记一次渗透 | 被骗4000花呗背后的骗局

原创夜无名 HACK学习呀
2020-07-04原文

作者：夜无名

***严正声明：本文仅限于技术讨论与分享，严禁用于非法途径。**

0X00 事情起因

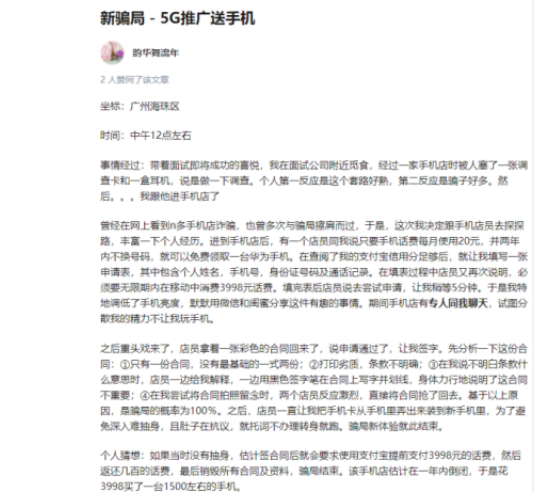
事情是这样子的，那天逛着街路过一家手机店，当场被店门口招揽客人的销售员拦下，硬塞了一张活动条和充电宝给我说什么充电宝免费送，但要到店里边填个卷就行了，七月的天异常的热，反正也没什么急事进去蹭蹭空调也不错，进店后里面的店员向我要了号码说是要查一下积分，通过短信查询告知我号码的积分是一千八百多，细节来了：这里他表现的很惊讶问我的积分为什么那么高，积分高的话这里好啊那里好的给我一顿吹嘘使我膨胀，后面他拿出个清单说你这积分已经可以领平板电脑了，清单上面有手充电宝、小风扇、手机、电饭锅和平板电脑等等，当然平板电脑排在最高积分那，按照常人的选择大部分人都会选择平板电脑我也不例外的选择了平板，出来逛个街白嫖个平板它不香么，我再三的跟他确认可以免费拿的吗，他是的是的回答，可正中了他的套路。

后面是另一位店员来接待我，把我拉到了店的最里边然后给我说到这边来跟你了解一些情况还有拿新的平板给你，问我有几张卡呀每个月所用的话费是多少，还有说这活动呢是针对一些信用高的用户做的回馈，然后让我打开支付宝看我的信用，我每月的花呗都会还本来信用就蛮高的，他又一顿的给我吹嘘我的信用有多高多高的使我膨胀，他又问我你这号码确定会使用一年以上吗之后他拿出一张表上面写着预存话费3999送平板什么什么字样，他见我犹豫了又给我列了一堆的公式各种计算话费跟你平时充值的费用一年下来多少多少的，涉

世未深的我还觉得挺有道理的，总之从一进店开始就一直被牵着鼻子走，然后他问我要了身份证号说什么后台做个审核还特地强调说有些信用不好不是谁都可以通过的，他说给我审核两分钟，实际是直接给我开了个户，然后在我签字那个表盖了审核通过的字样，这里细节来了：第一审核通过了或者没通过他都没跟我确认要不要开户，第二他直接在你户里给你预存了3999话费并不是让你先支付后预存的，这就是所谓的"免费送"这时我已经感觉到不对劲了想走不办理了，但被告知账户已帮我预存了话费不让走，无奈只好给他支付宝一顿操作又套现又转账的把我花呗都套走了。

回到家越发越觉得不对劲，越发越后悔，网上一搜关于这类的活动一抓一大把而且一模一样越看是越生气啊。

知乎



新骗局 - 5G推广送手机

韵华舞流年

2 人赞同了该文章

坐标：广州海珠区

时间：中午12点左右

事情经过：带着面试即将成功的喜悦，我在面试公司附近觅食，经过一家手机店时被人塞了一张调查卡和一盒耳机，说是做一下调查。个人第一反应是这个套路好熟，第二反应是骗子好多。然后。。。我跟他进手机店了

曾经在网上看到n多手机店诈骗，也曾多次与骗局擦肩而过，于是，这次我决定跟手机店员去探探路，丰富一下个人经历。进到手机店后，有一个店员同我说只要手机话费每月使用20元，并两年内不换号码，就可以免费领取一台华为手机。在查阅了我的支付宝信用分足够后，就让我填写一张申请表，其中包含个人姓名，手机号，身份证号码及通话记录。在填表过程中店员又再次说明，必须要无限期内在移动中消费3998元话费。填完表后店员说去尝试申请，让我稍等5分钟。于是我特地调低了手机亮度，默默用微信和闺蜜分享这件有趣的事情。期间手机店有专人同我聊天，试图分散我的精力不让我玩手机。

之后重头戏来了，店员拿着一张彩色的合同回来了，说申请通过了，让我签字。先分析一下这份合同：①只有一份合同，没有最基础的一式两份；②打印劣质，条款不明确；③在我说不明白条款什么意思时，店员一边给我解释，一边用黑色签字笔在合同上写字并划线，身体力行地说明了这合同不重要；④在我尝试将合同拍照留念时，两个店员反应激烈，直接将合同抢了回去。基于以上原因，是骗局的概率为100%。之后，店员一直让我把手机卡从手机里弄出来装到新手机里，为了避免深入难抽身，且肚子在抗议，就托词不办理转身就跑。骗局新体验就此结束。

个人猜想：如果当时没有抽身，估计签合同后就会要求使用支付宝提前支付3998元的话费，然后返还几百的话费，最后销毁所有合同及资料，骗局结束。该手机店估计在一年内倒闭，于是花3998买了一台1500左右的手机。

消费者"匿名"在3月29日向黑猫投诉平台再次反映："【中国移动线下活动】事情缘由:手机店店员以拉取路人投票为由，一步步诱导路人参与活动。一开始店员告知我只要移动手机积分达到一定分值以及移动卡年限为5年期以上就可以参与免费领手机的活动，此活动免费参与。我想，既然免费，参与也没什么问题。但当签好合同时，店员才告知其他注意事项(起先店员只告知我手机移动卡只需日后消费累计达3299元即可)！！店员要求我:①此号码不能停机断网超过半小时②每个月要按时接通客服人员打的电话，(不接后半小时没有回电则视为违规)③此卡要消费累积要达到3299元，此前如有一条违规则需从电话卡中扣取违约金，一次约200，扣除无上限！！！！起先店员对违约金闭口不谈，存在虚假宣传行为。我当时就意识到问题的严重性-----因为我是一个在校大学生，存在在校考试需要关机断网的现象，长期想必一定要付巨额违约金！店员发现这种情况后就向我推荐了另外一个方案，因为已经签约，现只能改方案。另一个方案如下:一次性充值3299(条件无限制)，首次返300，其后下一年每月按月套餐返还，直至剩余2999全部返还。想着不偿还巨额违约金，我无奈之下只好选择这个方案。可是2020年已经到了，话费却没有如期返还，此活动为中国移动线下活动，[illegible]中国移动大到小解释。"

最主要的呢，送的平板也是八百多的根本不值预存话费的这个价，且居然有卡死的现象，于是乎我决定深挖瞧瞧。

0X01　信息收集

通过验证短信发过来的短域名链接复制到浏览器解析得到网址xx.xxxx.xx好家伙这网址一看就不是移动官方旗下的,在通过站长工具查询该网址解析到阿里云且未启用cdn，该域名持有者系广东一家某科技公司，域名到今年11月份就到期了，在通过搜索该企业发现经营异常这四个大字，我这好几千的话费肯定是凉透了。

短信/彩信

6月27日 15:11 1

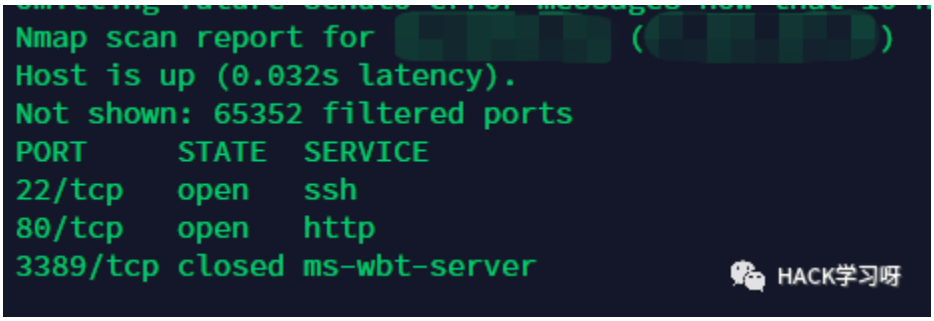
【[redacted]敬的用户13[redacted]，您申请的0元惠机业务已通过！身份证专享额度为3999元。感谢您参与活动，祝您生活愉快，详情请见http://t.cn/[redacted]。

