SECURITY NSFOCUS

2014 绿盟科技互联网金融安全报告

2014 Internet Finance Security Report

Content

执行摘要

互联网金融安全状况堪忧。据不完全统计，截至 2014 年底，已有近 165 家 P2P 平台由于黑客攻击造成系统瘫痪、数据被恶意篡改、资金被洗劫一空等。目前很多 P2P 平台整体安全技术水平跟其业务的风险性不相匹配，缺乏专业、核心的防范黑客攻击技术，给了黑客乘虚而入的机会，如何提升平台安全能力成为亟待解决的问题。中国人民银行原副行长、著名经济学家吴晓灵表示："根据世界反黑客组织的最新通报，中国 P2P 已经成为全世界黑客宰割的羔羊"。

互联网金融异军突起。2015 年 3 月 5 日，十二届全国人大三次会议盛大召开。李克强总理在《政府工作报告》中多次提到互联网金融，明确指出"互联网金融异军突起"，并提出要"促进互联网金融健康发展"。 民建中央向全国政协提交的关于进一步规范与发展我国互联网金融的提案，列出互联网金融行业存在的六大突出问题，其中安全性是其中一个重要方面。

近几年互联网金融行业新上线的系统非常多，绿盟科技 NSTRT 安全团队收集了在 2014 年互联网金融行业中的 134 份安全漏洞报告，并对漏洞类型和数量做了统计，报告中的主要观点如下：

- 观点 1：互联网金融安全敲诈事件攀升，利益驱动明显。
- 观点 2：安全漏洞呈现部分集中化，个别漏洞非常普遍。
- 观点 3：互联网金融行业入行门槛过低，安全开发重视不足。
- 观点 4：开发安全管理落后导致漏洞修复成本过高。

如果您需要了解更多信息，请联系：

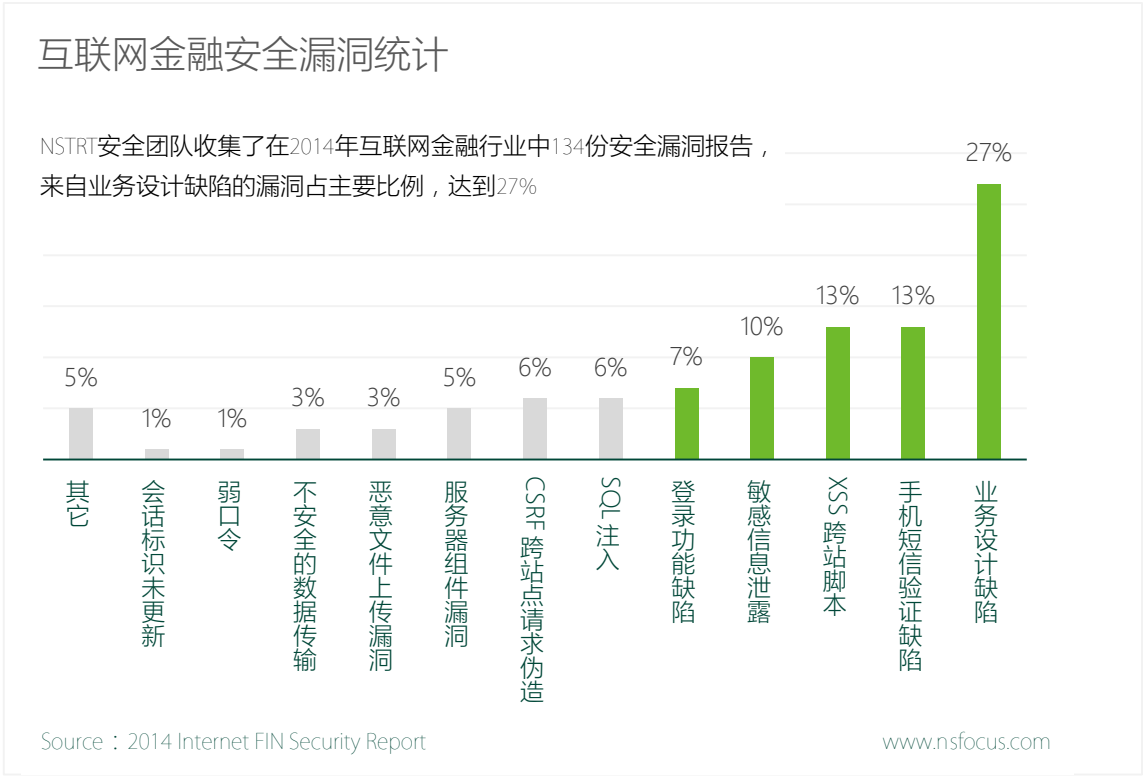
NSTRT 团队微博 http://www.weibo.com/u/5384465169

