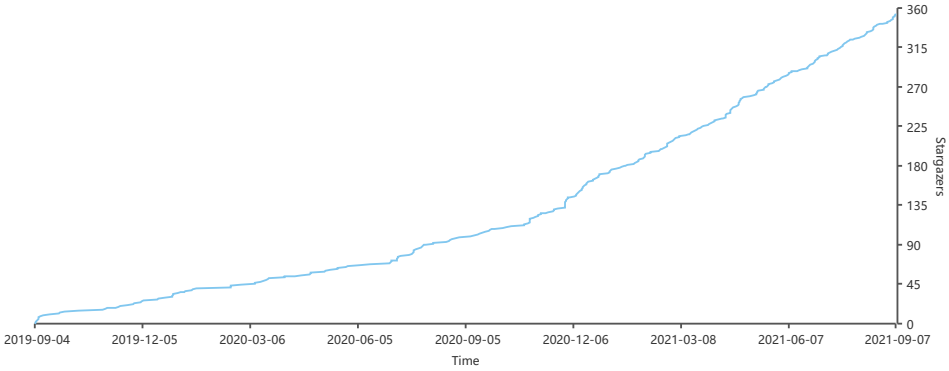
网络安全与渗透测试工具导航

> **郑重申明：此文档全是本人一点一点抄袭互联网的！！！致敬所有的工具开发者。**

> 可能是总结的最全的开源渗透工具!



1. SOMETHING_FUN

- Issue2
- SOMETHING_FUN

2. 目录

3. 入门指南

- Web Hacking 101 中文版：https://wizardforcel.gitbooks.io/web-hacking-101/content/
- 浅入浅出Android安全 中文版：https://wizardforcel.gitbooks.io/asani/content/
- Android 渗透测试学习手册 中文版：https://wizardforcel.gitbooks.io/lpad/content/
- Kali Linux Web渗透测试秘籍 中文版：https://wizardforcel.gitbooks.io/kali-linux-web-pentest-cookbook/content/
- Linux exploit 开发入门：https://github.com/hardenedlinux/linux-exploit-development-tutorial
- burpsuite实战指南：https://www.gitbook.com/book/t0data/burpsuite/details
- 渗透测试Node.js应用：http://www.kanxue.com/?article-read-1108.htm=&winzoom=1
- Web安全资料和资源列表：https://github.com/qazbnm456/awesome-web-security
- 安全维基百科：https://sec-wiki.com/sec-wiki
- 安全漏洞信息（精）：https://ninjia.gitbook.io/secskill/Web
- 安全学习笔记（精）：https://websec.readthedocs.io/zh/latest/
- 黑客清单：https://github.com/sunnyelf/awesome-hacking
- 思维导图: https://github.com/phith0n/Mind-Map
- 思维导图：https://github.com/SecWiki/sec-chart
- 渗透超全面的渗透资料💯 包含：0day，XSS，SQL注入，提权.....: https://github.com/w1109790800/penetration

3.1. 在线靶场

- `SQLi-LABS`: http://43.247.91.228:84/
- `DVMA`: http://43.247.91.228:81/
- `XSS`: http://59.63.200.79:8004/Feedback.asp

3.2. 文件上传漏洞靶场

- https://github.com/c0ny1/upload-labs
- https://github.com/LandGrey/upload-labs-writeup

3.3. 导航

- 渗透导航网站：渗透师导航、黑客街

3.4. payload

- `Payload`：https://github.com/swisskyrepo/PayloadsAllTheThings
- `BurpSuitePro-2.0.06-beta-Loader-Keygen`：https://github.com/h0nus/BurpSuitePro-2.0.06-beta-Loader-Keygen

4. 子域名枚举

- 经典的子域名爆破枚举脚本：https://github.com/lijiejie/subDomainsBrute
- 子域名字典穷举：https://github.com/ring04h/wydomain
- 子域名枚举与地图标记：https://github.com/le4f/dnsmaper
- 在线子域名信息收集工具：https://github.com/0xbug/orangescan
- 根据DNS记录查询子域名：https://github.com/TheRook/subbrute
- 基于谷歌SSL透明证书的子域名查询脚本：https://github.com/We5ter/GSDF
- 使用CloudFlare进行子域名枚举的脚本：https://github.com/mandatoryprogrammer/cloudflare_enum
- A domain scanner：https://github.com/18F/domain-scan
- Knock Subdomain Scan：https://github.com/guelfoweb/knock
- 多方式收集目标子域名信息：https://github.com/Evi1CLAY/CoolPool/tree/master/Python/DomainSeeker
- 兄弟域名查询：https://github.com/code-scan/BroDomain
- 基于dns查询的子域名枚举：https://github.com/chuhades/dnsbrute

