个人中心
我的贡献值/安全币
我提交的漏洞
我的首杀奖励
我的个人信息
我的礼品
我的消息

漏洞/情报详情

漏洞/情报名称: 美团存在任意用户劫持(可接管任意用户账号)

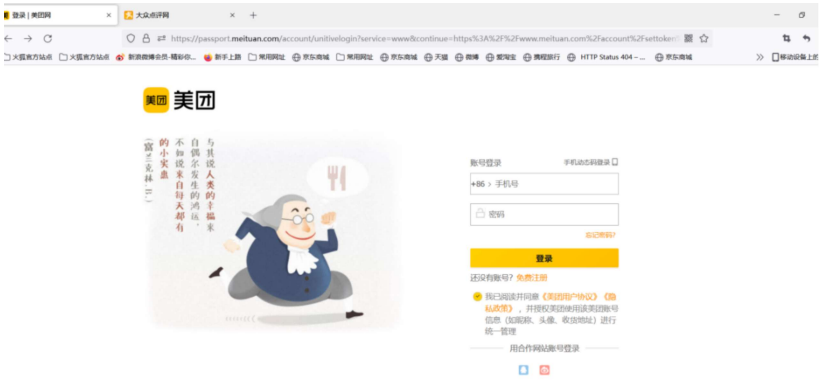
漏洞/情报类型: Web安全漏洞 设计缺陷/逻辑错误

漏洞/情报URL:
https://passport.meituan.com/account/unitivelogin?service=www&continue=https%3A%2F%2Fwww.meituan.com%2Faccount%2Fsettoken%3Fcontinue%3Dhttps%253A%252F%252Fxa.m

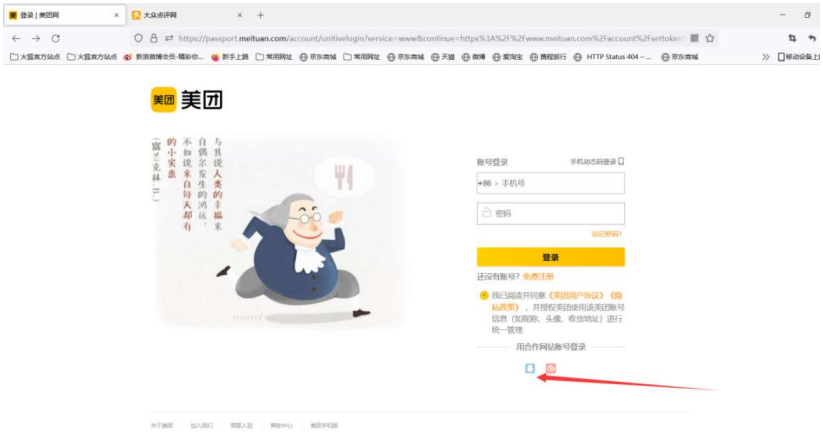
漏洞详情:

漏洞说明：测试发现大众点评和美团可以进行URL跳转交互 问题出现在此，发现QQ绑定code这个关键值可以把他发送给用户造成用户不知情 情况把Q绑定他的手机号从而实现通过Q看他所有信息

