

# 猖獗的网络犯罪及相关分析

演讲人：辛巴

## 议题大纲内容一览

都是些什么人被骗了？

国内最大的刷单诈骗团伙

针对国内的最大裸聊诈骗团伙

一次溯源跑分平台的过程（溯源到个人和公司）

分享几个涉及到网络犯罪常被使用的程序以及漏洞



# 一.都是些什么人被骗了?

- 1.刷单诈骗
- 2.裸聊诈骗
- 3.投资类型的诈骗 (虚拟币,彩票杀猪盘)
- 4.冒充公检法诈骗
- 5.擦边球式的诈骗 (活动茶叶, 活动手表)



涉世未深大学生



孤独寂寞单身男



倾家荡产一把梭



信息泄露后遗症



## 二.国内最大的刷单诈骗团伙

源头技术团队



下游一些产业链:

- 1.码商洗钱-租买商户微信-支付宝二维码
- 2.提供微信号, QQ号的号商
- 3.提供银行卡四件套
- 4.取钱背锅人

经常用的一些术语:

- 1.HX=后续 (二次诈骗的含义)
- 2.SH=商户
- 3.JD TB PDD=京东 淘宝 拼多多
- 4.码=使用的钓鱼二维码



## 二.国内最大的刷单诈骗团伙

源头技术团队



下游一些产业链:

- 1.码商洗钱-租买商户微信-支付宝二维码
- 2.提供微信号, QQ号的号商
- 3.提供银行卡四件套
- 4.取钱背锅人

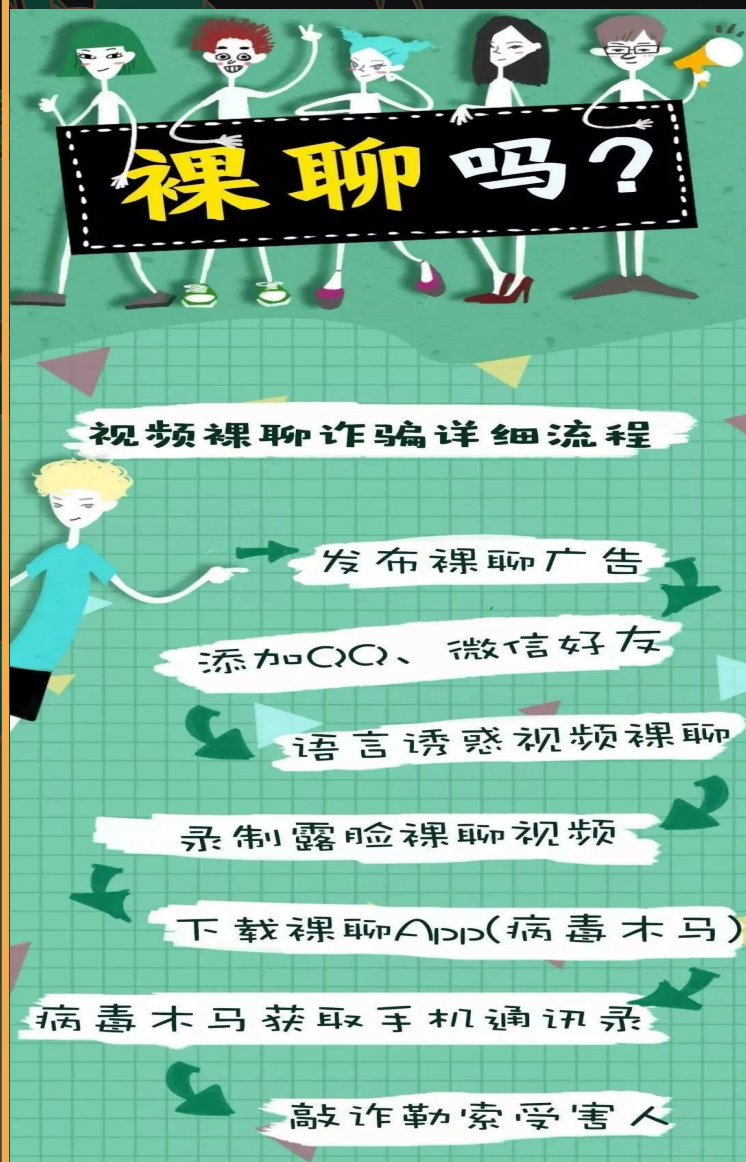
经常用的一些术语:

