Computer System Security **CS3312**

计算机系统安全

2024年 春季学期

主讲教师：张媛媛 副教授

上海交通大学 计算机科学与技术系

CS3312

- **主讲教师：**
  - 张媛媛，上海交大计算机系，副教授
    - 在重要学术会议与刊物上发表论文30余篇：
      - CCS(A)、ICSE(A)、DAC(A)、NDSS(A)、RAID(B)、TSE(A)等等
    - 主持参与10余项 计算机软件与系统安全相关的科研项目：
      - 国家自然科学基金项目、国家重点研发计划、科技部重大专项、上海市重大科研项目等
  - 联系方式：yyjess@sjtu.edu.cn
  - 研究方向：机密计算、可信执行、程序逆向、程序自动化分析、模糊测试
  - 实验室：https://gosec.sjtu.edu.cn

- **课程历史：**
  - 2014年设立研究生专业课《计算机系统安全分析》CS26009/CS7303
  - 2018年设立本科专业课《计算机系统安全》IS308，2023年春季变更课程号为 CS3312

开篇
初识 CS3312

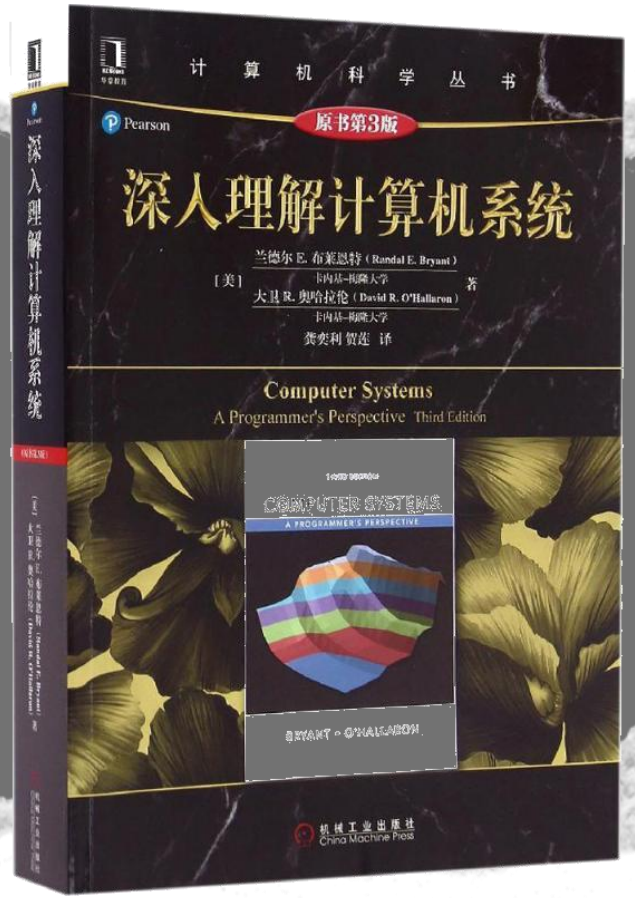
First Sight of CS3312

目录/CONTENTS

01
CS3312 内容简介

If you like System Security or not

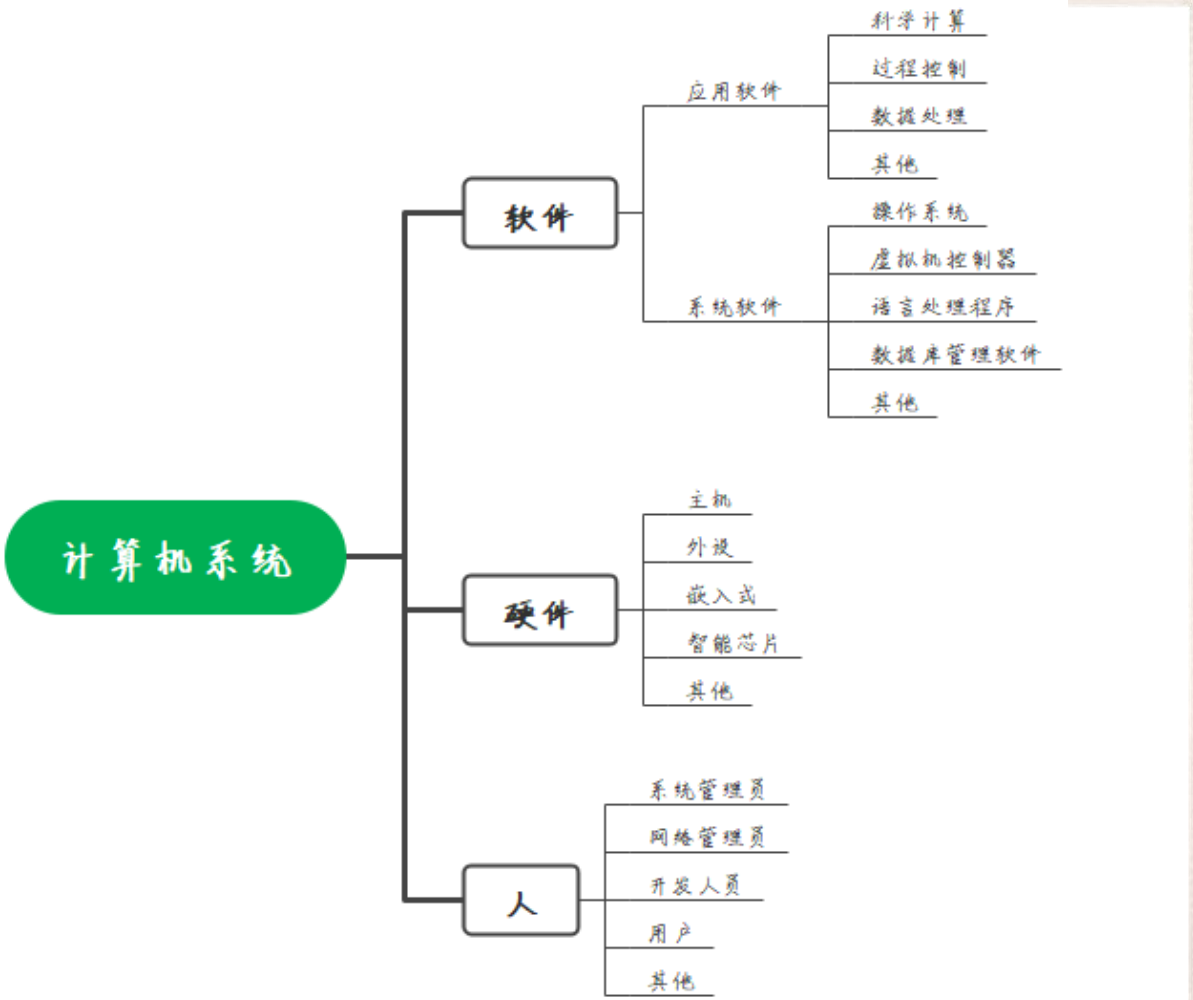
计算机系统



A computer system consists of hardware and systems software that work together to run application programs.

Specific implementations of systems change over time, but the underlying concepts do not. All computer systems have similar hardware and software components that perform similar functions.

计算机系统


计算机系统
软件
应用软件
科学计算
过程控制
数据处理
其他
系统软件
操作系统
虚拟机控制器
语言处理程序
数据库管理软件
其他
硬件
主机
外设
嵌入式
智能芯片
其他
人
系统管理员
网络管理员
开发人员
用户
其他

Computer System Security CS3312

计算机系统安全

National Institute of Standards and Technology
U.S. Department of Commerce

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

为实现信息系统资源(包括硬件、软件、固件、信息/数据和电信)的完整性、可用性和保密性的适用目标而提供的保护。

“安全”vs.“安全” Safety vs. Security

Safety :
The state of being away from hazards caused by natural forces or human errors randomly. The source of hazard is formed by natural forces and/or human errors.

Security :
The state of being away from hazards caused by deliberate intention of human to cause harm. The source of hazard is posed by human deliberately.

Editorial (ED) *Nas/ JEMS, 2015; 3(2): 53-54*

DOI ID: 10.5505/jems.2015.42713

Journal of ETA Maritime Science JEMS JOURNAL

Editorial (ED)

The Definitions of Safety and Security

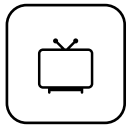
Selçuk NAS
snas@deu.edu.tr

It is seen that the words of safety and security are being used interchangeably in daily use of language. Yet these are defined as a synonym in many dictionaries. On the other hand, for a long while, there has been an attempt to clarify in what way “security” differs from “safety” in terms of meaning in aviation and maritime transportation. Following definitions have been made in the academic literature in order to make a distinction between these two words. In conclusion, the definitions of “safety” and “security” will be considered in the JEMS articles as stated below.

