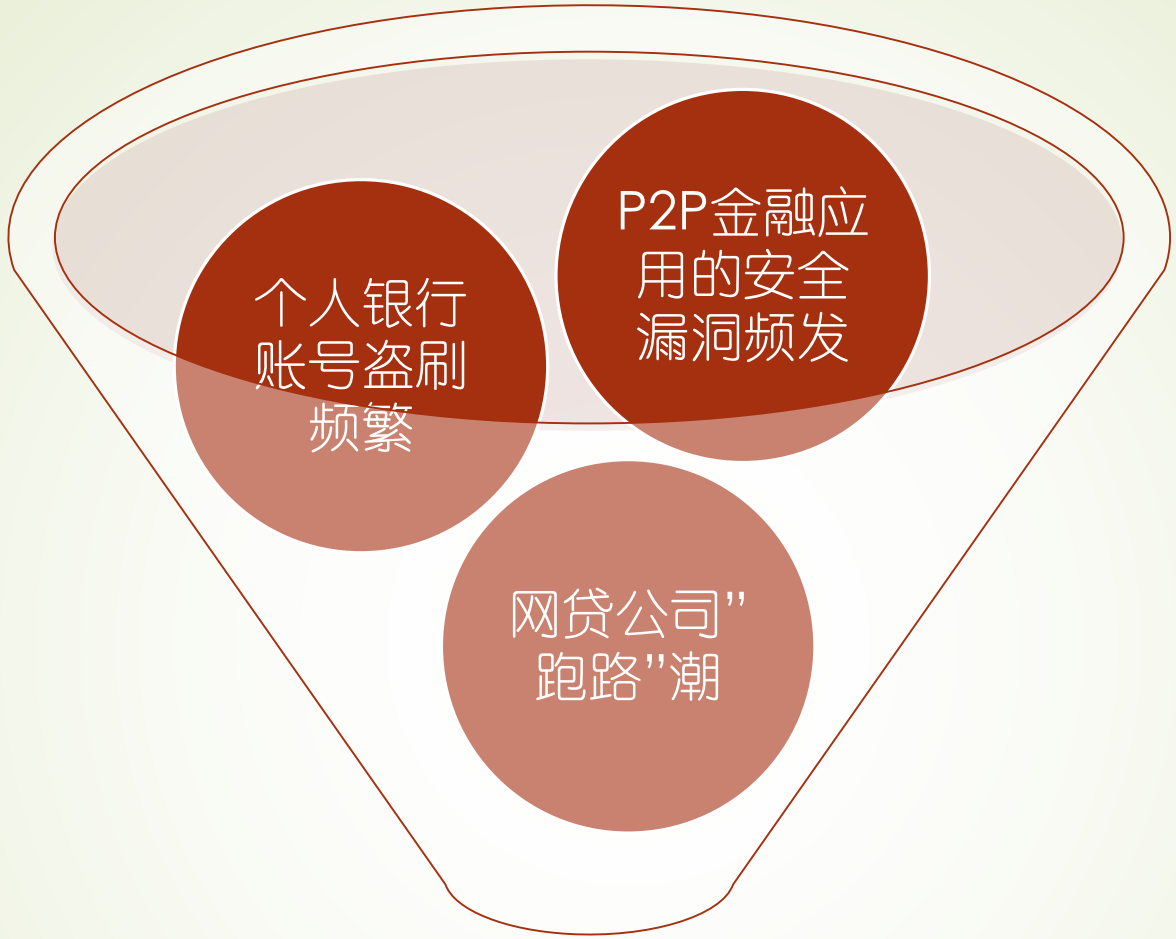
移动时代我怎么保证个人的金融安全

By 安全小飞侠

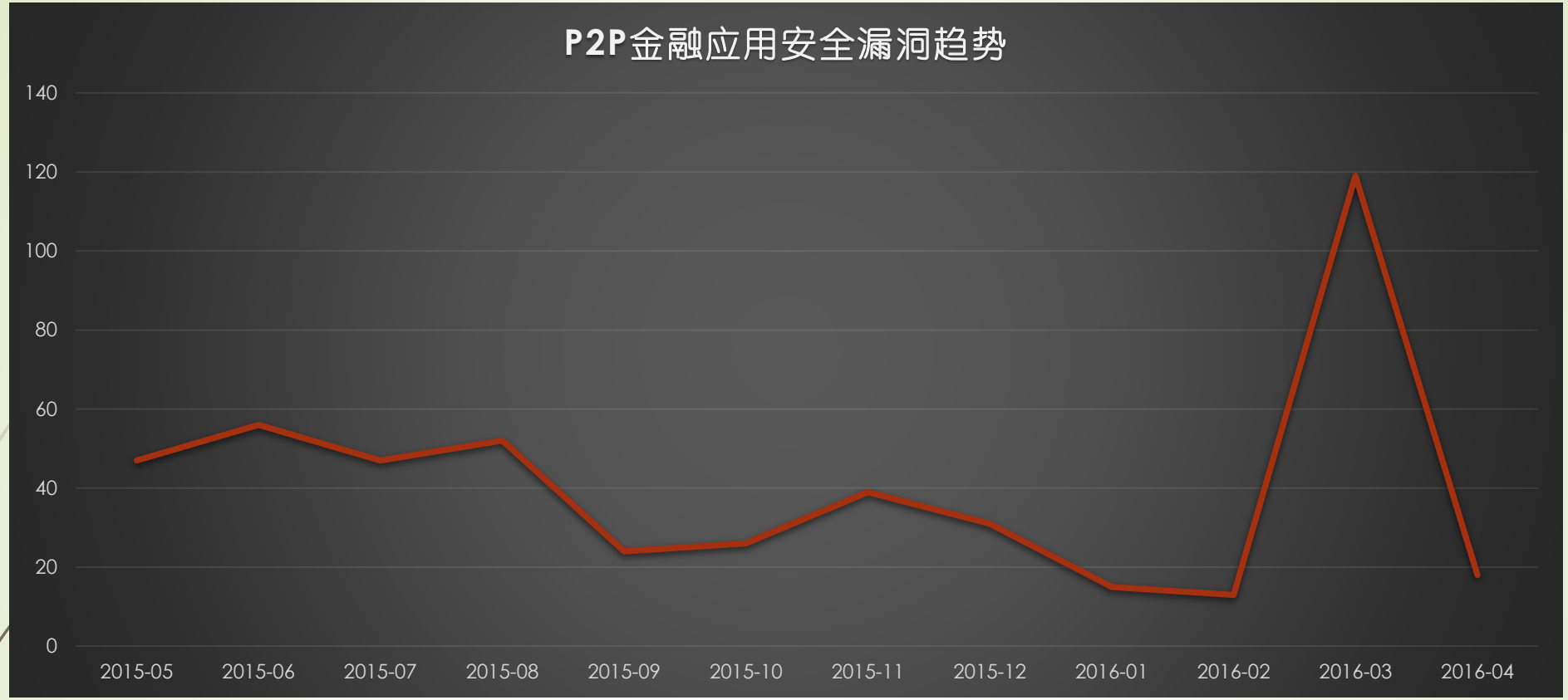
About Me

- ID: 安全小飞侠
- 安全工程师，目前就职于某国外电商企业的信息安全部
- 微信：<右方二维码>
- Github： https://github.com/brianwrf
- 个人博客：http://avfisher.win/

随着智能手机、平板等移动设备的出现和普及，我们已经进入了移动互联网时代。因为自身业务扩展的传统的金融行业以及移动时代产生的互联网金融衍生品如雨后春笋般地出现，但是随之而来的安全问题也接踵而至。



个人金融安全吗？



wooyun	2016-04-08 11:40:32	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-20
wooyun	2016-04-07 22:55:33	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-20
wooyun	2016-04-07 18:55:31	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-2016-
wooyun	2016-04-07 18:10:31	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-2016-
wooyun	2016-04-07 10:35:31	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-20
secpulse	2016-04-07 09:43:02	P2P金融安全之	http://www.secpulse.com/archive
secpulse	2016-04-07 09:43:01	p2p金融安全之	http://www.secpulse.com/archive
secpulse	2016-04-07 09:43:01	P2P金融安全之	http://www.secpulse.com/archives/
wooyun	2016-04-07 09:25:30	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-20
wooyun	2016-04-06 19:05:32	P2P金融易容恒信	http://www.wooyun.org/bugs/wooyun-2016-
wooyun	2016-04-06 18:35:30	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-2016-
wooyun	2016-04-05 17:20:32	P2P安全之乐豆	http://www.wooyun.org/bugs/wooyun-2016-
wooyun	2016-04-05 15:20:31	P2P安全之永利	http://www.wooyun.org/bugs/wooyun-2016-
wooyun	2016-04-04 22:20:31	P2P安全之看门	http://www.wooyun.org/bugs/wooyun-2016-
wooyun	2016-04-04 13:50:32	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-2016-
wooyun	2016-04-02 16:55:31	P2P金融安全之	http://www.wooyun.org/bugs/wooyun-2016-

