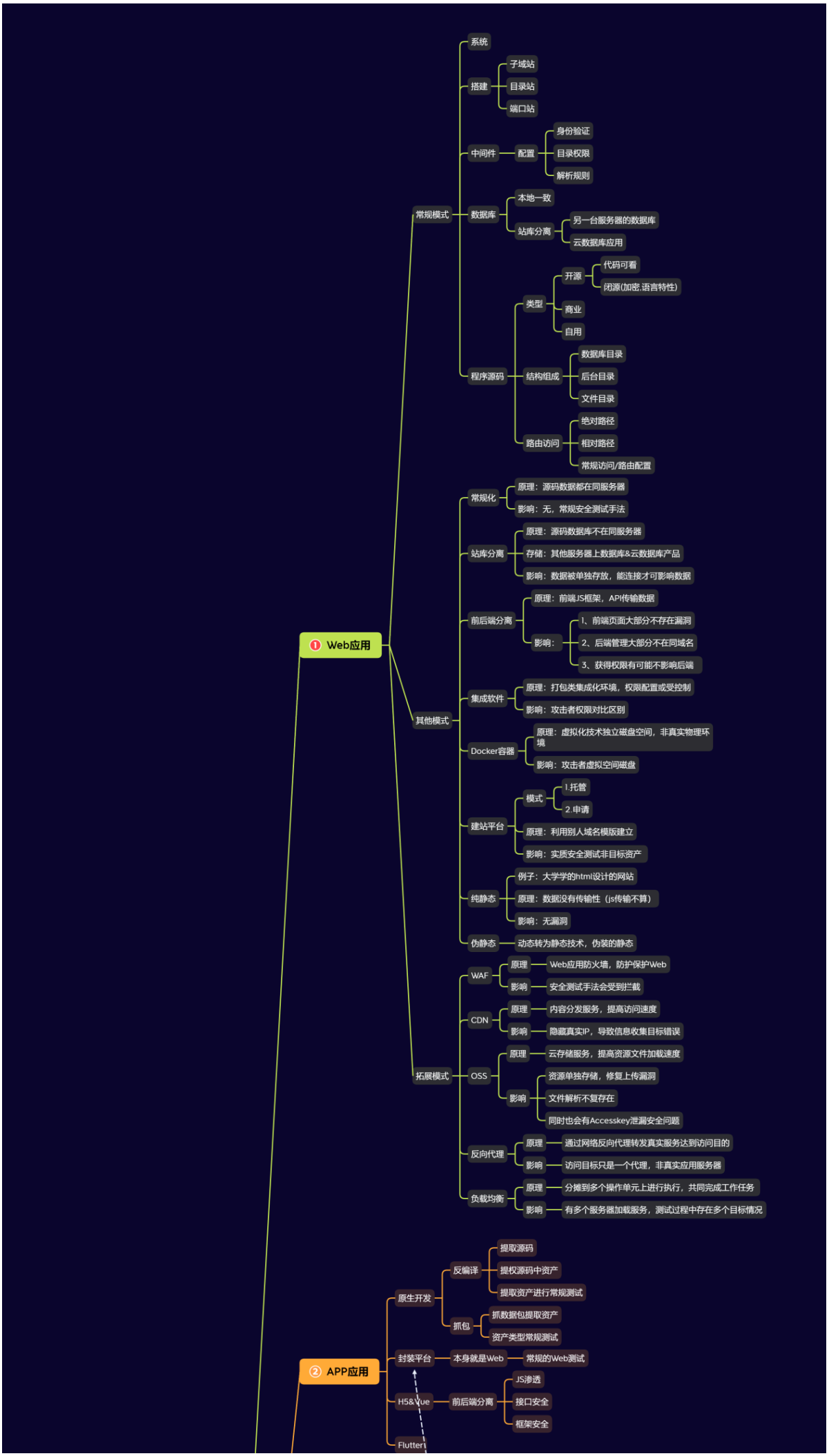
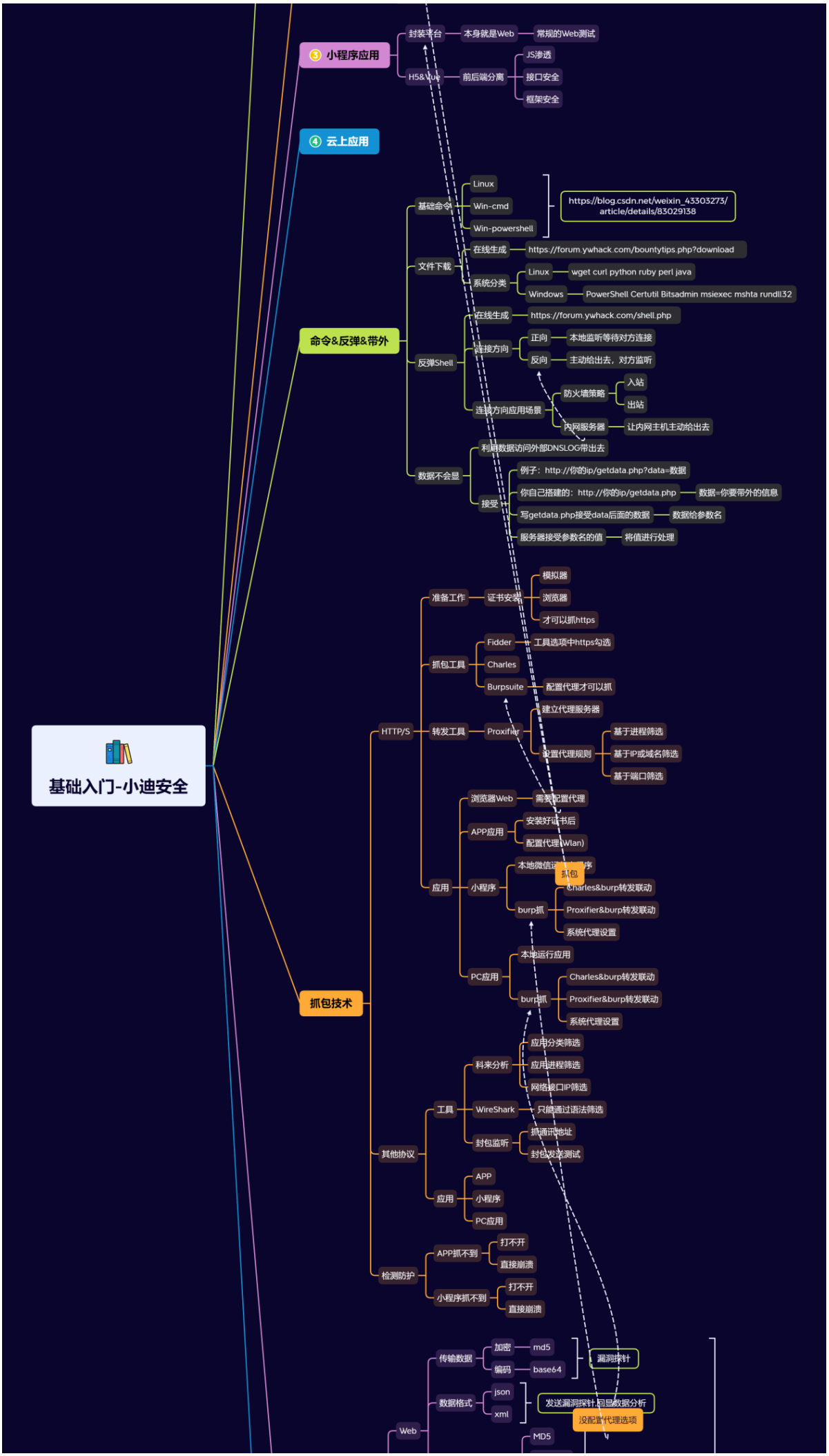