Safety *: The state of being away from hazards caused by natural forces or human errors randomly. The source of hazard is formed by natural forces and/or human errors.*

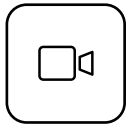
Security *: The state of being away from hazards caused by deliberate intention of human to cause harm. The source of hazard is posed by human deliberately.*

课程大纲



程序与系统

基础知识回顾、PE结构、函数调用过程等



软件安全

软件漏洞：缓冲区溢出、格式化字符串、整型溢出等

漏洞发现方法，漏洞缓解技术

系统安全

操作系统中的安全问题

Linux系统安全问题选析

硬件安全

物理攻击技术：冷冻攻击、总线攻击、侧信道攻击等

安全芯片防护技术

机密计算

可信执行环境技术系统性讲解

Intel SGX, TDX；AMD SEV；RISC-V支持的安全架构

安全热点话题

联邦学习、隐私计算、AI 安全等等

与同类课程内容比较

密码学与信息安全基础

密码算法、多方交互协议、模型设计与分析

抽象、可证明、普遍性

网络安全技术

计算机网络OSI模型

OSI各层次的安全

注意：与Web安全之间存在差异

计算机系统安全

软件安全：漏洞发掘与分析、恶意代码分析

操作安全：资源管理、逻辑冲突等；内存保护、安全执行等

体系结构安全：物理攻击缓解、安全处理器等

*计算机病毒原理

恶意软件的文件格式分析、运行行为分析

02
CS3312 教学物料

How to pass CS3312 and become a security guy

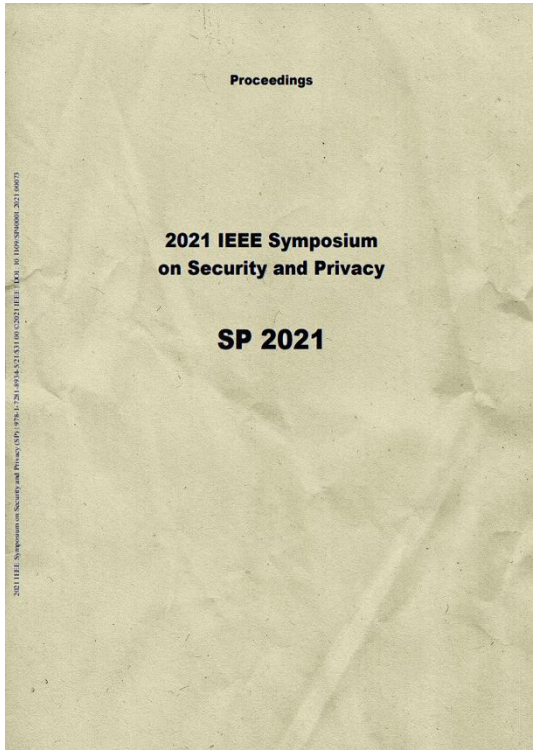
课件来源

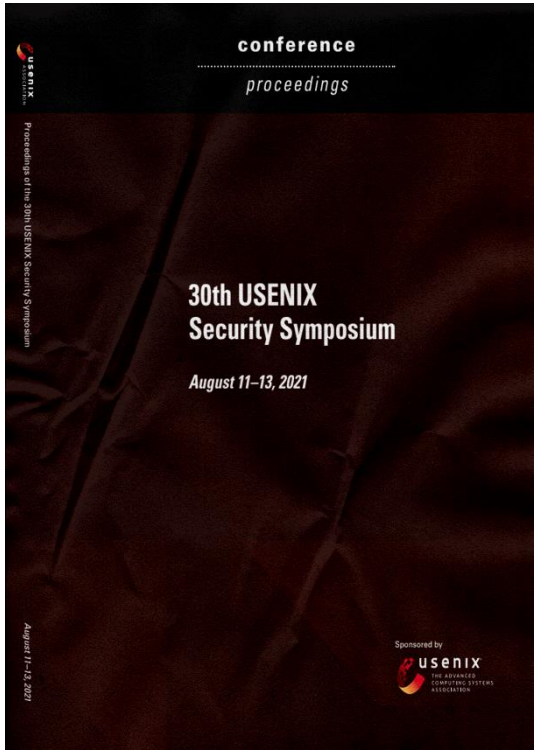
- Michael Goodrich, Roberto Tamassia. (2014). ***Introduction to Computer Security***. Pearson Education; New International Edition.
- 杜文亮.(2020).***计算机安全导论：深度实践***.高等教育出版社.
- 苏璞睿, 应凌云, 杨轶. (2017). ***软件安全分析与应用***. 清华大学出版社.

