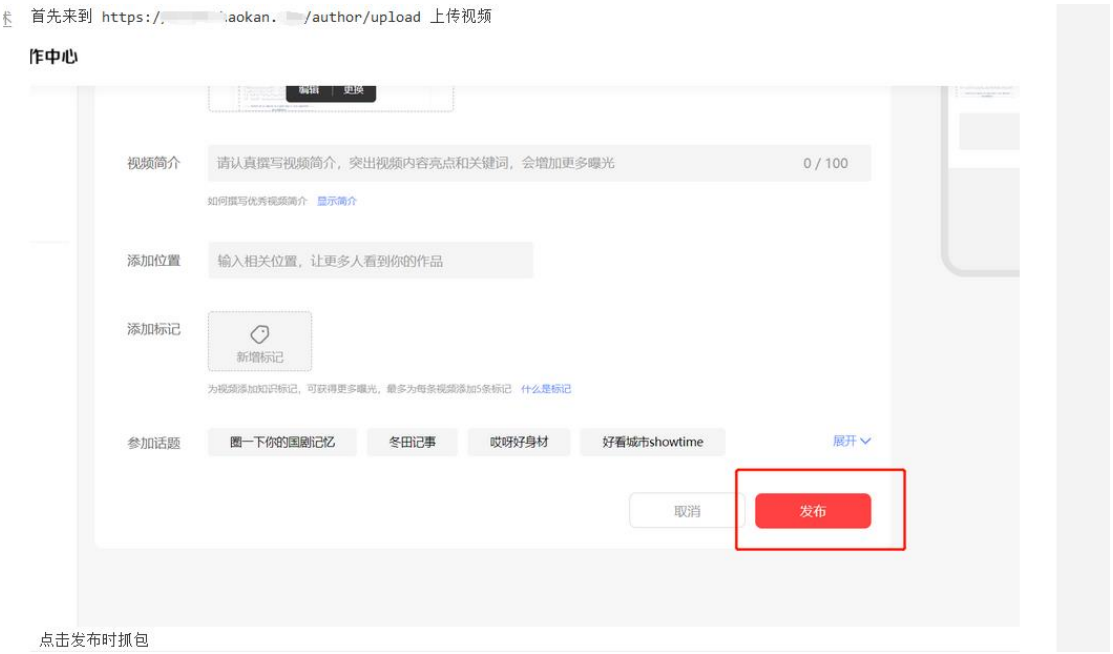
0x01：思考

结合上次的不安全对象直接调用引发的思考，因为在前站点发现我们可以通过构造 url 来免费观看别人的视频，从而可以思考，应该这个站点对鉴权做的很差，百分之八十都存在越权

所以当我们在挖一个站点的时候，出现了一个问题，肯定就还有别的地方点也可以利用这个点。

0x02：案例

某看视频的作者发布处存在越权发布别人的视频：



点击发布时抓包

可以看见我们下面的数据包出现了前面的熟悉的字眼：mad，于是猜想是否能直接调用别人的这个 mad 值来发布呢！

然后直接改为别人的视频的值：

mad 获取方法则是上一章讲述过了!!!