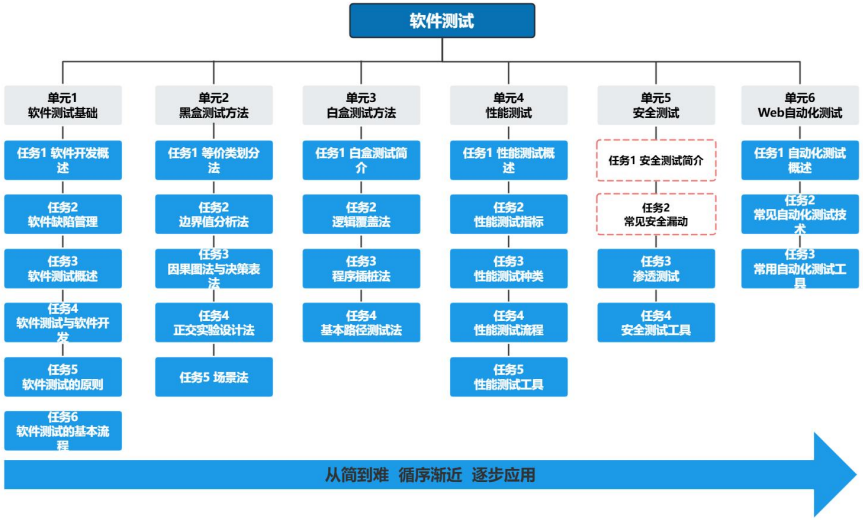
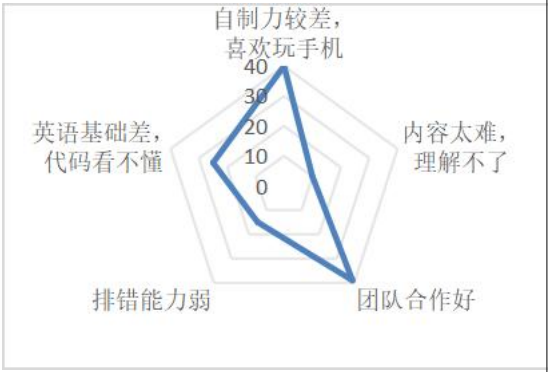
教学单元:安全测试（2 学时）

19.1 授课信息					
单元名称	安全测试	所属课程	软件测试	教学模式	线上线下混合式教学
授课学时	2 学时	授课地点	多媒体教室	授课对象	软件技术专业大二学生
教学内容分析	本次课是“软件测试”中的**第37-38学时**，是项目五“安全测试”的第一、二个任务，教学内容主要是本章讲以软件测试方法之一的安全测试进行讲解，安全测试时软件测试保障软件正常运行的方法之一。教师在教学过程中当列举实际的案例进行讲解，让学生掌握安全测试方法。 本次课的理论与实践并重，教学内容主要分为三个主要部分。 第一部分以理论知识讲解为主，重点介绍安全测试的简介、常见安全漏洞。 第二部分与第三部分通过做中学，学中练的方式，带领学生学习了解性能测试的流程。				
知识点梳理					

返回目录

19.2 学情分析

知识技能分析	1.知识基础：高职二年级学生，已学习多种程序设计语言（如C语言、JAVA、网页前端的知识等）。 2.技能运用情况：	
学习能力分析	1.学生熟悉软件开发工具，熟练应用学习平台完成课前预习及课后作业;经过磨合及调整，学习小组基本达到稳定的状态，能够合作产出成果，勇于上台展现，但总结能力和表达能力还有待加强。 2.理解长篇代码结构、代码排错能力有待加强。	
学习特点分析	1.对人工智能兴趣浓厚，初步掌握生成式AI的应用技巧。 2.部分学生处于被动学习状态，创新能力不足。	

