视频目录

第 1 章 视频

视频主要包括了以下几部分内容：
（1）什么是代码审计
（2）代码审计的背景及意义
（3）Java代码审计所需基础
（4）代码审计的常用思路（思路包括了接口排查、危险方法溯源、功能点定向审计、第三方组件与中间件版本比对、补丁比对、黑盒测试”+“白盒测试”、“代码静态扫描工具”+“人工研判”、开发框架安全审计）

链接:https://pan.baidu.com/s/10H9aQXClq8bZigmEU5RJIQ

密码:geak

第 2 章 视频

第二章主要介绍了Docker容器的使用，借助Vulhub快速启动漏洞环境，以及使用IDEA进行远程调试与项目构建。

链接:https://pan.baidu.com/s/1iGCk1CpIVVb-G2X1COVu5w

提取码：4u6z

第 3 章 没有视频

目前网上已有很多优秀的资料介绍了本章节的一些工具，故此不做视频介绍。
此处列了一些工具使用技巧的资料清单，各位可按需自取。

- IDEA技巧
  包括了安装、插件、快捷键和技巧，以及Git、SVN的一些知识。
  https://github.com/xiaoxiunique/awesome-IntelliJ-IDEA
- sublime快捷键技巧
  https://www.zhihu.com/question/289632274/answer/467362688
- Burpsuite使用技巧
  各种插件与教程。
  https://github.com/TWXsuperman/BurpSuite-collections/
- Java反编译工具 【掘金社区-杜春霞】
  JD Core、JD-GUI和JD Eclipse
  https://juejin.cn/post/6844904128057966605
- Java反编译技巧【凌天实验室】
  https://mp.weixin.qq.com/s?src=11×tamp=1611662146&ver=2852&signature=7HWsNRyDN6jliNKX-YwSjxMaG07jTBPqHqt-5TUSFh37hXGwhNRbuM2sKAsWea4EsIJpCcQdLc1CM3sWsUSQBKlfK62m28bEgrYdHq7vAGo7NI7myJEv5H3nMPDmAHOu&new=1
- 源代码比对工具 【博客园-Java技术栈】
  https://www.cnblogs.com/javastack/p/13083681.html
- diff工具
  可查看github里任意一个项目文件的的历史记录

https://wx.zsxq.com/dweb2/index/group/88855284584552#:~:text=GitHub%20-%20pomber/git-history%3A%20Quickly%20browse%20the%20hi...

第 4 章 视频

第一节课：

主要是Java 代码审计所要知道的一些简单的 Java 语法知识罗列，还有MVC 框架的演变过程，最后是一些总结和代码审计学习的建议。

链接:https://pan.baidu.com/s/1jD-6oIJt04KhQ3k_tRsYOA

密码: wma9

第二节课：

主要是讲述 Java Servlet的核心知识点，包括 servlet 的配置、servlet 的流程、servlet 的接口以及 servlet 的生命周期等，主要针对对 servlet 不太了解或者了解不多的学员。

链接: https://pan.baidu.com/s/1yKcyZum_XHkUIgY9Ia_8bw

密码: r86k

第三节课：

主要是讲述 Java Filter的核心知识点，包括 Filter 的配置、Filter 的流程、Filter 的接口以及 Filter 的生命周期、Filter 和 Servlet 的总结等，主要针对对 Filter 不太了解或者了解不多的学员。

注：在本节课中，最后演示的代码文件夹名称为Filter_Life_Demo，AccessControl 文件夹为 Filter 项目的简单示例代码，大家可以自己搭建看看，了解其原理和流程。

链接:https://pan.baidu.com/s/1H6s8zlrhY5XLTAjnb8bdFA

密码: khaf

第四节课：

主要是讲述 Java 反射机制的核心知识点，包括获取类、获取类的名称、获取类中的方法、实例化对象、调用实例对象等，主要针对对 Java 反射机制 不太了解或者了解不多的学员。 本节课同样是基础知识课程，基础比较好的同学可以等待后续漏洞讲解课程。

注：在本节课中，演示的代码文件夹名称为reflection，大家可以自己搭建并运行看看，了解反射原理和流程，弄清楚什么是不安全的反射，知道不安全的反射大概是一个什么样子的。

链接:https://pan.baidu.com/s/1eAo5Dv2u87_9Ibd0kH1lUg

密码: ohfu

第五节课：

主要是讲述的是类加载的过程、类加载器的种类、双亲委托机制、用户自定义类、加载恶意类、静态代理、动态代理、CGLib 代理、Javassist 动态编程以及 Java 安全开发框架的简单介绍等，主要针对这些内容不太了解或者了解不多的学员。
本节课是基础课程的最后一课，下节课开始我们讲解 Java 漏洞的相关知识

注：在本节课中，有三个演示代码的文件夹，分别是 loadClass——讲解的类加载的示例代码，dtProxy——讲解的动态代理的相关代码，javassist——讲解的 javassist 相关的示例代码，大家可以自行运行一遍加深理解。

链接:https://pan.baidu.com/s/1e_sdkiJRrhJlh8bqwM9XhA

密码: pifw

第 5 章 视频

第一节课：

本节介绍了Java中SQL注入的原理。配套的示例代码也一并打包了。各位在使用的时候将数据库连接信息按照实际修改即可。

链接：https://pan.baidu.com/s/1rlvXqvJCOyC9zcJPWHdd5Q

提取码：6f9b

第二节课：

这里主要介绍了注入的剩余部分（命令注入、代码注入、表达式注入和模板注入）。相关的运行代码和简要的笔记文件统一打包了，还附带一份俊杰师傅整理的ofcms模板注入漏洞的一份分析文档。

链接：https://pan.baidu.com/s/1Nb0d4X9LeU9fe_kcojzL3g

提取码：rpla

第三节课：

主要内容主要包括了：
（1）漏洞简介
（2）Webgoat8 JWT Token猜解实验
（3）其他攻击案例
（4）防御方式

注：WebGoat是OWASP组织研制出的用于进行WEB漏洞实验的Java靶场程序，用来说明web应用中存在的安全漏洞。我们可以借助这只“替罪羊”来学习代码审计。

链接：待补充

提取码：待补充

第四节课：

这次课程的主要内容包括了以下几个部分：
（1）漏洞简介
（2）TurboMail 5.2.0敏感信息泄露漏洞审计实战
（3）其他攻击案例
（4）防御方式

链接：https://pan.baidu.com/s/1m7ZvmoSX9A1GUcASSaFvbg

提取码：kpqf

第五节课：

本次课堂的大纲如下：
0x01 漏洞简介
0x02 实验探究：读取系统文件（以OpenRASP的testcase为例）
0x03 修复案例：禁用外部实体引用（以OpenRASP的testcase为例）
0x04 笔者的一次代码审计经历（org.jpmml 1.4.4是否受XXE漏洞影响）
0x05 小结
0x06 参考资料

在这次的课堂中还穿插了一点点little tricks，比如：
（1）使用CVE漏洞的搜索平台：http://cve.circl.lu/
（2）使用文本比对工具：BeyondCompare
（3）分析开源项目的补丁

链接：https://pan.baidu.com/s/1eJZpit-tsQ4fhC6rIRbjZA

提取码：jv98

第六节课：

本次课堂的大纲如下：
0x01 漏洞简介
0x02 横向越权实验探究（因酷网校在线教育系统的一处越权漏洞）
0x03 纵向越权实验探究（某租车系统演示网站的一处越权漏洞）
0x04 小结
0x05 参考资料

链接：https://pan.baidu.com/s/1pcZvOwP07XPkom3WQDpsVA

提取码：x7gm

第七节课：

本次课堂的大纲如下：
0x01 漏洞简介
0x02 反射型XSS
0x03 存储型XSS
0x04 DOM型XSS
0x05 修复建议
0x06 XSS模糊测试工具XSStrike
0x07 小结
0x08 参考资料

