DBSEC
安 华 金 和

2015 年 10 月数据安全漏洞分析报告

目录

报告核心观点

为了提高广大用户的安全意识，国内专业数据库安全厂商安华金和，综合来自补天、乌云、漏洞盒子等漏洞平台高危数据安全漏洞，发布每日安全资讯，数据库攻防实验室（DBSec Labs）以月为单位，将数百个高危漏洞汇总，形成分析报告，分享广大用户及合作伙伴。

10 月报告核心观点

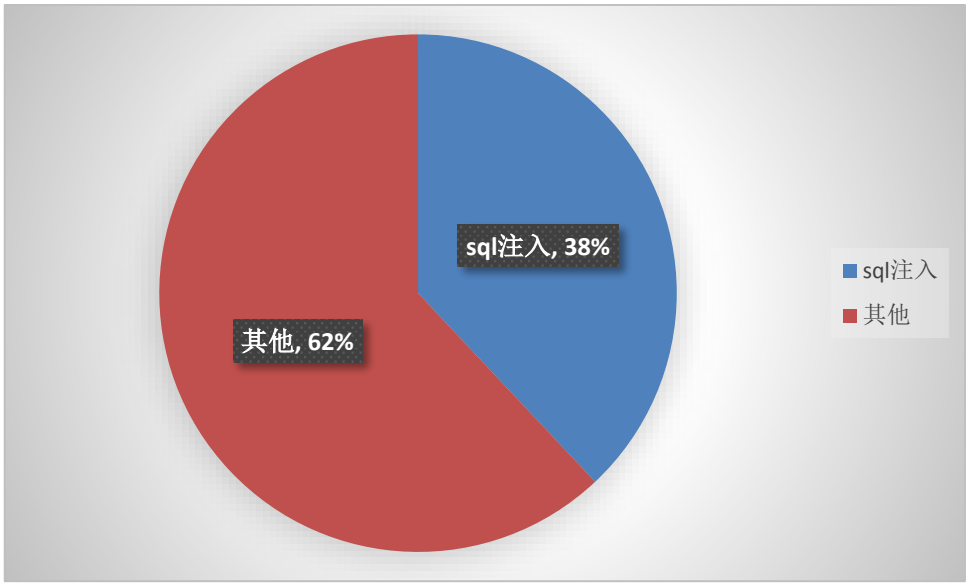
1. 格局不变，SQL 注入重回“王者”
2. 白帽子“独爱”政府，60 个漏洞
3. 10 月常见数据泄露原因分析
4. 从 SQL 角度防守 SQL 注入

报告正文

2015 年 10 月，安华每日安全资讯总结发布了 154 个数据泄密高危漏洞，这些漏洞分别来自乌云、补天、漏洞盒子等平台，涉及 8 个行业，公司机构、互联网、交通运输、教育、金融保险、能源、运营商、政府。同比 9 月份的 134 个，漏洞数量增加 20 个。10 月份的漏洞中，**SQL 注入漏洞数量占总量的 38%，重回“第一宝座”**。

格局不改，SQL 注入重回“王者”

数据安全问题多数是从 Web 端开始。10 月份 SQL 注入漏洞再次引爆新高潮，被白帽子挖掘出 58 个 SQL 注入相关漏洞，这些漏洞遍及公司机构、互联网、政府等 6 个行业。SQL 注入漏洞在 10 月份统计的漏洞总数中占据了近 4 成比例。