返回目录

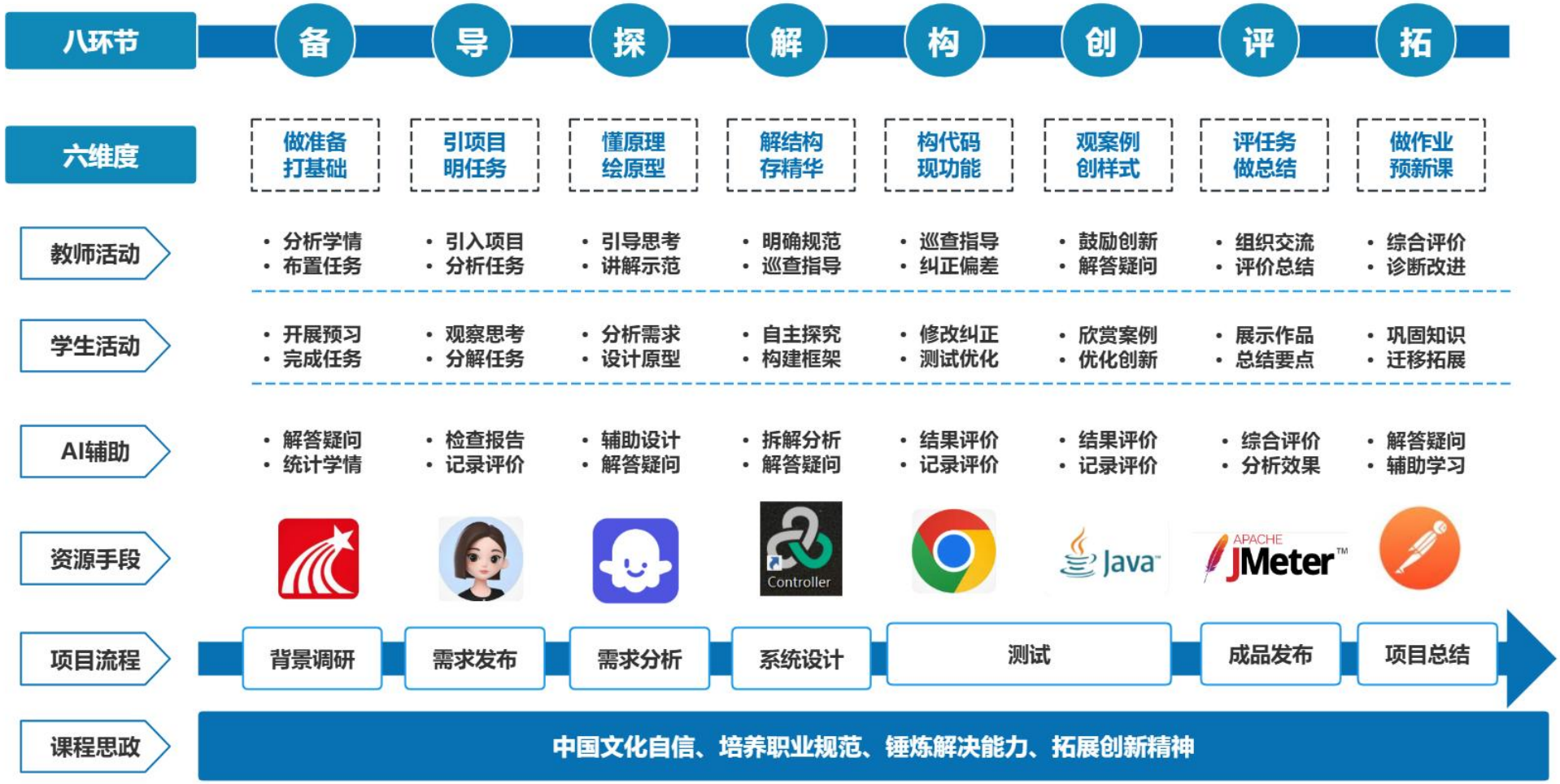
19.3 任务目标

教学目标	**知识**目标	1.了解安全测试的概念 2.熟悉安全测试的基本原则 3.了解SQL注入、XSS跨站攻击、CSRF攻击。
	能力目标	1.能够运用渗透测试的流程 2.能够运用渗透测试的工具
	思政目标	1.培养锤炼精品的工匠精神，坚守职业道德底线，遵纪守纪。 2.培养学生法律意识、职业道德、危机意识。
教学重难点	教学重点	1.熟悉安全测试的基本原则 2.熟悉常见的渗透测试的工具
	教学难点	1.了解SQL注入 2.熟悉常见的渗透测试的工具

