

Forum:[Hack Forums](#)

Thread: [\[Pen-Testing Tools:\]>_HUGE collection for all pen-testing enthusiasts](#)

mObile - July 2, 2018, 12:28 pm

Here's a huge collection of some very useful pen-testing tools for any pentesting enthusiast. Though there are many within the list that I already use. There's so many more I've never heard of or even tested but look very useful so I thought I'd share. ?

- Fuzz tools to collect:

Spoiler ([Click to View](#))

<https://github.com/ivanfratric/winafi>

<https://github.com/attekett/NodeFuzz>

<https://github.com/google/oss-fuzz>

http://blog.topsec.com.cn/ad_lab/alphafuzzer/

<http://llvm.org/docs/LibFuzzer.html>

<https://github.com/Fuzzapi/>

<https://github.com/mseclab/PyJFuzzer> Python JSON Fuzzer

- Subdomain Enumeration:

Spoiler ([Click to View](#))

<https://github.com/lijiejie/subDomainsBrute> (classic subdomain explosion enumeration script)

<https://github.com/ring04h/wydomain> (subdomain dictionary exhaustive)

<https://github.com/le4f/dnsmaper> (Subdomain Enumeration with Map Markers)

<https://github.com/0xbug/orangescan> (Online Subdomain Information Collection Tool)

<https://github.com/TheRook/subbrute> (Search subdomains based on DNS records)

<https://github.com/We5ter/GSDF> (Google SSL transparent certificate based subdomain query script)

https://github.com/mandatoryprogrammer/cloudflare_enum (a script that uses CloudFlare to enumerate subdomains)

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

<https://github.com/quelfoweb/knock> (Knock Subdomain Scan)

<https://github.com/Evi1CLAY/CoolPool/tree/master/Python/DomainSeeker> (Multi-collection target sub-domain information)

<https://github.com/code-scan/BroDomain> (brother domain name query)

<https://github.com/chuhades/dnsbrute> (enumeration of subdomains based on dns queries)

<https://github.com/bit4woo/Teemo> (domain name collection and enumeration tools)

- Web Application Scanner:

Spoiler ([Click to View](#))

<http://github.com/Arachni/arachni> (web application security scanner framework

<http://www.arachni-scanner.com>)

- Database Scanning, Injection Tools:

Spoiler ([Click to View](#))

<https://github.com/sqlmapproject/sqlmap> (King injecting tools sqlmap)

<https://github.com/ron190/jsql-injection> (jsql-injection java write injection tool to support the full database)

<https://github.com/0xbug/SQLiScanner> (a passive SQL injection vulnerability scanning tool based on SQLMAP and Charles)

<https://github.com/stamparm/DSSS> (99 lines of code to achieve sql injection vulnerability scanner, the general effect)

<https://github.com/youngyangyang04/NoSQLAttack> (a mongoDB attack tools)

<https://github.com/Neohapsis/bbqsql> (SQL blind use framework)

<https://github.com/NetSPI/PowerUpSQL> (Powershell scripting framework attacking SQL Server)

<https://github.com/WhitewidowScanner/whitewidow> (yet another database scanner)

<https://github.com/stampery/mongoaudit> (MongoDB Audit and Infiltration Tool)

<https://github.com/commixproject/commix> (Injection Point Command Execution Utilization Tool)

• Weak passwords or information leakage scanning, hash identification:

Spoiler ([Click to View](#))

<https://github.com/lijiejie/httpwdScan> (a simple HTTP brute-force attack, hit the database attack script)

<https://github.com/lijiejie/BBScan> (a mini-spill bulk scanning script)

<https://github.com/lijiejie/GitHack> (.git folder leak utility)

<https://github.com/LoRexxar/BScanner> (dictionary-based directory scanning gadget)

<https://github.com/wilson9x1/fenghuangscanner> (various ports and weak password detection)

<https://github.com/ysrc/F-Scrack> (script for weak password detection on various services)

<https://github.com/Mebus/cupp> (based on user habits to generate weak password detection dictionary script)

<https://github.com/RicterZ/genpAss> (Chinese weak password generator)

https://github.com/netxfly/crack_ssh (go co-written version of the ssh \ redis \ mongodb weak password cracking tools)

<https://github.com/n0tr00t/Sreg> (all Internet passport information registered by the user by returning email, phone, username)

<https://github.com/repoog/GitPrey> (GitHub Sensitive Information Scanner)

<https://github.com/dxa4481/truffleHog> (GitHub sensitive information scanning tools, including the detection of commit, etc.)

