"Face the challenge,Embrace the best practice"

EISS－2019
企业信息安全峰会
之深圳站

2019.8.16

自动化漏洞扫描系统开发和应用

李斌

系统建设背景

- 互联网应用系统大量使用开源软件和应用组件，且系统迭代快，可能存在各种安全漏洞，依靠手工检测需要投入大量人力。

- 通过建设自动化漏洞扫描系统，实现安全资产统一管理、漏洞自动化检测和安全漏洞生命周期管理，提升漏洞发现效率和能力，降低漏洞被利用风险。

系统建设目标

安全资产管理

- ✓ IP和端口
- ✓ 中间件及版本
- ✓ 组件库及版本
- ✓ 数据库
- ✓ 进程
- ✓ 运行用户
- ✓ 域名和URL

漏洞自动化扫描

- ✓ 端口开放
- ✓ 系统和中间件漏洞
- ✓ 弱口令、未授权访问
- ✓ Web安全漏洞

漏洞生命周期管理

- ✓ 漏洞确认
- ✓ 漏洞复核
- ✓ 漏洞跟踪和管理
- ✓ 统计和报表

系统功能架构

- 安全资产管理模块
- 漏洞扫描模块
- 漏洞管理模块

系统开发和设计思路

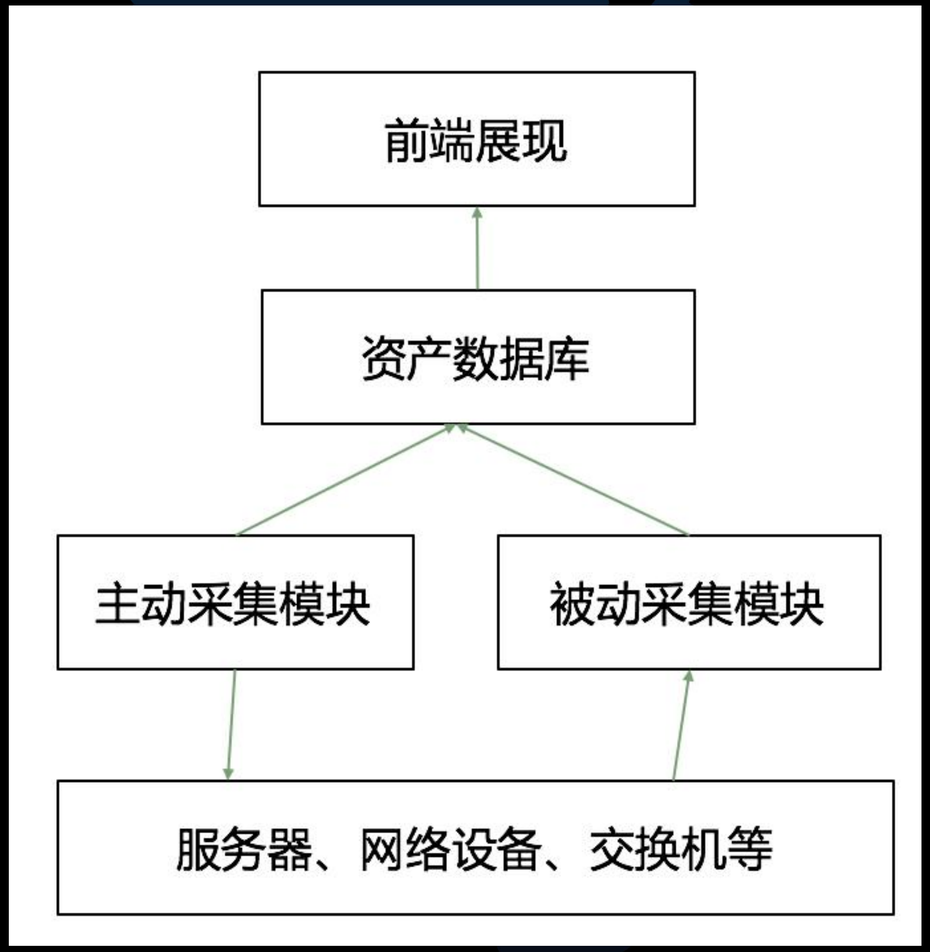
1、技术和开发语言

- ✓ Python3（后台）
- ✓ Django（Web前端和交互）
- ✓ MySQL（数据库）

2、设计思路

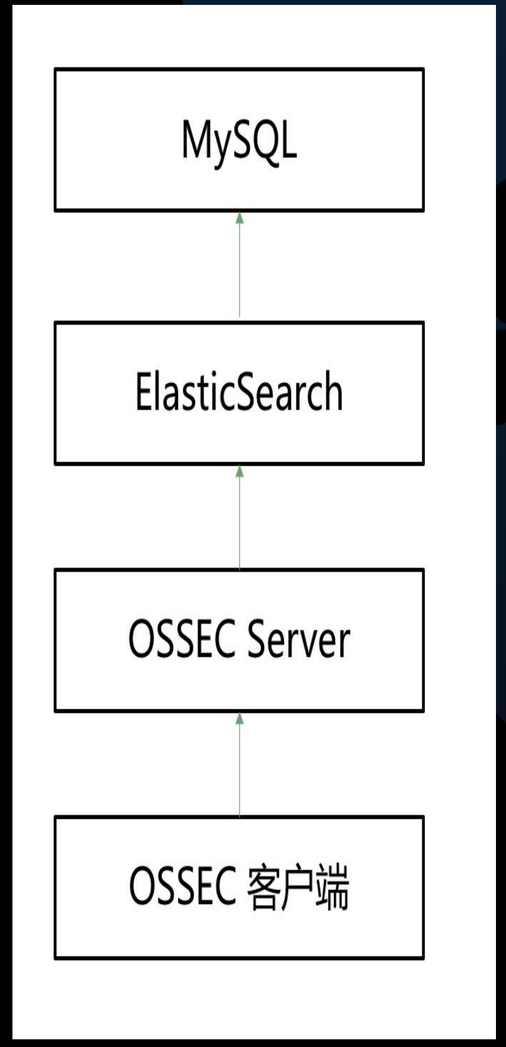
- ✓ 重度资产管理，被动+主动收集
- ✓ 尽量使用成熟开源组件和漏洞扫描模块进行二次开发
- ✓ 架构需有良好的扩展性