网页 **新闻** 贴吧 知道 百科 图片 视频 地图 文库 更多»

找到相关新闻约52,900篇 新闻全文 新闻标题 | 按焦点排序

男子误点短信链接银行卡被盗刷11万 骗子回扣拿三成
新浪财经 20小时前
王某某称,他以帮人盗刷银行卡提现牟取不法利益,每次获取提现金额的三成作为回扣。但诈骗短信不是他们发出的,他们只是通过网络与上家联系。 诈骗短信发送人 网上... 72条相同新闻 - 百度快照

最低4.88元,能保1万元银行卡盗刷
网易新闻 16小时前
此外,为了向银行证明被境外盗刷时,信用
ATM上使用该卡,必要时,银行可以调取你
6条相同新闻 - 百度快照

央视揭密银行卡盗刷产业链:5分钟
腾讯财经 2016年04月10日 16:00
央视揭密银行卡盗刷产业链:5分钟网上买
以上两种获取信息的方式,记者发现黑市
338条相同新闻 - 百度快照

揭秘银行卡盗刷黑色产业链 网上可
新浪安徽站 8小时前
揭秘银行卡盗刷黑色产业链 网上可买上
子已经形成了一条黑色产业链!他们先是
10条相同新闻 - 百度快照

网页 **新闻** 贴吧 知道 百科 图片 视频 地图 文库 更多»

找到相关新闻约109,000篇 新闻全文 新闻标题 | 按焦点排序

南昌又有3家P2P网贷平台"跑路"
网易新闻 17小时前
(原标题:南昌又有3家P2P网贷平台"跑路") 随着"互联网+金融"的兴起,通过网络平台为借款人与出借人之间建立桥梁的P2P公司也大行其道。然而,由于缺乏相关法规...
17条相同新闻 - 百度快照