网站基本信息

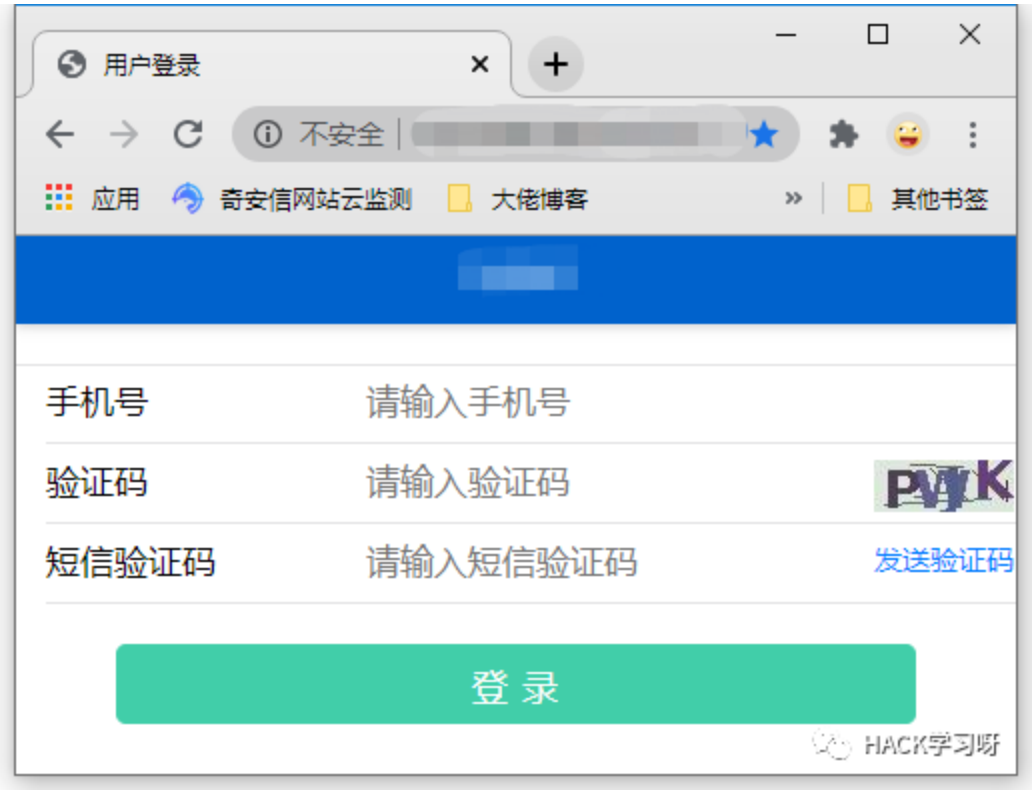
[redacted]登录 [更新]

SEO信息	百度权重: 0 移动权重: 0 360权重: 0 搜狗PC权重: 0 神马权重: 0 头条权重
域名解析	同IP网站: 0个 响应时间: 11毫秒 IP: [redacted] 阿里云]
域名年龄	1年7月29天（创建于2018年11月03日,过期时间为2020年11月03日）
域名备案	备案号: [redacted] 性质: 企业 名称: [redacted]科技有限公司 可信百科 未认证
安全认证	水滴信用: 未认证 创宇认证: 未认证 百度信誉: 未认证 SSL证书: 未启用 https
更多查询	ALEXA排名 友情链接检测 网站历史数据 Whois查询 备案查询 网站排名 网站安全

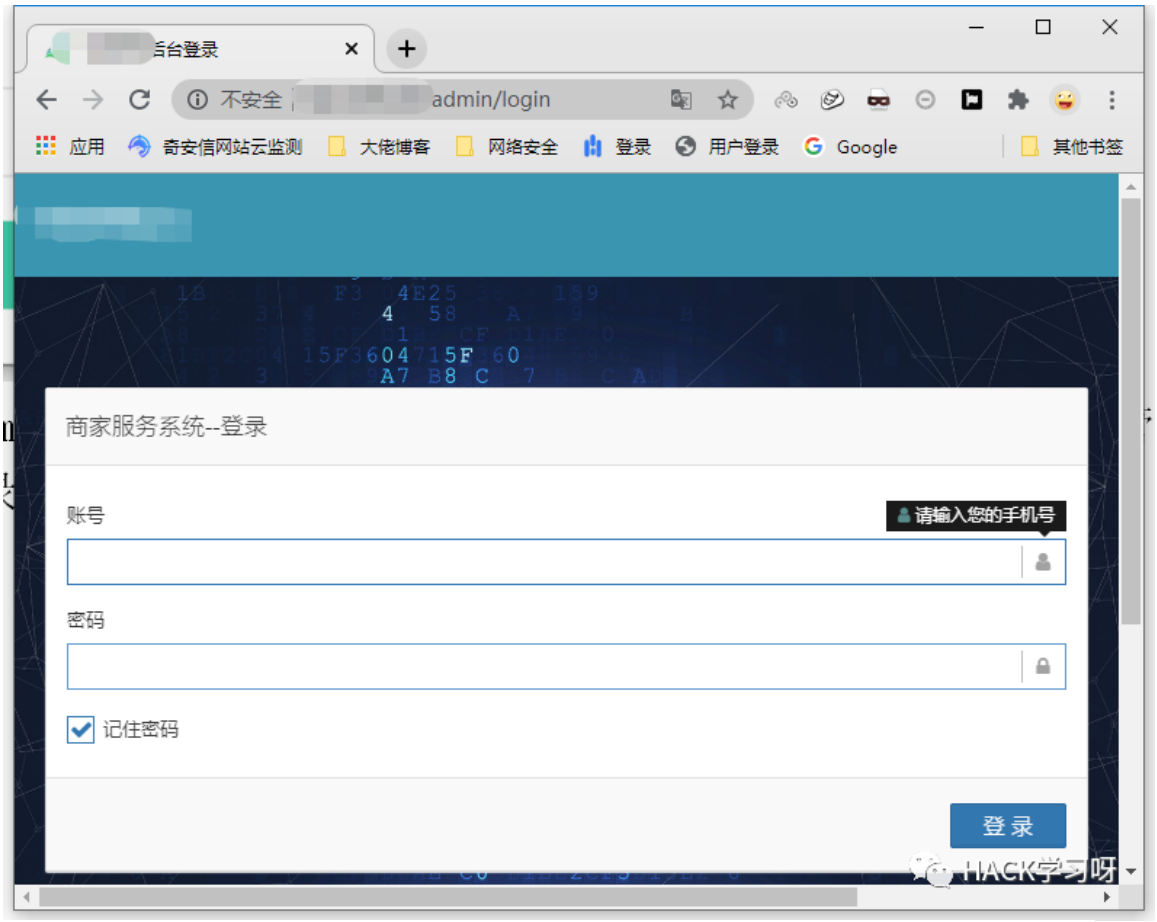
通过对得到的域名用nmap -p 1-65355 xx.xxxx.xx进行全端口扫描瞧瞧都开放了哪些服务，再从其服务进行入手，可以看到也就只有80跟22端口，唯一有用的信息就是22端口知道对方是Linux服务器的。



