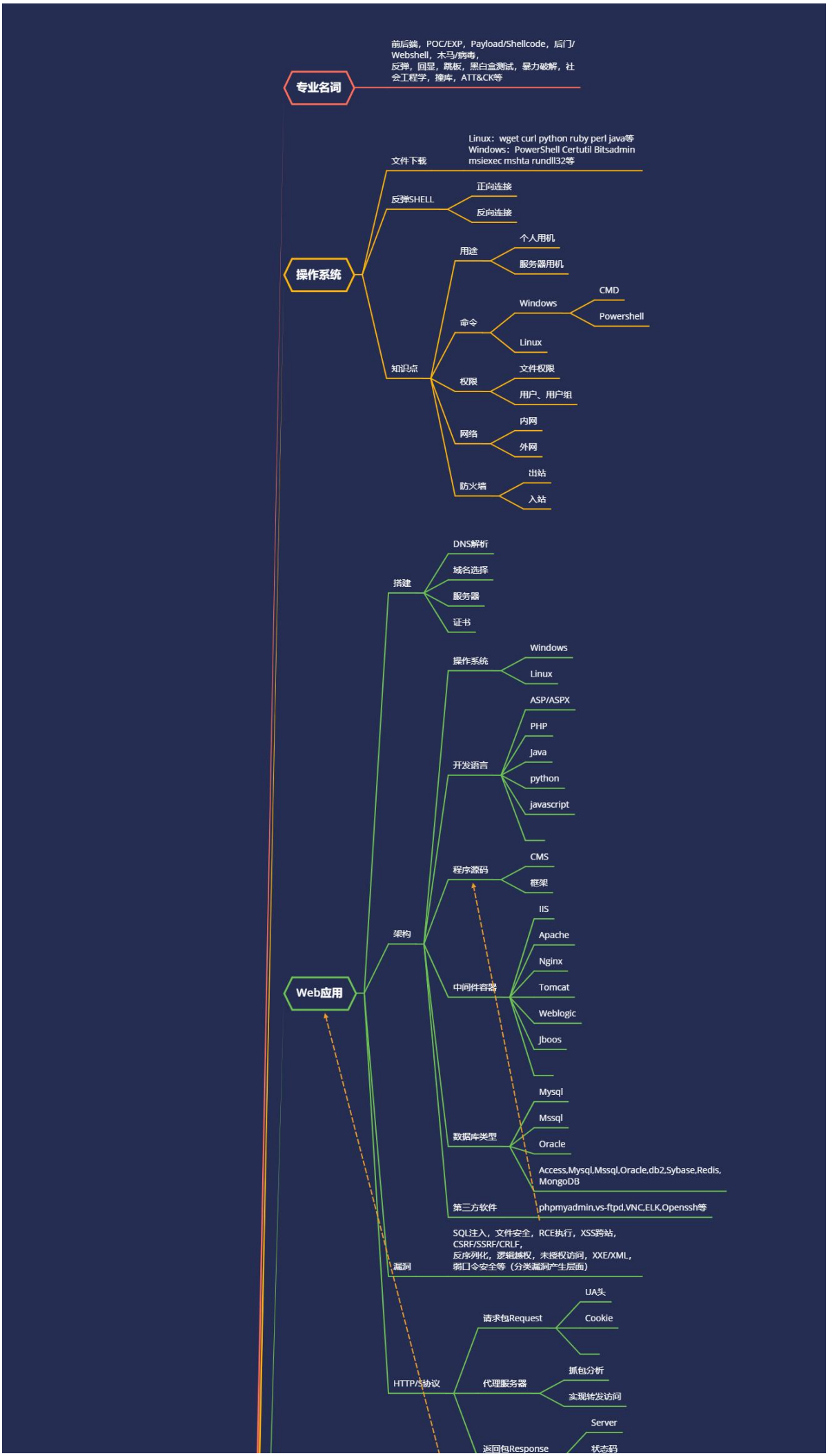
Day17　PHP 开发-个人博客项目&TP 框架&路由访问&安全写法&历史漏洞


