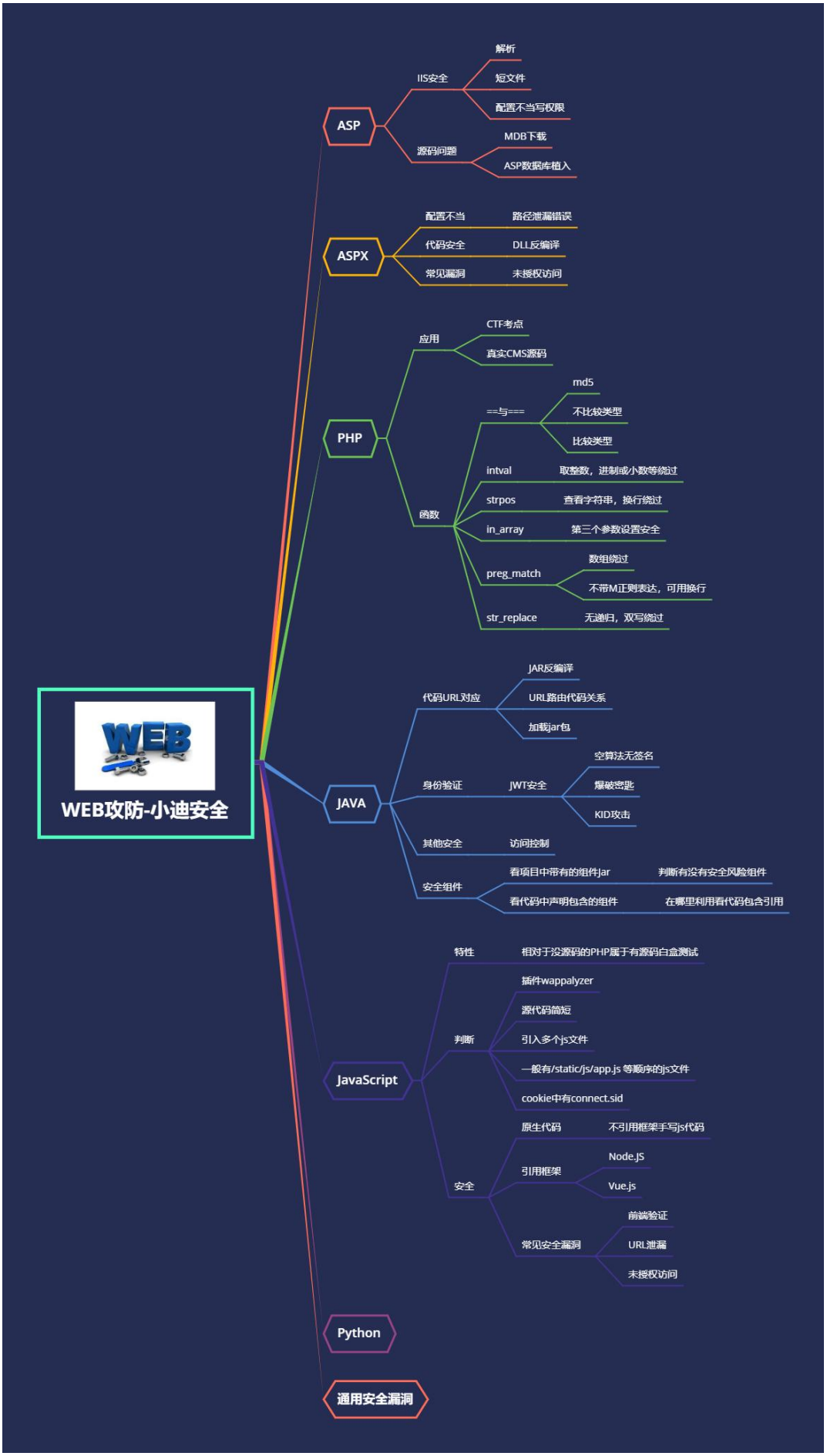
WEB 攻防-JS 项目&Node.JS 框架安全&识别审计&验证绕过


WEB攻防-小迪安全
ASP
IIS安全
解析
短文件
配置不当写权限
源码问题
MDB下载
ASP数据库植入
ASPX
配置不当
路径泄漏错误
代码安全
DLL反编译
常见漏洞
未授权访问
PHP
应用
CTF考点
真实CMS源码
函数
==与===
md5
不比较类型
比较类型
intval
取整数，进制或小数等绕过
strpos
查看字符串，换行绕过
in_array
第三个参数设置安全
preg_match
数组绕过
不带M正则表达，可用换行
str_replace
无递归，双写绕过
JAVA
代码URL对应
JAR反编译
URL路由代码关系
加载jar包
身份验证
JWT安全
空算法无签名
爆破密匙
KID攻击
其他安全
访问控制
安全组件
看项目中带有的组件jar
判断有没有安全风险组件
看代码中声明包含的组件
在哪里利用看代码包含引用
JavaScript
特性
相对于没源码的PHP属于有源码白盒测试
判断
插件wappalyzer
源代码简短
引入多个js文件
一般有/static/js/app.js 等顺序的js文件
cookie中有connect.sid
安全
原生代码
不引用框架手写js代码
引用框架
Node.JS
Vue.js
常见安全漏洞
前端验证
URL泄漏
未授权访问
Python
通用安全漏洞

#知识点：
1、原生 JS&开发框架-安全条件
2、常见安全问题-前端验证&未授权

#详细点：
1、什么是 JS 渗透测试？
在 Javascript 中也存在变量和函数，当存在可控变量及函数调用即可参数漏洞
JS 开发的 WEB 应用和 PHP，JAVA,NET 等区别在于即没有源代码，也可以通过浏览器的查看源代码获取真实的点。所以相当于 JS 开发的 WEB 应用属于白盒测试（默认有源码参考）
2、流行的 Js 框架有那些？
3、如何判定 JS 开发应用？
插件 wappalyzer
源代码简短
引入多个 js 文件
一般有/static/js/app.js 等顺序的 js 文件
cookie 中有 connect.sid
4、如何获取更多的 JS 文件？
JsFinder
Packer-Fuzzer
扫描器后缀替换字典
5、如何快速获取价值代码？
method:"get"
http.get("
method:"post"
http.post("
$.ajax
service.httppost
service.httpget

演示案例：

- 安全条件-可控变量&特定函数
- 开发框架-Vulhub-Node.JS 安全
- 真实应用-APP 应用直接重置密码
- 真实应用-违法彩彩文件上传安全

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址