NSTRT 微信号 搜索公众号 trt917

安全风险分析

安全漏洞

按照漏洞类型的分类和数量统计，我们得出了最常见的 12 种漏洞类型，漏洞类型按照数量和风险值进行叠加后排序，得出如下漏洞数据分布：



安全漏洞分析

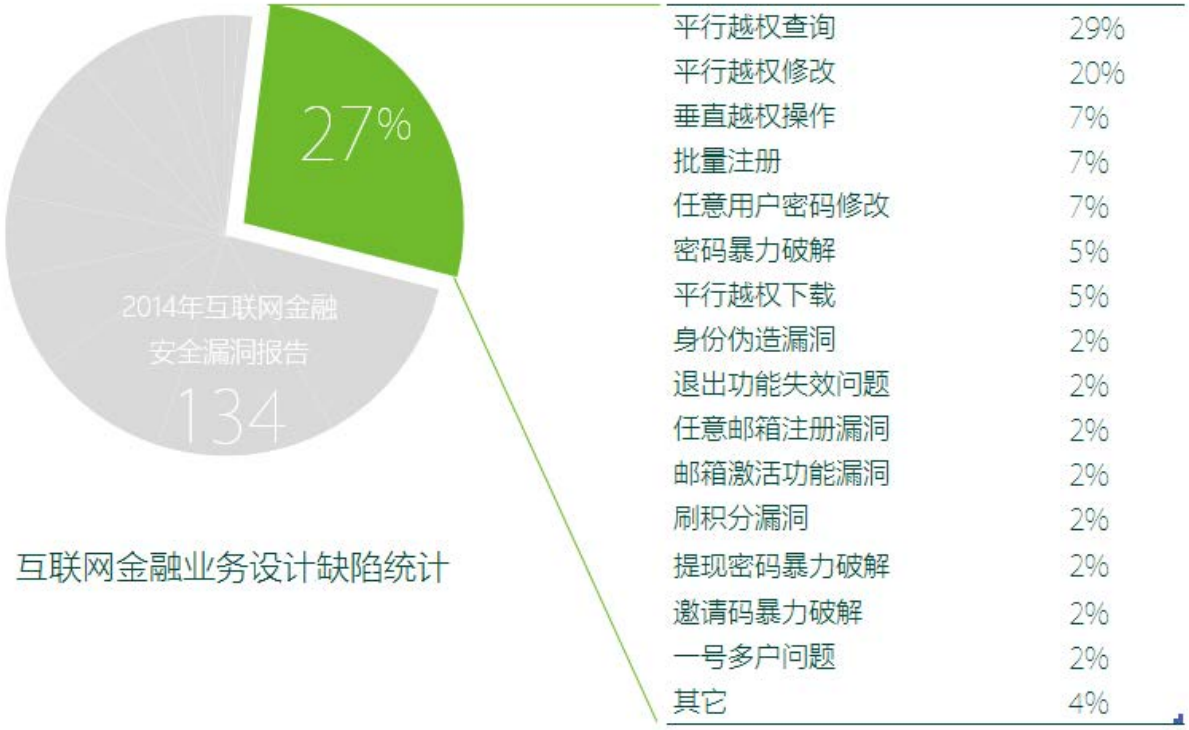
从上面的图表中可以看到，在漏洞统计结果中，除了常见的一些如注入、跨站、CSRF、恶意上传等 Web 漏洞外，部分金融平台在业务功能设计上存在着严重的风险，如任意用户密码重置、交易参数恶意篡改等，与常见的注入、恶意上传不同，这些业务逻辑的漏洞不会直接影响服务器的安全，但却会直接影响用户的资金、账号的安全，其风险程度有过之而无不及，若被黑客所利用或被曝光，将严重影响业务数据安全和平台公信力。下面报告就常见的几种情况做简要分析解读：

