信息安全工程师

综合技能实战

仅限于广西科技大学内部使用，原创内容，谢绝转发

实施周期：约 4 个月

作　　者：uplooking

目　录

一、项目课程背景介绍

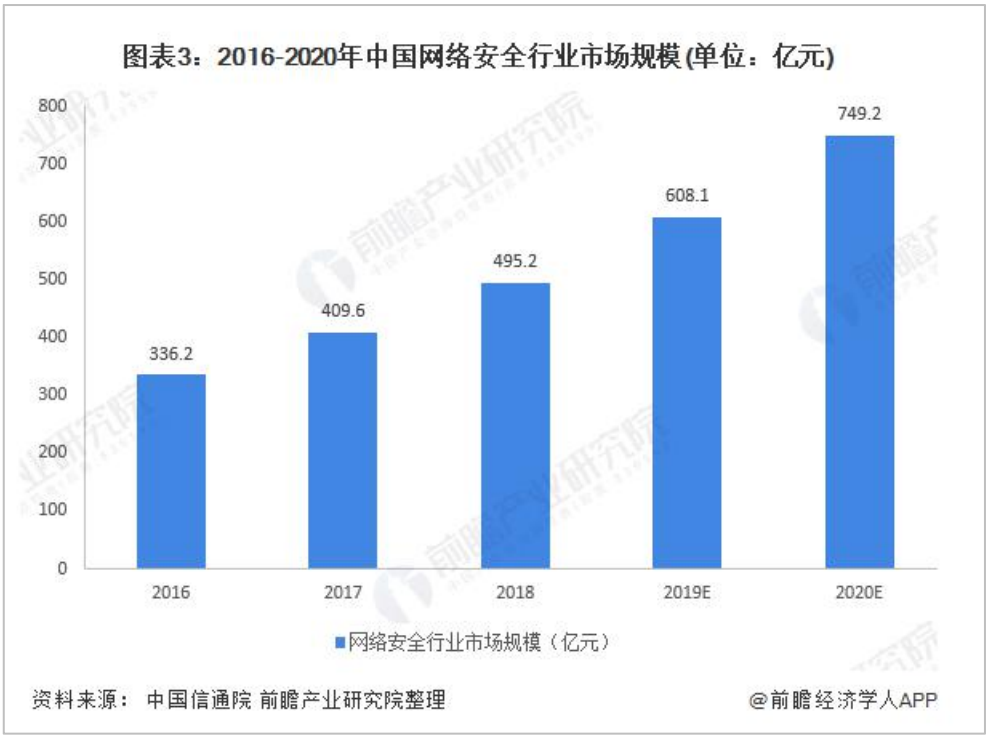
（一）国家层面对网络信息安全高度重视，行业发展迎来新高度

2014年2月27日，中央网络安全和信息化领导小组成立。习近平指出，“没有网络安全就没有国家安全，没有信息化就没有现代化。”国家互联网信息办公室于2016年底发布了《国家网络空间安全战略》，这是我国首次发布关于网络空间安全的战略。2019年上半年，发生在我国网络安全事件和威胁情况进一步加剧，各类网络安全事件数量占比仍然较高。2019年我国比较典型的网络安全事件包括：2019年3月，境外黑客利用勒索病毒攻击部分政府和医院机构;华为起诉美国政府，称其涉嫌入侵华为服务器；2019 年1月，超2亿的中国求职者简历泄露，不受保护状态持续一周等。

在国家层面上，2019年两会期间，政府工作报告也多次提及信息安全。高层高度关注网络安全，从立法到全网络安全检查以及网络安全国际合作，利好集中释放，有利于推动行业高速成长。

（二）网络安全威胁推动行业发展，网络安全行业规模有望超700亿

随着信息化的快速发展，信息安全产业市场空间不断扩大，政府和企业均越来越重视信息安全，用户法规遵从要求越来越高，企业投入逐步增加，安全产品更具自主创新性并且更加多元化。强劲的市场需求推动信息安全产业规模快速增长，2019年产业规模超过600亿元，年增长率超过20%，明显高于国际8%的平均增数，保持健康的发展态势。随着对网络安全的愈加重视及布局，市场规模将持续扩大，到 2021 年中国网络安全市场规模将达千亿元。



信息安全企业的数量和规模也有了较大提高，截至2019年底，国内信息安全相关企业已超过千家，另一方面，信息安全产品种类不断丰富，安全操作系统、安全芯片、安全数据库、密码产品等基础技术产品逐步成熟，防火墙、病毒防护、入侵检测、终端接入控制、网络隔离、安全审计、安全管理、备份恢复等网络安全产品服务取得明显进展，产品功能逐步向集成化、系统化方向发展。

网络安全行业的发展短期内是通过频繁出现的安全事件驱动，短中期离不开国家政策合规，中长期则是通过信息化、云计算、万物互联等基础架构发展驱动。2020年网络安全领域进一步迎来网络安全合规政策及安全事件催化，例如自2020年1月1日起施行《中华人民共和国密码法》，2020年3月1日起施行《网络信息内容生态治理规定》等。2021年作为 “十三五”收官之年，将陆续开始编制网络安全十四五规划。在各种因素的驱动下，我国网络安全行业将得到进一步发展。

二、信息安全人才现状：面临全球性“人才荒”

从总体上看，我国网络安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应”。即将实施的《网络安全法》第二十条也明确表示：“国家支持企业和高等院校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流”。

麦可思研究院发布《2020年中国大学生就业报告》，对2016-2020届毕业生就业量前120位的专业就业满意度较高的前十位本科和高职高专专业进行了研究分析，报告显示，在本科专业，“信息安全”专业本科毕业生就业满意度连续两年排名居首。

安全领域火爆的原因是安全人才的抢手，薪酬水平也直线上升。毫不夸张的说，网络安全是一份很有“钱”途的职业。网络安全专业凭借其高薪资、广阔的行业前景、极高的就业率俨然已经成为毕业生们优先选择的“香饽饽”。WEB开发工程师平均年薪最高，为48.60万元。

三、人才就业方向

网络信息安全专业学生毕业后可在政府机关、国家安全部门、银行、金融、证券、通信领域从事各类信息安全系统、计算机安全系统的研究、设计、开发和管理工作，也可在IT领域从事计算机应用工作，由于国内信息安全专业人才的紧俏，这一行业的起薪相对较高。相关职业岗位及典型工作任务如下表。

