《软件安全》课程大纲

一、课程名称（中英文）

中文名称：软件安全

英文名称：Software Security

二、课程代码

SCS2081

三、学时与学分

总学时：48 学时

总学分：3 学分

四、先修课程与后续课程

先修课程：《数据结构》、《C 语言程序设计》、《汇编语言》

后续课程：《计算机网络安全》、《无线网络安全》、《WEB 安全技术》、《工业网络安全综合实践》、《网络安全程序设计》、《计算机网络与安全工程实践》

五、教材与教辅

《软件安全》人民邮电出版社（第三版）

六、适用学科专业

信息安全、密码科学与技术

七、课程简介

·

“软件安全”是一门应用性、工程性、技术性和实践性都很强的核心专业课程，在网络空间安全学科系列专业课程中，是最核心的专业课程之一，软件安全是当前网络空间安全的支撑。课程以软件安全防护、软件安全问题的基本工作原理与实现方法为学习内容，全面讲述软件安全的基本理论知识和基本原理。涵盖软件漏洞分析与利用、恶意代码攻防、构建安全的软件以及软件安全保护等主要内容。详细讨论软件安全的漏洞机理与防御、恶意代码的工作原理与防御方法。课程着力加深学生对软件漏洞机理、软件安全开发和恶意代码以及软件安全防护的系统化理解，建立软件威胁分析、软件安全测试、漏洞分析与防御、恶意代码防御系统安全思想，并有效增强学生的软件安全系统设计能力和解决复杂工程问题的综合能力。课程主要教学内容与软件漏洞等复杂工程问题的特征相呼应，学生必须深入掌握工程原理并通过深入分析，建立相关复杂工程问题的原理模型，且根据原理模型，设计实现的软件安全防护系统，本课程在讲授软件安全威胁、漏洞机理方面，采用国产化目标系统，同时在构建安全的软件环节采用华为软件安全开发规范内容，并使用华为 C 语言技术编程规范中案例进行教学。

八、课程目标

加强学生对信息安全方向软件安全的理解和认识，有效促进学生对软件安全中各个研究和应用方向的把握与理解，并能为学生今后的发展提供专业引导；使学生更加深入地理解目前软件安全所面临的各类威胁本质与其实现机理，进一步激发学生的专业兴趣，加深学生对软件安全的理解，增强学生的专业使命感；使学生掌握目前软件安全防护领域的各类核心技术与理论，提升学生的实践创新能力；提高学生综合利用专业基础知识来设计和研发软件安全防护产品的能力。

课程的具体目标包括：

·

目标 1：加强学生对网络空间安全学科方向中软件安全的理解和认识，促进学生对软件安全中相关的概念、基本原理和基本方法的把握与理解， 使学生更加深入地理解目前软件安全所面临的各类威胁本质与其实现机理，激发学生的专业兴趣，增强学生的专业使命感；能够通过课程学习、文献研究，分析软件安全复杂工程问题中的关键影响因素，并由相关基本原理或推理论证得出有效结论。

目标 2：使学生掌握目前软件安全防护领域的各类技术与理论，尤其是软件漏洞分析与防御原理，提升学生的实践工程能力，能够基于软件执行原理、可计算方法等专业知识对软件脆弱性复杂工程问题进行研究，对软件脆弱性防护问题的解决方案进行分析与评估，并通过信息综合得到合理有效的结论。

目标 3：使学生掌握恶意代码的概念、复制、传播、感染、隐藏等基本原理；掌握采用当前最新的代码分析工具进行恶意软件分析，对比及判定方法， 理解恶意代码、安全与软件漏洞的关系，了解代码安全领域主要技术和相关工具的原理和使用方法，并理解其局限性。 理解漏洞与恶意代码判别的理论、过程，掌握漏洞与恶意软件的防范技术，提高软件安全问题的防范意识，在病毒分析过程中，能够理解和评价针对网络空间健康、可持续发展的影响，理解并掌握通过技术、管理手段降低计算机病毒的负面影响的作用。

九、 教学内容与教学环节

第一章　软件安全概论

1.教学内容

1）什么是软件安全

2）重要性分析

3）安全生命周期

·

4）安全标准

2.教学目标

1）了解软件安全发展动态、威胁与技术现状；

2）了解软件不安全的严重性；

3）掌握软件不安全的表现；

4）掌握软件不安全的原因及其特点；

5）掌握解决软件安全问题的技术措施与方法。

6）课程思政：了解我国软件安全技术的优势和不足；了解互联网中的软件安全问题及与国家安全的关系，学习漏洞攻防相关的法律法规。

本章教学支持的课程目标为目标 1、目标 2。

3.教学重点

1）软件安全问题的严重性

深刻理解当前软件安全的内涵，对软件安全有一个完整的认识和正确的概念。

2）软件不安全的原因

熟悉软件不安全的本质特征，分析存在软件安全问题的代码特点。

3）软件安全防护的措施与方法

熟悉软件开发过程与应用中的安全防护措施，理解措施的优缺点。

4.教学难点

1）软件不安全的本质及其存在原因

理解不安全的代码与安全问题以及威胁的关系。

5.教学环节

围绕教学重点和教学难点，综合应用课堂讨论、作业、课外实践、课外阅读等教学形式。

·

1）课堂讨论

围绕软件不安全的本质特征及其特点，以若干个存在安全问题的实例代码展开。

2）作业

围绕软件安全的特点、防护措施与方法布置。

3）课外实践

要求学生根据自己编写代码经验，设计几个可能存在安全问题的案例并将分析的结果应用于本章的课堂讨论。

4）课外阅读

阅读关于软件安全技术现状与发展的文献。

第二章 软件安全技术基础

本章的主要知识点包括 x64 汇编语言及处理器工作模式，系统引导与控制权，Linux 系统内存管理，Linux 系统权限管理，ELF 文件格式等。同时，结合实践案例，展示如何从攻击者的角度通过逆向分析与利用 ELF 二进制文件中的安全漏洞。

1. 教学内容

1）x64 汇编语言及处理器工作模式

2）系统引导与控制权

3）Linux 系统内存管理

4）Linux 系统权限管理

5）ELF 文件格式

2. 教学目标

1）熟练阅读 x64 汇编指令；

·

2）熟练掌握系统引导与控制权获取的工作原理和实现方法；

3）掌握 X86 处理器工作模式；

4）了解 Linux 内存管理的概念及基本原理；

5）学习并掌握 Ubuntu x86 ELF 二进制文件格式。

3. 教学重点

1）x64 汇编语言

2）系统内存管理

让学生理解虚拟内存与物理内存的映射机制，了解进程内存管理基本原理。

3）利用逆向分析工具对 ELF 文件的实战操作。

4．教学难点

理解 ELF 文件格式的各部分内容，并掌握动态链接的工作原理

5. 教学环节

围绕教学重点和教学难点，综合应用课堂讨论、作业、课外实践、课外阅读等教学形式。

1）课堂讨论

围绕不同操作系统（如 Ubuntu、CentOS）中的 ELF 文件格式展开，讨论与系统安全相关的实践应用。

2）作业

布置与 ELF 文件头、程序头表、节头表等内容相关的作业，以强化对 ELF 文件结构的理解。

3）课外实践

要求学生使用 pwntools、readelf、objdump 等工具对给定的 ELF 文件进行分析和修改，

以巩固课堂所学知识。

·

4）课外阅读

推荐阅读与 Linux 内核、ELF 文件格式相关的书籍和文档，深入理解系统内部结构。

第三章　内存安全与软件漏洞分析

本章的主要知识点包括漏洞生命周期，堆栈原理，函数调用原理与调用细则，栈缓冲区溢出，堆溢出，缓冲区溢出攻击，整数溢出，释放后使用漏洞，数组和字符串格式化问题。

1.教学内容

1）堆栈原理与函数调用

2）栈缓冲区溢出

3）堆溢出与整数溢出

4）缓冲区溢出攻击

5）释放后使用漏洞

6）数组和字符串格式化问题

2.教学目标

1）掌握函数调用堆栈变化过程；

2）掌握栈溢出基本原理；

3）掌握栈溢出攻击基本原理；

4）掌握堆溢出、整数溢出基本原理；

5）掌握格式化字符串漏洞原理。

6）课程思政：在网络空间对抗中，漏洞起到关键支撑作用，高质量漏洞已经成为国家战略资源。

本章教学支持的课程目标为目标 1、目标 2。

3.教学重点

·

1）栈溢出攻击原理

2）堆溢出基本原理

3）整数溢出原理

4.教学难点

1）栈溢出的溢出点攻击原理

掌握核心的间接跳转攻击原理以及堆栈相应变化过程。

2）整数溢出防御

让学生深刻理解整数溢出不可预见性与普遍性。

3）堆溢出攻击原理

掌握堆溢出攻击成功的前提条件。

5.教学环节设计

围绕教学重点和教学难点，综合应用课堂讨论、作业。

1）课堂讨论

本章课堂讨论主要围绕栈溢出过程、整数溢出的实际案例展开。

2）作业

本章作业针对多个代码实例进行分析。

第四章　漏洞利用、发现与防御

本章的主要知识点包括漏洞利用、ShellCode 开发与优化、代码复用技术、软件漏洞测试与发现、漏洞利用平台与框架、漏洞相关工具、漏洞防御技术手段等。

1.教学内容

1）漏洞利用与 ShellCode 开发

·

2）代码复用技术与原理

3）软件漏洞测试与发现

4）漏洞利用平台、工具与防御技术

2.教学目标

1）掌握堆栈溢出漏洞利用基本原理；

2）掌握 ShellCode 开发的工作原理；

3）掌握代码复用技术原理；

4）掌握软件漏洞测试与发现技术；

5）了解软件漏洞测试与挖掘平台、框架以及相关工具；

6）了解漏洞防御技术手段。

7）课程思政：从漏洞利用与防御博弈过程理解网络空间攻防发展态势，体会本专业所肩负的网络空间安全防护的责任。

本章教学支持的课程目标为目标 1、目标 2。

3.教学重点

1）ShellCode 开发原理

掌握 ShellCode 制作原理，理解缺乏上下文环境下 ShellCode 执行过程。

2）代码复用的工作原理

深刻理解代码复用的机理、前提条件及系统漏洞防御机制对代码复用影响。

3）漏洞测试与挖掘

掌握软件漏洞测试与挖掘技术。

4.教学难点

1）漏洞利用的间接跳转技术

·

2）代码复用中堆栈的变化过程

3）漏洞挖掘中的关键技术

5.教学环节

围绕教学重点和教学难点，综合应用课堂讨论、作业、课外阅读。

1）课堂讨论

本章课堂讨论围绕漏洞利用的间接跳转技术、代码复用中堆栈的变化过程等开展。

