### 计算机网络和网络安全

培训路径

上机、实践



CTF-WEB中级

2天

精讲、研讨、上机



CTF-MISC中级

0.5天

精讲、研讨、上机

0.5天



CTF-CRYPTO中级

精讲、研讨、上机

培训对象

* 有一定信息安全基础的信息安全爱好者
* 安全技术相关行业从业者

入学要求

* 能够用一门编程语言解决一些简单问题
* 熟悉部分安全相关技术
* 对信息安全有兴趣

培训目标

完成该课程培训后，您将能够：

* 独立解出大部分的WEB类CTF题目
* 独立解出大部分的MISC类CTF题目
* 独立解出大部分的CRYPTO类CTF题目
* 独立解出大部分的REVERSE类CTF题目
* 独立解出大部分的PWN类CTF题目

CTF-WEB中级

* SQL注入
* SQL注入盲注利用（各类时间函数、条件语句等）详解
* SQL注入特殊场景（order by、desc等场景）的利用
* SQL注入高级绕过技巧（注释加！、等于号代替等）详解
* SQL注入复杂赛题实践
* SQL注入复杂赛题详解
* RCE
* 系统命令执行/代码执行过滤绕过
* 系统命令执行/代码执行（空格、各类符号等）代替方案
* 命令执行/代码执行极限（无符号、短命令情况等）情况
* 系统命令执行与代码执行复杂赛题实践
* 系统命令执行与代码执行复杂赛题详解
* 文件上传
* 非常规文件上传（条件竞争、随机数文件名预测等）绕过详解
* 文件上传复杂赛题实践
* 文件上传复杂赛题详解
* 文件包含
* 文件包含高级方法详解
* 文件包含复杂赛题实践
* 文件包含复杂赛题详解
* SSRF
* SSRF与gopher结合利用（打mysql、redis等）详解
* SSRF特殊情况（不同函数解析不同）的绕过详解
* SSRF复杂赛题实践
* SSRF复杂赛题详解
* 反序列化
* 无unserialize函数（session、phar等）触发反序列化详解
* 特殊场景反序列化绕过详解
* 内置类简介
* 反序列化复杂赛题实践
* 反序列化复杂赛题详解

CTF-MISC初级

* 非常规考点
* NTFS流隐写详解
* 非常规隐写详解
* 社会工程类详解
* 相关复杂赛题实践
* 相关复杂赛题详解

CTF-CRYPTO初级

* 现代密码学系列
* 数论基础
* 常规现代密码学加密方法（RSA、DSA等）详解
* 常规现代密码学加密缺陷（RSA相关、CBC加密模式带来的安全问题等）详解
* 常规现代密码学赛题实践
* 常规现代密码学赛题详解

CTF-REVERSE中级

* (绕过保护)工具进阶
* Ollydbg脱壳技巧
* IDA对抗花指令
* 反OLLVM混淆
* 加密与解密进阶
* 进阶逆向赛题实践
* 进阶逆向赛题讲解

CTF-PWN中级

* 操作系统进阶
* 延迟绑定技术
* 保护机制进阶
* RELRO
* ROP利用进阶
* Ret2lib\_i386
* Retlib\_amd64
* Ret2csu
* Ret2\_dl\_runtime\_resolve
* Stack\_pivoting
* 格式化字符串进阶
* 64位格式化字符串的利用
* 高级fms利用
* 整数溢出
* 整数溢出