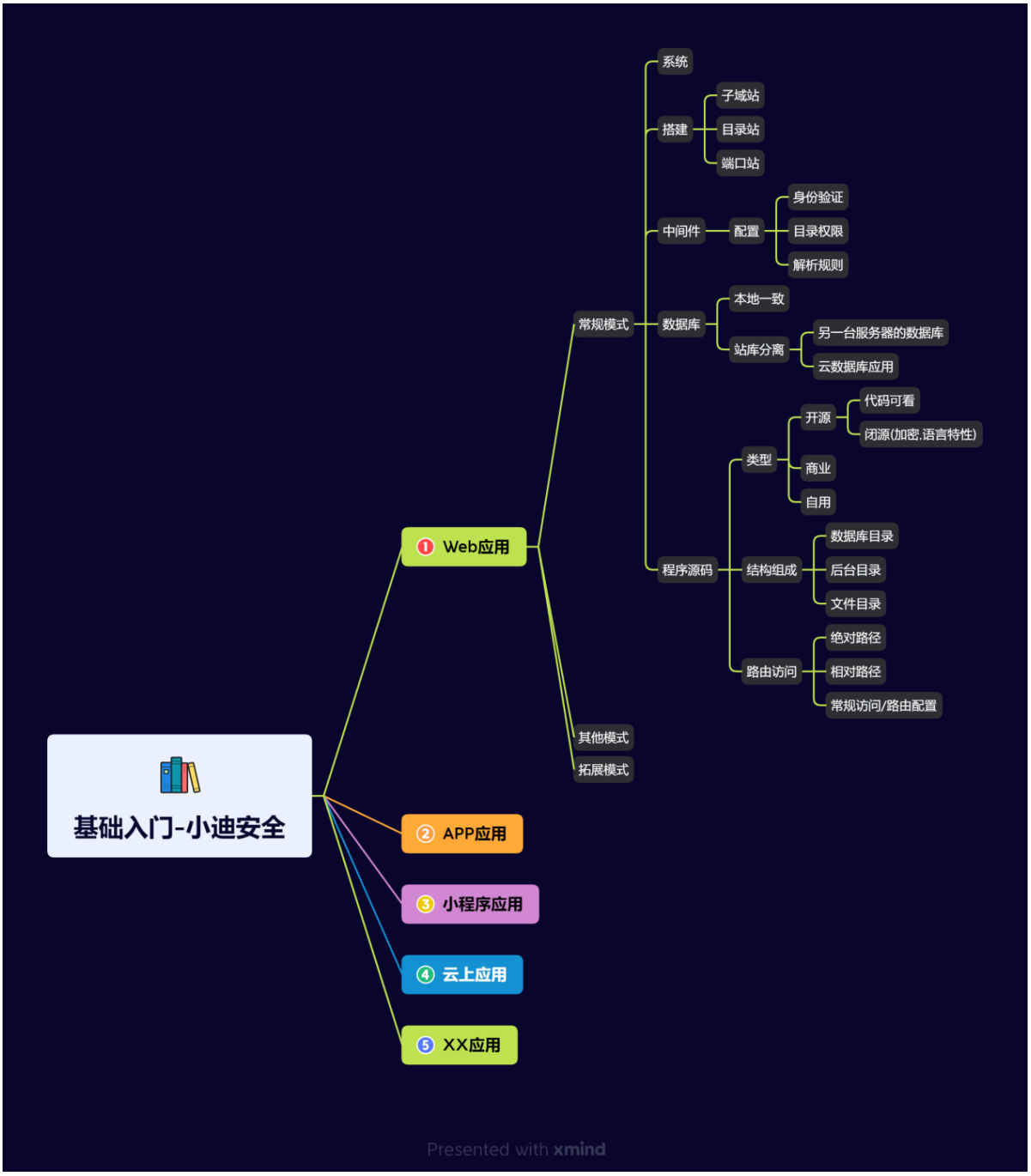
Day02　基础入门-Web架构&前后端分离站&Docker容器站&集成软件站&建站分配



1.知识点

- 1、Web常规-系统&中间件&数据库&源码等
- 2、Web其他-集成软件&Docker容器&分配站等
- 3、Web拓展-CDN&WAF&OSS&静态&负载均衡等

2.演示案例

2.1 Web架构-常规化&站库分离&前后端分离

```
#常规化
原理：源码数据都在同服务器
影响：无，常规安全测试手法
```

```
#站库分离：
原理：源码数据库不在同服务器
存储：其他服务器上数据库&云数据库产品
影响：数据被单独存放，能连接才可影响数据
```

```
#前后端分离
原理：前端JS框架，API传输数据
影响：
1、前端页面大部分不存在漏洞
2、后端管理大部分不在同域名
3、获得权限有可能不影响后端
```

2.2 Web架构-集成软件&Docker容器&分配站

```
#宝塔+Phpstudy
原理：打包类集成化环境，权限配置或受控制
影响：攻击者权限对比区别
```

```
拿到权限后

宝塔：
文件管理 锁定目录
命令执行 无法执行

phpstudy：
文件管理 锁定目录
命令执行 可以执行
whomi 获取用户权限- administrator
izsjxymy4Ezovoz\administrator

自己搭建的iis：
liis apppool\defaultapppool
```

```
#Docker容器
原理：虚拟化技术独立磁盘空间，非真实物理环境
影响：攻击者虚拟空间磁盘
```

```
#建站分配站
1.托管
2.申请
原理：利用别人域名模版建立
影响：实质安全测试非目标资产
```

```
#静态web
例子：大学学的html设计的网站
原理：数据没有传输性（js传输不算）
影响：无漏洞
```

```
#伪静态
动态转为静态技术，伪装的静态
```