2）作业

本章作业主要围绕 ShellCode 原理、代码复用设计等内容布置。

3）课外阅读

搜索漏洞分析最新研究和业界的新进展，并阅读。

第五章　构建安全的软件

本章的主要知识点参考华为的安全开发规范，包括软件开发生命周期、软件设计阶段威胁识别与建模、安全代码的编写、软件的安全性测试、漏洞响应和产品的维护等知识点。

1.教学内容

1）软件开发生命周期与威胁建模

2）安全代码编写与注意事项

3）软件安全性测试与漏洞响应

2.教学目标

1）掌握软件开发生命周期概念以及阶段；

2）掌握软件设计阶段威胁建模，深刻理解其建模过程；

3）掌握安全代码的编写需要注意的一些问题；

·

4）了解软件的安全性测试原理及其发展；

5）了解漏洞响应和产品的维护。

6）课程思政：理解安全问题的解决还需要从源头开始，体会系统观与全局观的重要性，采用我国华为公司的安全开发规范以及相应的编程技术规范，感受我国软件开发水平的提升。

本章教学支持的课程目标为目标 1、目标 2。

3.教学重点

1）软件开发生命周期

2）软件设计阶段威胁建模

3）安全代码的编写

4.教学难点

1）软件设计阶段威胁建模的完整性与前瞻性

掌握威胁建模是安全问题解决和安全软件设计的出发点及基本设计方法。

2）安全代码编写的关键问题

掌握安全代码编写中的一些关键技术。

5.教学环节

围绕教学重点和教学难点，除课堂讲授外，还需综合应用课堂讨论、作业、课外阅读。

1）课堂讨论

本章课堂讨论围绕威胁建模实例、安全代码实例等内容展开、部分采用华为安全编程中实例。

2）作业

根据目标场景做威胁建模。

3）课外阅读

搜索安全开发、SDL 相关文献，查找华为安全开发规范文档并阅读。

·

第六章　软件安全防护技术

本章的主要知识点包括代码混淆工作原理、软件防篡改原则与方法、软件水印等，重点介绍国产化自主版权水印以及混淆技术。

1.教学内容

1）软件安全防护技术概述

2）代码混淆工作原理与设计思想

3）软件防篡改基本原则与方法

4）软件水印的工作原理与国产化技术

2.教学目标

1）熟悉软件安全防护的主要技术及方法；

2）掌握代码混淆方法的设计思想与实现原理；

3）掌握软件防篡改基本方法；

4）掌握软件水印的工作原理。

5）课程思政：软件防护对保护知识产权的意义，介绍我国当前知识产权进步与发展。

本章教学支持的课程目标为目标 1、目标 2。

3.教学重点

1）代码混淆、软件防篡改和软件水印技术的基本概念和安全目标

2）现有软件保护技术及其存在的不足

4.教学难点

1）“虚拟黑盒”安全目标的不可能性

5.教学环节

·

围绕教学重点和教学难点，除课堂讲授外，还需综合应用课堂讨论、作业、课外阅读。

1）课堂讨论

本章课堂讨论围绕代码混淆、软件水印实现机制等内容展开。

2）作业

要求学生在指定目标软件上亲手实现一种现有的代码混淆或软件水印方法。

3）课外阅读

搜索软件安全防护相关文献，阅读并了解最新的一些技术动态。

第七章　计算机病毒概念及发展

本章的主要知识点包括计算机病毒的基本概念、发展历史、分类、命名规则、未来发展趋势。

1.教学内容

1）计算机病毒基本概念与内涵

2）计算机病毒发展历史与分类

3）恶意代码定义、特征及产生原因

4）恶意代码危害与防治方法

2.教学目标

1）了解计算机病毒的定义、内涵、不足；

2）了解恶意代码的定义、内涵、典型特征；

3）了解恶意代码产生的原因、历史发展的阶段；

4）了解恶意代码的主要危害、防治方法、病毒防护软件的概况。

5）课程思政：通过打印机中被植入病毒的历史事件，了解计算机病毒危害的严重性，甚至可以危及国家军事系统，形成专业学习的历史使命感与责任感。

·

本章教学支持的课程目标为目标 1、目标 2。

3.教学重点

1）计算机病毒产生是计算机技术发展的必然

2）计算机病毒的危害巨大，并随着技术进步而不断发展

4.教学难点

1）计算机病毒发展趋势

5.教学环节

围绕教学重点和教学难点，除课堂讲授外，还需综合应用课堂讨论、作业、课外阅读。

1）课堂讨论

本章课堂讨论围绕是否接触过计算机病毒、希望从课程中学到哪些相关内容展开。

2）作业

查找最近一个月的互联网安全威胁报告，了解目前各方面威胁数据的概况。

从病毒名称 Win32.Happy99.Worm 可以获得哪些信息?

