

# 女主沉迷赌博输了一套房，程序员见义勇为端了

女主沉迷赌博输了一套房，程序员见义勇为端了澳门赌场

CSDN云计算

以下文章来源于Hack，作者武汉九歌



**Hack**

关注我带你了解网络深处的阴暗面



戳蓝字“[CSDN云计算](#)”关注我们哦！



作者 | 武汉九歌

责编 | 阿秃



大家好，我是九歌。

这天，我和往常一样，翻看着粉丝给我发的消息，有一条消息引起了我的留意，这位粉丝的老婆因为迷上了网赌，把买房的一百多万存款全部输干净了。

您能不能帮我

大佬你好，我的老婆在网上认识了一个人带她赌输了100多万，然后到处说可以找人入侵网站又被骗了2w多，现在实在是走投无路了才告诉我，那是我们买房的钱啊，现在全都被输光了还欠了二十多万

按往常来说，我是不会对这种赌博输钱给予帮助，但看他向我如此哭诉，并说不指望找回了那笔钱，只要这个网站不会再害其他人就行了。

唉，大佬，我也不指望您能帮我找回那笔钱，那您能不能不要再让这个网站运营下去了，我也不知道这个网站害了多少家庭，但是肯定不少

微信号: zhack6

我也就答应他试一试，我加了他的微信。

你好，我是九歌



您好！

请问您可以帮我吗

我不保证可以查的到，我只能尽力尝试一下



嗯嗯，谢谢您

微信号: zhack6

接着我让他描述了一遍起因经过（这个哥们也太惨了，我看着都有点于心不忍了...）

你描述一下吧，怎么被骗的，网站多少

我老婆在两个月前网上认识了一个人，然后慢慢的忽悠她去赌博，刚开始让我老婆赢了三万多，之后就慢慢的输，也不是全部都输，就是赌十次只能赢一两次

到最后钱全部都输完了就让我老婆去借贷

到最近我才知道我老婆已经把买房子的一百多万全都输干净了

现在真的想死了

微信号: zhack6

安慰了他让他不要自杀后找他要了这个网站的网址。

网信快3 1分钟1期  
 网信时时彩 1分钟1期  
 大发快3 1分钟1期  
 大发PK10 1分钟1期  
 大发六合彩 1分钟1期  
 5分PK10 5分钟1期  
 5分快3 5分钟1期  
 5分时时彩 5分钟1期  
 香港六合彩 一周三期  
 大发时时彩 1分钟1期

### 全民代理 火热招募

### 携手合作 共赢财富

《0投资》《0风险》《高回报》

实时返点 无条件随时提现

江苏快3

北京PK10

上海11选5

+ + = 7

当前期: 第 20190930041 期 开奖号码: 2,2,3 和值: 7 形态: 小 单

#### 昨日盈利榜

	账号昵称: xx***0	1
	昨日盈利: ¥1968283	
	账号昵称: 沃拉	2
	昨日盈利: ¥837496	
	账号昵称: 利多利空	3
	昨日盈利: ¥680047	

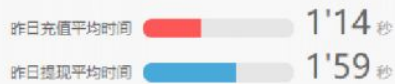
#### 中奖信息

	ah***m 在大发快3
	喜中 ¥5.91
	璀璨金星 在大发快3
	喜中 ¥1.97
	览胜在UU快3
	喜中 ¥35.46

#### 技术支持 Technical support



#### 服务体验 Service experience



#### 充值方式 Recharge method



[法律声明](#) | [关于我们](#) | [联系我们](#) | [商务合作](#) | [隐私声明](#)

Copyright © 网信彩票 Reserved | 18+

微信号: zhack6

研究了一下发现这个是彩票网站，彩种分别有重庆时时彩、北京赛车PK10、快3等以及一个私立的彩票，根据那位粉丝所说，他的老婆被人引导玩的自建的彩票，赌五块钱赢的话就会给她30，我推测，他的老婆刚开始玩的时候被提高了中奖率，到最后沉迷进去的时候慢慢的降低中奖率，但之后还是会让她偶尔赢一两次。

话不多说，我们直接开干，通过站长之家的Whois查询功能试了一下，注册人的信息已经全部被隐藏起来了，域名是在Godaddy注册的【GoDaddy是一家提供域名注册和互联网主机服务的美国公司】。

当前位置: [站长工具](#) > [Whois查询](#)