专业名词
前后端，POC/EXP，Payload/Shellcode，后门/Webshell，木马/病毒，
反弹，回显，跳板，黑白盒测试，暴力破解，社会工程学，撞库，ATT&CK等
操作系统
文件下载
Linux：wget curl python ruby perl java等
Windows：PowerShell Certutil Bitsadmin mshta rundll32等
反弹SHELL
正向连接
反向连接
知识点
用途
个人用机
服务器用机
命令
Windows
CMD
Powershell
Linux
权限
文件权限
用户、用户组
网络
内网
外网
防火墙
出站
入站
Web应用
搭建
DNS解析
域名选择
服务器
证书
架构
操作系统
Windows
Linux
开发语言
ASP/ASPX
PHP
Java
python
javascript
程序源码
CMS
框架
中间件容器
IIS
Apache
Nginx
Tomcat
Weblogic
Jboos
数据库类型
Mysql
Mssql
Oracle
Access,Mysql,Mssql,Oracle,db2,Sybase,Redis,MongoDB
第三方软件
phpmyadmin,vs-ftpd,VNC,ELK,Openssh等
漏洞
SQL注入，文件安全，RCE执行，XSS跨站，CSRF/SSRF/CRLF，
反序列化，逻辑越权，未授权访问，XXE/XML，
弱口令安全等（分类漏洞产生层面）
HTTP/S协议
请求包Request
UA头
Cookie
代理服务器
抓包分析
实现转发访问
返回包Response
Server
状态码