<https://github.com/LandGrey/pydictor> (brute force dictionary creation tool)

<https://github.com/GDSSecurity/xxe-recursive-download> (xxe loopholes recursive download tool)

<https://buer.haus/xxegen/> (xxe online build utility)

<https://github.com/AnimeshShaw/Hash-Algorithm-Identifier> (support more than 160 kinds of Hash encryption recognition)

<https://github.com/x90skysn3k/brutespry> (through nmap scan results to blast a variety of protocols weak password)

• IoT device scanning:

Spoiler ([Click to View](#))

<https://github.com/rapid7/IoTSeeker> (IoT device default password scan detection tool)

<https://github.com/shodan-labs/iotdb> (Scanning for IoT devices using nmap)

<https://github.com/jh00nbr/Routerhunter-2.0> (router vulnerability scanning)

<https://github.com/reverse-shell/routersploit> (Router Exploit Framework)

<https://github.com/scu-igroup/telnet-scanner> (telnet service password crash library)

<https://github.com/RUB-NDS/PRET> (Printer Attack Framework)

• XSS use related:

Spoiler ([Click to View](#))

<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 version of the reflective xss scan)
https://github.com/chuhades/xss_scan (batch scan xss python script)
<https://github.com/BlackHole1/autoFindXssAndCsrf> (browser plug-in to automate page inspection for XSS and CSRF vulnerabilities)
<https://github.com/bsmali4/xssfork> (a xss detection tools)
<https://github.com/evilcos/xssor2> (Hack with JavaScript)
<https://github.com/bugbountyforum/XSS-Radar> (A Chrome extension for fast and easy XSS fuzzing)

- Enterprise network self-test:

Spoiler ([Click to View](#))

<https://github.com/sowish/LNScan> (Detailed Internal Network Information Scanner)
<https://github.com/SkyLined/LocalNetworkScanner> (local network scanner implemented by javascript)
<https://github.com/ysrc/xunfeng> (Network Asset Identification Engine, Vulnerability Assessment Engine)
<https://github.com/laramies/theHarvester> (corporate search engine contains sensitive asset information monitoring script: employee mailbox, subdomains, Hosts)
<https://github.com/x0day/Multisearch-v2> (Search Engine Aggregation Search, which can be used to discover sensitive asset information that your business has been indexed by search engines)

- Collection of (asp,aspx,php,jsp,pl,py,C# and so on) Webshells:

Spoiler ([Click to View](#))

<https://github.com/tennc/webshell> (asp,aspx,php,jsp,pl,py)
<https://github.com/ysrc/webshell-sample> (asp,aspx,php,jsp)
<https://github.com/tdifg/WebShell> (asp,aspx,php,jsp,pl,py,C# and so on)
<https://github.com/bartblaze/PHP-backdoors> (Only PHP)
<https://github.com/xl7dev/WebShell> (asp,aspx,php,jsp,pl,py,mysql,ssh and so on)
<https://github.com/tanjiti/webshellSample> (asp,aspx,php,jsp)
<https://github.com/mattiasgeniar/php-exploit-scripts> (Only PHP)
<https://github.com/JohnTroony/php-webshells> (Only PHP)

- Webshell detection and virus analysis tools:

Spoiler ([Click to View](#))

