请不要在我喜欢的人身上下手，我“刀”呢？

原创 队员编号047 酒仙桥六号部队
2020-07-27原文

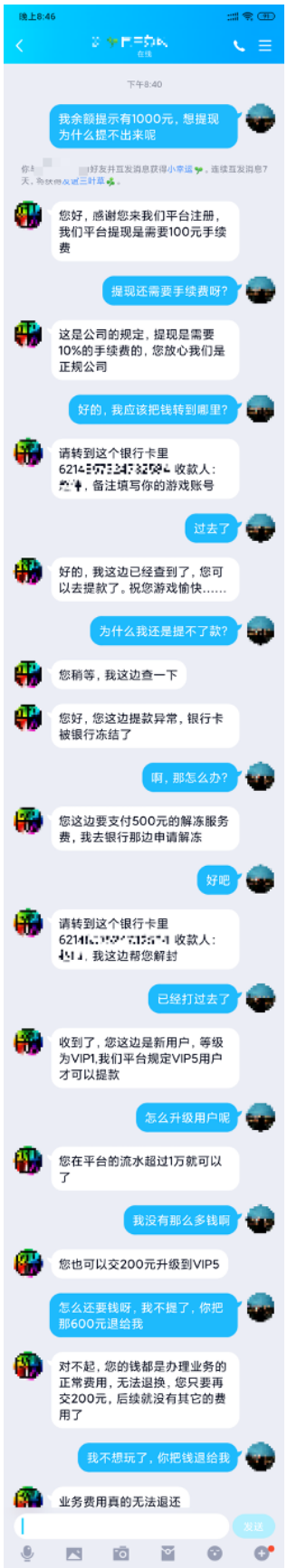
这是 **酒仙桥六号部队** 的第 **47** 篇文章。
全文共计3021个字，预计阅读时长10分钟。

1.背景

昨天一个漂亮的高中同学突然叫我，说被别人骗了钱，让我帮帮忙，美女的忙，充满正义感的我向来是不会推脱的。（另外我还是有点喜欢她，虽然是上学时期的事了，但现在印象还是很好地。要是通过这次帮忙，对我的印象有了极大的提高，成就一段美满的爱情，又何尝不是一段佳话……）

通过了解，我同学以前就有打麻将、打牌的爱好，每逢过节回家，都和邻家小妹在一起玩。由于疫情期间，同学无法正常上班，在家无聊就和邻家小妹在一起长达3个多月的娱乐，为了增加娱乐性，偶尔的还会有金钱上的“付出”，也不是很多，5毛、1块，多的时候5块、10块的。每天熬夜到清晨（友情提示，长时间熬夜对身体不好哦）。期间输了不少钱，由于邻家小妹的复工，缺少打牌的伙伴。我同学在QQ群里看到了玩游戏还能赚钱，就动了心思。进入游戏提示余额1000元，同学一时眼红，最近输了这么多钱，想着尽快提现。于是就开启了这次误入“博彩”的事件。

要出了同学和博彩客服的对话，看一看同学是怎么一步一步掉入陷阱的……

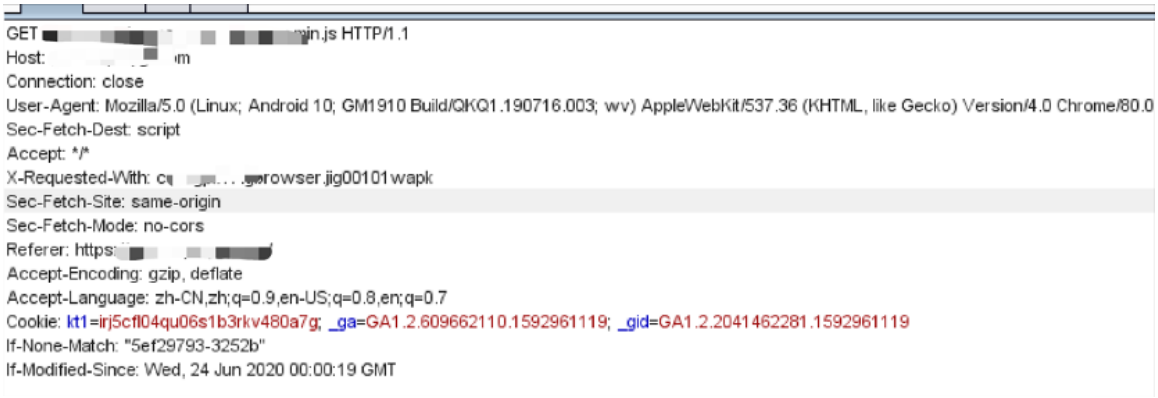

晚上8:46
在线
下午8:40
我余额提示有1000元，想提现为什么提不出来呢
你好，感谢您来我们平台注册，我们平台提现是需要100元手续费
提现还需要手续费呀?
这是公司的规定，提现是需要10%的手续费的，您放心我们是正规公司
好的，我应该把钱转到哪里?
请转到这个银行卡里 收款人：，备注填写你的游戏账号
过去了
好的，我这边已经查到了，您可以去提款了。祝您游戏愉快……
为什么我还是提不了款?
您稍等，我这边查一下
您好，您这边提款异常，银行卡被银行冻结了
啊，那怎么办?
您这边要支付500元的解冻服务费，我去银行那边申请解冻
好吧
请转到这个银行卡里 收款人：，我这边帮您解封
已经打过去了
收到了，您这边是新用户，等级为VIP1,我们平台规定VIP5用户才可以提款
怎么升级用户呢
您在平台的流水超过1万就可以了
我没有那么多钱啊
您也可以交200元升级到VIP5
怎么还要钱呀，我不提了，你把那600元退给我
对不起，您的钱都是办理业务的正常费用，无法退换，您只要再交200元，后续就没有其它的费用了
我不想玩了，你把钱退给我
业务费用真的无法退还
发送