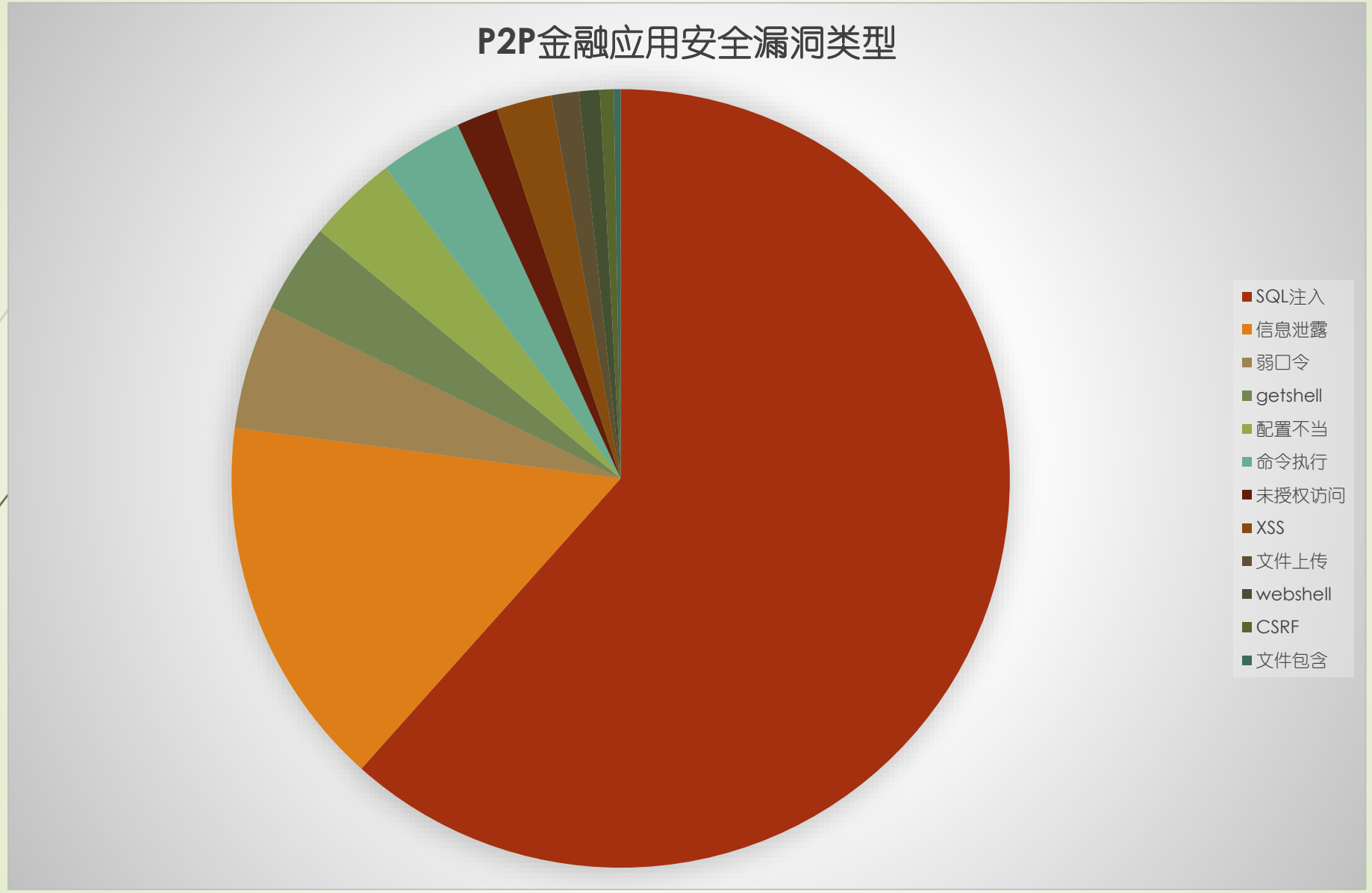
又一个理财平台倒塌 P2P跑路旁氏骗局都怎么来的?
好买理财 13小时前
本文转自微信公众号:P2P网贷圈 首先我们要问的问题...又一个理财平台倒塌 P2P跑路旁氏骗局都怎么来的? ...其实看财富管理公司是否是骗子公司,很简单的,主要总结...
4条相同新闻 - 百度快照

深圳:网贷平台被指跑路 投资者受损
人民网 8小时前
深圳:网贷平台被指跑路 投资者受损相关视频 精彩推荐上一页 下一页 雾霾天来碗南瓜盅 PTV新闻 雾霾天来碗南瓜盅PTV新闻 依靠手机一天内找到两位走失老人 PTV新闻... 百度快照

问题到底出在哪里呢？


企业
个人
监管

- 企业安全漏洞频发
- 个人安全意识薄弱
- 监管制度不健全
- ……


P2P金融应用安全漏洞类型
SQL注入
信息泄露
弱口令
getshell
配置不当
命令执行
未授权访问
XSS
文件上传
webshell
CSRF
文件包含

漏洞概要

关注数(0) 关注此漏洞

缺陷编号： WooYun-2015-14[illegible]7
漏洞标题： P2P安全之[illegible]存在SQL注入
相关厂商： [illegible]
漏洞作者： miracle
提交时间： 2015-10-02 14:49
公开时间： 2015-11-16 14:50
漏洞类型： SQL注射漏洞
危害等级： 中
自评Rank： 8
漏洞状态： 未联系到厂商或者厂商积
漏洞来源： http://www.wooy
Tags标签： 无
分享漏洞： 分享到

漏洞详情

披露状态：

2015-10-02： 积极联系厂商并且
2015-11-16： 厂商已经主动忽略

漏洞概要

关注数(0) 关注此漏洞

缺陷编号： WooYun-2015[illegible]77
漏洞标题： P2P安全之[illegible]系统后台弱口令(会员信息/贷款信息/财务信息)
相关厂商： [illegible]
漏洞作者： 路人甲
提交时间： 2015-12-26 21:28
公开时间： 2016-02-08 18:23
漏洞类型： 后台弱口令
危害等级： 高
自评Rank： 20
漏洞状态： 未联系到厂商或者厂商积极忽略
漏洞来源： http://www.wooyun.org
Tags标签： 弱口令 管理后台对外 敏感[illegible]足
分享漏洞： 分享到 0