4.1. 自动爬虫实现的子域名收集工具

- 快速子域枚举工具：https://github.com/aboul3la/Sublist3r
- 子域名枚举及信息搜集工具：https://github.com/jonluca/Anubis
- 子域名查询工具：https://github.com/n4xh4ck5/N4xD0rk
- 一款高效的子域名爆破工具：https://github.com/infosec-au/altdns
- 基于`AsyncIO`协程以及非重复字典的子域名爆破工具：https://github.com/FeeiCN/ESD
- 快速而灵活的子域名爆破工具：https://github.com/giovanifss/Dumb
- 通过域名透明证书记录获取子域名：https://github.com/UnaPibaGeek/ctfr
- Go语言开发的子域名枚举工具：https://github.com/caffix/amass
- 继承于sublist3r项目的模块化体系结构，一个强劲的子域名枚举工具：https://github.com/Ice3man543/subfinder

5. waf开源及规则

- https://github.com/xsec-lab/x-waf
- https://github.com/loveshell/ngx_lua_waf
- https://github.com/SpiderLabs/owasp-modsecurity-crs/tree/master/base_rules

6. web应用扫描工具

- web应用安全扫描器框架：http://github.com/Arachni/arachni
- 增强版`WeblogicScan`：https://github.com/dr0op/WeblogicScan

7. webshell检测以及病毒分析

- 简单的php后门检测工具以及webshell样本库：https://github.com/We5ter/Scanners-Box/tree/master/webshell/
- Webshell扫描工具：https://github.com/ym2011/ScanBackdoor
- PHP后门扫描：https://github.com/yassineaddi/BackdoorMan
- 又一款webshell检测工具：https://github.com/he1m4n6a/findWebshell
- 哈勃分析系统，linux系统病毒分析及安全检测：https://github.com/Tencent/HaboMalHunter
- 使用python实现的集成ClamAV、ESET、Bitdefender的反病毒引擎：https://github.com/PlagueScanner/PlagueScanner ()
- 一款高效率PHP-webshell扫描工具：https://github.com/nbs-system/php-malware-finder
- 测试效率高达99%的webshell检测工具：https://github.com/emposha/PHP-Shell-Detector/
- 一款简单的webshell检测工具: https://github.com/he1m4n6a/findWebshell
- 哈勃分析系统，LINUX系统病毒分析及安全检测: https://github.com/Tencent/HaboMalHunter
- 使用python实现的集成ClamAV，ESET，Bitdefender的反病毒引擎: https://github.com/PlagueScanner/PlagueScanner
- 一款高效率PHP-webshell扫描工具: https://github.com/nbs-system/php-malware-finder
- 测试效率高达99%的webshell检测工具: https://github.com/emposha/PHP-Shell-Detector/
- 一款简洁的的Webshell扫描工具: https://github.com/erevus-cn/scan_webshell
- Webshell扫描工具，支持php / perl / asp / aspx webshell扫描: https://github.com/emposha/Shell-Detector
- 一款木马，僵尸网络分析框架: https://github.com/m4rco-/dorothy2
- 高级安卓木马病毒分析框架: https://github.com/droidefense/engine

8. DDos防护

- https://github.com/ywjt/Dshield

9. Android系列工具

- http://sec-redclub.com/index.php/archives/439/

10. XSS扫描

- Cross-Site Scripting Bruteforcer：https://github.com/shawarkhanethicalhacker/BruteXSS
- A small python script to check for Cross-Site Tracing：https://github.com/1N3/XSSTracer
- PHP版本的反射型xss扫描：https://github.com/0x584A/fuzzXssPHP
- 批量扫描xss的python脚本：https://github.com/chuhades/xss_scan
- 自动化检测页面是否存在XSS和CSRF漏洞的浏览器插件：https://github.com/BlackHole1/autoFindXssAndCsrf
- 一款XSS扫描器，可暴力注入参数: https://github.com/shawarkhanethicalhacker/BruteXSS
- 小型XSS扫描器，也可检测CRLF，XSS，点击劫持的: https://github.com/1N3/XSSTracer
- PHP版本的反射型xss扫描: https://github.com/0x584A/fuzzXssPHP
- 批量扫描XSS的python脚本: https://github.com/chuhades/xss_scan

- 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/BlackHole1/autoFindXssAndCsrf
- 使用命令行进行XSS批量检测: https://github.com/shogunlab/shuriken
- 可识别和绕过WAF的XSS扫描工具: https://github.com/s0md3v/XSStrike
- 支持GET，POST方式的高效XSS扫描器: https://github.com/stamparm/DSXS

