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

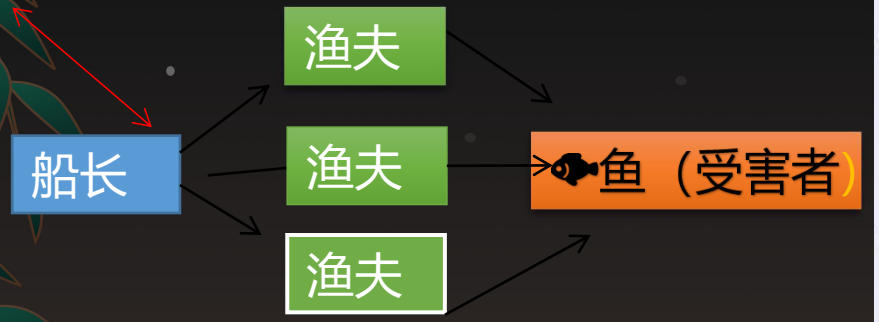
孤独寂寞单身男

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：

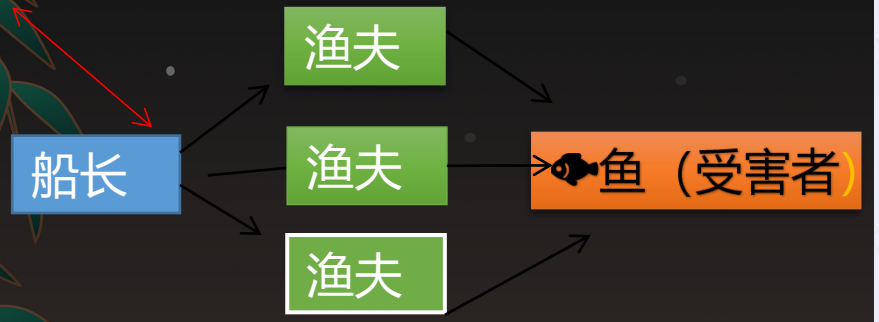
1.码商洗钱-租买商户微信-支付宝二维码
2.提供微信号，QQ号的号商
3.提供银行卡四件套
4.取钱背锅人