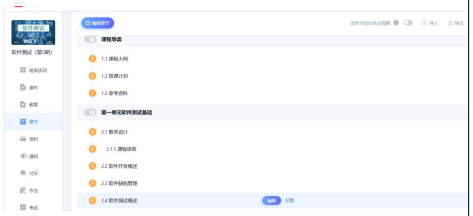
19.4 教学实施

六维度，即“教师活动”“学生活动”“AI辅助”“资源手段”“项目流程”“课程思政”，将教学内容与岗位要求进行结合;在理实一体环境下开展教学，将理论学习与实践操作相结合；师生共同探究，将传授知识与能力培养相结合。八环节，即按照“备、导、探、解、构、创、评、拓 ”八个环节实施教学，在此过程中借助豆包智能体(自主训练)等资源支撑教学活动开展。激发学生爱国主义、集体主义、社会主义精神的传承和发展。真正实现学有所用，学以致用。

教学过程


八环节
备
导
探
解
构
创
评
拓
六维度
做准备 打基础
引项目 明任务
懂原理 绘原型
解结构 存精华
构代码 现功能
观案例 创样式
评任务 做总结
做作业 预新课
教师活动
• 分析学情 • 布置任务
• 引入项目 • 分析任务
• 引导思考 • 讲解示范
• 明确规范 • 巡查指导
• 巡查指导 • 纠正偏差
• 鼓励创新 • 解答疑问
• 组织交流 • 评价总结
• 综合评价 • 诊断改进
学生活动
• 开展预习 • 完成任务
• 观察思考 • 分解任务
• 分析需求 • 设计原型
• 自主探究 • 构建框架
• 修改纠正 • 测试优化
• 欣赏案例 • 优化创新
• 展示作品 • 总结要点
• 巩固知识 • 迁移拓展
AI辅助
• 解答疑问 • 统计学情
• 检查报告 • 记录评价
• 辅助设计 • 解答疑问
• 拆解分析 • 解答疑问
• 结果评价 • 记录评价
• 结果评价 • 记录评价
• 综合评价 • 分析效果
• 解答疑问 • 辅助学习
资源手段
Controller
Java
APACHE JMeter™
项目流程
背景调研
需求发布
需求分析
系统设计
测试
成品发布
项目总结
课程思政
中国文化自信、培养职业规范、锤炼解决能力、拓展创新精神

返回目录

第一阶段 课前 • 自主学习					
教学环节	**教学内容**	**教师活动**	**学生活动**	**AI辅助**	**课程思政**
课前准备	【自主学习】 1.学生观看视频，理解安全测试的概念。 2.学生观看视频，理解安全测试工具的使用。 【训练智能力】 3.根据问题训练智能体，更好掌握本节课的知识点。 【调整策略】 4.收集预习数据，根据分析结果，调整重难点。	1.通过学习通平台发布任务、教学资源，督促学生按时完成。 2.训练智能体，调整工作流和评价标准。 3.收集课前学生预习作业，利用数据调整本节课的教学目标和重难点。	1.登录学习通平台完成课前学习。  2.使用“豆包”智能体解答疑问。	1.“豆包”智能体帮助学生自学，解答疑问。 2.统计以往评价结果，分析学情，支撑决策。	和谐友善和谐价值观、工匠精神、团队协作。

返回目录

第二阶段 课中 •导学实践				
教学环节	**教师活动**	**学生活动**	**信息化辅助**	**课程思政**
第一环节 课堂导入 10分钟	【任务发布】 1.什么是安全测试? 2.怎么熟练运行安全测试工具? 【导入】 以2019年1月拼多多现优惠券漏洞，遭黑产团伙盗取数千万元事件为导人，引人安全测试的基础理论概述，事件中团伙以平台漏洞进行不正当牟利，最后被依法制裁,引导学生树立正确的法律意识和职业道德。 以拼多多官网平台为实践案例，介绍安全测试工具Appscan，让学生在实践中深化思想教育行为的影响，对扫描漏洞报告和原因进行分析，提升危机意识。	小组讨论： 1.学生A回答：哇，安全测试很重要啊，没有进行安全测试企业损失严重。 2.学生B说：这种好事很吸引，但是我们不能这样做，被发现可是犯罪行为。 3.学生根据生活实际进行简单举例，依据安全测试将切近生活的例子作为本节知识的开头引入。	1.学生使用豆包智能体，搜索答案。	培养学生坚定责任主体意识，遵守社会规范，形成正确的伦理价值判断。让学生能够在生活和学习的过程中遵守法律法规及各项相关行业规则，具备法律意识，具备良好的职业素养以及职业道德意识。