漏洞详情

披露状态：

2015-12-26： 积极联系厂商并且等待厂商
2016-02-08： 厂商已经主动忽略漏洞，细

漏洞概要

关注数(4) 关注此漏洞

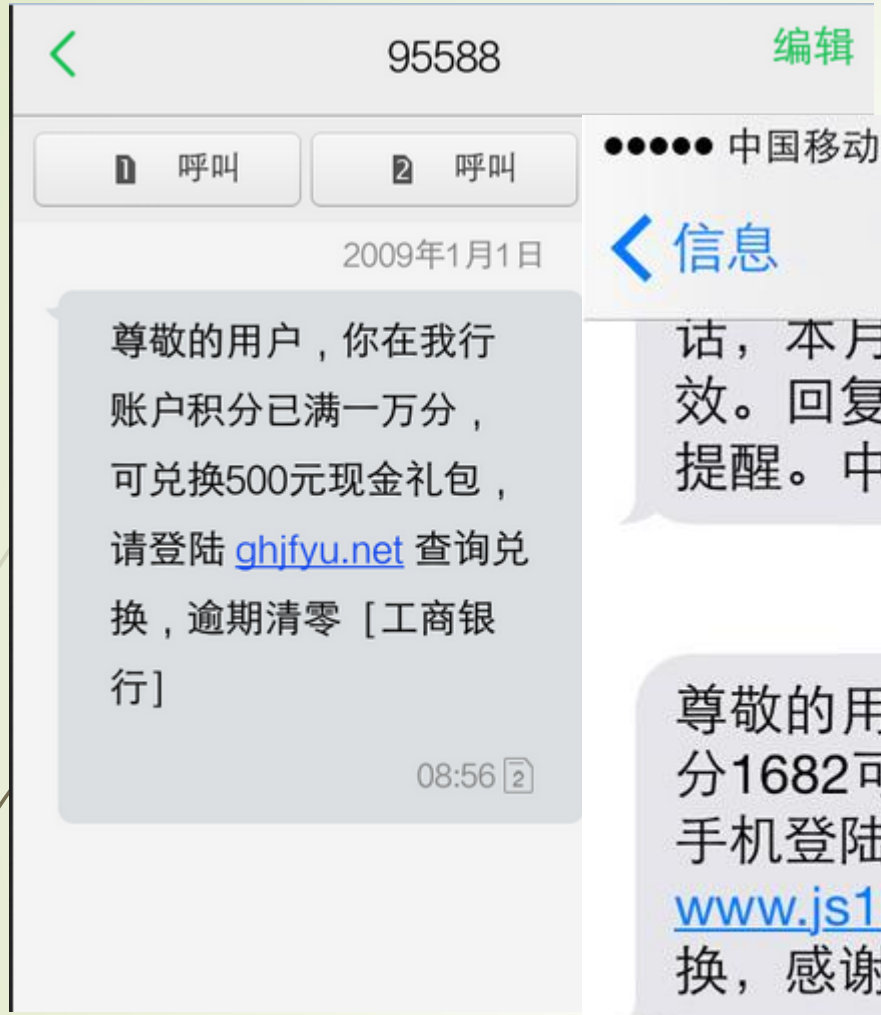
缺陷编号： WooYun-2015-[illegible]
漏洞[illegible]之mongodb未授权导致平台个人敏感信息泄露（薪资情况等）
企业应用安全漏洞
相关厂商： [illegible]
漏洞作者： myhalo
提交时间： 2015-07-06 17:26
公开时间： 2015-08-21 09:48
漏洞类型： 未授权访问/权限绕过
危害等级： 高
自评Rank： 20
漏洞状态： 厂商已经确认
漏洞来源： http://www.wooyun.org，如有疑问或需要帮助请联系 help@wooyun.org
Tags标签： 无
分享漏洞： 分享到 0

0人收藏 收藏

漏洞详情

披露状态：

2015-07-06： 细节已通知厂商并且等待厂商处理中
2015-07-07： 厂商已经确认，细节仅向厂商公开


95588
编辑
呼叫
呼叫
2009年1月1日
尊敬的用户，你在我行账户积分已满一万分，可兑换500元现金礼包，请登陆 ghjfyu.net 查询兑换，逾期清零［工商银行］
08:56


中国移动
10:36
24%
信息
10086
详细信息
话，本月申请，下月生效。回复QXYYTX可取消提醒。中国移动
昨天20:37
尊敬的用户：您的话费积分1682可兑换168.2元。请手机登陆 www.js10086s.com兑换，感谢您的支持！
今天10:33


