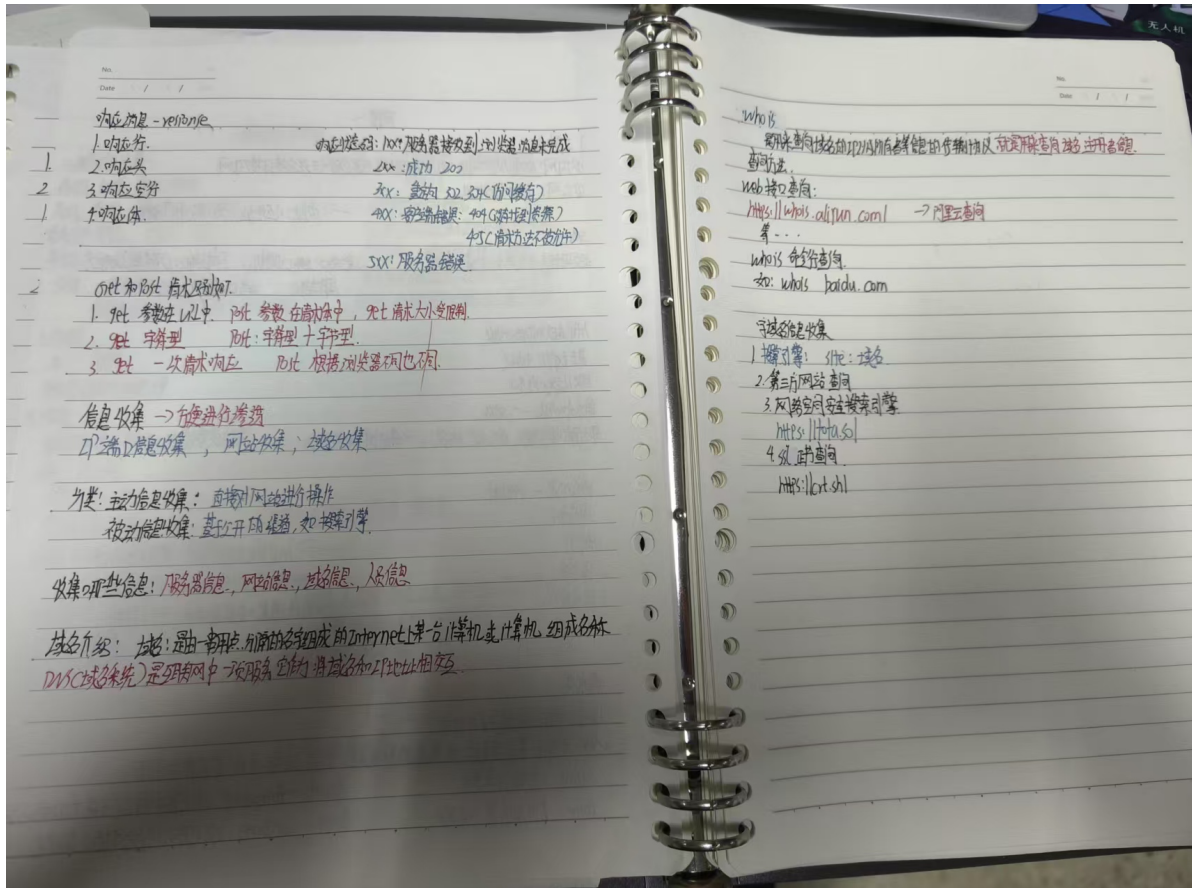


第五周周报

在本周的学习中，通过前几周的经验，我逐步从刚开始的茫然，感觉有很多不知道的知识点，不知道该如何下手学习网络安全，不知道先学习php还是html还是逆向工程，以及不知道该不该使用工具以及使用哪种工具，开始渐渐有了自己一定的经验，知道了面对get 和post两种请求方法有着不同的渗透方法，并开始在网找了许多相关的系统课程，通过在b站的视频学习中我学会了很多有关网络安全的基本知识，并计划在接下的两周把视频学习学完，走完基本知识方面，然后预计在五一放假结束前开始增强实践训练 方面并开始逐步学习渗透测试，和逆向工程以下是我在本周学习的有关笔记。



1. IP地址

网段~

①内网: 路由以内网网络, 可以连接互联网, 但是互联网无法直接访问内网

②公网: 互联网IP地址

端口:

→ 类比: 门牌地址, 户: 家的门牌

是应用程序在计算机中统一标识

源端口: 端口随机, 目标端口: (服务器) 端口

固定端口, 端口范围 0~65535

HTTP超文本传输协议

基于tcp/ip协议

默认端口为80

请求和响应一一对应

每次请求相互独立, 是无状态协议: → 保证传输的可靠性

请求消息 - request

组成如下:

1. 请求行

→ HTTP常见请求: 常用get, post

2. 请求头

get请求在URL地址中, 有URL长度限制

3. 请求主体

post请求: 在参数体中, 无长度限制

4. 请求体

请求头:

Host: 请求主机域名/IP地址

✓ User-Agent: 告诉服务器浏览器的版本信息, 供服务器解决浏览器兼容问题

Accept: 告诉服务器文件类型

Accept-encoding: 浏览器申明自己可接受的编码方法

Referer: 告诉服务器从哪里来

Accept-language: 浏览器申明自己可接收的语言