- 1.HX=后续 (二次诈骗的含义)
- 2.SH=商户
- 3.JD TB PDD=京东 淘宝 拼多多
- 4.码=使用的钓鱼二维码





### 三.针对国内的最大裸聊诈骗团伙



疫情到现在为止国内最活跃，诈骗人数最多，范围最广，金额最大的裸聊诈骗团伙----**抓狐1号**

该团伙几个显著特征：

- 1.组织框架完善
- 2.团队分工明确
- 3.内部技术支持
- 4.极度小心谨慎
- 5.诈骗手段多样





左右两边为从大交友平台引入受害者建立聊天，和发布的裸聊app的木马界面。



通讯录已被上传





手机号	创建时间	操作				
101	2020年10月12日 10:58 上午	短信	通讯录	定位	导出通讯录	导出短信
5	2020年10月12日 10:55 上午	短信	通讯录	定位	导出通讯录	导出短信
13	2020年10月12日 10:55 上午	短信	通讯录	定位	导出通讯录	导出短信
36	2020年10月12日 10:54 上午	短信	通讯录	定位	导出通讯录	导出短信
20	2020年10月12日 10:54 上午	短信	通讯录	定位	导出通讯录	导出短信
58	2020年10月12日 10:53 上午	短信	通讯录	定位	导出通讯录	导出短信
6	2020年10月12日 10:53 上午	短信	通讯录	定位	导出通讯录	导出短信
9	2020年10月12日 10:52 上午	短信	通讯录	定位	导出通讯录	导出短信
8	2020年10月12日 10:52 上午	短信	通讯录	定位	导出通讯录	导出短信
6	2020年10月12日 10:51 上午	短信	通讯录	定位	导出通讯录	导出短信
9	2020年10月12日 10:50 上午	短信	通讯录	定位	导出通讯录	导出短信
2	2020年10月12日 10:47 上午	短信	通讯录	定位	导出通讯录	导出短信
57	2020年10月12日 10:44 上午	短信	通讯录	定位	导出通讯录	导出短信
7	2020年10月12日 10:44 上午	短信	通讯录	定位	导出通讯录	导出短信
0	2020年10月12日 10:40 上午	短信	通讯录	定位	导出通讯录	导出短信
9	2020年10月12日 10:39 上午	短信	通讯录	定位	导出通讯录	导出短信
5	2020年10月12日 10:37 上午	短信	通讯录	定位	导出通讯录	导出短信
4	2020年10月12日 10:36 上午	短信	通讯录	定位	导出通讯录	导出短信
13	2020年10月12日 10:35 上午	短信	通讯录	定位	导出通讯录	导出短信

手机号	创建时间	操作			
827	2020年10月10日 5:10 下午	短信	通讯录	定位	导出通讯录
177	2020年10月10日 5:10 下午	短信	通讯录	定位	导出通讯录
179	2020年10月10日 5:03 下午	短信	通讯录	定位	导出通讯录
66	2020年10月10日 5:02 下午	短信	通讯录	定位	导出通讯录
309	2020年10月10日 4:58 下午	短信	通讯录	定位	导出通讯录
160	2020年10月10日 4:46 下午	短信	通讯录	定位	导出通讯录
50	2020年10月10日 4:45 下午	短信	通讯录	定位	导出通讯录
50	2020年10月10日 4:44 下午	短信	通讯录	定位	导出通讯录
4	2020年10月10日 4:22 下午	短信	通讯录	定位	导出通讯录
13	2020年10月10日 4:22 下午	短信	通讯录	定位	导出通讯录
375	2020年10月10日 4:04 下午	短信	通讯录	定位	导出通讯录
301	2020年10月10日 4:00 下午	短信	通讯录	定位	导出通讯录
12	2020年10月10日 3:52 下午	短信	通讯录	定位	导出通讯录
45	2020年10月10日 3:52 下午	短信	通讯录	定位	导出通讯录
9	2020年10月10日 3:51 下午	短信	通讯录	定位	导出通讯录
125	2020年10月10日 3:49 下午	短信	通讯录	定位	导出通讯录