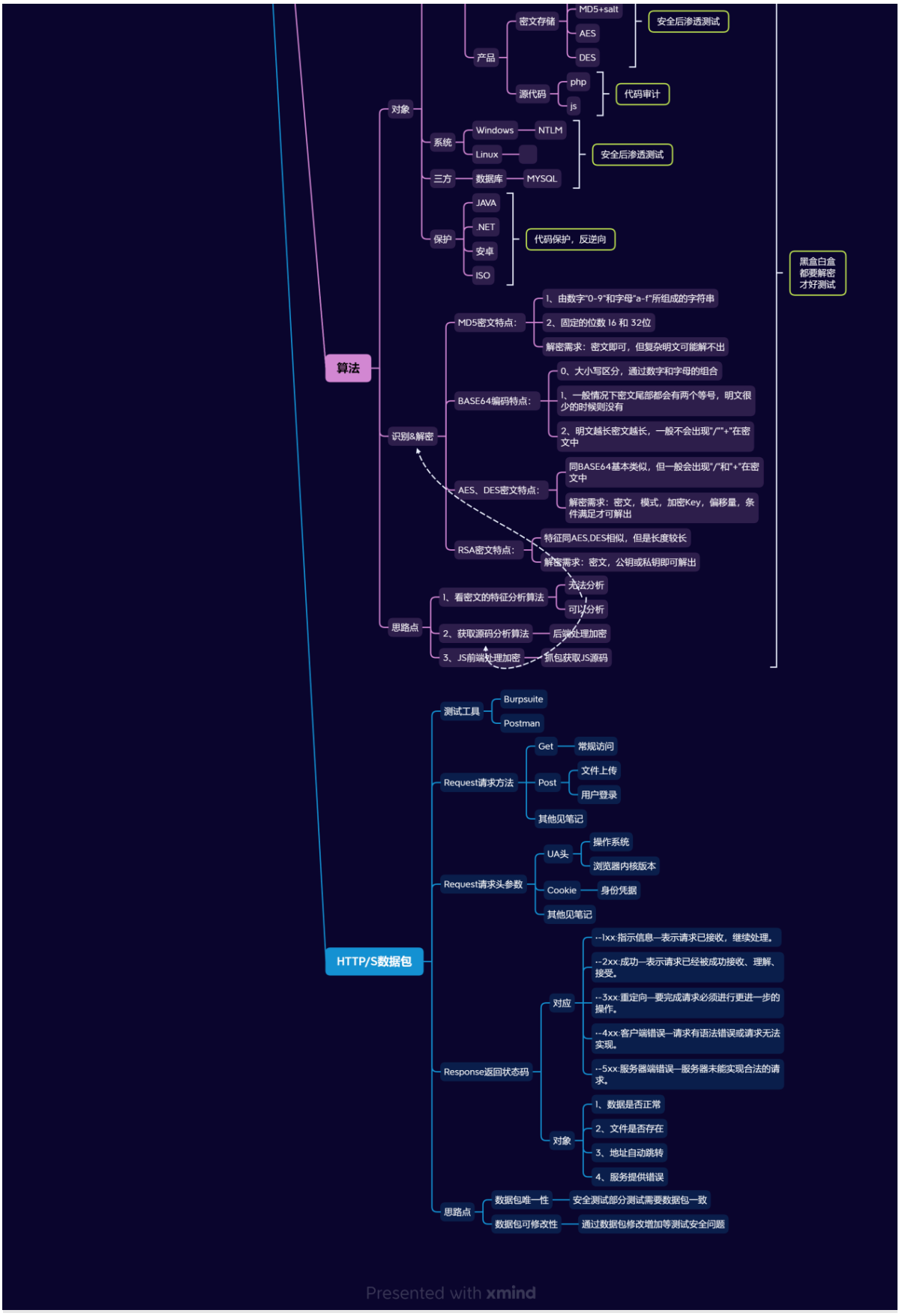
Day10　基础入门-HTTP数据包&Postman构造&请求方法&请求头修改&状态码判断


