

易车小程序存在云安全问题（可执行XSS语句并且可覆盖用户上传得文件）危害十分高危

高危

2022-04-10 14:53:14

编辑

关联厂商：	北京易车信息技术有限公司
奖励额度：	待定
漏洞编号：	QTVA-2022-2727917
漏洞类型：	配置错误
官方评级：	--
<div>温馨提示</div> <div>1、已通过的漏洞，定价后将无法查看漏洞详情。</div> <div>2、未通过审核的，七天后将无法查看漏洞详情。</div>	

漏洞描述

来到易车的摩卡小程序 用户反馈处发现可以上传图片，但尝试上传发现可以上传html等文件并且可以上传至根目录并且可以解析XSS语句

漏洞详情



此处蘑卡生活发现是易车小程序得

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang

Burp Project 测试器 重发器 窗口 帮助 Turbo Intruder

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

截断 HTTP历史记录 WebSocket/历史 选项

过滤器: CSS, 图片, 一般隐藏二进制文件

#	主机	方法	URL	参数	编辑	状态	长
2317	https://mgateway.yiche.com	GET	/member-coupon/coupon-history/stat			200	270
2318	https://mgateway.yiche.com	GET	/member-coupon/coupon-history/new/count			200	199
2319	https://mgateway.yiche.com	GET	/api/order/v2/latest/list			200	379
2320	https://mgateway.yiche.com	GET	/api/order/v2/statistics			200	235
2321	https://applog.yiche.com	POST	/api/v1/upload_web_info	✓		200	225
2322	https://applog.yiche.com	POST	/api/v1/upload_web_info	✓		200	225
2323	https://applog.yiche.com	POST	/api/v1/upload_web_info	✓		200	225

请求 响应

Raw 参数 头 Hex

GET /member-coupon/coupon-history/new/count HTTP/1.1
Host: mgateway.yiche.com
Connection: close
accept: application/json, text/plain, */*
unionid: obin41AVzTZxbGUzLmZ6A-IUPJM
cookie: SESSION=YWM4ZTBjZTMhNjU3NS00ZTVLTk3ZjktNTAzYWUwZWQZjQ0
x-requested-with: XMLHttpRequest
authentication: cX1Ap41lwJtEIA4uG8oix9Tz4dds
content-type: application/json
phone: OuEVLy23dTgICZqweZTw==
User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; iPhoneXR Build/V417/R; wx) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3208 MM/WEBSDK/201201 Mobile Safari/537.36

我的



我的订单

查看全部订单 >



待付款



待发货



待收货



已完成



退款/售后

最新
订单



美食餐券

卡拉宝50元优惠券

¥0.01



工具与服务



优惠券



地址管理



分享小程序



客服帮助



意见反馈



我的设置



蘑卡生活

关注获取更多专属福利



去收快递



首页



加油优惠



我的

来到我得 点击用户反馈

来到我得 [点击用户反馈](#)

The screenshot shows the Burp Suite Professional v2.0.11beta interface. The 'HTTP History' tab is active, displaying a list of intercepted HTTP requests. A red arrow points to the third request (ID 2343), which is highlighted in orange. The request is a POST to 'https://mgateway.yiche.com/api/member/memberForMini'. Below the list, the 'Raw' tab is selected, showing the raw HTTP request details.

#	主机	方法	URL	参数	编辑	状态	长
2341	https://wl.yccdn.com	POST	/report	✓		200	196
2342	https://wl.yccdn.com	POST	/report	✓		200	196
2343	https://mgateway.yiche.com	POST	/api/member/memberForMini	✓		200	1177
2344	https://applog.yiche.com	POST	/api/v1/upload_web_info	✓		200	225
2345	https://mgateway.yiche.com	POST	/api/base/config/getList	✓		200	204
2346	https://applog.yiche.com	POST	/api/v1/upload_web_info	✓		200	225

The 'Raw' tab shows the following raw HTTP request:

```
POST /api/member/memberForMini HTTP/1.1
Host: mgateway.yiche.com
Connection: close
Content-Length: 114
accept: application/json, text/plain, */*
accept-encoding: gzip, deflate, br
accept-language: zh-CN,zh;q=0.9,en;q=0.8
cookie: SESSIONID=VWMAZ7Dj7MMqU9H900ZVLTK3ZqHfTAzYVWwZW02yG0
e-requested-with: XMLHttpRequest
authentication: oK1Apd1WU6IA4uG8oicTz4dds
content-type: application/json
phone: jY8TFrcv4dL_jwQ2LhnePuyUGSPekRUG3gn2LE=
User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; iPhoneXR Build/V417R; wml AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/96.0.4240.99 XWEB/3306 MMWEBSDK/201201 Mobile Safari/537.36
```

发现进去之后资产确实为易车得

< 意见反馈



闪退



无法打开



卡顿



黑屏白屏



死机



界面错位



界面加载慢



其他反馈

请描述具体问题

尽情吐槽您不爽的地方，或对我们提出改进性建议，
我们每条都会看的

0/60

图片补充: (相关截屏能让我们尽快找到解决问题哦)



点击上传图片

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang

Burp Project 测试器 重发器 窗口 帮助 Turbo Intruder

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

截断 HTTP历史记录 WebSocket历史 选项

📝🔒 https://mocard-1251489075.cos.ap-beijing.myqcloud.com:443 [106.119.174.14] 请求

📁 放回 🗑️ 废包 🛑 拦截请求 ⚡ 行动

评论这个项目

Raw 参数 头 Hex

POST / HTTP/1.1
Connection: close
Accept-Encoding: gzip, deflate
accept: application/json, text/plain, */*
x-requested-with: XMLHttpRequest
referer: https://servicewechat.com/wxIDQbd1ead569e0f147/page-frame.html
User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; iPhoneXR Build/V417R; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/86.0.4240.99 XWEB/3208 MMW/EBSDK/201201 Mobile Safari/537.36
MMW/EBSDK/201201 Mobile Safari/537.36
Content-Type: multipart/form-data; boundary=1649573194036
Content-Length: 70833
Host: mocard-1251489075.cos.ap-beijing.myqcloud.com

--1649573194036
Content-Disposition: form-data; name="success_action_status"

200

--1649573194036
Content-Disposition: form-data; name="x-cos-security-token"

OdozRuAx6l8XmJnhqWYymG3Ks3ZJa6041dc7c7fa3a655364874648706374kEdthGVHpmwT0d-14DUXD8fsyz4UWA01PnuSPH7QawY11xjHqW2CGkYpFmZbCmY5oX73cB9sNqkBGa3yaZU0DSF+1Lem06p65WQxk6x80ndawZaUzC06rMhCJqH2j5nzyYIG80YIMGRv60hzTHVp2xUR0gaEZBTPUUX2sJnFmkFHqM7c6SITeIVeNnZuZ6u6LsL7KjsHtmK25sSapK3OGF07_d01kbyPIE5Myzk0YFvD5WpFmK18B5ZF32Alw69ryuNCGUJuyP8ETC0A4Uy76G_ANTAF9Y2DYakAgjpp1yphA6Hg77-63AGpW6C0Y7HU0q55atX1WTawOzvt5xM6BWU7Vw_bF0g7rAYQwsDXnubYphs9CMLK4M316YPh-kikweelC2ms3_tZn1IYOHCG3G_1hSp75eBUzYixqCQJ_ID5xT9Uq6DjqH5qMGuWkVhGnTAYgCCg7JNCXBMCcyM_mhAb_eo1L3cCvW0s0q8SVm3h0DL5LDhg15kZieU5pXbOncC3P9E1rGUF3

--1649573194036
Content-Disposition: form-data; name="Content-Type"

--1649573194036
Content-Disposition: form-data; name="key"

base/upload/feedback/x1Ap41wUb5IAuG80ix9Tz4dds/1649573193992/feedback.jpg

--1649573194036
Content-Disposition: form-data; name="Signature"

q-sign-algorithm=sha1&q-ak=AKIDK5wXkRBNxxBJUaBhwFFZ8mh80EcrrEfpU-9DXGhdKAIUroZzPH2xNurVLUC&q-sign-time=1649573192;1649574092&q-key-time=1649573192;1649574092&q-header-list=&q-ur-param-list=&q-signature=43366fa5ea6b2cc89a0c9bc6770c66690934

--1649573194036

抓到此包

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang

Burp Project 测试器 重发器 窗口 帮助 Turbo Intruder

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

1 2 3 4 5 6 7 ...

