Your contributions and suggestions are heartily welcome. Please check the [Contributing Guidelines](https://github.com/ByteSnipers/awesome-pentest-cheat-sheets/blob/main/.github/CONTRIBUTING.md) for more details.

Security Talks and Videos

- [Cybersecurity Conference Directory](https://infosec-conferences.com/site-map/#allevents) - All Cybersecurity, InfoSec & IT Conferences and Events.
- [Confsec](https://github.com/cryptax/confsec) - List of Security Events 2024.
- [InfoCon](https://infocon.org/cons/) - The Hacking Conference Archive.
- [Awesome Security Talks](https://github.com/PaulSec/awesome-sec-talks) - Curated list of Security Talks and Videos.

General cheat sheets

- [The Hackers' Choice Tips & Tricks Cheatsheet](https://github.com/hackerschoice/thc-tips-tricks-hacks-cheat-sheet)
- [Docker Cheat Sheet](https://github.com/wsargent/docker-cheat-sheet)
- [macOS Command Line Cheat Sheet](https://github.com/herrbischoff/awesome-osx-command-line)
- [PowerShell Cheat Sheet](https://pen-testing.sans.org/blog/2016/05/25/sans-powershell-cheat-sheet) - SANS PowerShell Cheat Sheet from SEC560 Course [(PDF version)](docs/PowerShellCheatSheet_v41.pdf).
- [Rawsec's CyberSecurity Inventory](https://inventory.raw.pm/) - An open-source inventory of tools, resources, CTF platforms and Operating Systems about CyberSecurity. ([Source](https://gitlab.com/rawsec/rawsec-cybersecurity-list)).
- [Regexp Security Cheat Sheet](https://github.com/attackercan/regexp-security-cheatsheet)
- [Security Cheat Sheets](https://github.com/teamghsoftware/security-cheatsheets) - A collection of security cheat sheets.
- [Unix Commands Cheat Sheet](https://www.stationx.net/unix-commands-cheat-sheet/)
- [Linux File Permissions Cheat Sheet](https://www.stationx.net/linux-file-permissions-cheat-sheet/)
- [DostoevskyLabs' Pentest notes](https://dostoevskylabs.gitbooks.io/dostoevskylabs-pentest-notes/content/) - Pentest Notes collection from DostoevskyLabs.
- [Thick Client Pentest Checklist](https://github.com/Hari-prasaanth/Thick-Client-Pentest-Checklist) - Pentest Checklist for Thick-Client Penetration Tests.
- [HauSec's Pentesting Cheat sheet](https://hausec.com/pentesting-cheatsheet/) - Pentest Cheat sheet from HauSec.

Mobile Pentesting

- [Mobile App Pentest Cheat Sheet](https://github.com/tanprathan/MobileApp-Pentest-Cheatsheet) - Collection of resources on Apple & iOS Penetration Testing.
- [Mobexler](https://mobexler.com/) - Customised virtual machine, designed to help in penetration testing of Android & iOS applications.

Android

- [Android Pentest Checklist Xmind](https://xmind.app/m/GkgaYH/#) - Xmind mindmap for Android Penetration Tests.
- [MASTG](https://github.com/OWASP/owasp-mastg) - OWASP Mobile Application Security Testing Guide [[PDF]](https://github.com/OWASP/owasp-mastg/releases/download/v1.4.0/OWASP_MSTG-v1.4.0.pdf).
- [Android Pentesting Checklist](https://github.com/Hrishikesh7665/Android-Pentesting-Checklist) -

Case-by-case Checklist for Android Pentests.
- [Android Pentesting Cheat sheet](https://github.com/ivan-sincek/android-penetration-testing-cheat-sheet) - Android Pentesting Resources #1.
- [HackTricks - Android Pentesting](https://book.hacktricks.xyz/mobile-pentesting/android-app-pentesting) - HackTricks Collection of Android Pentesting.

Vulnerable Android Applications

- [InjuredAndroid](https://github.com/B3nac/InjuredAndroid)
- [Damn vulnerable Bank](https://github.com/rewanthtammana/Damn-Vulnerable-Bank)
- [InsecureShop](https://github.com/optiv/InsecureShop)
- [AndroGoat](https://github.com/satishpatnayak/AndroGoat)
- [Android-Insecurebankv2](https://github.com/dineshshetty/Android-InsecureBankv2)
- [OVAA](https://github.com/oversecured/ovaa)
- [DIVA](https://github.com/payatu/diva-android)

Apple

- [iOS Pentest Checklist](https://github.com/ivan-sincek/ios-penetration-testing-cheat-sheet) - Checklist for iOS/IPA Penetration Tests.
- [Hacktricks iOS Checklist](https://book.hacktricks.xyz/mobile-pentesting/ios-pentesting-checklist) - Another Checklist for iOS/IPA Penetration Tests | Hacktricks Cloud.
- [PentestGlobal IOS gitbook](https://ios.pentestglobal.com/) - Gitbook about iOS Pentesting.
- [Can i jailbreak?](https://canijailbreak.com/) - List of each jailbreak needed for each iOS version.
- [Jailbreaks.app](https://jailbreaks.app/) - Downloads for Odyssey, Taurine Jailbreaks.

Cloud Pentesting

Kubernetes

- [Awesome Kubernetes (K8s) Security](https://github.com/magnologan/awesome-k8s-security) - Collection of Kubernetes security resources.
- [Kubetools](https://collabnix.github.io/kubetools/#security-tools) - Kubernetes security tools.
- [HackingKubernetes](https://github.com/g3rzi/HackingKubernetes) - Collection of Kubernetes Pentesting Resources.
- [Kubernetes Goat](https://github.com/madhuakula/kubernetes-goat) - Vulnerable-by-Design cluster environment for training.
- [KubePwn](https://github.com/alexivkin/kubepwn) - Another Collection of resources about Kubernetes security.
- [HackTricks - Kubernetes Pentesting](https://cloud.hacktricks.xyz/pentesting-cloud/kubernetes-security) - HackTricks Collection of Kubernetes Pentesting.

Kubernetes Pentest Methodology (CyberArk)

- [Part 1](https://cyberark.com/resources/threat-research-blog/kubernetes-pentest-methodology-part-1)
- [Part 2](https://www.cyberark.com/resources/threat-research-blog/kubernetes-pentest-methodology-part-2)
- [Part 3](https://www.cyberark.com/resources/threat-research-blog/kubernetes-pentest-methodology-part-3)

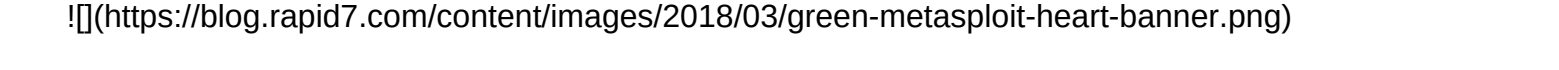
Azure

- [Awesome Azure Pentest](https://github.com/Kyuu-Ji/Awesome-Azure-Pentest) - A curated list of useful tools and resources for penetration testing and securing Microsofts cloud platform Azure.
- [HackTricks - Azure Pentesting](https://cloud.hacktricks.xyz/pentesting-cloud/azure-security) - HackTricks Collection of Kubernetes Pentesting.

Active Directory

- [Active Directory Exploitation Cheat Sheet](https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet) - Cheat sheet for Active Directory Exploitation.
- [OSCP Active Directory Cheat Sheet](https://github.com/brianlam38/OSCP-2022/blob/main/cheatsheet-active-directory.md) - Cheat sheet for Active Directory Attacks used in OSCP.
- [WADComs](https://wadcoms.github.io/) - Interactive cheat sheet - list of offensive security tools and their respective commands to be used against Windows/AD environments.
- [HackTricks - Active Directory Pentesting](https://book.hacktricks.xyz/windows-hardening/active-directory-methodology) - HackTricks Collection of Active Directory Pentesting.
- [GOAD](https://github.com/Orange-Cyberdefense/GOAD) - Vulnerable-by-Design Active Directory environment.
- [Ultimate BloodHound Guide](https://m4lwhere.medium.com/the-ultimate-guide-for-bloodhound-community-edition-bhce-80b574595acf) - The Ultimate Guide for BloodHound Community Edition (BHCE).
- [Windows Red Team Cheat sheet](https://github.com/morph3/Windows-Red-Team-Cheat-Sheet) - Windows for Red Teamers Cheat Sheet ([Moved to wiki](https://notes.morph3.blog/)).
- [Resource Collection #1](https://github.com/DeanOfCyber/Active-Directory-Penetration-Testing-and-Security) - Collection of Active Directory Pentesting resources #1.
- [Resource Collection #2](https://github.com/AD-Attacks/Active-Directory-Penetration-Testing) - Collection of Active Directory Pentesting resources #2.
- [Resource Collection #3](https://github.com/geeksniper/active-directory-pentest) - Collection of Active Directory Pentesting resources #3.
- [Resource Collection #4](https://github.com/Integration-IT/Active-Directory-Exploitation-Cheat-Sheet) - Collection of Active Directory Pentesting resources #4.

Pentest Methodology



Discovery

- [Google Dorks](https://www.exploit-db.com/google-hacking-database) - Google Dorks Hacking Database (Exploit-DB).
- [Shodan](https://github.com/ByteSnipers/awesome-pentest-cheat-sheets/blob/main/docs/shodan.md) - Shodan is a search engine for finding specific devices, and device types, that exist online.
- [ZoomEye](http://zoomeye.org) - Zoomeye is a Cyberspace Search Engine recording information of devices, websites, services and components etc.
- [Amass](https://github.com/OWASP/Amass) - OWASP Network mapping of attack surfaces and external asset discovery using open source information.

- [Censys](https://search.censys.io/) - Similar to shodan, search engine for specific devices including IoT.

Enumeration

- [enum4linux-ng](https://github.com/cddmp/enum4linux-ng) - Python tool for enumerating information from Windows/Samba systems.
- [0xdf - SMB Enumeration](https://0xdf.gitlab.io/2024/03/21/smb-cheat-sheet.html) - 0xdf's SMB Enumeration Cheat Sheet.
- [OSCP Enumeration Cheat sheet](https://github.com/oncybersec/oscp-enumeration-cheat-sheet) - Cheat sheet for Enumeration for OSCP Certificate.
- [CrackMapExec Cheatsheet](https://cheatsheet.haax.fr/windows-systems/exploitation/crackmapexec/) - Cheat sheet for CrackMapExec (CME).

Exploitation

- [Empire Cheat Sheet](https://github.com/HarmJ0y/CheatSheets/blob/master/Empire.pdf) - [Empire](http://www.powershellempire.com) is a PowerShell and Python post-exploitation framework.
- [Exploit Development Cheat Sheet](https://github.com/ByteSnipers/awesome-pentest-cheat-sheets/blob/main/docs/pentest-exploit-dev-cheatsheet.jpg) - [@ovid](https://twitter.com/ovid)'s exploit development in one picture.
- [Java Deserialization Cheat Sheet](https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet) - A cheat sheet for pentesters about Java Native Binary Deserialization vulnerabilities.
- [Local File Inclusion (LFI) Cheat Sheet #1](https://highon.coffee/blog/lfi-cheat-sheet/) - Arr0way's LFI Cheat Sheet.
- [Local File Inclusion (LFI) Cheat Sheet #2](https://www.aptive.co.uk/blog/local-file-inclusion-lfi-testing/) - Aptive's LFI Cheat Sheet.
- [Metasploit Unleashed](https://www.offensive-security.com/metasploit-unleashed/) - The ultimate guide to the Metasploit Framework.
- [Metasploit Cheat Sheet](https://www.tunnelsup.com/metasploit-cheat-sheet/) - A quick reference guide [(PNG version)](docs/Metasploit-CheatSheet.png)[(PDF version)](docs/Metasploit-CheatSheet.pdf).
- [PowerSploit Cheat Sheet](https://github.com/HarmJ0y/CheatSheets/blob/master/PowerSploit.pdf) - [PowerSploit](https://github.com/PowerShellMafia/PowerSploit) is a powershell post-exploitation framework.
- [PowerView 2.0 Tricks](https://gist.github.com/HarmJ0y/3328d954607d71362e3c)
- [PowerView 3.0 Tricks](https://gist.github.com/HarmJ0y/184f9822b195c52dd50c379ed3117993)
- [PHP htaccess Injection Cheat Sheet](https://github.com/sektioneins/pcc/wiki/PHP-htaccess-injection-cheat-sheet) - PHP htaccess Injection Cheat Sheet by PHP Secure Configuration Checker.
- [Reverse Shell Cheat Sheet #1](http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet) - Pentestmonkey Reverse Shell Cheat Sheet.
- [Reverse Shell Cheat Sheet #2](https://highon.coffee/blog/reverse-shell-cheat-sheet) - Arr0way's Reverse Shell Cheat Sheet.
- [SQL Injection Cheat Sheet](https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet) - Netsparker's SQL Injection Cheat Sheet.
- [SQLite3 Injection Cheat Sheet](http://atta.cked.me/home/sqlite3injectioncheatsheet)