身为发哥头号影迷的我，在看完《赌神》中发哥的高超千术真是惊叹不已，现实中赌场也不缺这种千术高手，真的是十赌九输，任人宰割。那么线上赌博的背后又有什么秘密呢！今天就带大家探索一下。

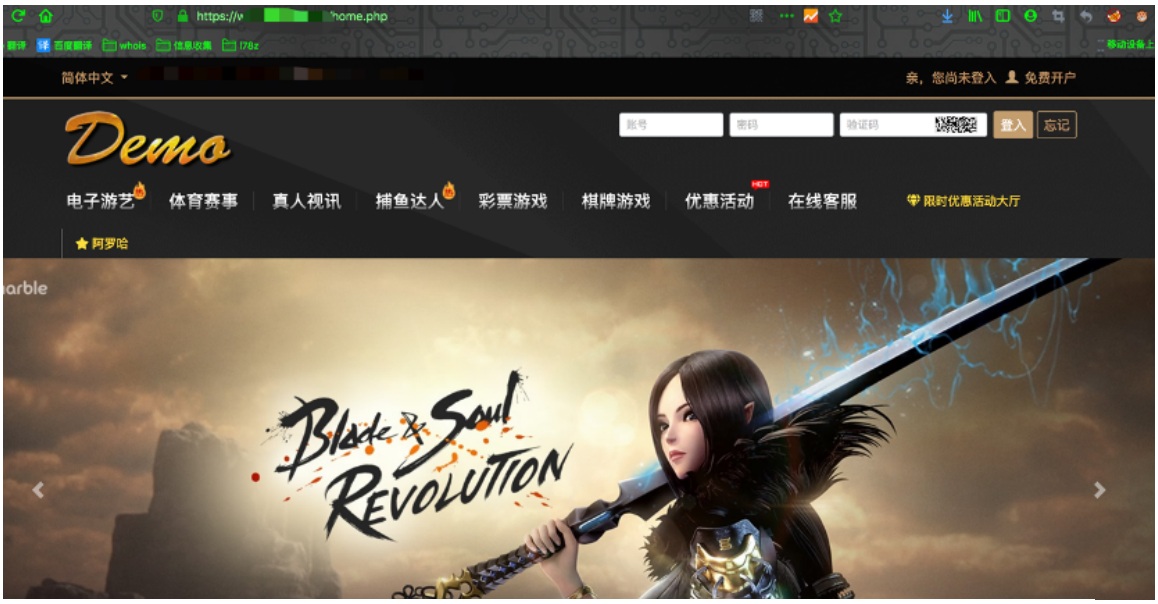
2.为爱而“站”之旁搜博采

通过同学提供的网站，下载app后发现是一个博彩网站app。

我们下载一个app实例分析一下，通过抓包分析看到一个url地址。该URL地址还采用了MD5+base64加密双层加密，通过解码后还原了真实的通讯地址。



我们打开url地址发现是一个web端网站，通过观察发现app内的功能与web端功能一致，为了测试方便我们从web端入手。



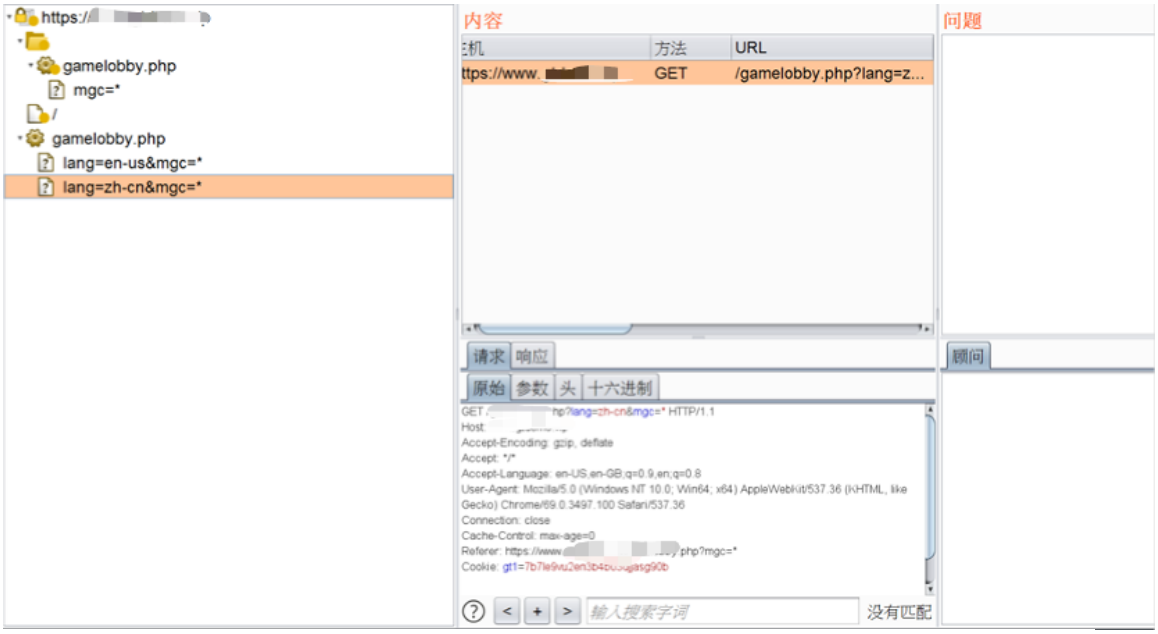
对网站进行初步信息收集，网站ip为日本ip，使用了Nginx中间件，php语言开发。

该网站使用了CDN，尝试使用扫描子域名、svn信息泄露、DNS历史记录、github信息泄露并借助在线工具等，均未能查到真实ip。

IDC服务商大全　　更多日本IDC公司

品牌	业务类型	运营商	iP规则
腾达互联	动态ipVPS	Softbank,Docomo,AU	动态
腾达互联	CDN	Softbank,Docomo,AU	共享
腾达互联	高防	Softbank,Docomo,AU	独享
腾达互联	大带宽	电信cn2,联通cn2,移动cn2,T-Mobile,Verizon,Sprint,Cogent	独享
腾达互联	云主机	电信cn2,Softbank,Docomo	静态

