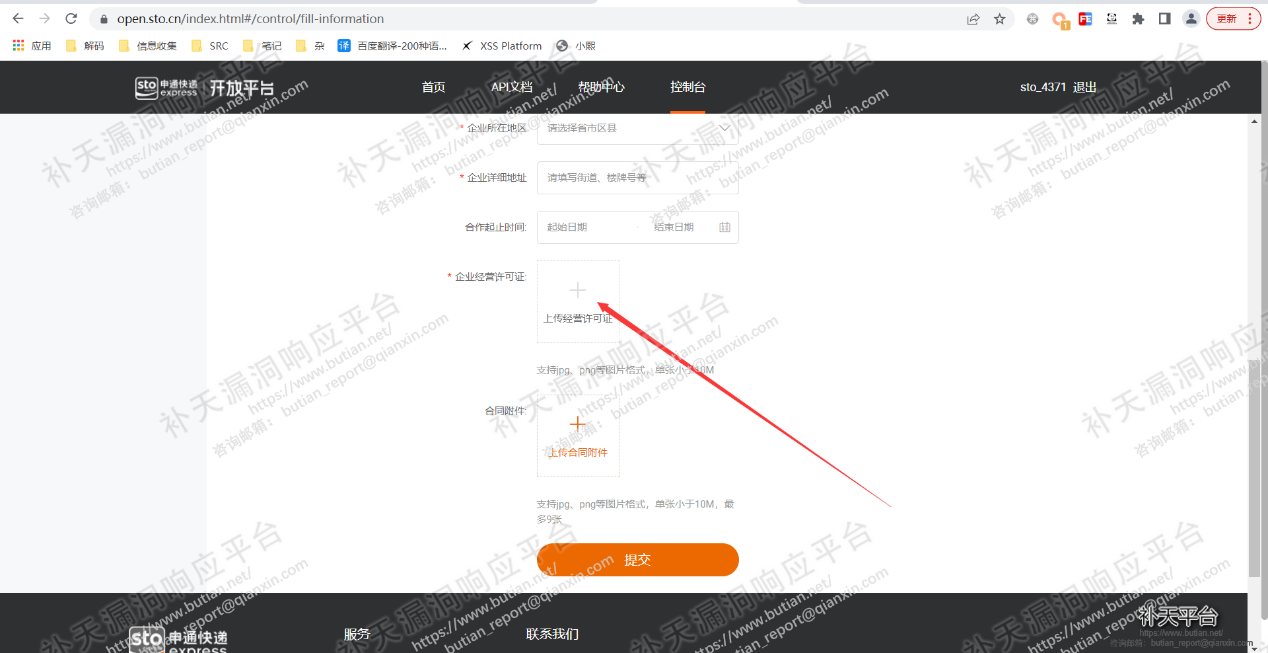
任意文件上传导致的存储型xss

漏洞详情

https://open.sto.cn/index.html#/control/fill-information