3）课外阅读

从 wildlist、病毒公告牌等网站，了解目前病毒发展趋势。

第八章　传统计算机病毒技术

本章的主要知识点包括可执行文件格式、传统典型计算机病毒原理、实验。

1.教学内容

1）可执行文件格式（COM、EXE、PE）

2）引导型病毒原理与实验

3）BIOS 和 UEFI 固件引导病毒

·

4）COM 文件病毒原理与实验

5）PE 文件型病毒原理与实验

6）DOC 宏病毒原理

2.教学目标

1）了解 COM、EXE、PE 可执行文件格式；

2）掌握引导型病毒原理及实验；

3）了解 BIOS、UEFI 固件引导病毒；

4）掌握 COM 文件病毒原理与实验；

5）掌握 PE 文件型病毒原理与实验；了解 DOC 的宏病毒原理。

6）课程思政：通过“方程式”组织在硬盘控制芯片中植入恶意代码的事件，了解恶意代码在固件方面的发展趋势，意识到技术是双刃剑，需要不断学习，坚定信念，坚守职业道德。

本章教学支持的课程目标为目标 1、目标 2、目标 3。

3.教学重点

1）软件恶意代码的自我复制；COM 病毒感染过程

2）计算机病毒的危害巨大，并随着技术进步而不断发展

4.教学难点

1）病毒为什么具有了自我复制的功能

2）感染的实现方法；不同病毒的感染实现不同

5.教学环节

围绕教学重点和教学难点，除课堂讲授外，还需综合应用课堂讨论、作业、课外阅读。

1）课堂讨论

本章课堂讨论围绕是否接触过计算机病毒、希望从课程中学到哪些相关内容展开。

·

2）作业

COM 病毒样本调试及简单分析。

3）课外阅读

早期病毒研究的相关文献阅读：Cohen 的论文；蠕虫分析论文。

第九章　网络类型病毒

本章的主要知识点包括网络病毒的分类，蠕虫、木马的结构。

1.教学内容

1）网络病毒分类

2）蠕虫病毒机制与逻辑结构

3）木马病毒机制与逻辑结构

2.教学目标

1）了解网络病毒的分类（按传播机制）；

2）掌握蠕虫病毒的机制、逻辑结构；

3）掌握木马的机制、逻辑结构。

4）课程思政：专业技术是双刃剑，比如木马技术，可以用在机房远程管理、远程协助类的软件中，病毒加密技术可以用于软件的版权保护中，所以我们必须坚定社会主义道路的信念，树立正确的价值观，坚守职业道德。

