中国通信企业协会文件

通企〔2021〕98 号

关于举办注册信息安全专业人员（CISP）和渗透测试工程师（CISP-PTE）认证培训班的通知

各有关单位：

为提高信息通信行业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，更好地支撑网络强国建设，中国通信企业协会于今年上半年举办了两期“国家注册信息安全专业人员（CISP）”认证培训，得到了信息通信行业各相关单位的积极参与。为满足培训需求，中国通信企业协会将联合授权机构于今年下半年继续举办 CISP 认证培训，并开展首期渗透测试工程师（CISP-PTE）认证培训。现将有关事宜通知如下：

一、认证介绍

（一）注册信息安全专业人员（CISP），是由中国信息安全测评中心于 2002 年推出的、业内公认的国内信息安全领域最权威的国

家级认证。可选择CISE（信息安全工程师）或CISO（信息安全管理人员）两个方向进行认证。

（二）注册渗透测试工程师（CISP-PTE）认证是由中国信息安全测评中心针对攻防专业领域实施的资质培训， 是国内唯一针对网络安全渗透测试专业人才的资格认证。

二、培训内容

（一）CISP主要模块：信息安全保障、信息安全监管、信息安全管理、业务连续性、安全工程与运营、安全评估、安全支撑技术、物理与网络通信安全、计算环境安全、软件安全开发。（详见附件2）

（二）CISP-PTE主要模块

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(详见附件3)。

三、培训时间、地点

（一）CISP培训

培训地点	西安 （可直播）	青岛 （可直播）	上海 （可直播）	北京 （可直播）	广州 （可直播）
培训时间	7 月 20—25 日	7 月 26—31 日	8 月 9-14 日	8 月 20-25 日	9 月 6-11 日
报名截止时间	7 月 19 日	7 月 23 日	8 月 6 日	8 月 18 日	9 月 3 日
培训地点	培训具体地点另行通知				
培训方式	面授或直播				
考试题型及分值	1、考试题型为单项选择题，共 100 题，每题 1 分。 2、70 分以上(含)为通过。				

（二）CISP-PTE 培训

培训地点	北京	广州	成都	北京
培训时间	7 月 31-8 月 5 日	9 月 23-28 日	10 月 15-20 日	22 年 1 月
报名截止时间	7 月 30 日	9 月 22 日	10 月 14 日	待定
培训地点	培训具体地点另行通知			
考试题型及分值	1.考试题型为客观题、实操题。 2.客观题为单项选择题，共 20 题，每题 1 分。 3.实操题 6 道题，共 80 分。5 道小题每题 10 分，1 道综合题 30 分。 4.总分 70 分以上(含)为通过。			

四、培训及考试费用

CISP 培训考试费（疫情优惠价）9600 元/人（含培训费 6600 元、考试费 3000 元、注册服务费、注册年金等），通过率 99%。考试不通过的学员可免费参加二次补考。

培训形式：面授和在线直播同时进行。如选择在线直播可送免费面授课程一次，视频课件一年内可随意观看。

CISP-PTE 培训考试费 19800 元/人（含培训费 14800 元、考试费 5000 元、注册服务费、注册年金等），高通过率。考试不通过的学员可免费参加二次补考。