- ✓ 考虑POC和漏洞库可维护性

安全资产管理系统



- 被动为主、主动为辅
- 全网覆盖
- 持续更新

安全资产管理-被动采集模块



利用Agent执行shell命令取服务器上资产信息：

- ✓ TCP监听端口、进程ID和进程名
- ✓ 进程运行用户、进程运行命令
- ✓ 所有部署的应用程序（微服务列表）
- ✓ 服务器上用户列表
- ✓ 服务器上类库，主要是jar包及版本（依赖标准化路径）

选择	ID	IP地址	端口	端口名称	更新时间
☐	47174874	1[redacted]10	10201	nginx	2019年6月27日 18:44
☐	47174859	1[redacted].10	8081	nginx	2019年6月27日 18:44
☐	47174860	1[redacted]10	8082	nginx	2019年6月27日 18:44
☐	47174868	1[redacted]10	8087	nginx	2019年6月27日 18:44
☐	47174869	1[redacted]10	8184	nginx	2019年6月27日 18:44
☐	47174861	1[redacted]10	8083	nginx	2019年6月27日 18:44
☐	47174865	10.[redacted]10	10100	nginx	2019年6月27日 18:44
☐	47174867	10.[redacted]10	22	sshd	2019年6月27日 18:44
☐	47174873	10.[redacted]10	8185	nginx	2019年6月27日 18:44

安全资产管理-主动采集模块

WINDOWS主机信息

Masscan
Nmap

URL列表

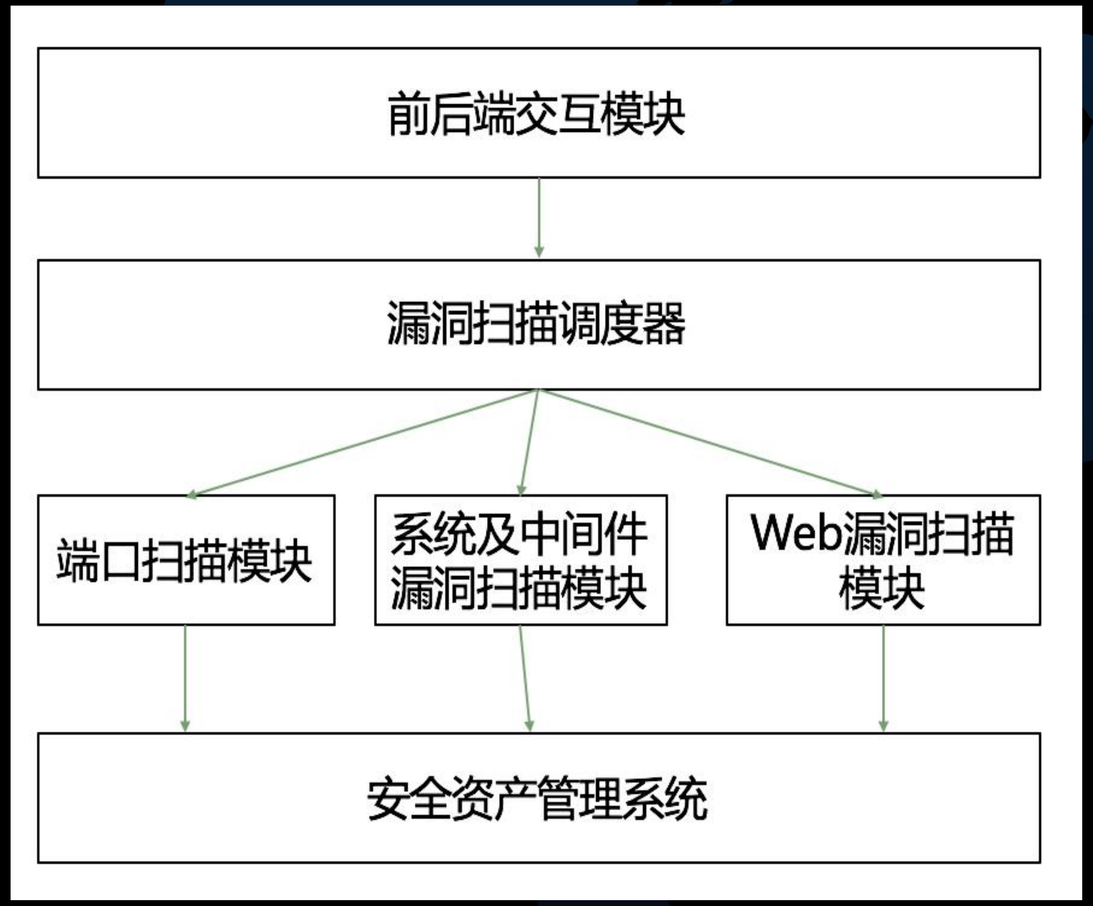
WIG
Accesslog

选择	ID	URL	名称	来源	Platform	Title
	587	http://10 2:81/	nginx	auto	nginx	
	588	http://10 :888/	nginx	auto	nginx 1	管理
	589	http://10 9220/	java	auto		
	590	http://10 32/	nginx	auto	PHP 7.0.20,nginx	Sig
	591	http://10. 21203/	nginx	auto	PHP 7.0.20,nginx	
	592	http://10 29092/		auto	an	
	593	http://10 80/	nginx	auto	PHP 7.0.20,nginx	
	594	http://10 8161/	java	auto	jett	Apache ActiveMQ
	595	http://10 :8162/	java	auto	jett	Apache ActiveMQ
	596	http://10. :8080/	java	auto	Tomca 5</title>	Apache Tomca
	597	http://10. 80/		auto	PHP 7.1.6,nginx	
	598	http://10 :1/		auto	PHP 7.1.6,nginx	台运营管理系统
	599	http://10 26:8161/	java	auto	jett	Apache ActiveMQ

特定组件和版本信息

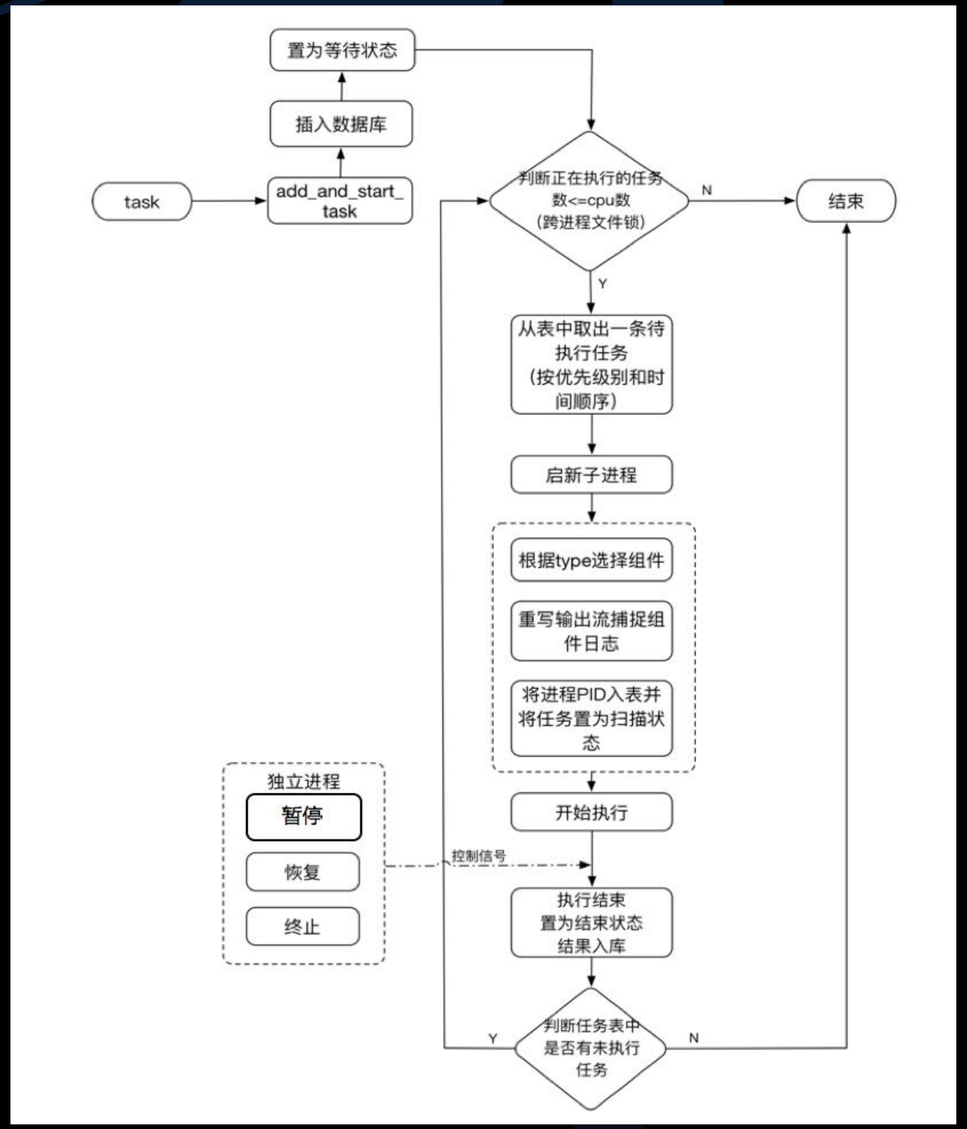
运维自动化平台API

漏洞扫描模块



- 调度器统一管理和调度扫描任务、管理扫描模块
- 扫描模块插拔式增加
- 安全资产管理系统提供输入源

漏洞扫描调度引擎



1、扫描模块注册

2、任务创建

- 任务名称
- 任务类型（调用哪个扫描模块）
- 扫描目标（可以是IP，或者是IP+端口，或者是URL等）
- 扫描参数（比如专门扫描SQL注入漏洞）

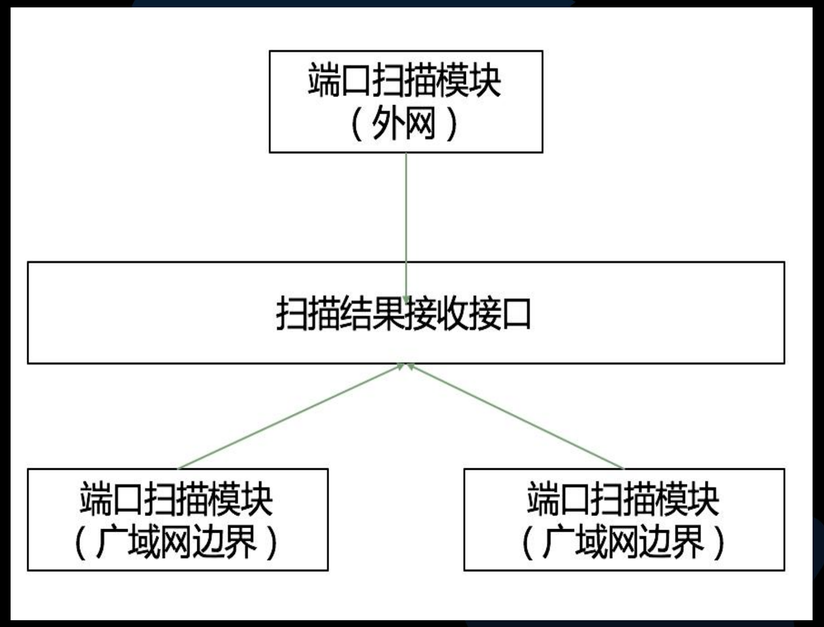
3、任务调度和管理

- 队列中、扫描中、扫描结束
- 终止、暂停、恢复
- 定时任务
- 完成扫描

4、结果解析入库

- 任务ID、标题、级别、类型
- 漏洞详情（建议为JSON格式，包括漏洞所有明细信息，如漏洞的IP、漏洞端口、探测方法、漏洞检测返回信息、漏洞CVE描述等，每种漏洞的详情可以不同）