<https://github.com/We5ter/Scanners-Box/tree/master/webshell/> (Simple php backdoor detection tool and webshell sample library)
<https://github.com/ym2011/ScanBackdoor> (Webshell scanning tool)
<https://github.com/yassineaddi/BackdoorMan> (PHP back door scan)
<https://github.com/he1m4n6a/findWebshell> (another webshell detection tool)
<https://github.com/Tencent/HaboMalHunter> (Hubble Analysis System, Linux System Virus Analysis and Security Detection)
<https://github.com/PlagueScanner/PlagueScanner> (ClamAV, ESET, Bitdefender Antivirus Engine with python)
<https://github.com/nbs-system/php-malware-finder> (a high-efficiency PHP-webshell scanning tool)
<https://github.com/emposha/PHP-Shell-Detector/> (webshell detection tool with up to 99% efficiency)
https://github.com/Huseck/scan_kill_php_shell (Regular killing of PHP nets)

- Intranet security penetration testing tool set:

Spoiler ([Click to View](#))

<https://github.com/0xwindows/VulScritp> (intranet penetration script, including banner scanning, port scanning; various common exploits, etc.)
https://github.com/lcatro/network_backdoor_scanner (Intranet detection framework based on

network traffic)

<https://github.com/fdiskyou/hunter> (Call Windows API Enumerate User Login Information)

<https://github.com/BlackHole1/WebRtcXSS> (automated use of XSS invasion of the intranet)

<https://github.com/AlessandroZ/LaZagne> (native password lookup extraction tool)

<https://github.com/huntergregal/mimipenguin> (linux password capture artifact)

• Port scanning, fingerprinting and middleware scanning:

Spoiler ([Click to View](#))

<https://nmap.org/download.html> (King of Nmap Port Scanner, <https://svn.nmap.org/>)

<https://github.com/ring04h/wyportmap> (Target Port Scan + System Service Fingerprint

Identification)

<https://github.com/ring04h/weakfilesan> (Dynamic Multithreading Sensitive Information Disclosure Detection Tool)

<https://github.com/EnableSecurity/wafw00f> (WAF Fingerprinting)

<https://github.com/rbsec/sslsan> (ssl type identification)

<https://github.com/urbanadventurer/whatweb> (web fingerprinting)

<https://github.com/tanjiti/FingerPrint> (web application fingerprinting)

<https://github.com/nanshihui/Scan-T> (web crawler fingerprinting)

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

<https://github.com/ywolf/F-NAScan> (Network Asset Information Scanning, ICMP Survival Probing,

Port Scanning, Port Fingerprint Service Identification)

<https://github.com/ywolf/F-MiddlewareScan> (middleware scanning)

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

<https://github.com/x0day/bannerscan> (C section banner and path scan)

<https://github.com/RASec/RAScan> (Port Services Scan)

https://github.com/3xp10it/bypass_waf (waf automatically break)

<https://github.com/3xp10it/xcdn> (try to figure out the real ip behind cdn)

<https://github.com/Xyntax/BingC> (Bing search engine based on the C segment / bypass query,

multi-threaded, support API)

<https://github.com/Xyntax/DirBrute> (multi-threaded WEB directory blasting tool)

<https://github.com/zer0h/httpscan> (a web crawler web crawler gadget)

<https://github.com/lietdai/doom> (ip port vulnerability scanner for distributed task distribution on

thorn)

<https://github.com/chichou/grab.js> (Similar to zgrab's fast TCP fingerprinting resolution tool that supports more protocols)

<https://github.com/Nitr4x/whichCDN> (CDN Identification, Detection)

<https://github.com/secfree/bcrpscan> (Crawler-based web path scanner)

<https://github.com/zerokeeper/WebEye> (a simple script to identify WEB, CMS, WAF, WHOIS, and language frameworks)

• Targeted vulnerability testing tools:

Spoiler ([Click to View](#))

<https://github.com/brianwrf/hackUtils> (java Deserialization Utilization Toolkit)

<https://github.com/frohoff/ysoserial> (java deserialization utility)

<https://github.com/mbechler/marshalsec> (java, json deserialization utility)

<https://github.com/blackye/Jenkins> (Jenkins vulnerability detection, user crawling blasting)

<https://github.com/code-scan/dzscan> (discuz vulnerability scanning)

<https://github.com/chuhades/CMS-Exploit-Framework> (CMS Attack Framework)

https://github.com/lijiejie/IIS_shortcode_Scanner (IIS short file name vulnerability scanning)

<https://github.com/riusksk/FlashScanner> (flashxss scan)