漏洞复现：此时先打开两个界面 一个大众点评 一个美团 大众点评用来迷惑用户 而美团是真正的核心



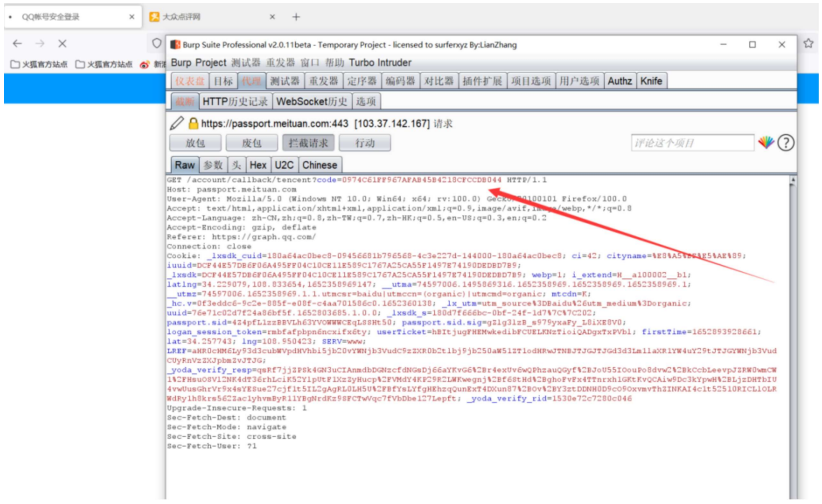
确保大众点评和美团都是打开的 此时我们来操作



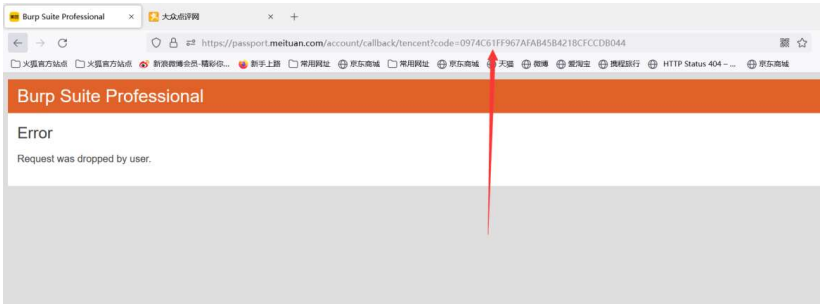
点击QQ登录

点击授权并登录然后抓包

看好 一直放到此包 此处是漏洞关键点



此处保存code值 然后废包一定要废包！！！！



此包有效 一定记住 此包有效

我们来到点评

https://passport.meituan.com/account/callback/tencent?code=0974C61FF967AFAB45B4218CFCCDB044

将此链接拼接到大众点评redir参数地下

https://account.dianping.com/pclogin?redir=https://passport.meituan.com/account/callback/tencent?code=0974C61FF967AFAB45B4218CFCCDB044

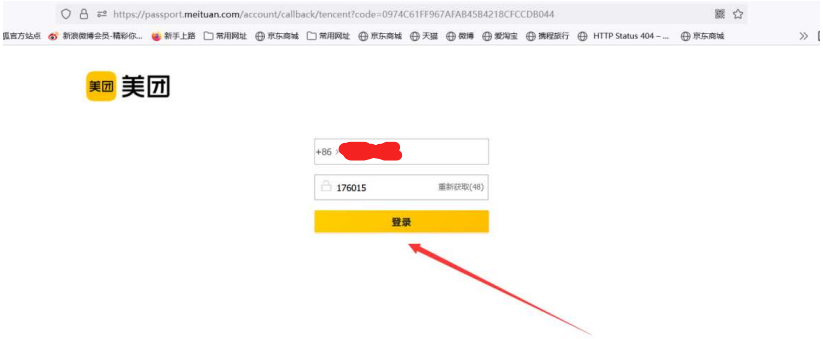
依旧可以访问 此处是迷惑用户 当然 你也可以直接把美团废包链

真实也不需要迷惑的

关键来了

用户点击登录

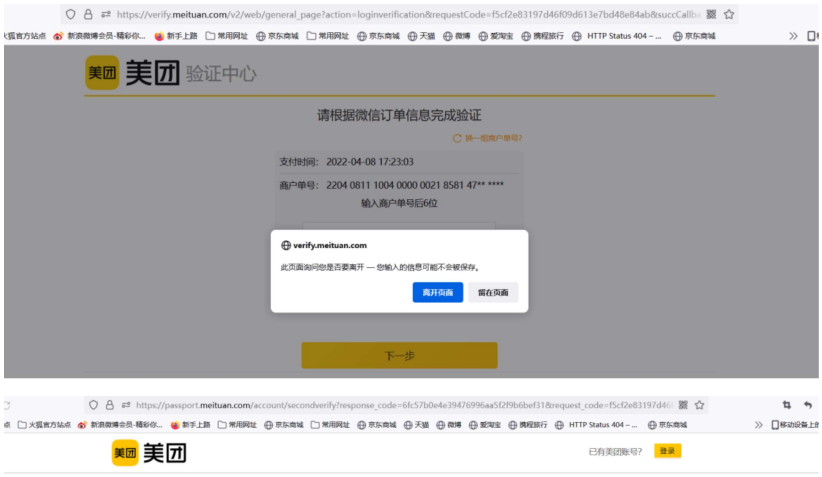
跳到了绑定美团处！！！！！我们模拟用户输入手机号然后绑定，关键就在于用户也不知道这个是什么



点击登录

用户以为美团认证呢

输入点击下一步



成功绑定 ！！！！！

重新输入QQ看是否可以登录用户美团

成功登录~~~~~~~~~~~~.

修复建议：绑定应当进行紧密联系，不应当让黑客变成可控URL

也可以将废包的那个链接直接发送给用户，用户察觉不到，已经成功接管了一名用户，查看到了用户所有信息，修复建议就是加入类似于token一样的校验 不让其他地方用户可打开 若其他用户点击链接 应当跳转美团主页就OK，修复参照例子来自于什么值得买

这里有问题的话，微信微博等多方面第三方登录是否存在一样的类似问题

还有 自己评严重 因为链接属于美团的 告诉用户登录账号即可 并且最严重的就是昨天接管了一名用户 可用APP登录查看此用户所有信息 家庭住址等详细信息 银行卡 等不用说了

还有一点 就是接管了此用户 无论用户怎么修改密码 都可以登陆上此用户账户 属于永久接管 因为绑定不会给用户提示

自评级别: 严重

漏洞情报系统信息

提交人	业务评级	漏洞状态	审核时间	安全币	贡献值	提交时间	备注
天然呆		已忽略	2022-05-19	0	0	2022-05-19	此漏洞内部已知，感谢关注

漏洞留言(0)

H B I U S A A

请填写内容

请向右拖动滑块

关注我们: