

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〕033号

关于举办《安全、渗透测试技术及实操应用》暨《高级信息安全管理工程师》职业技术网络专题研讨班的通知

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4月下旬线上举办《安全、渗透测试技术及实操演练》暨《高级信息安全管理工程师》职业技术网络专题研讨班。学习结束后，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《高级信息安全管理工程师》职业技术证书，并将学员信息录入工业和信息化技术人才数据库。

一、培训内容

信息安全测试基础应用

1、网络安全

- A、TCP/IP、OSI 网络体系结构；
- B、常见网络安全攻击原理及攻击演示（ARP 攻击、DDos 攻击等）

2、信息安全保障基础

- | | |
|-------------|----------------|
| A、信息安全定义 | B、信息安全问题的根源及特征 |
| C、威胁情报与态势感知 | D、信息安全的关键要素 |

- E、信息安全的视角
- F、工业控制系统基本架构、安全威胁、安全架构等

3、密码及应用技术基础

- | | |
|-----------|------------------------|
| A、保密通信模型； | B、对称密码体制和非对称密码体制； |
| C、哈希加密； | D、国密算法（SM2、SM3 和 SM4）； |
| E、消息认证； | F、数字签名 |

4、安全的软件开发生命周期

- | | |
|----------------|-----------|
| A、安全原则、规则及规章 | B、安全需求 |
| C、架构、设计评审和威胁建模 | D、安全的编码规则 |
| E、软件测试 | F、判定可用性 |

5、信息安全管理体制

- | | |
|----------------|------------------|
| A、信息安全管理体制控制类型 | B、信息安全管理体制控制措施结构 |
|----------------|------------------|

6、配置管理与风险分析

- | | |
|---------------|------------|
| A、系统安全配置基础 | B、安全配置核查方法 |
| C、安全风险分析与评估方法 | |

安全测试技术

1、软件安全测试概念、目的

- | | |
|------------|------------|
| A、软件安全测试定义 | B、软件安全测试目的 |
| C、安全测试相关概念 | |

2、软件安全测试方法分类

- | | |
|----------------------------------|--------------|
| A、按照不同视角分类（基于安全需求的测试，基于攻击者的渗透测试） | |
| B、按照执行方式分类 | C、根据渗透测试方法分类 |
| D、根据攻击目标分类 | E、模糊测试 |

3、代码审计

- | | |
|------------|-----------------|
| A、代码审计概念 | B、正向代码审计和逆向代码审计 |
| C、代码审计常用工具 | |

渗透测试技术

1、渗透测试的流程

- | | |
|-------------|-------------|
| A、明确目标 | B、分析风险并获得授权 |
| C、信息收集 | D、漏洞扫描及验证 |
| E、漏洞利用及信息整理 | F、系统状态恢复 |

G、测试评估和总结

2、信息收集方法及运用

A、识别主机

B、查看打开端口

C、系统指纹识别

D、服务指纹识别

3、威胁建模方法

A、确定对象

B、识别威胁

C、评估威胁

D、削减威胁

4、漏洞扫描及分析

5、漏洞利用

安全渗透技术演练

1、常见的软件安全漏洞原理、攻击方法及应对措施

2、工控系统常见威胁、攻防对抗技术以及示例

3、无线攻防技术实战（无线网 wifi 攻击）

4、C 内存泄漏安全分析

5、Html5 安全

6、代码审计 shiro 反序列化攻击

安全测试工具与环境建设

1、常用的渗透测试工具介绍

A、Appscan

B、Burpsuite

C、Sqlmap

D、Wireshark

E、Kali 工具集

2、测试环境、测试工具、测试靶机的安装与部署；

3、渗透测试实践（按照实验大纲，完成常见漏洞的攻防演练）

二、时间地点

线上集中学习时间：2021 年 5 月 8 日-9 日 （腾讯课堂）

（注：考试采用远程视频监控模式进行，使用软件：腾讯会议）

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《高级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

2021年3月20日

培训中心