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



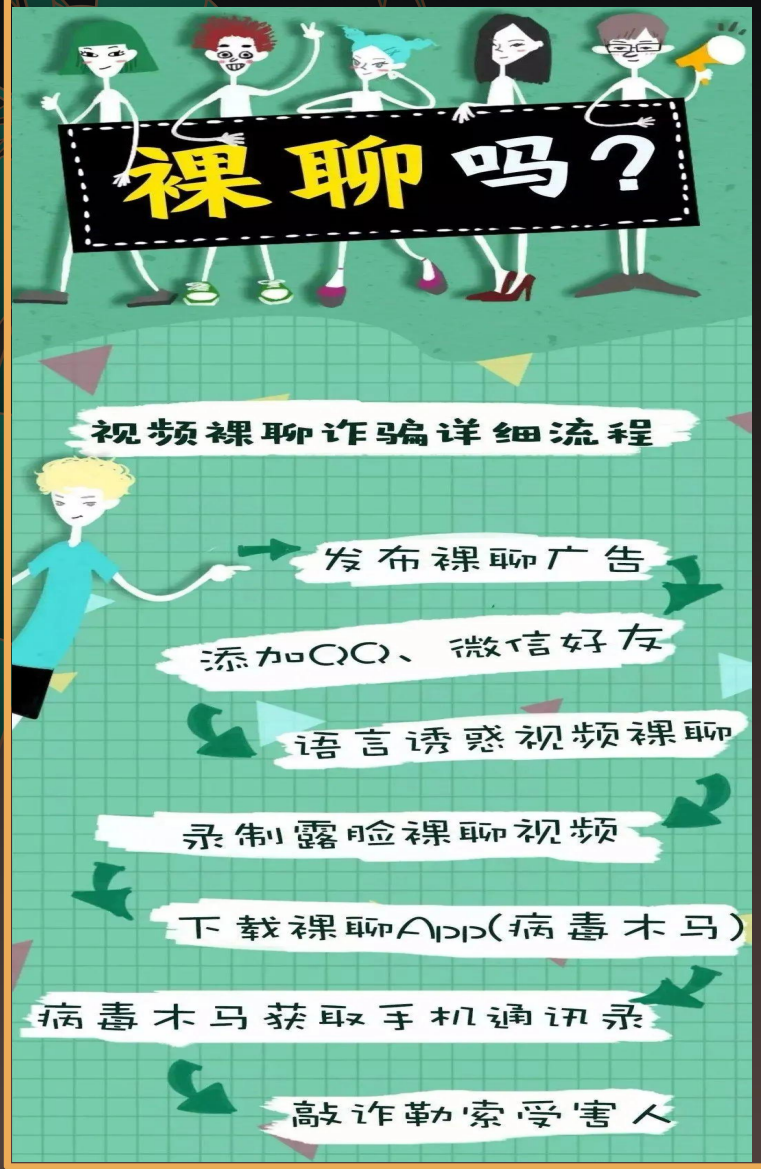
下游一些产业链：

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：

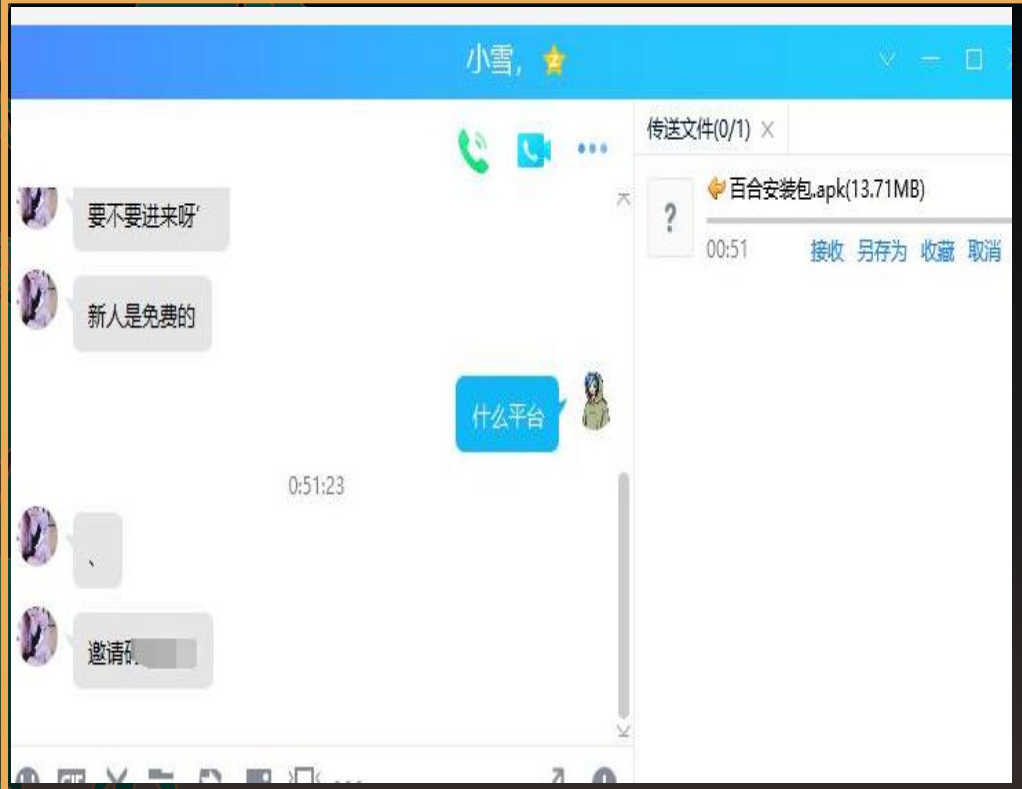
1.组织框架完善

2.团队分工明确

3.内部技术支持

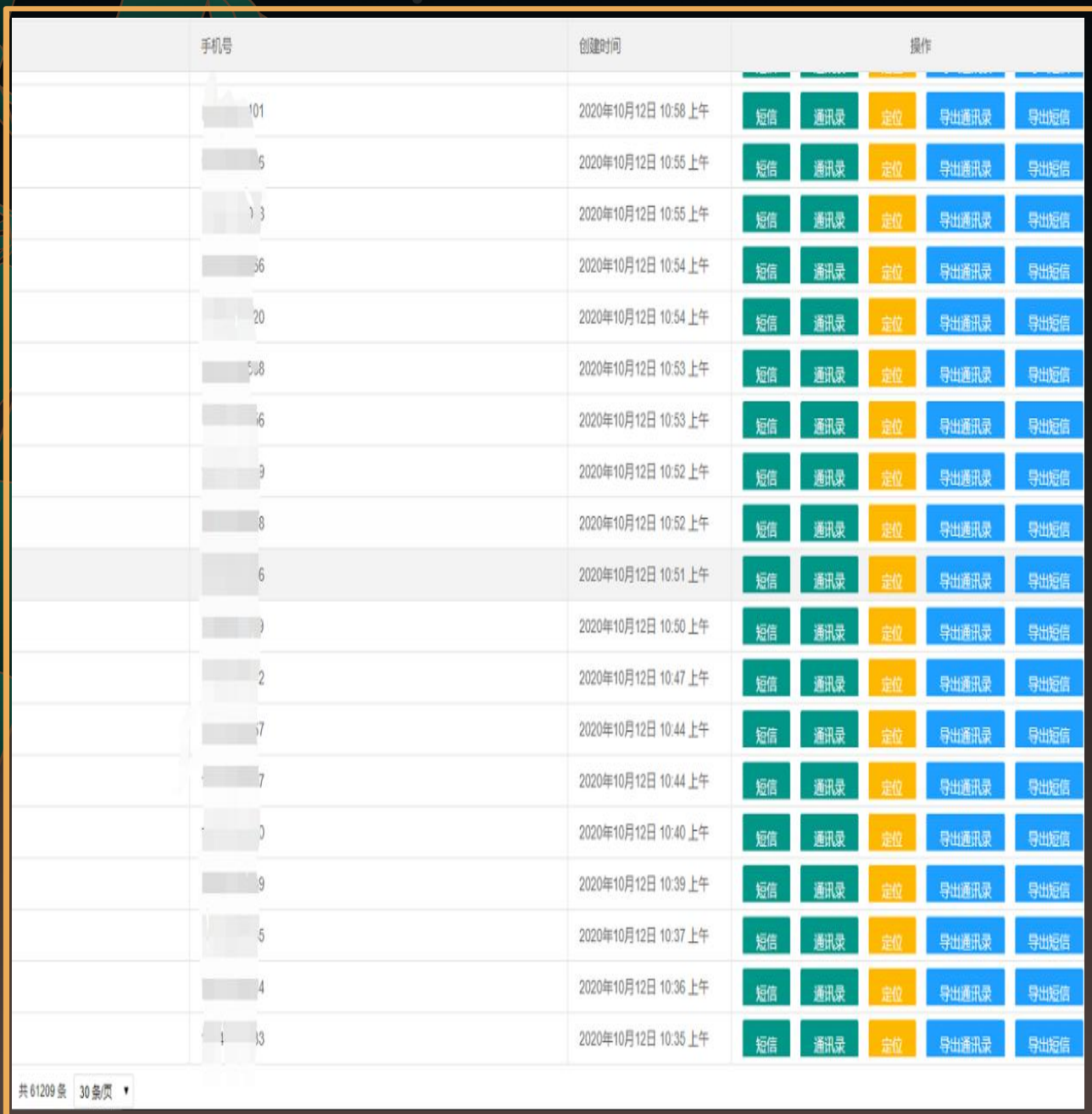
4.极度小心谨慎

5.诈骗手段多样



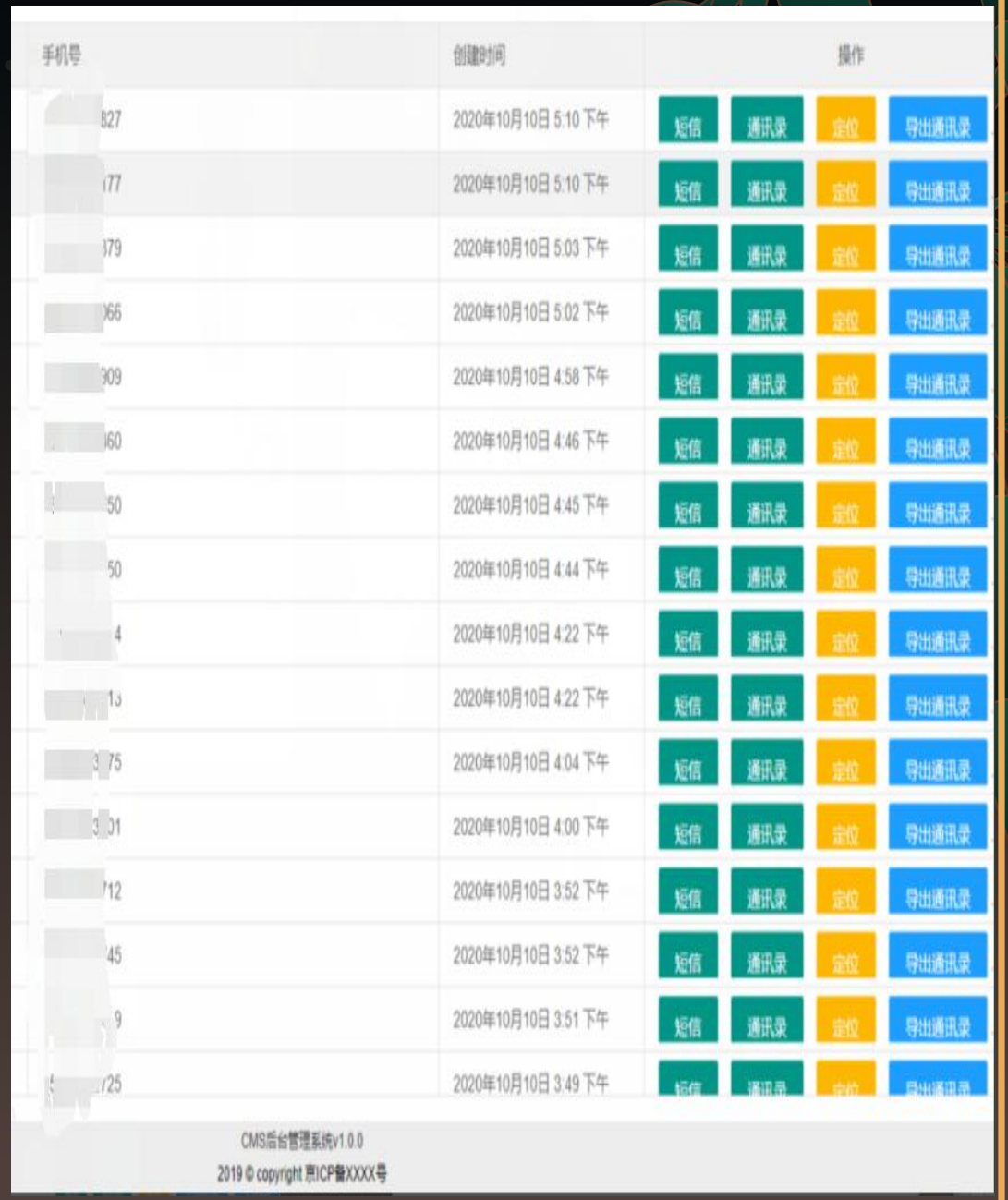
