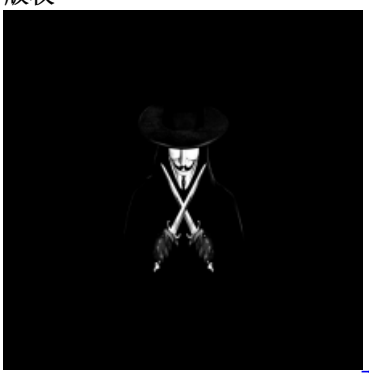
渗透测试学习工具

转载

北岸冷若冰霜 于 2020-10-27 20:53:42 发布 968 收藏 8
分类专栏： 安全 文章标签： 安全
原文链接：https://www.cnblogs.com/BOHB-yunying/p/11856178.html



原文作者：yunying
原文地址：github渗透测试工具库

声明：仅供学习交流使用！！！

导航

1.前言

今天看到一个博客里有这个置顶的工具清单，但是发现这些都是很早以前就有文章发出来的，我爬下来后一直放在txt里吃土。这里一起放出来。

2.漏洞练习平台

WebGoat漏洞练习平台：
https://github.com/WebGoat/WebGoat

webgoat-legacy漏洞练习平台:
https://github.com/WebGoat/WebGoat-Legacy

zvuldirll漏洞练习平台：
https://github.com/710leo/ZVulDrill

vulapps漏洞练习平台：
https://github.com/Medicean/VulApps

dvwa漏洞练习平台：
https://github.com/RandomStorm/DVWA

数据库注入练习平台 ：
https://github.com/Audi-1/sqli-labs

用node编写的漏洞练习平台，like OWASP NodeGoat：
https://github.com/cr0hn/vulnerable-node

Ruby编写的一款工具，生成含漏洞的虚拟机：
https://github.com/cliffe/secgen

3.花式扫描器

Nmap端口扫描器：
https://github.com/nmap/nmap

本地网络扫描器：
https://github.com/SkyLined/LocalNetworkScanner

子域名扫描器：
https://github.com/lijiejie/subDomainsBrute
https://github.com/aboul3la/Sublist3r
https://github.com/TheRook/subbrute
https://github.com/infosec-au/altdns

linux漏洞扫描：
https://github.com/future-architect/vuls

基于端口扫描以及关联CVE:
https://github.com/m0nad/HellRaiser

漏洞路由扫描器：
https://github.com/jh00nbr/Routerhunter-2.0

迷你批量信息泄漏扫描脚本：
https://github.com/lijiejie/BBScan

Waf类型检测工具：
https://github.com/EnableSecurity/wafw00f

服务器端口弱口令扫描器：
https://github.com/wilson9x1/fenghuangscanner_v3

Fox-scan扫描器：
https://github.com/fengxuangit/Fox-scan/

4.信息搜集工具

社工收集器：
https://github.com/n0tr00t/Sreg

Github信息搜集：
https://github.com/sea-god/gitscan

github Repo信息搜集工具：
https://github.com/metac0rtex/GitHarvester

信息探测及扫描工具：
https://github.com/darryllane/Bluto

内部网络信息扫描器：
https://github.com/sowish/LNScan

远程桌面登录扫描器：
https://github.com/linuz/Sticky-Keys-Slayer

网络基础设施渗透工具
https://github.com/SECFORCE/sparta

SNMAP密码破解:
https://github.com/SECFORCE/SNMP-Brute

5.WEB

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

渗透以及web攻击脚本：
https://github.com/brianwrf/hackUtils

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

XSS数据接收平台：
https://github.com/firesunCN/BlueLotus_XSSReceiver

XSS与CSRF工具：
https://github.com/evilcos/xssor

xss多功能扫描器：
https://github.com/shawarkhanethicalhacker/BruteXSS

web漏洞扫描器:
https://github.com/andresriancho/w3af

WEB漏洞扫描器：
https://github.com/sullo/nikto

渗透常用小工具包：
https://github.com/leonteale/pentestpackage

web目录扫描器:
https://github.com/maurosoria/dirsearch

web向命令注入检测工具：
https://github.com/stasinopoulos/commix

自动化SQL注入检查工具：
https://github.com/epinna/tplmap

SSL扫描器：
https://github.com/rbsec/sslscan

安全工具集合：
https://github.com/codejanus/ToolSuite

apache日志分析器：
https://github.com/mthbernardes/ARTLAS

php代码审计工具：
https://github.com/pwnsdx/BadCode

web指纹识别扫描：
https://github.com/urbanadventurer/whatweb

检查网站恶意攻击：
https://github.com/ciscocsirt/malspider

wordprees漏洞扫描器：
https://github.com/wpscanteam/wpscan

固件漏洞扫描器：
https://github.com/misterch0c/firminator_backend

数据库注入工具
https://github.com/sqlmapproject/sqlmap

Web代理：
https://github.com/zt2/sqli-hunter

新版中国菜刀：
https://github.com/Chora10/Cknife

git泄露利用EXP：
https://github.com/lijiejie/GitHack

浏览器攻击框架：
https://github.com/beefproject/beef

自动化绕过WAF脚本：
https://github.com/khalilbijjou/WAFNinja
https://github.com/owtf/wafbypasser

一款开源WAF：
https://github.com/SpiderLabs/ModSecurity

http命令行客户端：
https://github.com/jkbrzt/httpie

浏览器调试利器：
https://github.com/firebug/firebug

DISCUZ漏洞扫描器：
https://github.com/code-scan/dzscan

自动化代码审计工具
https://github.com/wufeifei/cobra

浏览器攻击框架：
https://github.com/julienbedard/browsersploit

tomcat自动后门部署：
https://github.com/mgeeky/tomcatWarDeployer

网络空间指纹扫描器：
https://github.com/nanshihui/Scan-T

burpsuit之J2EE扫描插件：
https://github.com/ilmila/J2EEScan

6.windows域渗透工具

mimikatz明文注入：
https://github.com/gentilkiwi/mimikatz

Powershell渗透库合集：
https://github.com/PowerShellMafia/PowerSploit

Powershell tools合集：
https://github.com/clymb3r/PowerShell

powershell的mimikittenz:
https://github.com/putterpanda/mimikittenz

域渗透教程:
https://github.com/l3m0n/pentest_study

7.Fuzz

Web向Fuzz工具
https://github.com/xmendez/wfuzz

HTTP暴力破解，撞库攻击脚本
https://github.com/lijiejie/htpwdScan

8.漏洞利用及攻击框架

msf框架：
https://github.com/rapid7/metasploit-framework

pocsscan攻击框架：
https://github.com/erevus-cn/pocscan

Pocsuite攻击框架:
https://github.com/knownsec/Pocsuite

Beebeeto攻击框架：
https://github.com/n0tr00t/Beebeeto-framework

漏洞POC&EXP:
ExploitDB官方git版本:
https://github.com/offensive-security/exploit-database

php漏洞代码分析：
https://github.com/80vul/phpcodz

CVE-2016-2107:
https://github.com/FiloSottile/CVE-2016-2107

CVE-2015-7547 POC：
https://github.com/fjserna/CVE-2015-7547

JAVA反序列化POC生成工具:
https://github.com/frohoff/ysoserial

JAVA反序列化EXP:
https://github.com/foxglovesec/JavaUnserializeExploits

Jenkins CommonCollections EXP:
https://github.com/CaledoniaProject/jenkins-cli-exploit

CVE-2015-2426 EXP (windows内核提权):
https://github.com/vlad902/hacking-team-windows-kernel-lpe

use docker to show web attack(php本地文件包含结合phpinfo getshell 以及ssrf结合curl的利用演示):
https://github.com/hxer/vulnapp

php7缓存覆写漏洞Demo及相关工具:
https://github.com/GoSecure/php7-opcache-override

XcodeGhost木马样本:
https://github.com/XcodeGhostSource/XcodeGhost

9.中间人攻击及钓鱼

中间人攻击框架:
https://github.com/secretsquirrel/the-backdoor-factory
https://github.com/secretsquirrel/BDFProxy
https://github.com/byt3bl33d3r/MITMf

