

CTF 正式学员进阶

课程安排：

模块	时间	内容	备注
基础知识	第 1 天	密码学	编码 古典密码 现代密码 真题解析
	第 2 天	JAVA 编程基础	语法 架构 常见函数
	第 3 天	CTF 杂项上	文件操作与隐写 图片隐写
	第 4 天	CTF 杂项下	压缩文件处理 流量取证技术
	第 5 天	逆向技术	逆向概述 逆向分析
	第 6 天	PWN 上	PWN 基础 栈相关漏洞 堆相关漏洞
	第 7 天	PWN 下	格式化字符串漏洞 整型漏洞 逻辑漏洞
Web 漏洞	第 8 天	信息搜集	子域名收集 同备案查询 C 段查询 旁站查询 代码托管网站查询
	第 9 天	Web 安全基础	Web 服务器介绍 HTTP 协议详解 OJASP Top 10 介绍 对应 CTF 中 Web 试题解析 目录遍历漏洞
	第 10 天	文件上传漏洞	文件上传漏洞 js 绕过 文件上传漏洞 MINE-Type 绕过 文件上传漏洞扩展名绕过 文件上传漏洞 00 截断 文件上传漏洞修改文件头绕过

	第 11 天	SQL 注入	SQL 注入基础知识 SQL 注入实战演练 SQL 注入工具使用 SQL 注入防御措施
	第 12 天	命令执行漏洞	PHP 命令执行 PHP 代码执行 PHP 动态函数调用 PHP 函数代码执行漏洞
	第 13 天	提权	了解提权 简单提权 Mysql 提权 03/08 溢出提权
	第 14 天	XSS	XSS 介绍 XSS 类型 payload 构造 XSS filter 绕过 Cookie 的获取及使用 XSS 漏洞挖掘 XSS 防御
	第 15 天	文件包含漏洞	初识文件包含 本地文件包含 远程文件包含 PHP 伪协议 防御文件包含
	第 16 天	CSRF SSRF	CSRF 原理 CSRF 实战 SSRF 原理 SSRF 实战
	第 17 天	条件竞争 XXE	条件竞争原理 条件竞争实例 XXE 原理 XXE 实战
	第 18 天	SSTI 服务端模板注入	SSTI 服务端模板注入原理 SSTI 服务端模板注入实战 相关试试题讲解
中间件	第 19 天	中间件基础 1	Apache 安装使用 jboss 中间件安装配置 NGINX 安装使用 Tomcat 安装使用
	第 20 天	中间件基础 2	WebLogic Server 安装与配置 控制台管理 命令行管理 配置 JDBC

			配置 JMS
代码审计	第 21 天	PHP	PHP 代码基础 PHP 代码审计
	第 22 天	JAVA	JAVA 编程基础 JAVA 代码审计
	第 23 天	Python	Python 编程基础 Python 代码审计
	第 24 天	ASP.NET	ASP.NET 编程基础 ASP.NET 代码审计
	第 25 天	JavaScript	JavaScript 基础 JavaScript 审计
应用程序	第 26 天	应用程序上	APP 逆向 APP 接口获取
	第 27 天	应用程序下	PC 客户端内存欺骗 逻辑漏洞及接口获取
后渗透	第 28 天	WebShell 提权	
	第 29 天	端口转发代理 MSF 使用	
	第 30 天	常见语言反序列化漏洞	
	第 31 天	数据库漏洞及不当配置 远程溢出漏洞	
	第 32 天	域渗透 横向渗透	
社会工程学	第 33 天	社会工程学	基础信息获取、信息整理、社工库、邮件伪造、短信伪造、无线热点、二维码、钓鱼网站
近源渗透	第 34 天	近源渗透	无线破解 WiFi 抓包 路由器 WPS 漏洞 无线钓鱼 NFC/RFID/BLE/ZigBee 攻击 BadUSB 制作与使用