**国家注册信息安全专业人员CISP-PTE渗透测试工程师认证**

**培训班**

|  |
| --- |
| **培训服务一览表** |
| **培训地点** | 北京 | 杭州 | 北京 | 上海 |
| **培训时间** | 4月24-28 | 6月26-30 | 8月27-31 | 11月26-30 |
| **培训方式** | · 现场面授 **· 线上**授课 **· 录播回放** |
| **专家授课** | **·4天录播+ 5天集中培训学习：每天6课时，实战专家授课****· 理论梳理 · 案例分享 · 实战演练** |
| **纸质资料** | **注册信息安全专业人员CISP-PTE渗透测试工程师培训讲义** |
| **考试系统** | **CISP-PTE考试练习靶场，学员通过率达95%以上** |
| **学习平台** | **PC端：http://it.zpedu.com/ 移动端APP：IT云课** |
| **社群服务** | **· 学员在线交流 · 专家在线答疑 · 班主任教学管理** |
| **此课程可根据具体需求定制企业内训解决方案** |

#### 组织形式

指导单位：中国信息安全测评中心

主办单位：北京中培伟业管理咨询有限公司

#### 课程背景

为提高各单位信息安全整体水平，加强信息安全人员专业技能，促进信息安全人员持证上岗，现组织开展注册信息安全专业人员攻防领域（CISP-PTE）培训及认证工作，此认证是信息安全从业人员的水平证书，证明证书持有者具备从事信息安全技术领域网站渗透测试工作，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。此证书为从事信息安全领域的工作人员提高专业资历提供了新的机遇，为各单位信息安全提供了技术储备、规范方法和专业人才，从根本上解决了信息安全从业人员的专业水平问题，从而提高各单位信息安全的综合实力，全面提升网络安全服务保障能力和水平，请各单位积极组织参加。

#### CISP-PTE介绍

注册信息安全专业人员攻防领域（CISP-PTE）培训是由中国信息安全测评中心统一管理和规范的信息安全专业培训，是目前国内最为主流及被业界认可的专业攻防领域的资质培训。CISP-PTE目前是国内唯一针对网络安全渗透测试专业人才的资格认证，也是国家对信息安全人员资质的最高认可。

在整个注册信息安全专业人员-渗透测试(CISP-PTE)的知识体系结构中， 共包括 web 安全基础、中间件安全基础、操作系统安全基础、数据库安全基础这四个知识类，每个知识类根据其逻辑划分为多个知识体，每个知识体包含多个知识域，每个知识域由一个或多个知识子域组成。

CISP-PTE 知识体系结构共包含四个知识类，分别为:

1. web安全基础: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. 中间件安全基础:主要包括Apache、IIS、Tomcat、weblogic、websphere、 Jboss 等相关的技术知识和实践。
3. 操作系统安全基础:主要包括Windows操作系统、Linux操作系统相关技术知识和实践。
4. 数据库安全基础: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。

#### 培训特色

1. 理论与实践相结合、案例分析与实验穿插进行；
2. 专家精彩内容解析、学员专题讨论、分组研究；
3. 通过全面知识理解、专题技能掌握和安全实践增强的授课方式。

#### 日程安排

课程体系严格遵照中国信息安全测评中心的课程大纲要求，具体培训课程设置如下：

**四天网课（理论部分）+五天面授（实操部分）**

|  |
| --- |
| CISP-PTE注册信息安全专业人员-渗透测试工程师知识体系大纲 |
| 第一部分 |
| 知识类 | 知识体 | 知识域 | 知识子域 | 知识点 |
| 第一章操作系统安全基础 | Windows | 账户安全 | 账户的基本概念 | Windows用户账户和组账户权限的分配 |
| 账户风险与安全策略 | 了解Windows用户空口令风险 |
| 了解多用户同时使用的安全配置 |
| 了解对用户登入事件进行审核方法 |
| 了解对远程登入账号的检查 |
| 文件系统安全 | 文件系统基础知识 | 掌握NTFS文件权限各类 |
| NTFS权限设置 | 掌握通过ACL控制列表，设置目录或者文件的用户访问权限 |
| 掌握命令行下修改目录或者文件的访问权限的方法 |
| 日志分析 | 系统日志的分类 | 了解Windows系统日志的种类 |
| 了解Windows安全日志的登入类型 |
| 日志的审计方法 | 掌握日志审计的方法 |
| Linux | 账户安全 | 账户的基本概念 | 了解Linux系统中的账号和组 |
| 账户风险与安全策略 | 了解弱口令密码带来的风险 |
| 掌握检查空口令的方法 |
| 掌握检查系统中是否存在其它ID为0的用户的方法 |
| 文件系统安全 | 文件系统的格式 | 了解Linux文件系统的文件格式分类 |
| 安全访问与权限设置 | 掌握如何检查系统中存在的SUID和SGID程序 |
| 掌握检查系统中任何人都有写权限的目录的方法 |
| 掌握修改目录和文件权限的方法 |
| 掌握搜索文件内容的方法 |
| 日志分析 | 系统日志的分类 | 了解Linux系统的日志种类 |
| 了解Linux日志文件 |
| 系统日志的审计方法 | 掌握使用常用的日志查看命令，进行日志审计的方法 |