Inject code, jam wifi, and spy on wifi users:
https://github.com/DanMcInerney/LANs.py

中间人代理工具:
https://github.com/intrepidusgroup/mallory

wifi钓鱼:
https://github.com/sophron/wifiphisher

10.密码破解

密码破解工具:
https://github.com/shinnok/johnny

本地存储的各类密码提取利器:
https://github.com/AlessandroZ/LaZagne

11.二进制及代码分析工具

二进制分析工具
https://github.com/devttys0/binwalk

系统扫描器
https://github.com/quarkslab/binmap

rp:
https://github.com/0vercl0k/rp

Windows Exploit Development工具
https://github.com/lillypad/badger

二进制静态分析工具（python）:
https://github.com/bdcht/amoco

Python Exploit Development Assistance for GDB:
https://github.com/longld/peda

对BillGates Linux Botnet系木马活动的监控工具
https://github.com/ValdikSS/billgates-botnet-tracker

木马配置参数提取工具:
https://github.com/kevthehermit/RATDecoders

Shellphish编写的二进制分析工具（CTF向）:
https://github.com/angr/angr

针对python的静态代码分析工具:
https://github.com/yinwang0/pysonar2

一个自动化的脚本（shell）分析工具，用来给出警告和建议:
https://github.com/koalaman/shellcheck

基于AST变换的简易Javascript反混淆辅助工具:
https://github.com/ChiChou/etacsufbo

12.EXP编写框架及工具

二进制EXP编写工具:
https://github.com/t00sh/rop-tool

CTF Pwn 类题目脚本编写框架:
https://github.com/Gallopsled/pwntools

an easy-to-use io library for pwning development:
https://github.com/zTrix/zio

跨平台注入工具:
https://github.com/frida/frida

哈希长度扩展攻击EXP：
https://github.com/citronneur/rdpy

13.隐写

隐写检测工具
https://github.com/abeluck/stegdetect

14.各类安全资料：

data_hacking合集:
https://github.com/ClickSecurity/data_hacking

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

《DO NOT FUCK WITH A HACKER》:
https://github.com/citypw/DNFWAH

各类安全脑洞图：
https://github.com/phith0n/Mind-Map

信息安全流程图：
https://github.com/SecWiki/sec-chart/

15.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

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

ctf向 python工具包
https://github.com/P1kachu/v0lt

16.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

python资源大全:
https://github.com/jobbole/awesome-python-cn

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

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

17.Python

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/

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

Veil-Evasion免杀项目：
https://github.com/Veil-Framework/Veil-Evasion

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

18.福利

微信自动抢红包动态库
https://github.com/east520/AutoGetRedEnv

微信抢红包插件（安卓版）
https://github.com/geeeeeeeeek/WeChatLuckyMoney

hardsed神器:
https://github.com/yangyangwithgnu/hardseed

19.甲方安全工程师生存指南

web索引及日志搜索工具：
https://github.com/thomaspatzke/WASE

开源日志采集器：
https://github.com/wgliang/logcool

扫描CS结构的web debuger
https://github.com/Kozea/wdb

恢复sqlite数据库删除注册信息：
https://github.com/aramosf/recoversqlite/

gps欺骗检测工具:
https://github.com/zxsecurity/gpsnitch

应急处置响应框架:
https://github.com/biggiesmallsAG/nightHawkResponse

web安全开发指南:
https://github.com/FallibleInc/security-guide-for-developers

各个知名厂商漏洞测试报告模板：
https://github.com/juliocesarfort/public-pentesting-reports

linux下恶意代码检测包：
https://github.com/rfxn/linux-malware-detect

操作系统运行指标可视化框架：
https://github.com/facebook/osquery

恶意代码分析系统：
https://github.com/cuckoosandbox/cuckoo

定期搜索及存储web应用：
https://github.com/Netflix/Scumblr

事件响应框架：
https://github.com/google/grr