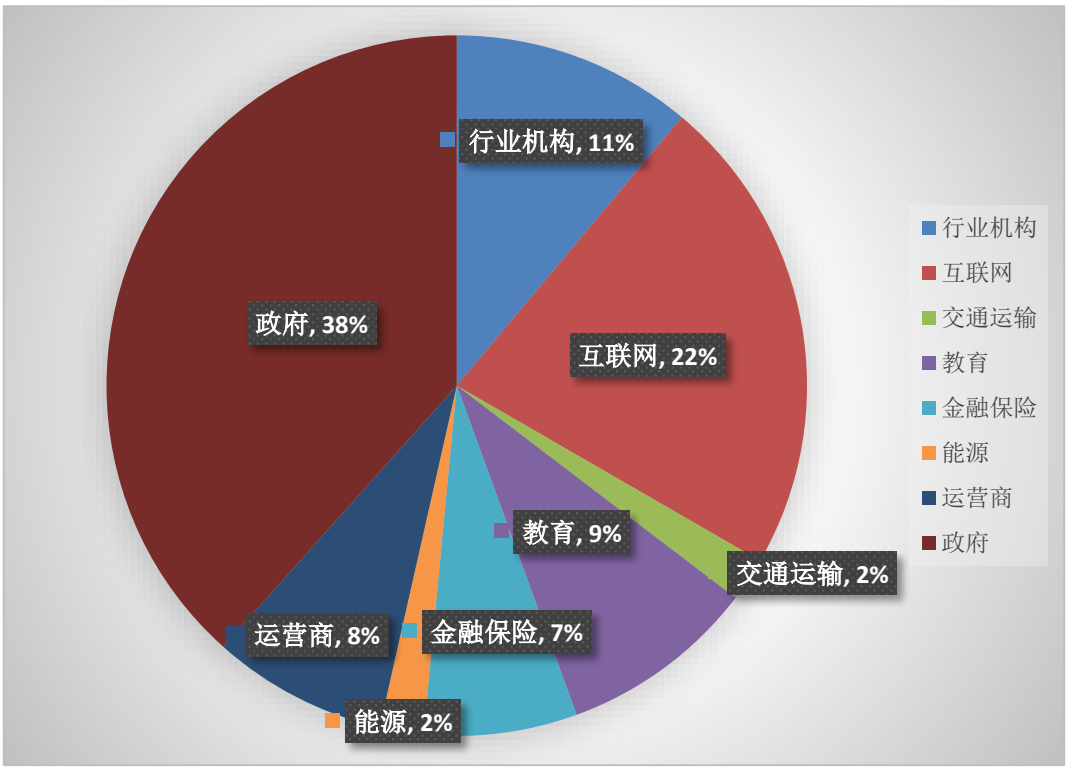


10 月平台 SQL 注入漏洞占主要比重

10 月的 SQL 注入漏洞与以往的 SQL 注入漏洞存在很大的不同点。以往 SQL 注入是由于平台缺乏对应的校验机制而导致注入成功。10 月的 SQL 注入案例中很多平台的后台存在 WAF，但入侵者绕过 WAF 进行 SQL 注入。这源于 WAF 的某些技术限制，确实存在一些手段可以绕过 WAF 进行 SQL 注入。

白帽子“独爱”政府，60 个漏洞显现

从 10 月 154 个受到数据泄露漏洞威胁的行业来看，政府、互联网、行业机构依旧是重灾区。10 月单月仅安华每日安全资讯统计出的 154 个高危漏洞中就有 60 个政府行业漏洞（包含了卫生医疗、教育、社保公积金几个子类）占比 38%，互联网行业占全部数据泄露威胁的 22%。行业机构紧随其后，漏洞比例占 11%。



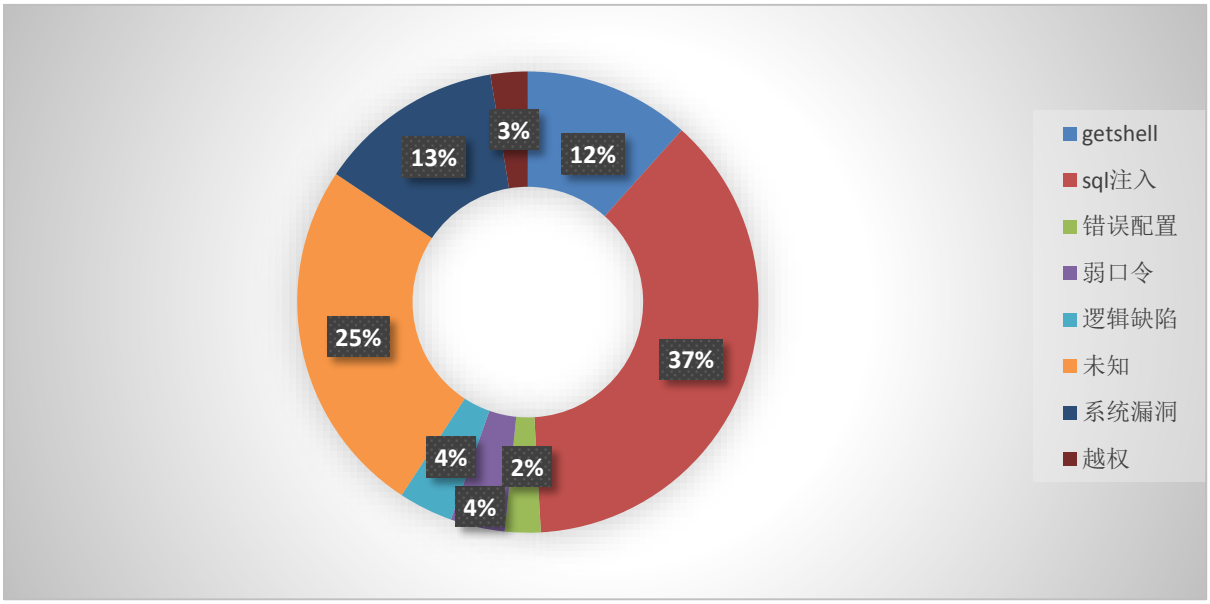
10 月数据安全漏洞行业分布情况

10 月政府行业漏洞数量暴涨，本月政府行业有 60 个漏洞,同比 9 月份的 43 个增加了 17 个，占整体漏洞总数的 38%。也是 9 月份以来三大高危行业（政府、互联网、行业机构）中，唯一漏洞数大幅攀升的行业。政府被集中爆出漏洞与自身网站的 WAF 策略配置有明显关系。政府漏洞中有 24 个漏洞是绕过 WAF 的 SQL 注入漏洞。60 个中还存在两个弱口令漏洞、三个配置错误漏洞，弱口令直接被白帽子用工具爆破出密码。相信通过合理的制度和一定的辅助工具弱口令和配置错误应该能够被杜绝。在企业机构、教育、运营商和互联网中，也存在上述问题。虽然本月平台系统漏洞有明显减少，但依旧活跃在各个行业。错误配置、弱口令等人为因素依旧没有杜绝。