边界端口开放扫描



1、端口扫描模块（外网）

用于扫描互联网对外开放IP和端口。

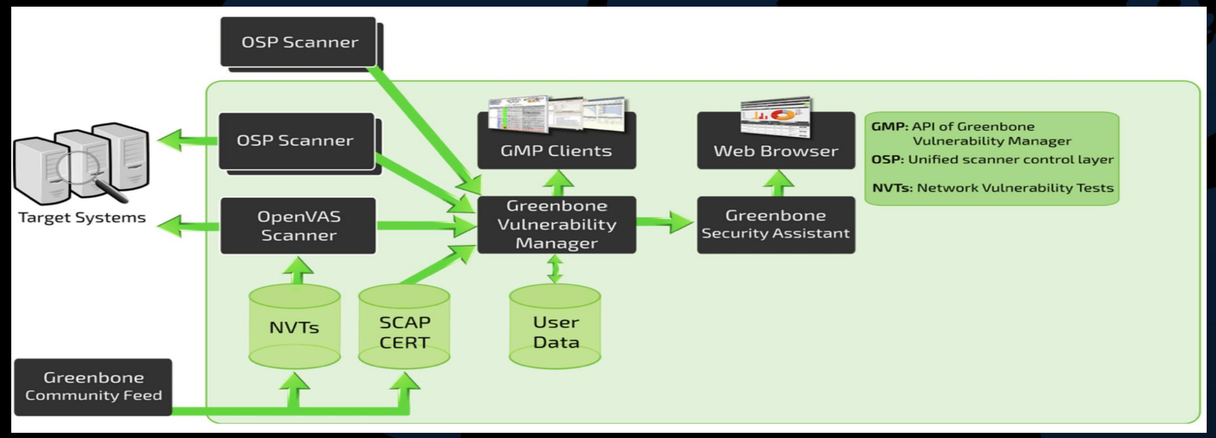
2、端口扫描模块（广域网边界）

用于扫描广域网边界开放IP和端口情况，如办公内网和IDC之间开放端口情况、外联区（专线、VPN）边界开放端口情况。

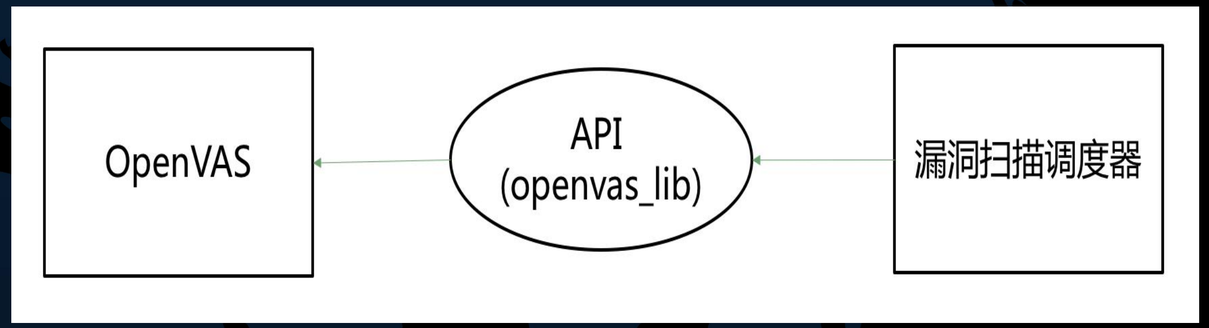
3、扫描结果接收接口

用于接收扫描结果，建议扫描结果为JSON格式，接收结果后入库。

系统漏洞扫描



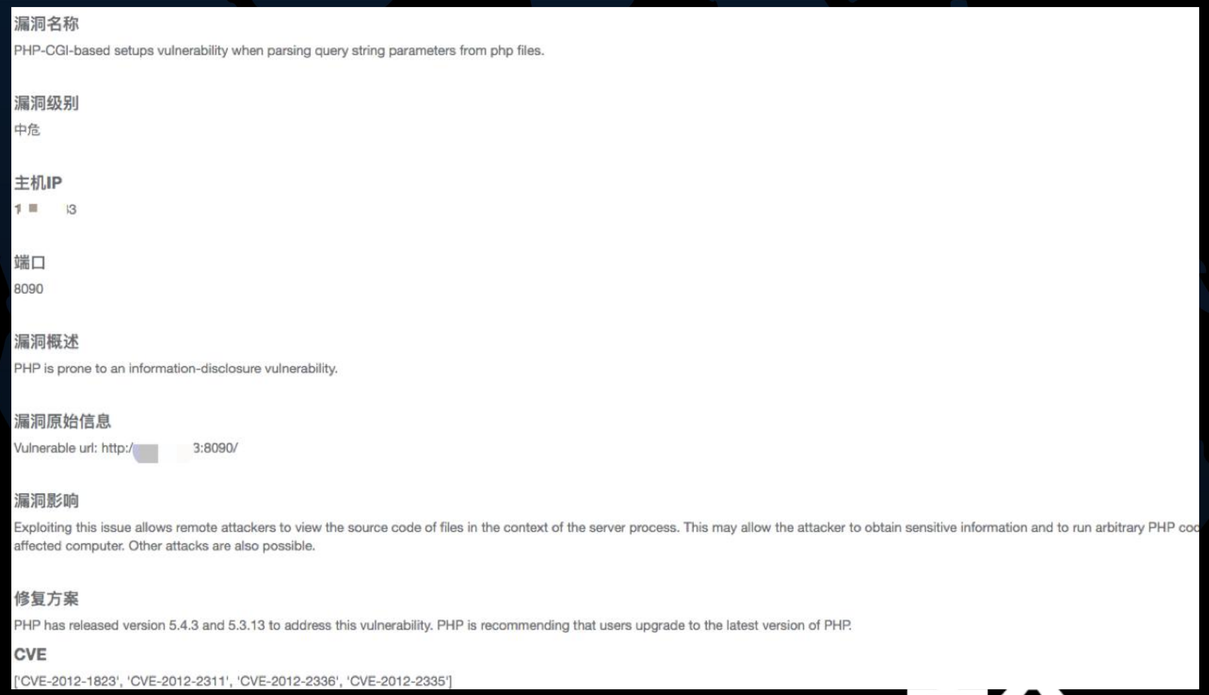
OpenVAS



1、Docker安装和部署

2、Openvas_lib库二次开发

- 任务终止功能
- 扫描结果字段格式化解析
- 扫描端口优化提升扫描效率



漏洞名称

PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

漏洞级别

中危

主机IP

端口

8090

漏洞概述

PHP is prone to an information-disclosure vulnerability.

漏洞原始信息

Vulnerable url: http:/ 3:8090/

漏洞影响

Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP coc affected computer. Other attacks are also possible.

