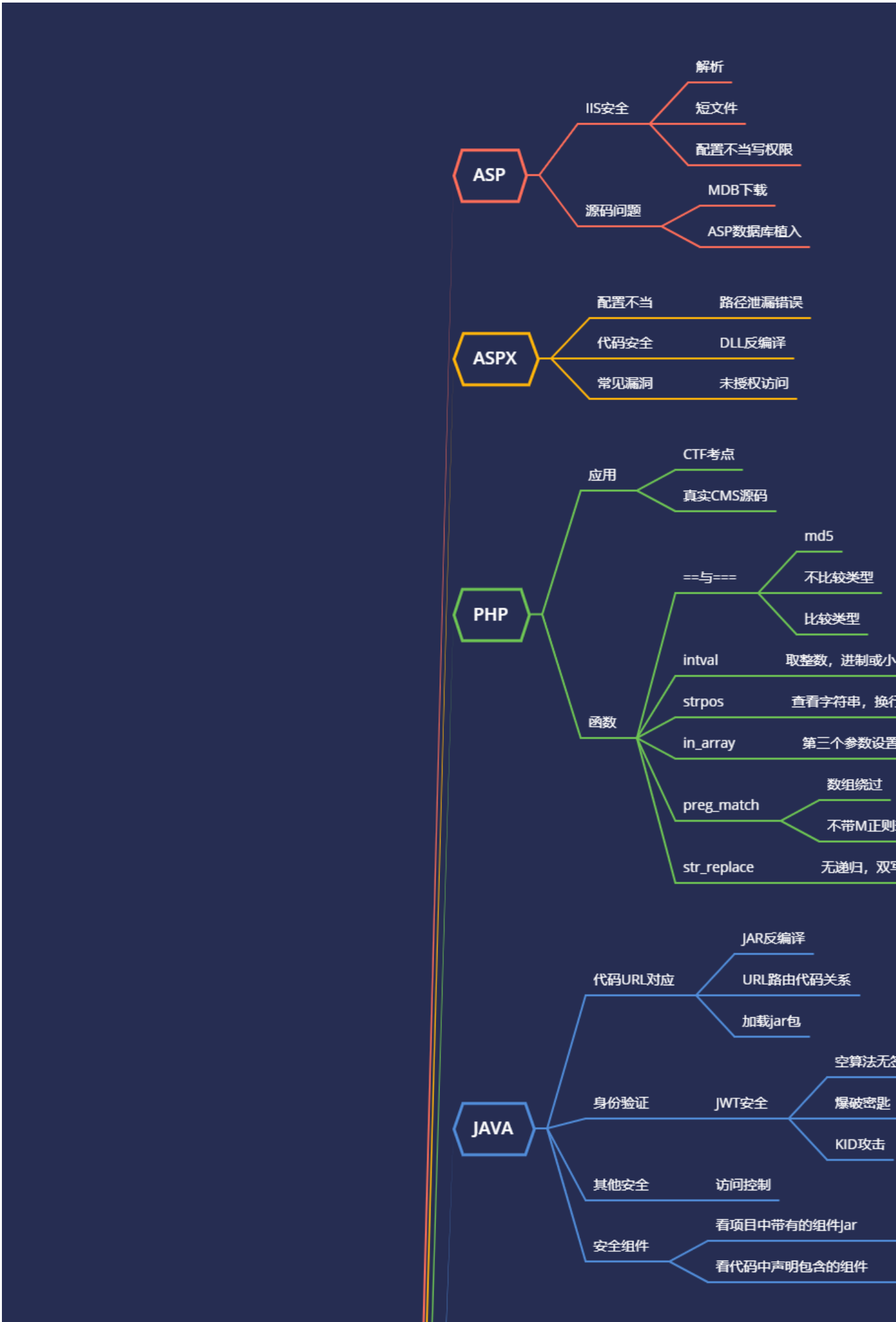
WEB 攻防-通用漏洞&XSS 跨站&反射&存储&DOM&盲打&劫持


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
空算法无签
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-原理&攻击&分类等

2、XSS 跨站-反射型&存储型&DOM 型等

3、XSS 跨站-攻击手法&劫持&盗取凭据等

4、XSS 跨站-攻击项目&XSS 平台&Beef-XSS

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；

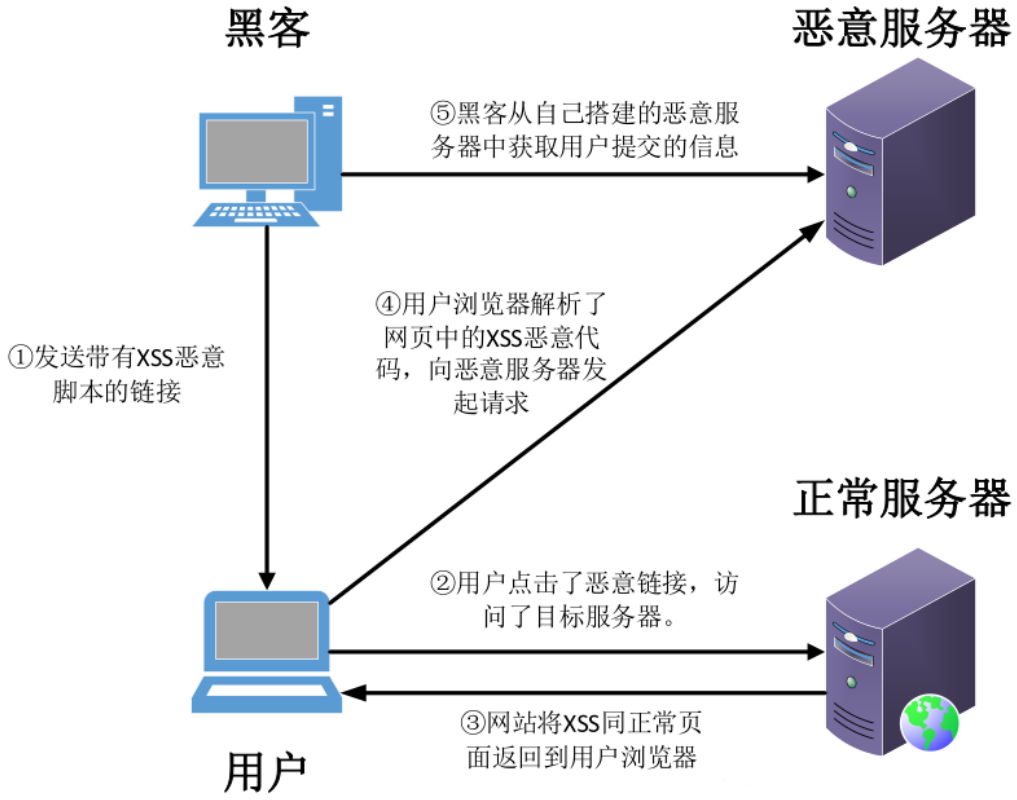
窃取用户 cookies 资料，从而获取用户隐私信息，或利用用户身份对网站执行操作；