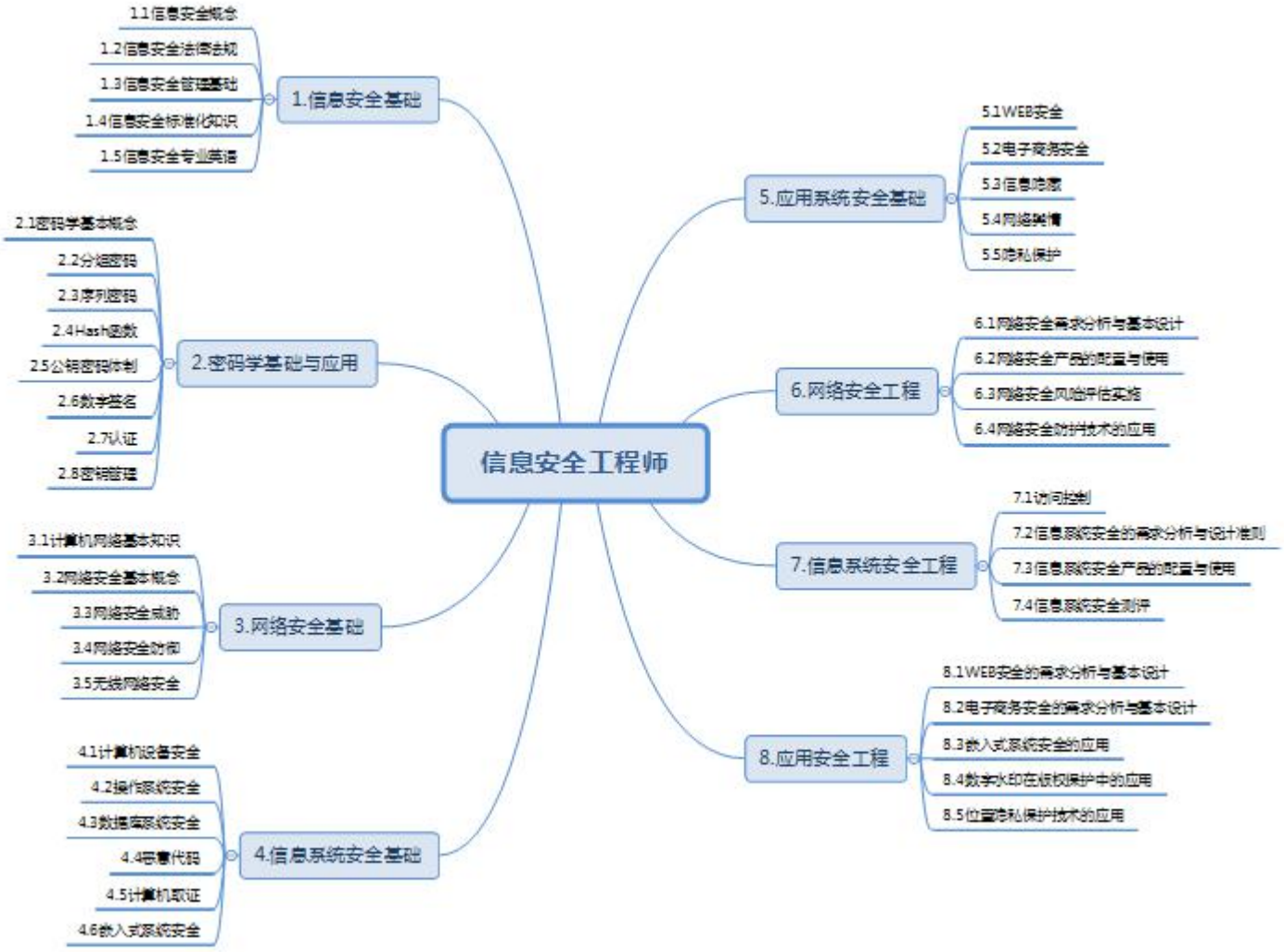
序号	工作岗位	岗位工作内容描述	职业素质与能力要求
1	信息安全/安全运维工程师	1.熟悉渗透测试的各类技术及方法，熟练掌握各种渗透测试工具；熟练操作各类操作系统、应用平台； 2.熟悉网络技术TCP/IP协议、HTTP协议，广泛理解各类网络、主机、数据库、Web安全知识技术技能和攻防手段； 3.掌握各类开源的安全漏洞检测扫描、安全防范、安全渗透测试、安全审计及信息管理工具； 4.熟悉防火墙、IDS/IPS、WAF、SIEM等主流安全产品及解决方案 5.熟悉主流Web安全技术，熟悉常见攻击和防御办法，自行进行web渗透测试，恶意代码监测和分析； 6.具有团结协作精神,以及良好的沟通和口头(文字)表达能力，学习能力强，能承受较强工作压力。	1.职业素质：信息安全建设、管理，网络安全评估及检查 2.能力要求： ●网络的安全设备安装和调试能力 ●服务器及网站日志审查能力 ●安全漏洞的跟踪、安全审核能力 ●安全风险评估与分析及加固能力 ●安全文档的书写能力 ●响应安全事件能力
2	渗透测试工程师	1.熟悉渗透测试步骤、方法、流程，熟练使用一定量的渗透测试工具； 2.熟悉攻击的各类技术及方法，对各类操作系统、应用平台的弱点有较深入的理解； 3.熟悉常见脚本语言，能够进行WEB渗透测试，恶意代码	1.职业素质：承接的渗透测试项目，跟踪安全动态，信息安全风险应急响应工作。 2.能力要求： ●跟踪国际/国内安全社区的安全动态，进行安全漏洞分析、研究与挖掘，并进行预警能力； ●协助做好信息安全风险应急响应工作；

		检测和分析； 4.有一定代码编写能力 5.主动性强，具有良好的沟通、协调和组织能力和文档编写能力，逻辑性强。	●编写渗透测试报告和对客户进行信息安全培训； ●完成安全评估任务和评估报告的编写工作。
3	等级保护测评工程师	1.有较好的安全理论基础，掌握主流安全产品的原理和应用； 2.掌握信息安全等级保护和风险评估技能 3.掌握安全应急响应知识； 4.熟悉主流信息安全规范，如ISO27000； 5.具备良好的文档编写能力； 6.具有团结协作精神,以及良好的沟通和口头(文字)表达能力和服务意识	1.职业素质：信息安全等级保护，信息安全审计，信息安全认证 2.能力要求： ●信息安全等级保护的评估与咨询能力； ●信息安全风险评估的咨询与服务能力； ●信息安全应急响应的咨询与服务能力； ●ISO27001认证咨询与服务能力。
4	安全服务工程师	1.掌握防火墙、VPN等安全产品的原理和应用维护知识和技能； 2.掌握入侵检测系统的原理和应用维护知识和技能； 3.具备一定的网络隔离技术； 4.有较好的安全理论基础，熟悉PKI、SSL等安全技术 5.具备一定的程序开发的能力。	1.职业素质：安全产品系统测试，安全产品的需求分析、功能定义 2.能力要求： ●安全产品系统测试方案设计和实施能力； ●安全产品的需求分析和功能定义能力； ●跟踪记录及推动问题的及时解决能力； ●编写、整理文档能力。
5	售前工程师	1.熟悉网络安全产品的相关知识； 2.具有良好的语言表达能力和快速应变能力； 3.具有资料收集与整理的能力、文字处理能力、数据分析能力； 4.具有团结协作精神,以及良好的沟通和口头(文字)表达能力和服务意识	1.职业素质：销售、售后服务与技术支持 2.能力要求： ●市场考察，发掘及选择顾客能力； ●演示产品，制订报价单能力； ●编写技术方案、合同草案文本能力； ●协助处理与客户方的联络及关系协调能力；

			●管理及统计客户信息资料能力； ●接受用户上报系统问题，分析记录、解答、上报问题，满意度回访能力。
6	系统工程师/实施工程师/技术支持工程师	1.熟悉当前流行操作系统(如windows、Linux等系统)的应用及安全机制和相关配置 2.有扎实的网络基础专业知识和网络互联设备及网络安全设备的应用维护能力； 3.具备一定的风险分析、防病毒和安全策略制定的能力； 4.具备较强的信息安全意识和安全管理能力。 5.编写、整理技术文档	1.职业素质：信息安全管理方案的设计和实施，安全咨询和服务，电子商务网站的安全管理 2.能力要求： ●方案概要设计能力； ●模块级详细设计能力； ●简单的排错及编写能力； ●编写、整理技术文档能力。