10 月常见数据泄露原因分析

SQL 注入是一种常见的黑客入侵 WEB 应用服务器的手法。SQL 注入产生的根本原理在于 SQL 语言是一种解释型语言。解释型语言是一种在运行时由一个运行时组件解释语言代码并执行其中包含指令的语言。

SQL 注入正是基于解释型语言的执行方式产生的。解释器处理的数据实际上是由程序员编写的代码和用户提交的数据共同组成的。黑客向 Web 应用发送精心构造的输入，这个输入中的一部分被解释成程序指令，改变原来的程序判断的逻辑。最终黑客可能通过 SQL 注入获取 Web 应用的管理员权限和 Web 应用存在数据库中的大量敏感信息。



10 月份数据泄漏威胁主要原因

WAF 虽然在一定程度上可以对 SQL 注入进行防护，但往往需要在性能和防护效果上做权衡。让 WAF 处于这种尴尬境地的原因在于 SQL 注入是从 http 和 SQL 两个角度进行入侵的手法，而 WAF 主要针对 HTTP 协议进行解析。如果绕过的手法是出现在 SQL 语法中，WAF 无法知道 WEB 应用中生成用于访问数据库完整的 SQL 语句，无法针对访问数据库的 SQL 语句进行分析、识别，于是只能考虑采用关键字过滤等方式来进行禁止，这种一个一个封堵的方式难以遍历所有 SQL 注入情况，在防守上存在遗漏，如果大量使用正则匹配又会降低性能。产生这些问题的根源都在于 WAF 无法对访问数据库的完整 SQL 语句做分析、识别。

由于 WAF 采用的是正则匹配的方式，于是出现了以下 3 中常见绕过 WAF 的手段：

（1）.编码绕过

在大小写绕过的基础上开始出现编码绕过，主要出现了三种：URL 编码、十六进制编码、Unicode 编码。在浏览器中输入 URL 会进行一次 URL 编码，黑客会通过多次编码来进行 WAF 绕过，例如：Id.php?id=1%2520union/**/select，数据库得到的 Id.php?id=1 union/**/select。如果只解码一次得到的是 Id.php?id=1%20union/**/select，很有可能绕过 WAF 入侵数据库。针对这一问题可以采用多次循环解码来应对。其中 Unicode 编码种类很多，如果只是基于黑名单过滤，无法处理全部情况，其中 UTF-32 曾经实现过对 GOOGLE 的绕过。

（2）.注释绕过

不但可以采用编码改写关键字，还可以采用注释改写关键字，避免正则匹配。例如 z.com/index.php?page_id=-15 %55nION/**/%53ElecT 1,2,3,4 'union%a0select pass from users# 。就是用符号编码代替一部分字母和判定的空格来逃避正则匹配。（selectxxx 不会被拦截，因为可能是函数名等。select 空格 xxx 则一定会被拦截，去掉空格成为绕过的关键）。同样还有针对 MYSQL 版本的/*!5000union*/系列。

（3）.等价替换

等价替换是个比较大的分类，主要可以分为等价函数、等价符号、特殊符号、比较符号等 4 类。

等价函数，就是同功能函数替换。WAF 禁止了一些函数，但对另外一些函数没有禁止例如 Substring()可以用 mid()，substr()这些函数来替换。还将可以采用生僻函数迂回完成原函数的功能，进行 WAF 关键字绕过。and or 这种关键字在 PHP 中可以用|| 和&&代替。于是语句 id=1 or 1=1 就可以写成 id=1 || 1=来进行绕过。同样！= 、>、<等都可以代替等号进行绕过。

除去绕过关键字和关键符号外，最关键的是绕过空格。想各种方式避免空格出现。

例如 原句 id=1 or 1=1

可以写成 id=1+or+1=1

id=1%0bor%0b1=1

id=1--s%0aor--s%0a1=1

id=1/*!or*/1=1

id=1()or(1=1) 等多种形式进行尝试绕过

Waf 解决上述问题的方法基本是在特征库中添加更多的过滤项。越多的过滤项，越慢的性能。

从 SQL 角度防守 SQL 注入

WAF 擅长解析过滤 http 协议，不能对 SQL 语句进行整体分析。针对这个缺陷，可以在 WEB 应用和数据库之间加入数据库防火墙进行 SQL 部分的解析和过滤。数据库防火墙对从 WEB 应用发向数据库的 SQL 语句进行语法解析，可以理解 SQL 语句的真实含义，并做以下四点判断：

1. 语句是否含有明显的 SQL 注入特征；
2. 语句访问的对象是否属于该用户访问权限；
3. 语句调用的核心函数是否存在高危漏洞；
4. 限制语句的返回行数，把危险控制在最低限。