在通过对80端口访问web服务得到以下信息，这界面也是短信内容里短域名所跳转过来的界面。



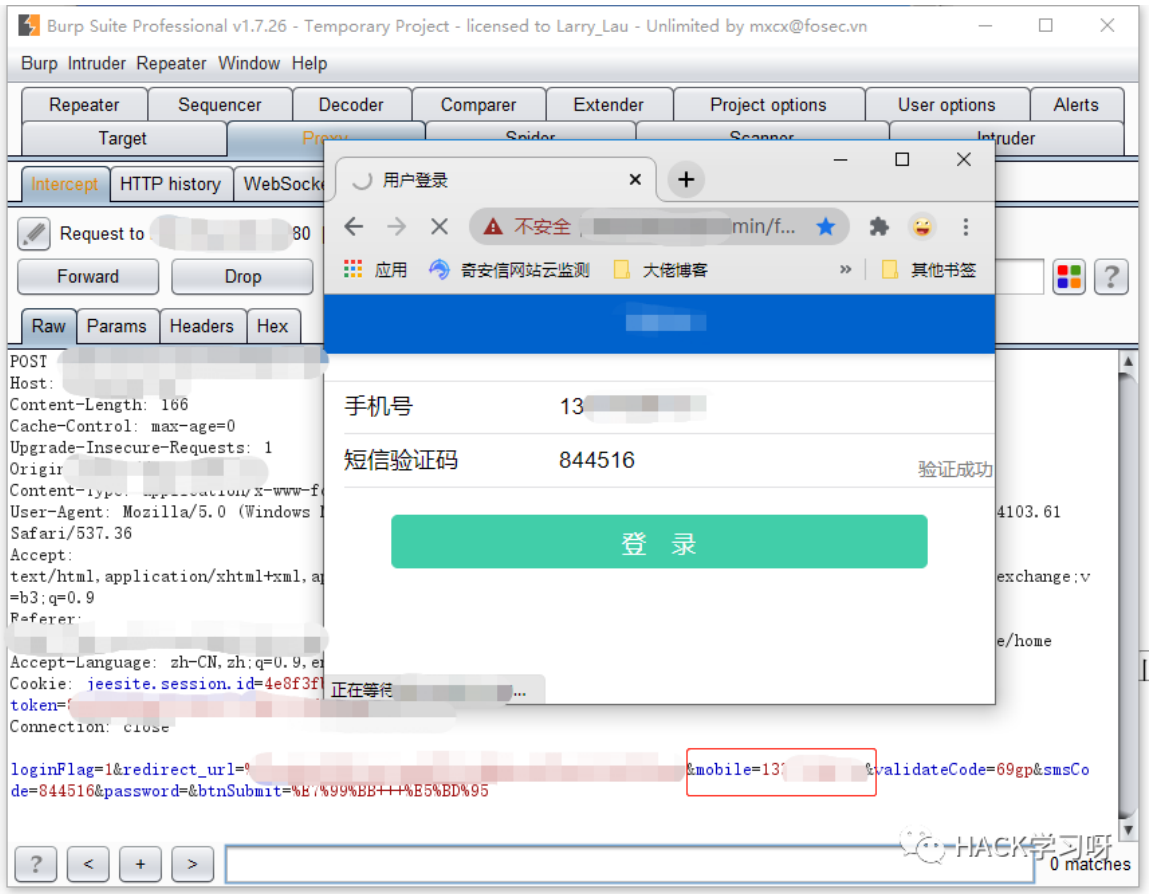
它的URL形式是/admin/user/login明显的用户登陆界面，众所周知admin是管理的意思，直觉让我逐层递减目录访问，果不其然跳转到了admin/login的商家管理界面。



