机缘巧合之下拿下个发卡网还撸了把羊毛

原创李公子 HACK学习呀
2020-08-05原文

0x01 事情经过

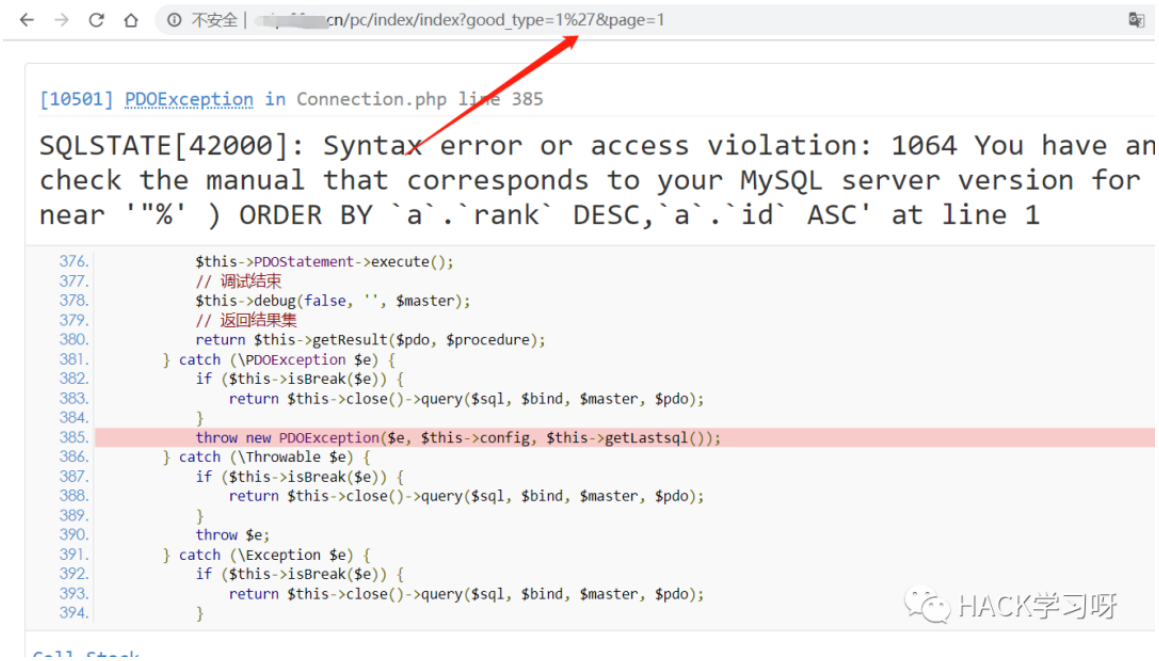
家乡群有个不是我们老家的广告狗天天发"出售微信抢红包软件"广告，发一次两次就算了，每天都发。最讨厌的是我在群里吹牛逼的时候他出来发广告？严重影响群内人员吹逼，十分可恶~，然后加了好友，居然发现这是我初中同学，在和他py一番了，他居然同意我对他的网站进行渗透测试，那就干就完事了，站长都同意授权了，开干