❶ Web应用
常规模式
系统
搭建
子域站
目录站
端口站
中间件
配置
身份验证
目录权限
解析规则
数据库
本地一致
站库分离
另一台服务器的数据库
云数据库应用
程序源码
类型
开源
代码可看
闭源(加密 语言特性)
商业
自用
结构组成
数据库目录
后台目录
文件目录
路由访问
绝对路径
相对路径
常规访问/路由配置
其他模式
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
集成软件
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
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
建站平台
模式
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
纯静态
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
拓展模式
WAF
原理
Web应用防火墙，防护保护Web
影响
安全测试手法会受到拦截
CDN
原理
内容分发服务，提高访问速度
影响
隐藏真实IP，导致信息收集目标错误
OSS
原理
云存储服务，提高资源文件加载速度
影响
资源单独存储，修复上传漏洞
文件解析不复存在
同时也会有Accesskey泄漏安全问题
反向代理
原理
通过网络反向代理转发真实服务达到访问目的
影响
访问目标只是一个代理，非真实应用服务器
负载均衡
原理
分摊到多个操作单元上进行执行，共同完成工作任务
影响
有多个服务器加载服务，测试过程中存在多个目标情况
② APP应用
原生开发
反编译
提取源码
提权源码中资产
提取资产进行常规测试
抓包
抓数据包提取资产
资产类型常规测试
封装平台
本身就是Web
常规的Web测试
H5&Vue
前后端分离
JS渗透
接口安全
框架安全
Flutter