加入数据库防火墙后，数据库防火墙会在 WEB 应用和数据库之间获取 WEB 应用发送给数据库的 SQL 语句。通过拿到的 SQL 语句，按照不同数据库进行 SQL 协议解析。通过协议解析把应用发送的 SQL 语句还原成标准模式（去掉各种数据库兼容符号和特殊用法）防止黑客利用上述绕过 WAF 的手法绕过数据库防火墙进行 SQL 注入。首先还原后的 SQL 语句和黑名单中的禁止语句结构进行匹配，如果认为是威胁语句，则禁止该语句发送到数据库端，并通过发送短信、邮件等方式及时通知管理员进行处理；语句结构判断没有问题后防火墙接下来会对语句中的操作对象和谓词进行判断，如果对象或谓词有控制，则依旧禁止该语句发送到数据库端；即便绕过全部防护，SQL 语句被发送到数据库端，数据库防火墙还可以通过限制返回行数来减小数据外泄的损失。

结束语

在防御 SQL 注入上 WAF 的最大问题是无法对 WEB 发给数据库的 SQL 语句进行获取、分析。只能通过正则匹配来尽量保证遍历每种情况，即使这样也无法保证完全遍历。如果为了达到完全遍历而设置大量的正则匹配，会对性能产生严重影响。因为技术路线原因导致 WAF 无法克服这种自身缺陷，而数据库防火墙则恰好弥补了 WAF 的技术路线缺陷。数据库防火墙的防护策略、手段都是基于 SQL 协议解析而来。数据库防火墙在防止 SQL 注入上彻底的解决了 WAF 以牺牲性能为代价的方式，相信如果数据库防火墙和 WAF 配合使用会使我们的数据库更加安全。

为了实现让数据使用更安全的使命，安华金和作为专业的数据库安全厂商，有义务和责任为客户提供创新前沿与稳定的数据库安全防护产品与解决方案。

最后，也是最重要的，用户还是要从主观因素上提高安全意识，加强内部安全管理防范。安全就是这样一种形态，平时不出状况看不到安全的效果，一旦企业出现了数据泄露事件，其经济损失、名誉损失将不可估量，更甚者会使企业形象一落千丈。

10 月数据安全漏洞列表

行业	标题	来源	编号
互联网	饿了么(外/内网)网络边界可全漫游(已撕进 VPN)	乌云	WooYun-2015-130015
政府	吉林省人设厅某养老保险认证系统存在漏洞可 getshell 泄漏用户敏感信息姓名/身份证/电话等	乌云	WooYun-2015-144331
政府	厦门市人社局某系统漏洞可导致全市数十万已育妇女敏感信息泄漏	乌云	WooYun-2015-144265
金融保险	恒泰证券某站注入泄露 26 万用户信息	乌云	WooYun-2015-144337
能源	电力安全之江苏省电力监管系统 getshell 导致几十万用户信息公司/姓名/地址/电话等泄漏	乌云	WooYun-2015-144339
互联网	小组饭严重设计缺陷（可使用他人积分/可登陆任意账号）	乌云	WooYun-2015-134352

运营商	中国电信之翼实习某处修复不完全仍可SQL 注入（DBA 权限+几十万用户泄漏+你的简历信息我知道）	乌云	WooYun-2015-144422
运营商	某市电信商城某处 SQL 未修复完可继续注入（DBA 权限+十几万用户信息泄漏+弱密码可入后台）	乌云	WooYun-2015-144355
政府	山东省卫生厅某居民档案管理系统 getshell 已进服务器可泄露大量数据	乌云	WooYun-2015-144383
政府	吉林省某敏感系统信息泄露 get 至少 1359w 户籍信息	乌云	WooYun-2015-144413
公司机构	山西航天信息敏感信息泄露(邮箱/vpn/电话/oa 系统)	乌云	WooYun-2015-144479
公司机构	惠普系列安全漏洞之 PC 机篇二（涉及 110 多万客户敏感信息包括姓名/电话/住址/邮箱等）	乌云	WooYun-2015-144178
金融保险	泰山保险某车险系统漏洞导致泄漏大量报案等信息	漏洞盒子	vulbox-2015-011421
金融保险	广州股权交易中心多处 SQL 注入/root 权限/140 个表/支持 UNION	乌云	WooYun-2015-144209
能源	中国石油销量录入系统权限缺失导致账户泄露（用户名、密码、姓名、身份证号码等信息）	乌云	WooYun-2015-144207
交通运输	航空安全之均瑶集团旗下航空公司内网漫游(泄漏敏感信息\40W 用户信息\内部系统)	乌云	WooYun-2015-144679
金融保险	内蒙古某银行主站 SQL 注入（DBA 权限&23 库大量表）	乌云	WooYun-2015-144624
政府	无锡市车管所 SQL 注入漏洞导致大量车辆信息泄漏	乌云	WooYun-2015-144647
政府	青岛市黄岛区人力资源和社会保障局互动交流平台 SQL 注入漏洞	乌云	WooYun-2015-144613
政府	某省公安厅网上办事大厅某处存在 SQL 注入（DBA 权限+涉及 25 个数据库+大量数据可泄露）	乌云	WooYun-2015-144582
互联网	p2p 安全之融贝网 SQL 注入漏洞，绕过 WAF 注入(大量用户信息泄露)	乌云	WooYun-2015-144817
互联网	搜课网 SQL 注入影响 30 万学生数据	乌云	WooYun-2015-144714
交通运输	UCS 官网 SQL 注入可导致 3000w 快递单信息泄露	乌云	WooYun-2015-144783
金融保险	四川金融资产交易所 SQL 注入(2160 用户/可脱裤)	乌云	WooYun-2015-144722