[whois查询](#)
[最新注册](#)
[邮箱反查](#)
[注册人反查](#)
[电话反查](#)
[域名批量反查](#)
[域名注册](#)
[历史查询](#)

域名  的信息

以下信息更新时间: 2019-10-03 09:12:57 [立即更新](#)

[获取API](#)

域名	<input type="text"/> <a href="#">[whois反查]</a>	<a href="#">申请删除隐私</a>
注册商	GoDaddy.com, LLC	
联系邮箱	abuse@godaddy.com <a href="#">[whois反查]</a>	



联系电话	*****42505 [whois反查]
创建时间	2019年05月14日
过期时间	2020年05月14日
域名服务器	whois.godaddy.com
DNS	NS1.DNS.COM NS2.DNS.COM

-----站长之家 Whois查询-----

微信号: zhack6

接着我又用站长之家的Ping功能查询了一下有没有加CDN。

如下图可知，所有的节点Ping此网站的返回值全部都是一个IP，可以推测出来并没有添加CDN，并且识别出了这个网站搭建在阿里云的香港服务器上（这个站长的胆子也太大了）。



我考虑到赌博网站会频繁更替域名，于是我通过同IP网站查询的功能进行搜索。

<div> <input type="text"/> <input type="button" value="查询"/> <input type="button" value="查询记录"/> </div>		
IP地址: 47.179 [香港 阿里云]		
序号	域名	标题
221	sc. .pm	--
222	s. .cc	--
223	s. .cc	--
224	sc. .pm	--
225	8. .n	--
226	sc. .pm	--
227	s. .cc	--
228	8. .n	--
229	8. .n	--
230	sc. .pm	--
231	5. .n	--
232	sc. .pm	--
233	8. .n	--
234	8. .n	--
235	xn--eh. .jsj.com	--
236	sc. .pm	--
237	8. .n	--

微信号: zhack6

不出所料，我们查询到了在此台香港阿里云的服务器上有着237个站点，并且用的网站模板全部都是同一个，估计是想大面积撒网

我在其中的一个网站里面看到了这个站长留下的QQ，我尝试着加他，发现是一个专门的客服QQ



昵称 网信客服专员 (仅此一个)

备注 添加

分组 我的好友

女 19岁 8月8日(公历) 狮子座 属龙

年SVIP3

最新说说: 请注意: 我们绝对不会跟任何一位会员要...

Q龄 0年

血型 AB型

职业 模特



网信客服专员

请注意：我们绝对不会跟任何...

发消息

个人说明

请注意：我们绝对不会跟任何一位会员要money，只会处理问题，且我们平台没有任何线下的支付方式哦~~

备注信息 添加


微信号: zhack6

我给他发送消息并没有理我，我去到他的空间进行痕迹的查找。

<

2019年09月

Q



网信客服专员（仅此一个）


09月29日10:34


QQ客服绝对不会跟任何一位会员要钱财，请注意不要上当受骗，QQ客服只会处理问题，且我们平台没有任何线下的充值方式哦~~

浏览51次

y、故作坚强

评论





网信客服专员（仅此一个）

09月21日21:52

在线时间：早上10点-22点

浏览62次



👍 扯淡的青春、  y

评论



网信客服专员（仅此一个）

09月18日16:06

九月VIP活动已经开启一半了哦~~充值就



微信号: zhack6

我发现他的空间的说说每一条都被一个昵称为y的QQ点赞过，并且这些说说的时间跨度很大，我推测这有可能是他的小号。我为了检测具体是不是同一个人，我用手机访问他的QQ空间进行添加好友的操作，获取到他的QQ。

取消

添加好友

发送



15 [REDACTED] 3

男 2岁

填写验证信息

我是九歌



## 设置备注和分组

备注

分组

我的好友



不让他看我的动态



微信号: zhack6

我利用QQ的忘记密码功能，查询了一下这两个QQ绑定的手机号，开头全部都是188的号段。

请用密保手机188\*\*\*\*\*发送一条短信

已换号?

