



认证介绍

» 注册信息安全专业人员-渗透测试工程师，英文为 Certified Information Security Professional - Penetration Test Engineer ，简称CISP-PTE。是由中国信息安全测评中心与信息安全企业联合推出的证书。证书持有人员主要从事信息安全技术领域安全渗透测试工作，具有规划测试方案、编写项目测试计划、编写测试用例、测试报告的基本知识和能力。 CISP-PTE专注于培养考核高级应用安全人才， **是业界首个理论与实践相结合的技能水平注册考试。**

认证机构

» 中国信息安全测评中心是我国专门从事信息技术安全测试和风险评估的权威职能机构。依据中央授权，开展信息安全服务和专业人员的能力评估与资质审核。测评中心自2002年开启“注册信息安全专业人员（ CISP)”资格认证注册工作。

认证价值

» 由CISP-PTE认证考试中心360企业安全与CISP-PTE认证考试授权培训机构天融信携手打造国内最专业的渗透测试认证工程师实战课程！ 课程内容从多个角度出发，通过客观知识与实际操作相结合的形式，教授学员最新的网络安全技术并跟踪最新的网络安全动态，在真实的网络环境中发现问题和解决问题，锻炼学员实际解决网络安全问题的能力，有效增强学员所在企事业单位网络防御能力。加入CISP-PTE队伍可以为网络安全专业的学生提高自身价值，提高自身影响力，提供更好学习素材，也为更多的网络安全爱好者提供了一个更加具有优势的平台。

知识体系

- 1、 Web安全：主要包括HTTP协议、注入漏洞、 XSS漏洞、 SSRF漏洞、 CSRF漏洞、文件处理漏洞、访问控制漏洞、会话管理漏洞等相关的技术知识和实践。
- 2、中间件安全：主要包括Apache、 IIS、 Tomcat、 Weblogic、 Websphere、 Jboss等相关的技术知识和实践。
- 3、操作系统安全：主要包括Windows操作系统、 Linux操作系统相关技术知识和实践。
- 4、数据库安全：主要包括MSsql数据库、 Mysql数据库、 Oracle数据库、 Redis数据库相关技术知识和实践。



培训课程

培训为脱产形式，上课时间8天，20%的课程为知识讲解，80%的课程为动手模拟实践。课程安排及知识体系大纲（见下图），*具体课程安排见当期培训指南

日期	课程	内容		
第一天	WEB安全基础	• 信息收集 • 漏洞发现 • 漏洞利用	• HTTP请求方法 • HTTP的状态码	• HTTP协议响应头信息 • HTTP协议中的URL
第二天	WEB安全基础	• SQL注入	• XML注入	• 代码注入
第三天	中间件安全	• Apache	• IIS	• Tomcat
第四天	中间件安全	• Weblogic	• Websphere	• Jboss
第五天	WEB安全基础	• 存储式XSS漏洞 • 反射式XSS漏洞	• DOM式XSS漏洞 • SSRF漏洞	• CSRF漏洞
第六天	WEB安全基础	• 任意文件上传 • 任意文件下载	• 横向越权 • 垂直越权	• 会话劫持 • 会话固定
第七天	操作系统安全	• Windows 操作系统	• Linux 操作系统	
第八天	数据库安全	• Mysql数据库 • Mssql数据库	• Oracle数据库	• Redis数据库

考试要求

» 成为注册信息安全专业人员-渗透测试工程师（CISP-PTE），必须同时满足以下基本要求：

- 1、申请成为注册信息安全专业人员-渗透测试工程师（CISP-PTE），具备一定渗透测试能力，或有意向从事渗透测试的人员，包含信息安全相关专业高校生；
- 2、申请成为注册信息安全专业人员-渗透测试工程师（CISP-PTE）无学历与工作经验的报考要求；
- 3、通过CISP-攻防领域考试中心组织的CISP-PTE考试；
- 4、同意并遵守CISP-PTE职业准则；
- 5、满足CISP-PTE注册要求并成功通过CISP-PTE审核；
- 6、注册信息安全专业人员-渗透测试工程师资质证书有效期三年，证书失效后，需重新参加CISP-PTE注册考试；

考试试题结构

CISP-PTE考试题型为客观题、实操题。客观题为单项选择题，共20题，每题1分；实操题共80分。总分共100分，得分70分以上（含70分）为通过。

“注册信息安全人员-渗透测试工程师”（CISP-PTE）需要学习和掌握CISP-PTE知识体系结构框架中的所有内容。

下图为CISP-PTE试题结构：

CISP-PTE 试题结构		
知识类别	占比	题型
Web安全基础	40%	实操
中间件安全基础	20%	客观+实操
操作系统安全基础	20%	客观+实操
数据库安全基础	20%	客观+实操