综合主机监控检测平台：
https://github.com/ossec/ossec-hids

分布式实时数字取证系统：
https://github.com/mozilla/mig

Microsoft & Unix 文件系统及硬盘取证工具：
https://github.com/sleuthkit/sleuthkit

20.蜜罐

SSH蜜罐：
https://github.com/desaster/kippo

蜜罐集合资源：
https://github.com/paralax/awesome-honeypots

kippo进阶版蜜罐：
https://github.com/micheloosterhof/cowrie

SMTP 蜜罐：
https://github.com/awhitehatter/mailoney

web应用程序蜜罐：
https://github.com/mushorg/glastopf

数据库蜜罐：
https://github.com/jordan-wright/elastichoney

web蜜罐：
https://github.com/atiger77/Dionaea

21.远控

用gmail充当C&C服务器的后门
https://github.com/byt3bl33d3r/gcat

开源的远控：
https://github.com/UbbeLoL/uRAT

c#远控：
https://github.com/hussein-aitlahcen/BlackHole

22.工具合集

https://github.com/torque59/Nosql-Exploitation-Framework (NoSQL扫描/爆破工具)

https://github.com/missDronio/blindy (MySQL盲注爆破工具)

https://github.com/fengxuangit/Fox-scan (基于SQLMAP的主动和被动资源发现的漏洞扫描工具)

https://github.com/NetSPI/PowerUpSQL (用于SQL Server审计的powershell脚本)

https://github.com/JohnTroony/Blisqy (用于http header中的时间盲注爆破工具，仅针对MySQL / MariaDB)

https://github.com/ron190/jsql-injection (Java编写的SQL注入工具)

https://github.com/Hadesy2k/sqliv (基于搜索引擎的批量SQL注入漏洞扫描器)

https://github.com/s0md3v/sqlmate (在sqlmap基础上增加了目录扫描，hash爆破等功能)

https://github.com/m8r0wn/enumdb (Mysys以及MSSQL爆破脱裤工具)

https://github.com/9tail123/wooscan (批量查询网站在乌云是否存在忽略的sql注入漏洞并自动调用sqlmap测试)

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

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/netxfly/crack_ssh (Go写的协程版的ssh \redis \ mongodb弱口令破解工具)

https://github.com/LandGrey/pydictor (暴力破解字典建立工具)

https://github.com/shengqi158/weak_password_detect(多线程探测弱口令)

https://github.com/s0md3v/Blazy (支持测试CSRF，Clickjacking，Cloudflare和WAF的弱口令探测器)

https://github.com/MooseDojo/myBFF (对CiscoVPN，Citrix Gateway等各类服务进行弱口令检测的脚本)

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)

https://github.com/googleinurl/RouterHunterBR (路由器设备漏洞扫描利用)

https://github.com/scu-igroup/telnet-scanner (Telnet服务密码撞库)

https://github.com/viraintel/OWASP-Nettacker (自动化信息搜集及渗透测试工具，比较适用于IoT扫描)

https://github.com/threat9/routersploit (嵌入式设备漏洞扫描及利用工具)

https://github.com/shawarkhanethicalhacker/BruteXSS (一款XSS扫描器，可暴力注入参数)

https://github.com/1N3/XSSTracer (小型XSS扫描器，也可检测CRLF，XSS，点击劫持的)

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)

https://github.com/BlackHole1/autoFindXssAndCsrf (自动化检测页面是否存在XSS和跨站请求伪造漏洞的浏览器插件)

https://github.com/shogunlab/shuriken (使用命令行进行XSS批量检测)

https://github.com/s0md3v/XSStrike (可识别和绕过WAF的XSS扫描工具)

https://github.com/stamparm/DSXS (支持GET，POST方式的高效XSS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/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，主持人)

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)

https://github.com/Ekultek/Zeus-Scanner (能成抓取搜索引擎隐藏的url，并交由sqlmap，nmap扫描)

https://github.com/0xbug/Biu-framework(企业内网基础服务安全扫描框架)

https://github.com/metac0rtex/GitHarvester(github Repo信息搜集工具)

https://github.com/shengqi158/svnhack(.svn文件夹泄漏利用工具)

https://github.com/repoog/GitPrey(GitHub敏感信息扫描工具)

https://github.com/0xbug/Hawkeye(企业资产，敏感信息GitHub泄露监控系统)

https://github.com/lianfeng30/githubscan(根据企业关键词进行项目检索以及相应敏感文件和文件内容扫描的工具)

https://github.com/UnkL4b/GitMiner(github敏感信息搜索工具)