登录账号访问，找到图片上传点，开启burp抓包

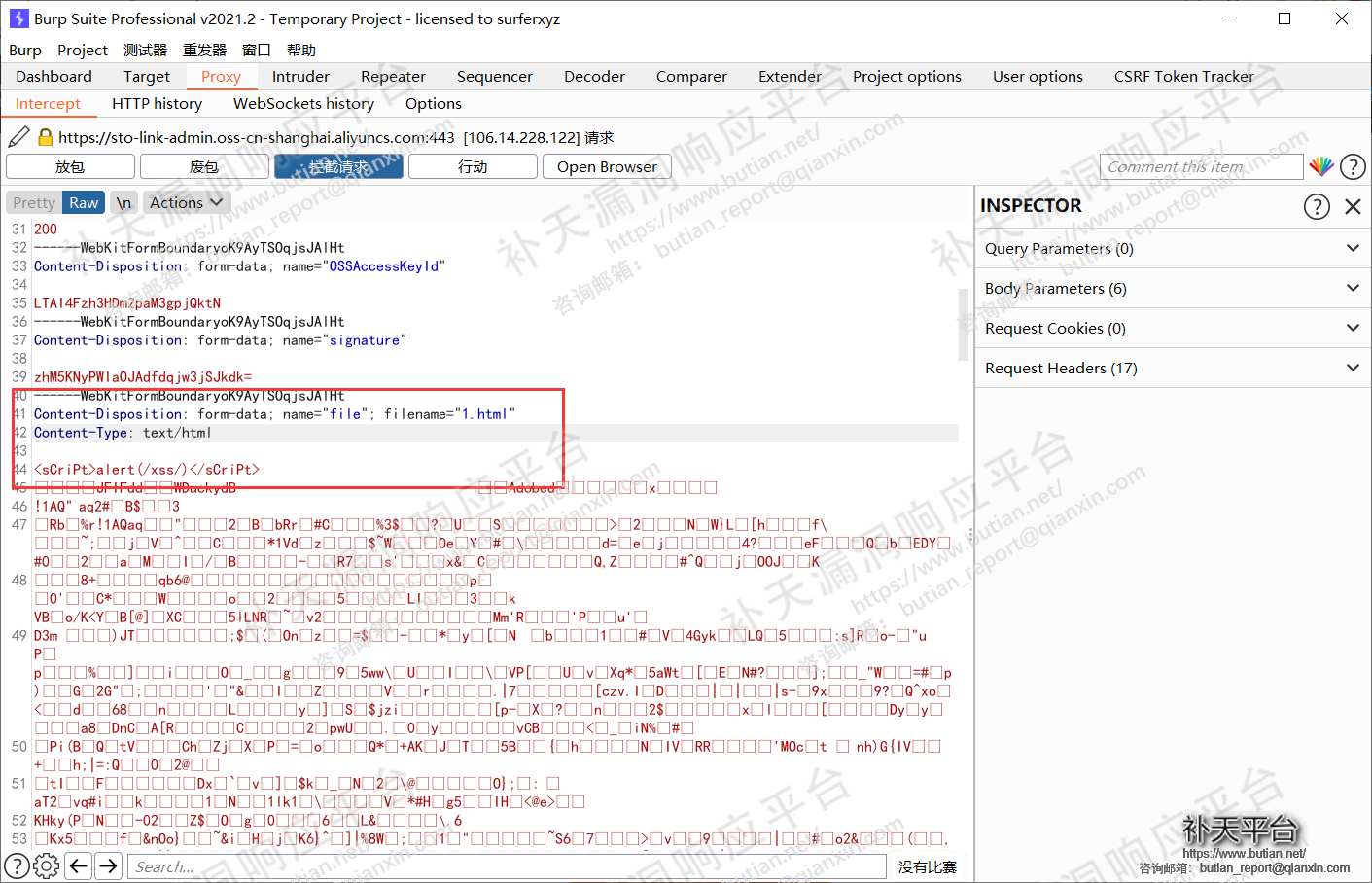


把文件后缀名修改成html

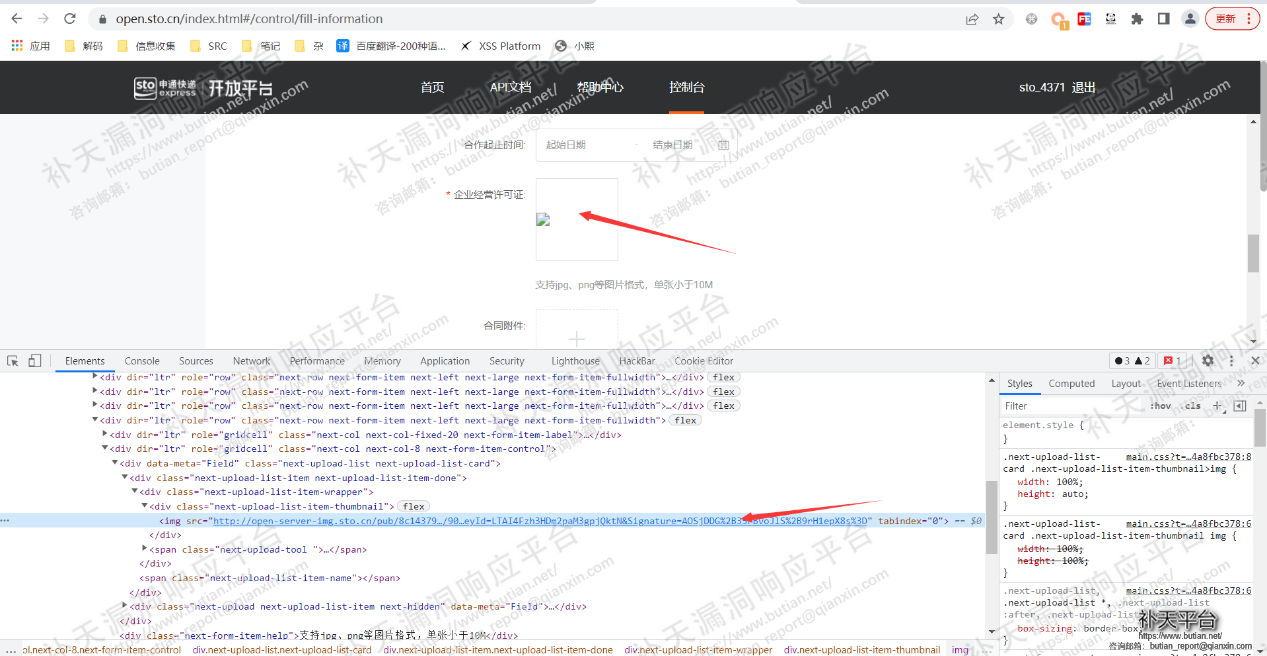