政府	某市住房管理基金网站 SQL 注入(10 数据库/22 张表/上万用户信息)	乌云	WooYun-2015-144774
互联网	驴妈妈旅游网某站 SQL 注入（tamper 绕 WAF/DBA 权限/27 个库）	乌云	WooYun-2015-144854
互联网	糖果网逻辑漏洞（泄露所有用户家庭地址等信息、冒充用户，盗取所有用户余额）	乌云	WooYun-2015-144844
互联网	同程全资子公司某系统存在通用型 SQL 注入(DBA 权限)	乌云	WooYun-2015-144814
运营商	中国电信某站存在高危 web 漏洞，导致 getshell	漏洞盒子	vulbox-2015-011432
政府	内蒙古某市住房公积金管理中心存在 SQL 注射漏洞	乌云	WooYun-2015-144837
公司机构	美的某接口越权查看任意用户保修单信息（可影响大量数据）	乌云	WooYun-2015-145010
公司机构	格林豪泰酒店管理集团所有内部员工密码修改进而实现多个内部站点进入	乌云	WooYun-2015-135468
互联网	安心贷主站多 SQL 注入打包(基于时间盲注/涉及多库)	乌云	WooYun-2015-144976
互联网	泛华普益主站 SQL 注入漏洞（百万数据泄露）	乌云	WooYun-2015-144987
互联网	中国电子商务信用认证平台 SQL 注射/大量信息泄露	乌云	WooYun-2015-145020
公司机构	华为某处缺陷导致十几万员工信息泄露(姓名/手机/邮箱/座机/办公位置)	乌云	WooYun-2015-145247
互联网	快的打车某重要系统逻辑漏洞可泄漏大量用户敏感信息包括姓名/车牌号等	乌云	WooYun-2015-145246
教育	青海省某学籍系统存在漏洞，涉及众多学生信息	漏洞盒子	vulbox-2015-011445
金融保险	恒邦财产保险某站存在漏洞，泄露大量敏感信息	漏洞盒子	vulbox-2015-011443
政府	国家税务局某省重要系统 getshell 可导致数百万企业信息泄漏	补天	WooYun-2015-145165
互联网	pptv 一接口设计不当可导致撞库攻击	漏洞盒子	vulbox-2015-011476
政府	青岛市食药监督管理局某系统存在 SQL 涉及大量商户信息泄漏	乌云	WooYun-2015-145228
政府	新益华系统漏洞可危及河南全省医疗系统数亿的医疗补助数据及数千万的个人信息	补天	QTVA-2015-307328

政府	河北沧州某卫生平台漏洞泄露 2002 年至今数百万儿童信息#出生信息、父母、家庭地址信息等	补天	QTVA-2015-306578
政府	江苏省人力资源社会保障局数千万公民信息泄漏	补天	QTVA-2015-306497
互联网	酷米游科技某站高危漏洞打包，泄露百万用户信息	补天	QTVA-2015-309749
互联网	天象互动某站点配置不当#影响千万用户信息#千万短信记录	补天	QTVA-2015-306878
教育	福建省毕业生就业公共服务平台泄露 300 多万学生信息，任意账户登录，SQL 注入等	补天	QTVA-2015-309689
金融保险	某省保险协会某系统大量敏感信息泄露（涉及几十个保险公司/手机邮箱/红头文件/财务报表等）	乌云	WooYun-2015-145522
运营商	长城宽带某处上传漏洞，泄露千万用户数据，且涉及大量企业用户	补天	QTVA-2015-307334
公司机构	天津图书大厦网上商城天添网存在漏洞三处 SQL 注入打包	乌云	WooYun-2015-145842
教育	福建省毕业生就业公共服务平台 GETSHELL，1G 数据库全泄露，可直接下载	补天	QTVA-2015-309953
政府	延边人力资源和社会保障局旗下某站远程命令执行漏洞导致 getshell 并获得服务器权限	漏洞盒子	vulbox-2015-011536
政府	某敏感部门网上办事大厅另一端口多个参数存在 SQL 注入	乌云	WooYun-2015-145686
政府	山东省工商局漏洞随意办理业务百万企业备案数据及数百万企业法人详细信息	补天	QTVA-2015-310175
公司机构	中国石化某分公司运输系统 SQL 注入漏洞（DBA 权限/涉及 7 个数据库）	乌云	WooYun-2015-145880
公司机构	中国 500 强企业永煤集团内网沦陷#vpn 泄漏导致代理漫游内网#	补天	QTVA-2015-309776
互联网	下厨房 app 敏感信息泄露	漏洞盒子	vulbox-2015-011563
政府	平顶山市房管局多个系统弱口令+SQL 注入威胁公民信息安全（已 shell\数据库数百张表）	乌云	WooYun-2015-145954
政府	浙江省就业管理服务局某系统漏洞（超过百万学生姓名/身份证扫描件/银行卡号/手机泄露）	补天	QTVA-2015-310439