Post-Exploitation

- [Awesome Windows Post Exploitation](https://github.com/emilyanncr/Windows-Post-Exploitation) - Collection of resources for Windows Post-Exploitation.
- [HackTricks - Post Exploitation](https://book.hacktricks.xyz/todo/post-exploitation) - HackTricks Collection of Post-Exploitation.

Privilege Escalation

Learn Privilege Escalation

- [Windows / Linux Local Privilege Escalation Workshop](https://github.com/sagishahar/lpeworkshop) - The Privilege Escalation Workshop covers all known (at the time) attack vectors of local user privilege escalation on both Linux and Windows operating systems and includes slides, videos, test VMs. <img src="https://pbs.twimg.com/media/DAZsE2VUQAA_bpZ.jpg">.

 Linux Privilege Escalation

- [Basic Linux Privilege Escalation](https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/) - Linux Privilege Escalation by [@g0tmi1k](https://twitter.com/g0tmi1k).
- [linux-exploit-suggester.sh](https://github.com/mzet-/linux-exploit-suggester) - Linux privilege escalation auditing tool written in bash (updated).
- [Linux_Exploit_Suggester.pl](https://github.com/PenturaLabs/Linux_Exploit_Suggester) - Linux Exploit Suggester written in Perl (last update 3 years ago).
- [Linux_Exploit_Suggester.pl v2](https://github.com/jondonas/linux-exploit-suggester-2) - Next-generation exploit suggester based on Linux_Exploit_Suggester (updated).
- [Linux Soft Exploit Suggester](https://github.com/belane/linux-soft-exploit-suggester) - Linux-soft-exploit-suggester finds exploits for all vulnerable software in a system helping with the privilege escalation. It focuses on software packages instead of Kernel vulnerabilities.
- [checksec.sh](https://github.com/slimm609/checksec.sh) - Bash script to check the properties of executables (like PIE, RELRO, PaX, Canaries, ASLR, Fortify Source).
- [linuxprivchecker.py](http://www.securitysift.com/download/linuxprivchecker.py) - This script is intended to be executed locally on a Linux box to enumerate basic system info and search for common privilege escalation vectors such as world writable files, misconfigurations, clear-text passwords and applicable exploits (@SecuritySift).
- [LinEnum](https://github.com/rebootuser/LinEnum) - This tool is great at running through a heap of things you should check on a Linux system in the post exploit process. This include file permissions, cron jobs if visible, weak credentials etc.(@Rebootuser).
-
[linPEAS](https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS) - LinPEAS - Linux Privilege Escalation Awesome Script. Check the Local Linux Privilege Escalation checklist from book.hacktricks.xyz.
- [MimiPenguin](https://github.com/huntergregal/mimipenguin) - A tool to dump the login password from the current linux desktop user. Adapted from the idea behind the popular Windows tool mimikatz. .

