漏洞发现-Web 框架中间件&联动

&Goby&Afrog&Xray&Awvs&Vulmap

#知识点：

1、Burp 简单介绍&使用说明

2、Xray 简单介绍&使用说明

3、Awvs 简单介绍&使用说明

4、Goby 简单介绍&使用说明

5、Afrog 简单介绍&使用说明

6、Vulmap 简单介绍&使用说明

7、Pocassist 简单介绍&使用说明

8、掌握工具安装使用&原理&联动&适用

市面上有很多漏扫系统工具脚本，课程讲到的基本都是目前主流推荐的优秀项目！

具体项目：Burpsuite，Awvs，Xray，Goby，Afrog，Vulmap，Pocassist，Nessus，Nuclei，Pentestkit，Kunyu，BP 插件(HaE,ShiroScan.FastJsonScan,Log4j2Scan 等)等。

#章节点：

1、漏洞发现-Web&框架层面

2、漏洞发现-服务&中间件层面

3、漏洞发现-APP&小程序层面

4、漏洞发现-PC 操作系统层面

Acunetix 一款商业的 Web 漏洞扫描程序，它可以检查 Web 应用程序中的漏洞，如 SQL 注入、跨站脚本攻击、身份验证页上的弱口令长度等。它拥有一个操作方便的图形用户界面，并且能够创建专业级的 Web 站点安全审核报告。新版本集成了漏洞管理功能来扩展企业全面管理、优先级和控制漏洞威胁的能力。

Burp Suite 是用于攻击 web 应用程序的集成平台，包含了许多工具。Burp Suite 为这些工具设计了许多接口，以加快攻击应用程序的过程。所有工具都共享一个请求，并能处理对应的 HTTP 消息、持久性、认证、代理、日志、警报。

pocassist 是一个 Golang 编写的全新开源漏洞测试框架。实现对 poc 的在线编辑、管理、测试。如果你不想撸代码，又想实现 poc 的逻辑，又想在线对靶机快速测试，那就使用 pocassist 吧。完全兼容 xray，但又不仅仅是 xray。除了支持定义目录级漏洞 poc，还支持服务器级漏洞、参数级漏洞、url 级漏洞以及对页面内容检测，如果以上还不满足你的需求，还支持加载自定义脚本。

afrog 是一款性能卓越、快速稳定、PoC 可定制的漏洞扫描（挖洞）工具，PoC 涉及 CVE、CNVD、默认口令、信息泄露、指纹识别、未授权访问、任意文件读取、命令执行等多种漏洞类型，帮助网络安全从业者快速验证并及时修复漏洞。

演示案例：

- 某 APP-Web 扫描-常规&联动-Burp&Awvs&Xray
- Vulfocus-框架扫描-特定-Goby&Vulmap&Afrog&Pocassist
- 某资产特征-联动扫描-综合&调用-Goby&Awvs&Xray&Vulmap

项目资源：

https://www.ddosi.org/awvs14-6-log4j-rce/

https://github.com/chaitin/xray/releases

https://github.com/zan8in/afrog/releases

https://github.com/zhzyker/vulmap/releases

https://github.com/jweny/pocassist/releases

https://github.com/gobysec/Goby/releases

其他特扫：

1、GUI_TOOLS_V6.1_by 安全圈小王子--bugfixed

2、CMS 漏洞扫描器名称　支持的 CMS 平台

Droopescan　WordPress，Joomla，Drupal，Moodle，SilverStripe

CMSmap WordPress，Joomla，Drupal，Moodle

CMSeeK WordPress，Joomla，Drupal 等

WPXF　WordPress

WPScan WordPress

WPSeku WordPress

WPForce　WordPress

JoomScan　Joomla

JoomlaVS　Joomla

JScanner　Joomla

Drupwn Drupal

Typo3Scan Typo3

致远 OA 综合利用工具 https://github.com/Summer177/seeyon_exp

seeyon_exp

通达 OA 综合利用工具 https://github.com/xinyu2428/TDOA_RCE　TDOA_RCE

蓝凌 OA 漏洞利用工具/前台无条件 RCE/文件写入

https://github.com/yuanhaiGreg/LandrayExploit　LandrayExploit

泛微 OA 漏洞综合利用脚本 https://github.com/z1un/weaver_exp

weaver_exp

锐捷网络 EG 易网关 RCE 批量安全检测

https://github.com/Tas9er/EgGateWayGetShell EgGateWayGetShell

CMSmap 针对流行 CMS 进行安全扫描的工具

https://github.com/Dionach/CMSmap CMSmap

使用 Go 开发的 WordPress 漏洞扫描工具

https://github.com/blackbinn/wprecon wprecon

一个 Ruby 框架，旨在帮助对 WordPress 系统进行渗透测试

https://github.com/rastating/wordpress-exploit-framework

wordpress-exploit-framework

WPScan WordPress 安全扫描器 https://github.com/wpscanteam/wpscan

wpscan

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址