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

https://github.com/dxa4481/truffleHog(GitHub敏感信息扫描工具，包括检测提交等)

https://github.com/1N3/Goohak(自动化对指定域名进行Google hacking搜索并收集信息)

https://github.com/UKHomeOffice/repo-security-scanner(用于搜索git的承诺中的敏感信息，例如密码，私钥等的客户端工具)

https://github.com/FeeiCN/GSIL(Github敏感信息泄露扫描)

https://github.com/MiSecurity/x-patrol(Github泄露巡航工具)

https://github.com/1N3/BlackWidow(Web站点信息搜集工具，包括邮箱，电话等信息)

https://github.com/anshumanbh/git-all-secrets (集合多个开源GitHub敏感信息扫描的企业信息泄露巡航工具)

https://github.com/s0md3v/Photon(可以提取网址，电子邮件，文件，网站帐户等的高速爬虫)

https://github.com/he1m4n6a/findWebshell(一款简单的webshell检测工具)

https://github.com/Tencent/HaboMalHunter(哈勃分析系统，LINUX系统病毒分析及安全检测)

https://github.com/PlagueScanner/PlagueScanner(使用python实现的集成ClamAV，ESET，Bitdefender的反病毒引擎)

https://github.com/nbs-system/php-malware-finder (一款高效率PHP-webshell扫描工具)

https://github.com/emposha/PHP-Shell-Detector/(测试效率高达99%的webshell检测工具)

https://github.com/erevus-cn/scan_webshell(一款简洁的的Webshell扫描工具)

https://github.com/emposha/Shell-Detector(Webshell扫描工具，支持php / perl / asp / aspx webshell扫描)

https://github.com/m4rco-/dorothy2 (一款木马，僵尸网络分析框架)

https://github.com/droidefense/engine(高级安卓木马病毒分析框架)

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)

https://github.com/BlackHole1/WebRtcXSS(自动化利用XSS入侵内网)

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 (基于Masscan和Zmap的网络扫描器)

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路径收集与扫描)

https://github.com/x0day/bannerscan(C段横幅与路径扫描)

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/xcdn (尝试找出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)

https://github.com/chichou/grab.js(类似zgrab的快速TCP指纹抓取解析工具，支持更多协议)

https://github.com/Nitr4x/whichCDN(CDN识别，检测)

https://github.com/secfree/bcrpscan(基于爬虫的web路径扫描器)

https://github.com/mozilla/ssh_scan(服务器ssh配置信息扫描)

https://github.com/18F/domain-scan (针对域名及其子域名的资产数据检测/扫描，包括http / https检测等)

https://github.com/ggusoft/inforfinder(域名资产收集及指纹识别工具)

https://github.com/boy-hack/gwhatweb(CMS识别python gevent实现)

https://github.com/Mosuan/FileScan(敏感文件扫描/二次判断降低误报率/扫描内容规则化/多目录扫描)

https://github.com/Xyntax/FileSensor(基于爬虫的动态敏感文件探测工具)

https://github.com/deibit/cansina(web路径扫描工具)

https://github.com/0xbug/Howl (网络设备web服务指纹扫描与检索)

https://github.com/mozilla/cipherscan(目标主机服务ssl类型识别)

https://github.com/xmendez/wfuzz(Web应用fuzz工具，框架，同时可用于web路径/服务扫描)

https://github.com/s0md3v/Breacher(多线程的后台路径扫描器，也可用于发现重定向漏洞后执行)

https://github.com/ztgrace/changeme (弱口令扫描器，不仅支持普通登录页，也支持ssh，mongodb等组件)

https://github.com/medbenali/CyberScan(渗透测试辅助工具，支持分析数据包，解码，端口扫描，IP地址分析等)

https://github.com/m0nad/HellRaiser (基于nmap的扫描器，与cve漏洞关联)

https://github.com/scipag/vulscan (基于nmap的高级漏洞扫描器，命令行环境使用)