 Windows Privilege Escalation

- [PowerUp](https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc) - Excellent powershell script for checking of common Windows privilege escalation vectors. Written by [harmj0y](https://twitter.com/harmj0y) [(direct link)](https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1).
- [PowerUp Cheat Sheet](https://github.com/HarmJ0y/CheatSheets/blob/master/PowerUp.pdf)
- [Windows Exploit Suggester](https://github.com/GDSSecurity/Windows-Exploit-Suggester) - Tool for detection of missing security patches on the windows operating system and mapping with the public available exploits.
- [Sherlock](https://github.com/rasta-mouse/Sherlock) - PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities.
- [Watson](https://github.com/rasta-mouse/Watson) - Enumerate missing KBs and suggest exploits for useful Privilege Escalation vulnerabilities.
- [Precompiled Windows Exploits](https://github.com/abatchy17/WindowsExploits) - Collection of precompiled Windows exploits.
- [Metasploit Modules](https://github.com/rapid7/metasploit-framework)
  - post/multi/recon/local_exploit_suggester - suggests local meterpreter exploits that can be used.
  - post/windows/gather/enum_patches - helps to identify any missing patches.

Web Pentesting

- [OWASP Web Security Testing Guide](https://owasp.org/www-project-web-security-testing-guide/v42/)
- [Web Pentest Checklist](https://pentestbook.six2dez.com/others/web-checklist) - Checklist for Web Application Penetration Tests.
- [SQL Injection Cheatsheet](https://portswigger.net/web-security/sql-injection/cheat-sheet) - PortSwigger SQL Injection Cheat Sheet.
- [Cross-Site-Scripting Cheat sheet](https://portswigger.net/web-security/cross-site-scripting/cheat-sheet) - PortSwigger Cross-Site-Scripting (XSS) Cheat sheet.
- [Google CSP Evaluator](https://csp-evaluator.withgoogle.com) - Google's CSP Evaluator [Chrome Extension](https://chromewebstore.google.com/detail/csp-evaluator/fjohamlofnakbnbfjkohkbdigoodcejf)
- [Awesome Web Hacking](https://github.com/infoslack/awesome-web-hacking) - Collection of resources for Web Pentesting #1.
- [Awesome Web Security](https://github.com/qazbnm456/awesome-web-security) - Collection of resources for Web Pentesting #2.

Payloads

- [XSS Polyglot Payloads #1](https://github.com/0xsobky/HackVault/wiki/Unleashing-an-Ultimate-XSS-Polyglot) - Unleashing an Ultimate XSS Polyglot list by 0xsobky.
- [XSS Polyglot Payloads #2](http://polyglot.innerht.ml/) - [@filedescriptor](https://twitter.com/filedescriptor)'s XSS.
- [Browser's-XSS-Filter-Bypass-Cheat-Sheet](https://github.com/masatokinugawa/filterbypass/wiki/Browser's-XSS-Filter-Bypass-Cheat-Sheet) - Excellent List of working XSS bypasses running on the latest version of Chrome, Safari, Edge created by Masato Kinugawa.

Labs

- [PortSwigger Web Penetration Testing Labs](https://portswigger.net/web-security/all-labs)

Binary Exploitation

- [Binary Exploitation Red Team Notes](https://www.ired.team/offensive-security/code-injection-process-injection/binary-exploitation) - Ired.team notes for Binary Exploitation.
- [Binary Exploitation Notes](https://ir0nstone.gitbook.io/notes) - Ir0nstone's Binary Exploitation Notes.
- [Sticky Notes Binary Exploitation](https://exploit-notes.hdks.org/exploit/binary-exploitation/) - Sticky Notes colletion for Binary Exploitation.
- [checksec.py](https://github.com/Wenzel/checksec.py/) - Cross-Platform CheckSec Tool for checking binary security properties.
- [HackTricks - Binary Exploitation](https://book.hacktricks.xyz/binary-exploitation/basic-binary-exploitation-methodology) - HackTricks Collection of Binary Exploitation.
- [Liveoverflow - Binary Exploitation](https://www.youtube.com/playlist?list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN) - LiveOverflow's Binary Exploitation YouTube playlist.
- [PwnTools Cheat sheet](https://gist.github.com/anvbis/64907e4f90974c4bdd930baeb705dedf) - Cheat sheet for PwnTools python library.
- [pwndbg Cheat sheet](https://drive.google.com/file/d/16t9MV8KTFXK7oX_CzXhmDdaVnjT8IYM4/view) -

Cheat sheet for pwndbg GDB plug-in.
- [GDB PEDA Cheat sheet](https://github.com/kibercthulhu/gdb-peda-cheatsheet/blob/master/gdb-peda%20cheatsheet.pdf) - Cheat sheet for PEDA GDB plug-in.

