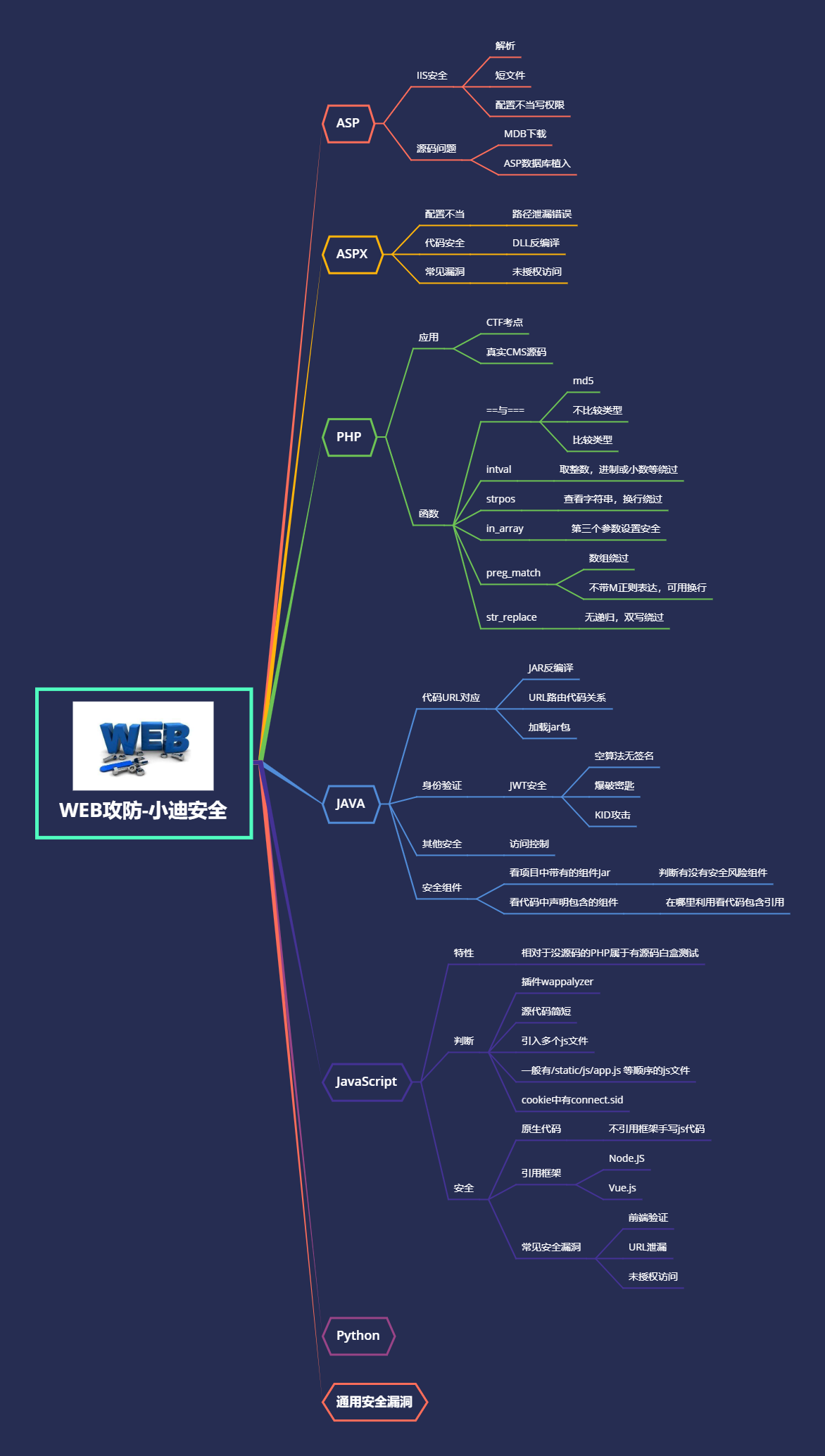
WEB攻防-JS项目&Node.JS框架安全&识别审计&验证绕过



#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](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)