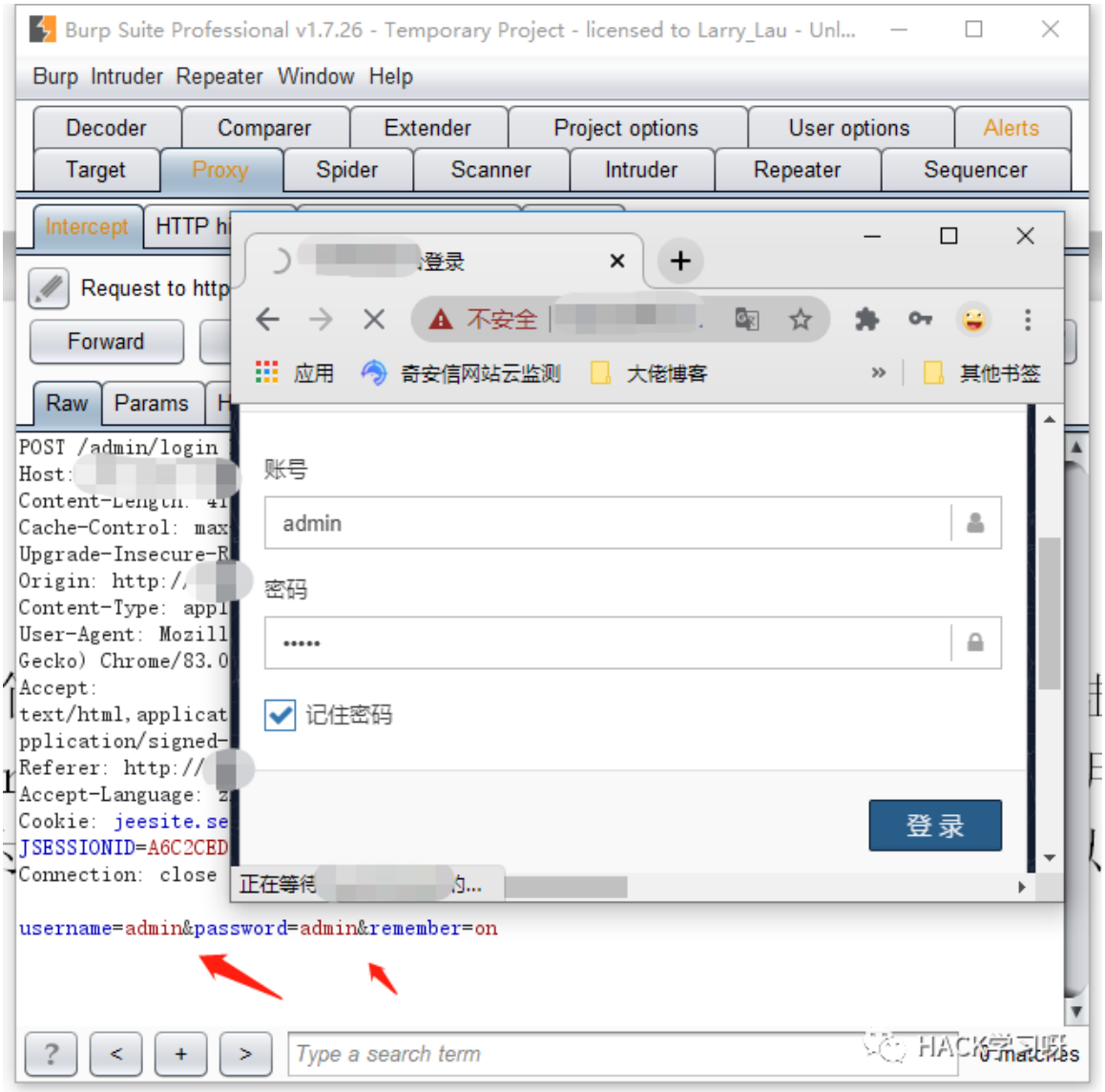
0X02　漏洞挖掘

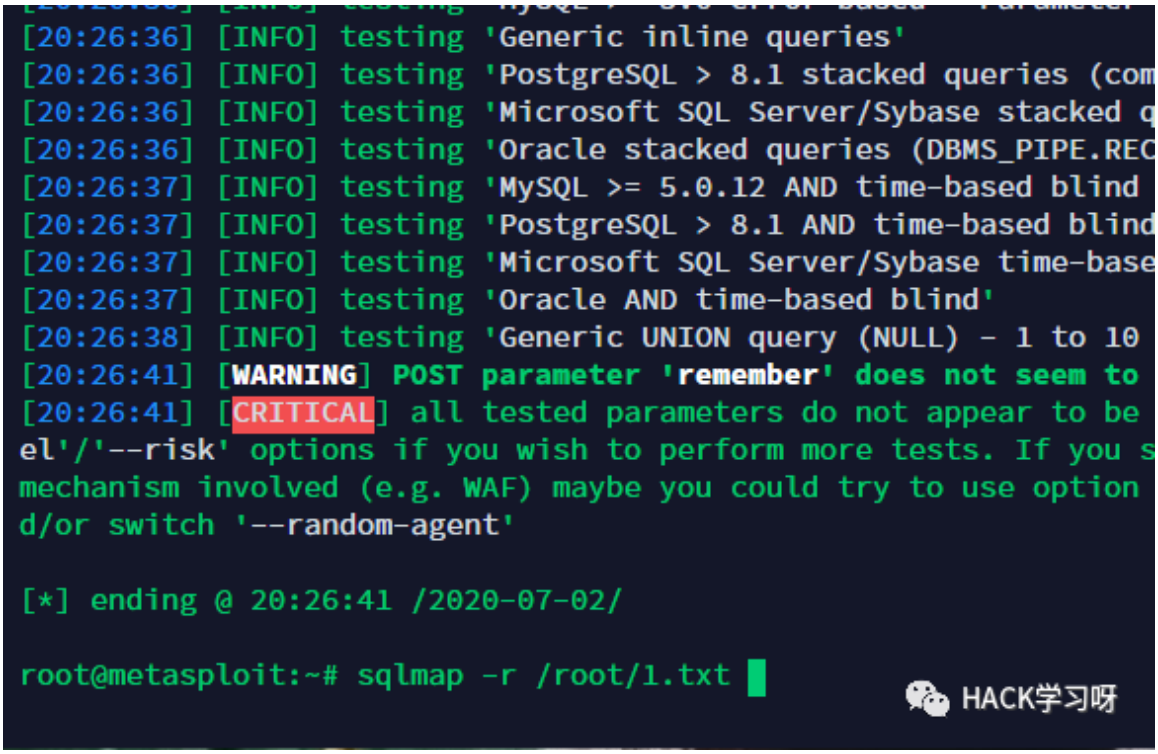
目前初步找出两个登陆界面，后台登陆是没有验证码的可进行爆破操作，但前提条件是知道商家的手机号，这里就先正常登陆我自己的用户瞧瞧里面有无可利用的地方，功能很简单并无可利用的地方头像处也无法进行编辑上传等操作该界面也只是提供显示话费的总额，我猜他们搭这样一个平台也只是显示个数字前几个月唬住消费者。

决定退出用户用burp抓个包分析分析传输的数据，输入正确的手机号验证码以及短信验证码开启抓包，可看到参数都是以明文传输的，验证码这些均与正确那我如果替换成别的用户是不是可以达到一个水平越权漏洞了呢，mobile处替换号码成功登陆别的用户斩获水平越权漏洞一枚。


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder
Intercept HTTP history WebSock
Request to 80
Forward Drop
Raw Params Headers Hex
POST
Host:
Content-Length: 166
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin
Content-Type: application/x-www-f
User-Agent: Mozilla/5.0 (Windows
Safari/537.36
Accept:
text/html,application/xhtml+xml,a
=b3;q=0.9
Referer:
Accept-Language: zh-CN,zh;q=0.9,e
Cookie: jeesite.session.id=4e8f3f
token=
Connection: close
loginFlag=1&redirect_url=
&mobile=13
validateCode=69gp&smsCo
de=844516&password=&btnSubmit=%E7%99%BB+++%E5%BD%95
4103.61
exchange;v
e/home
用户登录
不安全
min/f...
应用
奇安信网站云监测
大佬博客
其他书签
手机号
13
短信验证码
844516
验证成功
登 录
正在等待
...
HACK学习呀
0 matches

一样的个人中心一样的无任何利用的地方，转战后台登陆框框，像这类的后台二话不说直接使用burp抓个登陆的POST包在保存到本地txt文件使用sqlmap跑一跑说不定有意外的收获，因为是阿里云的服务器本地跑百分百的被拦截，所以我选择用与它相同的阿里云服务器去跑，username，password，remenbaer这三个均不存在注入。


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unl...
Burp Intruder Repeater Window Help
Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater Sequencer
Intercept HTTP hi
Request to http
Forward
Raw Params H
POST /admin/login
Host:
Content-Length: 41
Cache-Control: max
Upgrade-Insecure-R
Origin: http://
Content-Type: appl
User-Agent: Mozill
Gecko) Chrome/83.0
Accept:
text/html,applicat
pplication/signed-
Referer: http://
Accept-Language: z
Cookie: jeesite.se
JSESSIONID=A6C2CED
Connection: close
username=admin&password=admin&remember=on
登录
不安全
应用
奇安信网站云监测
大佬博客
其他书签
账号
admin
密码
记住密码
登录
正在等待
Type a search term
0 matches



没事，抓个包发个包看看响应回来的数据，可以看到账号的内容直接输出在了value的标签上。

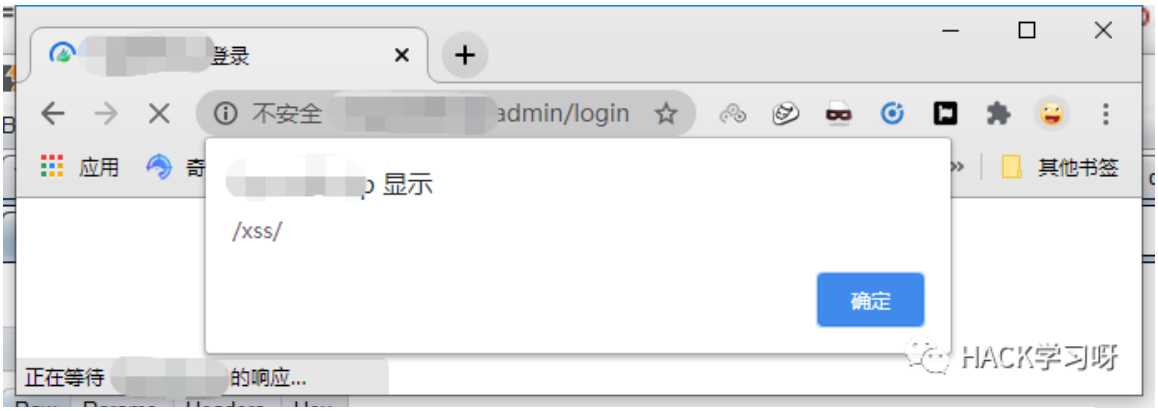
```
id="messageBox" class="alert alert-danger "><button data-dismiss="alert" class="close">×</
label id="label">用户或密码错误，请重试.</label>
>

label class="label">账号</label>
label class="input"> <i class="icon-append fa fa-user"></i>
       <input type="text" id="username" name="username" class="required" value="admin">
       <b class="tooltip tooltip-top-right"><i class="fa fa-user txt-color-teal"></i> 请输入
>
```


构造xss payload闭合插它！！”><script>alert(/xss/)</script>然后在重新发包斩获反射性xss一枚。

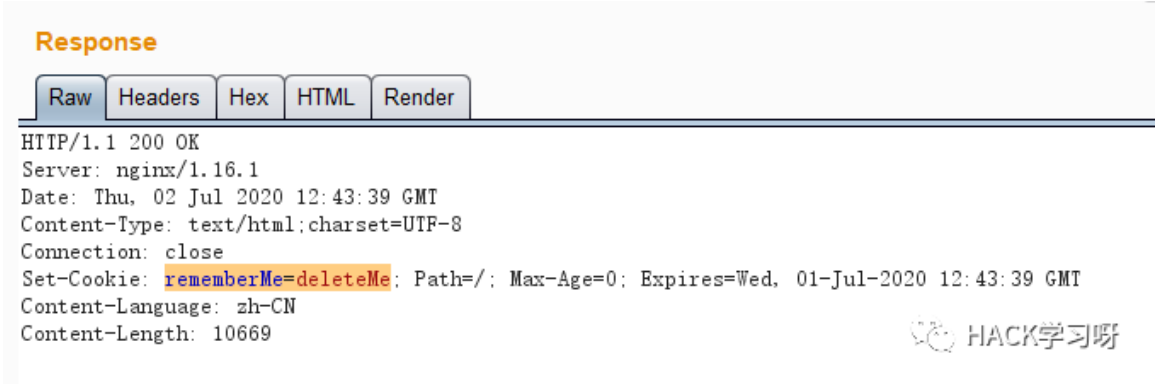
```
n>
 <label class="label">账号</label>
 <label class="input"> <i class="icon-append fa fa-user"></i>
        <input type="text" id="username" name="username" class="required" value=""><script>alert(/xss/)</script>">
        <b class="tooltip tooltip-top-right"><i class="fa fa-user txt-color-teal"></i> 请输入您的手机号</b></label>
on>

n>
 <label class="label">密码</label>
```