https://www.1jiahuo.com/

加密货币行情

币种	最新价	24H 最高价	24H 最低价	24H 量	涨幅	现货交易	K线交易
BTC / USD	11479.54	11724	11416.44	1603966.4137688198	-0.50% ↓	交易中	
ETH / USD	383.41	394.68	382	36778976.679791726	-0.45% ↓	交易中	
XRP / USD	0.25794	0.25991	0.2537	2649603670.051372	0.60% ↑	交易中	
BCH / USD	241.49	244	237.43	4838297.073262479	0.24% ↑	交易中	
LTC / USD	50.14	51.51	49.89	11278285.483547146	-1.67% ↓	交易中	
USC / USD	501.4224	538.1116	498.2819	1603966.4137688198	-2.66% ↓	交易中	

http://1jiahuo.com/index/login/login/token/6d63cc05955a88bae1c18893b7b2952e.html

密码登录

帐号/姓名

## 抓狐1号搭建的虚拟币交易所-杀猪盘

除此之外，该团伙还搭建了贷款诈骗网站等多个系统，诈骗一段时间之后删除数据，改换域名进行下一轮的诈骗。

## 四.一次溯源跑分平台的过程

接到任务，对一个跑分平台进行测试，在测试过程中，发现其中一个密码很有意思。在pass位置，中间的号码疑似电话号码。



DB_PORT	"3306"	远程端口
DB_DATABASE	"t..."	数据库名
DB_USERNAME	"roots"	用户名
DB_PASSWORD	"zq17...-...-..."	用户密码



17...手机归属

手机号码"17..." 上海 民生通讯

请输入手机号码(段)  查询

电话归属地数据由[百度手机卫士](#)提供

该手机号对应多个支付宝账户，请核实后选择

支付宝账户: ...@qq.com

充值教程: ...

诚付... (诚付数字信息...)

Baidu 170... 百度一下

诚付数字信息技术有限公司

公司地址: ... 联系电话: 未提供 经理: ...

理手机: 17... 电子邮件: ... 邮政编码: 200...

www.11467.com/...html 百度快照

## 五.分享几个涉及到网络犯罪常被使用的程序及漏洞

### 1.裸聊诈骗使用的两个程序样本

### 后台登录

账号

密码

安全码

登录

### APPV1通讯录后台管理

体验ThinkPHP5+Layui2的极速双飞快感

用户名

密码

验证码

☐ 记住账号

登入

内容管理系统

清空数据

54%  
0K/s

用户

用户资料

短信资料

通讯录资料

授权码

授权码管理

用户资料

批量删除

刷新

搜索

请输入授权码

查询

<input type="checkbox"/>	编号	授权码	手机号	创建时间	操作
<input type="checkbox"/>	11...	52136	151-1111-1111	2020年10月10日 5:10 下午	短信 通讯录 定位 导出通讯录
<input type="checkbox"/>	11...	487998	151-1111-1111	2020年10月10日 5:10 下午	短信 通讯录 定位 导出通讯录
<input type="checkbox"/>	11...	9134	151-1111-1111	2020年10月10日 5:03 下午	短信 通讯录 定位 导出通讯录
<input type="checkbox"/>	11...	0873	151-1111-1111	2020年10月10日 5:02 下午	短信 通讯录 定位 导出通讯录

