工 业 和 信 息 化 部
电子工业标准化研究院培训中心

电标培〔2021〕007-2 号

关于举办《安全及渗透测试技术》暨《信息安全管理工程师》职业技术专题研讨班的通知

各有关单位：

随着我国软件产业与信息化建设的深入发展，软件安全测试技术逐渐成为软件企业生存和信息化项目建设好坏的关键，提升我国软件测试能力，已成为保障软件质量的必要手段。培养测试高级人才、提供高效、优质的软件质量测试服务是当前共同的目标。

为进一步帮助各单位相关人员深入了解软件安全测试技术及渗透测试技巧，提升各相关单位的应变能力，培养软件应用管理高级人才，提供高效、优质的系统测试方法。增强国内行政、企事业单位等在软件测试方面的基础能力，从源头上减少系统运行可能存在的各种问题。工业和信息化部电子工业标准化研究院培训中心定于 1 月中旬线上举办“安全及渗透测试技术”专题研讨班。研讨结束后，可参加考核，合格者由工业和信息化部教育与考试中心颁发《信息安全管理工程师》职业技术证书。

一、培训内容

软件开发安全测试概述

1. 常用应用开发基础知识（包括 HTTP 协议、SSL 协议等内容）
2. 开发应用安全测试基础（安全测试、渗透测试，渗透测试分，代码审计，安全架构设计类等内容）
3. 安全测试方法（开放式 Web 应用程序安全项目（OWASP）、Web 应用安全联合威胁分类（WASC-TC）、渗透执行测试标准（PTES）、通用渗透测试执行框架（Kali linux）等）
4. 渗透测试过程及主要关注的问题

5. 常用的工具介绍（包括：nmap、Sqlmap、Nessus、Appscan、Metasploit、Burp Suite、Aircrack-ng、wireshark\fiddler、Checkstyle,FindBugs,PMD,FindSecurityBugs,fortify等）

渗透测试环境搭建与工具使用

1. Kali Linux 安装与配置
2. DVWA 网站测试靶机搭建
3. Metasploit 渗透测试环境搭建
4. Nmap 网络映射工具安装与使用
5. Sqlmap 安装与配置
6. Nessus 扫描工具安装与使用
7. Appscan 安装与配置
8. Burp Suite 安装与配置

信息的收集及利用

1. AppScan 扫描测试（首先利用 AppScan 对 Web 应用和服务器进行全面扫描，发现部分漏洞和问题）
2. 代码审计（使用 Checkstyle 进行缺陷模式匹配、FindBugs 缺陷模式匹配及数据流分析、使用 PMD 缺陷模式匹配，FindSecurityBugs，fortify）
3. 信息收集（使用 Nmap、Recon-NG 等工具收集 Web 应用、服务器、网络的信息，包括：运行账号权限测试、服务端口扫描、HTTP 方法测试、网络范围测试、服务器其他信息收集等）
4. 使用 Nessus/OpenVAS 进行漏洞扫描（包括：扫描本地漏洞、网络漏洞、扫描指定 Linux 的系统漏洞、扫描指定 Windows 的系统漏洞等内容）
5. 使用 Metasploit 发起渗透攻击（包括：对操作系统的攻击、对 Web 应用程序攻击、对 mysql 数据库的攻击等）

各种渗透测试

1. 权限管理测试（包括横向越权测试、纵向越权测试、使用 kali 社会工程学工具包实施测试等）
2. 文件、目录测试（包括目录列表测试、文件归档测试等）

3. 身份认证测试（包括：使用 Burp Suite 对网络认证服务的攻击、哈希密码破解、密码字典破解等内容）

4. 会话管理测试（包括：身份信息维护方式测试、Cookie 存储方式测试、用户注销登录方式测试、注销时会话信息是否清除测试、会话超时测试等）

5. 文件上传、下载测试（包括文件上传测试、下载测试等内容）

6. 信息泄露测试（借助 wireshark\fiddler 等工具嗅探敏感数据是否泄露）

7. SQL 注入测试（包括：手动 SQL 注入和借助 Sqlmap 工具注入等内容）

8. XSS 攻击（包括：XSS 漏洞、存储型 XSS、DOM 型 XSS、BeFF-XSS 渗透测试框架、BeFF-XSS 与 Metasploit 协同工作等内容）

9. CSRF 攻击（包括：CSRF 漏洞、利用条件、检测方法和对策等内容）

10. WebShell（包括：WebShell 介绍、检测方法及对策）

11. 无线安全渗透测试（包括无线网络嗅探、使用 Aircrack-NG 工具破解无线网络、使用 Arpspoof 实施 arp 攻击等）

12. 其他渗透测试（包括：逻辑测试，html5 安全测试，日志审计，class 文件反编译测试，Struts2 框架测试等）

软件源代码安全审查

1. 密码管理（包括各种常用的加密方式的审查）

2. 跨站脚本（利用 http 协议的特点，跨站脚本的可能攻击漏洞）

3. 资源管理（数据权限，功能权限的审查）

4. 配置管理（session，错误页面）

5. 检测工具使用（使用 Checkstyle 进行缺陷模式匹配、FindBugs 缺陷模式匹配及数据流分析、使用 PMD 缺陷模式匹配，FindSecurityBugs，fortify）

6. 代码质量的审查

漏洞实战专题

常见测试系统的搭建，以 DVWA 等为例案例分析，结合上述工具的整体使用，结合具体的案例讲述如何进行安全测试；

二、时间地点

线上集中学习时间：2021 年 1 月 16 日- 17 日

（注：线下考试地点—北京、上海、深圳，时间另行通知）

三、参加对象

大型软件用户单位信息中心技术主管或分管领导,软件需求方技术负责人或主管领导,软件升级项目负责人、技术主管等；软件开发企业技术主管、项目经理、测试经理等；其他对软件性能设计与测评感兴趣人员。从事质量管理相关工作人员；项目经理；分析人员、设计人员、开发人员和测试人员等软件工程师；外包管理工作人员；企业项目管理部门工作人员。

四、证书颁发

考试合格者，由工业和信息化部教育与考试中心统一颁发《信息安全管理工程师》职业技术证书。

五、学习费用

培训费：3600 元/人，（含师资、教材资料费、证书费等）。

六、报名须知

请参加研讨的学员认真填写报名回执表，以电话、传真及邮件的方式反馈至我中心。此次培训会务工作将由北京中标服检验技术研究院有限公司具体承办。

联系电话：010-68699678　64102658

联 系 人：胡恩萍　张筱悠

联系邮箱：weicheng200409@126.com

工业和信息化部电子工业标准化研究院

培训中心

2020年12月11日

附件2：报名回执表

“安全及渗透测试”专题研讨班报名回执表

单位名称（开票名称）					
通信地址					
培训联系人		电话		传真	
电子邮箱			联系人手机		
学员姓名	职务	是否食宿	手机	邮箱地址	

会务联系人：胡恩萍 13671317228（微信同号）　　报名邮箱：weicheng200409@126.com