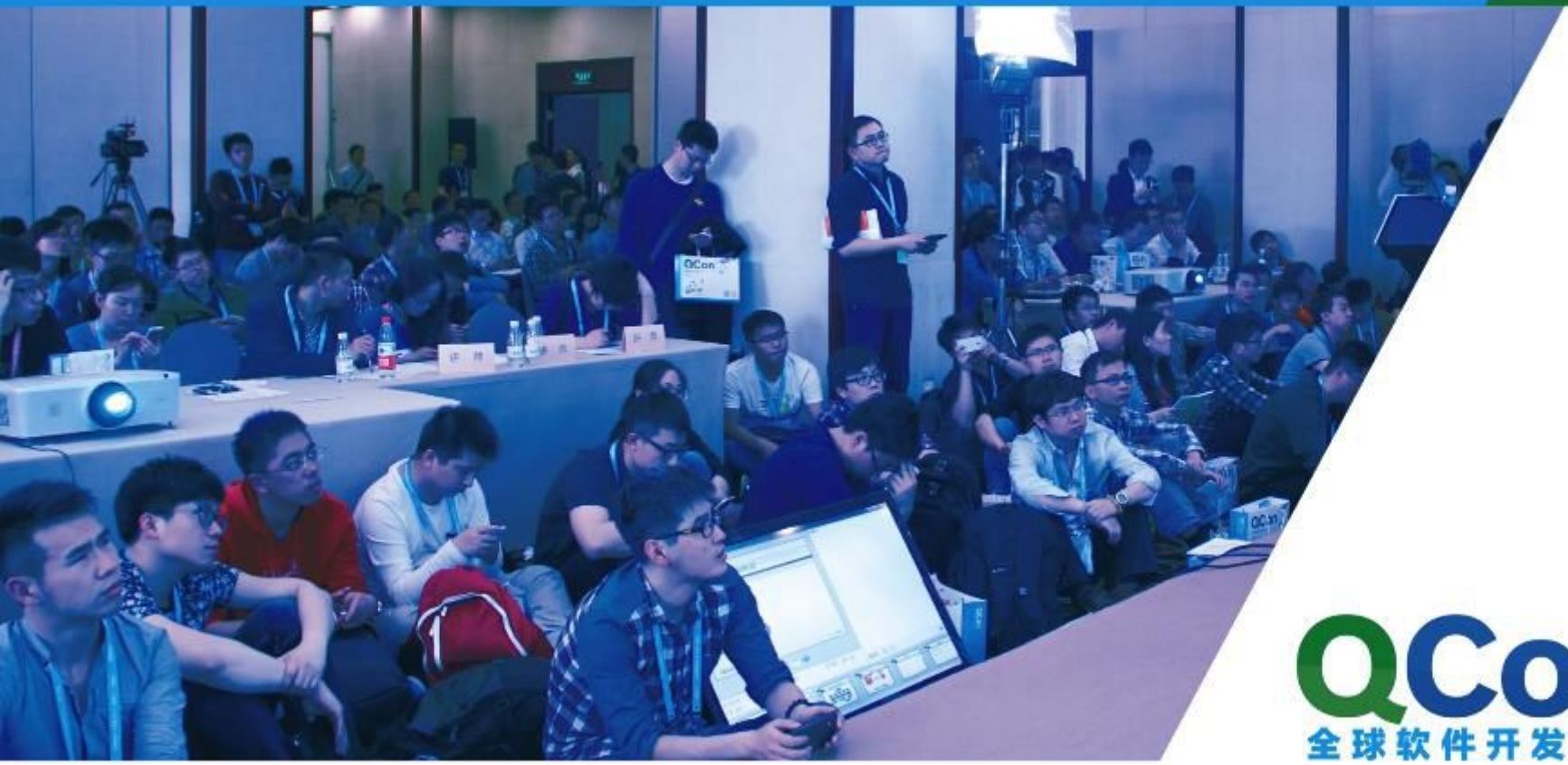
QCon全球软件开发大会

International Software Development Conference



QCon
全球软件开发大会

程序员与黑客 第二季

@余弦 | 2015.10

程序员

知道创宇 技术VP

JavaScript

Python

大数据

...

关于我

evilcos.me

黑客

web2hack.org

kcon.knownsec.com

sebug.net

zoomeye.org

...

内容

- 前情回顾
- 地下黑客形势
- 安全过程

前情回顾

这次只谈「程序员」
其他的环节不谈:)

思想①：黑客思维需要贯穿「...->架构->研发->运维->...」

理想状态：
技术团队每个人都具备黑客思维

思想②：优美的架构一定是健壮的

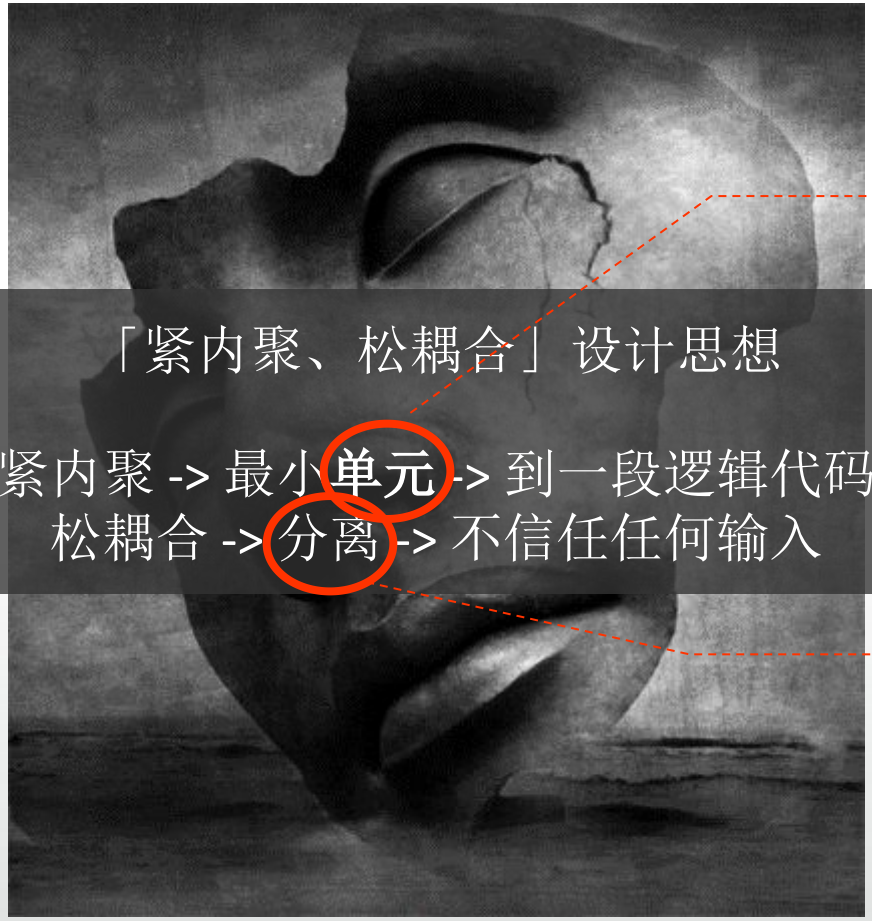
1. 想象下「生态系统」

2. 有漏洞/被黑这很正常

3. 能快速「自愈」才是关键

思想③：优美的架构一定是处处优美的

思想④：安全的本质是信任



「紧内聚、松耦合」设计思想

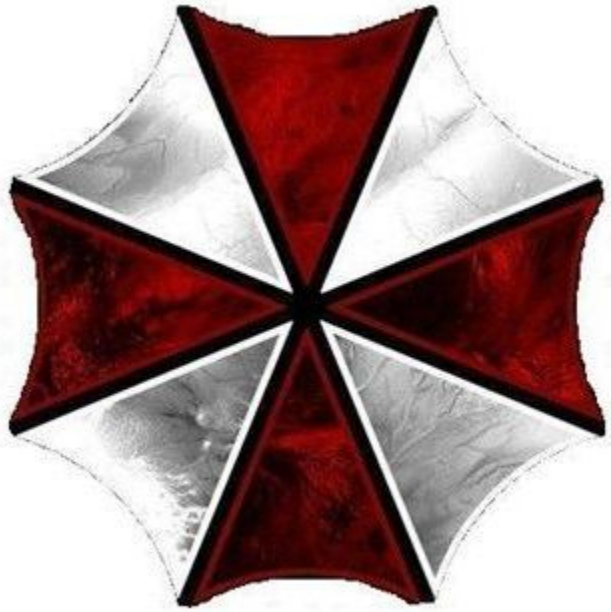
紧内聚 -> 最小**单元** -> 到一段逻辑代码
松耦合 -> 分离 -> 不信任任何输入

单元的重要性

分离的重要性

关键的分离

- 人员职权分离
- 服务器分离
- 账号权限分离
- 文件目录分离
- 代码分离
- Cookie分离
- 子域分离



技术选型

- 任何组件都有漏洞
  - 一般规律
    - 越流行的开源组件越靠谱
    - 越靠谱的团队打造的组件越靠谱
- 时刻做好被黑个透的准备
  - 优美的架构多重要
  - 分离设计能大大提高入侵门槛
  - 快速应急 -> 快速自愈

地下黑客形势

形势一

- 任何明面可见的产业链都对应着至少一条黑色/灰色产业链

形势二

- 撒网式攻击时时刻刻都在发生
  - 更可怕的是：撒网式攻击进阶到针对性攻击
  - 最可怕的是：直接面对针对性攻击，尤其是APT

形势三

- 网络空间遵守黑暗森林的游戏规则
  - 被发现即被干掉

形势四

- 没谁真敢、真能撼动地下黑客
  - 只有历史进程可以撼动一切 —— 物竞天择、适者生存
  - 一切的人为对抗都是不痛不痒

形势五

- 永远不要低估地下黑客的执行力
  - 漏洞的黄金应急时间：24h、12h、6h、1h

[举例]地下黑客游戏规则

- 针对性的撒网式攻击
- 适当剧透个例子：网贷里的宝藏

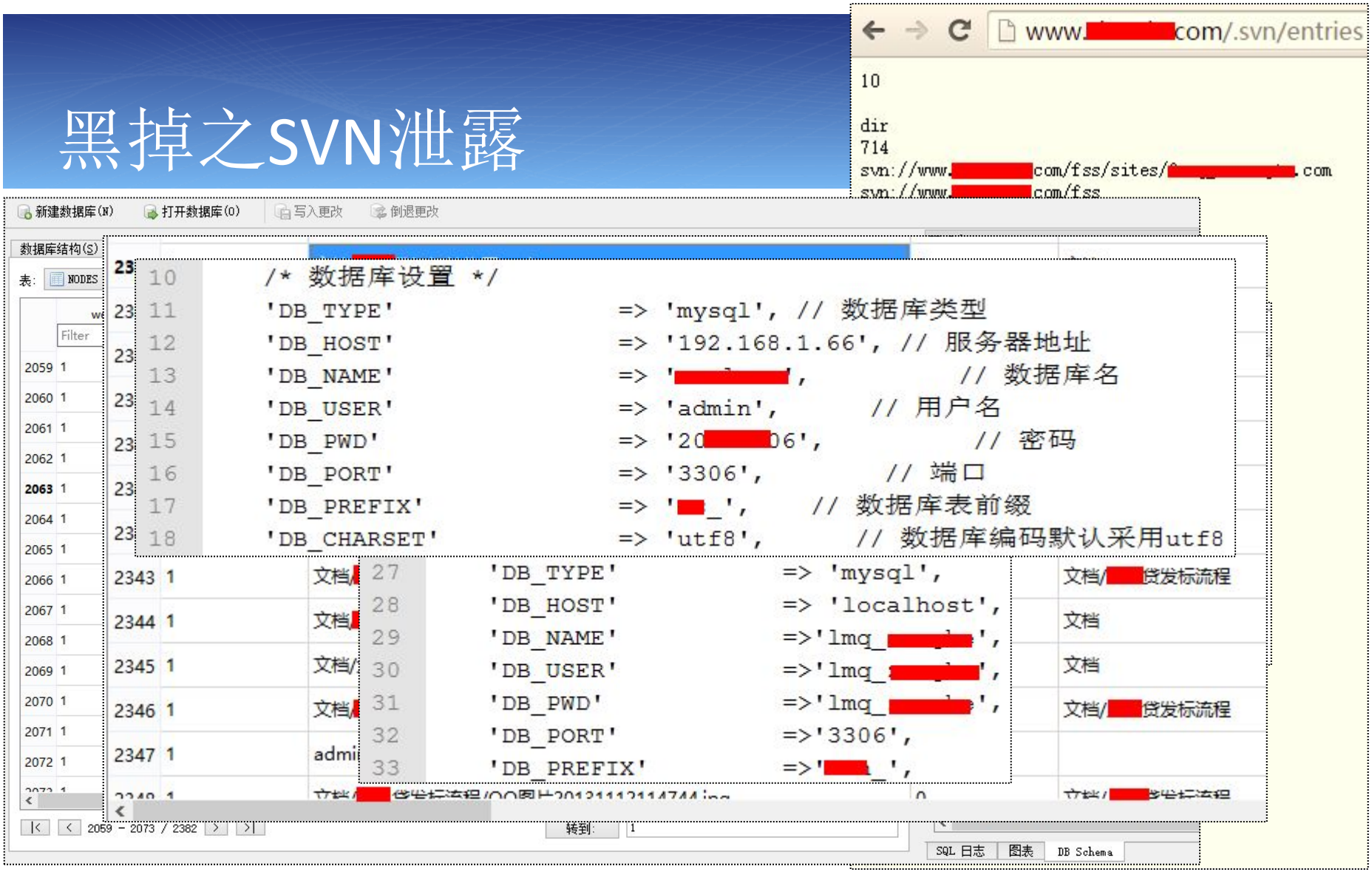
游戏规则

- 这个道理我们需要明白
  - 「以大多数人的努力程度之低，还不至于比天赋...」
  - 衍生一下：「以大多数网站的安全程度之低，还不至于高级黑...」
  - 全国1600家不错的网贷
  - 从概率上来说，一定存在一定比例的低级高危漏洞
  - 如：SVN泄露、心脏出血、Redis泄露、...

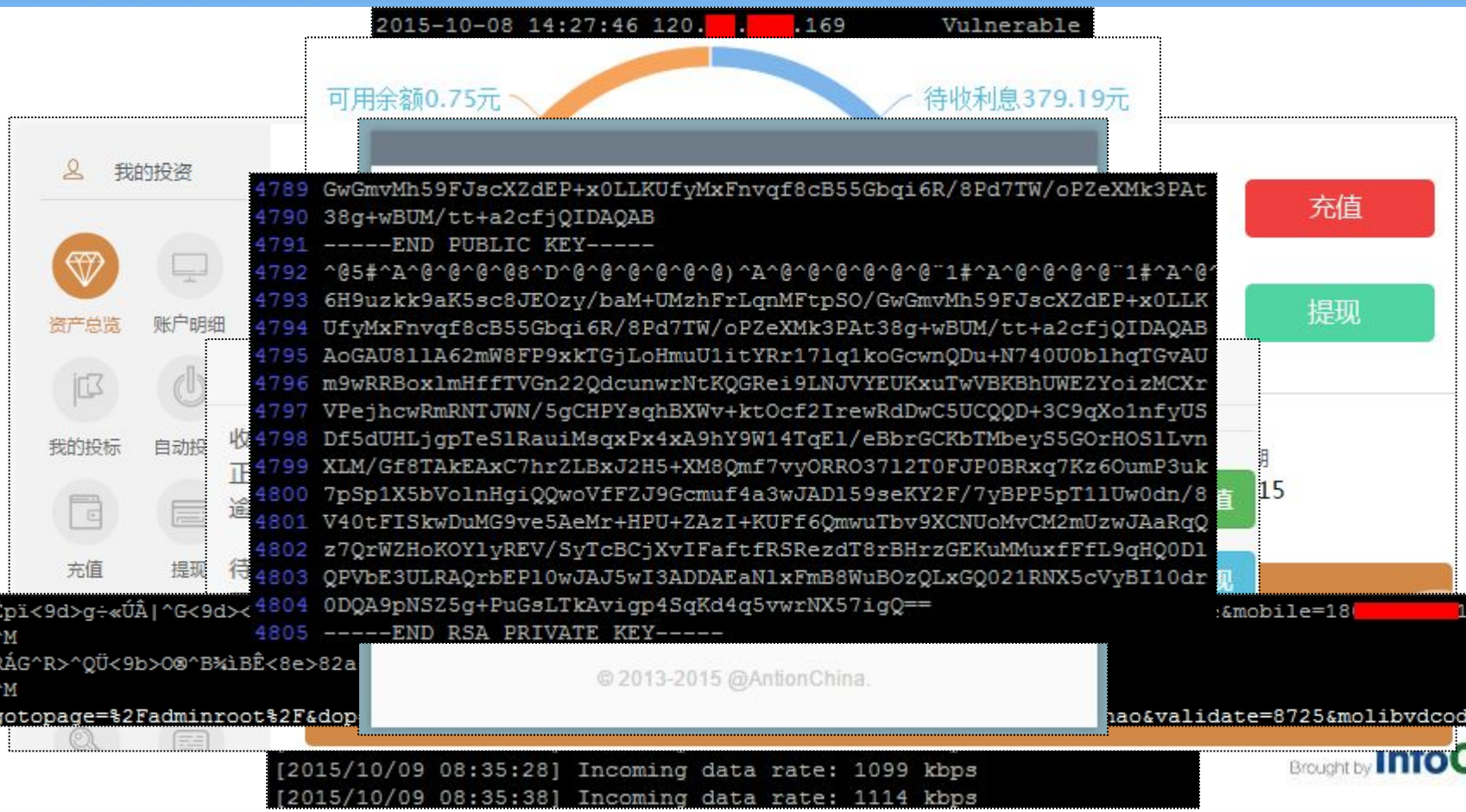
黑掉方式

- 得到1600家网贷的网站列表
- 写个自动化程序批量探测如下漏洞，插件化
  - SVN泄露、心脏出血、Redis泄露、...
- 扩大战果
  - 把C段一并探测了
  - 继续扩大，把CDN之后真实的IP得到再探测C段
  - 继续继续扩大，把不同子域的潜在C段都一并探测了

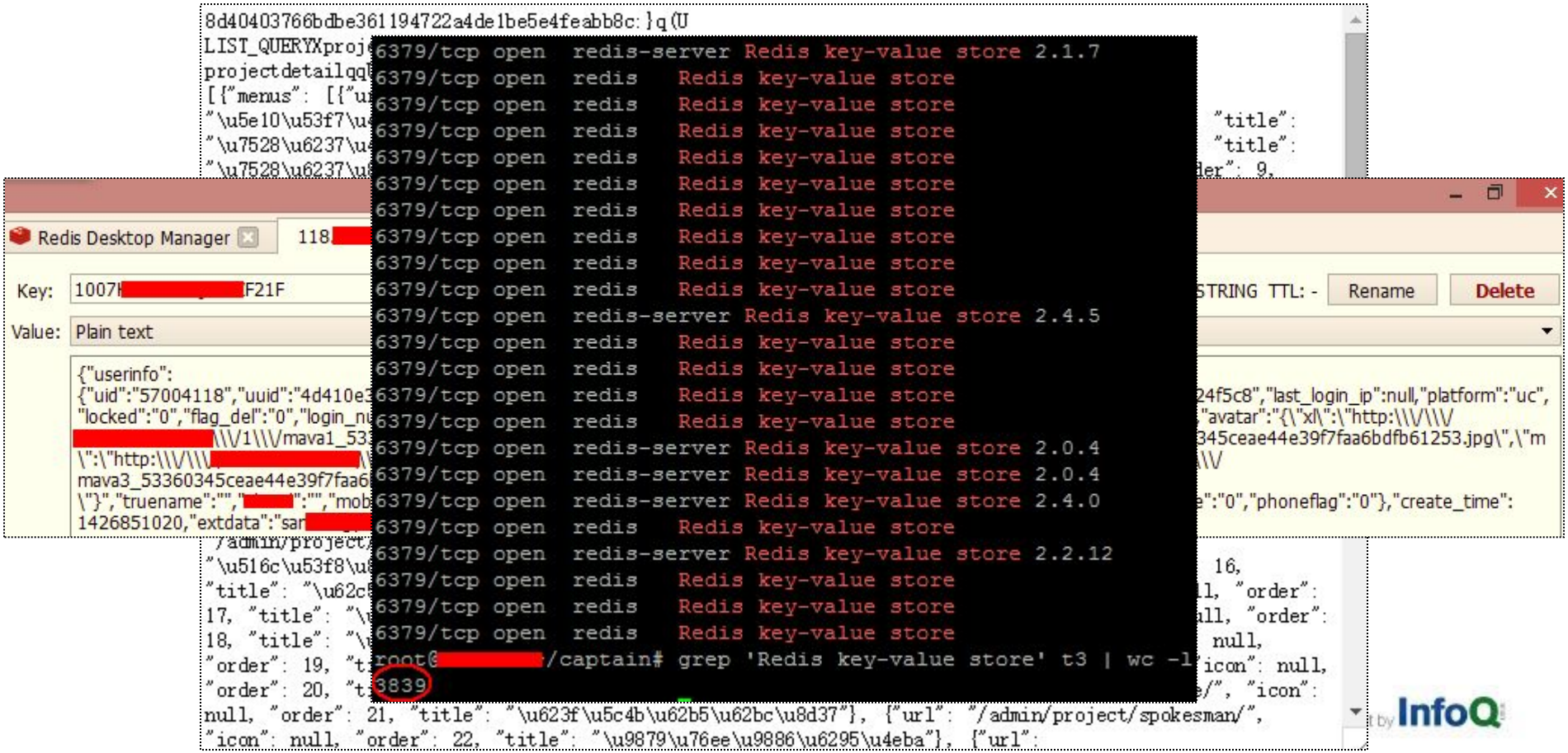
黑掉之SVN泄露


www.[redacted]com/.svn/entries
10
dir
714
svn://www.[redacted]com/fss/sites/[redacted].com
svn://www.[redacted]com/fss
新建数据库(N)
打开数据库(O)
写入更改
倒退更改
数据库结构(S)
表:
NODES
Filter
/* 数据库设置 */
'DB_TYPE' => 'mysql', // 数据库类型
'DB_HOST' => '192.168.1.66', // 服务器地址
'DB_NAME' => '[redacted]', // 数据库名
'DB_USER' => 'admin', // 用户名
'DB_PWD' => '20[redacted]06', // 密码
'DB_PORT' => '3306', // 端口
'DB_PREFIX' => '[redacted]_', // 数据库表前缀
'DB_CHARSET' => 'utf8', // 数据库编码默认采用utf8
'DB_TYPE' => 'mysql',
'DB_HOST' => 'localhost',
'DB_NAME' => 'lmq_[redacted]',
'DB_USER' => 'lmq_[redacted]',
'DB_PWD' => 'lmq_[redacted]',
'DB_PORT' => '3306',
'DB_PREFIX' => '[redacted]_',
SQL 日志
图表
DB Schema

黑掉之心脏出血


2015-10-08 14:27:46 120.[redacted].169 Vulnerable
可用余额0.75元
待收利息379.19元
我的投资
资产总览
账户明细
我的投标
充值
提现
4789 GwGmvMh59FJscXZdEP+x0LLKUfyMxFnvqf8cB55Gbqi6R/8Pd7TW/oPZeXMk3PAt
4790 38g+wBUM/tt+a2cfjQIDAQAB
4791 -----END PUBLIC KEY-----
4792 ^@5#^A^@^@^@^@8^D^@^@^@^@^@^@)^A^@^@^@^@^@^@¨1#^A^@^@^@^@¨1#^A^@
4793 6H9uzkk9aK5sc8JEOzy/baM+UMzhFrLqnMFtpSO/GwGmvMh59FJscXZdEP+x0LLK
4794 UfyMxFnvqf8cB55Gbqi6R/8Pd7TW/oPZeXMk3PAt38g+wBUM/tt+a2cfjQIDAQAB
4795 AoGAU811A62mW8FP9xkTGjLoHmuU1itYRr171q1koGcwnQDu+N740U0blhqTGvAU
4796 m9wRRBoxlmHffTVGn22QdcunwrNtKQGRei9LNJVYEUKxuTwVBKBhUWEZYoizMCXr
4797 VPejhcwRmRNTJWN/5gCHPYsqhBXWv+ktOcf2IrewRdDwC5UCQQD+3C9qXo1nfyUS
4798 Df5dUHLjgpTeSlRauiMsqxPx4xA9hY9W14TqEl/eBbrGCKbTMbeyS5GOrHOSlLvn
4799 XLM/Gf8TAkEAxC7hrZLBxJ2H5+XM8Qmf7vyORRO3712T0FJP0BRxq7Kz6OumP3uk
4800 7pSp1X5bVolnHgiQQwoVfFZJ9Gcmuf4a3wJADl59seKY2F/7yBPP5pT11Uw0dn/8
4801 V40tFISkwDuMG9ve5AeMr+HPU+ZAzI+KUFf6QmwuTbv9XCNUoMvCM2mUzwJAaRqQ
4802 z7QrWZHoKOYlyREV/SyTcBCjXvIFaftfRSRezdT8rBHrzGEKuMMuxfFfL9qHQ0Dl
4803 QPVbE3ULRAQrbEPl0wJAJ5wI3ADDAEaN1xFmB8WuBOzQLxGQ021RNX5cVyBI10dr
4804 0DQA9pNSZ5g+PuGsLTkAvigp4SqKd4q5vwrNX57igQ==
4805 -----END RSA PRIVATE KEY-----
19840 Èpï<9d>g÷«ÚÂ|^G<9d><
19841 ^M
19842 RÁG^R>^QÜ<9b>O®^B¾ìBÊ<8e>82a
19843 ^M
19844 gotopage=%2Fadminroot%2F&dop
&mobile=18[redacted]1Fû^Cs^G
hao&validate=8725&molibvdcode=jSD11
© 2013-2015 @AntionChina.
[2015/10/09 08:35:28] Incoming data rate: 1099 kbps
[2015/10/09 08:35:38] Incoming data rate: 1114 kbps
Brought by InfoQ

黑掉之Redis泄露


6379/tcp open redis-server Redis key-value store 2.1.7
6379/tcp open redis Redis key-value store
6379/tcp open redis-server Redis key-value store 2.4.5
6379/tcp open redis-server Redis key-value store 2.0.4
6379/tcp open redis-server Redis key-value store 2.0.4
6379/tcp open redis-server Redis key-value store 2.4.0
6379/tcp open redis-server Redis key-value store 2.2.12
root@ /captain# grep 'Redis key-value store' t3 | wc -l
3839
Redis Desktop Manager
Key:
Value: Plain text
STRING TTL: -
Rename
Delete

小结

- 你是否可以举一反三了？
- 这种游戏规则是黑客与程序员的博弈，想象下《三体》里的破壁者与面壁者？
- 明白地下黑客的游戏规则是做好安全的前提

安全过程

[聚焦]给中小型互联网团队打造一个安全过程

内容

- 环环相扣、一一剖析
- 血之劝告

安全过程

环环相扣、一一剖析

人

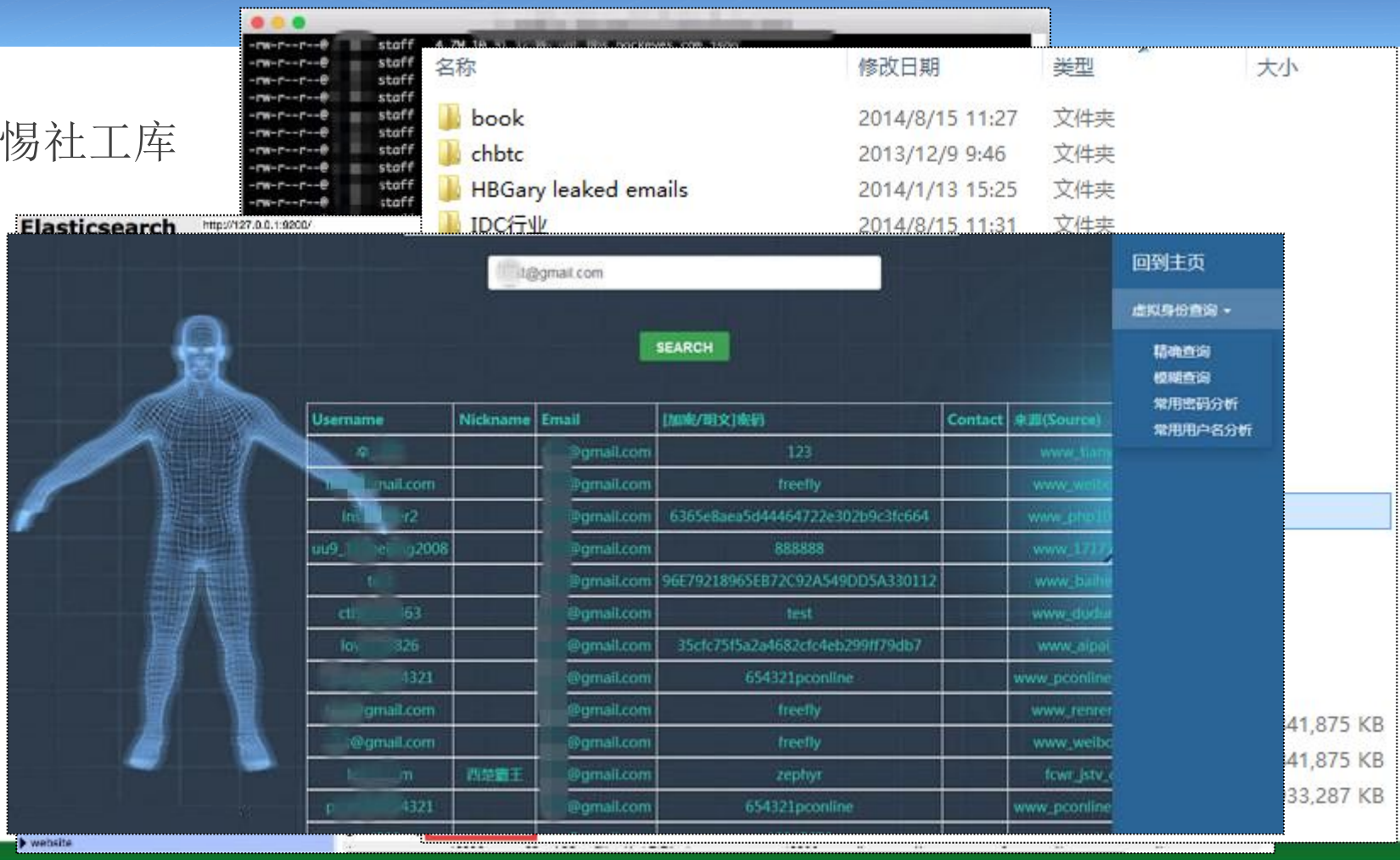
- 团队核心成员（eg: CXO）尤其必须具备安全意识
- 技术负责人、架构师、技术关键角色必须具备一定的安全经验
- 在没专门的安全团队时，运维团队或某技术关键角色接管安全应急
- 职权一定要分离清晰
  - 内部关键信息系统交给最靠谱的人
  - 提防「内鬼」或被「内鬼」
  - 回收离职人的权限

人

- 警惕惰性
  - 弱口令、随手备份、随手发布、随手开调试、忽视补丁的重要性、...
  - 地下黑客的撒网式攻击善于利用了人的这种惰性

人

- 警惕社工库


名称
修改日期
类型
大小
book
2014/8/15 11:27
文件夹
chbtc
2013/12/9 9:46
文件夹
HBGary leaked emails
2014/1/13 15:25
文件夹
IDC行业
2014/8/15 11:31
文件夹
Elasticsearch
SEARCH
回到主页
虚拟身份查询
精确查询
模糊查询
常用密码分析
常用用户名分析
Username
Nickname
Email
Contact
123
freefly
6365e8aea5d44464722e302b9c3fc664
888888
96E7921896SEB72C92A549DD5A330112
test
35cfc75f5a2a4682cfc4eb299ff79db7
654321pconline
freefly
freefly
zephyr
654321pconline
41,875 KB
41,875 KB
33,287 KB

内网

- Wi-Fi安全
  - 做好分离、WPA2安全加密（关闭WPS）、强密码+Portal二次认证、杜绝自建Wi-Fi AP、...
- 警惕ARP
  - 路由器需要支持ARP防御、客户端部署ARP监测
- 网络隔离
  - 重要的网络需要考虑严格隔离
  - LDAP统一认证
  - 必要时：堡垒机
  - ...

终端

- 这是一个复杂的话题
  - 终端是最接近人的，惰性很严重
  - 风险也可能是最大的
    - 比如：遭遇水坑攻击:)
    - 比如：遭遇ARP
    - 比如：软件后门
    - 比如：丢了...
    - 比如：离开终端时不「Win+L」

终端

- 给出一些建议
  - 勤打补丁
  - 安装安全防护软件，真不要觉得自己牛到一辈子裸奔
  - Firefox+NoScript
  - 类TrueCrypt分区加密软件
  - BIOS加密
  - 在陌生网络里不要乱开调试
  - 警惕陌生网络
    - 安装ARP防御/提醒软件
  - 警惕陌生USB
    - HID、BadUSB等攻击

研发环境

- 必要时可以考虑构建自家的可信源
- 严禁盗版与第三方不可信源的软件
  - 中文Putty事件、Xcode事件、...
- 使用Docker时，注意镜像本身的安全性
- 不要轻易把研发运维环境暴露到公网上
  - 比如：Jenkins、GitLab、Redis、Memcached、Zabbix 、Nagios、...
- 云端的那些协作平台:&

邮件系统

- 一个事实是
  - 邮件被黑，几乎意味着半个公司被黑:)
- Gmail企业版
  - 如果贵司无视GFW的话，Gmail企业版绝对是宇宙第一选择
- QQ企业邮箱
  - 国内有点情怀的企业邮箱，虽然安全性比起Gmail有差距
- 商业邮箱：Outlook、IBM Notes，土豪之友
- Foxmail等客户端收信，是个好习惯

服务器

- 勤打补丁
  - 这是一门艺术
- SSH证书，杜绝密码形式
  - 22可以留给蜜罐（如：Kippo）
  - 可以考虑来一个外网跳板进内部集群
- 注意万恶的0.0.0.0绑定
- Linux环境的Rootkit查杀
  - rkhunter、chkrootkit
  - 业界良心，何止Rootkit查杀：Lynis

HTTP服务

- Web与App的云端几乎都是HTTP服务，能用上HTTPS是最好的
- 严格控制RWX权限
- 警惕各类Web漏洞
  - 勤打补丁
  - 用上WAF类防御
- 警惕XSS盲打攻击（水坑攻击的一种形式）

机房或云服务

- 网络必须绝对隔离
- 选择这个就和买房似的，你总是有些无奈，就希望对方真的是好人...
  - 因为出的问题有可能是隐性的

DNS

- 选择靠谱的DNS服务
- 选择这个就和买房似的，你总是有些无奈，就希望对方真的是好人...
  - 因为出的问题有可能是隐性的

CDN

- 说个另类的，真实IP是如何泄露的
  - 子域名的IP如果不在CDN后面，那么C段一般可以发现目标域名的真实IP
  - 目标域名如果有发邮件功能，查看邮件的详情，可能可以发现真实IP
  - 如果目标网站有phpinfo这类的探针，也会暴露
  - 如果目标网站有相关漏洞可以执行系统命令或系统报错等，也有可能暴露真实IP
  - 善于Google、ZoomEye，可能可以发现某些平台的历史记录里有真实IP
  - 善于whois反查目标域名，一般会发现同一个人注册的多个域名，相似域名有可能是一个IP上或一个C段
  - DDoS打过去，一般流量够大，CDN平台如果对目标域名做回源处理那么就会暴露真实IP

防御DDoS/CC

- 选择靠谱的抗DDoS/CC服务
- 选择这个和买房就不一样了，因为出问题是立即可见的...

逻辑

- 这块是最有趣的
- 很多时候被黑就是因为这个逻辑出现致命缺陷
  - 比如：密码找回、会话重用、OAuth劫持、越权泄露、...
  - 比如：各类业务安全，这是一个很大的话题
    - 特别推荐好文：解析P2P金融的业务安全
      http://www.freebuf.com/news/special/81062.html

打造自家的威胁情报体系

- 被动日志分析
  - ELK还行
    - ElasticSearch、Logstash、Kibana组合
  - Splunk不错，土豪之友
  - OSSEC（开源的主机入侵检测系统）也不错
- 主动监测预警
  - 服务器IP分布、开放端口、架构组件等了如指掌
  - 可以周期监测+漏洞情报预警
  - ...

结束？

- 不不不，我们还需要再次强调这些「血之劝告」！

安全过程

血之劝告

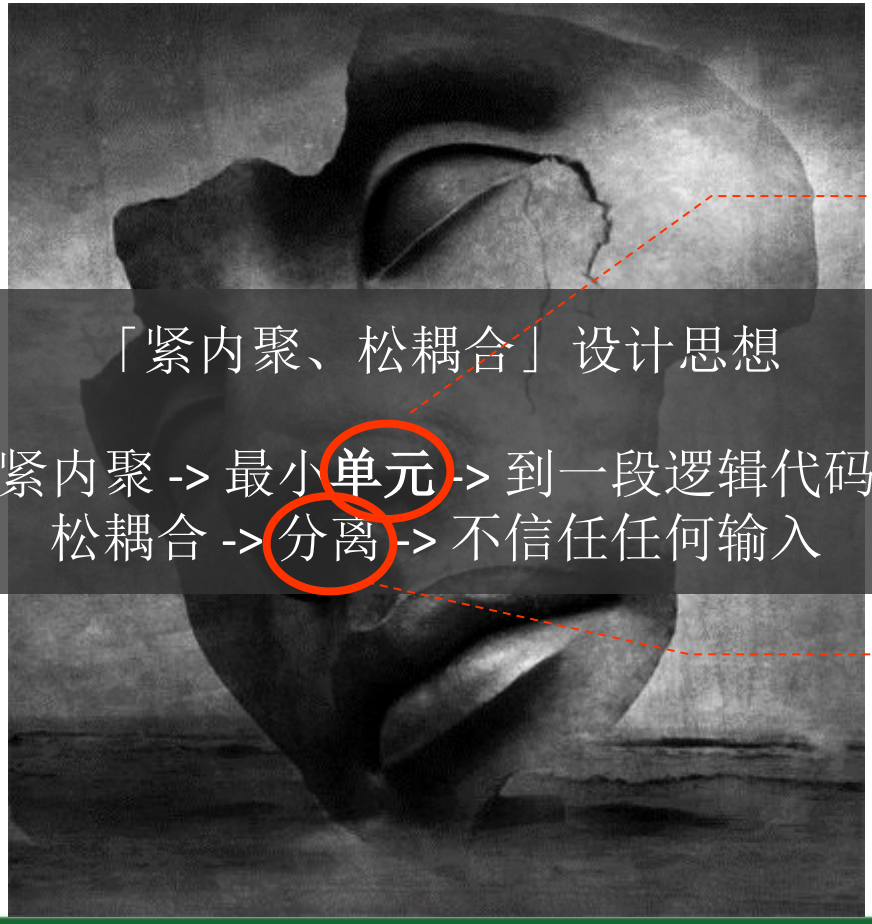
一定要有个优美的架构

1. 想象下「生态系统」

2. 有漏洞/被黑这很正常

3. 能快速「自愈」才是关键

透彻理解安全的本质是信任



「紧内聚、松耦合」设计思想

紧内聚 -> 最小**单元** -> 到一段逻辑代码
松耦合 -> **分离** -> 不信任任何输入

单元的重要性

分离的重要性

安全策略的部署一定要全面

- 顾此失彼丢三落四可不是个好习惯

```
4092  1 <!> 人力资源专区"
4093  1 <!> 人人网，中国领先的实名制sns社交网络。加入人人网，找到老同学，结识新朋友。
4094  1 <!> 交際クラブ□デートクラブなら東京□横浜にある交際倶楽部恋路へ"
4095  1 <!> 交大校友之家"
4096  1 <!> 亞美娛樂城online"
4097  1 <!> 亞洲廣播股份有限公司"
4098  1 <!> 亞太mass call web系統登入"
4099  1 <!> 亚伟商城 | - 用心服务，感动客户！"
4100  1 <!> 互联网+医疗众创学院 | 互联网思维,革新医疗价值"
4101  1 <!> 云赛云平台"
4102  1 <!> 云目管理系统登录"
4103  1 <!> 云杉网络"
4104  1 <!> 云总机后台管理系统"
4105  1 <!> 云思维-云思维"
4106  1 <!> 云南昱信科技有限公司"
4107  1 <!> 云动力"
4108  1 <!> 予約ページ | 大阪 業務促進システム「smooth(スムーズ)」の開発□販売なら一
4109  1 <!> 九闻网络会议"
```

心脏出血刷刷刷

定期备份机制一定需要有

- 快速Diff找出可疑文件（如后门）
- 灾备恢复，多么痛的领悟

Code Review值得提倡

- 说不定发现不仅是几个bugs

应急响应要争分夺秒

- 回顾前面说的「地下黑客形势」...

可以请专业的安全团队把脉

- 我私人微信：331861985 :)

THANKS