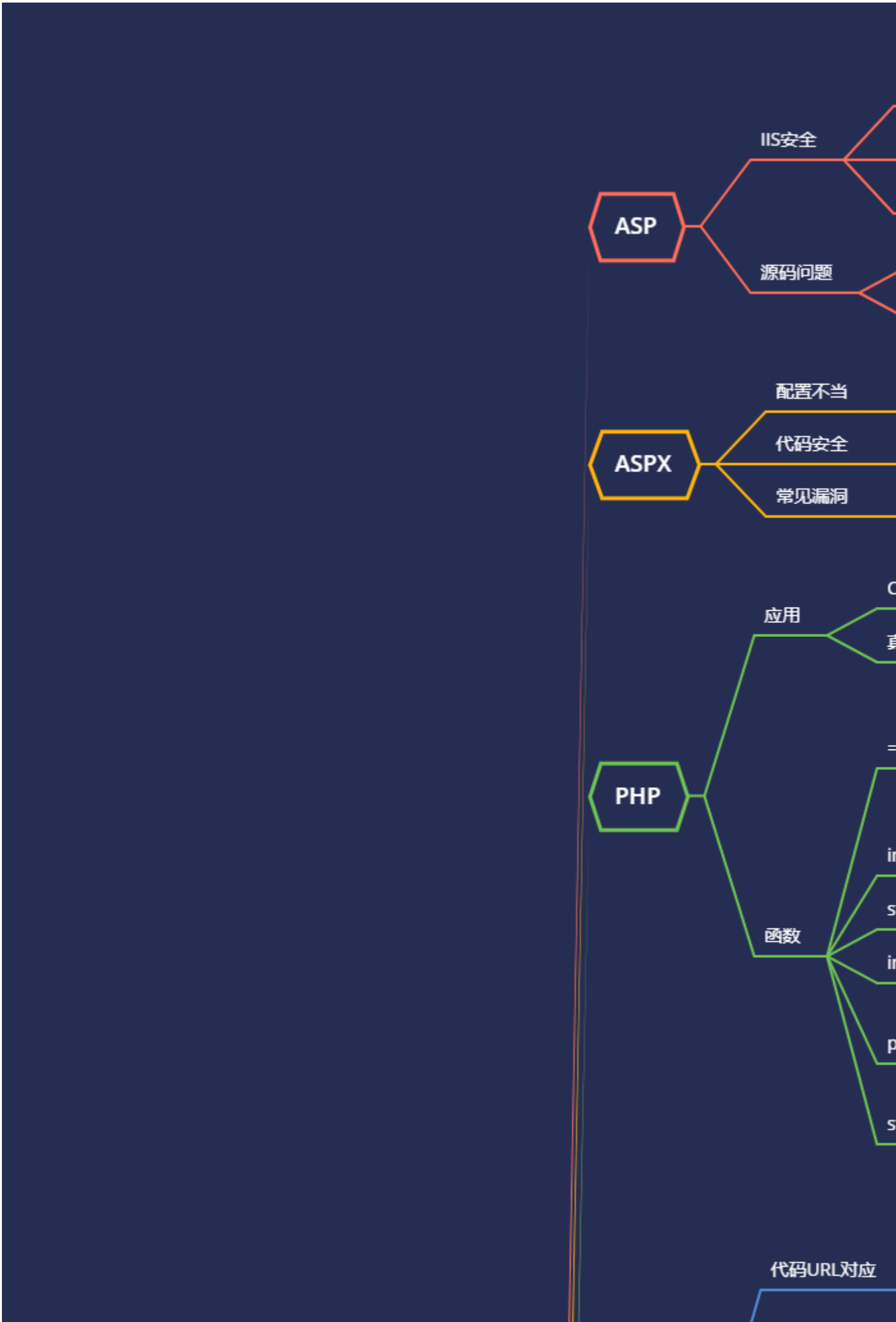
WEB 攻防-通用漏洞&PHP 反序列化&POP 链构造&魔术方法&原生类


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、什么是反序列化操作？-格式转换

2、为什么会出现安全漏洞？-魔术方法

3、反序列化漏洞如何发现？ -对象逻辑

4、反序列化漏洞如何利用？-POP 链构造

补充：反序列化利用大概分类三类

-魔术方法的调用逻辑-如触发条件

-语言原生类的调用逻辑-如 SoapClient

-语言自身的安全缺陷-如 CVE-2016-7124

#反序列化课程点：

-PHP&Java&Python

序列化：对象转换为数组或字符串等格式

反序列化：将数组或字符串等格式转换成对象

serialize()　　//将一个对象转换成一个字符串

unserialize()　//将字符串还原成一个对象

#PHP 反序列化漏洞

原理：未对用户输入的序列化字符串进行检测，导致攻击者可以控制反序列化过程，从而导致代码执行，SQL 注入，目录遍历等不可控后果。在反序列化的过程中自动触发了某些魔术方法。当进行反序列化的时候就有可能会触发对象中的一些魔术方法。

