Web 安全测试

职业技能等级标准

（2021 年 1.0 版）

北京神州数码云科信息技术有限公司 制定

2021 年 4 月 发布

目 次

前　言

本标准按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本标准起草单位：北京神州数码云科信息技术有限公司、中国职业技术教育学会教学工作委员会、机械工业出版社、华中科技大学、北京信息职业技术学院、山东商业职业技术学院、江苏信息职业技术学院、福建信息职业技术学院、重庆电子工程职业学院、深圳信息职业技术学院、邢台职业技术学院、陕西工业职业技术学院、咸阳职业技术学院、兰州资源环境职业技术学院、杭州市电子信息职业学校。

本标准主要起草人：王军伟、邹德清、张鹏、杨鹤男、闫立国、朱旭刚、史宝会、李宏达、武春岭、褚建立、蔡铁、唐林、张磊、张卫婷、华驰、佘运祥、梁伟、樊睿等（排名不分先后）。

声明：本标准的知识产权归属于北京神州数码云科信息技术有限公司，未经北京神州数码云科信息技术有限公司同意，不得印刷、销售。

1. 范围

本标准规定了Web安全测试职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于Web安全测试职业技能培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

2. 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 20272-2019 信息安全技术 操作系统安全技术要求

GB/T 21050-2019 信息安全技术 网络交换机安全技术要求

GB/T 18018-2019 信息安全技术 路由器安全技术要求

GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 37931-2019 信息安全技术 Web应用安全检测 系统安全技术要求和测试评价方法

GB/T 37933-2019 信息安全技术 工业控制系统专用 防火墙技术要求

GB/T 30283-2013 信息安全技术 信息安全服务分类

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

3. 术语和定义

3.1 信息安全

保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗依赖性、可靠性等性质。

3.2 计算机信息系统

由计算机及相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

3.3 可靠性

预期行为和结果保持一致的特性。

3.4 数据完整性

数据没有遭受以未授权方式所作的更改或破坏的特性。

3.5 安全功能策略

描述了特定安全行为的一组规则。

3.6 传输层安全协议

一种作为安全套接层协议的后继的正式互联网协议。

3.7 入侵检测

检测入侵的正式过程。该过程一般特征为采集如下知识：反常的使用模式，被利用的脆弱性及其类型、利用的方式，以及何时发生及如何发生。

3.8 攻击特征

执行某种攻击的计算机活动序列或其变体，通常通过检查网络流量或主机日志以确定，入侵检测系统也依其来发现已经发生的攻击。

4. 适用院校专业

中等职业学校：网络信息安全、计算机网络技术、计算机应用、网站建设与管理、软件与信息服务等专业。

高等职业学校：信息安全与管理、计算机网络技术、计算机应用技术、计算机信息管理、计算机系统与维护等专业。

应用型本科学校：信息安全、网络空间安全、网络工程、计算机科学与技术等专业。

5. 面向职业岗位（群）

【Web 安全测试】（初级）：主要面向计算机服务行业、网络安全领域的初级信息安全工程师职业岗位，从事信息安全相关工作，能够了解渗透测试的原理与方法，熟悉渗透测试工具的使用，完成网络渗透测试与安全加固、Web 安全基础测试等工作。

【Web 安全测试】（中级）：主要面向计算机服务行业、网络安全领域的中级信息安全工程师职业岗位，从事信息安全相关工作，能够完成 Windows 操作系统安全加固、Linux 操作系统安全加固、Web 安全渗透测试等工作。

【Web 安全测试】（高级）：主要面向计算机服务行业、网络安全领域的高级信息安全工程师职业岗位，从事信息安全相关工作，能够完成 Web 安全漏洞开发及加固、代码审计与逆向分析、综合渗透测试与安全开发、安全事件综合分析等工作。