|  |
| --- |
| 第二部分 |
| 第二章数据库安全基础 | 关系型数据库 | MSSQL | MSSQL角色与权限 | 了解MSSQL数据库在操作系统中启动的权限 |
| 掌握MSSQL数据库中服务器角色和数据库角色 |
| 掌握MSSQL存在SA弱口令和空口令带来的危害 |
| MSSQL存储过程安全 | 掌握MSSQL数据库执行系统命令或者操作系统文件的存储过程 |
| 掌握MSSQL提升权限的方法 |
| MYSQL | MYSQL权限与设置 | 了解MYSQL在操作系统中运行的权限 |
| 了解MYSQL账户的安全策略 |
| 了解MYSQL远程访问的控制方法 |
| 了解MYSQL数据库所在目录的权限控制 |
| MYSQL内置函数风险 | 掌握MYSQL数据库常用函数 |
| 掌握MYSQL数据库权限提升的方法 |
| Oracle | ORACLE角色与权限 | 了解ORACLE数据库的账号管理与授权 |
| 了解为不同管理员分配不同的账号的方法 |
| 了解设置管理public角色的程序包执行权限 |
| ORACLE安全风险 | 了解限制库文件的访问权限 |
| 掌握ORACLE执行系统命令的方法 |
| 非关系型数据库 | Redis | Redis权限与设置 | 了解Redis数据库运行权限 |
| 了解Redis数据库的默认端口 |
| Redis未授权访问风险 | 掌握Redis未授权访问的危害 |
| 掌握Redis开启授权的方法 |

|  |
| --- |
| 第三部分 |
| 第三章中间件安全基础 | 主流的中间件 | Apache | Apache服务器的安全设置 | 了解当前Apache服务器的运行权限 |
| 了解控制配置文件和日志文件的权限，防止未授权访问 |
| 了解设置日志记录文件、记录内容、记录格式 |
| 了解禁止Apache服务器列表显示文件的方法 |
| 了解修改Apache服务器错误页面重定向的方法 |
| 掌握设置WEB目录的读写权限，脚本执行权限的方法 |
| Apache服务器文件名解析漏洞 | 了解Apache服务器解析漏洞的利用方式 |
| 掌握Apache服务器文件名解析漏洞的防御措施 |
| Apache服务器日志审计方法 | 掌握Apache服务器日志审计方法 |
| IIS | IIS服务器的安全设置 | 了解身份验证功能，能够对访问用户进行控制 |
| 了解利用账号控制WEB目录的访问权限，防止跨目录访问 |
| 了解为每个站点设置单独的应用程序池和单独的用户的方法 |
| 了解取消上传目录的可执行脚本的权限的方法 |
| 启用或禁止日志记录，配置日志的记录选项 |
| IIS服务器常见漏洞 | 掌握IIS6、IIS7的文件名解析漏洞 |
| 掌握IIS6写权限的利用 |
| 掌握IIS6存在的短文件名漏洞 |
| IIS服务器日志审计方法 | 掌握IIS日志的审计方法 |
| Tomcat | Tomcat服务器的安全设置 | 了解Tomcat服务器启动的权限 |
| 了解Tomcat服务器后台管理地址和修改管理账号密码的方法 |
| 了解隐藏Tomcat版本信息的方法 |
| 了解如何关闭不必要的接口和功能 |
| 了解如何禁止目录列表，防止文件名泄露 |
| 掌握Tomcat服务器通过后台获取权限的方法 |
| 掌握Tomcat样例目录session操纵漏洞 |
| Tomcat服务器的日志审计方法 | 了解Tomcat的日志种类 |
| 掌握Tomcat日志的审计方法 |
| JAVA开发的中间件 | weblogic | Weblogic的安全设置 | 了解Weblogic的启动权限 |
| 了解修改Weblogic的默认开放端口的方法 |
| 了解禁止Weblogic列表显示文件的方法 |
| Weblogic的漏洞利用与防范 | 掌握Weblogic后台获取权限的方法 |
| 掌握Weblogic存在的SSRF漏洞 |
| 掌握反序列化漏洞对Weblogic的影响 |
| Weblogic的日志审计方法 | 掌握Weblogic日志的审计方法 |
| websphere | Websphere的安全设置 | 了解Websphere管理的使用 |
| 了解Websphere的安全配置 |
| Websphere的漏洞利用与防范 | 掌握反序列化漏洞对Websphere的影响 |
| 掌握Websphere后台获取权限的方法 |
| Websphere的日志审计方法 | 掌握Websphere的日志审计 |
| Jboss | Jboss的安全设置 | 了解设置jmx-console/web-console密码的方法 |
| 了解开启日志功能的方法 |
| 了解设置通讯协议，开启HTTPS访问 |
| 了解修改WEB的访问端口 |
| Jboss的漏洞利用与防范 | 掌握反序列化漏洞对Jboss的影响 |
| JMXInvokerServlet/jmx-console/web-console漏洞利用与防范 |
| Jboss的日志审计方法 | 掌握Jboss日志审计的方法 |