业务设计缺陷造成的风险最高

所谓业务设计缺陷造成的风险，是为区别于那些通用的常规安全漏洞。常规漏洞包括 SQL 注入、XSS 跨站脚本漏洞、系统命令执行漏洞、溢出漏洞等。业务设计缺陷造成的漏洞一般与系统业务挂钩，在漏洞的利用代码上无明显的攻击特征，也就难以用通用的 Web 应用防护设备（例如 WAF）来进行防护。在所有漏洞类型中，因业务设计缺陷造成的安全风险占的比重高达 27%。常规的安全漏洞大多数能够用 Web 应用防火墙等防护设施去进行防护，但是因业务设计缺陷造成的风险非常难以进行通用而全面的安全防护。因此对业务设计缺陷造成的安全风险防范和检测尤为重要。

业务设计缺陷分类统计

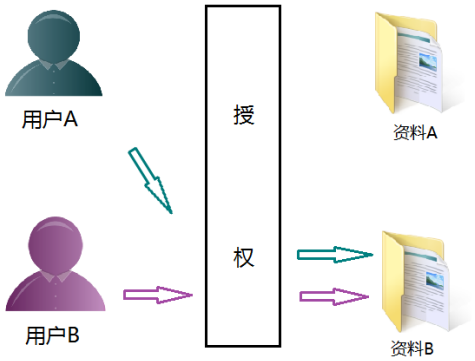
NSTRT 安全团队根据统计的类型和数量，列出了在互联网金融行业中比较常见的业务设计缺陷，并做了专门的典型案例介绍。值得一提的是，由于各个系统的业务有所差别，加上业务本身的复杂性，业务设计缺陷造成的漏洞可能是其它地方没有遇到过的，这些非常少见的漏洞也难以进行分类。最常见的一些业务设计缺陷分类统计如下表格：



平行越权查询	29%
平行越权修改	20%
垂直越权操作	7%
批量注册	7%
任意用户密码修改	7%
密码暴力破解	5%
平行越权下载	5%
身份伪造漏洞	2%
退出功能失效问题	2%
任意邮箱注册漏洞	2%
邮箱激活功能漏洞	2%
刷积分漏洞	2%
提现密码暴力破解	2%
邀请码暴力破解	2%
一号多户问题	2%
其它	4%

平行越权问题是指相同权限等级的不同用户之间可以越权获取或操作他人的数据。根据漏洞数量的统计结果，在所有业务设计造成的缺陷中，平行越权问题几乎占到了一半。平行越权问题主要包括平行越权查询、平行越权下载、平行越权修改这三种。

以越权查询为例，在很多的场景下，开发人员在设计用户查看本人信息的功能时，服务端会检查用户是否为登录状态，进而判断用户是否具有查看信息的权限。在这样的设计下，开发人员只考虑了用户是否具有查询权限或是否为登录状态，但没有考虑用户查询的具体内容是否与用户的权限匹配，由此造成了用户可能查询到其它人员的信息。

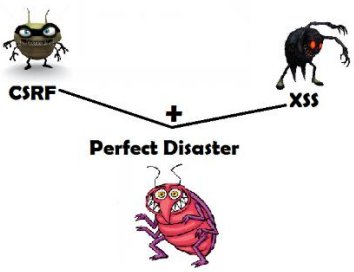


平行越权问题虽然原理上并不复杂，但是金融行业中非常常见。此类风险如此常见，安全开发意识不足是一个原因，另一方面原因是这种业务逻辑问题无法使用 Web 应用防火墙等设备来进行防护。要解决这类安全风险，还要从业务安全设计和安全编码两个方面抓起。

XSS 是最常见的安全漏洞

在每年的 OWASP TOP 10 中，跨站脚本漏洞（即 XSS）多年来一直名列前茅。在互联网金融行业中也不例外，在各种常规漏洞中，XSS 是出现频率最多的漏洞类型，占到了 13%。其中主要包括反射型 XSS 和存储型 XSS。

跨站脚本漏洞可能会导致网页挂马、用户权限被盗用、钓鱼攻击等多种安全风险。



值得一提的是，CSRF（跨站点请求伪造漏洞）也比较常见，在所有漏洞数量中占了 6%。在真实的攻击中，CSRF 往往会结合 XSS 来一起利用，进而形成巨大的威力。在很多情况下，利用一个存储型 XSS 加上一个 CSRF 漏洞，能够在短时间内对大量用户进行攻击，攻击效果非常明显。