教育	河南省大中专毕业生就业信息管理系统默认管理员密码，泄露千万学生信息	补天	QTVA-2015-308501
政府	铜陵人社局漏洞，近千万数据泄漏	补天	QTVA-2015-310814
政府	陕西省工商局核心业务系统(多个数据库)沦陷可随意办理业务#危及数百万企业以及企业法人等非常详细信息	补天	QTVA-2015-310433
政府	某省国家税务局某系统 getshell 泄漏大量信息可内网渗透多个税务局系统	乌云	WooYun-2015-146038
政府	某 12345 市民热线系统 getshell 可泄漏全部用户信息如姓名/地址/手机号/所反映问题等	乌云	WooYun-2015-145987
互联网	成人用品网站趣网某漏洞可泄露 130W 用户订单(包含姓名\电话\地址以及买了什么东西等)	乌云	WooYun-2015-146381
教育	河南毕业生就业信息网某站 HTTP 头注入，涉及学生学位信息（DBA 权限）	乌云	WooYun-2015-146411
教育	辽宁省招生考试之窗 SQL 漏洞泄露百万信息	补天	QTVA-2015-310016
政府	宁夏人社厅系统漏洞千万公民信息危险(社保卡/金额/身份证/姓名/住址/医疗药品等数据)	补天	QTVA-2015-309422
政府	山东省教育厅高校毕业生就业网注入漏洞泄露近 5 年所有毕业生信息	补天	QTVA-2015-310358
公司机构	长安马自达汽车有限公司某论坛后台未授权访问/涉及 27W 会员数据	乌云	WooYun-2015-146710
互联网	内蒙古招生考试信息网某站漏洞大量数据泄漏，近千万个人详细信息	补天	QTVA-2015-307454
互联网	窝窝团某系统存在多处漏洞打包（7 处 SQL 注入、5 处越权等）可导致所有员工等信息泄漏	补天	QTVA-2015-311798
教育	山东大学 DAB 权限注射漏洞涉及 67 个库可至大量信息泄露	乌云	WooYun-2015-146744
金融保险	交通银行康联人寿某站点存在多处漏洞可导致全部用户保单信息泄漏（姓名、身份证、保险内容等）	补天	QTVA-2015-310961
互联网	中国教育在线教育百事通 SQL 注入一枚泄露 170W 用户信息	乌云	WooYun-2015-147063
互联网	山东高校毕业生就业信息网大量数据泄漏	补天	QTVA-2015-307841
政府	广州市食品药品监督管理局某系统存在 POST 注入以及后台管理弱口令	乌云	WooYun-2015-146933

政府	广西壮族自治区人民政府多台服务器存在多个漏洞、文件包含/弱口令/Getshell/远程命令执行/可提权/内网大量主机可导致漫游！	漏洞盒子	vulbox-2015-011676
政府	铜川市人力资源和社会保障局漏洞进而深入省网数千万个人详细信息及历史数据合集	补天	QTVA-2015-311273
公司机构	合众速递(UCS）主站存在 SQL 注入漏洞，涉及 26 个数据库，800W 用户信息泄露	补天	QTVA-2015-309128
公司机构	山西焦煤集团内网沦陷#5T 的数据文档泄漏#所有网段服务器任意登录#OA、mail 等内部所有系统任意访问#集团所有员工信息、住房信息泄漏	补天	QTVA-2015-312221
互联网	一号店存在重大现金漏洞优惠卷无限领漏洞，不花钱买掉一号店所有东西	补天	QTVA-2015-312755
政府	淮北人社局某处漏洞导致全市用户百万身份证信息泄漏	补天	QTVA-2015-312407
政府	黑龙江省某居民公共卫生信息系统另一站漏洞打包，泄露三个省 1670w 用户信息和近 500w 家庭信息	补天	QTVA-2015-311975
教育	华东师范大学开放教育学院某管理系统存在漏洞泄漏大量学生信息	补天	QTVA-2015-312488
教育	安徽省成人高校招生网某漏洞导致十几万考试信息泄露	补天	QTVA-2015-311408
教育	河南省大中专毕业生就业信息管理系统 3 枚注入	补天	QTVA-2015-311279
教育	珠海某技术学校存在注入 泄露 2W 招生资料	补天	QTVA-2015-312299
政府	山东省教育厅工作人员安全意识不足可导致 1200W+学生信息泄漏	乌云	WooYun-2015-147323
互联网	启博软件微信分销平台漏洞#444w 用户信息#35w 订单信息#大量内部员工信息	补天	QTVA-2015-312476
互联网	优信二手车官网某处 SQL 注入，可泄露全站数据	漏洞盒子	vulbox-2015-011681
教育	大连理工大学奇葩漏洞一枚,成功修改管理员密码,可查全校 13 万学生,3 千教师资料.后台可任意上传文件	乌云	WooYun-2015-147404
政府	甘肃车管所漏洞打包，4000 万数据存在泄漏风险	补天	QTVA-2015-313526

