

.....  
**基础入门-抓包&封包&协议&APP&小程序&PC 应用&WEB 应用**  
.....



#知识点:

- 1、抓包技术应用意义
- 2、抓包技术应用对象
- 3、抓包技术应用协议
- 4、抓包技术应用支持
- 5、封包技术应用意义

总结点: 学会不同对象采用不同抓包封包抓取技术分析

基于网络接口抓包-网络接口

基于程序进程抓包-程序进程

基于数据协议抓包-HTTP/S&TCP&UDP

基于应用对象抓包-APP&小程序&PC\_UI

基于系统使用抓包-模拟器&WIN&LINUX

基于应用对象封包-WPE 动作数据包重放通讯

#参考点:

**Fiddler:**

是一个 **http** 协议调试代理工具, 它能够记录并检查所有你的电脑和互联网之间的 **http** 通讯, 设置断点, 查看所有的“进出”Fiddler 的数据 (指 **cookie**, **html**, **js**, **css** 等文件)。Fiddler 要比其他的网络调试器要更加简单, 因为它不仅仅暴露 **http** 通讯还提供了一个用户友好的格式。

**Charles:**

是一个 **HTTP** 代理服务器, **HTTP** 监视器, 反转代理服务器, 当浏览器连接 Charles 的代理访问互联网时, Charles 可以监控浏览器发送和接收的所有数据。它允许一个开发者查看所有连接互联网的 **HTTP** 通信, 这些包括 **request**, **response** 和 **HTTP headers** (包含 **cookies** 与 **caching** 信息)。

**TCPDump:** 是可以将网络中传送的数据包完全截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤, 并提供 **and**、**or**、**not** 等逻辑语句来帮助你去掉无用的信息。

**BurpSuite:** 是用于攻击 **web** 应用程序的集成平台, 包含了许多工具。Burp Suite 为这些工具设计了许多接口, 以加快攻击应用程序的过程。所有工具都共享一个请求, 并能处理对应的 **HTTP** 消息、持久性、认证、代理、日志、警报。

**Wireshark:** 是一个网络封包分析软件。网络封包分析软件的功能是截取网络封包, 并尽可能显示出最为详细的网络封包资料。Wireshark 使用 **WinPCAP** 作为接口, 直接与网卡进行数据报文交换。

**科来网络分析系统:** 是一款由科来软件全自主研发, 并拥有全部知识产品的网络分析产品。该系统具有行业领先的专家分析技术, 通过捕获并分析网络中传输的底层数据包, 对网络故障、网络安全以及网络性能进行全面分析, 从而快速排查网络中出现或潜在的故障、安全及性能问题。

**WPE&封包分析:** 是强大的网络封包编辑器, **wpe** 可以截取网络上的信息, 修改封包数据, 是外挂制作的常用工具。一般在安全测试中可用来调试数据通讯地址。

---

## 演示案例：

- WEB 应用站点操作数据抓包-浏览器审查查看元素网络监听
- APP&小程序&PC 抓包 HTTP/S 数据-Charles&Fiddler&Burpsuite
- 程序进程&网络接口&其他协议抓包-WireShark&科来网络分析系统
- 通讯类应用封包分析发送接收-WPE 四件套封包&科来网络分析系统

#环境配置：

1、安卓模拟器安装搭建

逍遥，雷电，夜神等自行百度下载安装

2、工具相关证书安装指南

Charles

[https://blog.csdn.net/weixin\\_45459427/article/details/108393878](https://blog.csdn.net/weixin_45459427/article/details/108393878)

Fiddler

[https://blog.csdn.net/weixin\\_45043349/article/details/120088449](https://blog.csdn.net/weixin_45043349/article/details/120088449)

BurpSuite

[https://blog.csdn.net/qq\\_36658099/article/details/81487491](https://blog.csdn.net/qq_36658099/article/details/81487491)

3、封包抓取调试见课程操作

为什么要抓包？-抓包应用的资产信息进行安全测试

2、抓包对象有那些？-小程序,APP,桌面应用等

3、抓包协议区别工具？-有部分应用不走 HTTP/S，需要用到全局协议抓包

4、封包和抓包不同之处？-零散整体的区别，封包能精确到每个操作的数据包

---

## 涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)

---