我们用burpsuite爬取一下目录信息，获取到的信息少的可怜。



用dirsearch、御剑、dirmap等工具进行目录扫描一波，看一看有没有网站备份文件，数据库文件。结果备受打击，依旧一无所获，管理员是处女座嘛?一点多余的东西都不留，可怕……

```
[17:31:33] 403 -    2KB - /.htaccess_sc
[17:31:33] 403 -    2KB - /.htgroup
[17:31:33] 403 -    2KB - /.htaccessBAK
[17:31:33] 403 -    2KB - /.htaccessOLD2
[17:31:33] 403 -    2KB - /.htaccess~
[17:31:33] 403 -    2KB - /.htaccessOLD
[17:31:34] 403 -    2KB - /.htpasswd-old
[17:31:34] 403 -    2KB - /.htpasswds
[17:31:34] 403 -    2KB - /.htusers
[17:31:34] 403 -    2KB - /.htpasswd_test
[17:31:44] 403 -    2KB - /admin/.htaccess
[17:31:52] 403 -    2KB - /administrator/.htaccess
[17:31:55] 403 -    2KB - /app/.htaccess
[17:31:56] 200 -  465B  - /app.php
[17:32:00] 301 -  169B  - /cache  →  http://www      .vip/cache/
[17:32:04] 200 -    1B  - /config.php
[17:32:06] 301 -  162B  - /css  →  https://www.      /ip/css/
[17:32:09] 301 -  169B  - /error  →  http://www      .vip/error/
[17:32:10] 403 -    2KB - /error/
[17:32:11] 200 -    1KB - /favicon.ico
[17:32:15] 200 -   35KB - /home.php
[17:32:16] 301 -  169B  - /icons  →  http://www      .vip/icons/
[17:32:17] 301 -  162B  - /img  →  https://www      /ip/img/
[17:32:17] 301 -  169B  - /in  →  http://www.g      p/in/
[17:32:18] 200 -   35KB - /index.php
[17:32:34] 200 -   21KB - /member.php
[17:32:43] 200 -   44B  - /robots.txt
[17:32:46] 200 -   26KB - /register.php
[17:32:46] 301 -  169B  - /setup  →  http://www      /.vip/setup/
[17:32:48] 200 -    0B  - /sitemap.xml
[17:32:55] 301 -  169B  - /ui  →  http://www      .vip/ui/
[17:32:55] 403 -    2KB - /ui/
[17:32:57] 200 -   33B  - /version.txt
```