基础入门-小迪安全
③ 小程序应用
封装平台
本身就是Web
常规的Web测试
H5&Vue
前后端分离
JS渗透
接口安全
框架安全
④ 云上应用
命令&反弹&带外
基础命令
Linux
Win-cmd
Win-powershell
https://blog.csdn.net/weixin_43303273/article/details/83029138
文件下载
在线生成
https://forum.ywhack.com/bountytips.php?download
系统分类
Linux
wget curl python ruby perl java
Windows
PowerShell Certutil Bitsadmin msiexec mshta rundll32
反弹Shell
在线生成
https://forum.ywhack.com/shell.php
连接方向
正向
本地监听等待对方连接
反向
主动给出去，对方监听
连接方向应用场景
防火墙策略
入站
出站
内网服务器
让内网主机主动给出去
数据不会显
利用数据访问外部DNSLOG带出去
接受
例子：http://你的ip/getdata.php?data=数据
你自己搭建的：http://你的ip/getdata.php
数据=你要带外的信息
写getdata.php接受data后面的数据
数据给参数名
服务器接受参数名的值
将值进行处理
抓包技术
HTTP/S
准备工作
证书安装
模拟器
浏览器
才可以抓https
抓包工具
Fiddler
工具选项中https勾选
Charles
Burpsuite
配置代理才可以抓
转发工具
Proxifier
建立代理服务器
设置代理规则
基于进程筛选
基于IP或域名筛选
基于端口筛选
应用
浏览器Web
需要配置代理
APP应用
安装好证书后
配置代理(Wlan)
小程序
本地微信运行小程序
抓包
Charles&burp转发联动
burp抓
Proxifier&burp转发联动
系统代理设置
PC应用
本地运行应用
Charles&burp转发联动
burp抓
Proxifier&burp转发联动
系统代理设置
其他协议
工具
科来分析
应用分类筛选
应用进程筛选
网络接口IP筛选
WireShark
只能通过语法筛选
封包监听
抓通讯地址
封包发送测试
应用
APP
小程序
PC应用
检测防护
APP抓不到
打不开
直接崩溃
小程序抓不到
打不开
直接崩溃
传输数据
加密
md5
编码
base64
漏洞探针
数据格式
json
xml
发送漏洞探针回显数据分析
没配置代理选项
Web
MD5