短信验证是最易受攻击的安全功能

在统计中高风险漏洞中，与手机短信相关的漏洞占比高达 13%。在所有安全功能中风险最高。手机短信验证功能是一个系统为了验证用户身份而增加的安全功能，但是这个安全功能本身却带来了一些直接的安全风险。在手机短信验证功能出现的风险类型中，最常见的有手机短信炸弹、手机短信验证流程绕过、手机短信破解、手机短信重复利用这几个问题。

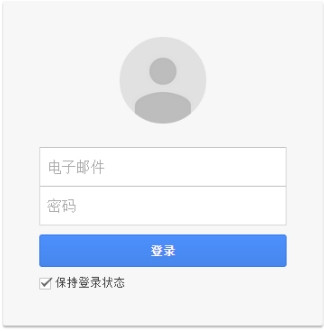
用户登录功能也是安全重灾区

在互联网金融系统中，用户登录功能是一项重要的系统安全功能之一，也是账号安全的第一道防线。遗憾的是，这一防线在很多地方都不够强大，导致攻击者往往能够有机会突破这一防线，形成各种各样的攻击。

用户登录功能处常见的安全风险主要包括暴力破解、登录流程绕过、用户信息泄露、批量账号锁定等。

大多数地方的用户登录功能都有各种类型的验证码校验，但是根据统计发现，很大一部分的登录验证码校验存在安全缺陷，导致攻击者可以绕过验证码进而执行暴力破解。

在大量用户信息被泄露的今天，账号的安全非常重要。在之前大量用户数据泄露之后，暴力破解用户账号密码的成功率越来越高。因此，账号和登录的安全值得我们重视。



互联网金融开发安全分析

互联网金融安全领域还不成熟

考虑到互联网金融行业的门槛低，效益高的特点，互联网金融行业在近几年呈大幅度的增长态势。在金融行业，银行使用的各种网银系统都已经经过了多年的安全检测，在安全性上已经有了明显的进步。但是互联网金融的各个平台都还比较年轻，很多企业还没有对自己的安全风险有足够的认识。例如：2014 年上半年， 国内互联网安全问题反馈平台乌云曝出某 p2p 平台系统存在严重安全漏洞，称"系统任意上传漏洞涉及涉及金钱交易数千万"，据统计，该漏洞涉及的国内网贷平台不少于 15 家。

互联网金融的研发团队大多都是新建立的团队，开发规范不够健全，开发人员的经验和安全意识也大多参差不齐。

紧急项目增加安全风险

有很多企业在进入互联网金融行业的时候，没有给系统的开发预留足够多的时间，导致出现了大量的快速开发现象。安全分析是一项需要耐心而又细致的工作。快速开发可能会导致开发人员为了进度而放弃安全上的考虑。同时，在进度的压力下，测试人员更多的会考虑系统的可用性，在安全上的测试则难以顾及。

互联网金融安全开发保障

我们不仅希望自己更少遇到风险，更希望自己遇到风险之后能够有足够强的能力应对。针对一个企业来说，开发人员应该通过安全培训来具备足够强的安全风险意识和安全开发能力。对于企业的安全管理，应该要具备一套健全的安全开发规范制度和系统上线运营安全流程。在一个互联网金融的项目上线之前，应该做好完善的安全准备，建立各个层面的安全防线，从项目的各个阶段引入安全控制，从源头上来避免安全风险。一个完善的开发项目应该引入 SDL（Security Development Lifecycle，安全开发生命周期）流程，从安全风险管理的视角来避免安全风险。

SDL 从需求阶段、设计阶段、实施阶段、测试阶段和发布响应阶段来引入安全管理。SDL 的各个阶段相关内容可参考下图：

互联网金融安全防御

在各种类型的安全漏洞中，大多数常规的安全漏洞（例如 XSS、SQL 注入等）能够使用 Web 应用防护设备等措施来进行通用的防护，但是业务设计缺陷造成的漏洞无法用这些措施来进行通用的防护，唯一解决方案就是从设计上避免它、在代码上修复它。

为了让互联网金融的研发团队能够避免重蹈覆辙，绿盟科技 NSTRT 报告曾经对最常见的一些业务设计缺陷做了详细的介绍[①]，并一一给出了对应的防护方案，这里提要如下：