11. 代码审计

- php静态扫描工具集：https://github.com/exakat/php-static-analysis-tools
- 白盒代码安全审计系统：https://github.com/wufeifei/cobra
- 静态php代码审计：https://github.com/OneSourceCat/phpvulhunter
- 跟踪、分析PHP运行情况的工具：https://github.com/Qihoo360/phptrace
- NodeJS应用代码审计：https://github.com/ajinabraham/NodeJsScan
- PHP代码审计：https://github.com/pwnsdx/BadCode
- ruby源码审计：https://github.com/thesp0nge/dawnscanner
- Ruby on Rails应用程序的安全漏洞：https://github.com/presidentbeef/brakeman
- app黑盒审计：https://github.com/ajinabraham/Mobile-Security-Framework-MobSF/
- iOS安全审计：https://github.com/alibaba/iOSSecAudit
- 白盒代码安全审计系统: https://github.com/wufeifei/cobra
- 静态PHP代码审计: https://github.com/OneSourceCat/phpvulhunter
- 跟踪，分析PHP运行情况的工具: https://github.com/Qihoo360/phptrace
- 的NodeJS应用代码审计: https://github.com/ajinabraham/NodeJsScan
- Python应用审计: https://github.com/shengqi158/pyvulhunter
- Ruby on Rails应用静态代码分析: https://github.com/presidentbeef/brakeman
- Python应用静态代码审计: https://github.com/python-security/pyt
- WordPress插件代码安全审计: https://github.com/m4ll0k/WPSploit
- 用于扫描PHP应用程序中可能存在SQL漏洞的ADOdb代码: https://github.com/emanuil/php-reaper

12. 端口扫描、指纹识别以及中间件扫描

- Nmap端口扫描器之王：https://nmap.org/download.html
- 目标端口扫描+系统服务指纹识别：https://github.com/ring04h/wyportmap
- 动态多线程敏感信息泄露检测工具：https://github.com/ring04h/weakfilescan
- WAF产品指纹识别：https://github.com/EnableSecurity/wafw00f
- ssl类型识别：https://github.com/rbsec/sslscan
- web指纹识别：https://github.com/urbanadventurer/whatweb
- web应用指纹识别：https://github.com/tanjiti/FingerPrint
- 网络爬虫式指纹识别：https://github.com/nanshihui/Scan-T
- a fast Network scanner inspired by Masscan and Zmap：https://github.com/OffensivePython/Nscan
- 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-NAScan
- 中间件扫描：https://github.com/ywolf/F-MiddlewareScan
- Web path scanner：https://github.com/maurosoria/dirsearch
- C段Banner与路径扫描：https://github.com/x0day/bannerscan
- 端口服务扫描：https://github.com/RASSec/RASscan
- waf自动暴破：https://github.com/3xp10it/bypass_waf
- 尝试找出cdn背后的真实ip：https://github.com/3xp10it/xcdn
- 基于Bing搜索引擎的C段/旁站查询，多线程，支持API：https://github.com/Xyntax/BingC

- 多线程WEB目录爆破工具：https://github.com/Xyntax/DirBrute
- 一个爬虫式的网段Web主机发现小工具：https://github.com/zer0h/httpscan
- thorn上实现的分布式任务分发的ip端口漏洞扫描器：https://github.com/lietdai/doom
- 类似 zgrab 的快速 TCP 指纹抓取解析工具，支持更多协议：https://github.com/chichou/grab.js
- CDN识别、检测：https://github.com/Nitr4x/whichCDN
- 基于爬虫的web路径扫描器：https://github.com/secfree/bcrpscan
- 目标端口扫描+系统服务指纹识别: https://github.com/ring04h/wyportmap
- 动态多线程敏感信息泄露检测工具: https://github.com/ring04h/weakfilescan
- WAF产品指纹识别: https://github.com/EnableSecurity/wafw00f
- SSL类型识别: https://github.com/rbsec/sslscan
- Web指纹识别: https://github.com/urbanadventurer/whatweb
- Web应用指纹识别: https://github.com/tanjiti/FingerPrint
- 网络爬虫式指纹识别: https://github.com/nanshihui/Scan-T
- 基于Masscan和Zmap的网络扫描器: https://github.com/OffensivePython/Nscan
- 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-NAScan
- 中间件扫描: https://github.com/ywolf/F-MiddlewareScan
- web路径收集与扫描: https://github.com/maurosoria/dirsearch
- C段横幅与路径扫描: https://github.com/x0day/bannerscan
- 端口服务扫描: https://github.com/RASSec/RASscan
- waf自动暴破: https://github.com/3xp10it/bypass_waf
- 尝试找出cdn背后的真实ip: https://github.com/3xp10it/xcdn
- 基于Bing搜索引擎的C段/旁站查询，多线程，支持API: https://github.com/Xyntax/BingC
- 多线程WEB目录爆破工具: https://github.com/Xyntax/DirBrute
- 一个爬虫式的网段Web主机发现小工具: https://github.com/zer0h/httpscan
- Thorn上实现的分布式任务分发的ip端口漏洞扫描器: https://github.com/lietdai/doom
- 类似zgrab的快速TCP指纹抓取解析工具，支持更多协议: https://github.com/chichou/grab.js
- CDN识别，检测: https://github.com/Nitr4x/whichCDN
- 基于爬虫的web路径扫描器: https://github.com/secfree/bcrpscan
- 服务器ssh配置信息扫描: https://github.com/mozilla/ssh_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/18F/domain-scan
- 域名资产收集及指纹识别工具: https://github.com/ggusoft/inforfinder
- CMS识别python gevent实现: https://github.com/boy-hack/gwhatweb
- 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/Mosuan/FileScan
- 基于爬虫的动态敏感文件探测工具: https://github.com/Xyntax/FileSensor
- web路径扫描工具: https://github.com/deibit/cansina
- 网络设备web服务指纹扫描与检索: https://github.com/0xbug/Howl
- 目标主机服务ssl类型识别: https://github.com/mozilla/cipherscan
- Web应用fuzz工具，框架，同时可用于web路径/服务扫描: https://github.com/xmendez/wfuzz
- 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/s0md3v/Breacher
- 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/ztgrace/changeme
- 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/medbenali/CyberScan