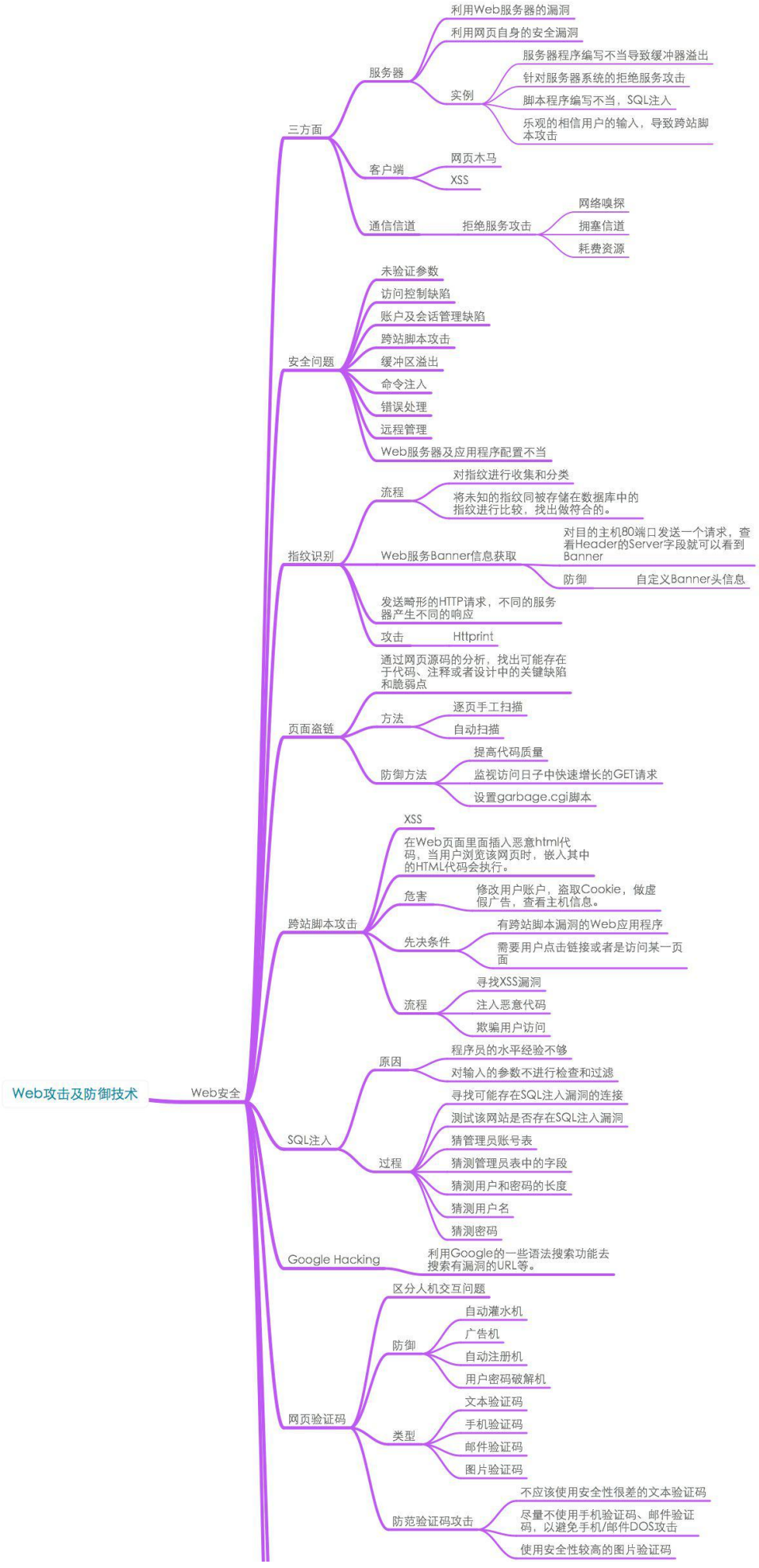
四、项目课程简介

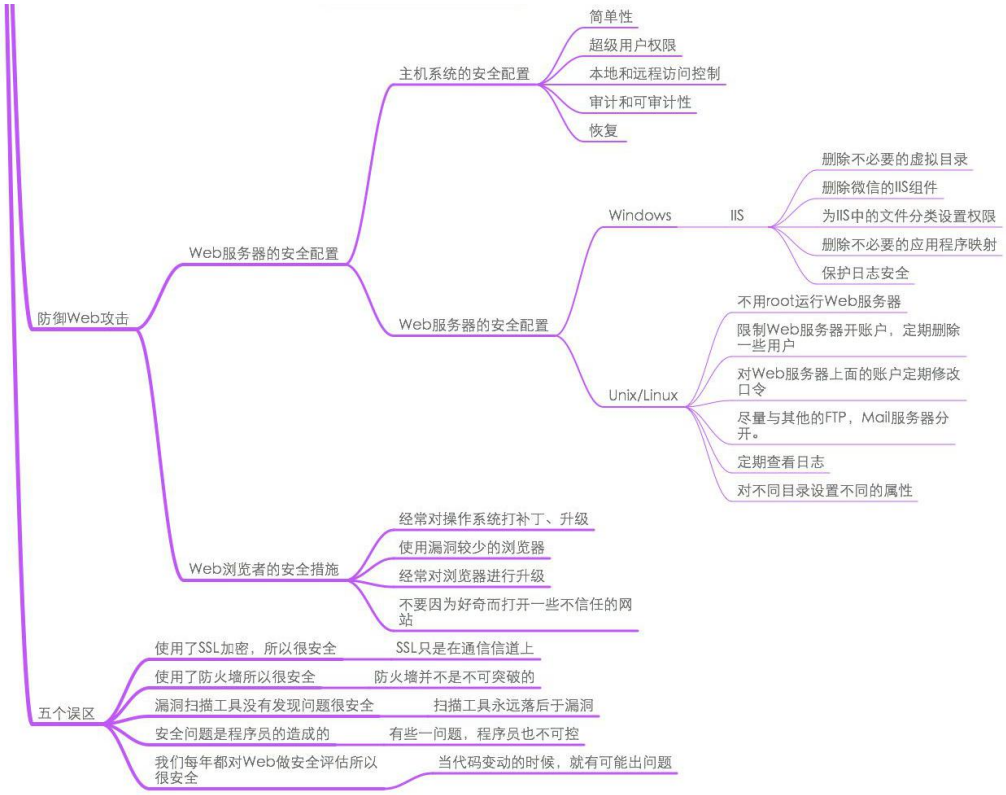
信息安全工程师技能树



五、课程具备丰富的专题内容（部分）

课程中根据企业需求，设置了多个独立的技术专题，**如 操作系统安全专题，网络安全专题，Web安全专题，数据库安全专题，代码审计专题，安全编程专题，主机渗透测试专题，外网渗透测试专题，云安全专题，大数据安全专题**等，每个版块清晰，内容全面且细致和深入，在大型架构中，将引用每一个版块的知识点，让学员既能够把握全局，又能对技术细节收放自如，且穿插大量的企业真实案例和 工作经验，让学员具备独立分析以及准确定位和解决问题的能力


Web攻击及防御技术
Web安全
三方面
服务器
利用Web服务器的漏洞
利用网页自身的安全漏洞
实例
服务器程序编写不当导致缓冲器溢出
针对服务器系统的拒绝服务攻击
脚本程序编写不当，SQL注入
乐观的相信用户的输入，导致跨站脚本攻击
客户端
网页木马
XSS
通信信道
拒绝服务攻击
网络嗅探
拥塞信道
耗费资源
安全问题
未验证参数
访问控制缺陷
账户及会话管理缺陷
跨站脚本攻击
缓冲区溢出
命令注入
错误处理
远程管理
Web服务器及应用程序配置不当
指纹识别
流程
对指纹进行收集和分类
将未知的指纹同被存储在数据库中的指纹进行比较，找出做符合的。
Web服务Banner信息获取
对目的主机80端口发送一个请求，查看Header的Server字段就可以看到Banner
防御
自定义Banner头信息
发送畸形的HTTP请求，不同的服务器产生不同的响应
攻击
Httprint
页面盗链
通过网页源码的分析，找出可能存在于代码、注释或者设计中的关键缺陷和脆弱点
方法
逐页手工扫描
自动扫描
防御方法
提高代码质量
监视访问日子中快速增长的GET请求
设置garbage.cgi脚本
跨站脚本攻击
XSS
在Web页面里面插入恶意html代码，当用户浏览该网页时，嵌入其中的HTML代码会执行。
危害
修改用户账户，盗取Cookie，做虚假广告，查看主机信息。
先决条件
有跨站脚本漏洞的Web应用程序
需要用户点击链接或者是访问某一页面
流程
寻找XSS漏洞
注入恶意代码
欺骗用户访问
SQL注入
原因
程序员的水平经验不够
对输入的参数不进行检查和过滤
过程
寻找可能存在SQL注入漏洞的连接
测试该网站是否存在SQL注入漏洞
猜管理员账号表
猜测管理员表中的字段
猜测用户和密码的长度
猜测用户名
猜测密码
Google Hacking
利用Google的一些语法搜索功能去搜索有漏洞的URL等。
网页验证码
区分人机交互问题
防御
自动灌水机
广告机
自动注册机
用户密码破解机
类型
文本验证码
手机验证码
邮件验证码
图片验证码
防范验证码攻击
不应该使用安全性很差的文本验证码
尽量不使用手机验证码、邮件验证码，以避免手机/邮件DOS攻击
使用安全性较高的图片验证码


