### CTF（初级）

培训路径



CTF-WEB初级

3天

精讲、研讨、上机



CTF-MISC初级

1天

精讲、研讨、上机

1天



CTF-CRYPTO初级

精讲、研讨、上级

培训对象

* 信息安全爱好者

入学要求

* 了解信息安全相关基本概念
* 了解安全相关技术
* 对信息安全有兴趣
* 接触过编程语言

培训目标

完成该课程培训后，您将能够：

* 独立解出简单的WEB类CTF题目
* 独立解出简单的MISC类CTF题目
* 独立解出简单的CRYPTO类CTF题目
* 独立解出简单的REVERSE类CTF题目
* 独立解出简单的PWN类CTF题目

CTF-WEB初级

* SQL注入
* SQL基本语法
* SQL注入基本原理与方法
* SQL注入场景（url、登陆框等）简介
* SQL注入基础赛题实践
* SQL注入基础赛题详解
* SQLMAP在SQL注入题中的利用
* RCE
* 命令/代码执行的基本原理
* 系统命令执行与代码执行漏洞相关函数解读
* 系统命令执行与代码执行基础赛题实践
* 系统命令执行与代码执行基础赛题详解
* 文件上传
* 文件上传基本原理
* 后门管理工具介绍与使用
* 常见文件上传防护（前端、后缀名黑白名单、内容检测等）的绕过
* 文件上传基础赛题实践
* 文件上传基础赛题详解
* 文件包含
* 文件包含基本原理
* 常见文件包含防护的绕过
* 常见文件包含和伪协议（filter、phar、zip等）结合的利用
* 文件包含基础赛题实践
* 文件包含基础赛题详解
* SSRF
* SSRF基本原理
* SSRF相关函数详解
* SSRF常见防护（ip变形、302跳转、短网址等）绕过
* SSRF常见利用（文件读取、内网探测等）详解
* SSRF基础赛题实践
* SSRF基础赛题详解
* XXE
* XML基本语法
* XXE相关函数详解
* XXE基本原理
* XXE常见利用（内网探测、文件读取等）详解
* XXE基础赛题实践
* XXE基础赛题详解
* 反序列化
* 反序列化基本原理
* 魔术方法详解
* 反序列化基础赛题实践
* 反序列化基础赛题详解

CTF-MISC初级

* zip压缩包系列
* zip格式详解
* zip常见攻击手段（伪加密、明文攻击、爆破等）详解
* zip相关基础赛题实践
* zip相关基础赛题详解
* 图片隐写系列
* 常见图片格式详解
* 常见图片隐写方法（追加、LSB等）详解
* 图片隐写相关基础赛题实践
* 图片隐写相关基础赛题详解
* 流量分析系列
* wireshark使用及语法详解
* tshark使用及语法详解
* 流量分析相关基础赛题实践
* 流量分析相关基础赛题详解

CTF-CRYPTO初级

* 古典密码学系列
* 常见古典加密方法（凯撒、栅栏、维吉尼亚、四方密码等）详解
* 常见古典密码学解密方法详解
* 常见古典密码学赛题实践
* 常见古典密码学赛题详解

CTF-REVERSE初级

* 汇编基础
* 大小端模式
* 寄存器
* 汇编指令
* 寻址方式
* Ollydbg工具
* 调试断点
* Ollydbg实战
* IDA Pro工具
* 结构类型
* 函数签名识别
* 修复栈平衡
* 加密与解密
* Z3约束求解
* 初级逆向赛题实践
* 初级逆向赛题讲解

CTF-PWN初级

* 操作系统相关
* 可执行文件的装载与进程
* 保护机制
* ASLR
* NX
* FORTIFY
* 栈溢出基础
* 函数调用约定
* 函数调用栈
* 栈溢出原理
* ROP利用技术
* ret2text
* ret2shellcode
* ret2syscall
* 格式化字符串利用技术
* 32位格式化字符串利用