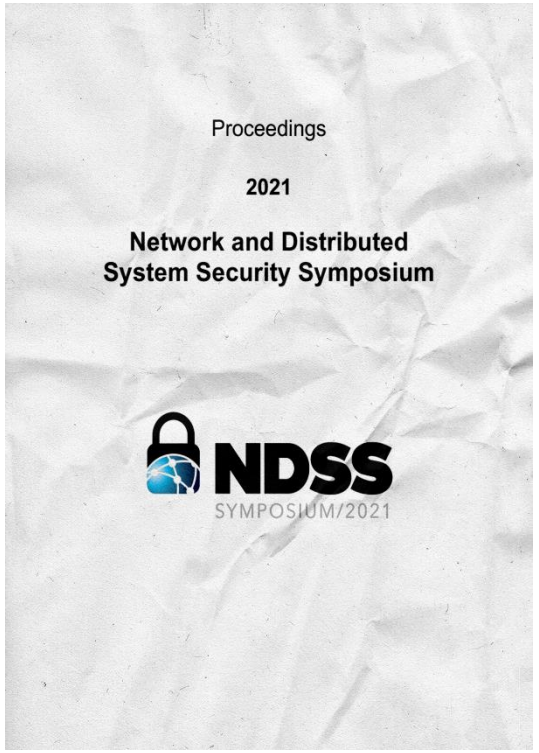
- CTF: Capture the Flag
- Protostar系列入门实验 (32位机) 本课提供配套视频
- Phoenix系列入门实验 (64位机)