https://github.com/jekyc/wig(web应用信息搜集工具)

https://github.com/eldraco/domain_analyzer (围绕web服务的域名进行信息收集和“域传送”等漏洞扫描，也支持针对背后的服务器端口扫描等)

https://github.com/cloudtracer/paskto (基于Nikto扫描规则的被动式路径扫描以及信息爬虫)

https://github.com/zerokeeper/WebEye(快速识别WEB服务器类型，CMS类型，WAF类型，WHOIS信息，以及语言框架)

https://github.com/m3liot/shcheck(用于检查web服务的http header的安全性)

https://github.com/aipengjie/sensitivefilescan(一款高效快捷的敏感文件扫描工具)

https://github.com/fnk0c/cangibrina(通过字典穷举，google，robots.txt等途径的跨平台后台管理路径扫描器)

https://github.com/n4xh4ck5/CMSsc4n(常规CMS指纹识别)

https://github.com/Ekultek/WhatWaf(WAF指纹识别及自动化绕过工具)

https://github.com/dzonerzy/goWAPT(网络应用模糊工具，框架，同时可用于网络路径/服务扫描)

https://github.com/blackye/webdirdig(web敏感目录/信息泄漏扫描脚本)

https://github.com/GitHackTools/BillCipher (用于网站或IP地址的信息收集工具)

https://github.com/boy-hack/w8fuckcdn(通过扫描全网获得真实IP的自动化程序)

https://github.com/boy-hack/w11scan (分布式WEB指纹识别平台)

https://github.com/Nekmo/dirhunt (爬虫式web目录扫描工具)

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

https://github.com/code-scan/dzscan (首款集成化的Discuz扫描工具)

https://github.com/chuhades/CMS-Exploit-Framework (一款简洁优雅的CMS扫描利用框架)

https://github.com/lijiejie/IIS_shortname_Scanner(IIS短文件名暴力枚举漏洞利用工具)

https://github.com/riusksk/FlashScanner(flashxss扫描)

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

https://github.com/epinna/tplmap (服务器端模板注入漏洞检测与利用工具)

https://github.com/cr0hn/dockerscan(Docker扫描工具)

https://github.com/m4ll0k/WPSeku (一款精简的wordpress扫描工具)

https://github.com/rastating/wordpress-exploit-framework (集成化wordpress漏洞利用框架)

https://github.com/ilmila/J2EEScan(用于扫描J2EE应用的一款burpsuite插件)

https://github.com/riusksk/StrutScan (一款基于perl的strut2的历史漏洞扫描器)

https://github.com/D35m0nd142/LFISuite(本地文件包含漏洞利用及扫描工具，支持反弹shell)

https://github.com/0x4D31/salt-scanner (基于Salt Open以及Vulners Linux Audit API的linux漏洞扫描器，支持与JIRA，slack平台结合使用)

https://github.com/tijme/angularjs-csti-scanner(自动化探测客户端AngularJS模板注入漏洞工具)

https://github.com/irsdl/IIS-ShortName-Scanner(Java编写的IIS短文件名暴力枚举漏洞利用工具)

https://github.com/swisskyrepo/Wordpresscan(基于WPScan以及WPSeku的优化版wordpress扫描器)

https://github.com/CHYbeta/cmsPoc(CMS渗透测试框架)

https://github.com/rudSarkar/crlf-injector(CRLF注入漏洞批量扫描)

https://github.com/3gstudent/Smbtouch-Scanner(自动化扫描内网中存在的由影子经纪人泄露的ETERNAL系列漏洞)

https://github.com/utiso/dorkbot (通过定制化的谷歌搜索引擎进行漏洞页面搜寻及扫描)

https://github.com/OsandaMalith/LFiFreak(本地文件包含漏洞利用及扫描工具，支持反弹shell)

https://github.com/mak-/parameth (用于枚举脚本的GET / POST未知参数字段)

https://github.com/Lucifer1993/struts-scan(struts2的漏洞全版本检测和利用工具)

https://github.com/hahwul/a2sv(SSL漏洞扫描，例如心脏滴血漏洞等)

https://github.com/NullArray/DorkNet(基于搜索引擎的漏洞网页搜寻)