1 职业技能要求

6.1 职业技能等级划分

Web 安全测试职业技能等级分为三个等级：初级、中级、高级。三个级别依次递进，高级别涵盖低级别职业技能要求。

【Web 安全测试】（初级）：能够根据工作任务要求，完成网络安全法律法规的分析、网络渗透测试及安全加固、WEB 工作流程安全分析等工作任务。

【Web 安全测试】（中级）：能够根据工作任务要求，完成 Windows 系统的渗透测试及安全加固、Linux 系统的渗透测试及安全加固、SQL 注入渗透测试、

XSS(跨站脚本)渗透测试、CSRF(跨站请求伪造)渗透测试、文件上传的渗透测试、文件包含的渗透测试等工作任务。

【Web 安全测试】(高级)：能够根据工作任务要求，完成 Web 安全漏洞开发及加固、堆栈溢出漏洞渗透测试、常见 Web 漏洞\系统漏洞的代码审计、安全代码的编写、逆向分析、操作系统 ShellCode 开发等工作任务。

6.2 职业技能等级要求描述

表 1 Web 安全测试职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1.网络安全渗透测试	1.1 网络安全基础分析	1.1.1 能根据网络安全基础分析工作任务要求，熟悉网络信息安全基础知识，准确识别安全风险。 1.1.2 能根据网络安全基础分析工作任务要求，熟练掌握网络安全相关的法律法规，准确识别网络安全法律法规边界。 1.1.3 能根据网络安全基础分析工作任务要求，完成对网络拓扑和网络结构的安全分析，准确识别网络结构中的安全风险。 1.1.4 能根据网络安全基础分析工作任务要求，完成网络与信息安全威胁的分析，准确识别安全风险。
	1.2 OSI 数据链路层渗透测	1.2.1 能够根据 OSI 数据链路层渗透测试工作任务要求，熟练掌握 MAC 泛洪\欺骗（MAC Flooding、MAC Spoofing）渗透测试的原理与方法，完成渗透测试，测试结果符合

工作领域	工作任务	职业技能要求
	试	工作任务要求。 1.2.2 能够根据 OSI 数据链路层渗透测试工作任务要求，熟练掌握生成树攻击（STP Spoofing、STP BPDU DOS）渗透测试的原理与方法，完成渗透测试，测试结果符合工作任务要求。 1.2.3 能够根据 OSI 数据链路层渗透测试工作任务要求，熟练掌握 VLAN 跳跃攻击（Nested VLAN Hopping Attack）渗透测试的原理与方法，完成渗透测试，测试结果符合工作任务要求。 1.2.4 能够根据 OSI 数据链路层渗透测试工作任务要求，熟练掌握 DTP 攻击渗透测试(Dynamic Trunking Protocol Attack）的原理与方法，完成渗透测试，测试结果符合工作任务要求。 1.2.5 能够根据 OSI 数据链路层渗透测试工作任务要求，熟练掌握 CDP、LLDP 攻击（CDP、LLDP Attack）渗透测试的原理与方法，完成渗透测试，测试结果符合工作任务要求。
	1.3 OSI 网络层渗透测试	1.3.1 能够根据 OSI 网络层渗透测试工作任务要求，熟练掌握 ARP 攻击（ARP DOS、The man in the middle ARP）渗透测试的原理与方法，完成渗透测试，测试结果符合

工作领域	工作任务	职业技能要求
		工作任务要求。 1.3.2 能够根据 OSI 网络层渗透测试工作任务要求，熟练掌握路由协议欺骗攻击（Routing Protocol Spoofing）渗透测试的原理与方法，完成渗透测试，测试结果符合工作任务要求。 1.3.3 能够根据 OSI 网络层渗透测试工作任务要求，熟练掌握被动监听攻击（Sniffer、Dsniff Attack）渗透测试的原理与方法，完成渗透测试，测试结果符合工作任务要求。
	1.4 OSI 传输与应用层渗透测试	1.4.1 能够根据 OSI 传输与应用层渗透测试工作任务要求，熟练掌握 DNS 攻击（DNS DOS、DNS Spoofing）渗透测试的原理与方法，完成渗透测试，测试结果符合工作任务要求。 1.4.2 能够根据 OSI 传输与应用层渗透测试工作任务要求，熟练掌握 SYN Flood（SYN 泛洪）等 DOS/DDOS 渗透测试的原理与方法，完成渗透测试，测试结果符合工作任务要求。 1.4.3 能够根据 OSI 传输与应用层渗透测试工作任务要求，熟练掌握 DHCP 攻击（DHCP Starvation、 DHCP Spoofing）渗透测试的原理与方法，完成渗透测试，测

工作领域	工作任务	职业技能要求
		试结果符合工作任务要求。
2.网络安全加固	2.1 OSI 数据链路层网络安全加固	2.1.1 能够根据 OSI 数据链路层网络安全加固工作任务要求，熟练掌握端口安全（Port-Security）加固的配置，配置结果符合工作任务要求。 2.1.2 能够根据 OSI 数据链路层网络安全加固工作任务要求，熟练掌握生成树安全（Root Guard、BPDU Guard、BPDU Filtering）的配置，配置结果符合工作任务要求。 2.1.3 能够根据 OSI 数据链路层网络安全加固工作任务要求，熟练掌握本征 VLAN（Native VLAN）的配置，配置结果符合工作任务要求。 2.1.4 能够根据 OSI 数据链路层网络安全加固工作任务要求，熟练掌握 CDP、LLDP 攻击（CDP、LLDP Attack&Solution）的配置，配置结果符合工作任务要求。
	2.2 OSI 网络层网络安全加固	2.2.1 能够根据 OSI 网络层网络安全加固工作任务要求，熟练掌握 DHCP 监听（IP DHCP Snooping）的配置，配置结果符合工作任务要求。 2.2.2 能够根据 OSI 网络层网络安全加固工作任务要求，熟练掌握动态 ARP 监控（Dynamic ARP Inspect）的配置，配置结果符合工作任务要求。 2.2.3 能够根据 OSI 网络层网络安全加固工作任务要求，

工作领域	工作任务	职业技能要求
		熟练掌握路由协议强认证（Routing Protocol Strong Authentication）的配置，配置结果符合工作任务要求。
	2.3 OSI 传输与应用层网络安全加固	2.3.1 能够根据 OSI 传输与应用层网络安全加固工作任务要求，熟练掌握 URL 过滤（URL Filter）的配置，配置结果符合工作任务要求。 2.3.2 能够根据 OSI 传输与应用层网络安全加固工作任务要求，掌握 TCP 干扰（TCP Intercept）的原理及配置，配置结果符合工作任务要求。 2.3.3 能够根据 OSI 传输层与应用层网络安全加固工作任务要求，掌握 Packet Filter Firewall（包过滤防火墙）的原理及配置，配置结果符合工作任务要求。 2.3.4 能够根据 OSI 传输层与应用层网络安全加固工作任务要求，掌握 Stateful Packet Filter Firewall（基于状态的包过滤防火墙）的原理及配置，配置结果符合工作任务要求。 2.3.5 能够根据 OSI 传输层与应用层网络安全加固工作任务要求，掌握 Application Proxy Firewall（应用代理防火墙）的原理及配置，配置结果符合工作任务要求。
3. Web 安全基础配	3.1 Web 工作流程	3.1.1 能够根据 Web 工作流程分析工作任务要求，了解 Web 工作机制，准确识别 Web 服务中可能存在的安全风险。

工作领域	工作任务	职业技能要求
置	分析	3.1.2 能够根据 Web 工作流程分析工作任务要求，熟悉 HTTP 协议及 HTTP 报文，准确识别其中可能存在的安全风险。 3.1.3 能够根据 Web 工作流程分析工作任务要求，掌握 web 客户端和服务端、URI、URL、URN 等概念，准确识别其中可能存在的安全风险。
	3.2 Web 服务器渗透测试流程分析	3.2.1 能够根据 Web 服务器渗透测试流程分析工作任务要求，了解 Web 服务器渗透测试原理，准确运用技术或工具进行渗透测试。 3.2.2 能够根据 Web 服务器渗透测试流程分析工作任务要求，熟练掌握 Web 服务器漏洞扫描流程及方法，准确运用技术或工具进行漏洞扫描。 3.2.3 能够根据 Web 服务器渗透测试流程分析工作任务要求，熟练掌握 SQL 注入渗透测试流程，准确运用技术或工具进行渗透测试。 3.2.4 能够根据 Web 服务器渗透测试流程分析工作任务要求，熟练掌握命令注入渗透测试流程，准确运用技术或工具进行渗透测试。
	3.3 Web 客户端渗	3.3.1 能够根据 Web 客户端渗透测试流程分析工作任务要求，了解 Web 客户端渗透测试原理，准确运用技术或

工作领域	工作任务	职业技能要求
	透测试流程分析	工具进行渗透测试。 3.3.2 能够根据 Web 客户端渗透测试流程分析工作任务要求，熟练掌握 Web 客户端漏洞扫描流程及方法，准确运用技术或工具进行漏洞扫描。 3.3.3 能够根据 Web 客户端渗透测试流程分析工作任务要求，熟练掌握 XSS 渗透测试流程，准确运用技术或工具进行渗透测试。 3.3.4 能够根据 Web 客户端渗透测试流程分析工作任务要求，熟练掌握 CSRF 渗透测试流程，准确运用技术或工具进行渗透测试。

表 2 Web 安全测试职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1. Windows 操作系统安全加固	1.1 操作系统基础安全配置	1.1.1 能够根据操作系统基础安全配置工作任务要求，了解 Windows 服务内容及功能，准确识别安全风险。 1.1.2 能够根据操作系统基础安全配置工作任务要求，完成本地用户管理与认证授权的配置，配置结果符合工作任务要求。 1.1.3 能够根据操作系统基础安全配置工作任务要求，完成域安全和组策略的配置，配置结果符合工作任务要求。

工作领域	工作任务	职业技能要求
		1.1.4 能够根据操作系统基础安全配置工作任务要求，完成 Windows 文件安全的配置，配置结果符合工作任务要求。 1.1.5 能够根据操作系统基础安全配置工作任务要求，完成 IP 安全策略的配置，配置结果符合工作任务要求。 1.1.6 能够根据操作系统基础安全配置工作任务要求，完成远程连接安全配置，配置结果符合工作任务要求。
	1.2 操作系统服务安全配置	1.2.1 能够根据操作系统服务安全配置工作任务要求，完成 IIS 服务加固的配置,配置结果符合工作任务要求。 1.2.2 能够根据操作系统服务安全配置工作任务要求，完成系统安全检测的配置，配置结果符合工作任务要求。 1.2.3 能够根据操作系统服务安全配置工作任务要求，完成安全日志审计的配置，配置结果符合工作任务要求。
	1.3 操作系统安全策略配置	1.3.1 能够根据操作系统安全策略配置工作任务要求，完成 IP 安全策略的配置，配置结果符合工作任务要求。 1.3.2 能够根据操作系统安全策略配置工作任务要求，完成加密文件系统的配置，配置结果符合工作任务要求。

工作领域	工作任务	职业技能要求
		1.3.3 能够根据操作系统安全策略配置工作任务要求，完成数据执行保护 DEP 的配置，配置结果符合工作任务要求。
2.Linux 操作系统安全加固	2.1 操作系统基础安全分析	2.1.1 能够根据操作系统基础安全分析工作任务要求，完成系统信息扫描，准确识别安全风险。 2.1.2 能够根据操作系统基础安全分析工作任务要求，完成操作系统指纹的安全性分析，准确识别安全风险。 2.1.3 能够根据操作系统基础安全分析工作任务要求，完成弱口令的利用分析，准确识别安全风险。 2.1.4 能够根据操作系统基础安全分析工作任务要求，完成后门程序的利用分析，准确识别安全风险。
	2.2 操作系统应用安全分析	2.2.1 能够根据操作系统应用安全分析工作任务要求，完成 Web 应用安全性利用分析，准确识别安全风险。 2.2.2 能够根据操作系统应用安全分析工作任务要求，完成 MySQL 安全性利用分析，准确识别安全风险。 2.2.3 能够根据操作系统应用安全分析工作任务要求，完成缓冲区溢出利用分析，准确识别安全风险。
	2.3 操作系统安全加固	2.3.1 能根据操作系统安全加固工作任务要求，完成安全口令的配置加固，配置结果符合工作任务要求。 2.3.2 能根据操作系统安全加固工作任务要求，完成针

工作领域	工作任务	职业技能要求
		对木马入侵的安全防护加固，配置符合工作任务要求。 2.3.3 能根据操作系统安全加固工作任务要求，完成 ESP 对监听攻击的安全防护加固，配置符合工作任务要求。 2.3.4 能根据操作系统安全加固工作任务要求，完成使用 IKE 实现安全密钥交换的加固，配置符合工作任务要求。 2.3.5 能根据操作系统安全加固工作任务要求，完成使用 SSL 实现对监听攻击的安全防护加固，配置符合工作任务要求。 2.3.6 能根据操作系统安全加固工作任务要求，完成操作系统和程序中的 DEP 和 ASLR 保护机制的加固，配置符合工作任务要求。 2.3.7 能根据操作系统安全加固工作任务要求，完成 PKI（公共密钥架构）技术加固，配置符合工作任务要求。
3.Web 安全渗透测试	3.1 XSS 跨站脚本攻击渗透测试	3.1.1 能够根据 XSS 跨站脚本攻击渗透测试工作任务要求，熟练掌握 XSS 渗透测试的原理，准确识别安全风险。 3.1.2 能够根据 XSS 跨站脚本攻击渗透测试工作任务要求，掌握 XSS 分类，准确识别安全风险。

工作领域	工作任务	职业技能要求
		3.1.3 能够根据 XSS 跨站脚本攻击渗透测试工作任务要求，完成 XSS 构造和变形手工渗透测试，测试结果符合工作任务要求。 3.1.4 能够根据 XSS 跨站脚本攻击渗透测试工作任务要求，编写 Python 程序实现 XSS 漏洞渗透测试，测试结果符合工作任务要求。
	3.2 CSRF 跨站请求伪造渗透测试	3.2.1 能够根据 CSRF 跨站请求伪造渗透测试工作任务要求，掌握 CSRF 渗透的原理，准确识别安全风险。 3.2.2 能够根据 CSRF 跨站请求伪造渗透测试工作任务要求，完成 CSRF 构造手动渗透测试，测试结果符合工作任务要求。 3.2.3 能够根据 CSRF 跨站请求伪造渗透测试工作任务要求，编写 Python 程序实现 CSRF 漏洞渗透测试，测试结果符合工作任务要求。
	3.3 SQL 注入渗透测试	3.3.1 能够根据 SQL 注入渗透测试工作任务要求，熟练掌握 SQL 注入渗透测试的原理，准确识别安全风险。 3.3.2 能够根据 SQL 注入渗透测试工作任务要求，完成 SQL 注入构造和变形手工渗透测试，测试结果符合工作任务要求。 3.3.3 能够根据 SQL 注入渗透测试工作任务要求，编写

工作领域	工作任务	职业技能要求
		Python 程序实现 SQL 注入漏洞渗透测试，测试结果符合工作任务要求。
	3.4 命令注入渗透测试	3.4.1 能够根据命令注入渗透测试工作任务要求，熟练掌握命令注入渗透测试的原理，准确识别安全风险。 3.4.2 能够根据命令注入渗透测试工作任务要求，完成命令注入构造和变形手工渗透测试，测试结果符合工作任务要求。 3.4.3 能够根据命令注入渗透测试工作任务要求，编写 Python 程序实现命令注入漏洞渗透测试，测试结果符合工作任务要求。
	3.5 文件上传渗透测试	3.5.1 能够根据文件上传渗透测试工作任务要求，熟练掌握文件上传渗透测试的原理，准确识别安全风险。 3.5.2 能够根据文件上传渗透测试工作任务要求，完成文件上传构造和变形手工渗透测试，测试结果符合工作任务要求。 3.5.3 能够根据文件上传渗透测试工作任务要求，编写 Python 程序实现文件上传漏洞渗透测试，测试结果符合工作任务要求。

工作领域	工作任务	职业技能要求
	3.6 目录穿越渗透测试	3.6.1 能够根据目录穿越渗透测试工作任务要求，熟练掌握目录穿越渗透测试的原理，准确识别安全风险。 3.6.2 能够根据目录穿越渗透测试工作任务要求，完成目录穿越构造和变形手工渗透测试，测试结果符合工作任务要求。 3.6.3 能够根据目录穿越渗透测试工作任务要求，编写 Python 程序实现目录穿越漏洞渗透测试，测试结果符合工作任务要求。