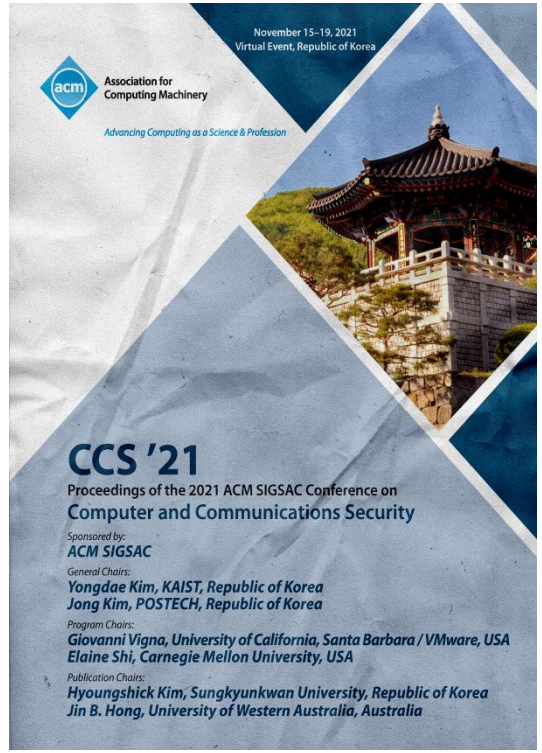
课件来源

论文：安全四大


Proceedings
2021 IEEE Symposium
on Security and Privacy
SP 2021

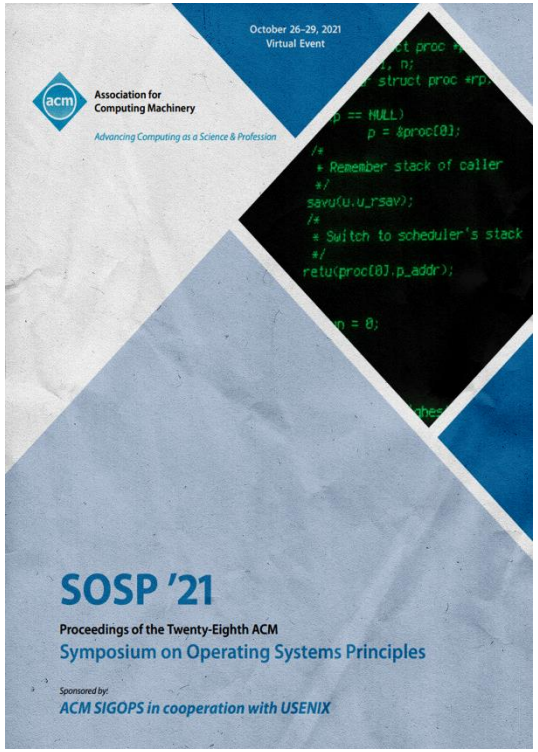

conference
proceedings
30th USENIX
Security Symposium
August 11–13, 2021
Sponsored by
usenix

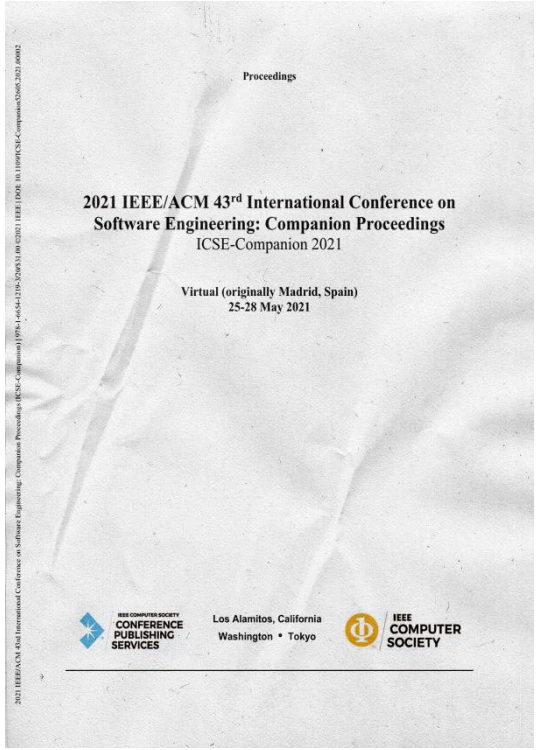

Proceedings
2021
Network and Distributed
System Security Symposium
NDSS
SYMPOSIUM/2021

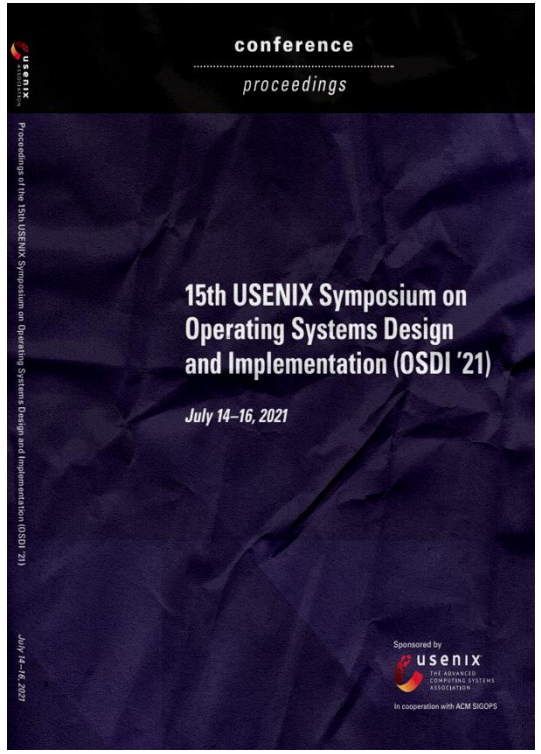

November 15–19, 2021
Virtual Event, Republic of Korea
Association for
Computing Machinery
Advancing Computing as a Science & Profession
CCS '21
Proceedings of the 2021 ACM SIGSAC Conference on
Computer and Communications Security
Sponsored by:
ACM SIGSAC
General Chairs:
Yongdae Kim, KAIST, Republic of Korea
Jong Kim, POSTECH, Republic of Korea
Program Chairs:
Giovanni Vigna, University of California, Santa Barbara / VMware, USA
Elaine Shi, Carnegie Mellon University, USA
Publication Chairs:
Hyoungshick Kim, Sungkyunkwan University, Republic of Korea
Jin B. Hong, University of Western Australia, Australia