<https://github.com/coffeehb/SSTIF> (a semi-automated tool for server-side template injection vulnerabilities)

<https://github.com/epinna/tplmap> (server-side template injection vulnerability detection and

utilization tools)

<https://github.com/cr0hn/dockerscan> (docker scanning tool)

<https://github.com/GoSecure/break-fast-serial> (Detects Java Deserialization Vulnerability Tools with DNS Resolve)

<https://github.com/dirtycow/dirtycow.github.io> (dirty oxi expiration exp)

<https://github.com/lianfeng30/githubscan> (github code leak scanning)

<https://github.com/Lucifer1993/struts-scan> (open source Struts2 full version vulnerability detection tool)

<https://github.com/Lucifer1993/AngelSword> (CMS3 prepared by the CMS vulnerability detection framework)

- Wireless network penetration, scanning:

Spoiler ([Click to View](#))

<https://github.com/savio-code/fern-wifi-cracker/> (Wireless Security Auditing Tool)

<https://github.com/m4n3dw0lf/PytheM> (Python Network / Penetration Test Tool)

<https://github.com/P0cL4bs/WiFi-Pumpkin> (Wireless Security Penetration Test Suite)

<https://github.com/chrisk44/Hijacker/> (an All-in-One Android-side WiFi Cracker)

- Code static scanning, code running stack tracking:

Spoiler ([Click to View](#))

<https://github.com/exakat/php-static-analysis-tools> (php static scan toolset)

<https://github.com/wufeifei/cobra> (white box code security audit system)

<https://github.com/LoRexxar/Cobra-W> (cobra white hat version)

<https://github.com/OneSourceCat/phpvulhunter> (static php code audit)

<https://github.com/Qihoo360/phptrace> (tool to track and analyze PHP's behavior)

<https://github.com/ajinabraham/NodeJsScan> (NodeJS Application Code Audit)

<https://github.com/pwnsdx/BadCode> (PHP Code Audit)

<https://github.com/thesp0nge/dawnscanner> (ruby source audit)

<https://github.com/presidentbeef/brakeman> (Ruby on Rails application security holes)

<https://github.com/ajinabraham/Mobile-Security-Framework-MobSF/> (app Black Box Audit)

<https://github.com/alibaba/iOSSecAudit> (iOS Security Audit)

<http://findbugs.sourceforge.net/> (java source audit, support for the IDE)

<https://github.com/find-sec-bugs/find-sec-bugs> ((java source security audit, support for the IDE)

<http://magic.360.cn/zh/index.html> (FireWire 360 Fireline is free static code analysis tool, tend Andrews code audit recommended)

<https://github.com/facebook/infer> (Java, Objective-C and C, written in OCaml, Recommended)

<https://github.com/Tencent/TscanCode> (TscanCode is a static code scanning solution for C ++ / C # / Lua code, produced by Tencent)

<https://github.com/chaitin/passionfruit> (Open Source iOS Application Security Analysis Tool)

<https://github.com/shengqi158/pyvulhunter> (python code audit tool)

<https://github.com/openstack/bandit> (Python code audit tool based on the AST syntax tree from the OpenStack security team)

<https://github.com/openstack/syntribos> (Python API Code Auditing Tool from the OpenStack Security Team)

<https://github.com/python-security/pyt> (python web code audit tool)

<https://github.com/spotbugs/spotbugs> (SpotBugs is the successor to FindBugs, a static analysis tool to find bugs in Java code)

- Modular scanning, integrated scanner:

Spoiler ([Click to View](#))

<https://github.com/az0ne/AZScanner> (Automatic Vulnerability Scanner, Subdomain Blasting, Port Scanning, Directory Burst, Common Framework Vulnerability Detection)