表 3 Web 安全测试职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1. Web 安全漏洞开发及加固	1.1 网站脚本漏洞开发及加固	1.1.1 能够根据网站脚本漏洞开发及加固工作任务要求，完成跨站脚本（XSS：Cross Site Script）漏洞开发，开发内容符合工作任务要求。 1.1.2 能够根据网站脚本漏洞开发及加固工作任务要求，对开发的跨站脚本（XSS：Cross Site Script）漏洞进行测试，漏洞可用并符合工作任务要求。 1.1.3 能够根据网站脚本漏洞开发及加固工作任务要求，通过安全编程完成网站脚本（XSS：Cross Site Script）漏洞加固，加固结果符合工作任务要求。

工作领域	工作任务	职业技能要求
	1.2 跨站请求伪造漏洞开发及加固	1.2.1 能够根据跨站请求伪造漏洞开发及加固工作任务要求，完成跨站请求伪造（CSRF：Cross Site Request Forgeries）漏洞开发，开发内容符合工作任务要求。 1.2.2 能够根据跨站请求伪造漏洞开发及加固工作任务要求，对开发的跨站请求伪造（CSRF：Cross Site Request Forgeries）漏洞进行测试，漏洞可用并符合工作任务要求。 1.2.3 能够根据跨站请求伪造漏洞开发及加固工作任务要求，通过安全编程完成跨网站请求伪造（CSRF：Cross Site Request Forgeries）漏洞加固，加固结果符合工作任务要求。
	1.3 SQL 注入漏洞开发及加固	1.3.1 能够根据 SQL 注入漏洞开发及加固工作任务要求，完成 SQL 注入（SQL injection）漏洞开发，开发内容符合工作任务要求。 1.3.2能够根据SQL注入漏洞开发及加固工作任务要求，对开发的 SQL 注入（SQL injection）漏洞进行测试，漏洞可用并符合工作任务要求。 1.3.3 能够根据 SQL 注入漏洞开发及加固工作任务要求，通过安全编程完成 SQL 注入（SQL injection）漏洞加固，加固结果符合工作任务要求。

工作领域	工作任务	职业技能要求
	1.4 命令注入漏洞开发及加固	1.4.1 能够根据命令注入漏洞开发及加固工作任务要求，完成命令注入（Command Injection）漏洞开发，开发内容符合工作任务要求。 1.4.2 能够根据命令注入漏洞开发及加固工作任务要求，对开发的命令注入（Command Injection）漏洞进行测试，漏洞可用并符合工作任务要求。 1.4.3 能够根据命令注入漏洞开发及加固工作任务要求，通过安全编程完成命令注入（Command Injection）漏洞的加固，加固结果符合工作任务要求。
	1.5 文件上传漏洞开发及加固	1.5.1 能够根据文件上传漏洞开发及加固工作任务要求，完成文件上传（File upload）漏洞开发，开发内容符合工作任务要求。 1.5.2 能够根据文件上传漏洞开发及加固工作任务要求，对开发的文件上传（File upload）漏洞进行测试，漏洞可用并符合工作任务要求。 1.5.3 能够根据文件上传漏洞开发及加固工作任务要求，通过安全编程完成文件上传（File upload）漏洞加固，加固结果符合工作任务要求。
	1.6 目录穿越漏洞	1.6.1 能够根据目录穿越漏洞开发及加固工作任务要求，完成目录穿越（Directory traversing）漏洞开发，

工作领域	工作任务	职业技能要求
	开发及加固	开发内容符合工作任务要求。 1.6.2 能够根据目录穿越漏洞开发及加固工作任务要求，对开发的目录穿越（Directory traversing）漏洞进行测试，漏洞可用并符合工作任务要求。 1.6.3 能够根据目录穿越漏洞开发及加固工作任务要求，通过安全编程完成目录穿越（Directory traversing）漏洞加固，加固结果符合工作任务要求。
2.代码审计与逆向分析	2.1 代码审计	2.1.1 能够根据代码审计工作任务要求，掌握代码审计工具的使用，正确运用代码审计工具。 2.1.2 能够根据代码审计工作任务要求，完成对常见 Web 漏洞、系统漏洞的代码审计，准确识别代码中的安全漏洞。 2.1.3 能够根据代码审计工作任务要求，运用代码审计流程完成测试工作，测试结果符合工作任务要求。
	2.2 代码的编写安全	2.2.1 能够根据代码编写安全工作任务要求，阅读复杂代码，准确识别代码中的安全漏洞。 2.2.2 能够根据代码编写安全工作任务要求，完成基本软件漏洞分析，准确识别安全漏洞。 2.2.3 能够根据代码编写安全工作任务要求，掌握安全代码编写方法，降低代码安全风险。