编辑短信内容：

CZ7295

发送到：

1069070069

我已发送

短信用不了？[更换其他验证方式](#)

 微信号: zhack6

但这并不能成为确凿的证明，我接着利用贴吧的高级搜索功能查询到网名为y的QQ号留了  
赌博网站客服的Qq，已经确定了是一个人了。



qq3[REDACTED]8

q1[REDACTED]3



初来乍到



 微信号: zhack6

现在缩小了目标范围，我们开始对此QQ进行调查。

我到社工库里面尝试了一下能不能查询到这个QQ的老密。



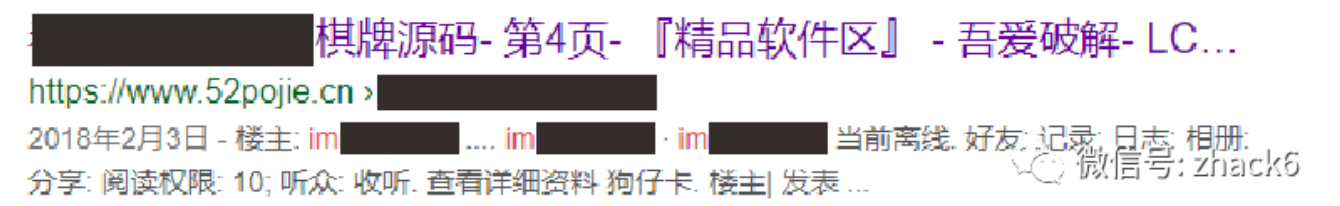
还真的让我查到了有用的信息！但是查到的密码用MD5进行加密了，我们到MD5的解密网站去进行解密。



查询到的密码是五个英文字母+123456，我尝试了一下登陆，可惜早已改了密码，我推测密码前的五位数字是他的常用ID【很多人都喜欢把自己的ID/姓名/手机号放到自己的密码里面】。

百度查询到的信息太少了，我们打开万能的谷歌搜索他的ID。

谷歌不负众望，我查询到了他在吾爱破解的账户。



用户名是他的ID+他QQ的前三位数字，他在这个帖子里面留下了另一个QQ。



这个QQ 里的空间全部都是些感叹，生活的吐槽之类的话，应该就是他的生活号了，我先申请添加他的好友，接着我继续在谷歌上搜索。

我在他的腾讯微博里面搜索到了一串18位数字。



4

2015年3月15日 12:57 全部转博和评论(1)

微信号: zhack6  
转博 | 评论 | 收藏

18位数字，格式和身份证号一模一样，我推测这是他的身份证号。

我接着用他的QQ邮箱尝试能不能搜索出支付宝。





¥

添加

请补全对方姓名，确保资金安全



取消

确定

微信号: zhack6

我利用支付宝转账功能的姓名验证获取到了他的全名，拿到了姓名和身份证号。

现在有一个黑科技就是只需要身份证号+姓名就可以查询出身份证上的照片，我们使用这个黑科技已经拿到了此人的身份证照片。

个查询接口查出了此人的身份证照片。

API调试工具

身份证验证返照片    身份证验证

POST

发送

Header 参数	值
-----------	---

+ 添加

Body 参数	值	说明
idcard		* 身份证号码
realname		* 真实姓名

+ 添加

请求链接

复制

返回 Header	返回 Body
<div></div> <div>微信号: zhack6</div>	

现在我们已经有了对方的如下信息：

姓名：王

使用的QQ：13, 11

支付宝账户：1@qq.com

身份证号：47

身份证照片：有

微信号: zhack6

现在我们要查询他的手机号码，我在搜索引擎并没有查询到关于手机号的信息，我尝试着用Telegram的社工库查询接口对他的生活进行查询。



查询到了两条老密，其中一条是一串和手机号格式一样的11位数字。  
我为了验证此手机号是否还在使用，我利用QQ的忘记密码功能验证了一番。

<

短信验证

为保护您的帐号安全，请您输入完整的密保手机号码180\*\*\*\*\*:

+86

请输入密保手机号码

下一步

短信用不了？请更换其他验证方式

 微信号: zhack6

现在我们又突破了一个点，获取到了他的手机号！  
我们通过他的生活QQ进行域名Whois反查。

whois查询最新注册邮箱反查注册人反查电话反查域名批量反查域名注册历史查询全球域名后缀

自定义时间

①

@qq.com

查看分析

查询记录

序号	域名	注册者	电话	注册商	DNS	注册时间	过期时间	更新
1	fu.com		--	阿里云技术有限公司 (万网)	dns13.hichina.com dns14.hichina.com	2019-06-16	2020-06-16	