通过浏览网站，发现该网站主要存在三个有价值的页面。

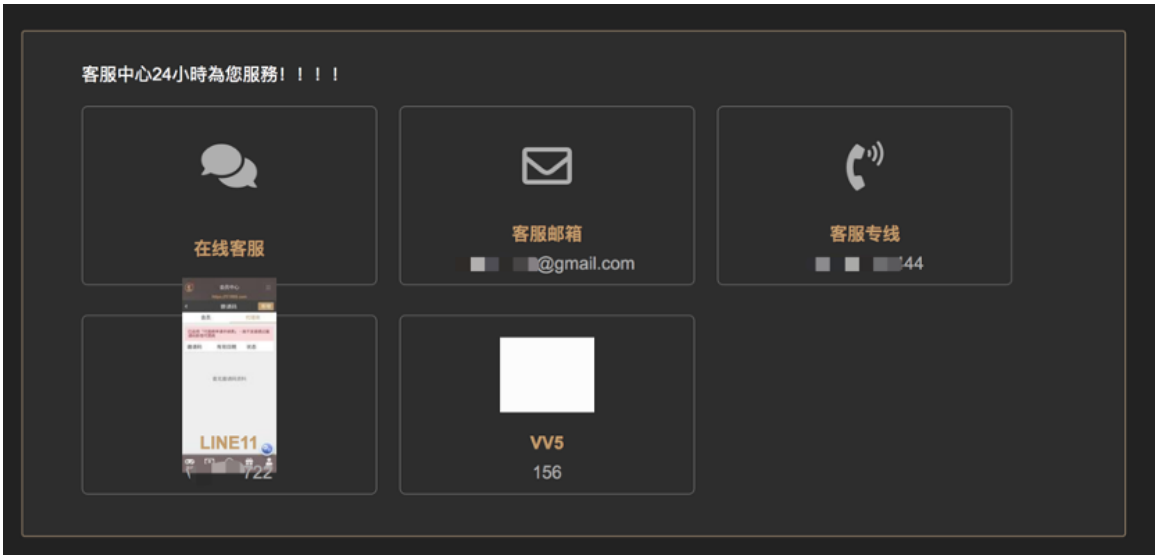
register.php　注册页面

login2page.php 登录页面

contactus.php　客服页面

使用万能密码、sql注入、存储xss等漏洞检测登录页面和注册页面未发现漏洞。

在客服页面发现一个邮箱账号，对该邮箱账号进行google、github搜索未收集到更多信息，不开森……与客服小妹的距离又远了一步。



既然不能旁敲侧击，那我们就正面开战。进行用户名爆破，通过抓包发现密码进行SHA1加密，连夜赶制python脚本爆破程序，配合burpsuite进行爆破。

通过近半小时的爆破，果然没让我失望，“没爆出来”……

既然爆破不出账户，那我们就注册一个账户，通过近三天的等待，我们注册的账户还在审核状态，管理员对我们有脾气呀，还是火眼金睛看破了我们的诡计。可怕……

由于网站访问较慢，暂停使用扫描器，弄挂掉可就没得玩了，使用简单的手工进行尝试漏洞挖掘，手工测试一下php常见路径，看看有什么收获。

/phpinfo.php

/robots.txt

/admin.php

/admin/login.php

/admin/index.php

/test.php

/admin_admin.php

/admin_config.php

/config.php

/install.php

/upfile.php

/upload.php

/admin_user.php

/phpMyAdmin/

/Upload/

/admin/

/DataBackup/

/User/

/WebAdmin/

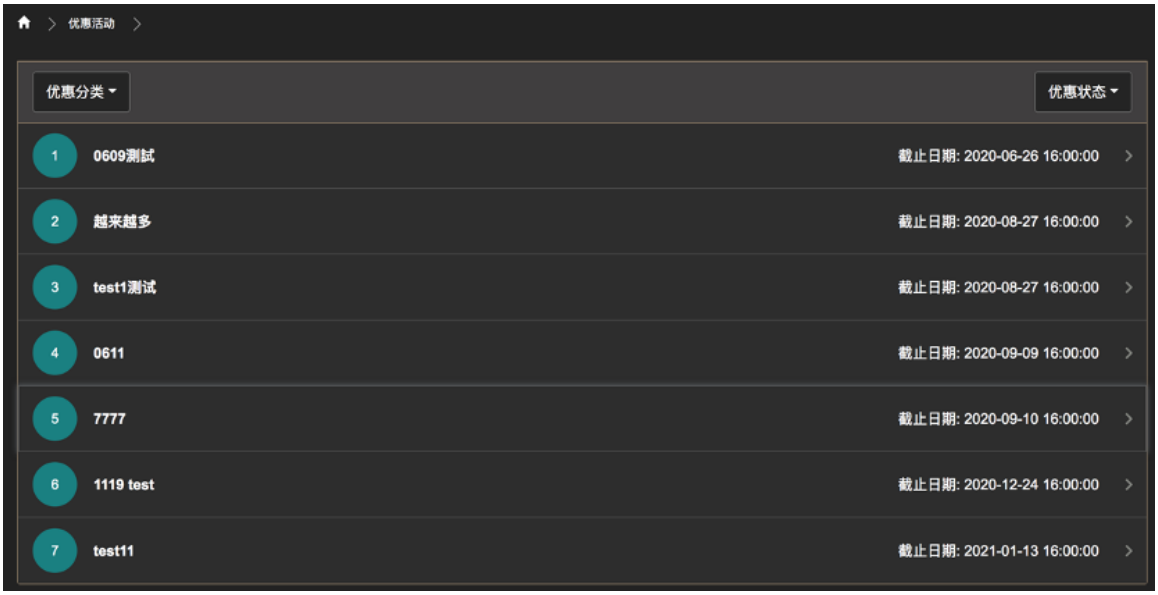
/config/

/test/

……

通过以上测试均无跨越性收获。通过查看页面版权信息、查看页面源代码等手段发现是类似的CMS，特征与：phpcms、dedecms、echshop等CMS有相近之处。但是！经过已有漏洞的排查和其它情况的发现，该CMS可能存在了二次开发或修改的情况，高权限漏洞均无法复现。竟不知是哪位高人门下调教出如此优秀的“程序猿”这难道就是传说中的绝世高手吗。 一筹莫展之际，发现漂浮的地址为“test”是5月13日的。