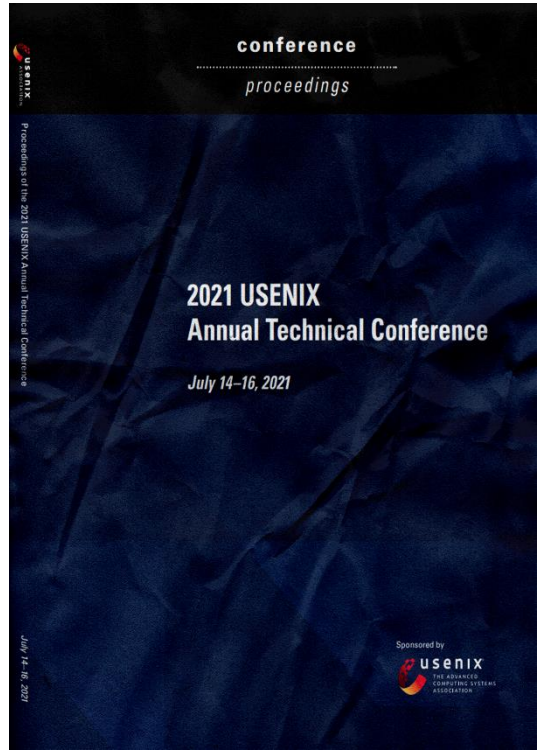
课件来源

论文：系统与软工顶会









考评方式

攻防实践 35%

完成Protostar实践题，提交实验记录：

- Stack 相关漏洞利用
- Format string相关漏洞利用
- Heap 相关漏洞利用
- 一个 SGX 迷你程序的开发实践

虚仿实验平台：
https://gosec.sjtu.edu.cn/gosecstar

课程报告 30%

系统安全作品：

- 一个GPU架构下的软件漏洞攻击利用
- 复现一个2024年最新的容器逃逸CVE
- 一次对可信执行技术(TDX,SEV等)的攻击
- 一次 AI 数据投毒攻击实践