- 基于nmap的扫描器，与cve漏洞关联: https://github.com/m0nad/HellRaiser
- 基于nmap的高级漏洞扫描器，命令行环境使用: https://github.com/scipag/vulscan
- web应用信息搜集工具: https://github.com/jekyc/wig
- 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/eldraco/domain_analyzer
- 基于Nikto扫描规则的被动式路径扫描以及信息爬虫: https://github.com/cloudtracer/paskto
- 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/zerokeeper/WebEye
- 用于检查web服务的http header的安全性: https://github.com/m3liot/shcheck
- 一款高效快捷的敏感文件扫描工具: https://github.com/aipengjie/sensitivefilescan
- 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/fnk0c/cangibrina
- 常规CMS指纹识别: https://github.com/n4xh4ck5/CMSsc4n
- WAF指纹识别及自动化绕过工具: https://github.com/Ekultek/WhatWaf
- 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/dzonerzy/goWAPT
- web敏感目录/信息泄漏扫描脚本: https://github.com/blackye/webdirdig
- 用于网站或IP地址的信息收集工具: https://github.com/GitHackTools/BillCipher
- 通过扫描全网获得真实IP的自动化程序: https://github.com/boy-hack/w8fuckcdn
- 分布式WEB指纹识别平台: https://github.com/boy-hack/w11scan
- 爬虫式web目录扫描工具: https://github.com/Nekmo/dirhunt

13. 高级持续性威胁(APT)相关工具

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

14. 工控系统及大型网络相关安全工

- ICS设备nmap扫描脚本: https://github.com/w3h/icsmaster/tree/master/nse
- SDN安全评估框架: https://github.com/OpenNetworkingFoundation/DELTA

15. 模块化扫描、综合扫描器

- 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/az0ne/AZScanner
- 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/lalascan
- BkScanner 分布式、插件化web漏洞扫描器：https://github.com/blackye/BkScanner
- 被动式漏洞扫描：https://github.com/ysrc/GourdScanV2
- WEB渗透测试数据库：https://github.com/alpha1e0/pentestdb
- 基于http代理的web漏洞扫描器：https://github.com/netxfly/passive_scan
- 自动化扫描器，包括中间件扫描以及设备指纹识别：https://github.com/1N3/Sn1per
- 定向全自动化渗透测试工具：https://github.com/RASSec/pentestEr_Fully-automatic-scanner
- 自动化渗透测试框架：https://github.com/3xp10it/3xp10it
- 扫描效果未验证：https://github.com/Lcys/lcyscan
- 渗透测试插件化并发框架：https://github.com/Xyntax/POC-T
- Scanner in Python3.5 for SQLi/XSS/LFI/RFI and other Vulns：https://github.com/v3n0m-Scanner/V3n0M-Scanner
- web端的在线漏洞扫描：https://github.com/Skycrab/leakScan
- https://github.com/zhangzhenfeng/AnyScan
- FuzzScanner: https://github.com/TideSec/FuzzScanner

- TrackRay: https://github.com/iSafeBlue/TrackRay
- 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/az0ne/AZScanner
- 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/lalascan
- BkScanner分布式，插件化web漏洞扫描器: https://github.com/blackye/BkScanner
- ysrc出品的被动式漏洞扫描工具: https://github.com/ysrc/GourdScanV2
- 基于http代理的web漏洞扫描器: https://github.com/netxfly/passive_scan
- 自动化扫描器，包括中间件扫描以及设备指纹识别: https://github.com/1N3/Sn1per
- 定向全自动化渗透测试工具: https://github.com/RASSec/pentestEr_Fully-automatic-scanner
- 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/3xp10it/3xp10it
- 蝟插件化漏洞扫描器，支持生成扫描报表: https://github.com/Lcys/lcyscan
- 渗透测试插件化并发框架: https://github.com/Xyntax/POC-T
- 支持检测SQLI / XSS / LFI / RFI等漏洞的扫描器: https://github.com/v3n0m-Scanner/V3n0M-Scanner
- Web图形化的漏洞扫描框架: https://github.com/Skycrab/leakScan
- 一款网络化的自动化渗透测试框架: https://github.com/zhangzhenfeng/AnyScan
- 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/Tuhinshubhra/RED_HAWK
- 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/Arachni/arachni
- 集成化渗透测试辅助平台及漏洞管理平台: https://github.com/infobyte/faraday
- 渗透测试集成框架，包含超过38,000+攻击: https://github.com/juansacco/exploitpack
- 基于铬/歌剧插件的被动式漏洞扫描: https://github.com/swisskyrepo/DamnWebScanner
- 支持多种网络漏洞扫描，命令行环境使用: https://github.com/anilbaranyelken/tulpar
- 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/m4ll0k/Spaghetti
- 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/Yukinoshita47/Yuki-Chan-The-Auto-Pentest
- 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/0xsauby/yasuo
- Web应用自动化扫描框架，支持自动化上传webshell: https://github.com/hatRiot/clusterd
- 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/erevus-cn/pocscan
- 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/TophantTechnology/osprey
- Web应用漏洞扫描框架: https://github.com/yangbh/Hammer
- Web应用漏洞扫描框架，基于python3: https://github.com/Lucifer1993/AngelSword
- 被动式漏洞扫描，支持历史cve编号漏洞识别: https://github.com/secrary/EllaScanner
- OWASP ZAP核心项目出品的综合性渗透测试工具: https://github.com/zaproxy/zaproxy
- 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/sullo/nikto
- 一款多方位信息收集，指纹识别及漏洞扫描工具: https://github.com/s0md3v/Striker
- 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/dermotblair/webvulscan

