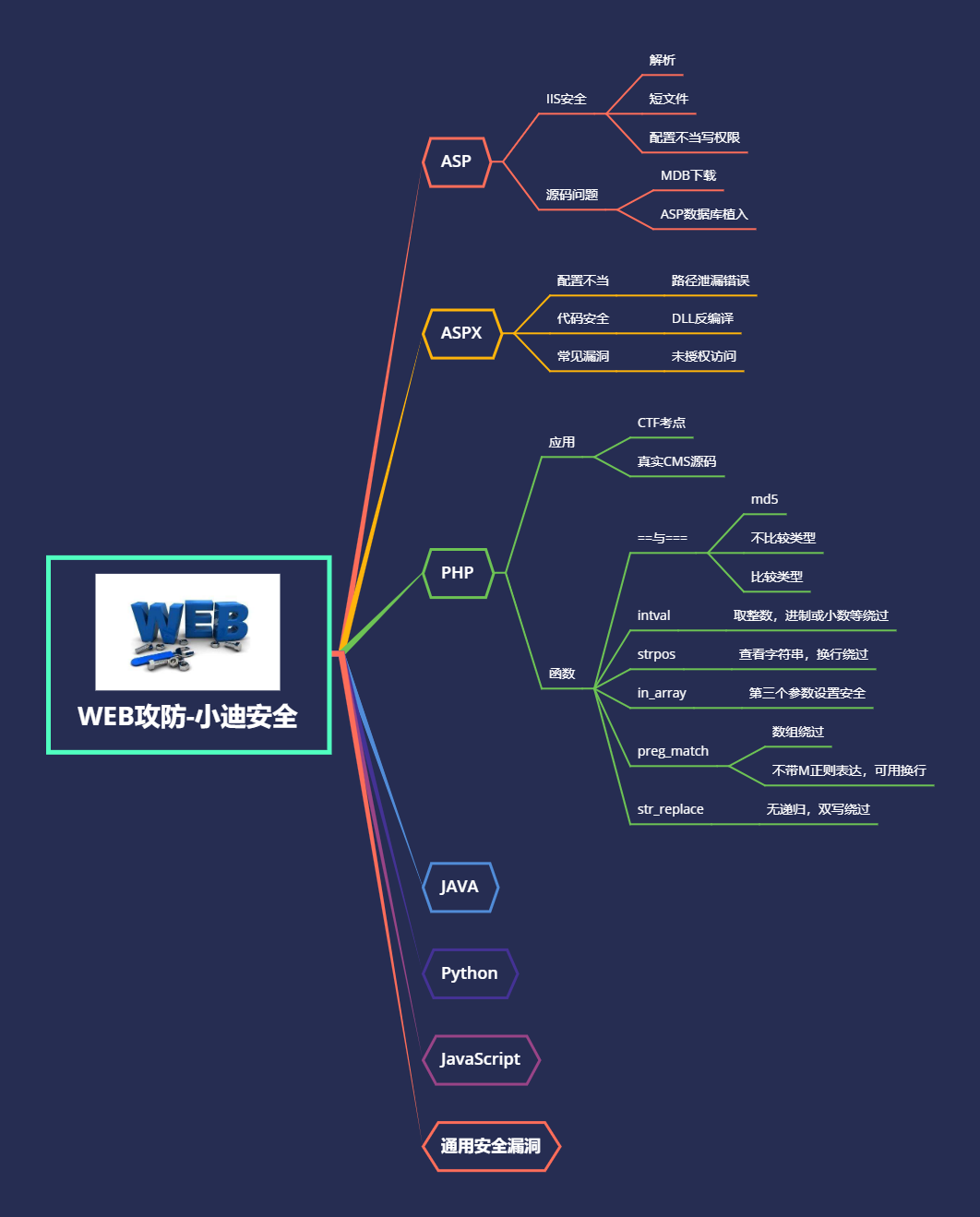
WEB攻防-PHP特性&缺陷对比函数&CTF考点&CMS审计实例



#知识点：

1、过滤函数缺陷绕过

2、CTF考点与代码审计

#详细点：

==与===

md5

intval

strpos

in\_array

preg\_match

str\_replace

<?php

header("Content-Type:text/html;charset=utf-8");

$flag='xiaodi ai chi xigua!';

//1、== ===缺陷绕过 == 弱类型对比 ===还会比较类型

$a=1;

if($a==$\_GET['x']){

echo $flag;

}

//1.0 +1 1a

$a='1';

if($a===$\_GET['y']){

echo $flag;

}

//1.0 +1等

//2、MD5函数缺陷绕过 ==弱对比 ===强类型对比

if($\_GET['name'] != $\_GET['password']){

if(MD5($\_GET['name']) == MD5($\_GET['password'])){

echo $flag;

}

echo '?';

}

//==

//echo MD5('QNKCDZO');

//echo MD5('240610708');

//===

//name[]=1&password[]=2

//3、intval缺陷绕过

$i='666';

$ii=$\_GET['n'];

if(intval($ii==$i)){

echo $flag;

}

// 666.0 +666

$i='666';

$ii=$\_GET['n'];

if(intval($ii==$i,0)){

echo $flag;

}

//0x29a

//4、对于strpos()函数，我们可以利用换行进行绕过（%0a）

$i='666';

$ii=$\_GET['h'];

if(strpos($ii==$i,"0")){

echo $flag;

}

//?num=%0a666

//5、in\_array第三个参数安全

$whitelist = [1,2,3];

$page=$\_GET['i'];

if (in\_array($page, $whitelist)) {

echo "yes";

}

//?i=1ex

//6、preg\_match只能处理字符串，如果不按规定传一个字符串，通常是传一个数组进去，这样就会报错

if(isset($\_GET['num'])){

$num = $\_GET['num'];

if(preg\_match("/[0-9]/", $num)){

die("no no no!");

}

if(intval($num)){

echo $flag;

}

}

//?num[]=1

//7、str\_replace无法迭代过滤

$sql=$\_GET['s'];

$sql=str\_replace('select','',$sql);

echo $sql;

//?s=sselectelect

?>

演示案例：

* 原理-缺陷函数-使用讲解-本地
* 实践-CTFShow-PHP特性-89关卡
* 实践-代码审计-过滤缺陷-文件读取

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)