

课程大纲

壹、 培训背景：

习总书记在自主创新推进网络强国建设的重要指示中提到：“没有网络安全就没有国家安全，就没有经济社会稳定运行。要研究制定网信领域人才发展整体规划，推动人才发展体制机制改革，让人才的创造活力竞相迸发、聪明才智充分涌流”。我劝天公重抖擞，不拘一格降人才。正是因为习总书记要求广大领导干部要具备这样识才的慧眼、用才的胆识、容才的雅量，我国的人才工作才能不断开创新局面。因此网络安全领域人才培养工作要牢记“不断增强‘四个意识’，坚持把党的政治建设摆在首位，加大力度建好队伍、全面从严管好队伍，选好配好各级网信领导干部，为网信事业发展提供坚强的组织和队伍保障”。

在中国移动 2021 年工作会议中，杨杰董事长提出要加快网络安全保障体系和能力建设，提高网络安全管理水平，严格做好电话卡、物联网卡入网管理，加大个人信息保护力度，深化内容安全集中治理，切实保障通信与网络信息安全。董昕总经理提出要加快 5G 精品网络建设，网络安全条线要推动网络安全研发运营一体化，增强 5G 网络内生安全能力，构建安全态势感知和防护处置能力。

贰、 培训需求：

随着网络信息技术的不断发展，人类已经迎来了万物互联的数字化时代，随之而来的网络安全问题频频发生，全球银行集体遭到大规模攻击、黑客利用人工智能等新技术手段辅助攻击企业等等这些迹象，都给我们敲响了新一轮的安全警钟。日益成熟的互联网意味着更多攻击。通过对主流网络空间安全攻防对抗技术的讲解，帮助网络安全人员更好地梳理 web、数据、软件和应用安全知识点，为进一步开展网络安全工作打好扎实基础。

参、 培训内容架构与设计思路：

(1) 培训内容架构：

作为入门安全人才培养的基础课程，课程架构清晰，着技术性员工的技能培养的全面性与专业性并贴合中移网络安全业务需求的变化发展作为驱动，方案以落地诉求作为出发点。形成安全转型必备知识内容的基本组合。围绕以下五点展开：

- Web 安全防护
- 代码审计
- 信息数据隐写法
- 数据加密与身份验证技术

(2) 设计思路：

本课程采用以学员具备的安全基本感知为切入点的方式，帮助学员找到更适合自己的安全学习和技能提升的过渡方式，掌握相应安全技术。故设计方法为以难易交叉的方式，先是大家最熟悉的简单 web 及背后安全问题分析，后从相对较难的开发视角及背后的审计和漏洞挖掘进行分析，然后又对大家容易理解隐写应用及背后隐写技术进行介绍、以及日常使用的加密技术介绍，最后讨论逆向工程，对学员提出更深层次的技术要求。

四、 培训对象：

网络空间安全人员。

伍、 培训时间及安排：共 1 期，1 天/期，6 小时/天

授课时间		授课内容	授课时长
第一天	上午	1. Web 安全防护 2. 信息数据隐写法	3 小时
	下午	3. 数据加密与 4. 软件的逆向工程	3 小时

六、 课程详细大纲：

1. **Web 安全防护**
 - 1.1 Web 安全简史
 - 1.2 浏览器安全
 - 1.3 跨站脚本攻击 (XSS)
 - 1.4 跨站点请求伪造 (CSRF)
 - 1.5 点击劫持
 - 1.6 SQL 注入
 - 1.7 Web 木马的原理
 - 1.8 文件包含攻击

2. **信息数据隐写法**
 - 2.1 信息隐藏方式
 - 2.1.1 数字水印版权保护
 - 2.1.2 隐蔽通信
 - 2.2 隐写法介绍
 - 2.2.1 Exif 照片隐写
 - 2.2.2 JPEG 图像的数字隐写流程
 - 2.2.3 LSB 插入隐写及改进
 - 2.2.4 F5 隐写算法

3. **数据加密与身份验证技术**
 - 3.1 古典密码与破解
 - 3.2 分组模式与相关攻击
 - 3.3 公钥密码体制

4. **软件的逆向工程**
 - 4.1 正向开发与逆向分析
 - 4.2 程序的保护机制

4.3 PWN 基本工具和常见利用方法

4.4 安卓基本架构和 ARM 架构知识

4.5 Dalvik 层逆向分析概念

5. 课程总结：

(1) 重点知识回顾与总结；

(2) 互动与讨论：问与答。

就学员提出的问题进行分析、讨论和点评。

七、 培训方式/工具及方法

培训方式及方法：

本课程采用模块化教学方法，通过理论讲授，案例分析，方法传授、动画演示、互动讨论，讲师点评、项目展示等多种教学手段与方法，达到学以致用、了解和认识安全问题的目的。

培训工具：PPT 讲义、项目案例演示、投影仪、白板、白纸、彩笔、音响设备、话筒等。

评估方法：（1）学员学习成果（项目解决方案）评估；（2）学员打分评估。