

java代码审计 深度解析



第一课 文件下载漏洞源码分析

免责声明
DISCLAIMER

本课程仅限于学习交流，请严格遵守国家法律法规！如利用技术从事违法活动，后果自负！



下载漏洞原理

任意文件下载漏洞，正常的利用手段是下载服务器文件，如脚本代码，服务器配置或者是系统配置等等。但是有的时候我们可能根本不知道网站所处的环境，以及网站的路径，这时候我们只能利用../来逐层猜测路径，让漏洞利用变得繁琐。



找下载功能的代码

IOException

OutputStream



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered throughout, suggesting themes of cybersecurity or digital privacy. The overall aesthetic is futuristic and high-tech.

谢谢观赏