左右两边为从大交友平台引入受害者建立聊天，和发布的裸聊app的木马界面。

通讯录已被上传

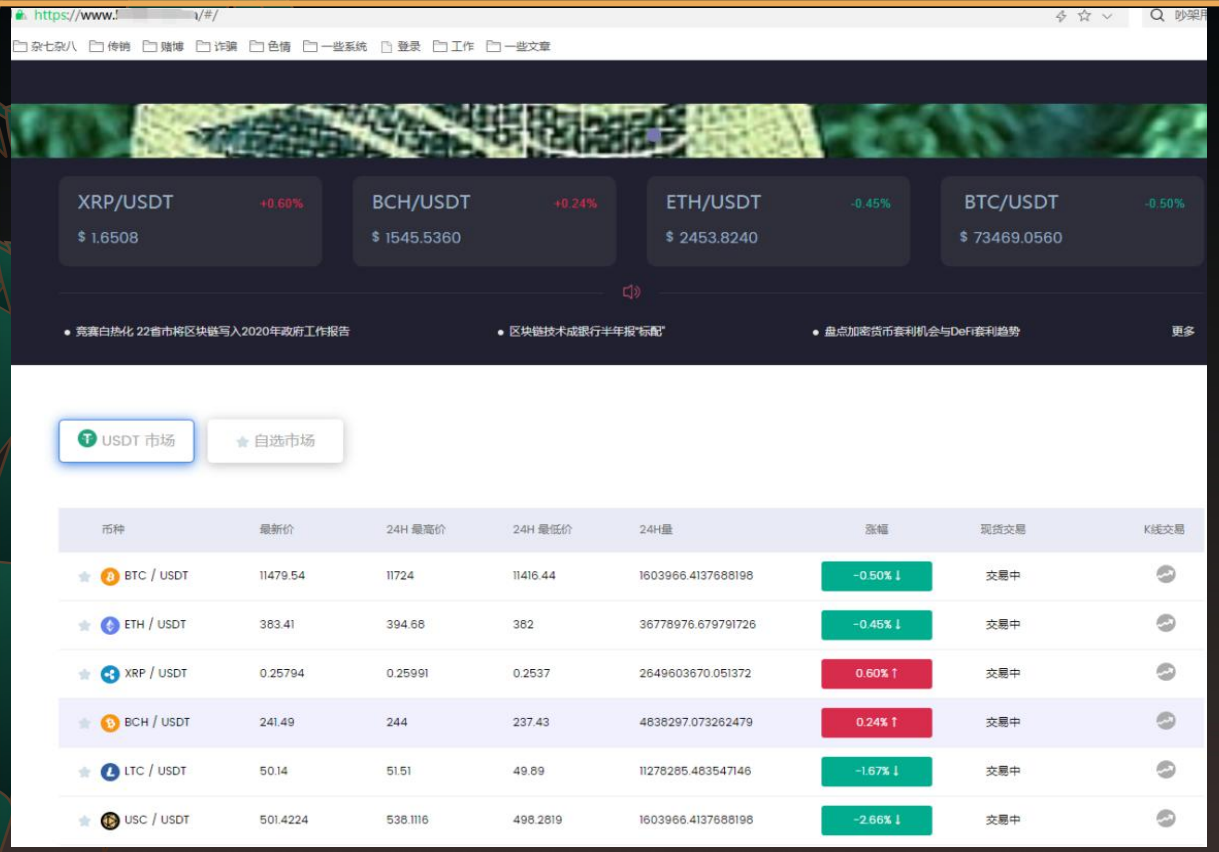


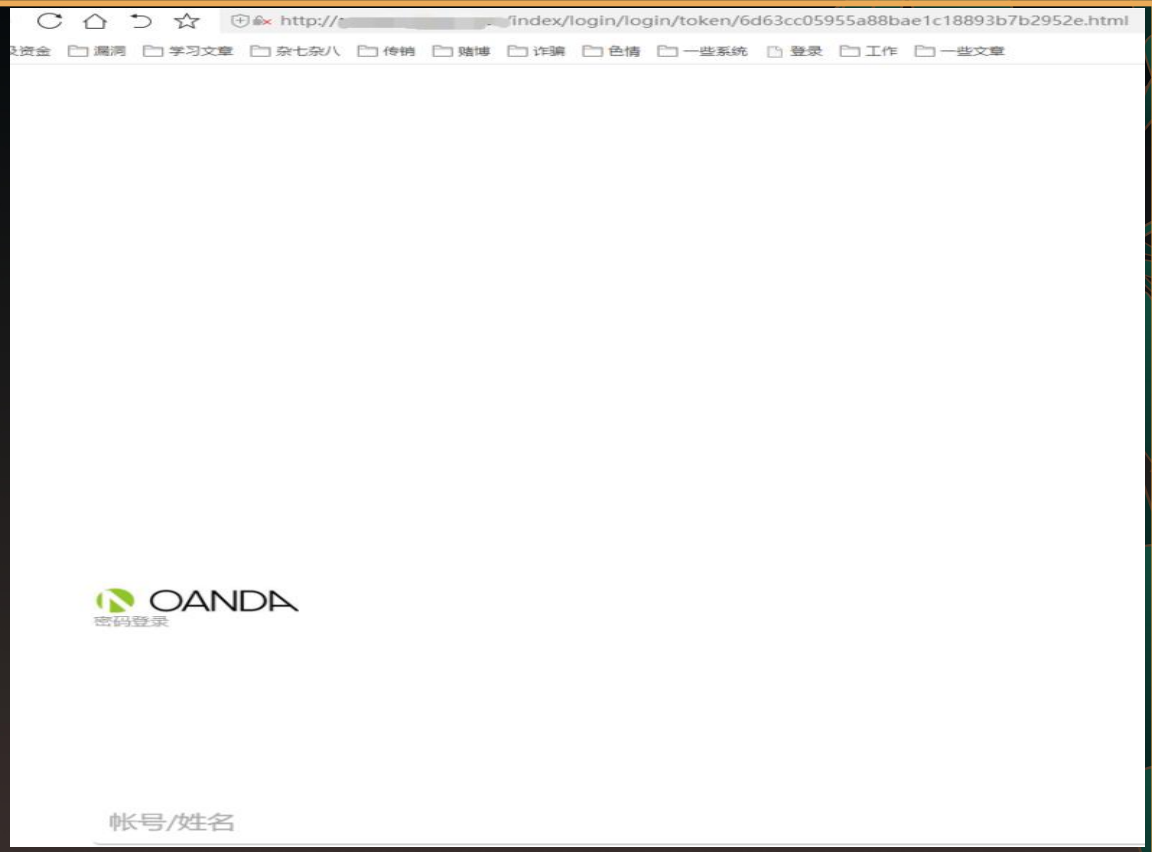
手机号	创建时间	操作
101	2020年10月12日 10:58 上午	短信 通讯录 定位 导出通讯录 导出短信
5	2020年10月12日 10:55 上午	短信 通讯录 定位 导出通讯录 导出短信
3	2020年10月12日 10:55 上午	短信 通讯录 定位 导出通讯录 导出短信
56	2020年10月12日 10:54 上午	短信 通讯录 定位 导出通讯录 导出短信
20	2020年10月12日 10:54 上午	短信 通讯录 定位 导出通讯录 导出短信
508	2020年10月12日 10:53 上午	短信 通讯录 定位 导出通讯录 导出短信
6	2020年10月12日 10:53 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
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
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
3	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