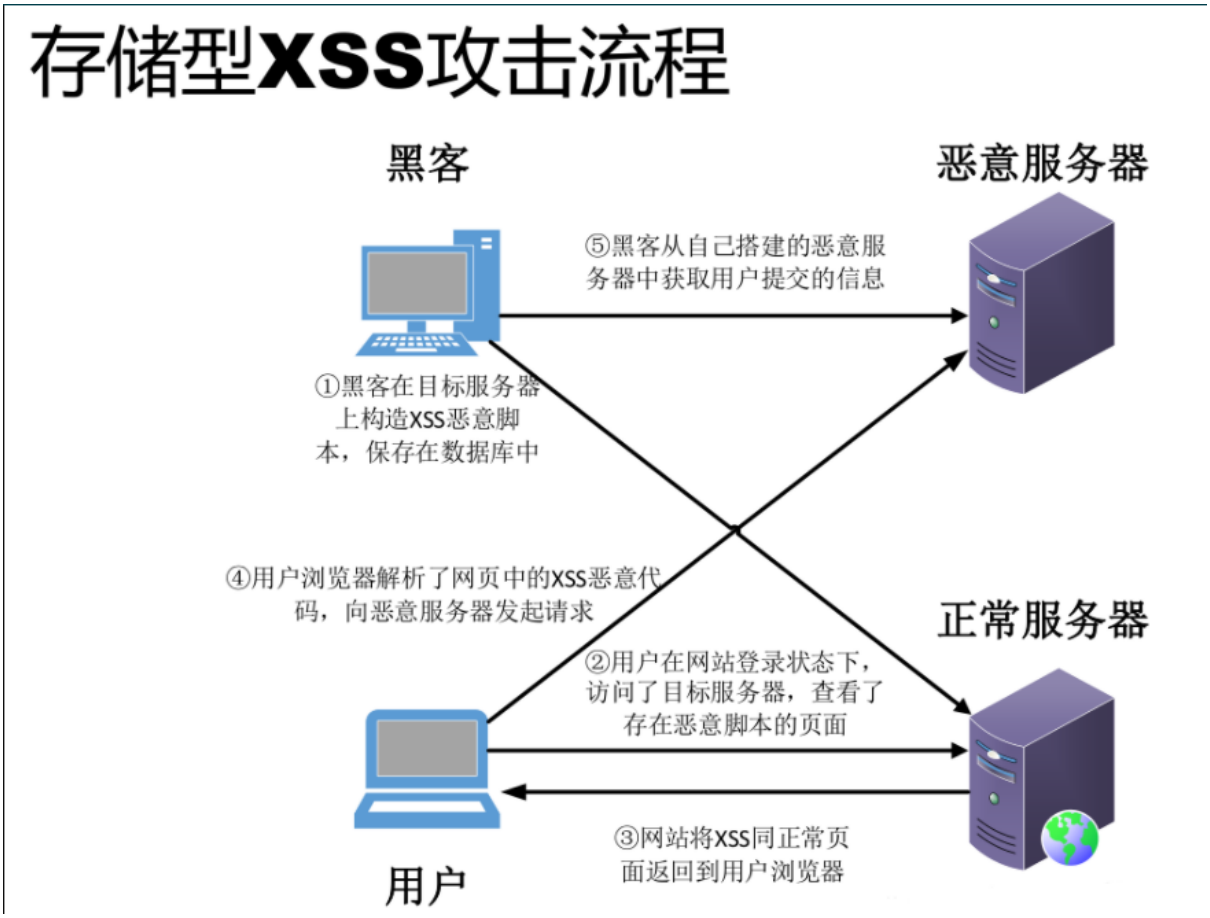
劫持用户（浏览器）会话，从而执行任意操作，例如非法转账、发表日志、邮件等；

强制弹出广告页面、刷流量等；

网页挂马

反射型XSS攻击流程


黑客
恶意服务器
⑤黑客从自己搭建的恶意服务器中获取用户提交的信息
①发送带有XSS恶意脚本的链接
④用户浏览器解析了网页中的XSS恶意代码，向恶意服务器发起请求
正常服务器
②用户点击了恶意链接，访问了目标服务器。
③网站将XSS同正常页面返回到用户浏览器
用户



演示案例：

- XSS 跨站-原理&分类&手法&探针
- 反射型实例-UA 查询平台数据输出
- 存储型实例-订单系统 CMS 权限获取
- DOM 型实例-EmpireCMS 前端页面审计
- XSS 利用环境-XSS 平台&Beef-XSS 项目

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