继续查看“优惠公告”发现服务器时间是错乱的，并且还有很多测试类的信息。

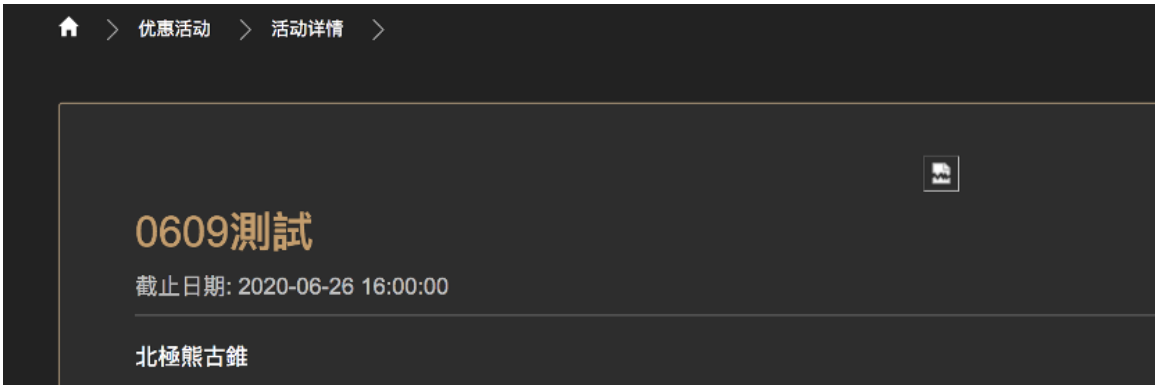


根据个人经验推测，2个可能性。

可能性一：已被攻击者拿下，并在后台尝试了下该功能。（有前辈造访）

可能性二：网站运营者初步搭建好没多久的站点，测试功能。

从单条测试的内容来看，有点像攻击者拿到了账号进入后台后，尝试了图片上传漏洞。



于是好奇，复制了该图片地址。

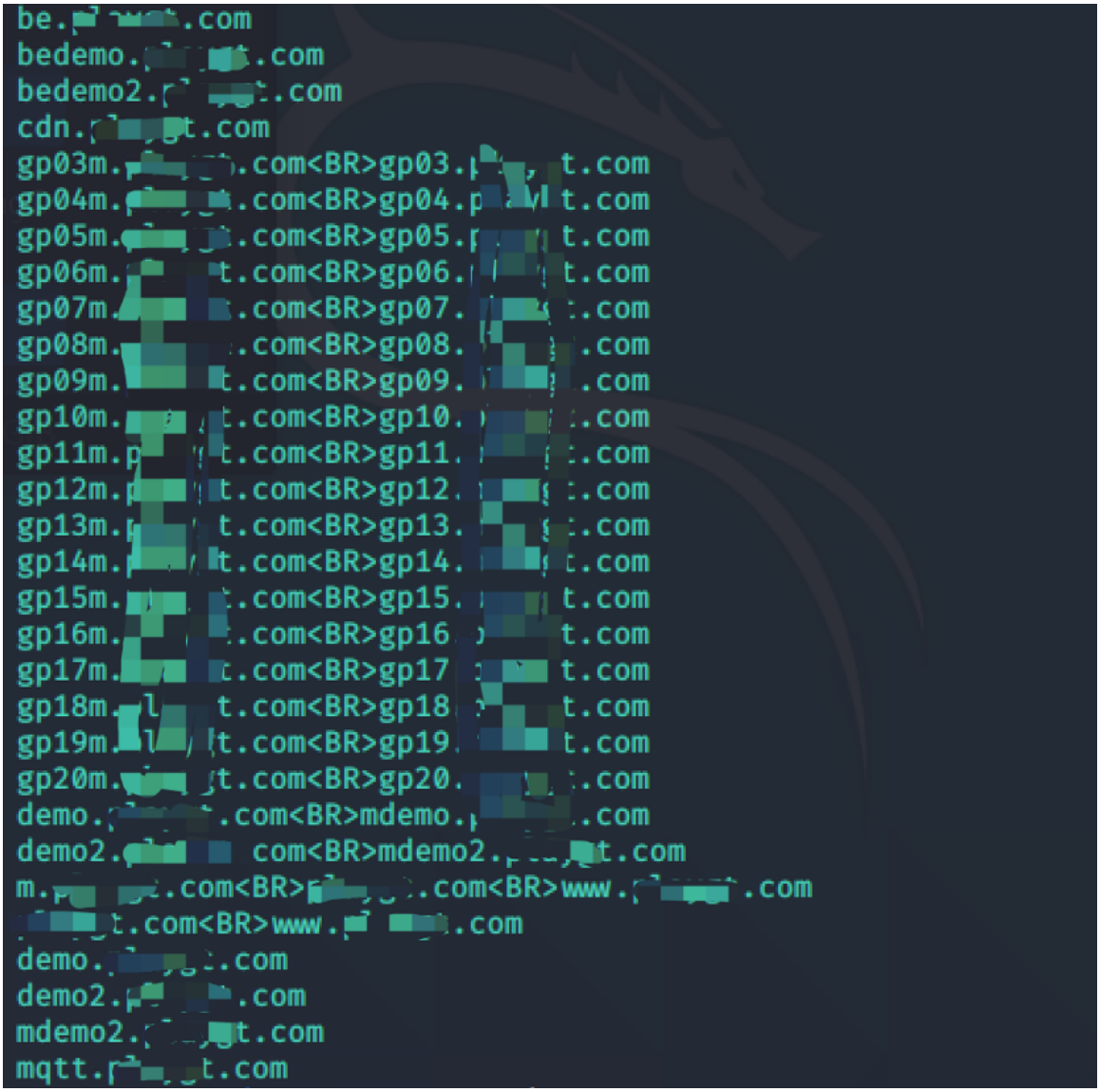
https://www.XXXX.com/url?sa=i&url=https%3A%2F%2Fwww.XXXX.com%2Fhottopic%2F20190730000007-260809&psig=AOvVaw3SR-d4gR-k0_fTvj4BhfGe&ust=1591758565017000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCJDs-ojh8-kCFQAAAAAdAAAAABAD

于是我更换了另外一个工号，发现该图片是正常的，于是又看了下图片地址，从而得到了新的信息：https://cdn.XXXXX.com/site/upload/promotions/7db335cc-e657-8a1b-e6b2-d61aaee1a675.png