共61209条 30条/页



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
379	2020年10月10日 5:03 下午	短信 通讯录 定位 导出通讯录
366	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
75	2020年10月10日 4:04 下午	短信 通讯录 定位 导出通讯录
01	2020年10月10日 4:00 下午	短信 通讯录 定位 导出通讯录
712	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
725	2020年10月10日 3:49 下午	短信 通讯录 定位 导出通讯录





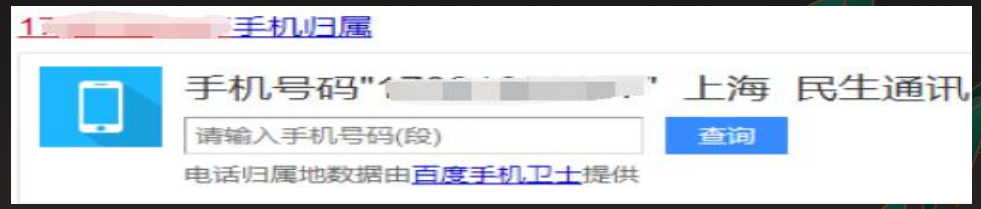
抓狐1号搭建的虚拟币交易所-杀猪盘

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

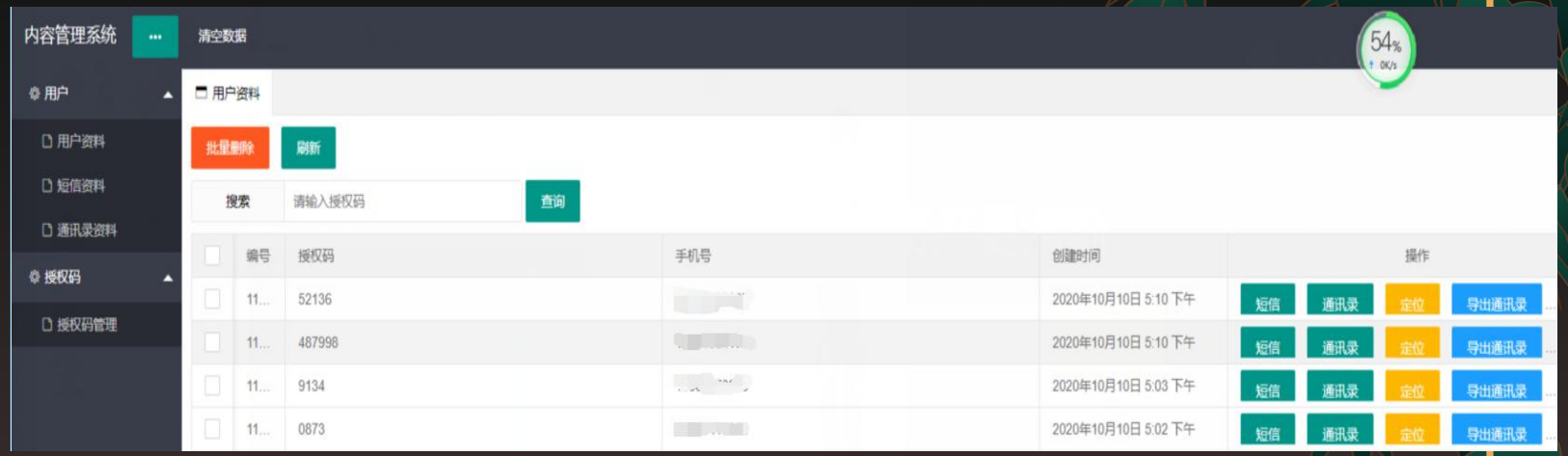
接到任务，对一个跑分平台进行测试，在测试过程中，发现其中一个密码很有意思。在pass位置，中间的号码疑似电话号码。

