



渗透测试工程师技术实战课

渗透工具篇渗透工具篇3 第1-4课

教学目标

★ 能够掌握Burpsuite工具得使用



赛博梦工厂
Cyber Works

★ 什么是BurpSuite

- BurpSuite是用于攻击Web应用程序的集成平台。它包含了许多Burp工具，这些不同的burp工具通过协同工作，有效的分享信息，支持以某种工具中的信息为基础供另一种工具使用的方式发起攻击。它主要用来做安全性渗透测试



Burpsuite基础

- Burp Suite 安装和环境配置
- Burp Suite代理和浏览器设置
- SSL和Proxy高级选项
- Burpsuite-intruder/Target
- Burpsuite-repeater, Sequencer, 编码, 代理截断工具
- Burpsuite-Scanner,Spider



● Burpsuite安装与环境配置

● install JAVA JDK

- <https://download.oracle.com/otn/java/jdk/8u231-b11/5b13a193868b4bf28bcb45c792fce896/jdk-8u231-linux-i586.tar.gz>
- 修改环境变量
- java-version
- 激活
- 删除/创建脚本burpsuite/修改桌面图标



- 浏览器代理设置
- 数据拦截与控制
 - Forward、Drop、Interception is on/off、Action
 - Comment 以及Highlight
- 历史记录History
- 可选项配置Options
 - 客户端请求消息拦截
 - 服务器端返回消息拦截
 - 服务器返回消息修改
 - 正则表达式配置
 - 其他配置项



● Burpsuite SSL和Proxy高级选项

- CA证书的安装
 - PortSwigger CA证书
- CA证书的卸载
- Proxy监听
 - Invisible(主机头/多目标域名)
 - CA(导入/导出)
- 隐形代理设置



● Burpsuite Target

- 目标域设置Target Scope

- 站点地图Site Map

- Target工具的使用

- > 手工获取站点地图

- > 站点比较

- > 攻击面分析



● Burpsuite Spider

- Spider控制(Control)
- Spider可选项设置(Options)
 - > 抓取设置
 - > 抓取代理设置
 - > 表单提交设置
 - > 应用登陆设置
 - > 蜘蛛引擎设置
 - > 请求消息头设置



●Burpsuite Scanner

Burp Scanner基本使用步骤

- Burp Scanner扫描方式

 - > 主动扫描

 - > 被动扫描

- Burp Scanner扫描控制

- Burp Scanner可选项设置



● Burpsuite Intruder

- Intruder使用场景
 - 标识符枚举
 - 提取有用的数据
 - 模糊测试
- Payload 位置和攻击类型
- Payload类型与处理



● Burpsuite Repeater、Sequencer、Decoder、Comparer

- Repeater的使用
 - change request method
 - change body encoding
 - copy as curl command
- Sequencer
 - 用于检测数据样本随机性质量的工具
 - Analyz（数据越多分析越准确）
 - 伪随机数算法
- Decoder
 - 使用各种编码绕过服务器端输入过滤
 - smart decode
- Comparer



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 concern. 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, symbolizing security or digital threats. The overall aesthetic is high-tech and futuristic.

谢谢观赏