培训形式：4 天网络点播+5 天线下面授

五、考试

（一）CISP 考试：由中国信息安全测评中心组织实施。测评

中心将根据学员考试及注册申请表（含所需资料）提交时间、考生属地分布情况及考生规模，统筹安排确定考试时间及地点。

（二）CISP-PTE 考试：培训完成后第二天考试。由中国信息安全测评中心组织实施。

六、申请条件：

（一）硕士及硕士以上学历，具备 1 年以上工作经历；

（二）大学本科学历，具备 2 年以上工作经历；

（三）大学专科学历，具备 4 年以上工作经历；

（四）具备 1 年以上从事信息安全领域工作经历。

需提前提交的材料（均为电子版）：

（一）个人近期免冠 2 寸白底深色照片 1 张；

（二）身份证（正反面复印在一张纸上）扫描件 1 份（务必清晰）；

（三）学历、学位证明扫描件 1 份；

（四）“注册信息安全人员考试及注册申请表”纸质盖章版 1 份。（申请表电子版文件待索）

七、报名方法及联系方式

（一）报名方法

请于报名截止日前将填写完整的《报名回执》、培训及考试费用汇款转账至中国通信企业协会 ztqx2021@163.com（注明单位名称或学员姓名及“CISP 或 CISP-PTE”）。如需开具增值税专用发票，请将经单位财务核对后的开票信息准确填写在报名回执中。

收款单位：中国通信企业协会

账　号：0200　0033　0900　5403　113

开 户 行：中国工商银行北京长安支行

（二）联系方式

中国通信企业协会培训部

宋老师　010-68200128、18612568779

王老师　010-68200127、13911072637

附件：1.报名回执

2.CISP 培训课程设置

3.CISP-PTE 培训课程设置

中国通信企业协会

2021年6月29日

附件 1

报名回执

注册信息安全专业人员（CISP）、渗透测试工程师（CISP-PTE）认证培训班

单位名称								
序号	姓　名	性别	民族	部门及职务	联系电话	电子邮箱	班　次	住　宿
							☐cisp_____（填城市）班 ☐cisp-pte_____（填城市）班	☐单住　☐合住 ☐不住宿
							☐cisp_____（填城市）班 ☐cisp-pte_____（填城市）班	☐单住　☐合住 ☐不住宿
							☐cisp_____（填城市）班 ☐cisp-pte_____（填城市）班	☐单住　☐合住 ☐不住宿
发 票 信 息	1.发票抬头： 2.纳税人识别码： 3.单位注册地址：					4.开户行名称： 5.账号： 6.联系电话：		
报名联系人及联系方式	部门：　　姓名：　　电话：　　邮箱：							

邮箱：ztqx2021@163.com　　电话：　010-68200128、68200127、18612568779、13911072637

附件 2

CISP 培训课程设置

时间	模块	大纲
第一单元	信息安全保障	内容一：信息安全保障基础 1 信息安全概念 2 信息安全属性 3 信息安全视角 4 信息安全发展阶段 5 信息安全保障新领域 内容二：安全保障框架模型 1.基于时间的 PDR 与 PPDR 模型 2 信息安全保障技术框架 3 信息系统安全保障评估框架 4 舍伍德的商业应用安全架构
第二单元	信息安全监管	内容一：网络安全法律体系建设 1 计算机犯罪 2 我国立法体系 3 网络安全法 4 网络安全相关法规 内容二：国家网络安全政策 1 国家网络空间安全战略 2 国家网络安全等级保护相关政策 内容三：网络安全道德准则 1 道德约束 2 职业道德准则 内容四：信息安全标准 1 信息安全标准基础 2 我国信息安全标准 3 网络安全等级保护标准族
第三单元	信息安全管理	内容一：信息安全管理基础 1 基本概念 2 信息安全管理的作用 内容二：信息安全风险管理 1 风险管理基本概念 2 常见风险管理模型 3 安全风险管理基本过程 内容三：信息安全管理体系建设 1 信息安全管理体系成功因素 2 PDCA 过程 3 信息安全管理体系建设过程