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&Fidder&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

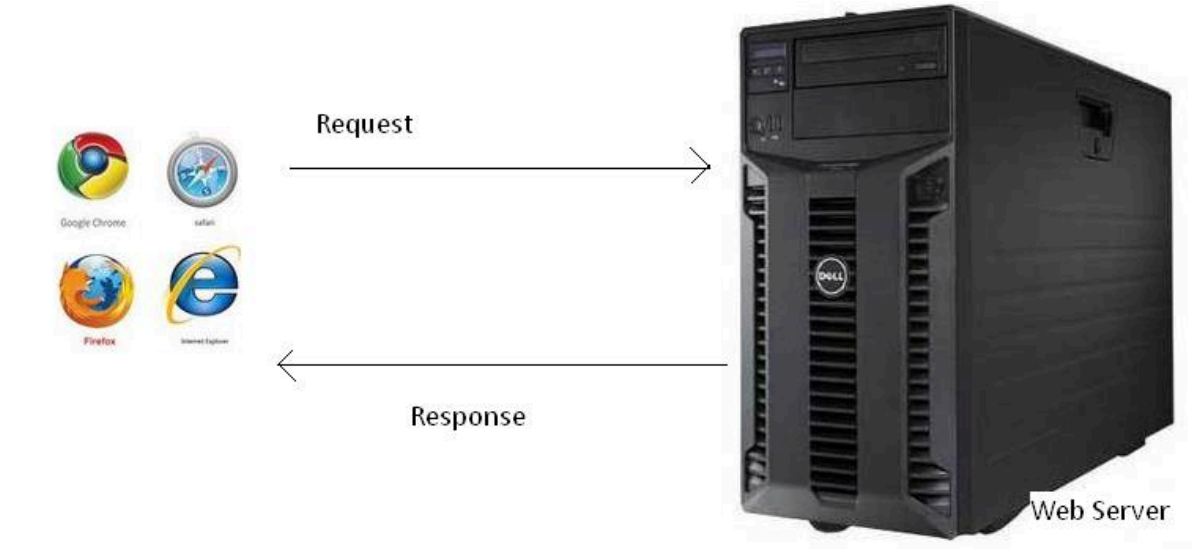
- 4、解密-识别&需求&寻找(前后端)&操作

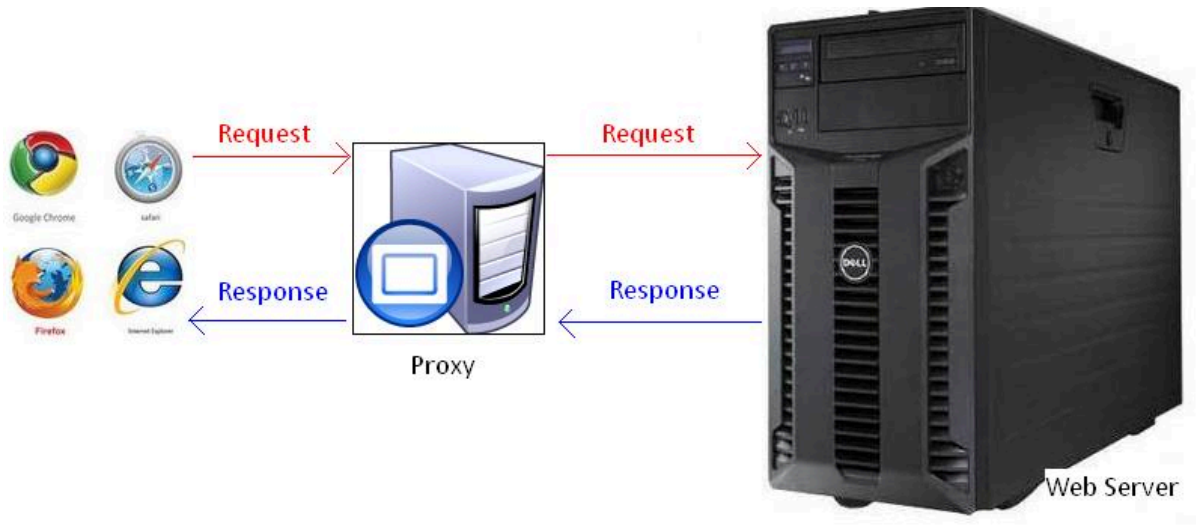
- 1、HTTP/S数据包请求与返回
- 2、请求包头部常见解释和应用
- 3、返回包状态码值解释和应用
- 4、HTTP/S测试工具Postman使用

2.演示案例

2.1 数据-方法&头部&状态码

HTTP/S数据包请求与返回:





Request:

Header	解释
Accept	指定客户端能够接收的内容类型
Accept-Charset	浏览器可以接受的字符编码集。
Accept-Encoding	指定浏览器可以支持的 web 服务器返回内容压缩编码类型。
Accept-Language	浏览器可接受的语言
Accept-Ranges	可以请求网页实体的一个或者多个子范围字段
Authorization	HTTP 授权的授权证书
Cache-Control	指定请求和响应遵循的缓存机制
Connection	表示是否需要持久连接。（HTTP 1.1 默认进行持久连接）
Cookie	HTTP 请求发送时，会把保存在该请求域名下的所有 cookie 值一起发送给 web 服务器。
Content-Length	请求的内容长度
Content-Type	请求的与实体对应的 MIME 信息
Date	请求发送的日期和时间
Expect	请求的特定的服务器行为
From	发出请求的用户的 Email
Host	指定请求的服务器的域名和端口号
If-Match	只有请求内容与实体相匹配才有效
If-Modified-Since	如果请求的部分在指定时间之后被修改则请求成功，未被修改则返回 304 代码
If-None-Match	如果内容未改变返回 304 代码，参数为服务器先前发送的 Etag，与服务器回应的 Etag 比较判断是否改变
If-Range	如果实体未改变，服务器发送客户端丢失的部分，否则发送整个实体。参数也为 Etag
If-Unmodified-Since	只在实体在指定时间之后未被修改才请求成功