0x02 渗透过程

网站打开这个样子↓↓↓

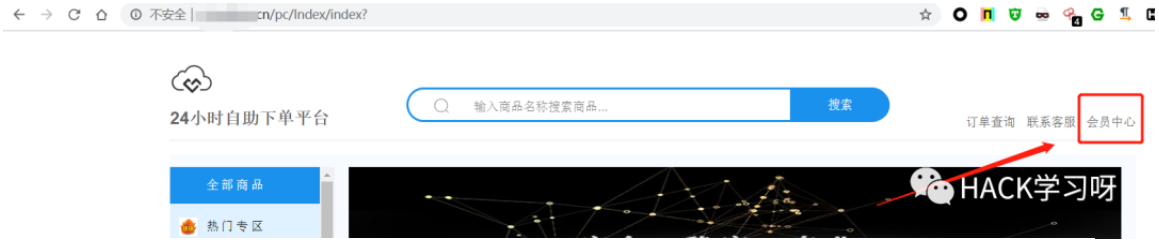
意外发现他还卖手机短信轰炸，电话轰炸的商品，必须干他啊！

随便点几个网页在参数的值后面加个'就找到个注入



SQLMap跑数据库没有发现后台管理员相关信息，陷入了沉思。

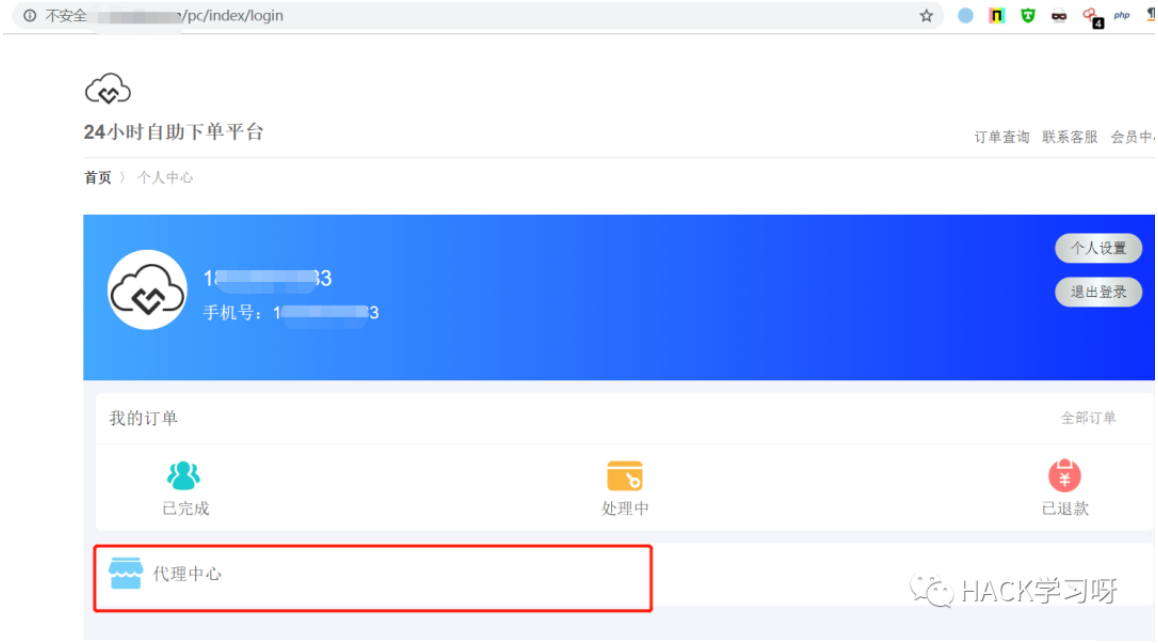
试试其他功能点吧，看到主页有个会员中心



注册个账号试试？会员中心的修改资料处有个上传提现二维码，试试上传一句话木马？

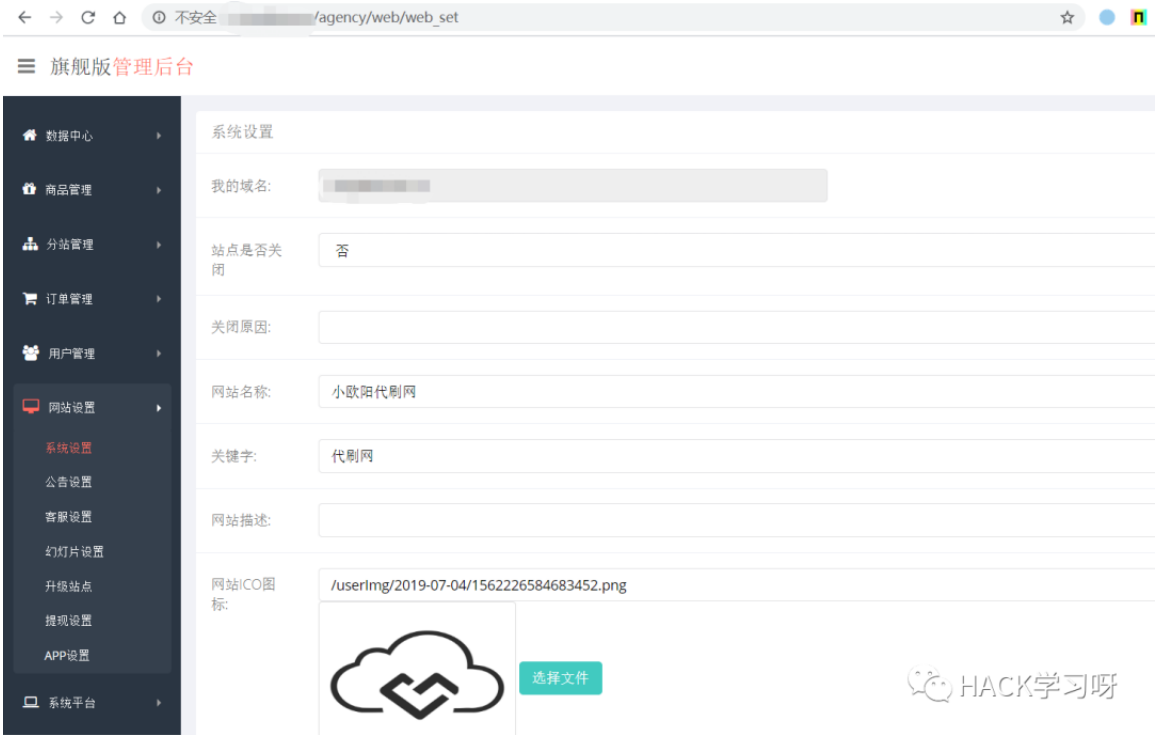
mmp，正常图片都上传不上去，只能想想其他办法。