时间	模块	大纲
		4 文档化 内容四：信息安全管理体系最佳实践 1 信息安全管理体系控制措施类型 2 信息安全管理体系控制措施结构 3 信息安全管理体系控制措施 内容五：信息安全管理体系度量 1 基本概念 2 测量要求与实现
第四单元	业务连续性	内容一：业务连续性 1 业务连续性管理基础 2 业务连续性计划 内容二：信息安全应急响应 1 信息安全事件与应急响应 2 网络安全应急响应预案 3 计算机取证与保全 4 信息安全应急响应管理过程 内容三：灾难备份与恢复 1 灾难备份与恢复基础 2 灾难恢复相关技术 3 灾难恢复策略 4 灾难恢复管理过程
第五单元	安全工程与运营	内容一：系统安全工程 1 系统安全工程基础 2 系统安全工程理论基础 3 系统安全工程能力成熟度模型 4 SSE-CMM 的安全工程过程 5SSE-CMM 的安全工程能力 内容二：安全运营 1 安全运营概述 2 安全运营管理 内容三：内容安全 1 内容安全基础 2 数字版权 3 信息保护 4 网络舆情 内容四：社会工程学与培训教育 1 社会工程学 2 培训教育
第六单元	安全评估	内容一：安全评估基础 1 安全评估概念 2 安全评估标准 内容二：安全评估实施 1 风险评估相关要素

时间	模块	大纲
		2 风险评估途径与方法 3 风险评估基本过程 4 风险评估文档 内容三：信息系统审计 1 审计原则与方法 2 审计技术控制 3 审计管理控制 4 审计报告
第七单元	安全支撑技术	内容一：密码学 1 基本概念 2 对称密码算法 3 公钥密码算法 4 其他密码服务 5 公钥基础设施 内容二：身份鉴别 1 身份鉴别的概念 2 基于实体所知的鉴别 3 基于实体所有的鉴别 4 基于实体特征的鉴别 5 Kerberos 体系 6 认证、授权和计费 内容三：访问控制 1 访问控制模型的基本概念 2 自主访问控制模型 3 强制访问控制模型 4 基于角色的访问控制模型 5 基于规则的访问控制模型 6 特权管理基础设施
第八单元	物理与网络通信安全	内容一：物理安全 1 环境安全 2 设施安全 3 传输安全 内容二：OSI 通信模型 1 OSI 模型 2 OSI 模型通信过程 3 OSI 模型安全体系构成 内容三：TCP/IP 协议安全 1 协议结构及安全问题 2 安全解决方案 内容四：无线通信安全 1 无线局域网安全 2 蓝牙通信安全 3 RFID 通信安全 内容五：典型网络攻击防范

时间	模块	大纲
		1 欺骗攻击 2 拒绝服务攻击 内容六：网络安全防护技术 1 入侵检测系统 2 防火墙 3 安全隔离与信息交换系统 4 虚拟专网
第九单元	计算环境安全	内容一：操作系统安全 1 操作系统安全机制 2 操作系统安全配置 内容二：信息收集与系统攻击 1 信息收集 2 缓冲区溢出攻击 内容三：恶意代码防护 1 恶意代码的预防 2 恶意代码的检测分析 3 恶意代码的消除 4 基于互联网的恶意代码防护 内容四：应用安全 1 web 应用安全 2 电子邮件安全 3 其他互联网应用 内容五：数据安全 1 数据库安全 2 数据泄露防护
第十单元	软件安全开发	内容一：软件安全开发生命周期 1 软件生命周期模型 2 软件危机与安全问题 3 软件安全生命周期模型 内容二：软件安全需求及设计 1 威胁建模 2 软件安全需求分析 3 软件安全设计 内容三：软件安全实现 1 安全编码原则 2 代码安全编译 3 代码安全审核 内容四：软件安全测试 1 软件测试 2 软件安全测试 内容五：软件安全交付 1 软件供应链安全 2 软件安全验收 3 软件安全部署

附件 3

CISP-PTE 培训课程设置

四天网课（理论部分）+五天面授（实操部分）

知识类	知识体	知识域	知识子域	知识点
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				
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

知识类	知识体	知识域	知识子域	知识点
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

知识类	知识体	知识域	知识子域	知识点
第三章 中间件安全基础	主流的中间件	IIS	IIS 服务器的安全设置	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

知识类	知识体	知识域	知识子域	知识点
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

知识类	知识体	知识域	知识子域	知识点
第四章 web 安全基础	注入漏洞	代码注入	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

知识类	知识体	知识域	知识子域	知识点
第四章 web 安全基础		任意文件下载	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				