根据图片的命名信息来看，已被后台过滤。并且该地址的子域名是CDN开头，大概率是采用了CDN专属服务器或相关系统来存储文件、图片等信息。

于是也是因为好奇心，对该CDN地址进行了初步的信息收集，发现该ip为台湾地址。

扫描同级子域名如下，真的是闪爆了，都是博彩网站。



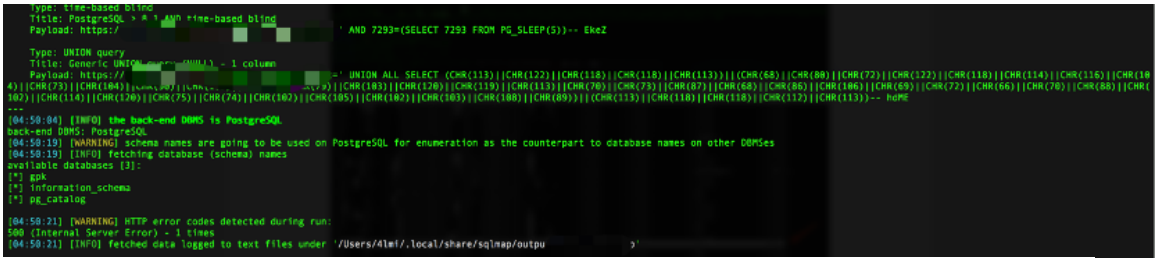
通过解析的两个ip地址旁站查询发现博彩网站数量极大，看来这个站只是凤毛麟角。

3.为爱而“站”之乘风破浪

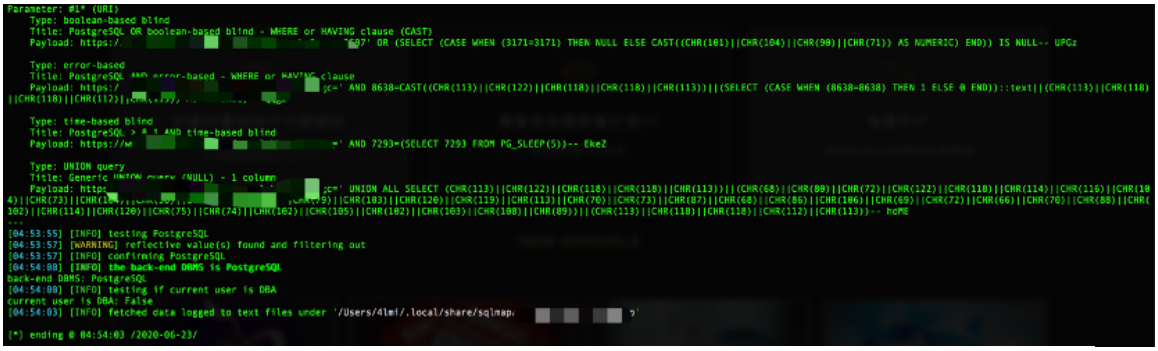
既然信息收集没有成果，那我们返回来继续看该站点的其它信息，随便点开一个功能页面发现数据传输类型为字符型，试一试有没有sql注入，单引号果然是万能的，数据库报错。