本章教学支持的课程目标为目标 1、目标 2、目标 3。

3.教学重点

1）蠕虫的传播过程

2）木马的伪装隐藏方法

·

4.教学难点

1）恶意代码技术具有时代特点，不断变化，需要对计算机不同层面的知识都有深入了解

2）具体传播的复现

5.教学环节

围绕教学重点和教学难点，除课堂讲授外，还需综合应用课堂讨论、作业、课外阅读。

1）课堂讨论

本章课堂讨论围绕是否接触过计算机病毒、希望从课程中学到哪些相关内容展开。

2）作业

网络蠕虫与计算机病毒都可以进行自我复制传播，具体有何区别？防护策略有哪些不同？远程控制型木马的控制端与被控制端有哪些连接方式？有何优缺点？木马样例阅读（选做）。

3）课外阅读

KidLogger 软件试用，对其特点、隐患、法律合规性进行评价。

第十章　恶意代码防治技术

本章的主要知识点包括恶意代码的查找技术、恶意代码的清除技术。

1.教学内容

1）恶意代码查找与清除技术

2）变形代码特点及检测

3）行为检测技术与宏观防治

2.教学目标

1）了解计算机病毒的定义、内涵、不足；

2）了解恶意代码的定义、内涵、典型特征；

·

3）了解恶意代码产生的原因、历史发展的阶段；

4）了解恶意代码的主要危害、防治方法、病毒防护软件的概况。

5）课程思政：通过计算机病毒及防治技术的对抗发展过程，理解专业领域需要终身学习及不怕困难勇攀科学高峰的顽强意志。

本章教学支持的课程目标为目标 1、目标 2、目标 3。

3.教学重点

1）恶意代码的查找技术；特点；算法

2）变形代码的特点及检测技术

3）行为检测技术

4）网络环境下病毒的宏观防治

4.教学难点

1）基于特征串的查杀技术

2）基于行为的特征建模及鉴别技术

5.教学环节

围绕教学重点和教学难点，除课堂讲授外，还需综合应用课堂讨论、作业、课外阅读。

1）课堂讨论

本章课堂讨论围绕代码变形的方法有哪些方式展开，探索相应的防护方法。

2）作业

基于 clamav 开源项目，阅读相关资料，了解查杀软件的构架、算法。

3）课外阅读

查阅 Cuckoo SandBox 相关文献，了解集成工具的功能；

阅读文献“Metamorphic malware detection using base malware identification

·

approach”了解恶意代码隐藏技术及检测。

第十一章　恶意代码理论模型

本章的主要知识点包括恶意代码与生物病毒的异同、生物病毒传播模型、感染率、治愈率、连接率、计算机病毒数学模型。

1.教学内容

1）恶意代码与生物病毒的异同

2）生物病毒传播模型（SIR、SEIR）

3）感染率、治愈率与连接率

4）计算机病毒数学模型

2.教学目标

1）了解计算机病毒的模型及不可判定性；

2）掌握病毒的基本功能机理；

3）掌握传统经典的传播模型。

4）课程思政：通过与计算机病毒传播模型类似的经典传染病模型对比，结合 Covid-19 传播曲线，了解控制病毒传播条件，坚定中国特色社会主义道路的信念，增加国家道路自信、培养历史使命感与社会责任感。

本章教学支持的课程目标为目标 1、目标 3。

3.教学重点

1）SIR、SEIR 模型

2）病毒的形式化定义

4.教学难点

·

1）病毒特征与病毒理论间的关系

5.教学环节设计

围绕教学重点和教学难点，除课堂讲授外，还需综合应用课堂讨论、作业、课外阅读。

1）课堂讨论

本章课堂讨论结合病毒传播模型的参数对传播的影响相关内容展开。

2）作业

能否对不同病毒的危害程度进行比较？需要哪种类型的模型？

3）课外阅读

阅读 2019 年期刊文章“A novel approach for early malware detection”了解早期恶意代码检测的进展。

十、学时分配

序号	主要内容	课内学时	课外学时
1	第一章 软件安全概述	4	
2	第二章 软件安全技术基础	4	
3	第三章 内存安全与软件漏洞分析	6	
4	第四章 漏洞利用、发现与防御	6	
5	第五章 构建安全的软件	2	
6	第六章 软件安全防护技术	2	
7	第七章 计算机病毒概念及发展	3	
8	第八章 传统计算机病毒技术	6	
9	第九章 网络病毒技术	6	

·

10	第十章 恶意代码检测及清除	6	
11	第十一章 恶意代码理论及传播模型	3	
总计		48	

十一、教学策略

1.教学方法

本课程的教学与学习过程中，要牢固树立并应用软件层次安全与开发安全周期的观点，以及恶意代码的原理及防范意识。注重培养、树立原理与实际应用相结合的观点：

1）讲述中注重把“软件安全的原理”与“操作系统原理”、“高级程序语言”、“软件工程”等课程有机结合起来，理解其编程的基础、技术和原理；

2）从软件安全问题的原因、分类中，给学生们解释清楚软件漏洞原理、软件漏洞与恶意代码及其检测与挖掘的机器特征，并把后续的软件安全防护技术的发展与一般的计算机、网络技术发展结合进来，再进一步解释防护技术的实现，同时要结合其它技术特征的发展等相关内容；

3）软件安全是技术应用性很强的课程，注重培养学生与高级程序设计语言(如 C 语言)和操作系统等软件课程的关系，将以功能模块的分解和设计为手段，鼓励学生对软件安全编程的设计、实现。

4）关于 PBL 教学案例的设计可根据不同培养模式以及学生的不同需求进行调整。下面给出两个 PBL 示例。

PBL 案例 1：针对大规模不间断网络服务，结合软件安全设计、编程、运行安全以及内存安全等措施实现一套稳定可靠的大规模多线程不间断服务软件；

PBL 案例 2：设计、实现以 Fuzzing 测试为主要原理的漏洞测试与挖掘平台；

·

PBL 案例 3：基于特征码的恶意代码识别。通过自己定义特征码、建立简单而精致的特征码库；设计并实现对计算机文件系统的特征码扫描技术。

2.学习方法

“软件安全”是一门应用性、技术性和实践性都很强的核心专业基础课程，学习过程中，首先要注重对课程基本原理的钻研，要引导学生积极参与课堂讨论，深刻理解原理和技术本质；其次，要站在系列课程的角度学习，本课程的学习需要汇编语言，C 语言程序设计等前导课的知识和技术支撑；第三，独立完成课程配套开设的独立实验，通过实验，加强对课程理论知识的理解，同时，训练学生发现问题、分析问题和解决问题的能力。