https://github.com/NickstaDB/BaRMIe(用于攻击爆破Java RemoteMethod Invocation服务的工具)

https://github.com/RetireJS/grunt-retire(扫描js扩展库的常见漏洞)

https://github.com/kotobukki/BDA(针对的hadoop /火花等大数据平台的的漏洞探测工具)

https://github.com/jagracey/Regex-DoS(RegEx拒绝服务扫描器)

https://github.com/milesrichardson/docker-onion-nmap(使用NMAP扫描的Tor网络上隐藏的“洋葱”服务)

https://github.com/Moham3dRiahi/XAttacker(Web CMS Exploit工具，包含针对主流CMS的66个不同的漏洞利用)

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

https://github.com/almandin/fuxploider (文件上传漏洞扫描器及利用工具)

https://github.com/Ice3man543/SubOver (子域名接管漏洞检测工具，支持30+云服务托管检测)

https://github.com/Jamalc0m/wphunter(WordPress的漏洞扫描器，同时也支持敏感文件泄露扫描)

https://github.com/retirejs/retire.js(检测网站依赖的JavaScript库中存在的已知通用漏洞)

https://github.com/3xp10it/xupload (自动检测上传功能是否可上传webshell)

https://github.com/mobrine-mob/M0B-tool(CMS指纹识别及自动化渗透测试框架)

https://github.com/rezasp/vbscan (论坛框架vBulletin黑盒漏洞扫描器)

https://github.com/MrSqar-Ye/BadMod(CMS指纹识别及自动化渗透测试框架)

https://github.com/Tuhinshubhra/CMSeeK(CMS漏洞检测和利用套件)

https://github.com/cloudsploit/scans(AWS安全审计工具)

https://github.com/radenvodka/SVScanner (针对wp，magento，joomla等CMS的漏洞扫描器及自动利用工具)

https://github.com/rezasp/joomscan(OWASP旗下joomla漏洞扫描项目)

https://github.com/6IX7ine/djangohunter(用于检测因错误配置导致敏感信息暴露的Django应用程序)

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)

https://github.com/MisterBianco/BoopSuite(无线网络审计工具，支持2-5GHZ频段)

https://github.com/DanMcInerney/LANs.py(ARP欺骗，无线网络劫持)

https://github.com/besimaltnok/PiFinger (检查wifi是否是“大菠萝”所开放的热点，并给予网络评分)

https://github.com/derv82/wifite2 (自动化无线网络攻击工具wifite的重构版本)

https://github.com/sowish/LNScan (基于BBScan via.lijiejie的本地网络扫描)

https://github.com/SkyLined/LocalNetworkScanner(基于JavaScript的的本地网络扫描)

https://github.com/wufeifei/cobra (白盒代码安全审计系统)

https://github.com/OneSourceCat/phpvulhunter (静态PHP代码审计)

https://github.com/Qihoo360/phptrace (跟踪，分析PHP运行情况的工具)

https://github.com/ajinabraham/NodeJsScan(的NodeJS应用代码审计)

https://github.com/shengqi158/pyvulhunter(Python应用审计)

https://github.com/presidentbeef/brakeman(Ruby on Rails应用静态代码分析)

https://github.com/python-security/pyt(Python应用静态代码审计)

https://github.com/m4ll0k/WPSploit(WordPress插件代码安全审计)

https://github.com/emanuil/php-reaper (用于扫描PHP应用程序中可能存在SQL漏洞的ADOdb代码)

https://github.com/lowjoel/phortress(用于检测潜在安全漏洞的PHP静态代码分析工具)

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 (集合owasp top10漏洞扫描和边界资产发现能力的分布式web漏洞扫描框架)

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

https://github.com/ysrc/GourdScanV2(ysrc出品的被动式漏洞扫描工具)

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(自动化渗透测试框架，支持cdn真实ip查找，指纹识别等)

https://github.com/Lcys/lcyscan(蠕插件化漏洞扫描器，支持生成扫描报表)

