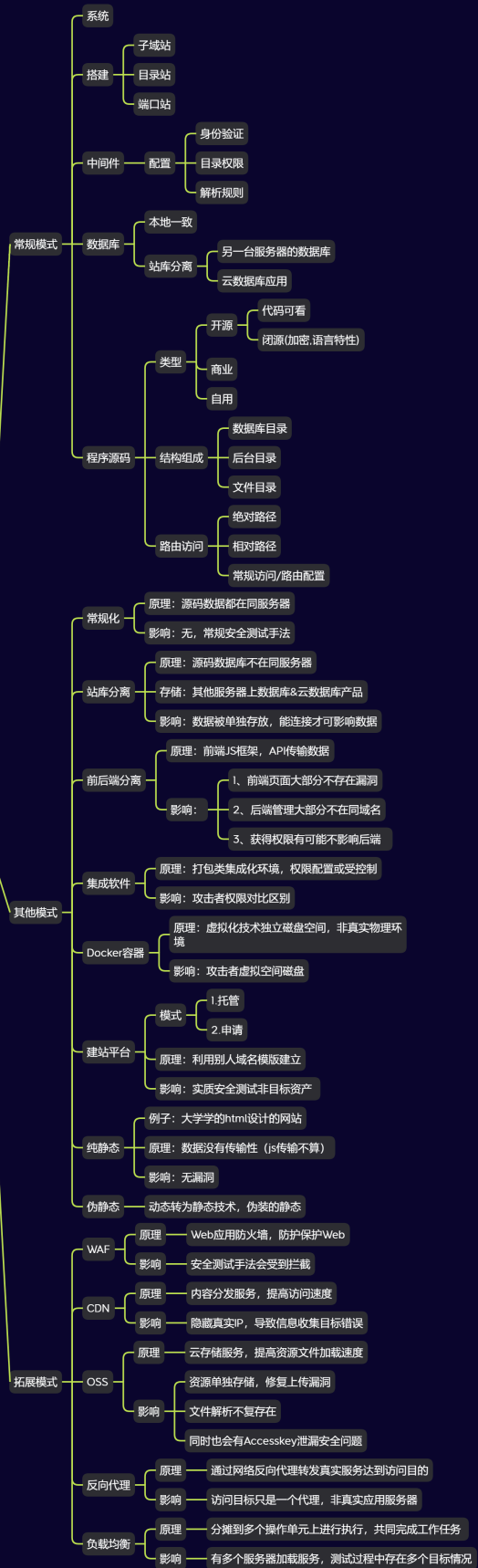
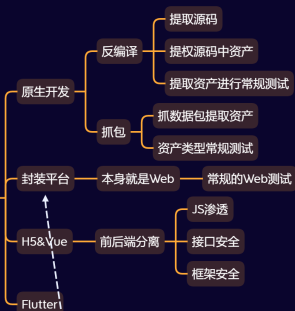


# **Day11 基础入门-ChatGPT 篇&注册体验&结合安全&融 入技术&高效赋能&拓展需求**

## ① Web应用



## ② APP应用



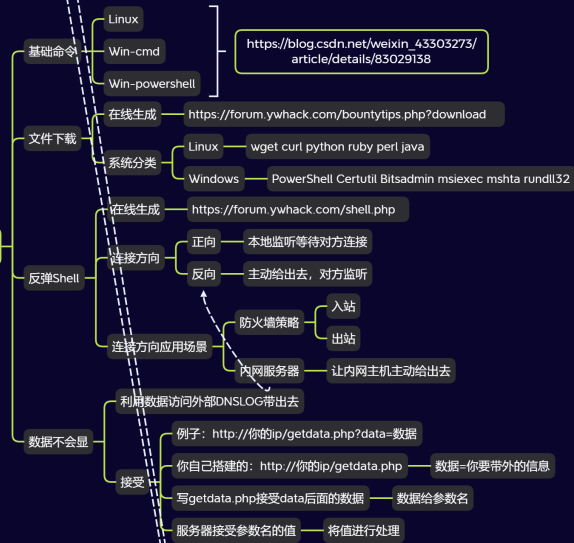
## 基础入门-小迪安全

### ③ 小程序应用

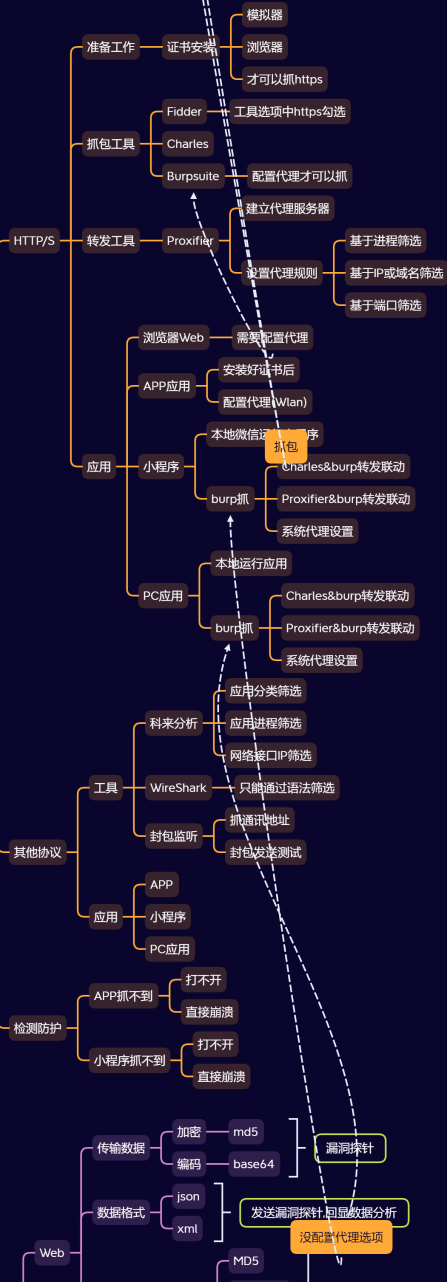


### ④ 云上应用

### 命令&反弹&带外



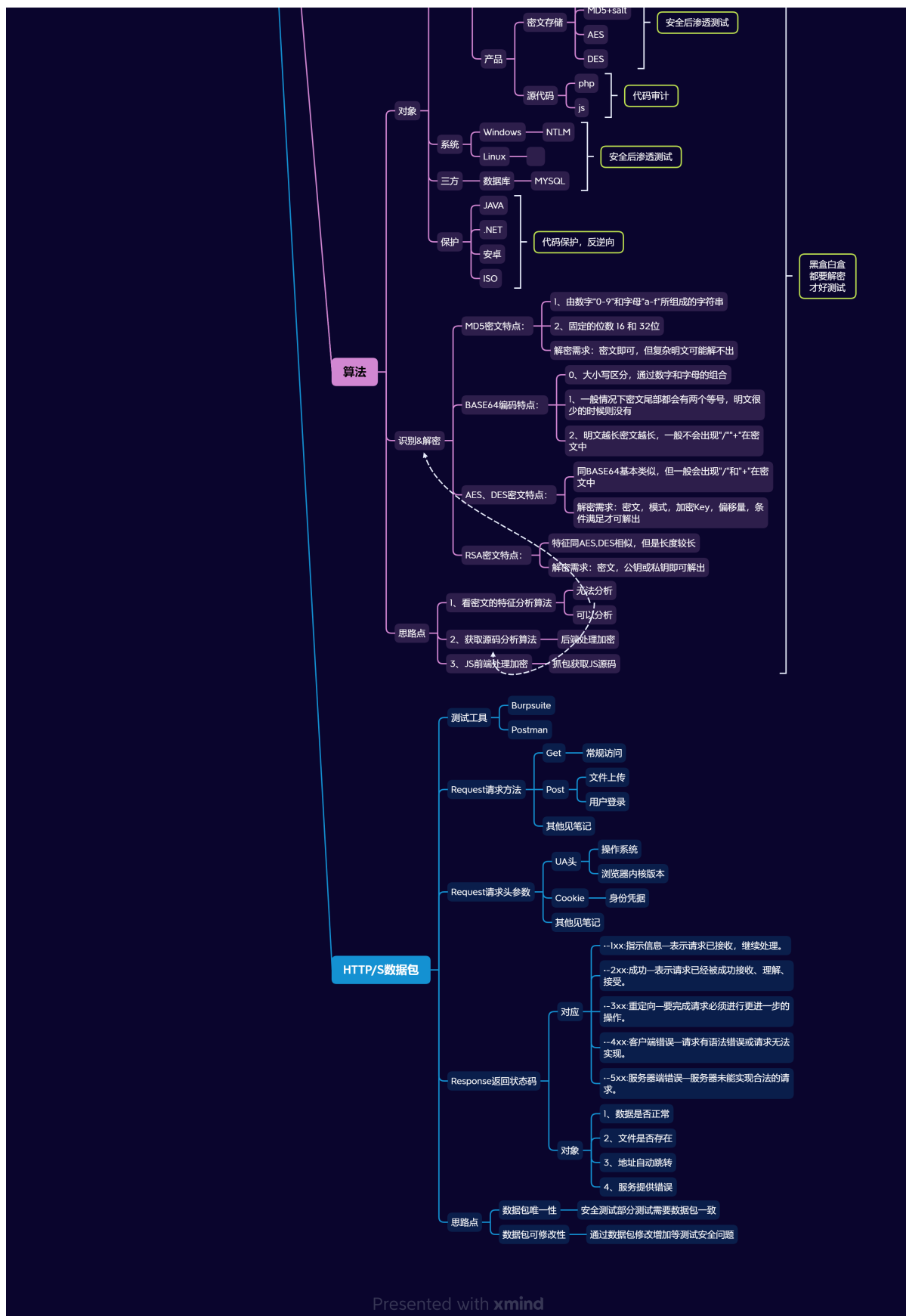
### 抓包技术



### 漏洞探针

发送漏洞探针包显示数据分析

没配置代理选项



## 1.知识点

- 1、Web常规-系统&中间件&数据库&源码等
- 2、Web其他-前后端&软件&Docker&分配站等

- 3、Web拓展-CDN&WAF&OSS&反向&负载均衡等

-----

- 1、APP架构-封装&原生态&H5&flutter等
- 2、小程序架构-Web&H5&JS&VUE框架等

-----

- 1、渗透命令-常规命令&文件上传下载
- 2、反弹Shell-防火墙策略&正反向连接
- 3、数据回显-查询带外&网络协议层级

-----

- 1、抓包技术-HTTP/S-Web&APP&小程序&PC应用等
- 2、抓包工具-Burp&Fiddler&Charles&Proxifier

-----

- 1、抓包技术-全局-APP&小程序&PC应用
- 2、抓包工具-Wireshark&科来分析&封包

-----

- 1、存储密码加密-应用对象
- 2、传输加密编码-发送回显
- 3、数据传输格式-统一格式
- 4、代码特性混淆-开发语言

-----

- 1、单向散列加密 -MD5, HASH
- 2、对称加密 -AES DES
- 3、非对称加密 -RSA

- 4、解密-识别&需求&寻找(前后端)&操作

- 
- 1、HTTP/S数据包请求与返回
  - 2、请求包头部常见解释和应用
  - 3、返回包状态码值解释和应用
  - 4、HTTP/S测试工具Postman使用
- 

- 1、ChatGPT科普&注册&使用
- 2、ChatGPT高效融入安全测试

---

## 2.演示案例

### 2.1 ChatGPT-科普&注册使用



- 1 1、ChatGPT是什么？