- 渗透测试辅助工具，综合利用框架: https://github.com/alienwithin/OWASP-mth3l3m3nt-framework
- 基于被动式扫描框架的自动化web漏洞扫描工具: https://github.com/toyakula/luna
- 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/Manisso/fsociety
- 内置1200+插件的web漏洞扫描框架: https://github.com/boy-hack/w9scan
- 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/YalcinYolalan/WSSAT
- 使用去开发的可扩展以及高并发渗透测试框架: https://github.com/AmyangXYZ/AssassinGo
- 基于Flask应用框架的漏洞扫描系统: https://github.com/jeffzh3ng/InsectsAwake
- 一个操作上类似metasploit的web应用安全审计框架: https://github.com/m4ll0k/Galileo
- 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/joker25000/Optiva-Framework
- 集成104个模块的Web应用程序渗透测试框架: https://github.com/theInfectedDrake/TIDoS-Framework

16. 内网安全渗透测试工具集

- 企业内网渗透脚本，包括banner扫描、端口扫描；各种通用漏洞利用等：https://github.com/0xwindows/VulScritp
- 基于网络流量的内网探测框架：https://github.com/lcatro/network_backdoor_scanner
- 调用 Windows API 枚举用户登录信息：https://github.com/fdiskyou/hunter
- 自动化利用XSS入侵内网：https://github.com/BlackHole1/WebRtcXSS
- 本机密码查看提取工具：https://github.com/AlessandroZ/LaZagne
- linux密码抓取神器：https://github.com/huntergregal/mimipenguin
- 基于网络流量的内网探测框架: https://github.com/lcatro/network_backdoor_scanner
- 调用Windows API枚举用户登录信息: https://github.com/fdiskyou/hunter
- 自动化利用XSS入侵内网: https://github.com/BlackHole1/WebRtcXSS
- 基于BBScan via.lijiejie的本地网络扫描: https://github.com/sowish/LNScan
- 基于JavaScript的的本地网络扫描: https://github.com/SkyLined/LocalNetworkScanner

17. 企业网络自检

- 详细的内部网络信息扫描器：https://github.com/sowish/LNScan
- javascript实现的本地网络扫描器：https://github.com/SkyLined/LocalNetworkScanner
- 网络资产识别引擎，漏洞检测引擎：https://github.com/ysrc/xunfeng
- 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/laramies/theHarvester
- 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/x0day/Multisearch-v2
- 网络资产识别引擎，漏洞检测引擎: https://github.com/ysrc/xunfeng
- 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/laramies/theHarvester
- 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/x0day/Multisearch-v2

- 能成抓取搜索引擎隐藏的url，并交由sqlmap，nmap扫描: https://github.com/Ekultek/Zeus-Scanner
- 企业内网基础服务安全扫描框架: https://github.com/0xbug/Biu-framework
- github Repo信息搜集工具: https://github.com/metac0rtex/GitHarvester
- .svn文件夹泄漏利用工具: https://github.com/shengqi158/svnhack
- GitHub敏感信息扫描工具: https://github.com/repoog/GitPrey
- 企业资产，敏感信息GitHub泄露监控系统: https://github.com/0xbug/Hawkeye
- 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/lianfeng30/githubscan
- github敏感信息搜索工具: https://github.com/UnkL4b/GitMiner
- .git文件夹泄漏利用工具: https://github.com/lijiejie/GitHack
- GitHub敏感信息扫描工具，包括检测提交等: https://github.com/dxa4481/truffleHog
- 自动化对指定域名进行Google hacking搜索并收集信息: https://github.com/1N3/Goohak
- 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/UKHomeOffice/repo-security-scanner
- Github敏感信息泄露扫描: https://github.com/FeeiCN/GSIL
- Github泄露巡航工具: https://github.com/MiSecurity/x-patrol
- Web站点信息搜集工具，包括邮箱，电话等信息: https://github.com/1N3/BlackWidow
- 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/anshumanbh/git-all-secrets
- 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/s0md3v/Photon