防御Web攻击
Web服务器的安全配置
主机系统的安全配置
简单性
超级用户权限
本地和远程访问控制
审计和可审计性
恢复
Web服务器的安全配置
Windows
IIS
删除不必要的虚拟目录
删除微信的IIS组件
为IIS中的文件分类设置权限
删除不必要的应用程序映射
保护日志安全
Unix/Linux
不用root运行Web服务器
限制Web服务器开账户，定期删除一些用户
对Web服务器上面的账户定期修改口令
尽量与其他的FTP，Mail服务器分开。
定期查看日志
对不同目录设置不同的属性
Web浏览者的安全措施
经常对操作系统打补丁、升级
使用漏洞较少的浏览器
经常对浏览器进行升级
不要因为好奇而打开一些不信任的网站
五个误区
使用了SSL加密，所以很安全
SSL只是在通信信道上
使用了防火墙所以很安全
防火墙并不是不可突破的
漏洞扫描工具没有发现问题很安全
扫描工具永远落后于漏洞
安全问题是程序员的造成的
有些一问题，程序员也不可控
我们每年都对Web做安全评估所以很安全
当代码变动的时候，就有可能出问题

六、课程目标

为满足社会经济各领域对信息安全人才的需求，需要在信息安全基础建设、管理、应用技术开发等多个层次进行人才的培养。培养具有系统安全管理与应用分析能力、掌握信息安全应用趋势的高端技能型专门人才。学生通过学习掌握操作系统安全知识，具备操作系统安全管理与维护能力，学习掌握安全设备部署及应用知识，具备网络安全管理、应用、维护能力，学习掌握Web安全技术知识、主机渗透测试技术知识、内网渗透测试技术知识，具备渗透测试攻击及防护能力，学习掌握python安全开发技术知识，具备安全应用设计与开发能力，学习掌握CTF攻防夺旗知识，具备高级信息安全应用、管理能力。

毕业生目标工作岗位是系统安全工程师、网络安全工程师、渗透测试工程师、安全运维工程师，主要从事系统安全运维、Web渗透测试、代码安全分析、系统安全审计等岗位，需要具备的知识是操作系统安全知识、网络安全知识、渗透测试知识、安全编程知识等，能够完成安全设备部署及应用，安全工具设计与开发实现，网站渗透测试，内网渗透测试，应急响应等工作。

通过实训让学员具备等同1-3年信息安全工程师的经验，并拥有实际线上大型项目经历，确保学员进入到金融、汽车、电商、科技、医疗、通信等行业的信息安全工程师岗位。学员技能应达到以下要求：

1、熟练应用操作系统安全配置技巧：Linux 服务器安全部署、Linux系统安全、Linux账号基本安全、Linux远程访问安全、Windows 操作系统安全配置、Windows 安全策略配置等

2、掌握Shell安全编程：利用Shell编写自动扫描脚本、Shell脚本在CTF比赛中的应用

3、掌握网络安全攻击技术：IP欺骗、源路由地址欺骗、ARP毒化攻击、DNS信息劫持。通过欺骗进行钓鱼攻击。

4、掌握网络安全设备应用技术：防火墙、安全审计、WAF、IDS、VPN等安全设备的部署及应用。

5、掌握Web安全技术及安全分析技术：Web常见漏洞利用、网站木马、Web渗透测试特殊姿势、网站安全加固、PHP代码审计技术。

6、掌握数据库安全技术：数据库安全配置、数据库备份与恢复。

7、熟悉安全编程技术：敏捷开发思想、扫描期流程设计、安全扫描器框架搭建、安全扫描器并行化、SQL注入漏洞扫描器、具备生成漏洞报表功能的SQL注入漏洞扫描器、命令执行漏洞扫描功能、本地文件包含漏洞扫描功能、目录浏览漏洞扫描功能、Cookie 漏洞扫描功能。

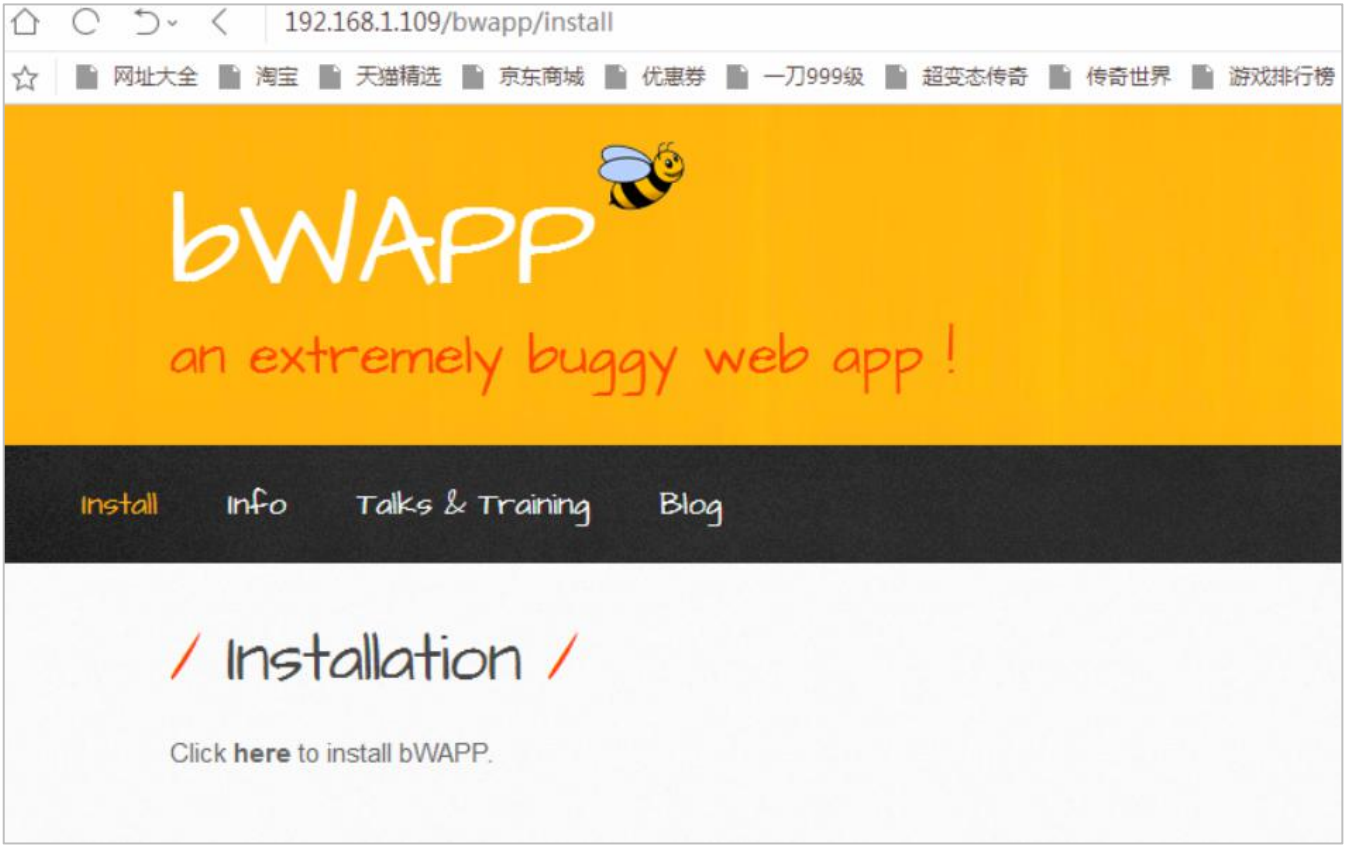
8、掌握渗透测试技术：信息搜集、口令攻击、Web扫描、服务器控制（后门）、无线安全。内网横向渗透技术。渗透测试神器CobaltStrike框架应用等实用渗透技能攻防。