- 2 ChatGPT--可能很多人被这个缩写的名字搞糊涂了，第一眼无法看出到底什么意思，GPT 的英文原文是 **Generative Pre-training Transformer**（预训练生成模型），业界有人将 ChatGPT 概括为聊天机器人+搜索工具+文本创造工具的组合，或者简单理解它是一个生成式 **AI**（内容生成器）。
- 3 2、ChatGPT能做什么？
- 4 它的主要功能是协助回答问题、提供信息和生成有关历史、科学、地理等各种主题的信息，这些信息仅限于它所接受的训练，但其知识在不断扩展。
- 5 3、ChatGPT牛在哪里？
- 6 （1）它是个通用的模型，只要提示词引导，就能快速适应不同领域。
- 7 （2）它能理解你的问题，只要给的引导越多，它就能给出你想要的答案。

8 安全行业影响：  
9 (1) 整合多种恶意软件  
10 (2) 提升漏洞发现能力  
11 (3) 给新手攻击者赋能  
12 (4) 便于社会工程学攻击  
13 (5) 快速筛选和锁定目标  
14 (6) 模拟网络防御攻击技术  
15  
16 注册：  
17 必要准备  
18 1、能科学上网（全局模式，不支持HK）  
19 2、能确认登录的电子邮箱或微软账户  
20 3、能接受国外手机验证码的平台，推荐<https://sms-activate.org/>  
21 4、ChatGPT注册地址：<https://chat.openai.com/chat>  
22 参考：  
<https://www.gongshengyun.cn/yunying/portal.php?mod=view&aid=121506>

## 2.2 ChatGPT-有效的安全测试

● ● ●  
1 利用：  
2 -安全开发  
3 1、如何使用Python写一个jwt爆破脚本？  
4 2、如何使用Python写一个webshe11检测脚本？  
5 3、如何使用Python写一个MS17010漏洞检测脚本？  
6 4、使用PHP开发一个免杀混淆复杂的webshe11脚本  
7 4.1、在渗透测试靶机中，发现PHP脚本被禁用了敏感函数，如何生成一个绕过的webshe11

## 资源:



- 1 最全的ChatGPT注册使用攻略，含验证码接收教程（图文步骤）：
- 2 <https://www.gongshengyun.cn/yunying/portal.php?mod=view&aid=121506>