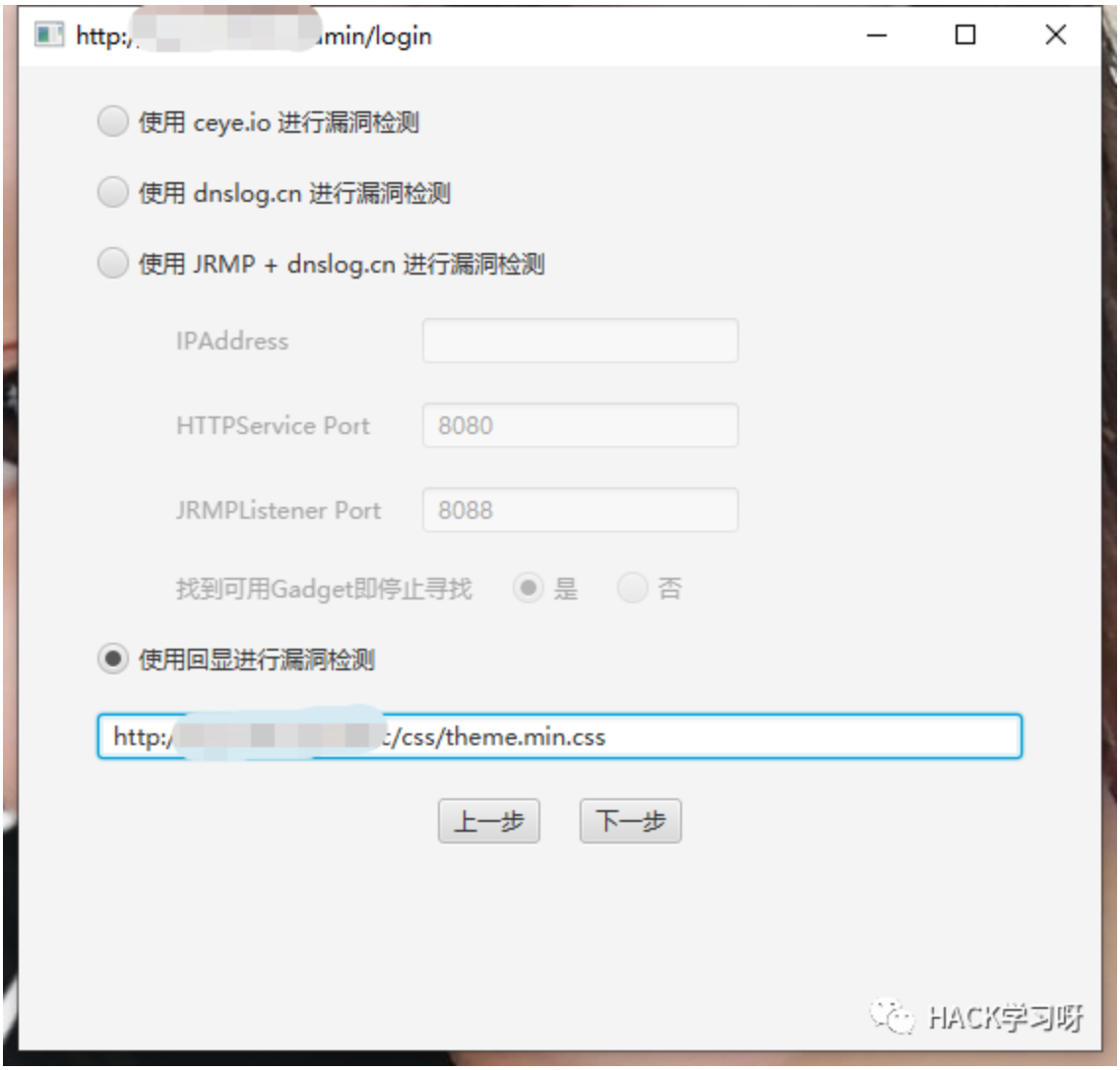


0X03 Getshell

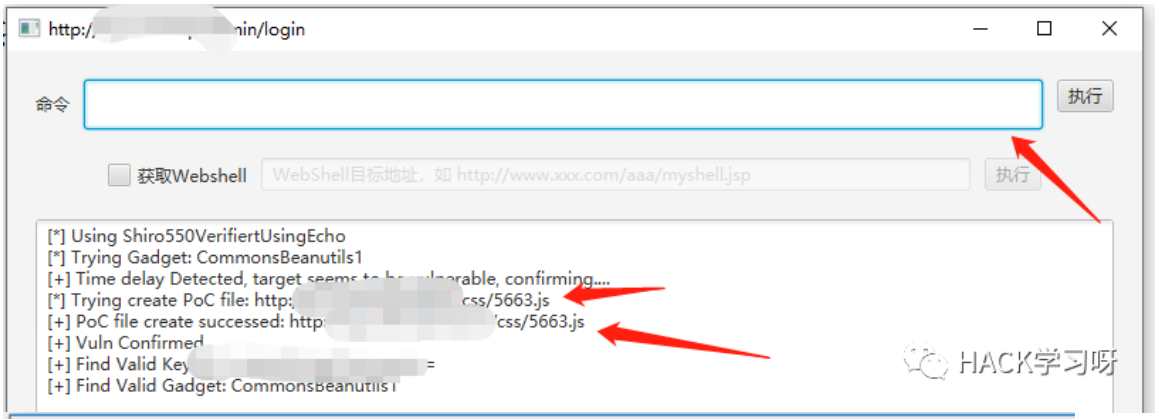
挖到的那个两个漏洞太鸡肋了，思路也暂时断了回过头再分析分析抓到的数据包，一直没太注意响应包仔细一看发现rememberMe=deleteMe字样，shiro反序列化漏洞呀。