9、掌握CTF攻防技术：Crypto初级/中级、Misc初级/中级、Web高级、逆向分析初级/中级、PWN分析、AWD攻击与防御思路、AWD模拟竞赛。学员能掌握信息安全攻防竞赛的各种操作技巧。

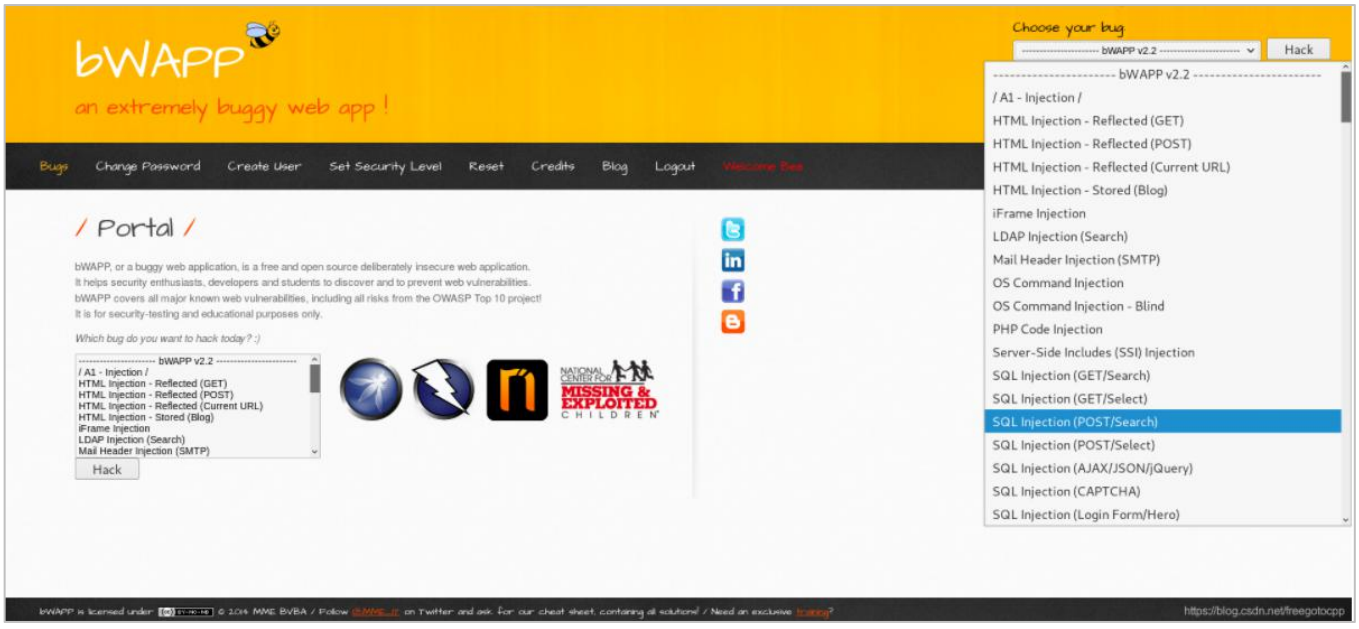
七、实战项目案例（部分列出）

Web渗透测试靶场

①部署安装bWAPP靶场

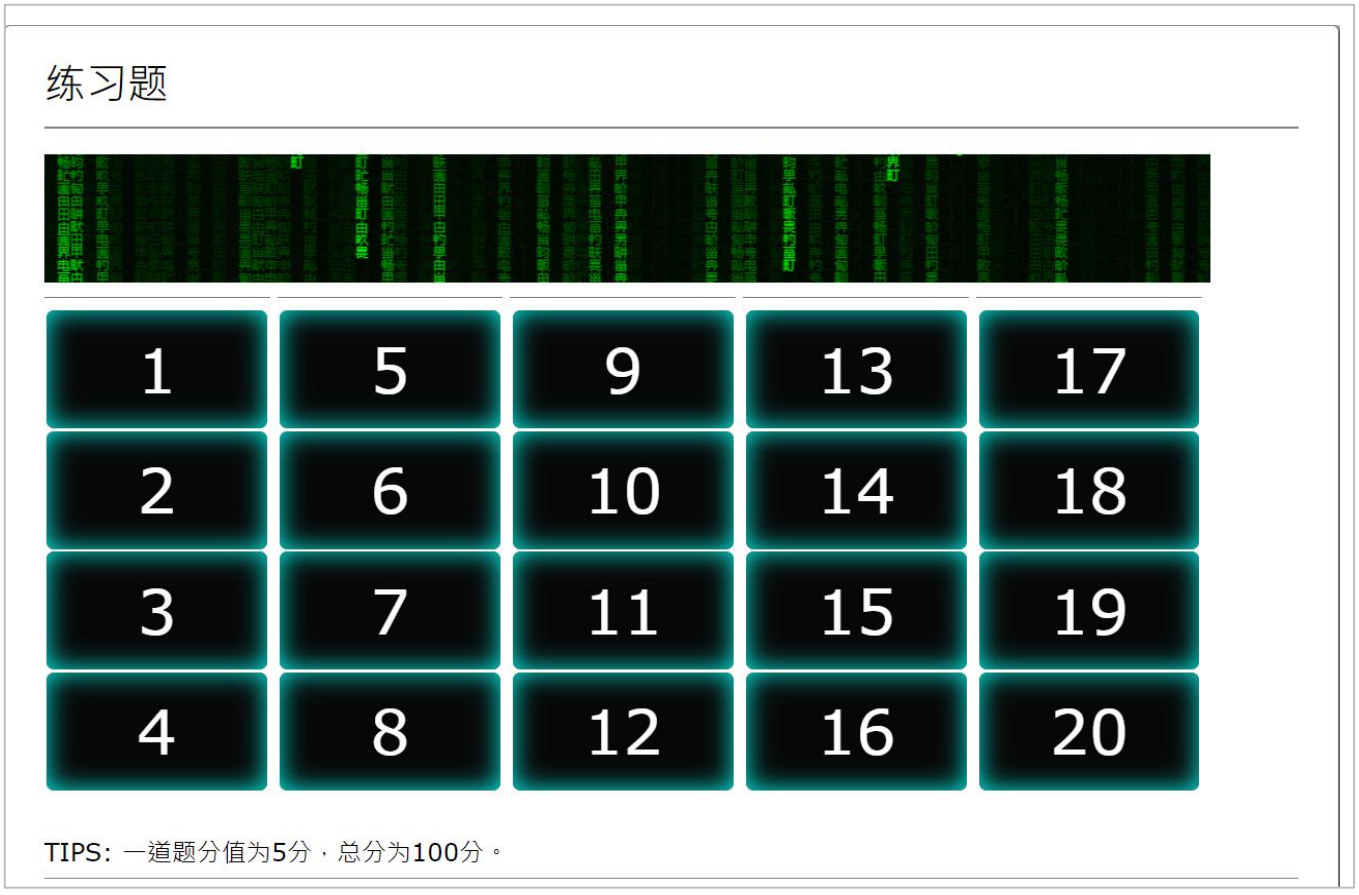


②选择指定靶场进行练习

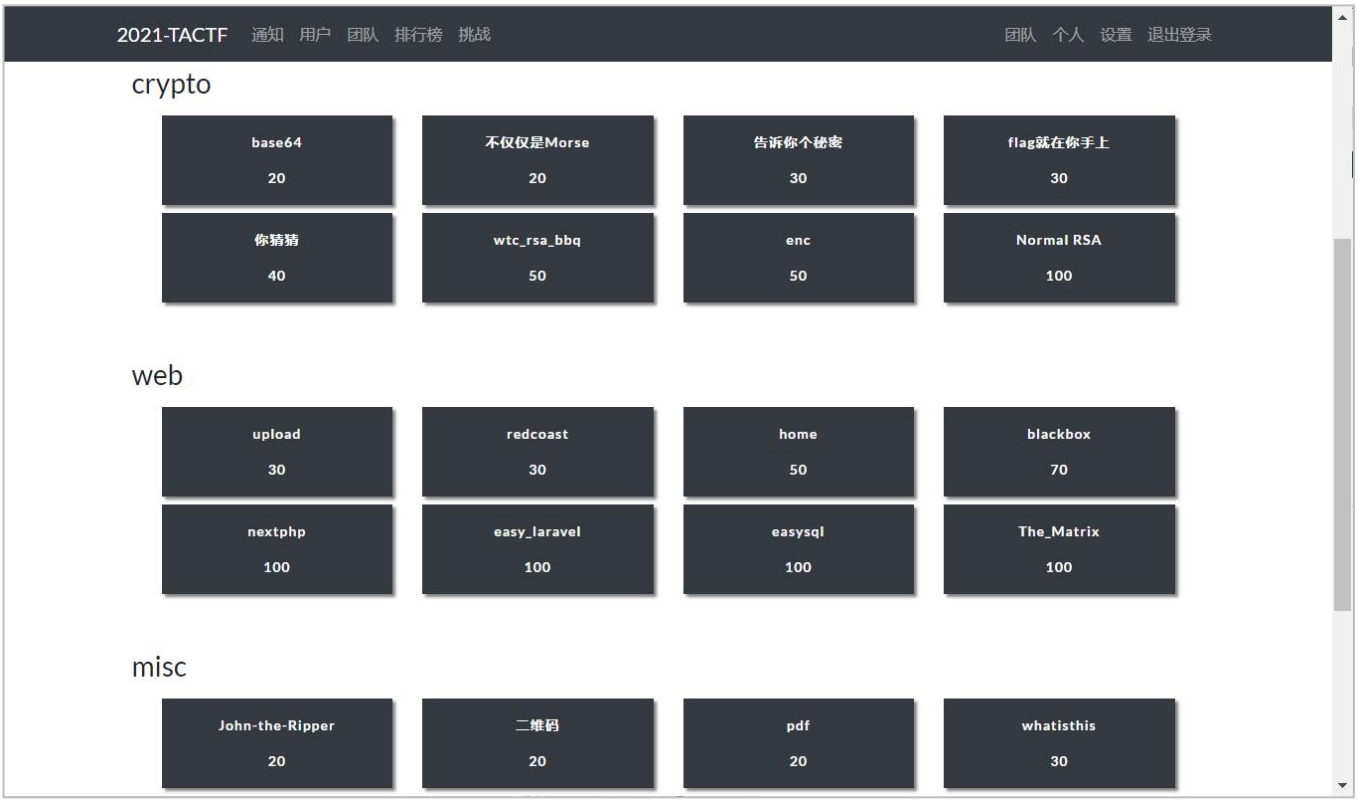


③对漏洞进行攻击

网络攻防初级练习靶场



网络攻防中级训练靶场



网络攻防高级训练靶场

攻防演练及应急响应综合训练靶场

八、课程具体安排（约 4 个月）

信 息 安 全 课 程 大 纲		
阶段	名称	内容简介
第一阶段: 安全运维技术	Linux安全	1、Linux 服务器安全部署 ❖ 安装php、mysql、apache ❖ 配置httpd支持php ❖ Httpd的默认虚拟主机 ❖ Httpd的用户认证 2、Linux系统安全 ❖ Linux安全概述 ❖ 硬件和物理安全 ❖ 系统更新安全 ❖ 系统服务配置 ❖ 系统日志配置 3、Linux账号基本安全 ❖ 账号通用配置 ❖ 保护root账号 ❖ 口令安全策略 ❖ PAM配置 4、Linux远程访问安全 ❖ 禁用telnet,使用SSH进行管理 ❖ 限制能够登录本机的IP地址 ❖ 禁止root用户远程登陆 ❖ 限定信任主机 ❖ 修改banner信息 5、Linux服务器安全 ❖ 常用服务器的安全配置