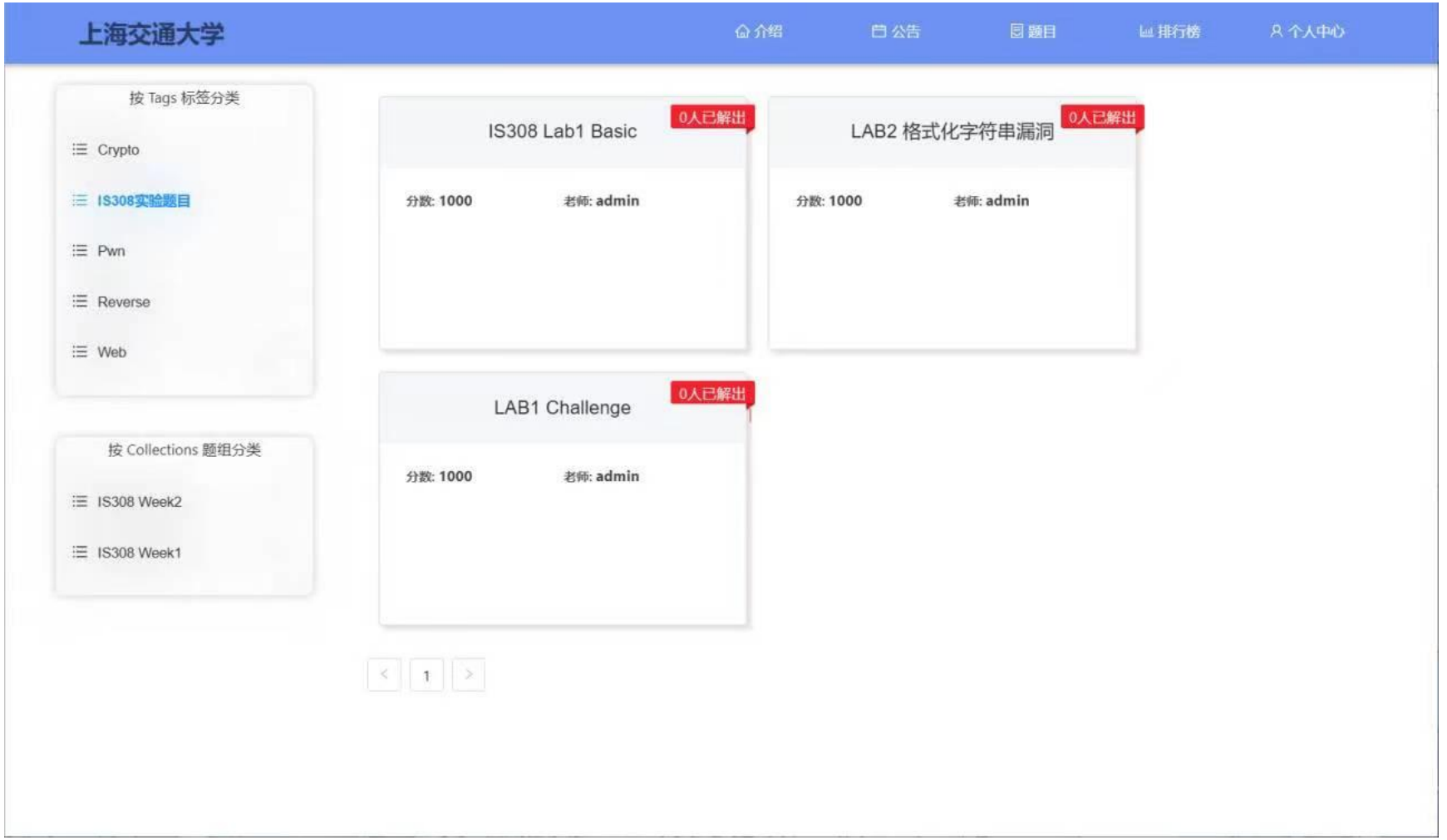
03

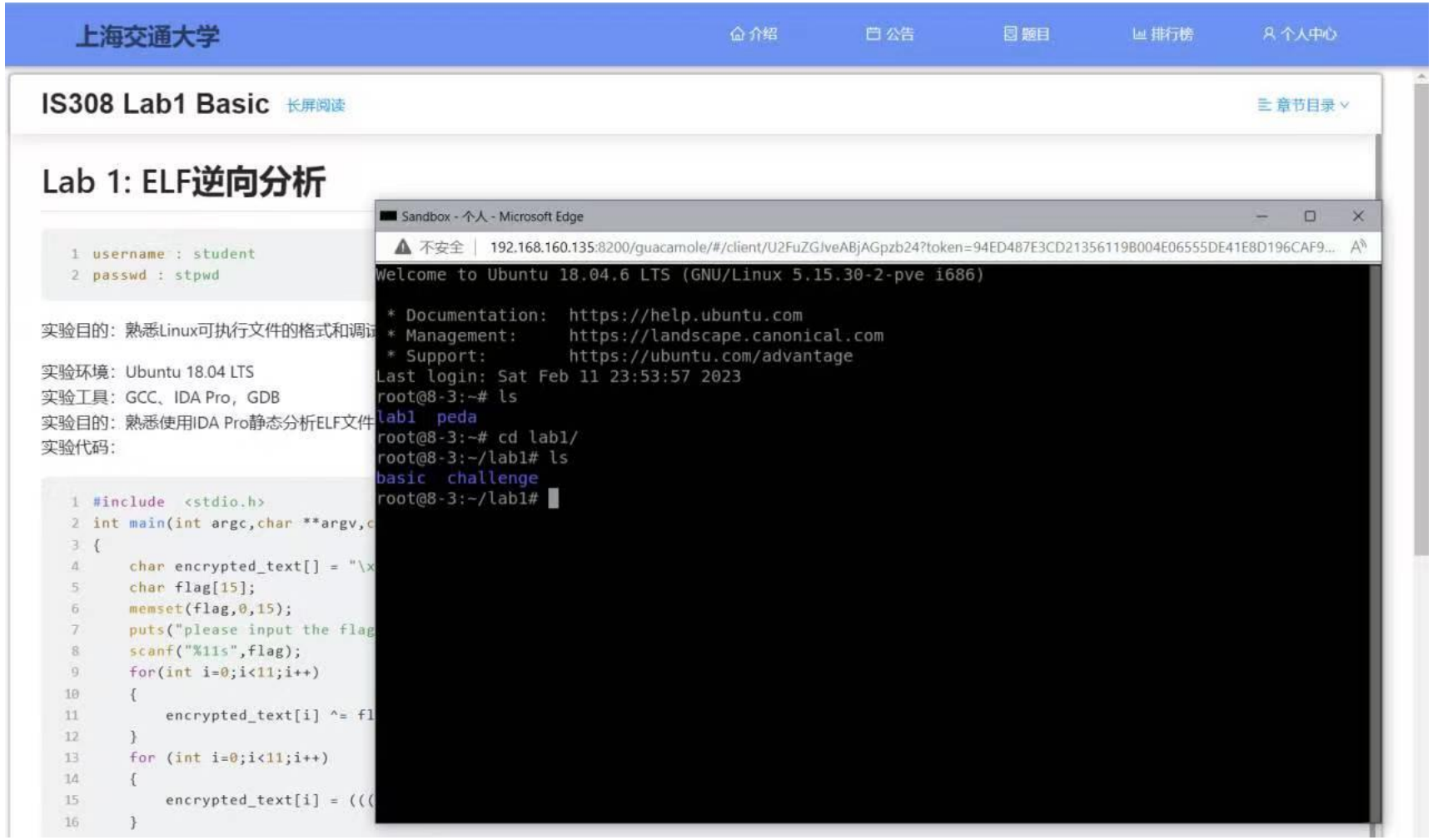
CS3312 课程安排

CS3312 Administrivia

教学安排

课程名称	计算机系统安全 CS3312 Computer System Security	**课程网站**	https://oc.sjtu.edu.cn/courses/ 一切信息：课件、作业、实验大平台、公告
时间地点	1-16周，周一 [3-4节] 1- 8 周，周四 [1-2节] 答疑：微信群内随时提问 线下咨询时间需要提前预约	**参考书(可选)**	1. David R. O ‘Hallaron Randal E. Bryant. (2016). ***Computer Systems: A Programmer’s Perspective***. Pearson Education; 3 Edition.（计算机基本功，5颗星） 2. Michael Goodrich, Roberto Tamassia. (2014). ***Introduction to Computer Security***. Pearson Education; New International Edition.（安全入门，3.5颗星）
实验环境	在线实验平台即将上线， 提供 **线上** 和 **线下** 实验两种方式。 1. 线上环境browser-based 2. 线下自行配置环境 (安装说明视频指引)	**其他资料**	1. 社会工程学也是计算机安全的重要技术 2. 90%以上的有效情报都来自公开渠道 3. 善用数据库：dl.acm，IEEExplore，Google Scholar


上海交通大学
介绍
公告
题目
排行榜
个人中心
按 Tags 标签分类
Crypto
IS308实验题目
Pwn
Reverse
Web
按 Collections 题组分类
IS308 Week2
IS308 Week1
IS308 Lab1 Basic
0人已解出
分数: 1000
老师: admin
LAB2 格式化字符串漏洞
0人已解出
分数: 1000
老师: admin
LAB1 Challenge