4.0K/s
21:37
中国移动(1)
10086
短信/彩信
2014-12-18 16:14
尊敬的用户,您的积分已到账,请您尽快登录移动商城 10086.vip3mn.cn 兑换249.36元现金,以免积分过期失效！

一万积分可兑换五百现金？ 骗子假冒建行小心中招

金融界网站 2015-11-08 05:35:37 阅读(663) 评论(0)

声明：本文由入驻搜狐公众平台的作者撰写，除搜狐官方账号外，观点仅代表作者本人，不代表搜狐立场。 举报

“你的账户已满一万积分，可兑换5%现金，请登录手机网www.ccbalu.com查询兑换。”6日，哈市李女士向本报反映，在填写兑换信息时，对方竟让输入取款密码。庆幸的是李女士及时识破骗局，她提醒广大市民不要上当受骗。

5日，李女士收到中国建设银行(601939,买入)“95533”发来的信息，称积分可兑换现金。“我确实有一张建设银行的储蓄卡，里面的积分也有一万多，当时没多想就打开了网址链接。”李女士点击“储蓄卡用户”按钮后开始输入信息，“上面不仅要输入注册卡号，还要填取款密码，这样不是很容易就把银行卡里的钱取走了吗？”李女士马上上网搜索，发现已有一些外地市民被骗，幸好自己及时发现。

记者向建行95533客服人员咨询，客服人员表示：“95533从未发送过含网站链接的积分兑现或额度调整的短信。”