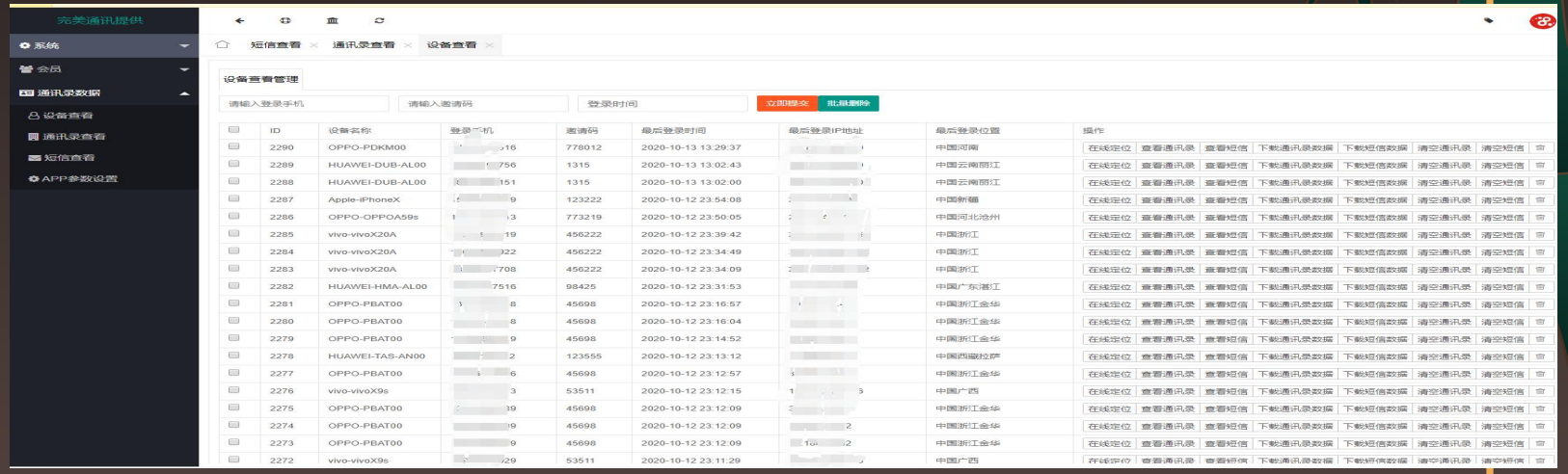
DB_PORT	"3306"	远程端口
DB_DATABASE	"t[redacted]"	数据库名
DB_USERNAME	"roots"	用户名
DB_PASSWORD	"zq17[redacted]"	用户密码