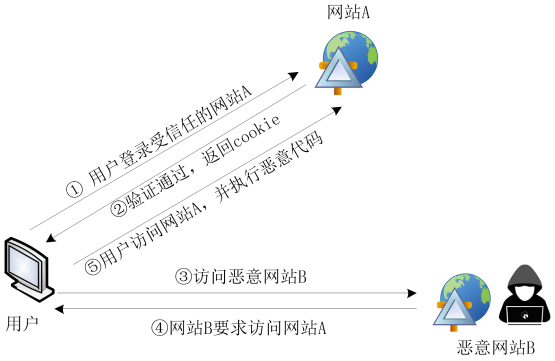
返回目录

第二环节 新知讲解 30分钟	**1.安全测试概述** 安全测试是在IT软件产品的生命周期中，特别是产品开发基本完成到发布阶段，对产品进行检验以验证产品符合安全需求定义和产品质量标准的过程。 **2.常见的安全漏洞** （1）SQL注入：所谓SQL注入就是把SQL命令人为的输入URL、表格域、或者其他动态生成的SQL查询语句的输入参数中，最终达到欺骗服务器执行恶意的SQL命令。 【案例1】某个网站通过网页获取用户输入的数据，并将其插入数据库。正常情况下的URL地址是：http://localhost/id=222。 用户输入的id数据222会被插入数据库执行下列SQL语句：select * from users where id = 222 【案例2】用户可能输入下列URL：http://localhost/id=’ ’ or 1=1。 此时用户输入的数据插入到数据库后执行的SQL语句：select * from users where id = '' or '1'='1' QL注入是风险非常高的安全漏洞，我们可以在应用程序中对用户输入的数据进行合法性检测，包括用户输入数据的类型和长度，同时，对SQL语句中的特殊字符（如单引号、双引号、分号等）进行过滤处理。 （2）XSS跨站攻击：Web应用系统最常见的安全漏洞之一，它主要源于Web应用程序对用户输入检查和过滤不足。攻击者可以利用XSS漏洞把恶意代码注入到网站中，当有用户浏览该网站时，这些恶意代码就会被执行，从而达到攻击的目的。 XSS攻击过程： ● 攻击者通过邮件或其他方式诱使用户点击包含恶意代码的链接，例如攻击者通过E-mail向用户发送一个包含恶意代码的网站home.com。 ● 用户点击链接后，浏览器会在用户毫不知情的情况下执行链接中包含的恶意代码。 ● 将用户与home.com交互的cookie和session等信息发送给攻击者。 ● 攻击者拿到这些数据之后，就会伪装成用户与真正的网站进行会话，从事非法活动。	1.学生认真听讲思考。安全测试方法，尝试自己去测试。 2.结合微课学习，突破难点。	1.使用豆包智能体，验证一下老师讲解的答案是否一致。	学生思考严谨的探究精神。

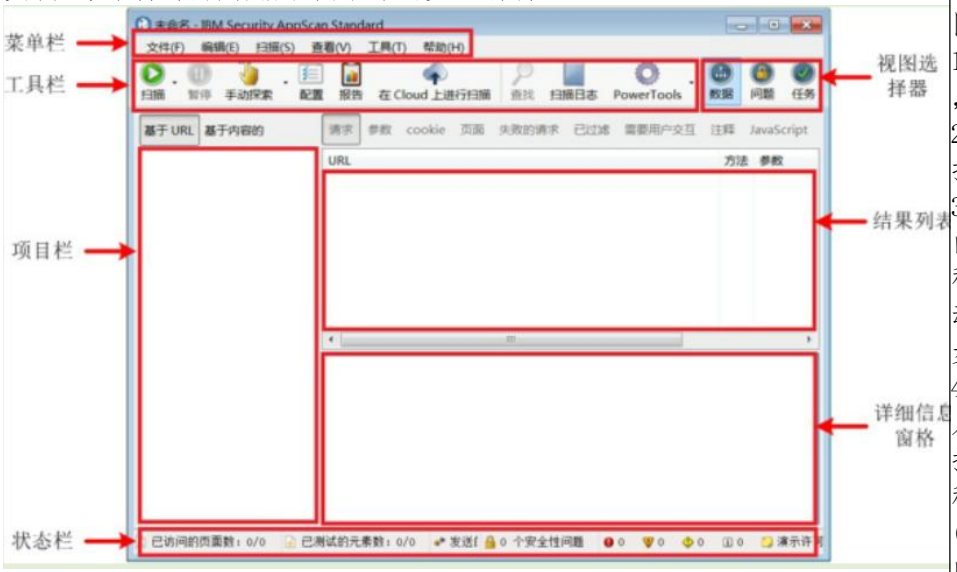
返回目录

（3）CSRF攻击：为跨站请求伪造，它是一种针对Web应用程序的攻击方式，攻击者利用CSRF漏洞伪装成受信任用户的请求访问受攻击的网站。

在CSRF攻击中，当用户访问一个信任网站时，在没有退出会话的情况下，攻击者诱使用户点击恶意网站，恶意网站会返回攻击代码，同时要求访问信任网站，这样用户就在不知情的情况下将恶意网站的代码发送到了信任网站。