完美通讯提供

系统

会员

通讯录数据

设备查看

通讯录查看

短信查看

APP参数设置

设备查看管理

请输入登录手机

请输入验证码

登录时间

立即提交

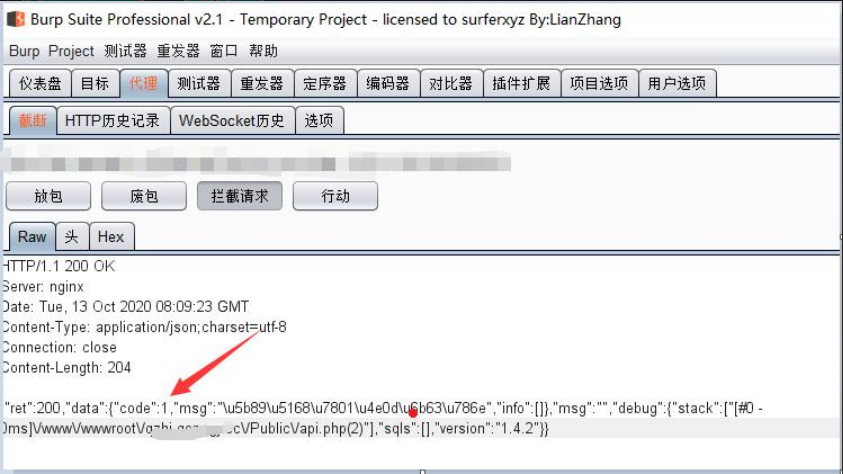
批量删除

ID	设备名称	登录手机	邀请码	最后登录时间	最后登录IP地址	最后登录位置	操作
2290	OPPO-PDKM00	151-1111-1111	776012	2020-10-13 13:29:37	192.168.1.1	中国河南	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2289	HUAWEI-DUB-AL00	151-1111-1111	1315	2020-10-13 13:02:43	192.168.1.1	中国云南丽江	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2288	HUAWEI-DUB-AL00	151-1111-1111	1315	2020-10-13 13:02:00	192.168.1.1	中国云南丽江	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2287	Apple-iPhoneX	151-1111-1111	123222	2020-10-12 23:54:08	192.168.1.1	中国新疆	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2286	OPPO-OPPOA59s	151-1111-1111	773219	2020-10-12 23:50:05	192.168.1.1	中国河北沧州	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2285	vivo-vivoX20A	151-1111-1111	456222	2020-10-12 23:39:42	192.168.1.1	中国浙江	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2284	vivo-vivoX20A	151-1111-1111	456222	2020-10-12 23:34:49	192.168.1.1	中国浙江	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2283	vivo-vivoX20A	151-1111-1111	456222	2020-10-12 23:34:09	192.168.1.1	中国浙江	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2282	HUAWEI-HMA-AL00	151-1111-1111	98425	2020-10-12 23:31:53	192.168.1.1	中国广东湛江	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2281	OPPO-PBAT00	151-1111-1111	45698	2020-10-12 23:16:57	192.168.1.1	中国浙江金华	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2280	OPPO-PBAT00	151-1111-1111	45698	2020-10-12 23:16:04	192.168.1.1	中国浙江金华	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2279	OPPO-PBAT00	151-1111-1111	45698	2020-10-12 23:14:52	192.168.1.1	中国浙江金华	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2278	HUAWEI-TAS-AN00	151-1111-1111	123555	2020-10-12 23:13:12	192.168.1.1	中国西藏拉萨	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2277	OPPO-PBAT00	151-1111-1111	45698	2020-10-12 23:12:57	192.168.1.1	中国浙江金华	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2276	vivo-vivoX9s	151-1111-1111	53511	2020-10-12 23:12:15	192.168.1.1	中国广西	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2275	OPPO-PBAT00	151-1111-1111	45698	2020-10-12 23:12:09	192.168.1.1	中国浙江金华	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2274	OPPO-PBAT00	151-1111-1111	45698	2020-10-12 23:12:09	192.168.1.1	中国浙江金华	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2273	OPPO-PBAT00	151-1111-1111	45698	2020-10-12 23:12:09	192.168.1.1	中国浙江金华	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可
2272	vivo-vivoX9s	151-1111-1111	53511	2020-10-12 23:11:29	192.168.1.1	中国广西	在线定位 查看通讯录 查看短信 下载通讯录数据 下载短信数据 清空通讯录 清空短信 可