五.分享几个涉及到网络犯罪常被使用的程序及漏洞

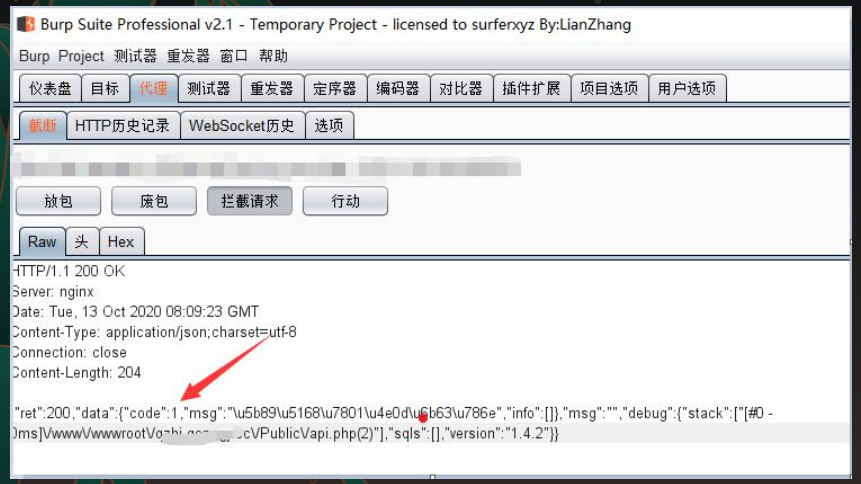
1.裸聊诈骗使用的两个程序样本



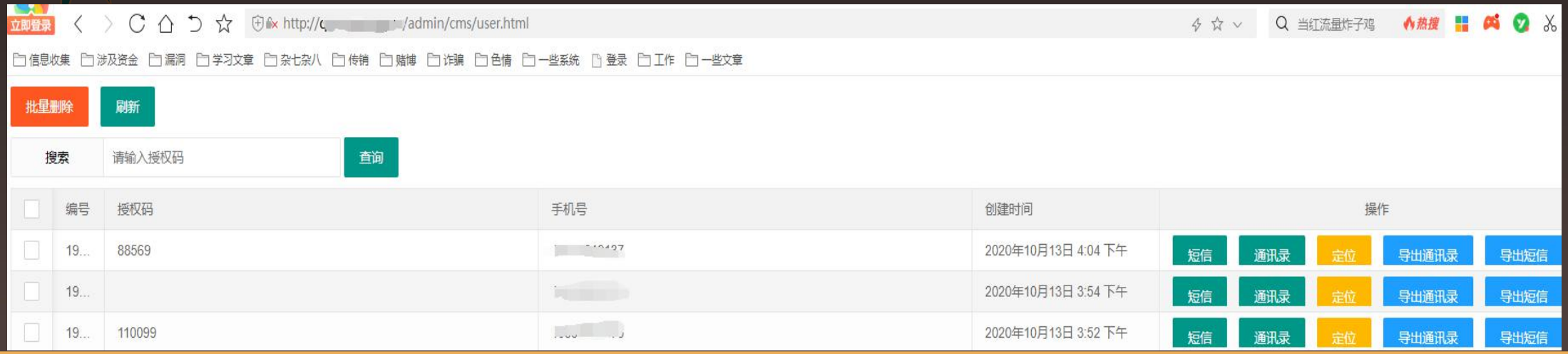


抓狐1号使用的裸聊程序后台漏洞

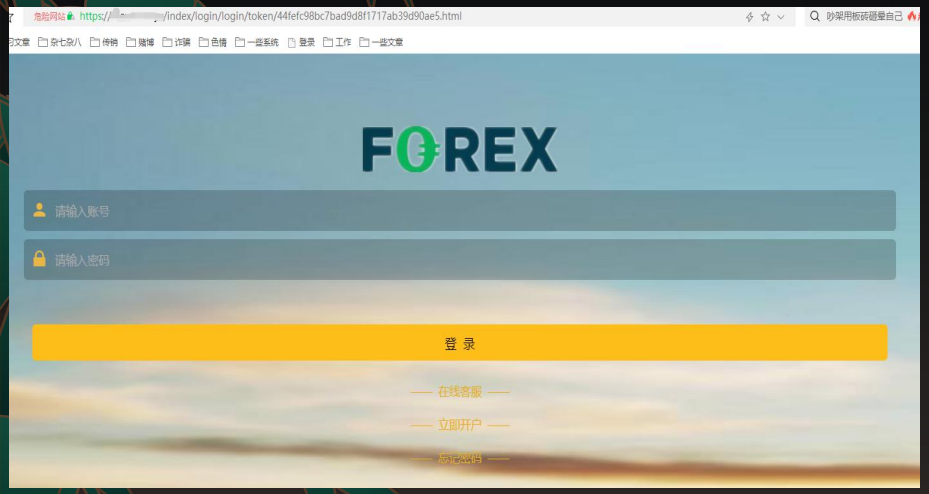
1.修改响应包进入后台



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