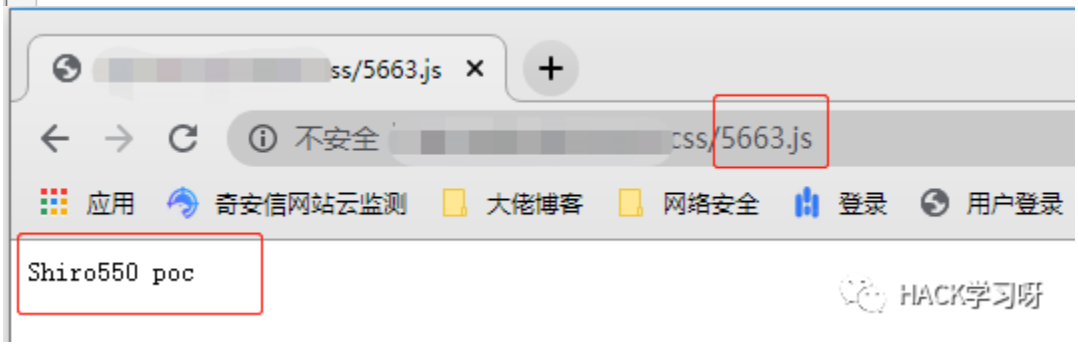


直接怼上exp，这里直接查看源代码取网站内的静态文件填入做检测。

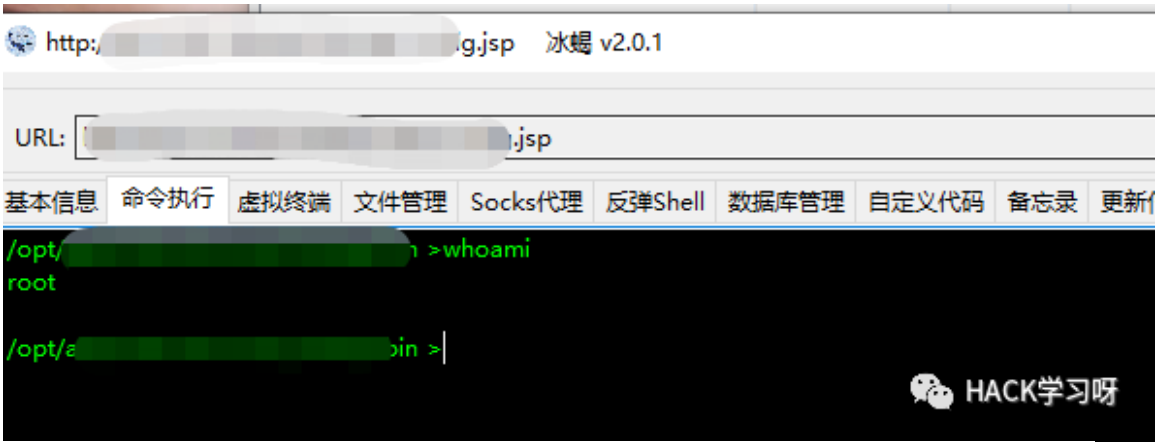


可看到命令执行框内是可输入的证明存在该漏洞相反不存在则不可输入，且在/css的同级目录下生成了5663.js的验证文件，访问测试是否成功写入文件。

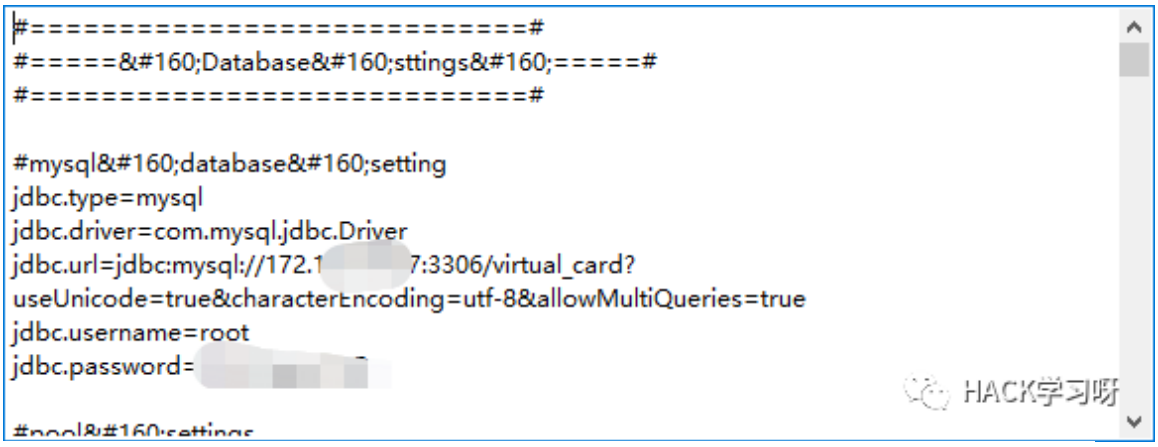




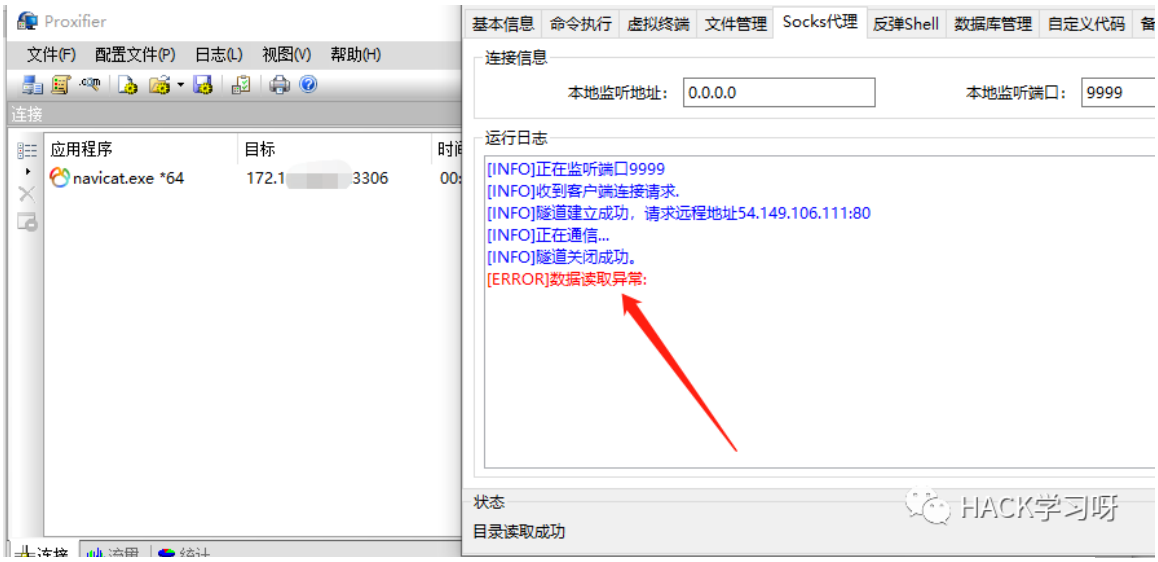
成功写入文件，接下来写入shell冰蝎连接执行whoami查看当前权限，Linux的环境直接root最高权限省去了需要提权的麻烦。



权限有了，并且服务器对外开放22端口可以直接写入公钥免密登陆，但考虑对方是阿里云的服务器异地登陆的话会有短信提醒动静太大所以没执行该方案，继续挖掘有用的信息，翻了半天翻到了个数据库的配置文件，数据库连接的地址是172.xx.xx.xx（各位师傅技艺高超内网地址也给码上防止爆菊）一看就知道是内网的ip站库分离啊，想办法代理转发出来连接瞧瞧。



冰蝎上有个Socks代理配合Proxifier在加上Navicat Premium数据程序管理进行隧道代理打入其内网数据库，常规的配置好Proxifier后添加程序进行连接，可问题来了反反复复试了好几次一点连接就直接数据异常，十有八九的被拦截了。



在内网代理这块踩了不少的坑总而言之还是自己经验不足，也有各位师傅指点使用adminer.php(这里手动@Uncia大佬)，adminer确实不错很轻量便捷只需上传web目录即可但奈何使处的环境是Java环境只支持jsp脚本adminer也只有php的脚本。

0X04　内网代理

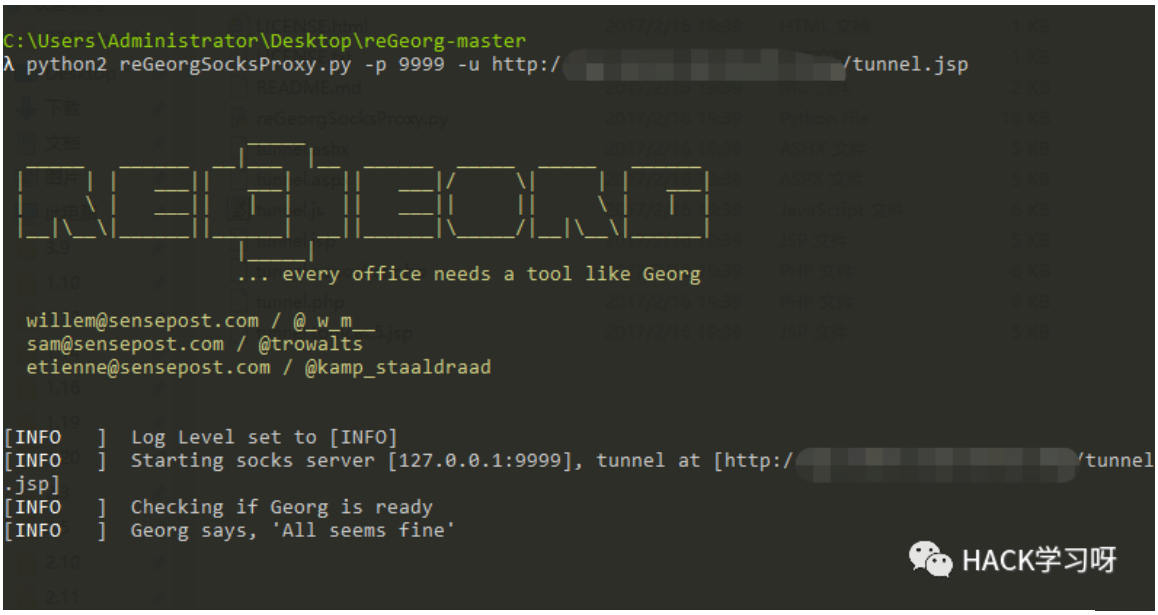
既然adminer不支持冰蝎也代理不出，那咱们就自己搭一条代理的隧道出来，在这里踩了不少的坑尝试利用reDuh和Tunna要么就是没流量要么就是连上一下子就断开，不知道是不是我的姿势不对还是受当前环境的限制，最终在GitHub上找到reGeorg神器。