Response：

Header	解释
Accept-Ranges	表明服务器是否支持指定范围请求及哪种类型的分段请求
Age	从原始服务器到代理缓存形成的估算时间（以秒计，非负）
Allow	对某网络资源的有效的请求行为，不允许则返回 405
Cache-Control	告诉所有的缓存机制是否可以缓存及哪种类型
Content-Encoding	web 服务器支持的返回内容压缩编码类型。
Content-Language	响应体的语言
Content-Length	响应体的长度
Content-Location	请求资源可替代的备用的另一地址
Content-MD5	返回资源的 MD5 校验值
Content-Range	在整个返回体中本部分的字节位置
Content-Type	返回内容的 MIME 类型
Date	原始服务器消息发出的时间
ETag	请求变量的实体标签的当前值
Expires	响应过期的日期和时间
Last-Modified	请求资源的最后修改时间
Location	用来重定向接收方到非请求 URL 的位置来完成请求或标识新的资源
Pragma	包括实现特定的指令，它可应用到响应链上的任何接收方
Proxy-Authenticate	它指出认证方案和可应用到代理的该 URL 上的参数
Retry-After	如果实体暂时不可取，通知客户端在指定时间之后再次尝试
Server	web 服务器软件名称
Set-Cookie	设置 Http Cookie

get请求&&post请求:

http请求之get请求

http请求之post请求


```
-方法
1、常规请求-Get
2、用户登录-Post
•get：向特定资源发出请求（请求指定页面信息，并返回实体主体）；
```

•post：向指定资源提交数据进行处理请求（提交表单、上传文件），又可能导致新的资源的建立或原有资源的修改；
•head：与服务器索与get请求一致的相应，响应体不会返回，获取包含在小消息头中的原信息（与get请求类
似，返回的响应中没有具体内容，用于获取报头）；
•put：向指定资源位置上上传其最新内容（从客户端向服务器传送的数据取代指定文档的内容），与post的区别是put为幂等，post为非幂等；
•trace：回显服务器收到的请求，用于测试和诊断。trace是http8种请求方式之中最安全的l
•delete：请求服务器删除request-URL所标示的资源*（请求服务器删除页面）
•option：返回服务器针对特定资源所支持的HTML请求方法 或web服务器发送*测试服务器功能（允许客户 端查看服务器性能）；
•connect ： HTTP/1.1协议中能够将连接改为管道方式的代理服务器

-参数
演示：
1、UA头-设备平台
2、Cookie-身份替换
见上图

-Response状态码
1、数据是否正常
2、文件是否存在
3、地址自动跳转
4、服务提供错误
注：容错处理识别
•-1xx:指示信息–表示请求已接收，继续处理。
•-2xx:成功–表示请求已经被成功接收、理解、接受。

```
28  •-3xx:重定向–要完成请求必须进行更进一步的操作。
29  •-4xx:客户端错误–请求有语法错误或请求无法实现。
30  •-5xx:服务器端错误–服务器未能实现合法的请求。
31  •200 OK：客户端请求成功
32  •301 redirect：页面永久性移走，服务器进行重定向跳转；
33  •302 redirect：页面暂时性移走，服务器进行重定向跳转，具
    有被劫持的安全风险；
34  •400 BadRequest：由于客户端请求有语法错误，不能被服务器
    所理解；
35  •401 Unauthonzed：请求未经授权。
36  •403 Forbidden：服务器收到请求，但是拒绝提供服务。
37  •404 NotFound：请求的资源不存在，例如，输入了错误的
    URL；
38  •500 InternalServerError：服务器发生不可预期的错误，
    无法完成客户端的请求；
39  •503 ServiceUnavailable：服务器当前不能够处理客户端的
    请求
```

2.2 案例-文件探针&登录爆破

```
1  -实验：
2  1、页面正常访问
3  2、网站文件探针
4  3、后台登录爆破
```

2.3 工具-Postman自构造使用

```
1  https://zhuanlan.zhihu.com/p/551703621
```

资源：

```
Postman中文版：
https://zhuanlan.zhihu.com/p/551703621
```