把文件类型修改成text/html

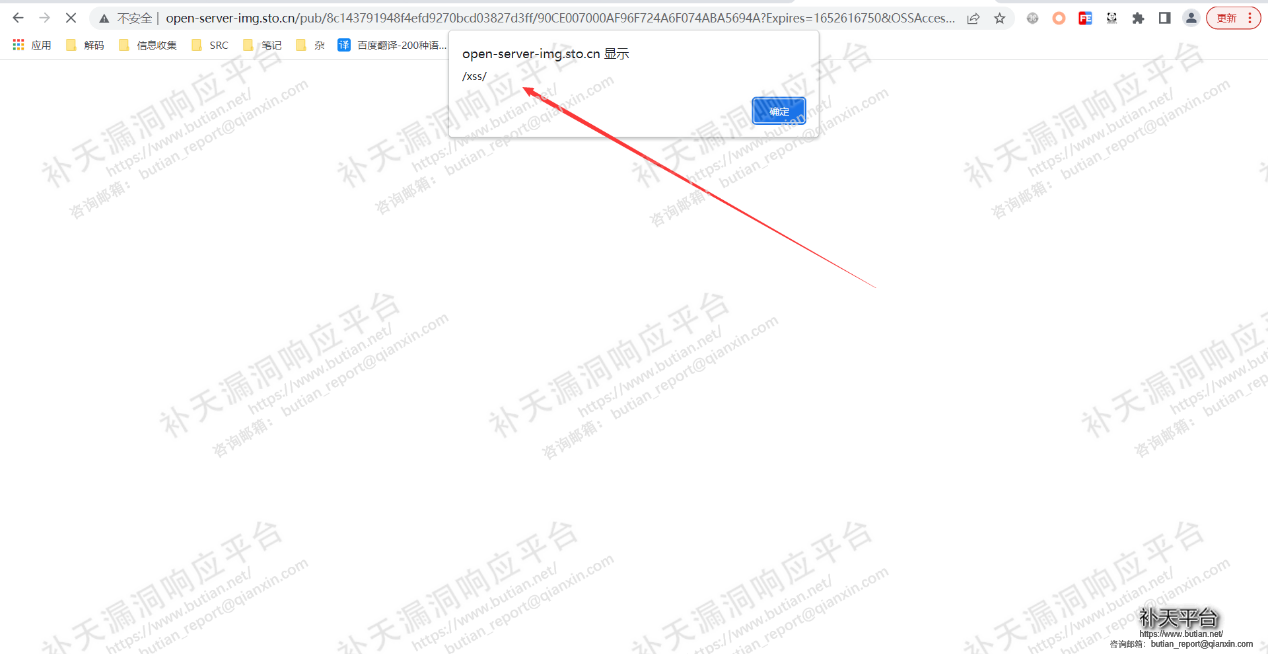
在内容中加入xss

<sCriPt>alert(/xss/)</sCriPt>



在源代码中找到图片路径，访问即可





ss