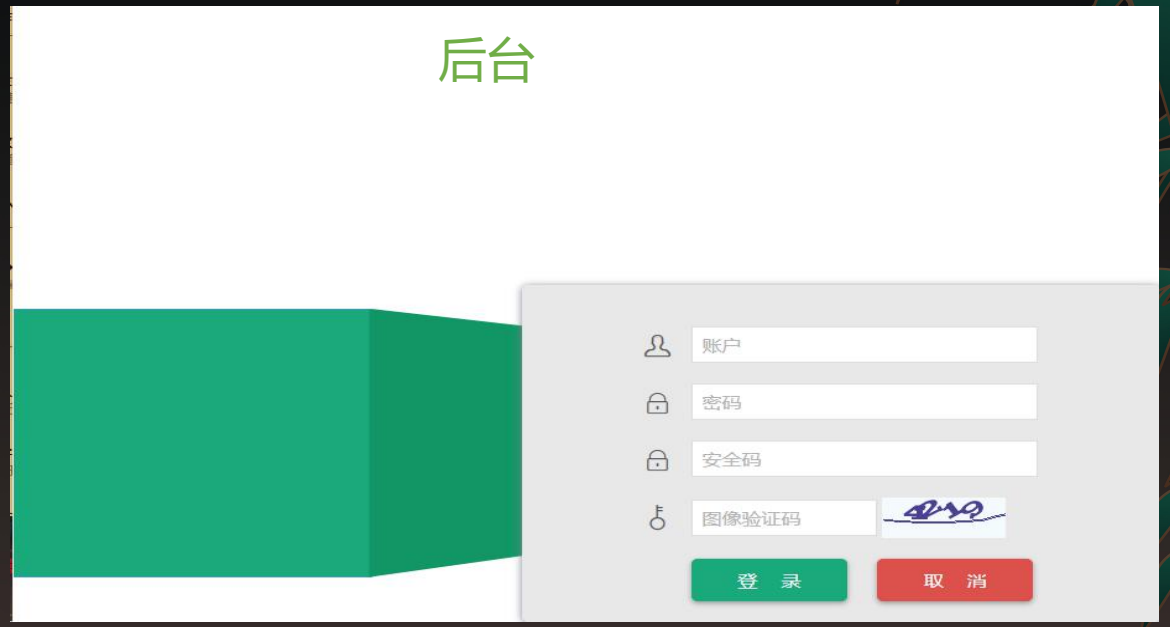
在网站前台订单，用户名处存在xss漏洞，可以打cookie

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

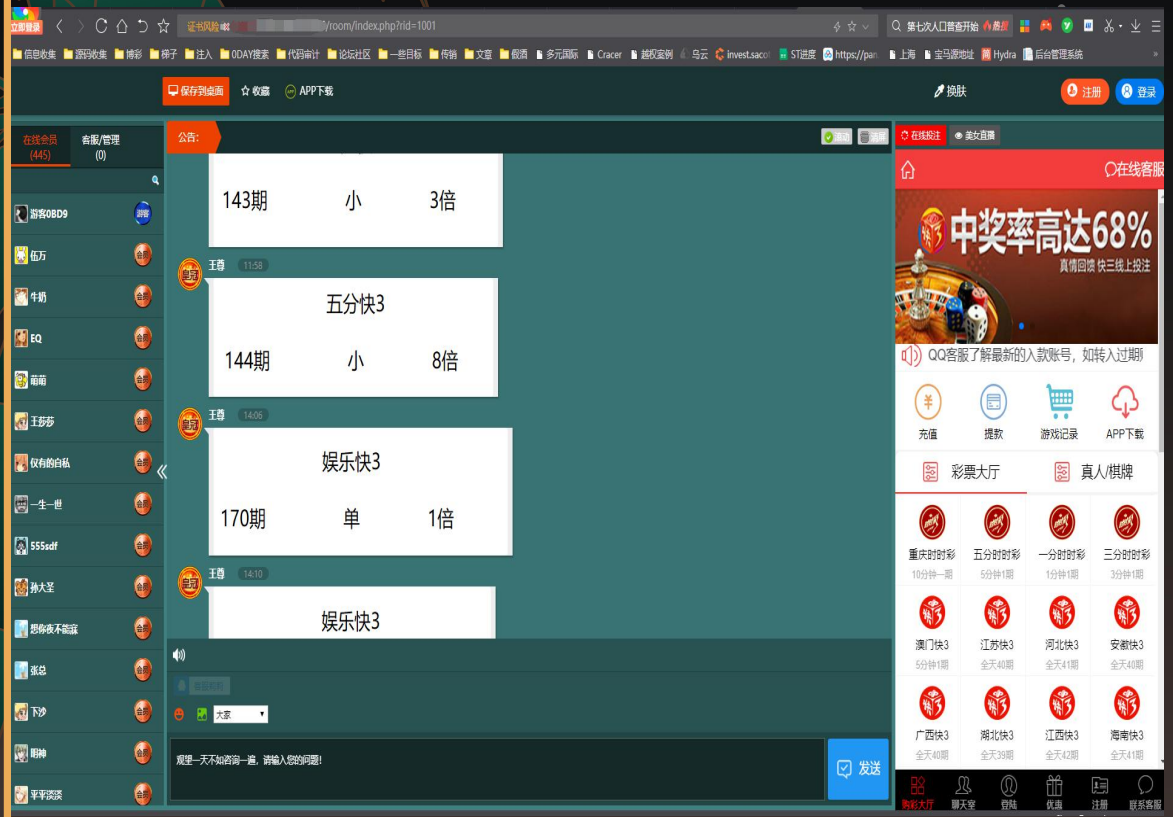
后台

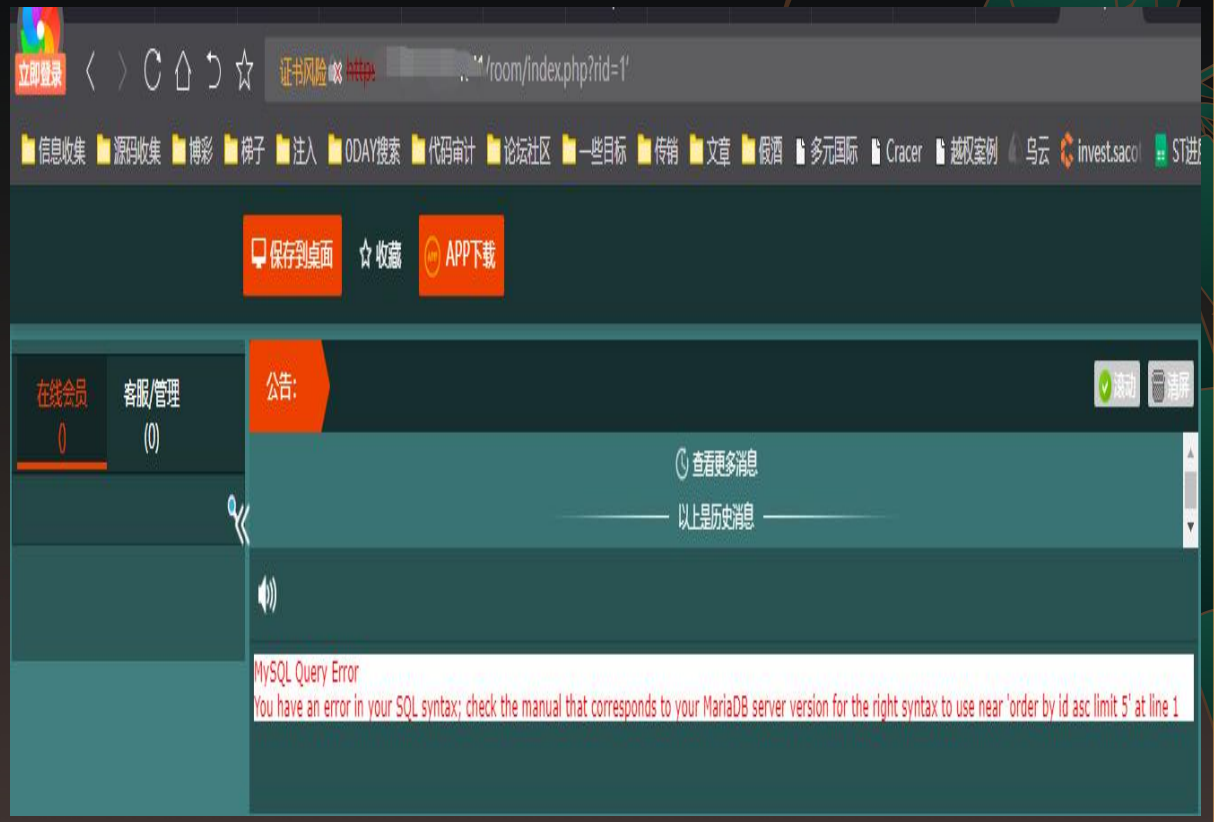


漏洞1.后台登录处，安全码位置sql盲注

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