# 抓狐1号使用的裸聊程序后台漏洞

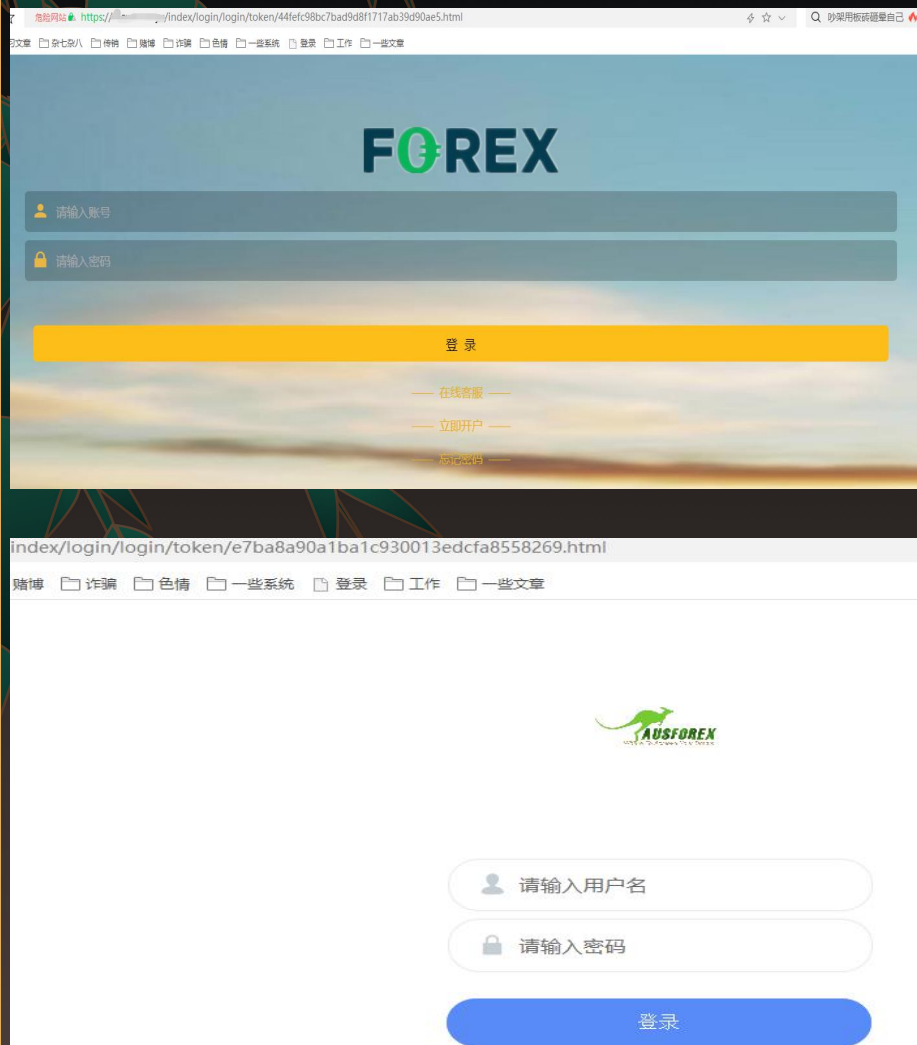
## 1.修改响应包进入后台



## 2.越权漏洞



## 2.微盘程序（投资理财类型的杀猪盘诈骗通用程序）



后台跳转页面特征



## 微盘程序漏洞

1. 伪造cookie进入后台

2. 后台getshell





### 3.博彩类的程序

#### 天恒博彩程序



#### 1.前台xss漏洞

#### 2.暴力猜解

在网站前台订单，用户名处存在xss漏洞，可以打cookie

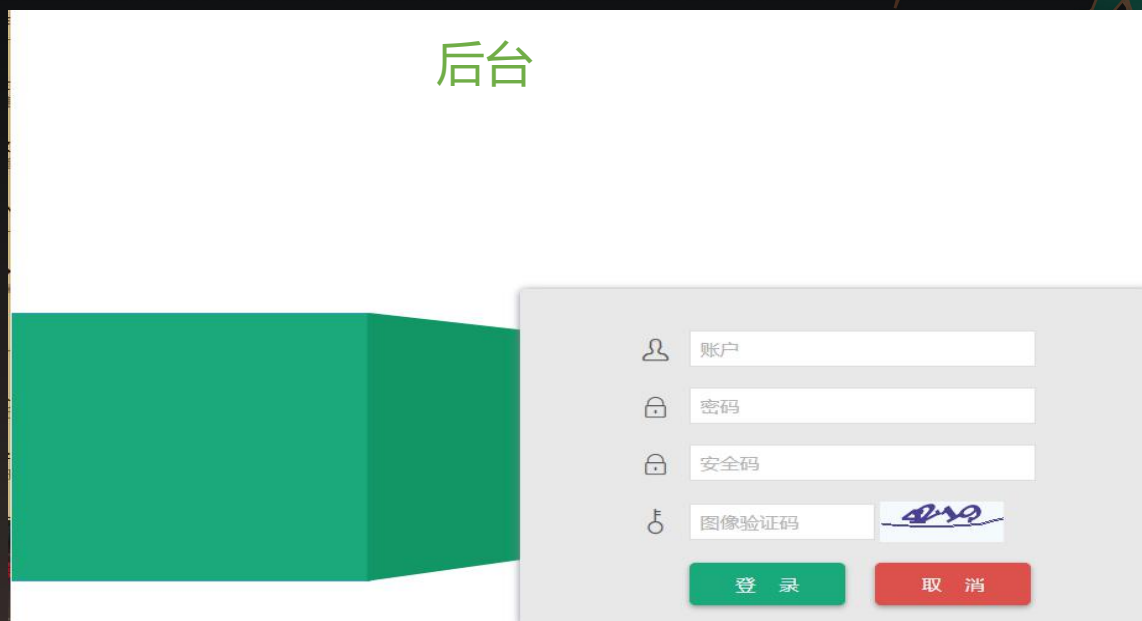
网站默认用户名为admin，进入第二个跳转页面输入密码和安全码，这个位置，信息显示的很明显，可以先爆破安全码，在通过正确的安全码反馈信息爆破密码。