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

https://github.com/v3n0m-Scanner/V3n0M-Scanner(支持检测SQLI/ XSS / LFI / RFI等漏洞的扫描器)

https://github.com/Skycrab/leakScan(Web图形化的漏洞扫描框架)

https://github.com/zhangzhenfeng/AnyScan(一款网络化的自动化渗透测试框架)

https://github.com/Tuhinshubhra/RED_HAWK(一款集成信息收集，漏洞扫描，指纹识别等的多合一扫描工具)

https://github.com/Arachni/arachni (高度集成化的Web应用漏洞扫描框架，支持REST，RPC等api调用)

https://github.com/infobyte/faraday(集成化渗透测试辅助平台及漏洞管理平台)

https://github.com/juansacco/exploitpack(渗透测试集成框架，包含超过38,000+攻击)

https://github.com/swisskyrepo/DamnWebScanner(基于铬/歌剧插件的被动式漏洞扫描)

https://github.com/anilbaranyelken/tulpar(支持多种网络漏洞扫描，命令行环境使用)

https://github.com/m4ll0k/Spaghetti(web应用扫描器，支持指纹识别，文件目录爆破，SQL / XSS / RFI等漏洞扫描，也可直接用于struts，ShellShock等扫描)

https://github.com/Yukinoshita47/Yuki-Chan-The-Auto-Pentest (集成子域名枚举，nmap，waf指纹识别等模块的web应用扫描器)

https://github.com/0xsauby/yasuo (使用ruby开发的扫描网络中主机存在的第三方web应用服务漏洞)

https://github.com/hatRiot/clusterd(Web应用自动化扫描框架，支持自动化上传webshell)

https://github.com/erevus-cn/pocscan (一款开源Poc调用框架，可轻松调用
Pocsuite，Tangscan，Beebeeto，Knowsec老版本POC，可使用docker部署)

https://github.com/TophantTechnology/osprey (斗象能力中心出品并长期维护的开源漏洞检测框架)

https://github.com/yangbh/Hammer(Web应用漏洞扫描框架)https://github.com/Lucifer1993/AngelSword(Web应用漏洞扫描框架，基于python3)https://github.com/secrary/EllaScanner(被动式漏洞扫描，支持历史cve编号漏洞识别)

https://github.com/zaproxy/zaproxy(OWASP ZAP核心项目出品的综合性渗透测试工具)

https://github.com/sullo/nikto(Web服务综合型扫描器，用于指定目标的资产收集，安全配置缺陷或者安全漏洞扫描)

https://github.com/s0md3v/Striker(一款多方位信息收集，指纹识别及漏洞扫描工具)

https://github.com/dermotblair/webvulscan (一款web应用漏洞扫描器，支持扫描反射型以及存储型xss，sql injection等漏洞，支持输出pdf报告)

https://github.com/alienwithin/OWASP-mth3l3m3nt-framework(渗透测试辅助工具，综合利用框架)

https://github.com/toyakula/luna(基于被动式扫描框架的自动化web漏洞扫描工具)

https://github.com/Manisso/fsociety(渗透测试辅助框架，包含信息搜集，无线渗透，网络应用扫描等功能)

https://github.com/boy-hack/w9scan(内置1200+插件的web漏洞扫描框架)

https://github.com/YalcinYolalan/WSSAT(Web服务安全评估工具，提供基于windows操作系统的简单.exe应用)

https://github.com/AmyangXYZ/AssassinGo(使用去开发的可扩展以及高并发渗透测试框架)

https://github.com/jeffzh3ng/InsectsAwake (基于Flask应用框架的漏洞扫描系统)

https://github.com/m4ll0k/Galileo(一个操作上类似metasploit的web应用安全审计框架)

https://github.com/joker25000/Optiva-Framework (一款web应用漏洞扫描器，支持扫描反射型以及存储型xss，sql injection等漏洞)

https://github.com/theInfectedDrake/TIDoS-Framework (集成104个模块的Web应用程序渗透测试框架)

https://github.com/Neo23x0/Loki(一款APT入侵痕迹扫描器)

https://github.com/w3h/icsmaster/tree/master/nse(ICS设备nmap扫描脚本)

https://github.com/OpenNetworkingFoundation/DELTA(SDN安全评估框架)