为了验证sql注入的真实性，我们用 ’and ’1’=’1 测试发现页面返回异常用 ’and ’1’=’2 测试页面返回正常，断定为字符型注入。

果断将url放入sqlmap里跑了一下，成功爆出数据库。



可惜不是dba权限。



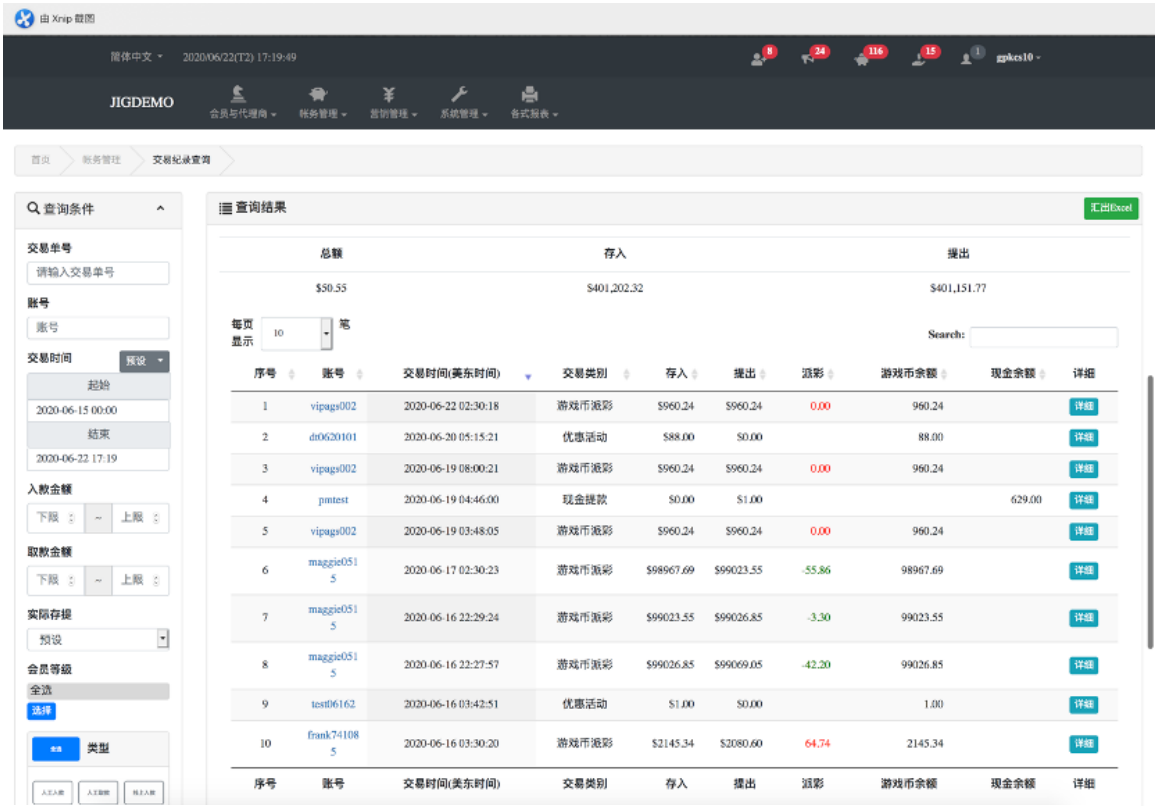
4.为爱而“站”之峰回路转

翻阅了三个数据库都没有找到管理员的账号密码，只找到了用户表，此时的我万念俱灰。无奈之下，只能找几个用户的账号密码，登陆进去看看有没有其它的漏洞，接着爆表。

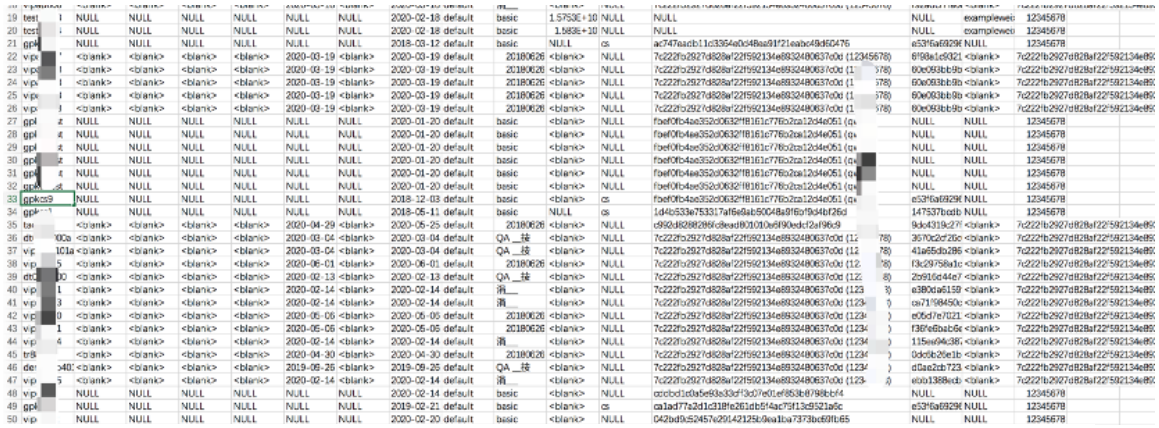
等等我看到了什么……

居然在用户表里爆出了一个客服的账号密码，what……生活就是这样，在绝望中给你一点希望。通过工具扫描成功找到后台地址：

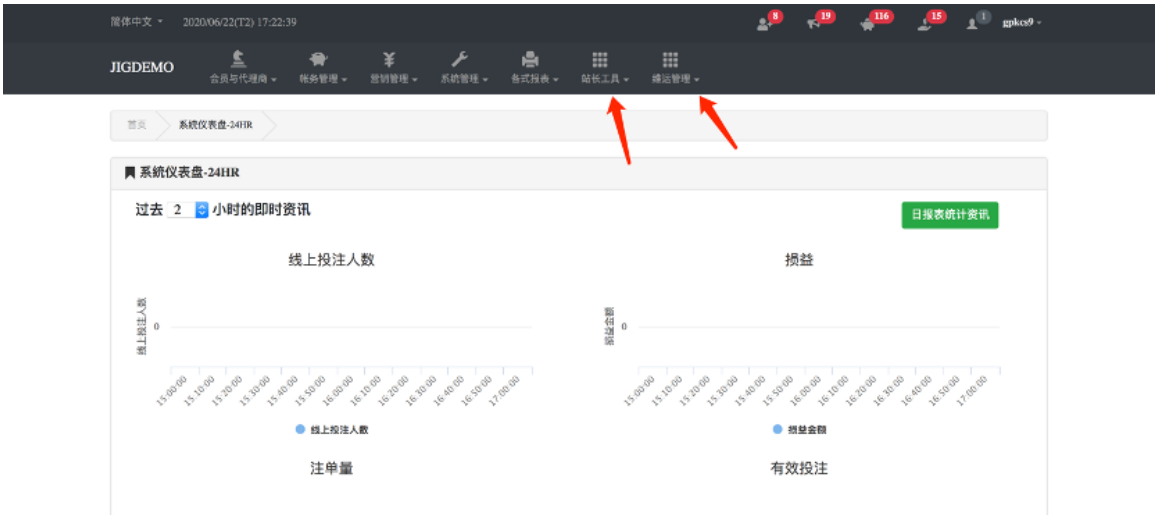
登入客服账号，可以看到用户的流水还是挺大的。



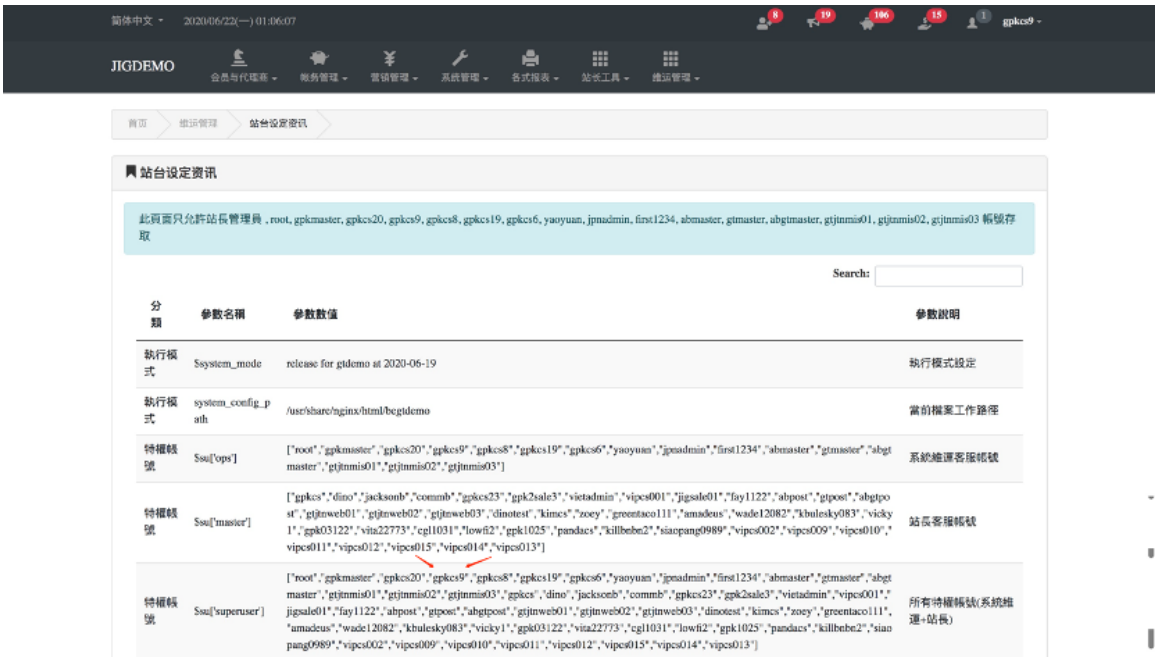
经过一系列的漏洞排查，未能找到突破口，感觉还是客服权限太低了。又经过一段时间的数据库信息排查，找到了另外一个用户数据表，发现里边存在一个“gpkcs9”的用户，果断脱裤。果然，我同学注册的账号也在里面。