政府	江苏省某市疾控中心某查询系统 SQL 注入导致 80 多万信息泄露（儿童、家长姓名/籍贯/住址/电话等）	乌云	WooYun-2015-147351
公司机构	中石化集团总部深入内网#多个重要系统沦陷(安全设备/存储服务器/磁带库等)	补天	QTVA-2015-314030
政府	石家庄民政局 SQL 注入漏洞,可进后台，泄露全站数据库	乌云	WooYun-2015-147708
政府	湖南省社保厅某社会保障卡系统存在漏洞导致 getshell#泄漏数千万敏感信息（姓名/地址/身份证等）	补天	QTVA-2015-313484
政府	浙江省公安厅泄露大量公民敏感信息	补天	QTVA-2015-312893
政府	南宁市某局近千万个人数据信息以及历史数据集合 3.9 亿详细记录	补天	QTVA-2015-312758
运营商	中国铁通移动业务管理系统 SQL 注入/SA 权限/泄露 50WEOMS 工单信息/学校名称/楼号/房间号	乌云	WooYun-2015-148196
运营商	中国铁通某故障单系统 SQL 注入/root 权限/188 个表	乌云	WooYun-2015-148111
运营商	云南电信宽带信息查询系统存在漏洞导致将近上亿信息泄漏#	补天	QTVA-2015-314402
运营商	中国电信某系统漏洞再次泄露 719 万工单信息（姓名、号码、地址、级别等）、安全类工单信息	补天	QTVA-2015-313733
运营商	广州联通办公系统漏洞导致 4 万多代理商用户信息泄漏以及大量工单信息#任意文件上传 getshell	补天	QTVA-2015-313766
公司机构	东风标致某站 SQL 注入漏洞，十万注册车主及其他用户的数据	漏洞盒子	vulbox-2015-011833
互联网	淘宝旗下淘点点(现口碑外卖)逻辑漏洞可黑产利用无限刷钱（人生巅峰不是梦）	补天	QTVA-2015-314333
金融保险	奇瑞徽银汽车金融多个系统存在安全漏洞，漏洞能量过大大导致标题都无法表达	补天	QTVA-2015-315263
政府	四川省工商局某系统 getshell 导致几十万用户敏感信息泄漏（姓名/身份证/手机号等）联通/中石油/建设银行/PICC 等躺枪	乌云	WooYun-2015-148492
政府	重庆市某交通安全信息系统 SQL 注入(泄露大量敏感信息+35W 驾驶员个人信息)	乌云	WooYun-2015-148432

政府	廊坊市人力资源和社会保障局某系统服务器 getshell	乌云	WooYun-2015-148576
政府	厦门人社局主站存在 POST 注入漏洞，泄露千万敏感数据	补天	QTVA-2015-314729
政府	阜阳市人社局危及大量数据以及敏感业务系统(随意登陆银行业务人员账号)	补天	QTVA-2015-315668
政府	河北社保厅某漏洞导致上百万用户社保信息泄漏（包括姓名地址身份证社保号）	补天	QTVA-2015-314753
政府	蚌埠人社局某系统漏洞危及数千万详细信息以及数亿的历史数据集合(疑似省网数据库)	补天	QTVA-2015-314600
互联网	中石化车 e 族 APP 存在 SQL 注入漏洞之一（可跨 9 个库）	乌云	WooYun-2015-148952
互联网	海尔旗下日日顺商城 SQL 注入可导致 300 万会员信息泄漏	乌云	WooYun-2015-148958
交通运输	香港航空某站 SQL 注入（涉及 156 万乘客信息/268 万机票信息/八千多员工信息）	乌云	WooYun-2015-148931
运营商	中国电信某系统漏洞泄露 400 万用户信息、支付交易明细信息（超市购物/加油站加油）以及充值等数据	补天	QTVA-2015-315377
政府	邯郸市工信办漏洞危及大量个人信息以及金额等数据，百万用户数据	补天	QTVA-2015-315437
互联网	世纪开元网存在注入漏洞导致大量用户敏感数据泄露（DBA 权限）(涉及姓名/电话/支付宝/邮箱/qq/家庭住址/qq 密码/支付宝密码等)	补天	QTVA-2015-316439
互联网	新浪微博某分站存在 SQL 注入漏洞(46W+用户信息泄露)	乌云	WooYun-2015-149138
运营商	中国联通宁安分公司办公系统 SQL 注入/root 权限/356 个表	乌云	WooYun-2015-148806
政府	黑龙江省某信息采集系统漏洞泄漏大量开房信息	补天	QTVA-2015-313832
互联网	到家美食会某隐蔽 SQL 注入#数百万用户信息泄露	补天	QTVA-2015-317258
互联网	爱抢购某多个数据库弱口令（60W 用户/300G 数据/活动码/API）	乌云	WooYun-2015-149332
教育	辽宁高校毕业生就业信息网漏洞几十万数据泄漏	补天	QTVA-2015-315989