0人已解出
分数: 1000
老师: admin
1


上海交通大学
介绍
公告
题目
排行榜
个人中心
IS308 Lab1 Basic
长屏阅读
章节目录
Lab 1: ELF逆向分析
1 username : student
2 passwd : stpwd
实验目的：熟悉Linux可执行文件的格式和调试
实验环境：Ubuntu 18.04 LTS
实验工具：GCC、IDA Pro，GDB
实验目的：熟悉使用IDA Pro静态分析ELF文件
实验代码：
1 #include <stdio.h>
2 int main(int argc,char **argv,c
3 {
4 char encrypted_text[] = "\x
5 char flag[15];
6 memset(flag,0,15);
7 puts("please input the flag
8 scanf("%11s",flag);
9 for(int i=0;i<11;i++)
10 {
11 encrypted_text[i] ^= fl
12 }
13 for (int i=0;i<11;i++)
14 {
15 encrypted_text[i] = (((
16 }
Sandbox - 个人 - Microsoft Edge
不安全 | 192.168.160.135:8200/guacamole/#/client/U2FuZGJveABjAGpzb24?token=94ED487E3CD21356119B004E06555DE41E8D196CAF9...
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.15.30-2-pve i686)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
Last login: Sat Feb 11 23:53:57 2023
root@8-3:~# ls
lab1 peda
root@8-3:~# cd lab1/
root@8-3:~/lab1# ls
basic challenge
root@8-3:~/lab1#

Welcome to CS3312

Computer System Security