安全资源整理

转载

dicewcj953644 于 2017-11-20 09:37:00 发布 120 收藏
文章标签： 人工智能 php 爬虫
原文链接：http://www.cnblogs.com/maplered/p/7864943.html

一、内网资料

https://github.com/l3m0n/pentest_study

二、安全脑图

https://github.com/phith0n/Mind-Map

三、sql注入学习

https://github.com/Audi-1/sqli-labs

四、各类扫描器

子域名扫描

https://github.com/lijiejie/subDomainsBrute

迷你信息泄露扫描

https://github.com/lijiejie/BBScan

五、web工具

webshell：https://github.com/tennc/webshell

web渗透小工具大合集： https://github.com/rootphantomer/hack_tools_for_me

六、python security教程

python security教程

https://github.com/smartFlash/pySecurity

mobile-security-wiki

https://github.com/exploitprotocol/mobile-security-wiki

书籍《reverse-engineering-for-beginners》

https://github.com/veficos/reverse-engineering-for-beginners

一些信息安全标准及设备配置

https://github.com/luyg24/IT_security

APT相关笔记

https://github.com/kbandla/APTnotes

Kcon资料

https://github.com/knownsec/KCon

ctf及黑客资源合集

https://github.com/bt3gl/My-Gray-Hacker-Resources

ctf和安全工具大合集

https://github.com/zardus/ctf-tools

《DO NOT FUCK WITH A HACKER》

https://github.com/citypw/DNFWAH

各类CTF资源

近年ctf writeup大全

https://github.com/ctfs/write-ups-2016

https://github.com/ctfs/write-ups-2015

https://github.com/ctfs/write-ups-2014

fbctf竞赛平台Demo

https://github.com/facebook/fbctf

ctf Resources

https://github.com/ctfs/resources

各类编程资源

大礼包（什么都有）

https://github.com/bayandin/awesome-awesomeness

bash-handbook

https://github.com/denysdovhan/bash-handbook

git学习资料

https://github.com/xirong/my-git

安卓开源代码解析

https://github.com/android-cn/android-open-project-analysis

python框架，库，资源大合集

https://github.com/vinta/awesome-python

JS 正则表达式库（用于简化构造复杂的JS正则表达式）

https://github.com/VerbalExpressions/JSVerbalExpressions

Python

python资源大全

https://github.com/jobbole/awesome-python-cn

python 正则表达式库（用于简化构造复杂的python正则表达式）

https://github.com/VerbalExpressions/PythonVerbalExpressions

python任务管理以及命令执行库

https://github.com/pyinvoke/invoke

python exe打包库

https://github.com/pyinstaller/pyinstaller

py3 爬虫框架

https://github.com/orf/cyborg

一个提供底层接口数据包编程和网络协议支持的python库

https://github.com/CoreSecurity/impacket

python requests 库

https://github.com/kennethreitz/requests

python 实用工具合集

https://github.com/mahmoud/boltons

python爬虫系统

https://github.com/binux/pyspider

ctf向 python工具包

https://github.com/P1kachu/v0lt

以下内容来自：https://github.com/We5ter/Scanners-Box/blob/master/README_CN.md

子域名枚举类

https://github.com/lijiejie/subDomainsBrute (经典的子域名爆破枚举脚本)

https://github.com/ring04h/wydomain (子域名字典穷举)

https://github.com/le4f/dnsmaper (子域名枚举与地图标记)

https://github.com/0xbug/orangescan (在线子域名信息收集工具)

https://github.com/TheRook/subbrute （根据DNS记录查询子域名)

https://github.com/We5ter/GoogleSSLdomainFinder (基于谷歌SSL透明证书的子域名查询脚本)

https://github.com/mandatoryprogrammer/cloudflare_enum （使用CloudFlare进行子域名枚举的脚本）

https://github.com/18F/domain-scan (A domain scanner）

https://github.com/Evi1CLAY/Cool ... Python/DomainSeeker（多方式收集目标子域名信息）

数据库漏洞扫描类

https://github.com/0xbug/SQLiScanner (一款基于SQLMAP和Charles的被动SQL注入漏洞扫描工具)

https://github.com/stamparm/DSSS (99行代码实现的sql注入漏洞扫描器)

https://github.com/LoRexxar/Feigong（针对各种情况自由变化的MySQL注入脚本）

https://github.com/youngyangyang04/NoSQLAttack (一款针对mongoDB的攻击工具)

https://github.com/Neohapsis/bbqsql（SQL盲注利用框架）

https://github.com/NetSPI/PowerUpSQL（攻击SQLSERVER的Powershell脚本框架）

弱口令或信息泄漏扫描类

https://github.com/lijiejie/htpwdScan (一个简单的HTTP暴力破解、撞库攻击脚本)

https://github.com/lijiejie/BBScan (一个迷你的信息泄漏批量扫描脚本)

https://github.com/lijiejie/GitHack (.git文件夹泄漏利用工具)

https://github.com/wilson9x1/fenghuangscanner_v3 (端口及弱口令检测)

https://github.com/ysrc/F-Scrack (对各类服务进行弱口令检测的脚本)

https://github.com/Mebus/cupp （根据用户习惯生成弱口令探测字典脚本）

https://github.com/RicterZ/genpAss （中国特色的弱口令生成器）

https://github.com/netxfly/crack_ssh （go写的协程版的ssh\redis\mongodb弱口令破解工具）

物联网设备扫描

https://github.com/rapid7/IoTSeeker （物联网设备默认密码扫描检测工具)

https://github.com/shodan-labs/iotdb (使用nmap扫描IoT设备)