📤 发送 🚫 取消 < >

目标: https://mocard-1251489075.cos.ap-beijing.myqcloud.com

请求

Raw 参数 头 Hex

WxChatArm32 Weixin NetType/WIFI Language/zh_CN ABI/arm64 MiniProgramEnv/android
Content-Type: multipart/form-data; boundary=1649573194036
Content-Length: 70833
Host: mocard-1251489075.cos.ap-beijing.myqcloud.com

--1649573194036
Content-Disposition: form-data; name="success_action_status"

200

--1649573194036
Content-Disposition: form-data; name="x-cos-security-token"

OdozRuAx6l8XmJnhqWYymG3Ks3ZJa6041dc7c7fa3a655364874648706374kEdthGVHpmwT0d-14DUXD8fsyz4UWA01PnuSPH7QawY11xjHqW2CGkYpFmZbCmY5oX73cB9sNqkBGa3yaZU0DSF+1Lem06p65WQxk6x80ndawZaUzC06rMhCJqH2j5nzyYIG80YIMGRv60hzTHVp2xUR0gaEZBTPUUX2sJnFmkFHqM7c6SITeIVeNnZuZ6u6LsL7KjsHtmK25sSapK3OGF07_d01kbyPIE5Myzk0YFvD5WpFmK18B5ZF32Alw69ryuNCGUJuyP8ETC0A4Uy76G_ANTAF9Y2DYakAgjpp1yphA6Hg77-63AGpW6C0Y7HU0q55atX1WTawOzvt5xM6BWU7Vw_bF0g7rAYQwsDXnubYphs9CMLK4M316YPh-kikweelC2ms3_tZn1IYOHCG3G_1hSp75eBUzYixqCQJ_ID5xT9Uq6DjqH5qMGuWkVhGnTAYgCCg7JNCXBMCcyM_mhAb_eo1L3cCvW0s0q8SVm3h0DL5LDhg15kZieU5pXbOncC3P9E1rGUF3

--1649573194036
Content-Disposition: form-data; name="Content-Type"

--1649573194036
Content-Disposition: form-data; name="key"

base/upload/feedback/x1Ap41wUb5IAuG80ix9Tz4dds/1649573193992/feedback.jpg

--1649573194036
Content-Disposition: form-data; name="Signature"

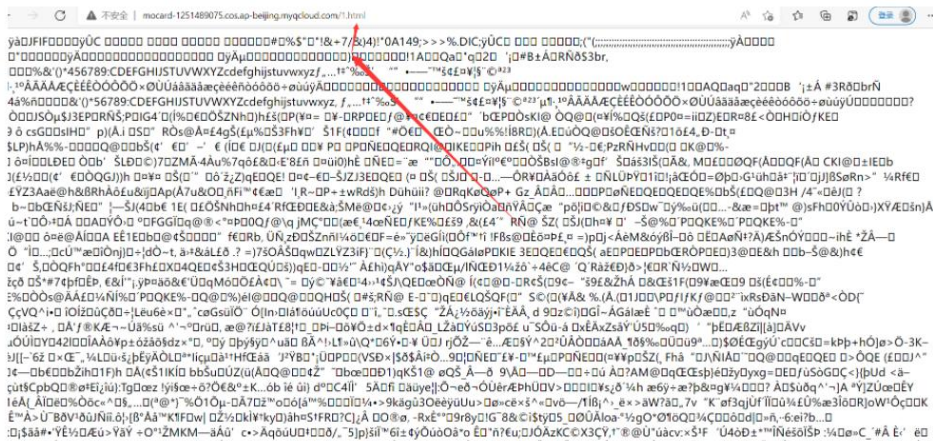
q-sign-algorithm=sha1&q-ak=AKIDK5wXkRBNxxBJUaBhwFFZ8mh80EcrrEfpU-9DXGhdKAIUroZzPH2xNurVLUC&q-sign-time=1649573192;1649574092&q-key-time=1649573192;1649574092&q-head

响应

Raw

修改此处路径 改成1.html

再此之前我已经上传了一个html



为没有放入XSS语句得html

我们现在上传一个名字一样的html

看看是否会被顶替并且执行XSS语句