1.知识点

- 基于 TP 框架入门安装搭建使用
- 基于 TP 框架内置安全写法评估
- 基于 TP 框架实例源码安全性评估

2.演示案例

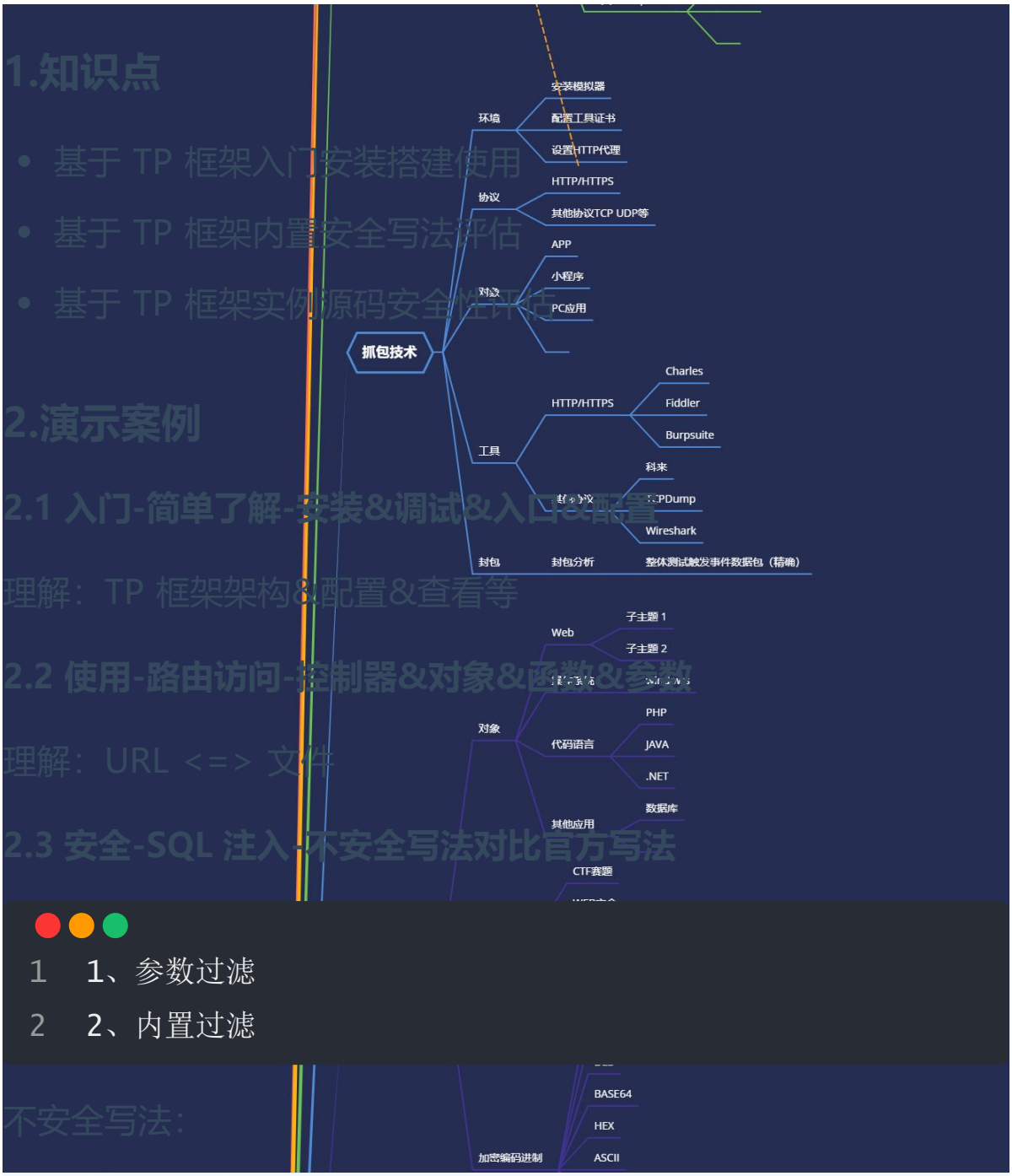
2.1 入门-简单了解-安装&调试&入口文件配置

理解：TP 框架架构&配置&查看等

2.2 使用-路由访问-控制器&对象&函数&参数

理解：URL <=> 文件

2.3 安全-SQL 注入-不安全写法对比官方写法



1. 1、参数过滤
2. 2、内置过滤

不安全写法：

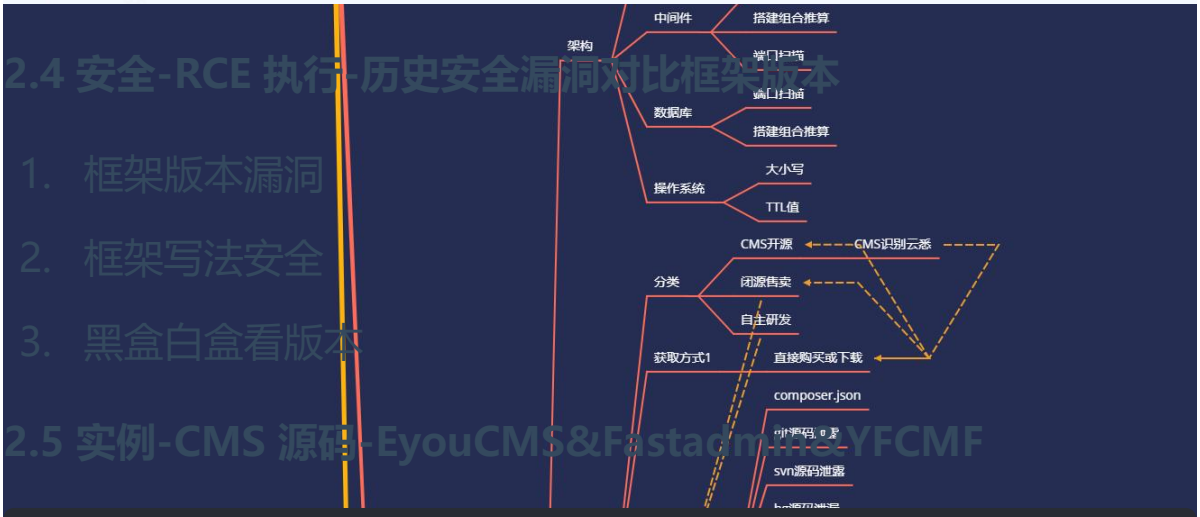
```php
public function sqlin()
{
    //常规类的PHP数据库操作写法 有安全SQL注入漏洞
    //return '<style type="text/css">*{ padding: 0; margin: 0; } .think_default_text{
    $id=$_GET['x'];
    $conn=mysql_connect( server: 'localhost', username: 'root', password: 'root');
    mysql_select_db( database name: 'syguestbook');
    $sql="select * from sy_message where id=$id";
    $result=mysql_query($sql,$conn);
    while($row=mysql_fetch_array($result)){
        echo '<br><br><hr>';
        echo $row['gid'];
        echo $row['name'];
    }

}
```