#魔术方法利用点分析：

触发：unserialize 函数的变量可控，文件中存在可利用的类，类中有魔术方法：

__construct(): //构造函数，当对象 new 的时候会自动调用

__destruct(): //析构函数当对象被销毁时会被自动调用

__wakeup(): //unserialize()时会被自动调用

__invoke(): //当尝试以调用函数的方法调用一个对象时，会被自动调用

__call(): //在对象上下文中调用不可访问的方法时触发

__callStatci(): //在静态上下文中调用不可访问的方法时触发

__get(): //用于从不可访问的属性读取数据

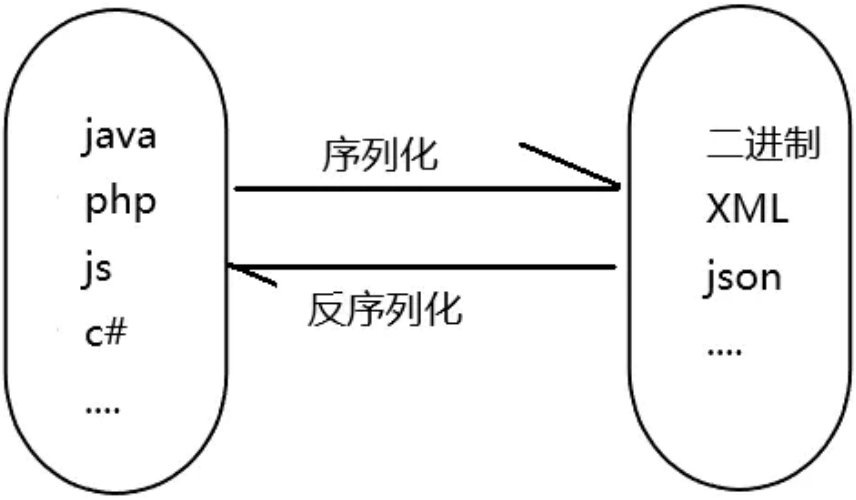
__set(): //用于将数据写入不可访问的属性

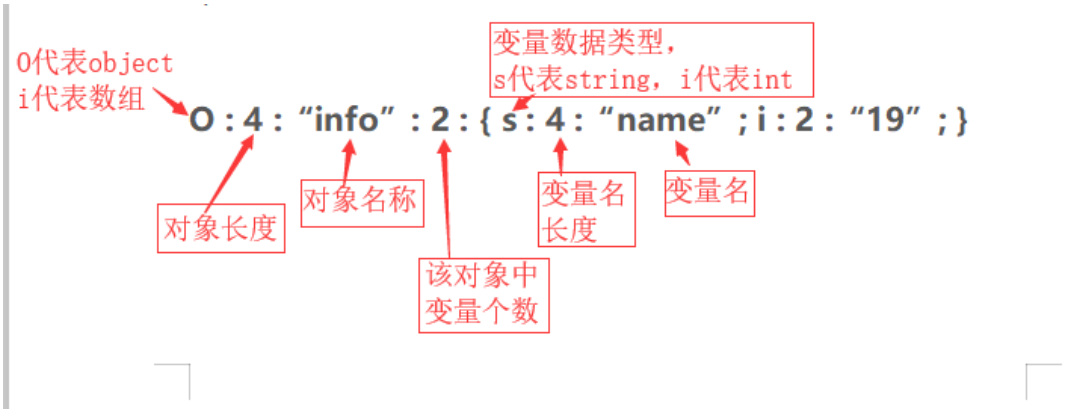
__isset(): //在不可访问的属性上调用 isset()或 empty()触发

__unset(): //在不可访问的属性上使用 unset()时触发

__toString(): //把类当作字符串使用时触发

__sleep(): //serialize()函数会检查类中是否存在一个魔术方法__sleep() 如果存在，该方法会被优先调用





演示案例：

- 反序列化-魔术方法&漏洞引发&变量修改等
- CTFSHOW-关卡 254 到 260-原生类&POP 构造
- CMS 代码审计-Typecho 反序列化&魔术方法逻辑

```
#反序列化-魔术方法&漏洞引发&变量修改等
<?php
//序列化&反序列化
class demotest{
    public $name='xiaodi';
    public $sex='man';
    public $age='29';
}
$example=new demotest();
$s=serialize($example);//序列化
$u=unserialize($s);//反序列化
echo $s.'<br>';
var_dump($u);
echo '<br>';
//O:8:"demotest":3:{s:4:"name";s:6:"xiaodi";s:3:"sex";s:3:"man";s
:3:"age";s:2:"29";}
//object(demotest)#2 (3) { ["name"]=> string(6) "xiaodi"
["sex"]=> string(3) "man" ["age"]=> string(2) "29" }

//安全问题
class A{
    public $var='echo test';
     public function test(){
         echo $this->var;
     }
    public function __destruct(){
         echo 'x'.'<br>';
     }
    public function __construct(){
        echo '__construct'.'<br>';
    }
    public function __toString(){
        return '__toString'.'<br>';
    }
}
//无需函数，创建对象触发魔术方法
//$a=new A();//触发__construct
//$a->test();//触发 test
//echo $a;//触发__toString
//触发__destruct
echo serialize($a);
$t=unserialize('O:1:"A":1:{s:3:"var";s:9:"echo test";}');
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址