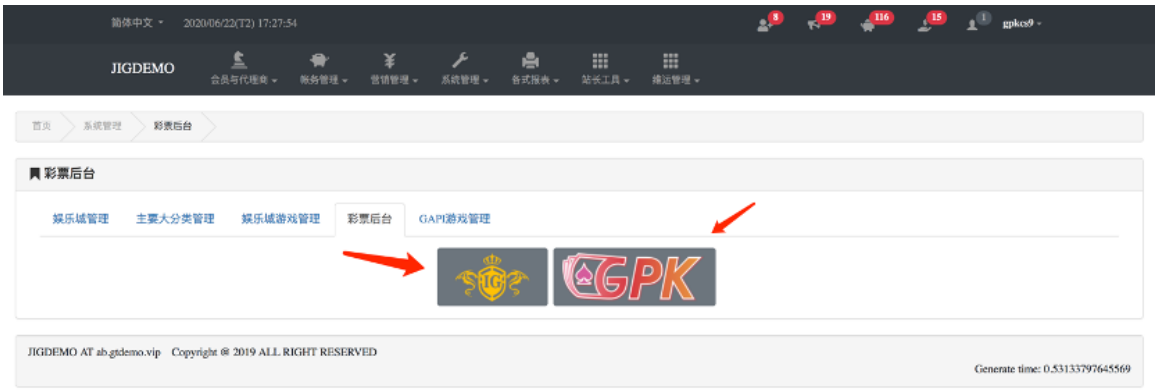
登录查看确实比“gpkcs10”用户权限高。多出两个功能。



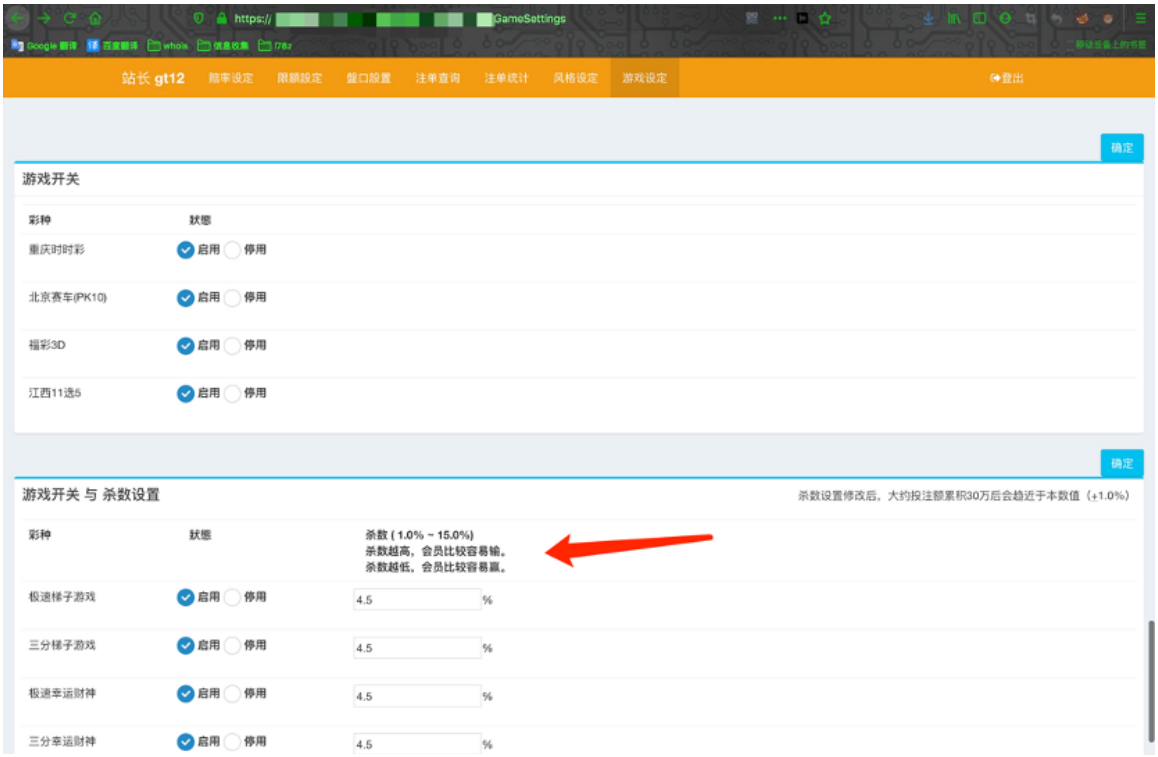
在系统配置中看到“gpkcs9”管理用户为系统运维账号并为最高权限账号。这么多的管理员账号，看来是一个博彩帝国呀！



那我们就看看他在运维哪些网站，这里发现了两个彩票后台的登录入口。



其中一个需要登录账号密码，爆破无果，另一个不需要账号密码登录。



妥妥的“杀猪盘”有木有。在这样的环境下，你又怎么可能会赢钱呢，到此为止今天的目的算是达到了，带大家看一看博彩网站背后的奥秘。果断将脱下来的数据交到警察叔叔手里边，做一个遵纪守法的好公民。

5.为爱而“站”之因材施教

正所谓“十赌九输，不赌为赢”赢的时候不收手，脑海里给自己定的目标一次次提高希望能赢更多。输的时候更不收手，并认为前面赢的都是自己的本钱，越赌越大，想着一次翻本，必须输光才肯离场。输光后想尽一切办法，筹集赌资，继续进入赌局，以此轮回。最终的结局就是“家破人亡”在这里也奉劝各位看官老爷“久赌神仙输，常赢必出术”！

最后再安慰妹子一波，做一个十足的暖男（提升男人魅力的时候到了）。

这样的事情内心性格分析：

1.好奇心理：以旁观者的视角在观望打牌中使自己好奇心得到满足，从而迷恋

2.刺激心理：通过打牌、打麻等相关娱乐手段将动用金钱增加娱乐性和刺激性

3.贪婪心理：对于这种不劳而获获得的钱，初尝甜头，难以放手

4.翻本心理：由于内心的不甘，越输钱越想翻盘拿回本金，逐渐堕落

5.侥幸心理：通过别人的引诱，始终相信自己输掉的钱会赢回来

最后该任务成果已移交有关部门处理。

精选留言

用户设置不下载评论