安去写法：

```php
public function tp_sqlin1()
{
    $id=input( key: 'get.x');
    Db::table( table: 'sy_message')->where( field: 'id',$id)->select();


}
```

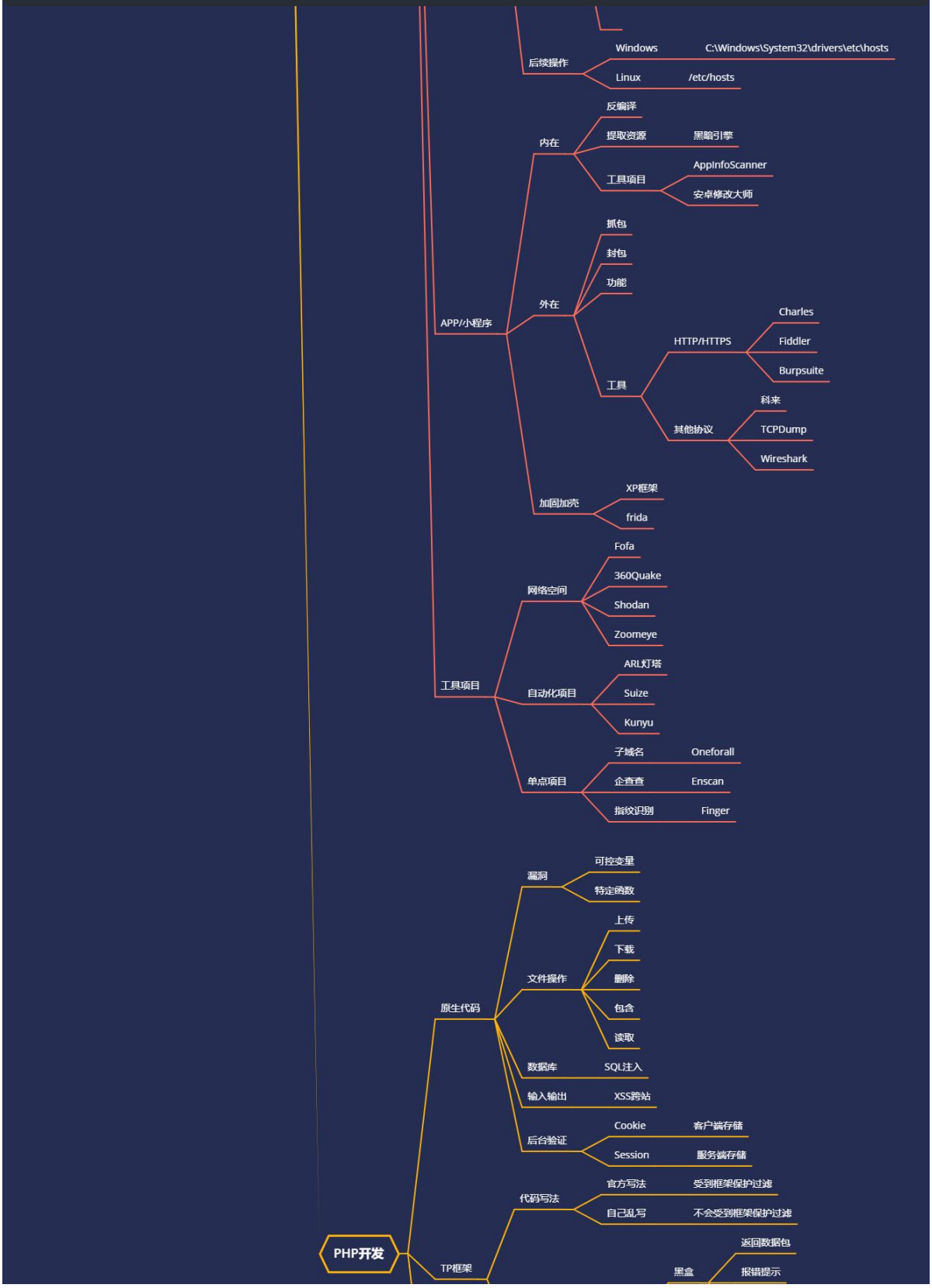


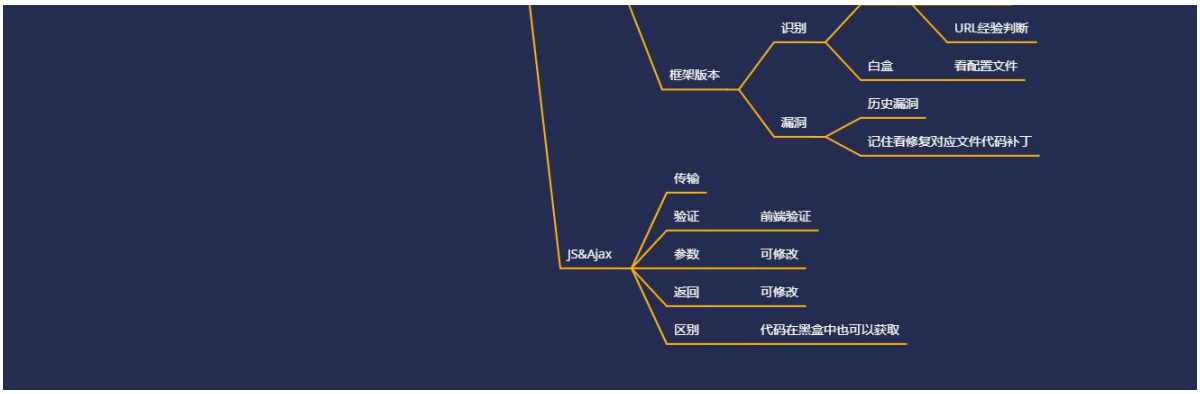

```
AdminLTE 后台管理系统
layui 后台管理系统
thinkcmf
H-ui.admin 后台管理系统
tpshop
FsatAdmin
eyoucms
LarryCMS 后台管理系统
tpadmin 后台管理系统
snake 后台管理系统
ThinkSNS DolphinPHP 后台管理系统
WeMall 商城系统
CLTPHP
齐博 CMS
DSMALL
YFCMF
HisiPHP 后台管理系统
Tplay 后台管理系统
lyadmin 后台管理系统
```

```
20  haoid 后台管理系统
```

资源：


```
1  TinkPHP源码地址：
2  https://github.com/Mochazz/ThinkPHP-Vuln
```




识别
URL经验判断
框架版本
白盒
看配置文件
历史漏洞
漏洞
记住看修复对应文件代码补丁
传输
验证
前端验证
JS&Ajax
参数
可修改
返回
可修改
区别
代码在黑盒中也可以获取