18. 弱口令或信息泄漏扫描

- 一个简单的HTTP暴力破解、撞库攻击脚本：https://github.com/lijiejie/htpwdScan
- 一个迷你的信息泄漏批量扫描脚本：https://github.com/lijiejie/BBScan
- .git文件夹泄漏利用工具：https://github.com/lijiejie/GitHack
- 基于字典的目录扫描小工具：https://github.com/LoRexxar/BScanner
- 各种端口及弱口令检测，作者wilson9x1，原地址失效：https://github.com/she11c0der/fenghuangscanner_v3
- 对各类服务进行弱口令检测的脚本：https://github.com/ysrc/F-Scrack
- 根据用户习惯生成弱口令探测字典脚本：https://github.com/Mebus/cupp
- 中国特色的弱口令生成器：https://github.com/RicterZ/genpAss
- go写的协程版的ssh\redis\mongodb弱口令破解工具：https://github.com/netxfly/crack_ssh
- 通过输入email、phone、username的返回用户注册的所有互联网护照信息：https://github.com/n0tr00t/Sreg
- GitHub敏感信息扫描工具：https://github.com/repoog/GitPrey
- GitHub敏感信息扫描工具,包括检测commit等：https://github.com/dxa4481/truffleHog
- 暴力破解字典建立工具：https://github.com/LandGrey/pydictor
- xxe漏洞递归下载工具：https://github.com/GDSSecurity/xxe-recursive-download
- xxe在线生成利用工具：https://buer.haus/xxegen/
- 一个简单的HTTP暴力破解，撞库攻击脚本: https://github.com/lijiejie/htpwdScan
- 对各类服务进行弱口令检测的脚本: https://github.com/ysrc/F-Scrack
- 根据用户习惯生成弱口令探测字典脚本: https://github.com/Mebus/cupp
- Go写的协程版的ssh \ redis \ mongodb弱口令破解工具: https://github.com/netxfly/crack_ssh
- 暴力破解字典建立工具: https://github.com/LandGrey/pydictor

- 多线程探测弱口令: https://github.com/shengqi158/weak_password_detect
- 支持测试 `CSRF，Clickjacking，Cloudflare` 和 `WAF` 的弱口令探测器: https://github.com/s0md3v/Blazy
- 对CiscoVPN，Citrix Gateway等各类服务进行弱口令检测的脚本: https://github.com/MooseDojo/myBFF

19. 社工库

```
邮箱
https://haveibeenpwned.com/
https://www.cmsky.com/findmima-com/
http://ww3.xiaoanrui.com/
http://ww1.qqqun.org/?subid1=16d504fe-3fbe-11e9-9e07-b1a27d263d9b
https://infotracer.com/email-lookup/
https://www.spydialer.com/
http://www.114best.com/
https://usersearch.org/
https://hunter.io
https://pipl.com/search/
黑客
http://www.hac-ker.com/index.php
http://www.hackerschina.org/
网站
https://www.reg007.com/
推特
https://tweettunnel.com/
https://ja.whotwi.com/hqsb2
http://www.twitur.com
http://twicountry.org/u/kwzwz
企业
https://hkg.18dao.net/zh-hans/gongsimingdan/sousuo?keywords=
https://webb-site.com/dbpub/searchorgs.asp
香港导航网站
http://im123.com
香港公司名录
https://www.hkcompanydir.com/
http://www.hkcompanycheck.com/
https://www.search.gov.hk/search
英国企业名录
https://www.gbrbusiness.com/
国家企业信用信息公示系统
http://www.gsxt.gov.cn/index.html
个人信用查询搜索
https://www.creditchina.gov.cn/
佛教名单
http://www.rushiwowen.org/jymd/?index=2017
http://www.nanputuo.com/nptzt/gy/guide.asp?Mid=1&Sid=0&Nid=767
中国禁闻网
https://www.bannedbook.org
自由百科
https://zh-yue.wikipedia.org/wiki
中国人权
https://www.hrichina.org/chs/topic/rights-defenders
```

```
靶场：
https://www.cnblogs.com/hac425/p/9403595.html
https://www.anquanke.com/post/id/105462
https://www.freebuf.com/sectool/170713.html
https://blog.csdn.net/bfboys/article/details/52485086
船公司博客：
http://www.chuangongsi.com/blog/archives/category/contact
http://www.chuangongsi.com/blog/?s=CMA
航运公司简介：
http://www.etcline.com/Freight.aspx?Code=0505
安全论坛：
https://www.t00ls.net/navi.html
web安全学习笔记：
https://websec.readthedocs.io/zh/latest/
乌云漏洞库
https://shuimugan.com/bug/view?bug_no=64260
```