第一阶段: 安全运维技术	主机安全运维与shell编程	1、Shell初级应用 ❖ Shell脚本结构和执行 ❖ Date命令用法 ❖ Shell脚本中的逻辑判断 ❖ 文件目录属性判断 ❖ Shell中的函数 ❖ Shell中的数组 2、Shell进阶应用 ❖ 告警系统需求分析 ❖ 告警系统主脚本 ❖ 告警系统配置文件 ❖ 告警系统监控项目 3、Shell安全开发 ❖ 利用Shell编写自动扫描脚本 ❖ Shell脚本在CTF比赛中的应用

第一阶段: 安全运维技术	Windows安全	1、Windows 操作系统安全配置 ❖ 账户与权限安全 ❖ 进程与服务安全 ❖ 日志安全 ❖ 防火墙 ❖ 杀毒软件 ❖ 系统漏洞与补丁 2、Windows 安全策略配置 ❖ 组策略和注册表配置 ❖ 本地安全策略配置
第一阶段: 安全运维技术	网络安全	1、协议欺骗 ❖ IP欺骗 ❖ 源路由地址欺骗 ❖ ARP毒化攻击 ❖ DNS信息劫持 2、社会工程学攻击 ❖ 钓鱼邮件 ❖ 真·假“二维码” ❖ 利用伪AP制作钓鱼WIFI ❖ 黑客电影场景复现---社工U盘 3、拒绝服务 ❖ CC攻击实现 ❖ 编写脚本实现DDOS
第一阶段: 安全运维技术	安全设备	1、防火墙 ❖ 防火墙原理 ❖ 防火墙部署方式 ❖ 防火墙安全策略 ❖ 防火墙安全产品部署及应用 2、安全审计 ❖ 上网行为审计技术原理 ❖ 数据库与业务应用安全审计的技术原理 ❖ 账号集中管理与审计的技术原理 ❖ 堡垒机部署方法 ❖ 堡垒机单点登录部署实战 3、Web应用防护系统 ❖ WAF基本概念及原理 ❖ WAF系统的策略建模方式 ❖ WAF的防护功能类型 ❖ WAF的应用部署模式 ❖ WAF安全产品安装及配置 ❖ WAF拦截Web攻击流量实战 ❖ WAF拦截CC攻击实战 4、入侵检测 ❖ 入侵检测系统基本概念 ❖ 网络入侵检测和主机入侵检测概念及原理 ❖ 基于特征的检测分类 ❖ 用户行为模型与统计分析原理 ❖ 蜜罐系统原理

