

乌云平台视角下的信息安全

wooyun

目录

- 关于我
- 当我们讨论信息安全时我们在想些什么
- 关于乌云漏洞报告平台
- 从乌云漏洞报告平台里看到的
- Q/A

关于我

- 跨站师，web渗透师，业余渗透手
- 戴着镣铐跳舞的黑客实用主义者
- 百度安全架构师
- 80sec/wooyun创始人

当我们讨论信息安全时我们在想些什么



场景一

- 甲方
 - 不存在任何____安全问题，对于造谣抹黑的我们将采取____处理

场景二

- 乙方
 - 这个新兴的____安全问题很严重，已经导致____

场景三

- 技术主管
 - 我们已经买了___设备了，我们在安全上已经足够投入了

场景四

- 安全工程师
 - 我们已经按照某top10上的清单进行了排查，现在只剩下边边角角的xss没有处理了

场景五

- 安全研究人员
 - 我想我发现了____的一个严重漏洞，在_____条件下能够导致很危险的后果

关于乌云

- 中立开放负责任的第三方漏洞报告平台

漏洞报告流程

- 从漏洞报告到厂商修复期间内容保密
- 公开以确保用户能够了解到安全漏洞细节
- 让信息安全回归本质

信息安全本质

- 影响的数据
- 产生的危害
- 发生的概率

乌云安全威胁top1

- 引用不安全的第三方应用

案例1

最新公开

提交日期	漏洞名称
2013-07-17	淘宝某分站最新Struts命令执行漏洞又一枚
2013-07-17	苹果某业务分站S2-016任意命令执行漏洞（已证明）
2013-07-17	完美世界多个S2-016命令执行
2013-07-17	走秀网某站命令执行(已证明能执行命令)
2013-07-17	去哪儿Struts2命令执行漏洞和权限绕过
2013-07-17	新网某分站最新struts2命令执行
2013-07-17	优酷某分站命令执行
2013-07-17	土豆网某站命令执行
2013-07-17	中国民生银行某分站命令执行漏洞
2013-07-17	寻医问药某分站SQL注入漏洞
2013-07-17	搜狗某分站最新Struts命令执行漏洞（证明可执行命令）
2013-07-17	百合网某分站存在代码执行漏洞
2013-07-17	大众点评官网命令执行漏洞（以证明可执行任意代码）
2013-07-17	搜狐邮箱业务命令执行漏洞
2013-07-17	网易三个s2-016命令执行
2013-07-17	搜狗某分站最新struts命令执行漏洞
2013-07-17	百度某业务命令执行
2013-07-17	土豆某后台struts2任意命令执行（已证明可执行任意代码）
2013-07-17	百度某分站最新Struts命令执行漏洞一枚
2013-07-17	sohu分站最新Struts命令执行漏洞

案例2

- 看我是如何利用zbbix渗透sogou&sohu内网的
- <http://www.wooyun.org/bugs/wooyun-2010-022537>

乌云安全威胁top2

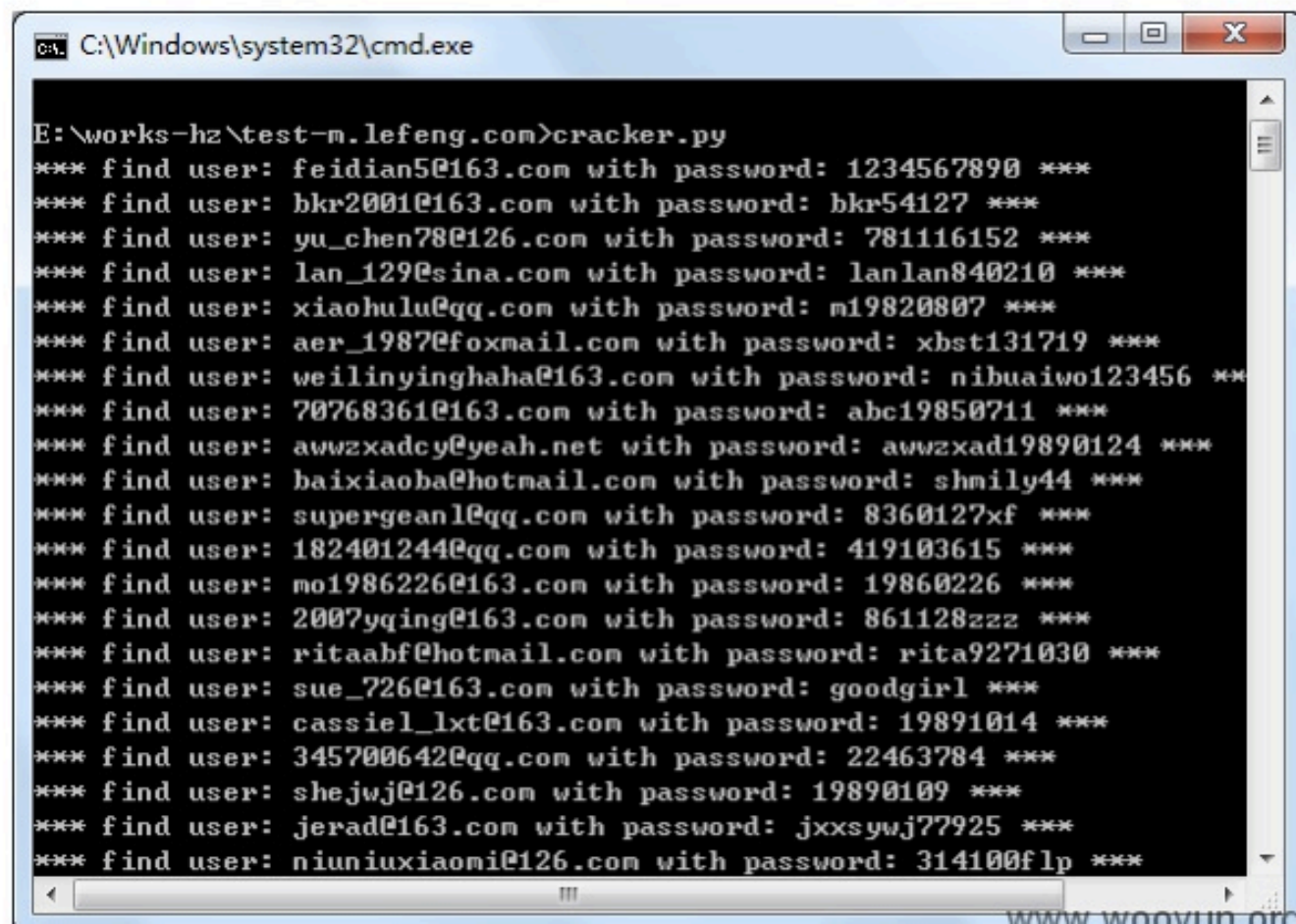
- 互联网泄密/撞库事件

漏洞证明：

使用曾经流出来的某库，

随机抽取记录扫了下号，

成功了一百来个号。



```
C:\Windows\system32\cmd.exe

E:\works-hz\test-m.lefeng.com>cracker.py
*** find user: feidian5@163.com with password: 1234567890 ***
*** find user: bkr2001@163.com with password: bkr54127 ***
*** find user: yu_chen78@126.com with password: 781116152 ***
*** find user: lan_129@sina.com with password: lanlan840210 ***
*** find user: xiaohulu@qq.com with password: m19820807 ***
*** find user: aer_1987@foxmail.com with password: xbst131719 ***
*** find user: weilinyinghaha@163.com with password: nibuaiwo123456 ***
*** find user: 70768361@163.com with password: abc19850711 ***
*** find user: awwxadcy@yeah.net with password: awwxad19890124 ***
*** find user: baixiaoba@hotmail.com with password: shmily44 ***
*** find user: supergean1@qq.com with password: 8360127xf ***
*** find user: 182401244@qq.com with password: 419103615 ***
*** find user: mo1986226@163.com with password: 19860226 ***
*** find user: 2007yqing@163.com with password: 861128zzz ***
*** find user: ritaabf@hotmail.com with password: rita9271030 ***
*** find user: sue_726@163.com with password: goodgirl ***
*** find user: cassiel_lxt@163.com with password: 19891014 ***
*** find user: 345700642@qq.com with password: 22463784 ***
*** find user: shejwj@126.com with password: 19890109 ***
*** find user: jerad@163.com with password: jxxsywj77925 ***
*** find user: niuniuxiaomi@126.com with password: 314100flp ***
```

乌云安全威胁top3

- xss/csrf

当前位置：WooYun >> 白帽信息

胯下有杀气

34人关注

关注

大姐，你黄瓜掉了。。。

等级：核心白帽子

个人主页：<http://跟各位大姐学习已久，是时候了！>

Rank值：241

漏洞列表：

提交日期	漏洞名称
2013-04-25	一个XSS导致汉庭酒店几个内部关键系统的沦陷，以及盲打后台无法访问的利用与分析技巧 ⚡
2013-03-26	口袋购物之1999元iPad mini 究竟是肿么回事揭秘~
2012-10-21	美团后台“聊天杀”，代金券、用户等信息泄露
2012-09-03	大众点评后台未授权访问，泄露大量用户GPS地理位置与手机号码等信息
2012-08-22	金山UED中心再次暴菊，管理员大屠杀 ⚡
2012-08-20	xss盲打天使湾投资后台
2012-08-17	手机feedback xss盲打金山词霸UED中心 ⚡
2012-08-09	猎头网被反猎，在绕过帐号只能一台电脑登陆限制！！
2012-07-26	守株待兔沦陷大街网后台，可登陆修改站内任意用户
2012-07-23	利用xss测试36氪重要系统后台
2012-07-17	您的企业缺少优秀的职员吗？来大街，跨就送！
2012-07-17	XSS漏洞渗透新浪微博《头条新闻》账号
2012-07-13	雪球网xss盲打后台
2012-07-12	用xss平台沦陷百度投诉中心后台（原来百度的后台是酱紫的） ⚡

乌云安全威胁top4

- 信息安全边界的缺失

案例

- 一次失败的漫游腾讯内部网络

乌云安全威胁top5

- SQL注射漏洞

案例

- 虾米网的一个SQL注射 <http://www.wooyun.org/bugs/wooyun-2010-021894>

乌云安全威胁top6

- 错误的应用配置/默认配置

案例

- Nginx
- Tomcat
- Jboss
- IIS
-

乌云安全威胁top7

- 不安全的账号/认证体系
 - 缺乏认证
 - 流程缺陷

案例

- 任意找回tom邮箱密码
- <http://www.wooyun.org/bugs/wooyun-2010-036446>

乌云安全威胁top8

- 企业内部重要资料/文档外泄

案例

- 通过公开信息可进入某敏感部门内网
- <http://www.wooyun.org/bugs/wooyun-2010-023503>

解决

- 安全是个整体
 - 业务
 - 研发
 - 运维
 - IT
- 以数据为中心
 - 降低数据敏感性
 - 提高攻击的门槛
 - 关注乌云

Q/A