20. 数据库防火墙

- https://nim4.github.io/DBShield/

21. 数据库扫描及注入

- 注入工具之王sqlmap：https://github.com/sqlmapproject/sqlmap
- 一款基于SQLMAP和Charles的被动SQL注入漏洞扫描工具：https://github.com/0xbug/SQLiScanner
- 99行代码实现的sql注入漏洞扫描器：https://github.com/stamparm/DSSS
- 一款针对mongoDB的攻击工具：https://github.com/youngyangyang04/NoSQLAttack
- SQL盲注利用框架：https://github.com/Neohapsis/bbqsql
- 攻击SQLSERVER的Powershell脚本框架：https://github.com/NetSPI/PowerUpSQL
- 又一款数据库扫描器：https://github.com/WhitewidowScanner/whitewidow
- MongoDB审计及渗透工具：https://github.com/stampery/mongoaudit
- 注入点命令执行利用工具：https://github.com/commixproject/commix
- 一款基于SQLMAP和查尔斯的被动SQL注入漏洞扫描工具：https://github.com/0xbug/SQLiScanner
- 99行代码实现的sql注入漏洞扫描器：https://github.com/stamparm/DSSS
- 针对各种情况自由变化的MySQL注入脚本：https://github.com/LoRexxar/Feigong
- 一款针对MongoDB中的攻击工具：https://github.com/youngyangyang04/NoSQLAttack
- SQL盲注利用框架：https://github.com/Neohapsis/bbqsql
- 攻击SQLSERVER的Powershell的脚本框架：https://github.com/NetSPI/PowerUpSQL
- 一款数据库扫描器：https://github.com/WhitewidowScanner/whitewidow
- MongoDB审计及渗透工具：https://github.com/stampery/mongoaudit
- NoSQL扫描/爆破工具：https://github.com/torque59/Nosql-Exploitation-Framework
- MySQL盲注爆破工具：https://github.com/missDronio/blindy
- 基于SQLMAP的主动和被动资源发现的漏洞扫描工具：https://github.com/fengxuangit/Fox-scan
- 用于SQL Server审计的powershell脚本：https://github.com/NetSPI/PowerUpSQL
- 用于http header中的时间盲注爆破工具，仅针对MySQL / MariaDB：https://github.com/JohnTroony/Blisqy
- Java编写的SQL注入工具：https://github.com/ron190/jsql-injection
- 基于搜索引擎的批量SQL注入漏洞扫描器：https://github.com/Hadesy2k/sqliv

- 在sqlmap基础上增加了目录扫描，hash爆破等功能：https://github.com/s0md3v/sqlmate
- Mysys以及MSSQL爆破脱裤工具：https://github.com/m8r0wn/enumdb
- 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/9tail123/wooscan

22. 无线网络渗透审计

- 无线安全审计工具：https://github.com/savio-code/fern-wifi-cracker/
- Python网络/渗透测试工具：https://github.com/m4n3dw0lf/PytheM
- 无线安全渗透测试套件：https://github.com/P0cL4bs/WiFi-Pumpkin
- 无线安全审计工具: https://github.com/savio-code/fern-wifi-cracker/
- Python网络/渗透测试工具: https://github.com/m4n3dw0lf/PytheM
- 无线安全渗透测试套件: https://github.com/P0cL4bs/WiFi-Pumpkin
- 无线网络审计工具，支持2-5GHZ频段: https://github.com/MisterBianco/BoopSuite
- ARP欺骗，无线网络劫持: https://github.com/DanMcInerney/LANs.py
- 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/besimaltnok/PiFinger
- 自动化无线网络攻击工具wifite的重构版本: https://github.com/derv82/wifite2

23. 物联网设备扫描

- 物联网设备默认密码扫描检测工具：https://github.com/rapid7/IoTSeeker
- 使用nmap扫描IoT设备：https://github.com/shodan-labs/iotdb
- 路由器漏洞扫描利用：https://github.com/jh00nbr/Routerhunter-2.0
- 路由器漏洞利用框架：https://github.com/reverse-shell/routersploit
- telnet服务密码撞库：https://github.com/scu-igroup/telnet-scanner
- 打印机攻击框架：https://github.com/RUB-NDS/PRET
- 物联网设备默认密码扫描检测工具: https://github.com/rapid7/IoTSeeker
- 使用nmap扫描IoT设备: https://github.com/shodan-labs/iotdb
- 路由器设备漏洞扫描利用: https://github.com/googleinurl/RouterHunterBR
- Telnet服务密码撞库: https://github.com/scu-igroup/telnet-scanner
- 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/viraintel/OWASP-Nettacker
- 嵌入式设备漏洞扫描及利用工具: https://github.com/threat9/routersploit