正常用户不能上传图片，哪么代理商是不是有上传图片的功能呢，

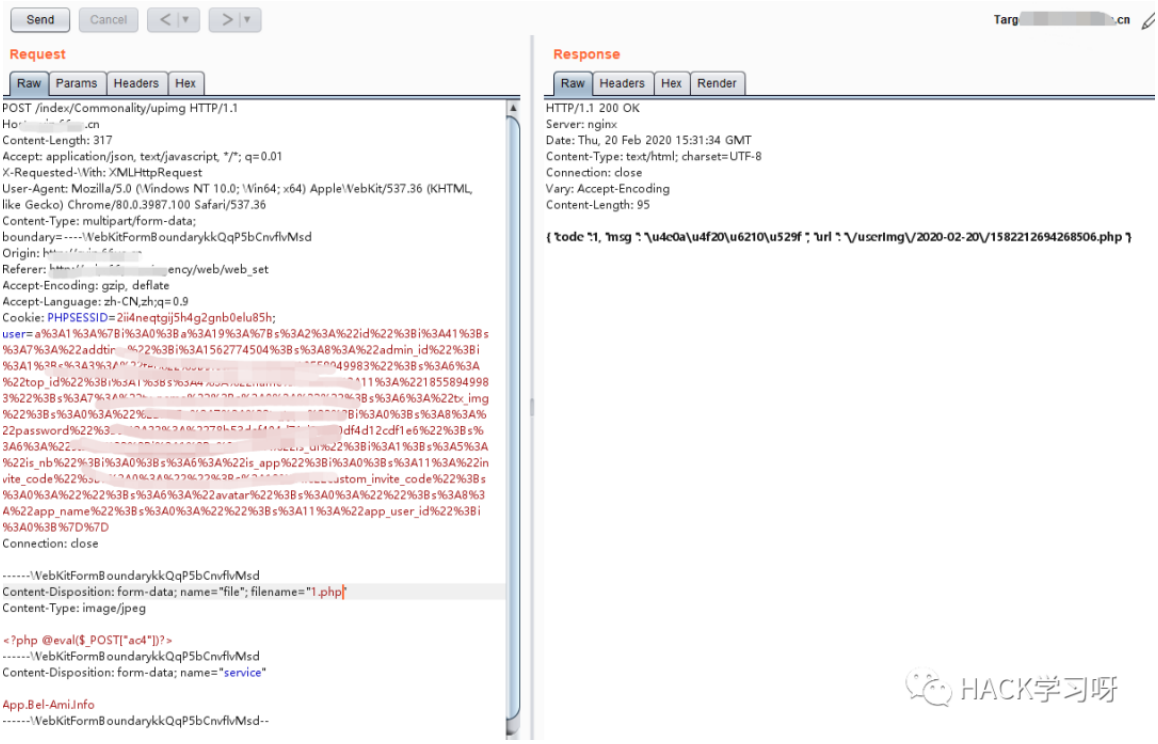


前面已经找到了注入，虽然没找到管理员的账号，但是搞个代理商的账号没问题。

代理商的后台有个网站ICO图标上传的功能，上传一句话试试吧。



狗屎运，上传点只校验了前端，简单的绕过然后就上传成功了~

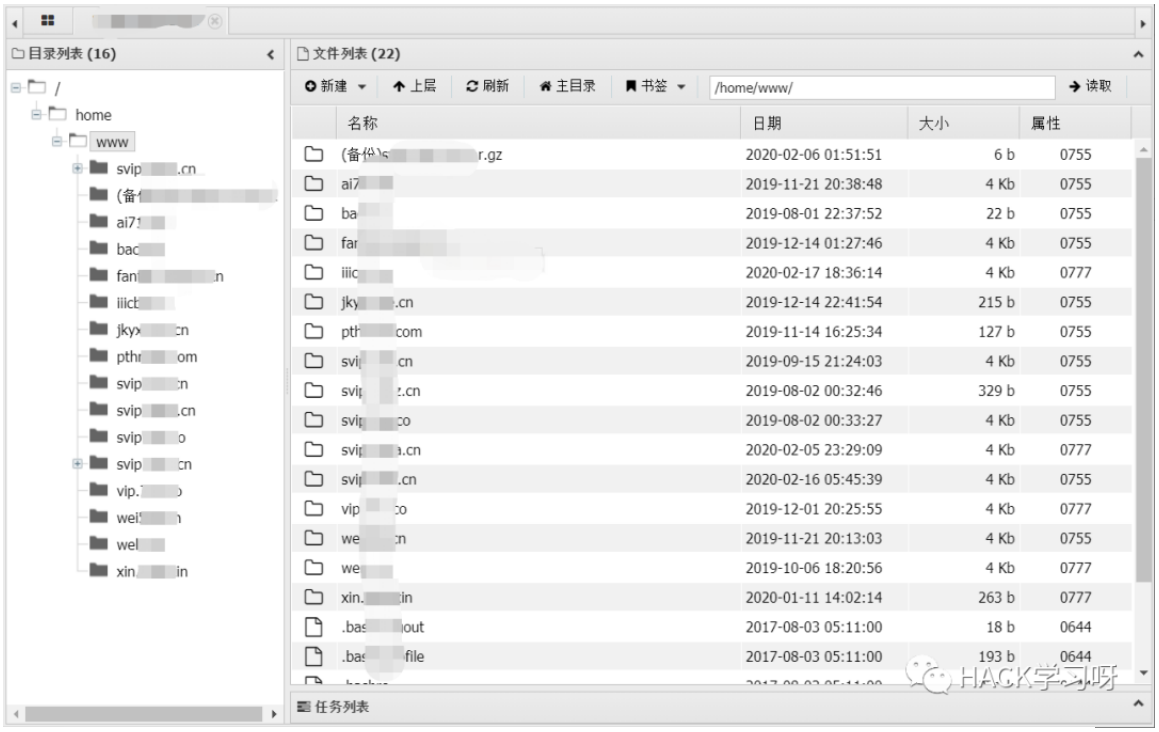


webshell客户端连接我先是用菜刀发现连接不上去，最后发现对方服务器PHP版本是7.0，到网上去看了下文章尝试了下用蚁剑连接，发现可以正常连接了。菜刀连接不上的原因是PHP高版本中过滤了一些字符和函数。