修复方案

PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

CVE

['CVE-2012-1823', 'CVE-2012-2311', 'CVE-2012-2336', 'CVE-2012-2335']

中间件漏洞扫描

巡风系统-扫描模块

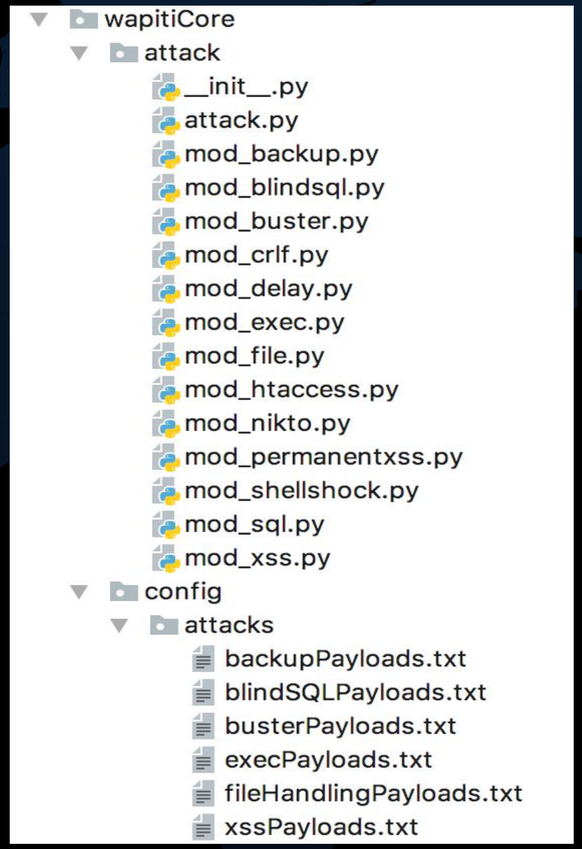
- ✓ vulscan.py
- ✓ Vuldb漏洞POC库
- ✓ 支持全模块或单独某个模块扫描
- ✓ 弱口令字典自定义

标题	类型	级别	详情
Redis弱口令	弱口令	高危	{"target": "1C :7510", "result": "未授权 "}
Redis弱口令	弱口令	高危	{"target": "1C :7514", "result": "未授权 "}
Redis弱口令	弱口令	高危	{"target": "10.0. 6:7610", "result": "未授 "}
Redis弱口令	弱口令	高危	{"target": "10 .16:7518", "result": "未授权访问"}
Redis弱口令	弱口令	高危	{"target": "10 .16:7619", "result": "未授 问"}
Redis弱口令	弱口令	高危	{"target": "10. 6:7504", "result": "未授权访问"}
Hadoop REST API未授权访问	未授权访问	高危	{"target": ["1C 2", "50070"], "result": "未授权访问"}

WEB漏洞扫描

Wapiti3.0

Wapiti是开源的Web应用漏洞扫描系统-黑盒漏洞扫描系统，通过爬取网页，获取网页结构、表单和参数输入点，通过注入payload检测是否存在安全漏洞。



主要功能如下：

- ✓ 文件包含
- ✓ 注入
- ✓ XSS
- ✓ 命令执行
- ✓ CRLF
- ✓ XXE
- ✓ SSRF
- ✓ 敏感信息泄露

二次开发和整合：

- 支持手动输入cookie
- 可选择单独模块或全扫描
- 扫描参数自定义（爬虫深度、代理等）
- 漏洞扫描结果解析

漏洞管理模块

1、漏洞管理功能：

- ✓ 用户管理、登录和权限管理
- ✓ 安全资产管理
- ✓ 漏洞扫描任务管理
- ✓ 漏洞扫描结果管理
- ✓ 统计、报表和导出功能

2、开发实现

- ✓ Django Web框架
- ✓ 任务输入和前后端交互
- ✓ 前端模块（Bootstrap、Jquery、Layui、Echarts）

漏洞管理系统应用实践

1、持续运营，确保资产库新鲜、全面

2、漏洞库持续更新、POC手动编写和更新

3、定期开展漏洞扫描，控制扫描强度

4、漏洞发现要从多方面入手，自动化扫描是其中重要一环

欢迎交流

“安全+”专注于信息安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，培养安全人才，提升行业的整体素质，助推安全生态圈的健康发展。

官方网站：www.anquanjia.net.cn

微信公众号：anquanplus