越权漏洞代码防护

针对平行越权漏洞，我们建议让访问和操作的对象增加用户属性，当对目标对象进行访问和操作时，服务端对会话和对象的用户属性进行校验，通过校验后再执行读取和操作。

针对垂直越权漏洞，我们建议使用默认拒绝所有的访问机制，然后对于每个功能的访问，-明确授予特定角色的访问权限，同时用户在使用该功能时，系统应该对该用户的权限与访问控制机制进行校对。

任意用户密码修改

针对重置密码功能中的任意用户密码重置问题，首先要保证短信验证码校验功能本身的安全，给随机验证码的认证次数设定限制，当认证超过次数限制则使当前验证码失效。其次，要保证短信验证码的验证流程不会被绕过，在短信验证通过之后重置密码操作时，需要从服务端会话信息来判断用户是否经过了短信验证码的校验。最后，要保证重置密码功能不能被换位使用，重置密码的目标账号不能从客户端参数中获得，而应该从服务端会话信息中获得。

① http://www.freebuf.com/news/special/61082.html，《金融行业平台常见安全漏洞与防御》

恶意注册代码防护

恶意注册漏洞一般是由于手机短信或邮箱认证功能存在缺陷或能被恶意利用导致。在设计注册功能时，要注意对手机短信或邮件的错误认证次数设置限制。尤其要注意邮箱认证内容要具备不可预测性。在经过手机或邮箱认证后，要保证注册的目标账号为会话中保存的认证的手机或邮箱。

恶意短信代码防护

针对恶意短信类的安全问题，我们建议可以通过以下 3 种方式进行防护：

1、 从服务端限制每个号码的发送频率和每天的发送次数，防止攻击者利用短信接口进行恶意轰炸。

2、 在发送短信之前要求经过图形验证码的认证，防止攻击者遍历手机号来发送短信。

3、 发送短信的内容应直接由系统内部进行定义，客户端可通过数字或字符的方式，对所需要发送的内容进行选择，如 messagetype=1 为密码找回，messtype=2 为注册，然后通过数字来索引要发送的内容。

结束语

在曾经很长一段时间，金融行业中最典型的网银系统经历了多年的安全教训和考验。如今，我们欣然看到多年前那些常见的高危漏洞在网银系统中已经很难被发现。

曾几何时，互联网金融浪潮给金融行业带来了一轮新的风雨。它比网银系统更加开放和多样化，自身风险更高，防护起来更加复杂。2014 年的各大安全事件让我们认识到，在商业利益驱动下，风险来得比大家想的还要快。

捻乱止于河防。在 2014 年对互联网金融行业的信息安全领域依然缺乏足够的监管，但我们相信，在各方的努力下，互联网金融行业一定能够变得安全、健康。

您还想看什么内容？

您可以联系报告作者，将您的见解与我们分享，如果您有更多想看的内容，也可以告诉我们，在这里先行致谢！

请致函 laidongfang@nsfocus.com

作者和贡献者

作者

赖东方	Email：laidongfang@nsfocus.com	绿盟科技 TRT 代码安全组长、负责开发安全研究。
张佳发	Email：zhangjiafa@nsfocus.com	绿盟科技 TRT leader、负责团队建设和攻防研究。

贡献者

侯俊	Email：houjun@nsfocus.com	绿盟科技深圳办技术经理
吴昊	Email：wuhao2@nsfocus.com	绿盟科技广州分公司安全顾问

NSTRT Report

TRT 成立于 2002 年，是绿盟科技华南大区的安全技术研究团队，目前有十多名核心技术研究员和大量的安全成员，长年致力于移动终端安全、高级渗透测试、代码审计、SDL、工控安全、逆向工程、智能终端及物联网安全等领域的安全研究，有深厚的技术积累和大量成果，这些成果将会不断的转化为报告的形式，与大家分享。

关注 NSTRT

NSTRT 英文全称为"Network Security Technology Research Team"，简称 TRT。TRT 紧跟安全界最新动态，不定期分享最新研究成果并公布到微信、微博及业界各媒体。

如果您希望与我们一起持续关注这个项目，请关注：

- 微博：NSTRT 团队　http://www.weibo.com/u/5384465169
- NSTRT 微信号　搜索公众号 trt917

- 绿盟科技官方微博　http://weibo.com/nsfocus
- 绿盟科技官方微信　搜索公众号 绿盟科技

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS