

Web安全技术

Web Security

课程大作业

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室



中国科学院大学
University of Chinese Academy of Sciences

课程成绩

- CTF之Web安全中期考核: **10%**
- CTF之Web安全期末考核: **10%**
- 大作业: **30%**
- 期末考试: **50%**



□ 大作业：30%

- 大作业一个
- 分组进行
- 要求：认真思考，按时提交
- 布置时间：待选课结束之后

大作业内容：方案一

Password





- ❑ 口令(Password)常用于进入：计算机、加密文件、邮箱、社交网站、网银、电子商务、即时通工具等。
- ❑ 每个人一般拥有2~6个口令，用得最多的口令包括：password, 123456, iloveyou, qwert, football等。



口令泄漏事件



- 2011-12-21: 有网友爆料称, 今天有黑客在网上公开了知名网站CSDN的用户数据库, 这是一次严重的暴库泄密事件, 涉及的账户总量高达600万。

```
0 10 20 30 40 50
1 [redacted] # 12344321 # zdg@csdn.net
2 [redacted] # 6702033137 # chengming_zheng@163.com
3 [redacted] # 730413 # fsta@tom.com
4 [redacted] # 2535263 # hu...ye@263.net
5 [redacted] # KIC43dk6! # cedcjl@21cn.com
6 [redacted] # s12345 # sornail@21cn.com
7 [redacted] # apple # appalp@netease.com
8 [redacted] # 1j7202 # junl@peoplemail.com.cn
9 [redacted] # 12345 # j...buhuan@163.net
10 [redacted] # hebeibdh # fwg@xifw.com
11 [redacted] # 8398518 # mainroad@public.cta.cq.cn
12 [redacted] # priverhe # river1999@netease.com
13 [redacted] # 12345 # lei...ong@21cn.com
14 [redacted] # kingdom # chzhy1@263.net
15 [redacted] # wang...e # chzhy1@263.net__csdn_1
16 [redacted] # today # rss@tjmail.com
17 [redacted] # 6crx99tj # alex@21cn.com__csdn_1
18 [redacted] # smart1010 # guila@21cn.com
19 [redacted] # 980527 # onic...hm@sina.com
20 [redacted] # zzzz # zava@163.net
```

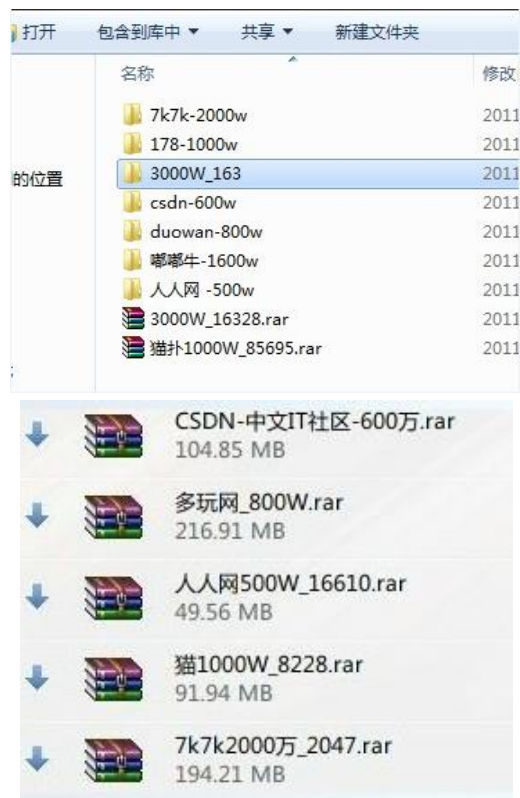


口令泄漏事件——爆发

- 21日16时左右，网友“潇洒小姐燕子”在微博上列出一长串名单，除了CSDN，有同样问题的大网站还有CNBETA、CNZZ、ENET硅谷动力、百合网、珍爱网、开心网、YY、酷6等，并上传了一个类似数据库的东西作为证据。
- 截至22日17时，被点名的网站均没有对此回应



口令泄漏事件——后果

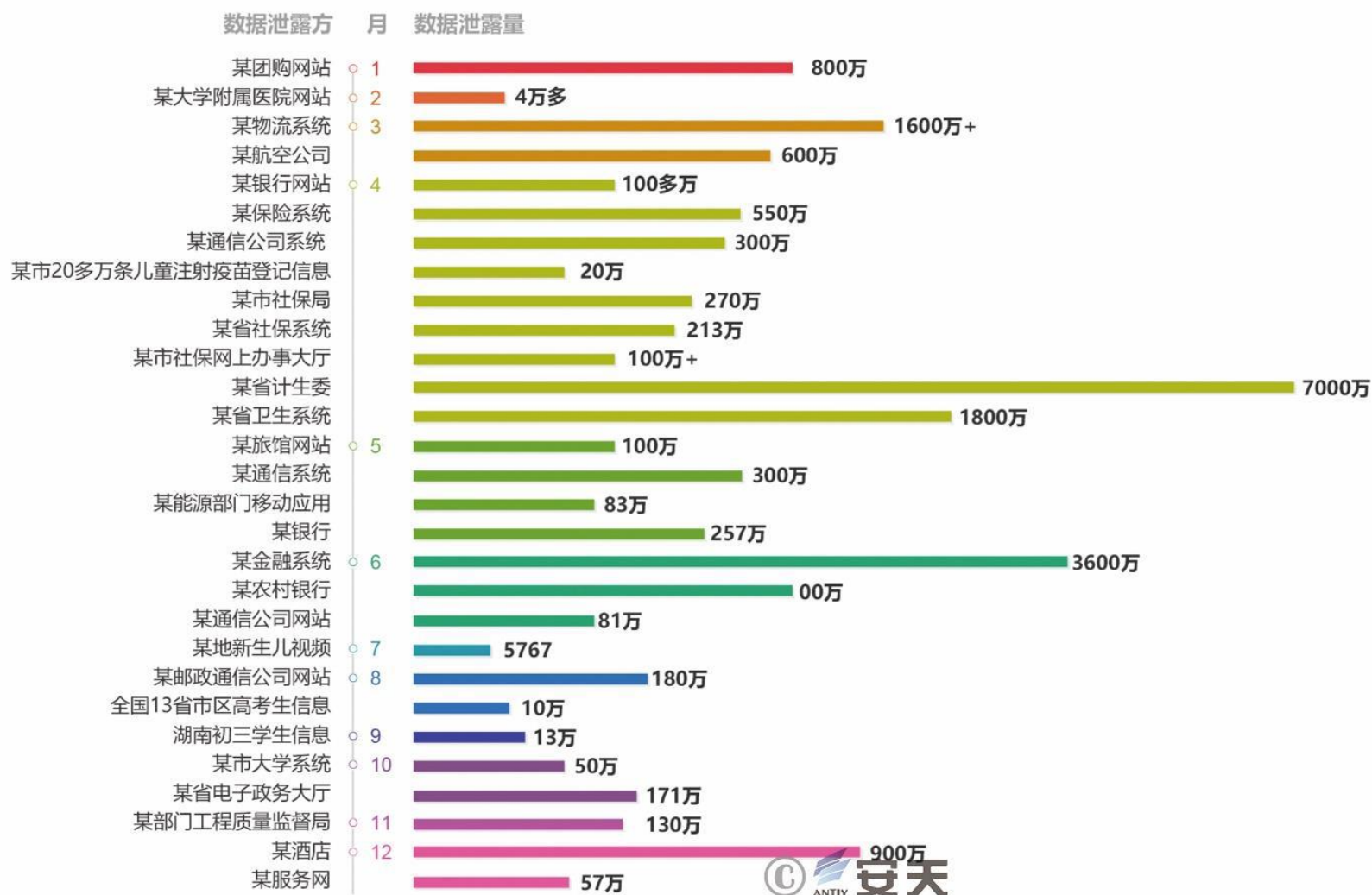


51CTO20110620.rar
360buy.com20111129.sql
cnbeta.com.sql
Discuz.net20110909.sql
dzh.mop.com.sql
hotmail.com(部分).rar
jiayuan.com20110909.sql
kaixin.com20110401.sql
php.net.rar
renren.com20111111.sql
tianya.com2010.sql
weibo.com20110220.sql
youku.com20080604.rar
zhenai.com_20111103.sql

51job.com.sql
alipay.com20100908.sql
CNZZ.com.sql
douban.com20101222.sql
facebook_mail_20111011.sql
it168.com_user_mail20090808.sql
job.dajie.com.rar
mysql.de.rar
PHPWind20101111.sql
sougou_bbs2011.sql
tudou.com200910.sql
xunlei_VIP_20110103.sql
zhaopin.com.rar

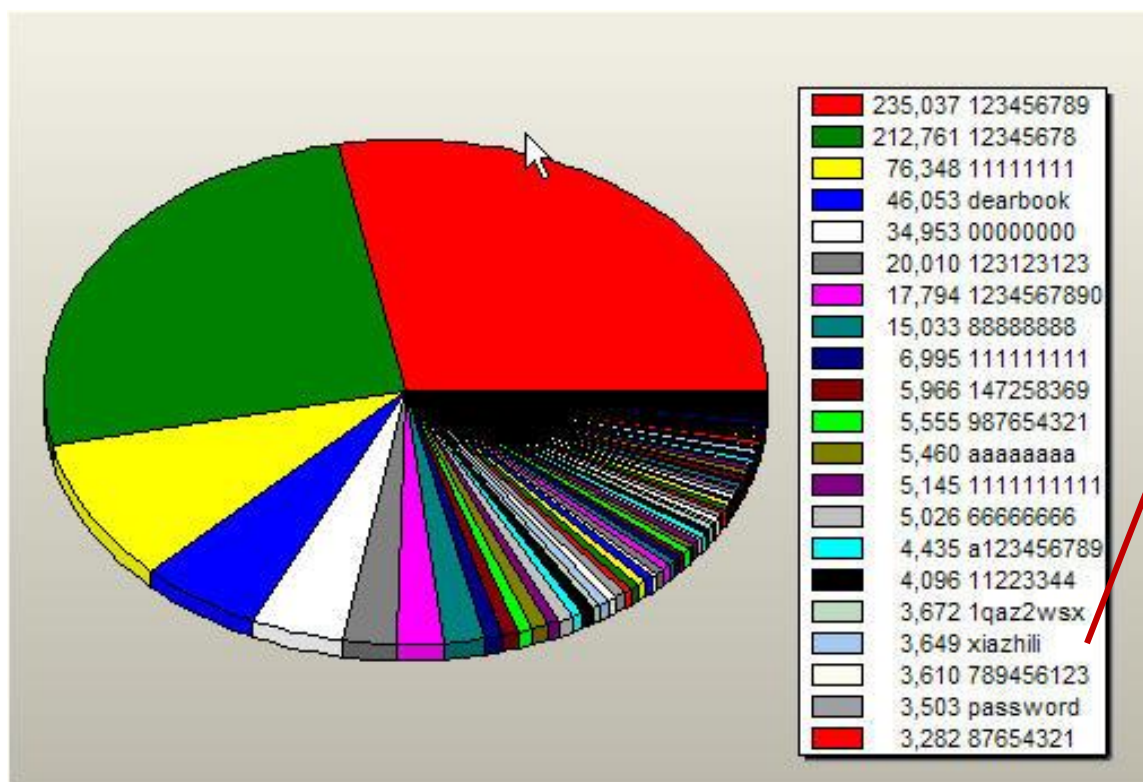


2016年重大数据泄露事件



口令背后那点事儿

——CSDN最常用口令



xiazhili



□ xiazhili 是csdn下载频道09年上传比较多的一MM会员，众多程序员yy的对象，故xiazhili作为密码不足为奇。

CSDN——谁是你的最爱

□ CSDN杯我最喜爱的CSDN密码活动，统计了一下包含ilove***的密码，其中被爱得死去活来的前20位如下：

排名	ilove***	口令数量
1	you	3567
2	you1314	110
3	U	92
4	csdn	68
5	you123	57
6	china	49
7	you520	43
8	thisgame	41
9	java	31
10	chu	20

排名	ilove***	口令数量
11	123	30
12	2hcx	29
13	you1	26
14	myself	22
15	you521	22
16	r	19
17	jay	19
18	qsr	18
19	520	18
20	1314	18



CSDN——爱的就是你

- 排在最前的国家是：**China**
 - 排在最前的网站是：**csdn**
 - 排在最前的编程语言是：**Java**
 - 排在最前的操作系统是：**Linux**
 - 排在最前的电脑品牌是：**apple**
 - 排在最前的明星是：**周杰伦**
 - 排在最前的动物分别是：
 - 1. 猪
 - 2. 猫
 - 3. 猪头
 - 4. 狗
- 排在最前的mm名字是
 - 1. yan (燕)
 - 2. mei (梅)
 - 3. jing (静)
 - 4. ling (玲)
 - 5. ping (萍)
 - 6. dan (丹)
 - 7. fang (芳)
 - 8. wei (薇)
 - 9. juan (娟)
 - 10. nana (娜娜)



CSDN——爱的就是你



学术状态帝
@xueshudi



暗恋了她好几年，一直不敢表白。
后来，他下载到一份CSDN泄露的
用户名密码名单，习惯性的查找她的
邮箱，发现她使用的是ilove加自己
名字的拼音作为密码，正感动得
无以复加时电话响起，只听她在电
话那头颤抖着说：傻瓜，我看到了
你的密码。——程序猿伤不起
啊。。故事好感人啊。。

翻译自中文

2017/9/27 上午9:43



排名	域名	数量	归属
1	mail.ustc.edu.cn	2035	中国科学技术大学
2	sjtu.edu.cn	1874	上海交通大学
3	bjtu.edu.cn	1322	北京交通大学
4	fudan.edu.cn	981	复旦大学
5	stu.xjtu.edu.cn	929	西安交通大学
6	zju.edu.cn	872	浙江大学
7	mails.tsinghua.edu.cn	718	清华大学
8	bit.edu.cn	691	北京理工大学
9	mail.nankai.edu.cn	640	南开大学
10	stu.edu.cn	554	汕头大学



CSDN——口令生成的艺术

□ CSDN的600万用户数据被泄露后，有人发现其中几个最牛的密码：

鱼和熊掌不可兼得

hold?fish:palm

hanshansi.location()! \in [gusucity]

FLZX3000cY4yhx9day

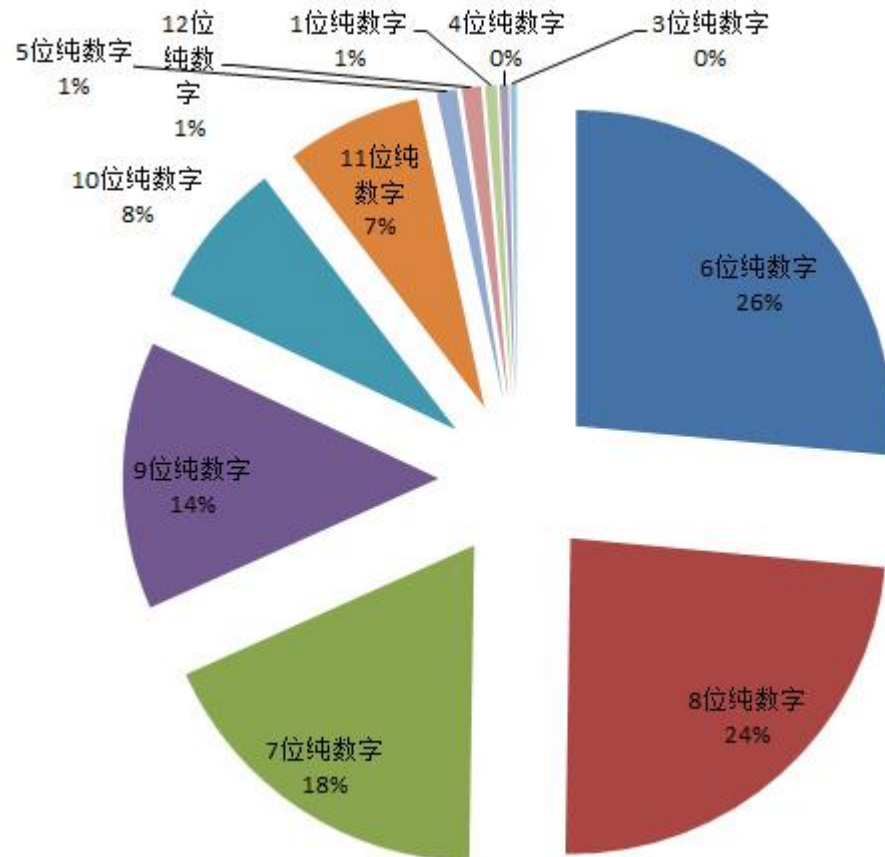
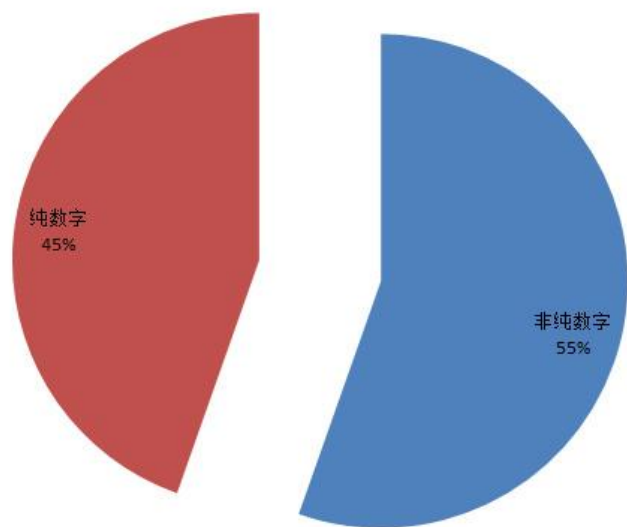
姑苏城外寒山寺

飞流直下三千尺，疑似银河下九天



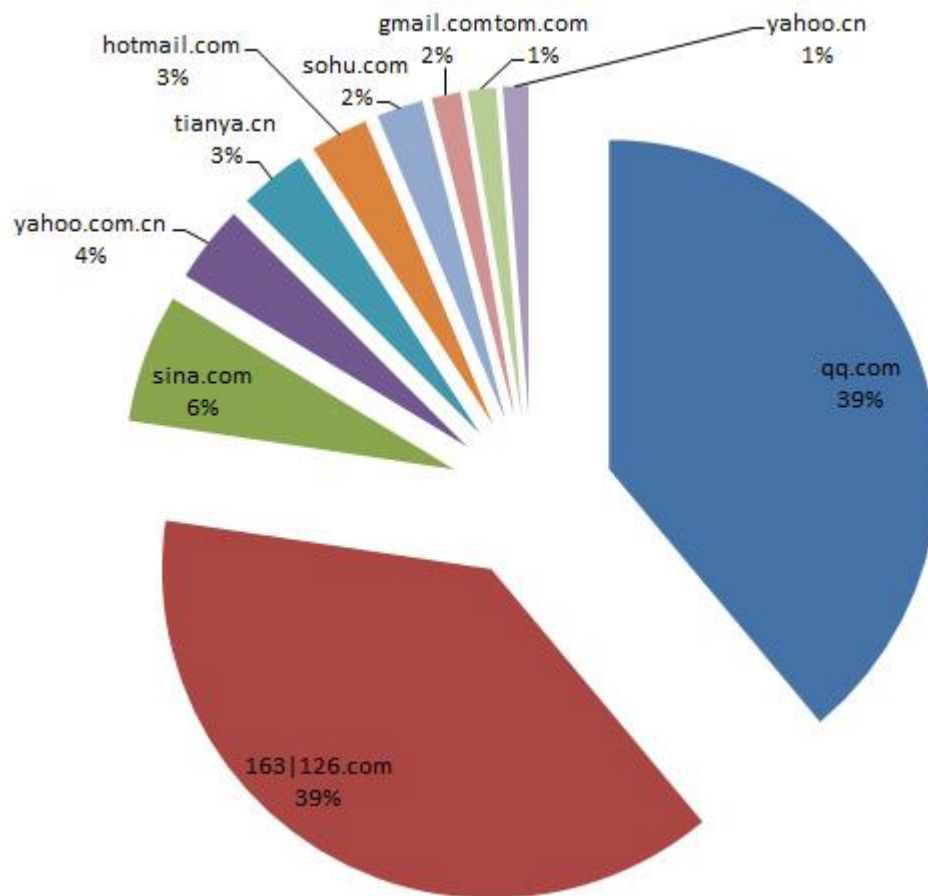
全部泄露口令——纯数字的比例

□ 45%之巨（大约1700万）的被统计用户选择了纯数字作为他们的密码，这反应出国内大多数网民安全意识还相当淡薄



全部泄露口令——纯数字的比例

- 网易和腾讯几乎瓜分了80%的市场份额，在本次统计中两者差距在10万以内



规律性？

□ 为了便于记忆，口令结构和设置方法一般都具有规律性

- 口令结构规律
- 口令设置方法规律

● 例如：password123! 规律 $L_8D_3S_1$

● MySpace口令统计规律

- L_6D_1 是最常见的口令结构，占9.98%，例如loveme8
- 1是使用最多的数字，占有所有数字的27.47%
- !是使用最多的特殊字符，占38.46%



网络与系统安全顶级会议

S&P (Oakland)	IEEE Symposium on Security and Privacy
CCS	ACM Conference on Computer and Communications Security
Security	Usenix Security Symposium
NDSS	ISOC Network and Distributed System Security Symposium



Safer Sign-Ons

Harbor DEF

Session Chair: Tadayoshi Kohno, *Microsoft Research and University of Washington*

Password Managers: Attacks and Defenses

David Silver, Suman Jana, and Dan Boneh, *Stanford University*; Eric Chen and Collin Jackson, *Carnegie Mellon University*

The Emperor's New Password Manager: Security Analysis of Web-based Password Managers

Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song, *University of California, Berkeley*

SpanDex: Secure Password Tracking for Android

Landon P. Cox, Peter Gilbert, Geoffrey Lawler, Valentin Pistol, and Ali Razeen, Bi Wu, and Sai Cheemalapati, *Duke University*

SSOScan: Automated Testing of Web Applications for Single Sign-On Vulnerabilities

Yuchen Zhou and David Evans, *University of Virginia*

Passwords

Harbor DEF

Session Chair: David Wagner, *University of California, Berkeley*

A Large-Scale Empirical Analysis of Chinese Web Passwords

Zhigong Li and Weili Han, *Fudan University*; Wenyuan Xu, *Zhejiang University*

Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts

Dinei Florêncio and Cormac Herley, *Microsoft Research*; Paul C. van Oorschot, *Carleton University*

Telepathwords: Preventing Weak Passwords by Reading Users' Minds

Saranga Komanduri, Richard Shay, and Lorrie Faith Cranor, *Carnegie Mellon University*; Cormac Herley and Stuart Schechter, *Microsoft Research*

Towards Reliable Storage of 56-bit Secrets in Human Memory

Joseph Bonneau, *Princeton University*; Stuart Schechter, *Microsoft Research*

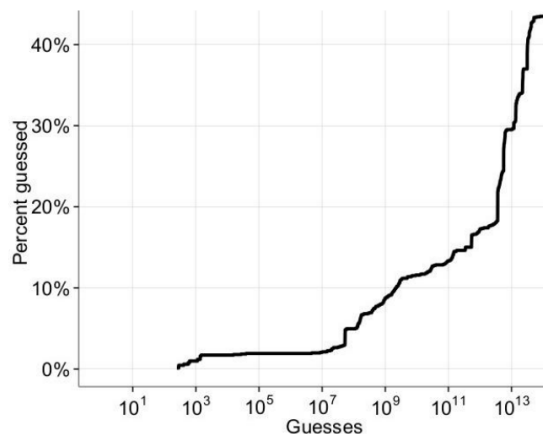


Measuring Real-World Accuracies and Biases in Modeling Password Guessability

Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, and Darya Kurilova, *Carnegie Mellon University*; Michelle L. Mazurek, *University of Maryland*; William Melicher and Richard Shay, *Carnegie Mellon University*

<https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/ur>

Guessability Plots



This paper is included in the Proceedings of the
24th USENIX Security Symposium

August 12–14, 2015 • Washington, D.C.

ISBN 978-1-931971-232

Open access to the Proceedings of
the 24th USENIX Security Symposium
is sponsored by USENIX





Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks

William Melicher, Blase Ur, Sean M. Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor, *Carnegie Mellon University*

<https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/melicher>

This paper is included in the Proceedings of the
25th USENIX Security Symposium

August 10–12, 2016 • Austin, TX

ISBN 978-1-931971-32-4

Open access to the Proceedings of the
25th USENIX Security Symposium
is sponsored by USENIX

推文 14 正在关注 31 关注者 72 喜欢 68

@lorriweet

回复给 Per Thorsheim

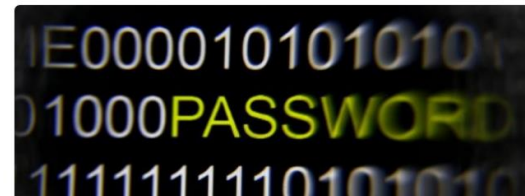


Lujo Bauer @lujobauer · 8月18日
How to measure pwd strength better: goo.gl/BNCYxJ @thorsheim
@adamcaudill @brutemorse @solardiz @hashcat @lakiw
@lorriweet

Lujo Bauer 转推了



Nicolas Christin @nc2y · 8月12日
Story from @washingtonpost summarizes outcomes of some of the password research we've been doing @CarnegieMellon



Password Leakage



English

rockyou

YAHOO!

Chinese

CSDN

全球最大中文IT社区

天涯社区

www.tianya.cn

都都牛

WWW.DUODUONEW.COM

7k7k

178.COM

Over 100 million plaintext passwords



作业要求

分析目标

国内

The logo for CSDN, featuring the letters 'CSDN' in a bold, sans-serif font. The 'C' is red, and the 'SDN' is black.

全球最大中文IT社区

600W

国外



73W

快讯 | 雅虎承认其30亿用户信息全部被黑

👤 Akane ⌚ 2017-10-05 👥 共14246人围观 📄 资讯

近日，已被Verizon电信收购的雅虎公司宣布2013年8月发生的大规模数据泄露事件，影响范围包括所有雅虎用户，这意味着全球30亿雅虎账户无一幸免。据悉，雅虎最初只披露了10亿用户账号被泄露，后续也有陆续增加，但昨天的公告表明，如果你有一个雅虎账号，那么很不幸，你也被曝光了。

去年12月15日，雅虎承认，其系统曾在2013年遭到黑客攻击，约10亿账号的用户姓名、生日、邮箱地址、密码、电话、安全问题和答案全被泄露。除2013年的重大泄露事件以外，雅虎2014年也有至少5亿用户资料落入黑客之手。

作业要求

分组： 每组1-7人

1、基础分析（至少选择下列内容中的三种进行分析）：

- ① 密码构成元素分析（数字、字符、字母等）和结构分析，得到密码中这些基本元素常用的组合方法；
- ② 键盘密码的模式分析，键盘密码就是基于键位变化的一类密码，比如asdfgh；
- ③ 日期密码及其格式分析，难点在于识别日期密码，区分不同的日期格式，日期与其他字符混排的组合方式统计
- ④ 拼音的使用统计，Top10，大小写等，难点是如何识别
- ⑤ 英文单词的使用统计，Top10，大小写等，难点是如何识别
- ⑥ 其他，可以自己想

2、基于分析结果，编写口令字典生成器

3、开放（可选），密码强度分析器：

基于于以上分析结果，采用传统方式或机器学习算法对口令的安全性进行分析和评估，并编程实现。（要求说明评估依据）。

推荐语言：分析（Python、R）；字典生成器（java, C#）

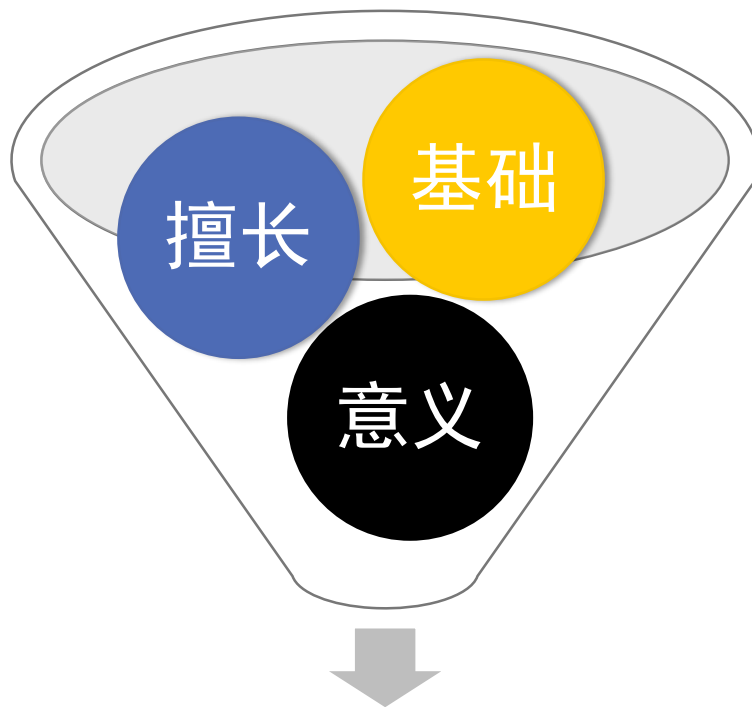
大作业内容：方案二

自 选



大作业内容：方案二

人员组成：每组1-7人



更值得交流分享

年度 year	2017							
月份 month	十月(Oct)			十一月(Nov)				
周次 week	6	7	8	9	10	11	12	13
星期一 (Mon)	9	16	23	30	6	13	20	27
星期二 (Tue)	10	17	24	31	7	14	21	28
星期三 (Wed)	11	18	25	1	8	15	22	29
星期四 (Thu)	12	19	26	2	9	16	23	30
星期五 (Fri)	13	20	27	3	10	17	24	1
星期六 (Sat)	14	21	28	4	11	18	25	2
星期日 (Sun)	15	22	29	5	12	19	26	3

 作业布置

 作业提交

 课堂交流
(暂定)

作业提交

□ 确定分组

- 2017年10月20日之前，组长将组员名单邮件发给助教zhangfangjiao@iie.ac.cn，分组名单包括姓名、学号。

□ 提交时间：2017年11月12日23：00

□ 提交内容：

- 【必须】分组名单-指定组长
- 【必须】课堂交流PPT
- 【必须】相关程序源代码、程序使用说明
- 【可选】附属材料（相关视频、参考资料等）

□ 格式要求

- **各组组长**以**压缩包的形式**上传到课程网站，组员无需上传。若压缩包太大，可以单独联系助教，通过其他方式提交大作业。压缩包命名规则：学号_姓名.rar



[首页](#)

Web安全技术17-18秋季

课程首页

[课程内容](#)[课程大纲](#)[课程目录](#)[讲义课件](#)[课程视频](#)[课堂作业](#)[练习测验](#)[成绩册](#)[课程管理](#)[教务信息](#)[日程安排](#)[通知公告](#)[互动交流](#)

课堂作业

[作业清单](#)[新建作业](#)[评分报告](#)[学生视图](#)[权限设置](#)

学生视图

浏览

作业清单

浏览 1 - 1 / 共 1 项目

[作业标题](#)[<](#)

作业标题	状态	开始	截止日期	已提交 / 最近提交
大作业 修改 复制 评分	开始	2017-10-9 下午9:00	2017-11-12 下午11:00	0/0

[更新](#)



[2017秋]Web Security

扫一扫二维码，加入该群。

谢谢大家

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室



中国科学院大学
University of Chinese Academy of Sciences