reGeorg 可以说是 reDuh 的升级版，主要是把内网服务器的端口通过 http/https

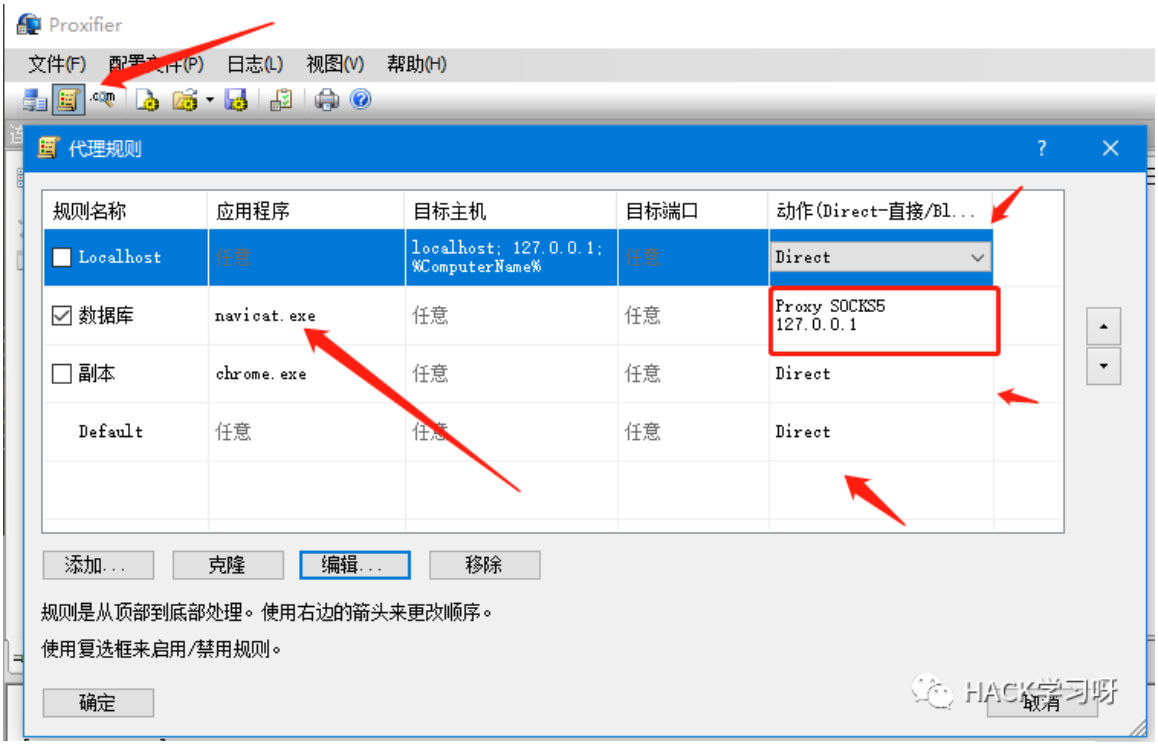
隧道转发到本机，形成一个回路，用于目标服务器在内网或做了端口策略的情况下连接目标服务器内部开放端口，它利用 webshell 建立一个 socks 代理进行内网穿透，因为当前环境是java所以我们上传.jsp的转发文件到网站目录下。

上传脚本后访问其脚本，显示Georg says, 'All seems fine',代理成功。

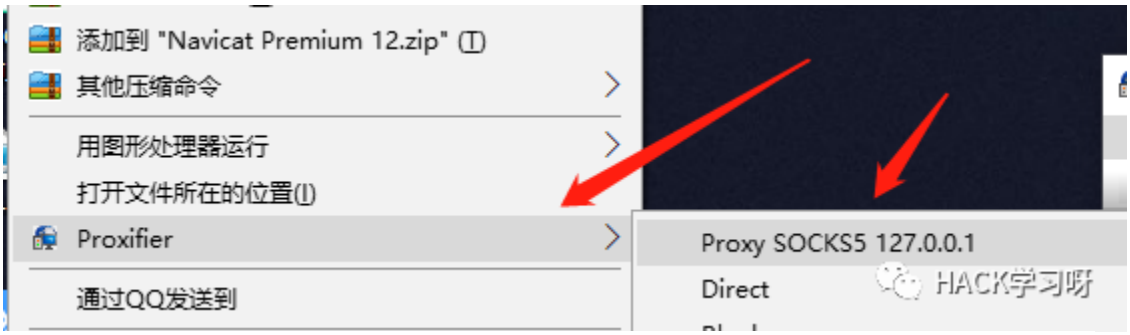
后在本地执行python2 reGeorgSocksProxy.py -p 9999 -u http://xx.xxxx.xx/tunnel.jsp在命令行界面同样显示Georg says, 'All seems fine'即可。



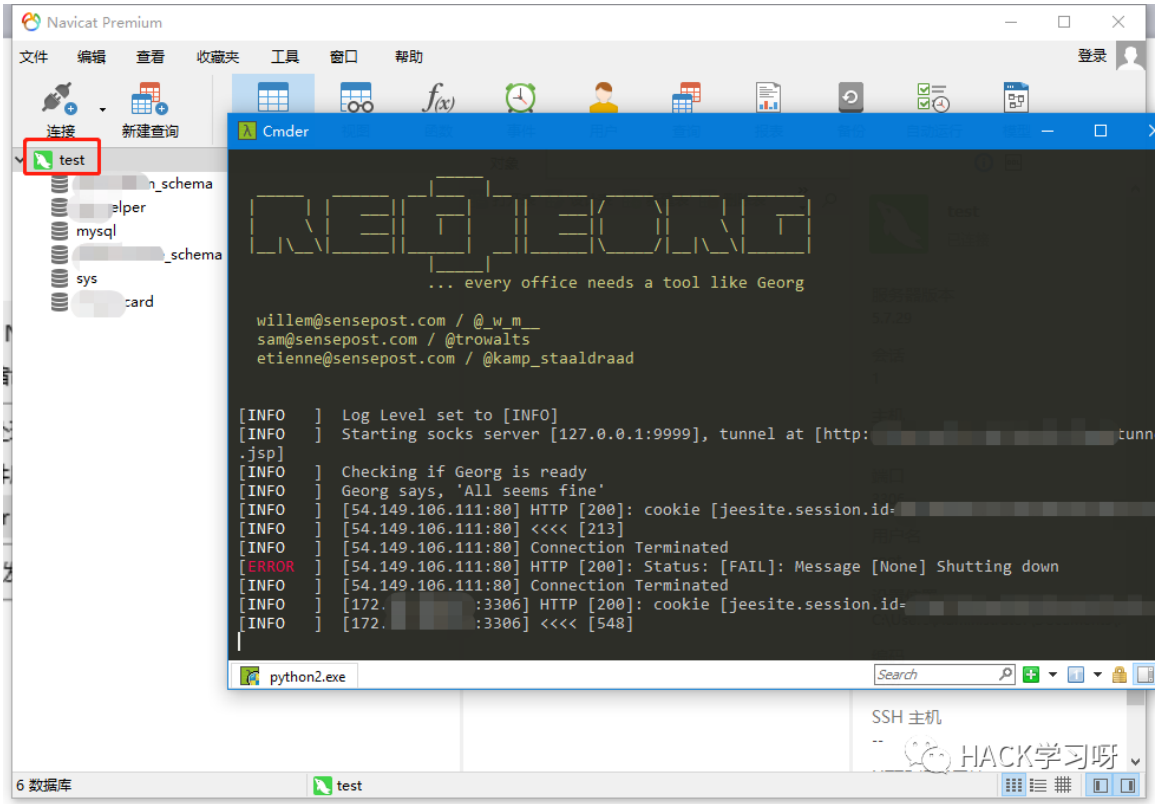
打开Proxifier基本配置好监听本地127.0.0.1的9999端口，然后设置代理规则添加Navicat程序，其他动作选择Direct关闭状态唯独只允许Navicat流量通过。