微信号: zhack6

打开这个网站发现是一个美腿网站....里面还包含了这个人自己拍摄的照片。





因为他上传的都是高清图，所以我发现他自己拍摄的照片全都包含了经纬度的信息，我通过MagicEXIF定位到了他的家庭地址【涉及隐私往死里打马】。

MagicEXIF 元数据编辑器 v1.08 (未注册) - 11.jpg

文件(F) 编辑(E) 查看(V) 图像(I) 工具(T) 帮助(H)

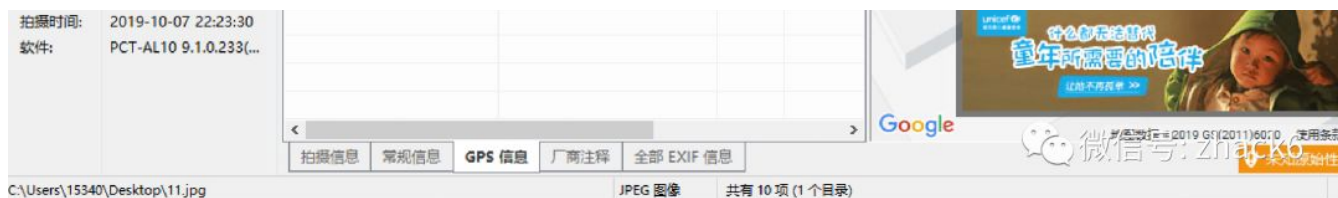
新建 打开 保存 另存为 导入 导出 编辑项 添加项 删除项 JPEG段 原图重构 编辑向导 批处理 查找 注册产品

11.jpg  
JPEG 图像

文件大小: 14.54 MB  
图像大小: 8000 × 6000 像素  
位深度: 24 位  
压缩指纹: 9110367B (Unknown)  
字节序: Motorola (大端字节序)  
创建时间: 2019-10-06 20:08:08  
最后修改: 2019-10-07 22:23:46

项目	值	标签号	标签名
GPS信息 (GPS Info IFD)			
GPS 版本	Ver. 2.2	0000	GPSVersio
GPS 纬度参考	北纬 (N)	0001	GPSLatitud
GPS 纬度		0002	GPSLatitud
GPS 经度参考	东经 (E)	0003	GPSLongit
GPS 经度		0004	GPSLongit
GPS 高度参考	海平面以下	0005	GPSAltitud
GPS 高度	0m	0006	GPSAltitud
GPS 时间戳		0007	GPSTimeSt
GPS 定位方法		001B	GPSProces
GPS 日期戳		001D	GPSDateSt