		❖ 入侵检测系统安装及配置 ❖ 入侵检测规则配置 ❖ 入侵检测应用实战 ❖ 蜜罐系统部署 ❖ 蜜罐系统应用实战 5、VPN ❖ VPN基本概念 ❖ VPN的分类及关键技术 ❖ L2TP VPN技术原理 ❖ PPTP VPN技术原理 ❖ IPSec VPN技术原理 ❖ SSL VPN部署及应用实战 ❖ IPSec VPN部署及应用实战
第一阶段: 安全运维技术	Web安全	1、Web安全基础 ❖ Web安全现状与威胁 ❖ Web服务器 ❖ HTTP协议基础 ❖ BurpSuite基础 ❖ 编码与简单加解密 ❖ BurpSuite爆破Web密码 2、Web常见漏洞介绍 ❖ 漏洞产生原因 ❖ 主流的漏洞类型 ❖ OWASP TOP 10安全风险 3、网站木马 ❖ 网站木马概念 ❖ 一句话木马（php、asp、aspx、jsp） ❖ 功能小马 ❖ 网站大马（php、asp、jsp） ❖ 网站木马的检测与防范 4、Web漏洞利用（中级） ❖ SQL注入漏洞实践 ❖ 命令执行漏洞实践 ❖ XSS漏洞实践 ❖ 跨站请求伪造漏洞实践（XSS+CSRF） ❖ SSRF漏洞实践 ❖ 文件上传漏洞实践 ❖ 文件包含漏洞实践 ❖ 中间件漏洞利用 ❖ 逻辑漏洞 ❖ 越权（水平越权、垂直越权） 5、Web漏洞实战（高级） ❖ Web网站扫描 ❖ 敏感信息收集 ❖ 帝国CMS网站渗透实战 ❖ 骑士人才系统网站渗透实战 ❖ DiscuzX3网站渗透实战 6、Web渗透测试特殊姿势

		❖ 钻GPC等转义的空子 ❖ 字符串函数报错信息泄露 ❖ 字符串截断 ❖ php伪协议 ❖ 正则表达式特殊利用 ❖ PHP代码解析标签 7、网站安全加固 ❖ Web安全检测分析 ❖ Web服务器加固
第一阶段: 安全运维技术	数据库安全	1、MySQL数据库安全配置 ❖ MySQL账户安全 ❖ MySQL用户权限配置 ❖ MySQL日志安全审计 ❖ MySQL禁用或限制远程访问 ❖ MySQL其他安全配置 2、MySQL数据库备份与恢复 ❖ MySQL数据库全面备份 ❖ MySQL数据库增量备份 ❖ MySQL数据库差异备份 3、MySQL主从 ❖ MySQL数据库主从配置
第一阶段: 安全运维技术	PHP代码审计	1、代码审计环境部署 ❖ Wamp/Wnmp环境搭建 ❖ Lamp/Lnmp环境搭建 ❖ PHP核心配置详解 2、审计辅助与漏洞验证工具 ❖ 代码编辑器（Notepad++、UltraEdit） ❖ 代码审计工具 ❖ 漏洞验证辅助 3、通用代码审计思路 ❖ 敏感函数回溯参数过程 ❖ 通读全文代码 ❖ 根据功能点定向审计 4、漏洞挖掘与防范（基础篇） ❖ SQL注入漏洞挖掘与防范 ❖ XSS漏洞挖掘与防范 ❖ CSRF漏洞挖掘与防范 5、漏洞挖掘与防范（进阶篇） ❖ 文件操作漏洞挖掘与防范（文件包含、文件读取/下载、文件上传、文件删除） ❖ 代码执行漏洞挖掘与防范 ❖ 命令执行漏洞挖掘与防范 6、漏洞挖掘与防范（深入篇） ❖ 变量覆盖漏洞挖掘与防范 ❖ 逻辑处理漏洞挖掘与防范 ❖ 会话认证漏洞挖掘与防范 7、二次漏洞审计 ❖ 二次漏洞审计技巧

		❖ 二次注入漏洞分析 8、PHP安全编程规范 ❖ 参数的安全过滤 ❖ 使用安全的加密算法 ❖ 业务功能安全设计 ❖ 应用安全体系建设
第二阶段： 攻防渗透技术	Python编程巩固与练习	1、Python变量 ❖ Python数据类型 ❖ Python运算符 2、Python控制语句 ❖ 循环语句 ❖ 条件语句 ❖ 测试语句 3、Python函数、类与对象 ❖ 什么是函数 ❖ 函数的声明与使用 ❖ 什么是类与对象 ❖ 类的声明与对象调用 4、Python文件操作 5、Python错误与异常处理 ❖ Python的异常与错误类型 ❖ 处理错误与异常 6、Python综合项目应用 ❖ 竞猜游戏开发 ❖ 学生管理系统图形化操作界面 ❖ 井字棋开发 ❖ 五子棋开发
第二阶段： 攻防渗透技术	Python运维	1、系统基本信息获取 ❖ 查看CPU、内存、磁盘等信息 ❖ 查看网络信息 ❖ 查看进程信息 2、DNS解析查询与利用 ❖ DNS域名轮询业务监控 3、文件与目录差异对比 ❖ 内容差异对比 ❖ 文件与目录差异对比 ❖ 校验源于备份目录的差异 4、数据报表之Excel操作 ❖ 基于Python的Excel基本操作 ❖ 插入数据、插入表 ❖ Chart类的常用方法 ❖ 定制自动化业务流量报表周报 5、Socket编程 6、运维之snmp 7、自动化运维平台
		1、敏捷开发思想 ❖ 敏捷开发思想介绍 ❖ 敏捷开发的主要实现方式（SCRUM、XP等）

第二阶段： 攻防渗透技术	安全扫描器开发	❖ CRUM的工作流程 ❖ 简单的敏捷开发实验 2、扫描期流程设计 ❖ 项目管理思想 ❖ 需求分析 ❖ 方案设计 ❖ 应用开发 ❖ 结尾验收 ❖ 创建扫描器项目 3、安全扫描器框架搭建 ❖ 网页爬虫技术 ❖ 网络编程 ❖ 第一版扫描器（网页爬虫工具） 4、安全扫描器并行化 ❖ 网页去重功能实现 ❖ 优化爬取速度-多线程 ❖ 生产者消费者模式 ❖ 网页去重开发 ❖ 多线程代码开发 ❖ 生产者消费者模型开发 ❖ 扫描器迭代开发（多线程网页爬虫工具） 5、制作SQL注入漏洞扫描器 ❖ SQL注入实现原理 ❖ 通过编程实现特定页面SQL注入 ❖ 第三版扫描器（SQL注入漏洞扫描器） 6、制作具备生成漏洞报表功能的SQL注入漏洞扫描器 ❖ 漏洞报表功能 ❖ HTML文本语言教学 ❖ HTML文本语言实验 ❖ 第四版扫描器（具备生成漏洞报表功能的SQL注入漏洞扫描器） 7、命令执行漏洞扫描功能 ❖ 命令执行实现原理 ❖ 通过编程实现命令执行 ❖ 第五版扫描器（具备命令执行漏洞扫描功能） 8、本地文件包含漏洞扫描功能 ❖ 本地文件包含实现原理 ❖ 通过编程实现本地文件包含 ❖ 第六版扫描器（具备本地文件包含漏洞扫描功能） 9、目录浏览漏洞扫描功能 ❖ 目录浏览漏洞原理 ❖ 第七版扫描器（具备目录浏览漏洞扫描功能） 10、Cookie 漏洞扫描功能 ❖ Cookie 漏洞 第八版扫描器（具备 Cookie 漏洞扫描功能）