xss扫描器

https://github.com/shawarkhanethicalhacker/BruteXSS （Cross-Site Scripting Bruteforcer）

https://github.com/1N3/XSSTracer (A small python script to check for Cross-Site Tracing)

https://github.com/0x584A/fuzzXssPHP (PHP版本的反射型xss扫描)

https://github.com/chuhades/xss_scan (批量扫描xss的python脚本）

企业网络自检

https://github.com/sowish/LNScan （详细的内部网络信息扫描器）

https://github.com/ysrc/xunfeng (网络资产识别引擎，漏洞检测引擎）

https://github.com/SkyLined/LocalNetworkScanner (javascript实现的本地网络扫描器)

https://github.com/laramies/theHarvester （企业被搜索引擎收录敏感资产信息监控脚本：员工邮箱、子域名、Hosts）

https://github.com/x0day/Multisearch-v2 (bing、google、360、zoomeye等搜索引擎聚合搜索，可用于发现企业被搜索引擎收录的敏感资产信息）

webshell检测

https://github.com/We5ter/Scanners-Box/tree/master/Find_webshell/ （php后门检测，脚本较简单，因此存在误报高和效率低下的问题）

https://github.com/yassineaddi/BackdoorMan （A toolkit find malicious, hidden and suspicious PHP scripts and shells in a chosen destination）

内网渗透

https://github.com/0xwindows/VulScritp （企业内网渗透脚本，包括banner扫描、端口扫描；phpmyadmin、jenkins等通用漏洞利用等）

https://github.com/lcatro/network_backdoor_scanner（基于网络流量的内网探测框架）

https://github.com/fdiskyou/hunter（调用 Windows API 枚举用户登录信息）

中间件扫描、指纹识别类

https://github.com/ring04h/wyportmap (目标端口扫描+系统服务指纹识别)

https://github.com/ring04h/weakfilescan (动态多线程敏感信息泄露检测工具)

https://github.com/EnableSecurity/wafw00f (WAF产品指纹识别)

https://github.com/rbsec/sslscan （ssl类型识别）

https://github.com/urbanadventurer/whatweb (web指纹识别)

https://github.com/tanjiti/FingerPrint (web应用指纹识别)

https://github.com/nanshihui/Scan-T （网络爬虫式指纹识别）

https://github.com/OffensivePython/Nscan (a fast Network scanner inspired by Masscan and Zmap)

https://github.com/ywolf/F-NAScan (网络资产信息扫描, ICMP存活探测,端口扫描，端口指纹服务识别）

https://github.com/ywolf/F-MiddlewareScan （中间件扫描）

https://github.com/maurosoria/dirsearch (Web path scanner)

https://github.com/x0day/bannerscan （C段Banner与路径扫描）

https://github.com/RASSec/RAScan (端口服务扫描)

https://github.com/3xp10it/bypass_waf （waf自动暴破）

https://github.com/3xp10it/mytools/blob/master/xcdn.py（获取cdn背后的真实ip）

https://github.com/Xyntax/BingC（基于Bing搜索引擎的C段/旁站查询，多线程，支持API）

https://github.com/Xyntax/DirBrute（多线程WEB目录爆破工具）

https://github.com/zer0h/httpscan（一个爬虫式的网段Web主机发现小工具）

https://github.com/lietdai/doom（thorn上实现的分布式任务分发的ip端口漏洞扫描器）

专用扫描器

https://github.com/blackye/Jenkins (Jenkins漏洞探测、用户抓取爆破)

https://github.com/code-scan/dzscan (discuz扫描)

https://github.com/chuhades/CMS-Exploit-Framework (CMS攻击框架)

https://github.com/lijiejie/IIS_shortname_Scanner (an IIS shortname Scanner)

https://github.com/We5ter/Scanne ... ter/FlashScanner.pl (flashxss扫描)

https://github.com/coffeehb/SSTIF（一个Fuzzing服务器端模板注入漏洞的半自动化工具）

无线网络

https://github.com/savio-code/fern-wifi-cracker/ (无线安全审计工具)

https://github.com/m4n3dw0lf/PytheM（Python网络/渗透测试工具）

https://github.com/P0cL4bs/WiFi-Pumpkin（无线安全渗透测试套件）

综合类

https://github.com/az0ne/AZScanner (自动漏洞扫描器，子域名爆破，端口扫描，目录爆破，常用框架漏洞检测)

https://github.com/blackye/lalascan (自主开发的分布式web漏洞扫描框架，集合owasp top10漏洞扫描和边界资产发现能力)

https://github.com/blackye/BkScanner (BkScanner 分布式、插件化web漏洞扫描器)

https://github.com/ysrc/GourdScanV2 （被动式漏洞扫描)

https://github.com/alpha1e0/pentestdb (WEB渗透测试数据库)

https://github.com/netxfly/passive_scan (基于http代理的web漏洞扫描器)

https://github.com/1N3/Sn1per (自动化扫描器，包括中间件扫描以及设备指纹识别)

https://github.com/RASSec/pentestEr_Fully-automatic-scanner （定向全自动化渗透测试工具）

https://github.com/3xp10it/3xp10it （3xp10it自动化渗透测试框架）

https://github.com/Lcys/lcyscan（python插件化漏洞扫描器）

https://github.com/Xyntax/POC-T（渗透测试插件化并发框架）

CTF平台

http://www.shiyanbar.com/

http://oj.xctf.org.cn/

http://ctf.bugku.com/

http://rookiehacker.org/

转载于:https://www.cnblogs.com/maplered/p/7864943.html