24. 针对性漏洞测试工具

- java反序列化利用工具集：https://github.com/brianwrf/hackUtils
- java反序列化利用工具：https://github.com/frohoff/ysoserial
- Jenkins漏洞探测、用户抓取爆破：https://github.com/blackye/Jenkins
- discuz漏洞扫描：https://github.com/code-scan/dzscan
- CMS攻击框架：https://github.com/chuhades/CMS-Exploit-Framework
- IIS短文件名漏洞扫描：https://github.com/lijiejie/IIS_shortname_Scanner
- flashxss扫描：https://github.com/riusksk/FlashScanner
- 服务器端模板注入漏洞的半自动化工具：https://github.com/coffeehb/SSTIF
- 服务器端模板注入漏洞检测与利用工具：https://github.com/epinna/tplmap
- docker扫描工具：https://github.com/cr0hn/dockerscan
- 借助DNS解析来检测Java反序列化漏洞工具：https://github.com/GoSecure/break-fast-serial
- 脏牛提权漏洞exp：https://github.com/dirtycow/dirtycow.github.io
- Jenkins漏洞探测，用户抓取爆破: https://github.com/blackye/Jenkins
- 首款集成化的Discuz扫描工具: https://github.com/code-scan/dzscan

- 一款简洁优雅的CMS扫描利用框架: https://github.com/chuhades/CMS-Exploit-Framework
- IIS短文件名暴力枚举漏洞利用工具: https://github.com/lijiejie/IIS_shortname_Scanner
- flashxss扫描: https://github.com/riusksk/FlashScanner
- 一个起毛服务器端模板注入漏洞的半自动化工具: https://github.com/coffeehb/SSTIF
- 服务器端模板注入漏洞检测与利用工具: https://github.com/epinna/tplmap
- Docker扫描工具: https://github.com/cr0hn/dockerscan
- 一款精简的wordpress扫描工具: https://github.com/m4ll0k/WPSeku
- 集成化wordpress漏洞利用框架: https://github.com/rastating/wordpress-exploit-framework
- 用于扫描J2EE应用的一款burpsuite插件: https://github.com/ilmila/J2EEScan
- 一款基于perl的strut2的历史漏洞扫描器: https://github.com/riusksk/StrutScan
- 本地文件包含漏洞利用及扫描工具，支持反弹shell: https://github.com/D35m0nd142/LFISuite
- 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/0x4D31/salt-scanner
- 自动化探测客户端AngularJS模板注入漏洞工具: https://github.com/tijme/angularjs-csti-scanner
- Java编写的IIS短文件名暴力枚举漏洞利用工具: https://github.com/irsdl/IIS-ShortName-Scanner
- 基于WPScan以及WPSeku的优化版wordpress扫描器: https://github.com/swisskyrepo/Wordpresscan
- CMS渗透测试框架: https://github.com/CHYbeta/cmsPoc
- CRLF注入漏洞批量扫描: https://github.com/rudSarkar/crlf-injector
- 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/3gstudent/Smbtouch-Scanner
- 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/utiso/dorkbot
- 本地文件包含漏洞利用及扫描工具，支持反弹shell: https://github.com/OsandaMalith/LFiFreak
- 用于枚举脚本的GET / POST未知参数字段: https://github.com/mak-/parameth
- struts2的漏洞全版本检测和利用工具: https://github.com/Lucifer1993/struts-scan
- SSL漏洞扫描，例如心脏滴血漏洞等: https://github.com/hahwul/a2sv
- 基于搜索引擎的漏洞网页搜寻: https://github.com/NullArray/DorkNet
- 用于攻击爆破Java Remote Method Invocation服务的工具: https://github.com/NickstaDB/BaRMIe
- 扫描js扩展库的常见漏洞: https://github.com/RetireJS/grunt-retire
- 针对的hadoop /火花等大数据平台的的漏洞探测工具: https://github.com/kotobukki/BDA
- RegEx拒绝服务扫描器: https://github.com/jagracey/Regex-DoS
- 使用NMAP扫描的Tor网络上隐藏的“洋葱”服务: https://github.com/milesrichardson/docker-onion-nmap
- 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/Moham3dRiahi/XAttacker
- 一个迷你的信息泄漏批量扫描脚本: https://github.com/lijiejie/BBScan
- 文件上传漏洞扫描器及利用工具: https://github.com/almandin/fuxploider
- 子域名接管漏洞检测工具，支持30+云服务托管检测: https://github.com/Ice3man543/SubOver
- WordPress的漏洞扫描器，同时也支持敏感文件泄露扫描: https://github.com/Jamalc0m/wphunter

- 检测网站依赖的JavaScript库中存在的已知通用漏洞: https://github.com/retirejs/retire.js
- 自动检测上传功能是否可上传webshell: https://github.com/3xp10it/xupload
- CMS指纹识别及自动化渗透测试框架: https://github.com/mobrine-mob/M0B-tool
- 论坛框架vBulletin黑盒漏洞扫描器: https://github.com/rezasp/vbscan
- CMS指纹识别及自动化渗透测试框架: https://github.com/MrSqar-Ye/BadMod
- CMS漏洞检测和利用套件: https://github.com/Tuhinshubhra/CMSeeK
- AWS安全审计工具: https://github.com/cloudsploit/scans
- 针对wp，magento，joomla等CMS的漏洞扫描器及自动利用工具: https://github.com/radenvodka/SVScanner
- OWASP旗下joomla漏洞扫描项目: https://github.com/rezasp/joomscan
- 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/6IX7ine/djangohunter

25. LICENSE