链接：https://pan.baidu.com/s/19gz6tU7CsRmQyvLTqBD7Dw

提取码: ffry

第八节课：

Tomcat 任意文件写入漏洞原理分析
Tomcat AJP文件包含漏洞原理分析

链接：https://pan.baidu.com/s/1Hq9r9AOHfp_GUPV2XGROrA

密码:bkae

第九节课：

本小节介绍了基本的序列化和反序列化知识，以及JDK序列化字节流的格式和漏洞产生的必要条件。

链接：https://pan.baidu.com/s/1bFfQyL_yqxNkYPxQmMDdtw

提取码：ap4h

第十节课：

本节简单介绍和演示了RMI和JNDI利用方式，以及简单介绍了Apache Commons Collections反序列化漏洞漏洞。

链接：https://pan.baidu.com/s/1dEy-elQFQjPndqRbIldFLA

提取码：rfzs

第十一节课：

待补充

第6章 视频

第一节课：

在本节课中主要讲了第六章的时间安排、具体的更新时间，CSRF 漏洞的原理、实例、防御方式以及实际中的一些 tips ，希望大家有所收获

链接: https://pan.baidu.com/s/1bqeQSjwxgawWziLWhJTKAQ

密码: s3jp

第二节课：

主要介绍了 SSRF 漏洞的原理、实际案例、修复方法以及一些 TIPS 等等，希望大家有所收获

链接: https://pan.baidu.com/s/19TI0LSCdn31nIyABXUY35A

密码: wi7s

第三节课：

主要对 URL 跳转漏洞进行了讲解，买书的朋友可以参考书籍，对着学和理解，这个漏洞还是比较简单的，更深入的利用还是要看业务场景，更深入的审计也是要根据具体的功能来看

链接: https://pan.baidu.com/s/1ViNw9ZrbeivnXZwODRzFJw

提取码:y4w6

第四节课：

在这一章主要讲述了文件包含、文件上传、文件读取、文件下载、文件写入、文件解压等与文件操作相关的漏洞，希望大家有所收获！

链接:https://pan.baidu.com/s/1wUhYxAIAzgoLvn92vIWrpQ

密码: 77ck

第五节课：

主要讲了后门的一些分类，经典示例，与代码审计之间的关系，如何通过人工的方式审计后门、编写后门等，知彼知己，百战不殆。

链接:https://pan.baidu.com/s/1LJ7kfR8Oen7KudlvSAXSwg

密码: 3n3e

第六节课：

这一节 PPT 内容较少，说的内容比较多，大家可以多听几遍，其实逻辑漏洞的关键点在于对业务场景的具体理解，技术本身反而不是那么难，希望大家有所收获

链接:https://pan.baidu.com/s/1asS1EHxat0HB7GUncj6w0g

密码: hqhm

第七节课：

这节课主要说了 SOP、CORS、CSP 的相关概念和小示例，还有在审计代码的时候需要注意事情，比如大多数人可能会忽略常量的审计，CORS、CSP 配置问题还是比较常见的，本节课说的只是这两个知识点的小内容，更多的内容还是需要大家课后去搜索学习，希望本节课能够对大家有所帮助！

链接：https://pan.baidu.com/s/1IjSIBeUYcZTnhH0uFlEXxg

密码: fr8q

第八节课

这一节课主要说了一些拒绝服务漏洞相关的知识点，比如 ReDos、解压导致的拒绝服务攻击等，还介绍了由反序列化漏洞导致的拒绝服务攻击的内容，其中主要说了 NFA和 DFA 相关的知识点和实例，希望本节课对大家有所帮助！

链接：https://pan.baidu.com/s/1Wh8W8eK0ryhQp3sFLKuVkA

密码: aso3

第九节课：

点击劫持漏洞精讲，这个漏洞比较简单，因此简单讲解了下漏洞的原理和示例，大家理解下漏洞就行，写报告的时候可以作为一个测试项加上去

链接: https://pan.baidu.com/s/12TtVc9JLYcM3MSXCZlr3Qg
密码: 6ol9

第十节课：

这是第六章的最后一节课，由于第九节比较简单，所以我两节课一起录了发出来，在这节课里我后面提了一下由异构导致的相关漏洞，这个漏洞实际上是由 HPP 漏洞定义的引申，在大厂中和 SRC 中出现的频率还是比较高的。另外我也简单说了下对安全研究或者漏洞挖掘的看法，希望大家在理解漏洞的原理的时候，更多的去发散自己的思想，看看能不能拓展引申新的安全风险或漏洞，希望对大家有所帮助！

链接: https://pan.baidu.com/s/1KbiMNHVN44qbMUMmZAVnTw

密码: 6817