十二、课程评价

1.课程成绩构成

课程最终成绩由平时成绩和课程期末考试成绩综合而成，各部分成绩的比例如下：

平时成绩：30%。作业将引导学生复习和巩固讲授的内容(基本理论、基本方法、基本理论分析与计算、课外阅读报告等），主要考察作业完成率和完成质量。另外，按学校要求，适当进行考勤抽查，不满足规定的不能参加课程考试。

期末考试成绩：70%。主要考核软件安全基础知识和基本能力的掌握程度，是对学生学习情况的全面检验。考试强调对软件安全的基本概念、基本方法和技术的掌握，并通过综合型试题考核学生运用所学知识、解决复杂工程问题的能力。考试采用书面闭卷考试形式。题型为计算、分析、设计、综合应用等题型。

课程考核成绩评定如表 1 所示。

表 1 软件安全课程考核与成绩评定

课程目标	考核与评价方式及成绩占所在项的比例(约)

·

	平时成绩	期末考试成绩
1	30%	70%
2	30%	70%
3	30%	70%
总成绩	平时总成绩×0.3+期末考试总成绩×0.7	

2.考核与评价标准（考试成绩评价标准见参考答案评价）

（1）课程目标 1 的评价标准

平时成绩**评价标准**			
优秀	良好	及格	不及格
通过文献研究、数据分析等方法，分析信息安全领域复杂工程问题内在规律，比较解决方案的优缺点与合理性，得到有效结论。	通过较为充分的文献研究与数据分析，较好地分析了信息安全领域复杂工程问题的规律。能够比较解决方案的优缺点，并且做出合理的分析与选择，结论具有一定的实际应用价值。论证过程较为完整，引用的文献具有参考性，思路清	通过基本的文献研究与数据分析，能够初步分析信息安全领域复杂工程问题的某些规律。解决方案的比较存在一定的局限性。论证过程不够严谨，文献引用较少，但能够达到基本的学术要求，具备一定的分析与解决问题的能力。	不能进行有效的文献研究与数据分析，无法清晰分析信息安全领域复杂工程问题的内在规律。对解决方案的比较浅显，合理性分析严重不足，结论无实际意义。论证过程存在明显逻辑漏洞，文献引用不当或缺失，缺乏基本的独立思考和

·

	晰，具有较好的问题解决能力。		问题解决能力。

(2) 课程目标 2 的评价标准

平时成绩**评价标准**			
优秀	良好	及格	不及格
能够基于信息安全和相关科学原理，主动发现信息安全领域复杂工程问题及其关键要素，明确研究的内容与目标。	能够基于信息安全和相关科学原理，较为主动地发现信息安全领域复杂工程问题及其关键要素，并清晰地定义研究的内容与目标。	在信息安全和相关科学原理的基础上，能够基本发现信息安全领域复杂工程问题的部分关键要素，但主动性不足。研究内容与目标的定义较为笼统，存在一定模糊性，部分研究方向不够明确。	不能有效运用信息安全及相关科学原理，无法主动发现信息安全领域复杂工程问题及其关键要素。研究内容与目标不明确，缺乏方向性，问题分析无法识别关键要素。

(3) 课程目标 3 的评价标准

平时成绩**评价标准**			
优秀	良好	及格	不及格
能够理解用技术、管理手段降低负面影响的作用与其局	能够较好理解技术和管理手段在减少信息安全领域负面	对技术和管理手段在降低负面影响中的作用有基本的理	不能有效理解技术和管理手段在降低负面影响中的作

•

限性。	影响中的重要作用，准确识别其应用场景与局限性。	解，能够识别常见的局限性，但分析不够深入。	用，无法识别其局限性。选择和应用技术或管理措施时缺乏针对性，难以形成可行的解决方案。

•