政府	甘肃省委组织部危及全省 2.2W 干部个人信息(姓名,身份证,手机号,职位)	补天	QTVA-2015-317003
政府	上海市财务局某惠民基金管理系统 getshell 导致几十万用户姓名/银行卡/交易详情等信息泄漏	乌云	WooYun-2015-149433
公司机构	格林豪泰酒店主站存在 SQL 注入（涉及 94w 用户）	乌云	WooYun-2015-149567
公司机构	新疆经济报某系统漏洞内网数十台服务器沦陷(可随意编辑发布新闻稿)	补天	QTVA-2015-317948
互联网	易车网某处存在 SQL 注入漏洞（可跨 25 个库及所有数据）附验证脚本	乌云	WooYun-2015-149383
教育	汕头大学某处存在漏洞导致 20+网站沦陷/内网数据库漫游/getShell/	补天	QTVA-2015-317033
金融保险	泛华保险某站存在多处 OR 延时注入（DBA 权限+涉及 19 个 users）	乌云	WooYun-2015-149456
运营商	中国电信某系统多处注入#可查全国上亿用户信息#涉及姓名、证件号、余额，并可进行充值、销户、换卡等操作	补天	QTVA-2015-318323
政府	沈阳医疗保险局漏洞可导致大量数据泄漏	补天	QTVA-2015-316271
政府	新疆地税局漏洞危及数亿发票信息以及发票密码以及个人信息#多台服务器沦陷	补天	QTVA-2015-317579
政府	黑龙江省某局漏洞危机全省数百万车主详细信息以及相关证件证明等数据	补天	QTVA-2015-318209
政府	河北省地税局数千万发票数据#内网多台服务器沦陷#多台网络核心设备沦陷	补天	QTVA-2015-318704
互联网	日日顺网上商城漏洞修复不完善，可继续泄露数千万用户信息（姓名/地址/手机号等）	补天	QTVA-2015-317990
互联网	爱丽时尚网某处高危漏洞，泄露 377w 用户信息	补天	QTVA-2015-318332
金融保险	中国民生银行某系统出现安全漏洞导致(Getshell/敏感数据泄漏/大量内部企业邮箱地址泄漏/多台外网主机泄漏）	补天	QTVA-2015-318758
政府	四川某市住房公基金 SQL 注入控制后台可导致泄露 60 多万用户数据	乌云	WooYun-2015-149937
政府	内蒙古税务局某系统弱口令导致 getshell 泄漏几十万用户敏感信息（账号/密码/姓名/手机号）	乌云	WooYun-2015-150203
公司机构	中国商业港多处 SQL 注入可导致 395 万会员信息泄漏（影响大量企业）	乌云	WooYun-2015-150404

公司机构	畅流云某站存在远程代码执行漏洞（可获取数据库）+多站存在登录弱口令	漏洞盒子	vulbox-2015-011989
政府	江西省工商局某服务平台某漏洞泄露企业登记信息	乌云	WooYun-2015-150198
政府	云南省交通厅两处注入漏洞，泄漏百万公民信息	补天	QTVA-2015-318446
政府	成都某口令导致政府内网入侵事件，特殊人群定位系统，国资委车辆信息，人口信息，短信平台和 IT 服务支撑系统，大屏幕切换等	补天	QTVA-2015-318302
互联网	西北工业大学某校园相亲网存在 SQL 注入导致服务器 getshell	乌云	WooYun-2015-150386
能源	某电网系统 SQL 注入 16 个库 DBA 权限	乌云	WooYun-2015-150772
政府	辽宁省某市公积金查询系统 SQL 注入打包/DBA 权限/大量用户信息泄露	乌云	WooYun-2015-150512
政府	贵州省地税局漏洞危及 200W 纳税人详细信息	补天	QTVA-2015-320258
政府	宁夏地税局系统漏洞危及 600W 纳税人详细信息	补天	QTVA-2015-320261

联系作者

刘思成：安华金和数据库攻防实验室（DBSec Labs）安全研究员，专注于研究数据库漏洞的原理、利用方法和数据库防护技术。

Email：liusicheng@dbsec.cn

付蓉洁：安华金和市场部总监，负责公司整体品牌、产品及行业市场推广

Email：furongjie@dbsec.cn

沈雪峰：安华金和网络运营主管，安华每日安全资讯整理者

Email：shenxuefeng@dbsec.cn

关于安华金和

安华金和是我国专业的数据库安全产品和服务提供商，由长期致力于数据库内核研发和信息安全领域的专业资深人员共同创造，是国内唯一提供全面的数据库安全产品、服务和解决方案服务商，覆盖数据库安全防护的事前检查、事中控制和事后审核，帮助用户全面实现数据库安全防护和安全合规。

安华金和数据库安全产品已经广泛地应用于政府、军队、军工、运营商、金融、企业信息防护等领域，建立了良好声誉，成为众多企业在该领域寻求安全产品和服务的首选。

了解更多有关数据库安全信息，请访问： 官方网站>>数据库安全

安华金和官方微博：**安华数据** http://weibo.com/DBSecurity

安华金和官方微信 搜索公众号 **安华金和**