|  |
| --- |
| 第四部分 |
| 第四章web安全基础 | HTTP协议 | HTTP请求方法 | HTTP1.0的请求方法 | 掌握HTTP1.0三种请求方法：GET/POST/HEAD |
| 掌握GET请求的标准格式 |
| 掌握POST请求提交表彰，上传文件的方法 |
| 了解HEAD请求与GET请求的区别 |
| HTTP1.1新增的请求方法 | 了解HTTP1.1新增了五种请求方法：OPTIONS/PUT/DELETE/TRACE和CONNECT方法的基本概念 |
| 掌握HTTP1.1新增的五种请求的基本方法和产生的请求结果 |
| HTTP状态码 | HTTP状态码的分类 | 了解HTTP状态码的规范 |
| 了解HTTP状态码的作用 |
| 掌握常见的HTTP状态码 |
| HTTP状态码的含义 | 了解HTTP状态码2\*\*、3\*\*、4\*\*、5\*\*代表的含义 |
| 掌握用计算机语言获取HTTP状态码的方法 |
| HTTP协议响应头信息 | HTTP响应头的类型 | 了解常见的HTTP响应头 |
| 掌握HTTP响应头的作用 |
| HTTP响应头的含义 | 了解HTTP响应头的名称 |
| 掌握HTTP响应头的格式 |
| HTTP协议的URL | URL的定义 | 了解URL的基本概念 |
| URL的格式 | 了解URL的结构 |
| 掌握URL编码格式 |
| 注入漏洞 | SQL注入 | SQL注入概念 | 了解SQL注入漏洞原理 |
| 了解SQL注入漏洞对于数据安全的影响 |
| 掌握SQL注入漏洞的方法 |
| SQL注入漏洞类型 | 了解常见数据库的SQL查询语法 |
| 掌握MSSQL\MYSQL\ORACLE数据库的注入方法 |
| 掌握SQL注入漏洞的类型 |
| SQL注入漏洞安全防护 | 掌握SQL注入漏洞修复和防范方法 |
| 掌握一些SQL注入漏洞检测工具的使用方法 |
| XML注入 | XML注入概念 | 了解什么是XML注入漏洞 |
| 了解XML注入漏洞产生的原因 |
| XML注入漏洞检测与防护 | 掌握XML注入漏洞的利用方式 |
| 掌握如何修复XML注入漏洞 |
| 代码注入 | 远程文件包含漏洞（RFI） | 了解什么是远程文件包含漏洞 |
| 了解远程文件包含漏洞所用到的函数 |
| 掌握远程文件包含漏洞的利用方式 |
| 掌握远程文件包含漏洞代码审计方法 |
| 掌握修复远程文件包含漏洞的方法 |
| 本地文件包含漏洞（LFI） | 了解什么是本地文件包含漏洞 |
| 了解本地文件包含漏洞产生的原因 |
| 掌握本地文件包含漏洞利用的方式 |
| 了解PHP语言中的封装协议 |
| 掌握本地文件包含漏洞修复方法 |
| 命令执行漏洞（CI） | 了解什么是命令注入漏洞 |
| 了解命令注入漏洞对系统安全产生的危害 |
| 掌握脚本语言中可以执行系统命令的函数 |
| 了解第三方组件存在的代码执行漏洞，如struts2 |
| 掌握命令注入漏洞的修复方法 |
| XSS漏洞 | 存储式XSS | 存储式XSS的概念 | 了解什么是存储式XSS漏洞 |
| 了解存储式XSS漏洞对安全的影响 |