0x03 撸羊毛

拿下shell发现网站是宝塔搭建的，尝试了下绕过disable_functions，遂失败~

浏览目录发现还有服务器上面还有其他网站,但是可以执行sql语句



打开svip.xxx.cn

还可以充Q钻，来两个吧，重回初中年代充Q币开QQ会员体验飞一般的感觉

网站上面注册个用户，然后sql语句将money调整为100，充了个球球超级会员，开心！

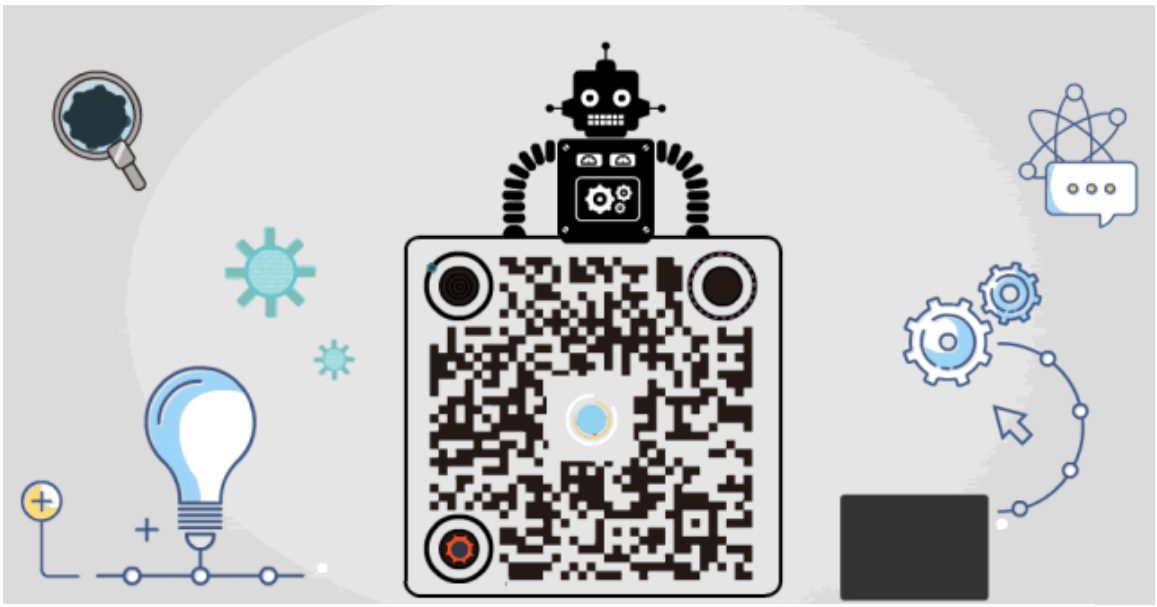
充完后删除了我注册的用户、充值记录、ip信息。

最后告诉了朋友，修复了该站的漏洞，舒服

END

点赞，转发，在看

投稿作者:李公子



精选留言

用户设置不下载评论