返回目录

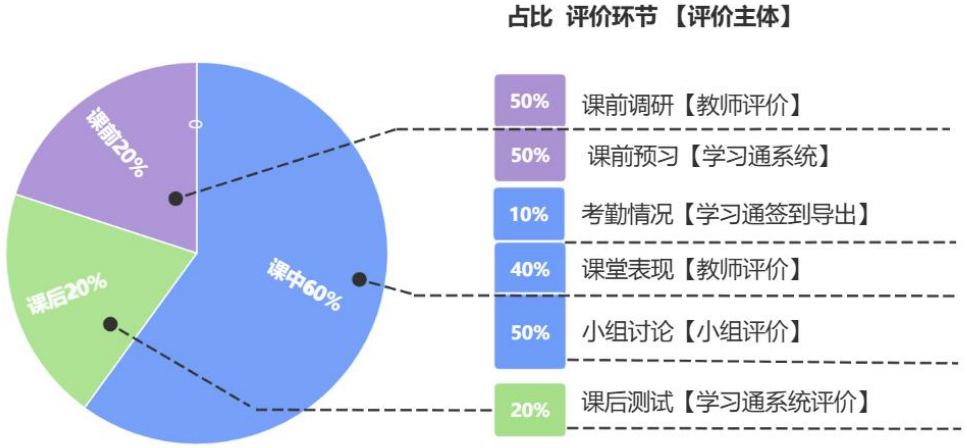
第三环节 动手实践 40分钟	实训：完成扫描传智播客图书库的安全漏洞。  	小组讨论： 同学D回答：我来介绍一下步骤 1.在菜单栏中单击【文件】【新建】，弹出新建扫描对话框。 2.选择“常规扫描”单击之后，弹出扫描配置向导对话框。 3.在步骤2图中选择探索站点的方法，由于本案例是在本机上扫描 Web 应用程序，因此选择“AppScan(自动或手动)”选项选择完毕之后，单击【下一步(N)】按钮，进入 URL配置页面。 4.在步骤 3 图中的“起始 URL” 输入框中输入传智播客图书库地址，选择扫描方式。AppScan 扫描方式有两种:仅扫描此目录中或目录下的链接(L):只扫描起始 URL 目录或者子目录中的链接。将所有路径作为区分大小写来处理(Unix、Linux 等)(T):扫描所有路径，并且区分大小写进行扫描。 5.登录 AppScan 登录网站的选择有4种:记录、自动、提示、无1)记录:单击【记录(R)】按钮，选择下拉列表中的任一浏览器。经历11个步骤 最后结果分析:此次扫描发现2个高级别的安全漏洞，4个中级别的安全漏洞，326个低级别的安全漏洞。其中2 个高级别安全漏洞为跨站点脚本漏洞。	1.使用豆包智能体，找一下漏洞解决的方法，形成最终答案。	引导学生运用教辅工具研究，培养学生的团队合作精神。
第四环节 总结点评 10分钟	1. 点评班级同学本节课任务完成情况 2. 总结安全测试等相关内容 3. 布置课后练习题作业	在学习通上交实训报告。		加深学生对本次课重点内容的印象。

返回目录

第三阶段 课后 •巩固拓展	
教师(引导)	学生(主体)
1. 检查学生课后习题完成情况 2. 完成本次课的教学反思，及时调整教学策略。	1. 完成本次课总结测试。

19.5 教学评价

本次课的评价由学生的课前评价 (20%)+ 课中评价(60%)+课后评价(40%)组成，突出全过程、多主体、多样化的评价方式。各部分占比、评价环节以及评价主体详见下图所示。



19.6 教学反思

1. 给予课前测试优异的同学在回顾引入扮演教师身份的机会，能够有效激励学生在课前自主学习的积极性
2. 课前作业的难度可能设置的较为简单，可以在之后的课程中适当增加本教学单元课前测试的难度

返回目录

返回目录