| 存储式XSS的检测 | 了解存储式XSS漏洞的特征和检测方法 |
| 掌握存储式XSS漏洞的危害 |
| 存储式XSS的安全防护 | 掌握修复存储式XSS漏洞的方式 |
| 了解常用WEB漏洞扫描工具对存储式XSS漏洞扫描方法 |
| 反射式XSS | 反射式XSS的概念 | 了解什么是反射式XSS漏洞 |
| 了解反射式XSS漏洞与存储式XSS漏洞的区别 |
| 反射式XSS的利用与修复 | 了解反射式XSS漏洞的触发形式 |
| 了解反射式XSS漏洞利用的方式 |
| 掌握反射式XSS漏洞检测与修复方法 |
| DOM式XSS | DOM式XSS的特征 | 了解什么是DOM式XSS漏洞 |
| 掌握DOM式XSS漏洞的触发形式 |
| DOM式XSS的防御 | 掌握DOM式XSS漏洞的检测方法 |
| 掌握DOM式XSS漏洞的修复方法 |
| 请求伪造漏洞 | SSRF漏洞 | 服务端请求伪造漏洞概念 | 了解什么是SSRF漏洞 |
| 了解利用SSRF漏洞进行端口探测的方法 |
| 服务端请求漏洞的检测与防护 | 掌握SSRF漏洞的检测方法 |
| 了解SSRF漏洞的修复方法 |
| CSRF漏洞 | 跨站请求伪造漏洞概念 | 了解CSRF漏洞产生的原因 |
| 理解CSRF漏洞的原理 |
| 跨站请求漏洞的危害与防御 | 了解CSRF漏洞与XSS漏洞的区别 |
| 掌握CSRF漏洞的挖掘和修复方法 |
| 文件处理漏洞 | 任意文件上传 | 上传漏洞的原理与分析 | 了解任意文件上传漏洞产生的原因 |
| 了解服务端语言对上传文件类型限制方法 |
| 上传漏洞的检测与防范 | 了解任意文件上传漏洞的危害 |
| 掌握上传漏洞的检测思路和修复方法 |
| 任意文件下载 | 文件下载漏洞的原理与分析 | 了解什么是文件下载漏洞 |
| 掌握通过文件下载漏洞读取服务端文件的方法 |
| 文件下载漏洞的检测与防范 | 掌握能够通过代码审计和测试找到文件下载漏洞 |
| 掌握修复文件下载漏洞的方法 |
| 访问控制漏洞 | 横向越权 | 横向越权漏洞的概念 | 了解横向越权漏洞的基本概念 |
| 了解横向越权漏洞的形式 |
| 横向越权漏洞的检测与防范 | 了解横向越权漏洞对网站安全的影响 |
| 掌握横向越权漏洞的测试和修复方法 |
| 垂直越权 | 垂直越权漏洞的概念 | 了解垂直越权漏洞的基本概念 |
| 了解垂直越权漏洞的种类和形式 |
| 垂直越权漏洞的检测与防范 | 了解对网站安全的影响 |
| 掌握越权漏洞的测试方法和修复 |
| 会话管理漏洞 | 会话劫持 | 会话劫持漏洞的概念与原理 | 了解什么是会话劫持漏洞 |
| 了解会话劫持漏洞的危害 |
| 会话劫持漏洞基本防御方法 | 了解Session机制 |
| 了解httponly的设置方法 |
| 掌握会话劫持漏洞防御方法 |
| 会话固定 | 会话固定漏洞的概念与原理 | 了解什么是会话固定漏洞 |
| 了解会话固定漏洞的检测方法 |
| 会话固定漏洞基本防御方法 | 了解会话固定漏洞的形成的原因 |
| 了解会话固定漏洞的风险 |
| 掌握会话固定漏洞的防范方法 |
| 第6天 考试 |