工作领域	工作任务	职业技能要求
	2.3 逆向分析	2.3.1 能够根据逆向分析工作任务要求，完成 Integer/Float 数据类型逆向分析，分析结果符合工作任务要求。 2.3.2 能够根据逆向分析工作任务要求，完成 Bool/NULL 数据类型逆向分析，分析结果符合工作任务要求。 2.3.3 能够根据逆向分析工作任务要求，完成 Char/Pointer 数据类型逆向分析，分析结果符合工作任务要求。 2.3.4 能够根据逆向分析工作任务要求，完成 Array 数据类型逆向分析，分析结果符合工作任务要求。 2.3.5 能够根据逆向分析工作任务要求，完成 String 数据类型逆向分析，分析结果符合工作任务要求。 2.3.6 能够根据逆向分析工作任务要求，完成 Struct 数据类型逆向分析，分析结果符合工作任务要求。 2.3.7 能够根据逆向分析工作任务要求，完成 Function/ Procedure 逆向分析，分析结果符合工作任务要求。
3. 综合渗透测试	3.1 二进制安全（PWN）	3.1.1 能够根据二进制安全（PWN）渗透测试工作任务要求，完成栈溢出漏洞渗透测试，测试结果符合工作任

工作领域	工作任务	职业技能要求
与安全开发	渗透测试	务要求。 3.1.2 能够根据二进制安全（PWN）渗透测试工作任务要求，完成堆溢出漏洞渗透测试，测试结果符合工作任务要求。 3.1.3 能够根据二进制安全（PWN）渗透测试工作任务要求，完成针对缓冲区溢出漏洞的安全开发，开发内容符合工作任务要求。
	3.2 操作系统漏洞利用开发	3.2.1 能够根据操作系统漏洞利用开发工作任务要求，完成 Windows 操作系统 ShellCode 开发，开发内容符合工作任务要求。 3.2.2 能够根据操作系统漏洞利用开发工作任务要求，完成 Windows 操作系统 ShellCode 利用，测试结果符合工作任务要求。 3.2.3 能够根据操作系统漏洞利用开发工作任务要求，完成 Linux 操作系统 ShellCode 开发，开发内容符合工作任务要求。 3.2.4 能够根据操作系统漏洞利用开发工作任务要求，完成 Linux 操作系统 ShellCode 利用，测试结果符合工作任务要求。
	3.3 网络安	3.3.1 能够根据网络安全分析及渗透测试工作任务要

工作领域	工作任务	职业技能要求
	全分析及渗透测试	求，完成 ARP、IP、TCP\UDP 安全性分析及渗透测试，测试结果符合工作任务要求。 3.3.2 能够根据网络安全分析及渗透测试工作任务要求，完成路由协议安全性分析及渗透测试，测试结果符合工作任务要求。 3.3.3 能够根据网络安全分析及渗透测试工作任务要求，完成 IPv6 网络安全性分析及渗透测试，测试结果符合工作任务要求。

参考文献

[1] 中等职业学校专业目录（征求意见稿）

[2] 普通高等学校高等职业教育（专科）专业目录及专业简介（截至 2019 年）

[3] 普通高等学校本科专业目录

[4] 中等职业学校专业教学标准（试行）

[5] 高等职业学校专业教学标准（2019 年）

[6] 本科专业类教学质量国家标准

[7] 2019 年全国职业院校技能大赛 GZ-2019028 信息安全管理与评估赛项规程

[8] 普通高等学校高等职业教育（专科）专业目录及专业简介

[9] 国家职业技能标准编制技术规程. 2018 年版

[10] 中华人民共和国网络安全法

[11] SJ/T 11623-2016 信息技术服务从业人员能力规范

[12] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[13] GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

[14] GB/T 20270-2016 信息安全技术 网络基础安全技术要求信

[15] GB/T 20272-2019 信息安全技术 操作系统安全技术要求