<https://github.com/blackye/lalascan> (Distributed web vulnerability scanning framework, collection

owasp top10 vulnerability scanning and border asset discovery capabilities)
<https://github.com/blackye/BkScanner> (BkScanner Distributed, Plug-In Web Vulnerability Scanner)
<https://github.com/ysrc/GourdScanV2> (Passive Vulnerability Scan)
<https://github.com/alpha1e0/pentestdb> (WEB penetration test database)
https://github.com/netxfly/passive_scan (http proxy based web vulnerability scanner)
<https://github.com/1N3/Sn1per> (Automated scanners, including middleware scanning and device fingerprinting)
https://github.com/RASec/pentestEr_Fully-automatic-scanner (Directional Fully Automated Penetration Testing Tool)
<https://github.com/3xp10it/3xp10it> (Automated Penetration Test Framework)
<https://github.com/Lcys/lcyscan> (Scanning results are not verified)
<https://github.com/Xyntax/POC-T> (penetration testing plug-in concurrent framework)
<https://github.com/v3n0m-Scanner/V3n0M-Scanner> (Scanner in Python3.5 for SQLi/XSS/LFI/RFI and other Vulns)
<https://github.com/Skycrab/leakScan> (web-side online vulnerability scanning)

- Industrial safety tools set:

Spoiler ([Click to View](#))

<http://icsmaster.com/tool/icstools.html>

- Android series tools:

Spoiler ([Click to View](#))

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

https://github.com/blackarbiter/Android_Code_Arbiter (Source Security Scanner for Android Studio, modified according to Find-Sec-Bugs)

- DDOS protection:

Spoiler ([Click to View](#))

<https://github.com/ywjt/Dshield>

- Database firewall

Spoiler ([Click to View](#))

<https://nim4.github.io/DBShield/>

- WAF open source and rules:

Spoiler ([Click to View](#))

<https://github.com/xsec-lab/x-waf>

https://github.com/loveshell/nginx_lua_waf

<https://github.com/SpiderLabs/owasp-modsecurity-crs/>

https://github.com/lanzsec/tengine_waf

- Honey jar:

Spoiler ([Click to View](#))

<https://github.com/dtag-dev-sec/> (Pot multi honeypot platform, reference article
<http://www.freebuf.com/sectool/134504.html>)

<https://github.com/threatstream/mhn>

<https://github.com/micheloosterhof/cowrie>

<https://github.com/ohmyadd/wetland> (Paramiko's highly interactive SSH honeypots)

<https://github.com/gento/dionaea>

<https://github.com/atiger77/Dionaea> (Web_Dionaea: Honeypot system based on Docker)

<https://github.com/Cymmetria/StrutsHoneypot>

<https://github.com/mushorg/conpot> (Industrial Honey Pot)

SOURCE:

Spoiler ([Click to View](#))

PHP Code

<?php

<https://github.com/she11c0der/Scanners-Box>

#Legends4life

#WillHack4Food

Dr. Gonzo - July 2, 2018, 12:42 pm

Very nice collection mobile! I will be bookmarking this for future reference/

BARTOLOME - July 2, 2018, 1:44 pm

thank you for giving link

__Digital__ - July 2, 2018, 1:52 pm

Here is another good one for ddos protection, i use this on alot of the servers i manage.

<https://github.com/jgmdev/ddos-deflate>

anonymy - September 29, 2018, 2:21 am

nice and overwhelming collection for share. Thanks for sharing !

DAVID PALMER - September 29, 2018, 12:11 pm

genial !!

merci d'avoir partagé ..

richgang007 - February 11, 2019, 9:43 am

(Sep 29, 2018 12:11 PM)DAVID PALMER Wrote: [CITE](#) genial !!

merci d'avoir partagé ..pas beaucoup d'utilisateurs français ici mon ami ? Comment vas-tu? ?

GO135 - March 2, 2019, 5:55 am

cool!!! thanks for sharing!

Sitrep - March 2, 2019, 10:53 am

This thread is great! Thanks for sharing those awesome tools in a great manner with title and everything!

Banditoclassic - March 12, 2019, 7:54 am

You just saved me a lot of lifetime. Thank you very much for this collection! :)

BTW im very interested in your Web Shell Noob course. i just started to become a bit more active here and follow up with you asap. Have a great day!

tulamba - December 9, 2019, 7:54 pm

How can I enroll in your course?

Abducted - December 21, 2019, 11:30 am

Adding an entry for the [RALEPES](#) as version v0.2.2 has been released.