#### 授课专家

**刘老师** 曾任阿里巴巴高级工程师，超过15年IT运维与IT培训从业经验，主要从事企业网络服务的运维、大数据和云平台的运维、企业网络服务需求分析和网络构建、网络割接等项目;通过和企业对接进行IT运维的培训，培养IT运维、IT安全运维学员超过3000名;具备丰富的企业运维和网络构建等项目经验，尤其在金融、运营商、政府等行业有丰富的项目实施经验。目前主要专业领域集中于Linux&Cisco企业服务、IT服务管理、信息安全等方面，曾服务的主要客户有：阿里巴巴、北京市丰台区人民政府、北京XXX金融有限公司、北京吉利大学、北京XXXXIT培训中心、中兴集团大数据中心等。长期从事Linux&Cisco、信息安全(CISP/CISSP/Secrity+,cisp-pte等培训工作。

**高老师** 曾任北京丁牛科技有限公司安全部，渗透测试组组长，中国金融认证中心信息安全工程师，银联系统CTF线下赛-三等奖，主要项目经历包括Web渗透、APP安全测试(android)、微信小程序、API接口、CTF、逆向、后渗透及持久化方面，知识面比较广。

**徐老师** 十年信息安全工作经验，热爱研究网络安全技术。主攻Web、渗透测试、安全研究、漏洞挖掘、代码审计擅长 web方向，热爱ctf和awd。在web方向的php代码审计尤为擅长，曾参与审计某司自研项目并审计到高危漏洞。有丰富的政府，内网 外网项目渗透经验。多次在 ctf比赛中获取名次，并担任出题者和裁判。曾任职国内某top10安全公司奇安信及多个公司的特聘安全培训讲师。

#### 考试及取证

考试由中国信息安全测评中心组织实施，考试合格后可获得由中国信息安全测评中心颁发的“注册信息安全人员-渗透测试工程师”(CISP-PTE)证书。

**培训考试：见中国信息安全测评中心考试计划安排**

考试说明：由中国信息安全测评中心出试卷

考试要求： 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，得到 70 分以上(含 70 分)为通过。

**注：考试不通过的学员可免费参加一次补考。**

**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** |

**CISP-PTE考试形式**

|  |  |  |
| --- | --- | --- |
| **安全加固与防御** | **单项选择** | **240分钟** |
| **Web安全基础** | **实操** |
| **日志与数据分析** | **实操** |
| **渗透测试基础** | **实操** |

#### 培训费用

全国统一收费标准：19800元/人，（含培训费、考试费、注册费、注册年金等），食宿可统一安排，费用自理。

其中：

培训费：14800元/人，(包含：教材、培训费等)

注册费：5000元/人，(包含：认证费、三年年金)。

需提前提交的材料：

1.个人近期免冠2寸蓝底彩色照片2张（后面标注姓名，不粘贴）

2.身份证（正反面）复印件1份

3.学历、学位证明复印件1份

4.考试注册申请表纸质盖章版1份。

#### 报名回执《CISP-PTE渗透测试工程师》

|  |  |
| --- | --- |
| 单位名称（开发票名称） |  |
| 快递地址 |  | 邮编 |  |
| 联 系 人 |  | 职位 |  | 电话 |  |
| Email |  | 传真 |  |
| 学员姓名 | 身份证号（做证书使用） | 邮箱 | 联系电话 | 培训地点 | 是否住宿 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 汇 款账 户 | 户 名：北京中培伟业管理咨询有限公司开户行：北京农村商业银行卢沟桥支行账 号：0203 0101 0300 0033 172 | 备注： |
| 发票信息： | 单位名称： 统一社会信用代码： 开户银行： 账号： 地址： 电话： |

#### 联系方式

联系人：赵娟

手 机（微信）：13261046023

邮 箱：1164082541@qq.com

 二〇二四年六月一日

**附件：关于严格执行CISP-PTE收费标准的通知**



CISP-PTE证书样本