# 大发的仿制品，大富彩票杀猪盘程序

## 前台



## 后台

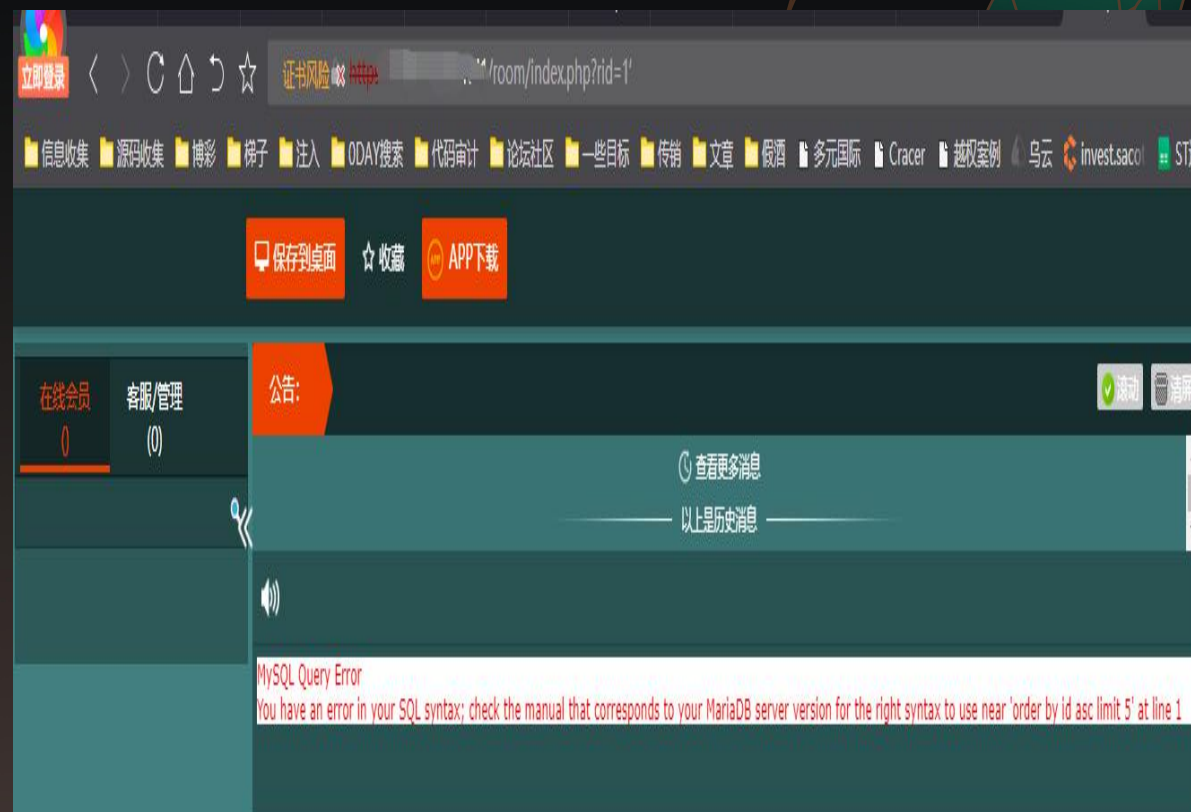
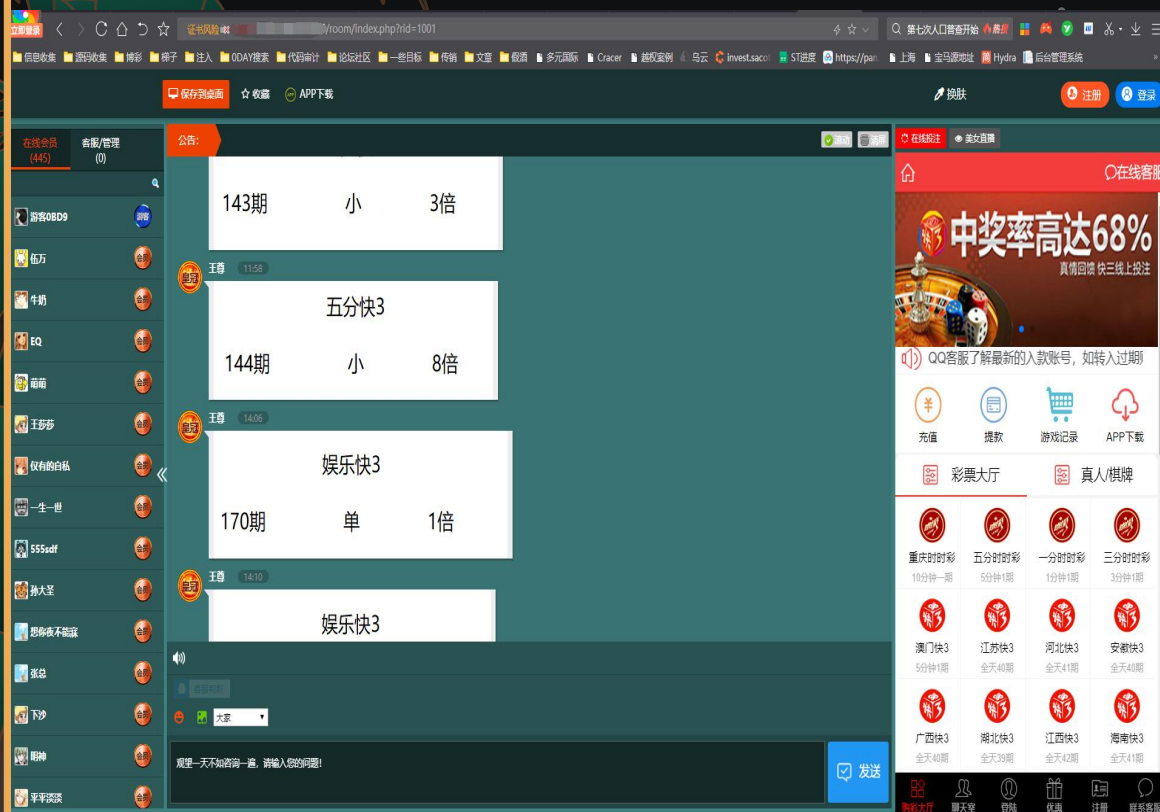


漏洞1.后台登录处，安全码位置sql盲注

漏洞2.后台任意文件上传漏洞



## 彩票博彩聊天室程序



多被用于彩票，博彩的洗脑聊天室，打开以后出现的首页链接，把rid参数改为1就是注入。





# 谢谢各位，议题结束

告辞！