第二阶段： 攻防渗透技术	渗透测试平台与工具	1、渗透测试平台搭建 ❖ Back Track five的介绍 ❖ Parrot Security OS的介绍 ❖ Kali Linux平台优化 2、信息搜集 ❖ 信息收集概述 ❖ 从一个ip开始信息搜集 ❖ dnsenum，Fierce工具的使用 ❖ nmap工具的使用 ❖ p0f、Whois、dig工具的使用 ❖ Dmitry工具的使用 ❖ dirbuster工具的使用 3、口令攻击 ❖ 口令安全概述 ❖ Crunch工具的使用实验 ❖ awk、uniq、sort三个命令使用实验 ❖ 弱口令字典及密码破解实验 4、Web扫描 ❖ Web扫描概述 ❖ OWASP TOP10 ❖ Nikto 扫描实验 ❖ Wapiti扫描实验 ❖ OWASP ZAP扫描实验 ❖ w3af扫描实验 ❖ Vega扫描实验 ❖ Metasploit 中的Wmap扫描工具的使用实验 5、服务器控制 ❖ 后门技术概述 ❖ webacoo工具使用实验 ❖ weevely工具使用实验 ❖ PHP Meterpreter工具的使用实验 ❖ 结合crontab做定时反弹木马实验 6、无线安全 ❖ 无线安全讲解 ❖ Aircrack-ng、Reaver介绍 ❖ Fern Wifi、ghost phisher 介绍 ❖ Aircrack-ng、Reaver工具使用实验 ❖ Fern Wifi、ghost phisher工具使用实验 7、漏洞利用库 ❖ Exploit-DB的介绍 ❖ Exploit-DB库使用实验 ❖ Exploit-DB库搜索及更新实验 Exploit-DB payload制作实验
		1、外网渗透测试项目基础 ❖ 项目介绍 ❖ 拓扑规划 ❖ 内网环境搭建 2、隐藏通信隧道——绕过防火墙 ❖ 隐藏通信隧道概述 ❖ 网络层隧道技术 ❖ 传输层隧道技术

第二阶段： 攻防渗透技术	外网渗透测试实战及防御	❖ 应用层隧道技术 3、内网信息收集 ❖ 内网信息收集概述 ❖ 查询当前权限 ❖ 判断是否存在域 ❖ 扫描域内端口 ❖ 收集域内信息 ❖ 确定内网拓扑结构 4、域内横向移动分析 ❖ 常用Windows远程连接和相关命令 ❖ Windows系统散列值获取分析 ❖ 常见域内横向分析工具的使用 5、渗透测试神器Cobalt Strike ❖ Cobalt Strike部署安装 ❖ Cobalt Strike模块介绍 ❖ Cobalt Strike功能介绍 ❖ Cobalt Strike的常用命令 ❖ Cobalt Strike工具的扩展应用 6、权限提升分析 ❖ 系统内核溢出漏洞提权分析 ❖ Windows操作系统配置错误利用分析 ❖ 组策略首选项提权分析 ❖ 绕过UAC提权分析 ❖ 令牌窃取分析 7、权限维持分析 ❖ 操作系统后门分析 ❖ 域控制器权限持久化分析 ❖ Nishang下的脚本后门分析 8、渗透测试防御 ❖ Windows操作系统安全加固 ❖ Linux操作系统安全加固
第三阶段： 安全拓展与实践	虚拟化及云计算	1、虚拟化技术 ❖ 虚拟化介绍 ❖ 常见虚拟化软件 ❖ 虚拟化架构 ❖ KVM介绍 ❖ KVM安装配置 ❖ KVM虚拟机创建与配置 2、云计算 ❖ 云计算介绍 ❖ 云计算架构 ❖ OpenStack云计算平台部署实践
第三阶段： 安全拓展与实践	云安全	1、云安全介绍 ❖ 云安全概念及发展过程 ❖ 云安全需求 ❖ 云安全联盟CSA ❖ 十二大云安全威胁 3、云安全关键技术

		❖ 云安全架构 ❖ 网络边界安全 ❖ 主机安全 ❖ 数据安全 ❖ 应用安全 4、云安全产品应用 ❖ 网络威胁检测系统 ❖ 云安全扫描产品 ❖ 云主机安全产品 ❖ Web 应用防火墙（WAF） ❖ 数据安全网关（堡垒机）
第三阶段： 安全拓展与实践	大数据平台及安全	1、Hadoop大数据平台 ❖ Hadoop概述 ❖ HDFS介绍 ❖ MapReduce介绍 ❖ 基于Hadoop+Spark的大数据平台部署实战 2、大数据安全概述 ❖ 大数据安全威胁 ❖ 大数据安全保障技术 ❖ 基于hadoop的安全保障实践 ❖ 大数据安全应用技术 ❖ 大数据安全趋势与应对策略
第三阶段： 安全拓展与实践	安全讲座	1、区块链安全 ❖ 比特币与粉尘攻击 ❖ 密码学与区块链的联系 1、 人工智能安全 ❖ 比人工智能未来展望 ❖ 人工智能未来展望 2、 《网络安全法》 ❖ 网络安全法的重要性和迫切性 ❖ 网络安全法重点条款介绍 3、 应急响应和灾难恢复 ❖ 应急响应概述 ❖ 信息系统灾难恢复 ❖ 灾难恢复相关技术 4、 等级保护2.0 ❖ 等级保护的基本概念 ❖ 等级保护工作的基本流程 ❖ 等级保护2.0的具体内容 ❖ 等级保护实践 5、 《ISO27001》 ❖ 什么是信息安全 ❖ 如何实施信息安全管理 ❖ 信息安全管理体系标准介绍 6、 “护网行动”介绍 ❖ 安全背景与严峻形式 7、 简历的制作 -人事 8、 面试与沟通技巧-人事

第三阶段： 安全拓展与实践	CTF攻防夺旗	1、CTF介绍 ❖ 什么是CTF ❖ CTF竞赛规则 ❖ CTF常见题型 ❖ CTF解题工具及思路 2、Crypto初级 ❖ 常用编码方式 ❖ 古典密码和其他密码 ❖ 代码混淆与加密 3、Crypto中级 ❖ 多表代换加密等古典密码 ❖ 对称加密、非对称加密和哈希函数加密等现代密码 4、Misc初级 ❖ 常见编码 ❖ 脚本语言操作二进制数据 ❖ 常见工具使用 ❖ 压缩包、图片隐写、音频隐写等 5、Misc中级 ❖ Wireshark/Tshark等流量分析工具使用 ❖ 流量包修复和分析 ❖ 内存取证 6、Web高级 ❖ 条件竞争 ❖ PHP弱类型 ❖ SSRF绕过技术 ❖ XXE利用 ❖ PHP反序列化 7、逆向分析初级 ❖ 逆向技术简介 ❖ 逆向基础知识 ❖ Re初探与工具使用 ❖ Windows Rej基础知识 8、逆向分析中级 ❖ Android逆向分析 ❖ 加密算法识别 ❖ 反调试 ❖ 花指令 ❖ 加壳与脱壳技术 9、PWN分析 ❖ Pwn环境以及工具准备 ❖ 栈溢出相关知识点分析 ❖ PWN入门级题目训练
第三阶段： 安全拓展与实践	AWD攻防	1、AWD介绍 ❖ 什么是AWD ❖ AWD竞赛规则 ❖ AWD常见题型 ❖ AWD攻击与防御思路

		2、AWD模拟竞赛 ❖ 分组3-5人一组，进行AWD攻防模拟竞赛 3、AWD靶场部署 ❖ 讲解如何通过部署Docker环境实现AWD题目分发环境
终极阶段	就业课程（职业礼仪、面试技巧、模拟面试、推介就业）	

九、教学模式与就业保证

尚观科技始终坚持“技术为王”的理念，课程每 6 个月更新一次，坚持以一线最新技术为指引；教学采用上百个企业案例进行场景教学，以项目为驱动使学生的学习与工作零距离。**对于培训学员入学即签订就业和薪水双保障就业协议，100%保证对口岗位高薪就业，一遍学不好终身免费重听制。**

十、尚观资质

- 尚观科技，成立于 2005 年，由一批“IT 愤青”创建，在高端技术教育领域深耕 至今 15 年
- 技术为王，是尚观体内始终流淌的血液，课程每 6 个月更新一次，坚持以一线最新技术为指引
- 在尚观人共同努力下，如今在北京、上海、深圳、沈阳、大连、成都、广州、西安、武汉等地均设有近千平米教室的高端 IT 培训公司。
- 多年获得 RedHat 及 Oracle 在中国最大最佳授权合作伙伴殊荣
- 成为国内数百所高校校企合作的优秀典范
- 对于培训学员 100%保证对口岗位就业，一遍学不好终身免费重听制

十一、教学环境

十二、宿舍环境