2017 年网络与信息安全攻防技能提升班（第五期）

日程安排

第一天:

一、渗透测试基础

渗透测试概念、流程、思路、行业内的术语解释，主要讲解关于渗透的流程、Google Hacking 常见 Web 扫描和端口扫描工具的使用等；讲解暴力破解的方法、场景、使用的工具、针对常见服务如 SSH、FTP、MySQL 等破解案例以及防范方法。

二、SQL 注入攻击与防御

主要讲解 ASP+Access、ASPX+Mssql、Php+Mysql、JSP+Oracle 等手工注入常用语句、语法结构、练习和实践；以及常见应用场景下的 SQL 注入攻击，如：获取数据库信息、获取 Webshell、提权等等；着重讲解针对不同数据库的 SQL 注入漏洞中的各种防御手段，如使用参数化语句、输入输出验证、使用存储过程等。

第二天:

一、XSS 攻击与防护

主要讲解 XSS 基本原理、各种类型的 XSS；如何挖掘 XSS 漏洞、XSS Worm 攻击、各种 XSS 漏洞的利用、深入理解 XSS 漏洞的形成，以及如何防御 XSS 漏洞；着重讲解针对 XSS 漏洞的防护方式，如：使用 XSS Filter 等。

二、文件上传攻击与防护

主要讲解文件文件上传漏洞、文件解析漏洞、编辑器漏洞等漏洞的利用方法；以及关于文件上传的利用方法，掌握相关的上传截断工具进行上传突破；着重讲解针对文件上传漏洞的防护手段,从代码层和服务器层进行讲解，主要四针对上传的文件进行后缀名判断，文件类型判断，并且利用 time()函数进行时间重写、安装第三方防护软件、文件上传目录禁止脚本解析等。

第三天:

一、漏洞综合利用与防护

回顾近几年信息安全大事件，更深层次的认识 Hacking Team 泄露、个人隐私信息泄露等安全事件的影响；通过实操环境练习，掌握 Redis 未授权访问、Java 反序列化、Git 泄露等漏洞的利用方式，并深入了解其产生的原理；着重讲解针对这些漏洞的具体防护方式。

二、提权攻击与防护

主要讲解在 web 端常见的提升权限的方法，包含文件上传漏洞的原理以及利用、代码执行漏洞的成因以及利用、常见 cms 和中间件的权限提升、其他第三方软件的 web 端权限提升；讲解常见的导致服务器权限提升的方法，包含权限配置不当导致的权限提升；最新 windows 以及 linux 系统中的溢出漏洞、第三方软件和常见数据库导致的权限提升；在安装防护软件情况下的权限提升；常见的无法提权的情况；着重讲解针对提权漏洞具体的防护措施和常见思路。