扬子晚报网 www.yangtse.com

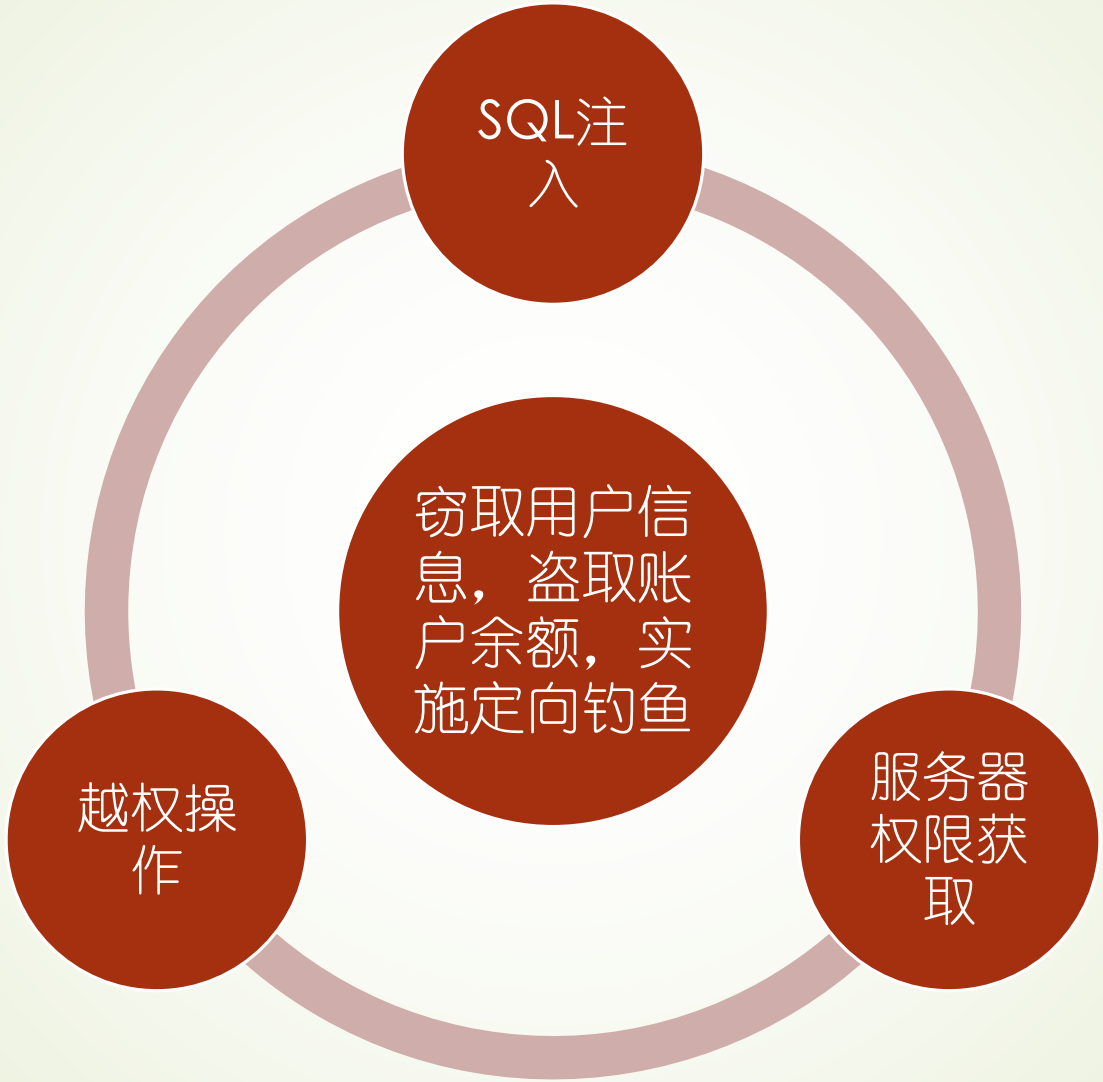
“10086”叫你积分兑换现金 轻信钓鱼网站被骗1200

来源: 扬子晚报网 发布于：2015-05-27 16:19:24

安全圈有句名言：未知攻，焉知防！

那么黑客通常是怎么攻击我们的呢？

应用漏洞攻击



撞库攻击

某邮箱数据库泄露

整理用户名和密码

对其他网站实施撞库操作

获取成功登录的账户信息

窃取个人资料，盗取金融账户余额，实施定向钓鱼攻击

蛮力攻击

借助搜索引擎或者社工库获取用户相关的个人信息

利用社会工程学和弱密码字典生成爆破密码字典

对其金融账户网站或者应用进行蛮力破解

获取成功登录的账户信息

窃取个人资料，盗取金融账户余额，实施定向钓鱼攻击

钓鱼攻击


架设伪基站
发送钓鱼短信
打开钓鱼链接
诱骗输入银行卡号和密码
下载短信拦截软件
获取短信验证码
盗取金融账户余额
架设钓鱼WiFi
伪造常见WiFi热点
诱骗用户连接钓鱼WiFi
劫持所有流量数据
提取敏感信息
盗取个人信息或金融账户余额

作为企业怎么才能抵御外部的安全威胁将显得尤为重要！！！

内网安全

- 生产网络：网络隔离，防火墙，IPS，监控，安全加固等
- 办公网络：WiFi，反病毒，补丁更新，OA，邮件系统，VPN等
- 内部人员安全意识

业务安全

- 风控系统
- 支付安全
- 第三方安全评估

产品安全

- SDL：设计，代码审计，黑盒测试，威胁建模（STRIDE）等
- 攻防：渗透测试，漏洞扫描等
- 防护体系：WAF，DDoS，防篡改等
- 应急响应流程

说完企业，那么我们自己又该如何保证个人的金融安全呢？

- 不使用相同的密码，比如利用PasswordSafe来管理密码
- 不使用弱密码以及姓名，生日，手机号，QQ号，身份证号等的组合密码
- 不点击任何不信任链接并养成检查链接URL的习惯
- 不轻易在互联网上透露个人的资料信息
- 下载官方渠道发布的手机APP并及时更新补丁
- 尽量避免连接非信任的WiFi热点，若必须连接，不要进行网购或者转账等操作
- 多关注最新的安全漏洞信息，比如国内各家漏洞平台WooYun，补天，漏洞盒子等等

P2P金融安全之
来源: wooyun时间: 2016-04-07 22:55:33

P2P金融安全之 手机号密码重置
来源: wooyun时间: 2016-04-07 18:55:31

P2P金融安全之 发起人资料泄露
来源: wooyun时间: 2016-04-07 18:10:31

P2P金融安全之 用户个人信息侧绕过验证机制
任意身份申请住卡任意身份申请贷款来源: wooyun时间: 2016-04-07...

P2P金融安全之 处重置登陆/交易密码等缺陷
来源: secpulse时间: 2016-04-07 09:43:02

最后，我想说的是，移动时代的金融安全不仅仅是企业和个人的责任，健全监管制度亦刻不容缓！！！

The End

谢谢大家！