X 移除广告

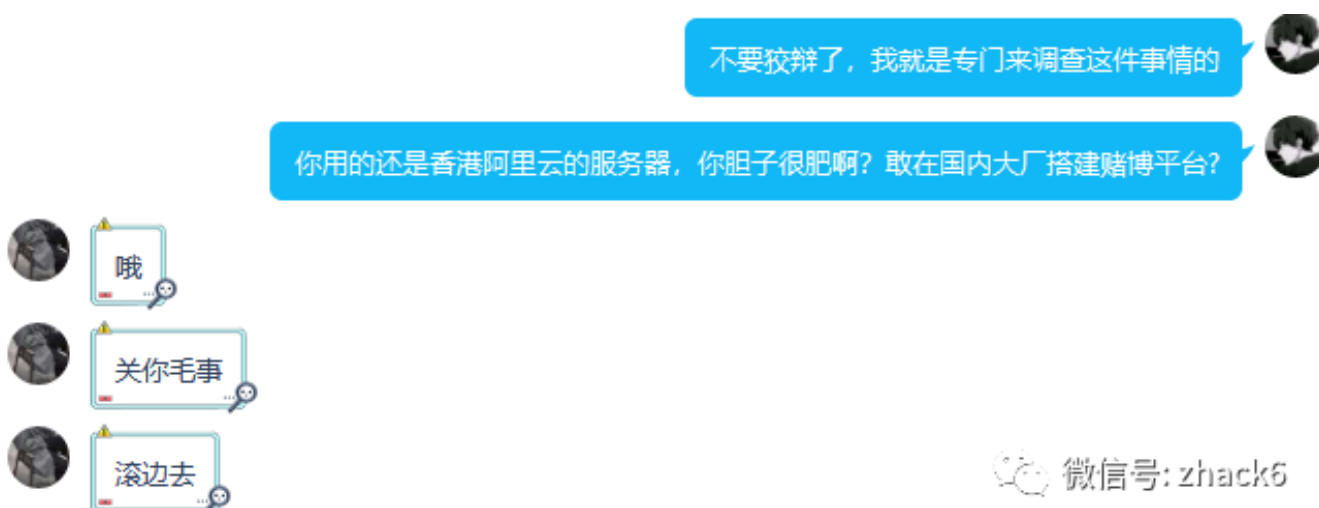


到这个时候我已经有了他的所有信息了，我现在来找他谈判。

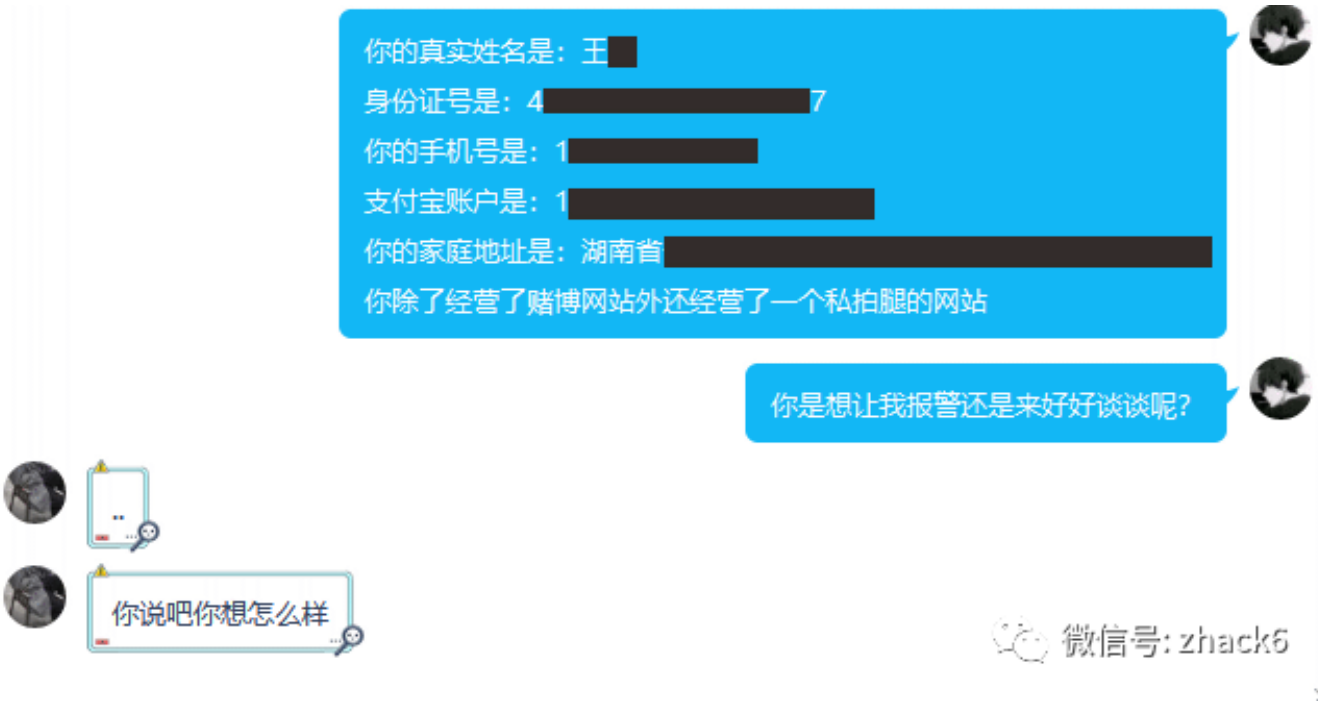
他的生活号已经同意了我的QQ好友申请。



他竟然死活不承认，敢做不敢当，真令人轻视了几分。



撕破脸皮厚就直接开骂了，我知道我已经占了上风，心理学里面有研究表示人通常会用无休止的谩骂来掩饰他们内心的恐惧。



我直接把他的个人资料发送给他了，瞬间安分下来了。



让他闭站的同时我也没忘记了我的初衷，能把钱要回来还是帮帮他们吧。





看到他们这么快服软松了一口气，就怕他们死鸭子嘴硬。

我找那位读者要了他的银行卡账号，让这位站长将钱转给了他。

并且监督这个人将所有赌博网站给关闭了，那个私拍网站因为没有过度暴露，全部都是腿照，我也没有逼得太紧就没管了。

最后，你当我有这么好心的放他一马吗？



# 报警电话

## 1 110

微信号: zhack6