配置完后，右键Navicat以Proxifier本地代理模式打开。

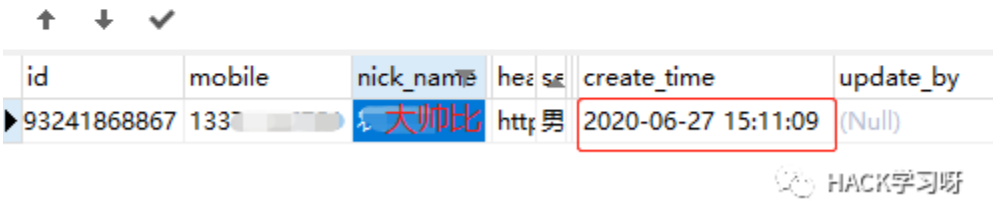


可以看到已稳定链接且Python窗口有流量传输（切记代理过程中请勿关闭窗口）。

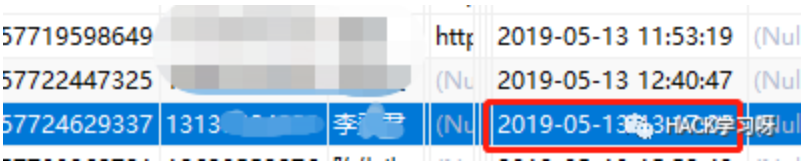


0X05　实锤骗局

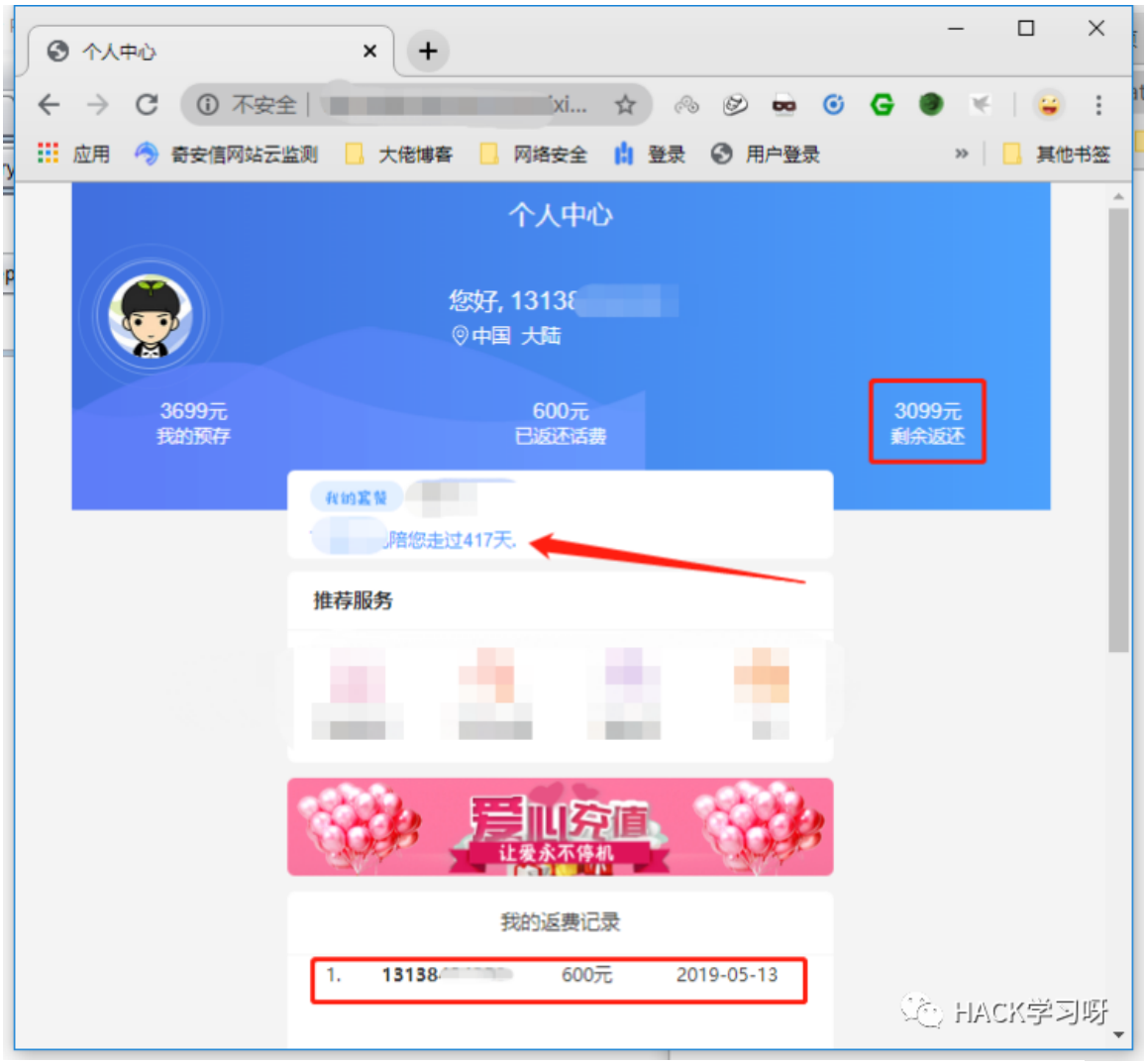
数据库咱也连上了，看看会员表里的账号，通过筛选member会员表里的name字段查找自己的名字，果不其然自己就躺在那里数据的时间跟被套路的时间相吻合。



如何实锤？很简单库里的第一批用户是2019年5月份的，到现在也相差一年了，这是不是骗局登录19年的账号看看返现记录就一幕了然，就随机抽取一位幸运玩家结合前面的水平越权漏洞登录其账号。



这都过去一年时间了果然也就只首次返现一次，前几个月唬住消费者过后又以各种理由的欺骗你，总之永远吃亏的还是消费者。



0X06　写到最后

至于为何写这篇文章，因为我也是受害者我想通过这样的方式去剖析它让大家更直观的了解这个局以免更多的人被套路，你去办理的时候他们会跟你说这是移动授权下来的活动（之前也是这么跟我说的），但这一路下来可以看出跟移动半毛钱关系没有，只不过是他们自主搭建的一个平台，里边的余额也只是唬

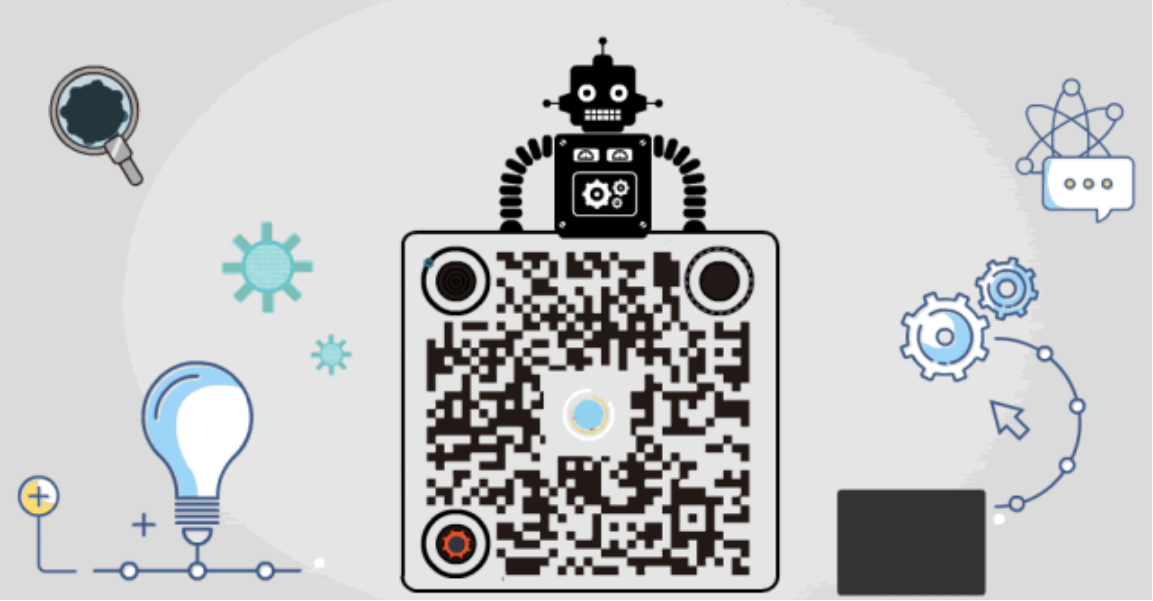
住你，有这么一个平台一个数字显示出来让你放心而已，至于首月到账的那几百块也只是从你那套的好几千手动给你充值给几百而已。

不说了，接下来的一年里我要吃土还花呗了嘤嘤嘤，商家登录系统那我估计还会有更多的猫腻，但渗透测试点到为止，我的目的就是证明这是不是一个骗局既然实锤了咱们也没必要在深入了。

我们所做的安全对抗，正如同没有硝烟的战争，战争的结果除了输赢之分，还有正义与非正义之别，唯一的区别就是我们要时刻站在正义的视角，探索了其漏洞原理，却不因此对其造成损害。

END

点赞，转发，在看



精选留言

用户设置不下载评论