Learning Platforms

Online

- [Hack The Box :: Penetration Testing Labs](https://www.hackthebox.eu) - Leading penetration testing training labs platform.
- [TryHackMe](https://tryhackme.com/) - Free online platform for learning cyber security & penetration testing.
- [OWASP Vulnerable Web Applications Directory Project (Online)](https://owasp.org/www-project-vulnerable-web-applications-directory/#div-online) - List of online available vulnerable applications for learning purposes.
- [Pentestit labs](https://lab.pentestit.ru) - Hands-on Pentesting Labs (OSCP style).
- [Root-me.org](https://www.root-me.org) - Hundreds of challenges are available to train yourself in different and not simulated environments.

Off-Line

- [Vulnhub.com](https://www.vulnhub.com) - Vulnerable By Design VMs for practical 'hands-on' experience in digital security.
- [Damn Vulnerable Xebia Training Environment](https://github.com/davevs/dvxte) - Docker Container including several vurnerable web applications (DVWA,DVWServices, DVWSockets, WebGoat, Juiceshop, Railsgoat, django.NV, Buggy Bank, Mutilidae II and more).
- [OWASP Vulnerable Web Applications Directory Project (Offline)](https://owasp.org/www-project-vulnerable-web-applications-directory/#div-offline) - List of offline available vulnerable applications for learning purposes.
- [Vulnerable SOAP Web Service](https://github.com/anil-yelken/Vulnerable-Soap-Service) - Vulnerable SOAP web service lab environment.
- [Vulnerable Flask Web App](https://github.com/anil-yelken/Vulnerable-Flask-App) - Vulnerable Flask Web App lab environment.

Bug Bounty

- [Awesome BugBounty Tools](https://github.com/vavkamil/awesome-bugbounty-tools) - A curated list of various bug bounty tools.
- [bug-bounty-platforms](https://github.com/disclose/bug-bounty-platforms) - Open-Sourced Collection of Bug Bounty Platforms.
- [m0chan - Bug Bounty Methodology](https://m0chan.github.io/2019/12/17/Bug-Bounty-Cheetsheet.html) - m0chan's Bug Bounty Methodology Collection.
- [NahamSec - Resources for Beginners](https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters) - NahamSec's Resources for Beginner Bug Bounty Hunters Collection.
- [AllAboutBugBounty](https://github.com/daffainfo/AllAboutBugBounty?tab=readme-ov-file) - BugBounty notes gathered from various sources.
- [Bug-Bounty-Resources](https://github.com/Tikam02/Bug-Bounty-Resources) - Collection of Bug Bounty Resources #1.
- [Bug-Bounty-Resources](https://github.com/AnLoMinus/Bug-Bounty) - Collection of Bug Bounty

Resources #2.

Free video courses

- [Ryan John Bug Bounty Playlist](https://www.youtube.com/watch?v=wMO_My5gsDI&list=PLtZtNPs3fJyDUJttw2sJVU69IKfqY7XPn) - Collection of Ryan John's BugBounty videos ([11h Full Course Video](https://www.youtube.com/watch?v=TTw-EY7F1rM)).
- [LiveOverFlow Bug Bounty Playlist](https://www.youtube.com/watch?v=LrLJuyAdoAg&list=PLhixgUqwRTjxKYsPTegCyL5adZaq5eILt) - Collection of LiveOverflow's Bug bounty videos.

Podcasts

- [BBRE Podcast](https://www.youtube.com/watch?v=CfE0-GZk4v8&list=PLvxs_epf2X91Dn3pWeRxPQSV6SWvWqDE3&index=2) - Bug Bounty Reports Explained Podcast.
- [Critical Thinking Podcast](https://www.youtube.com/watch?v=t6cTvajgYsM&list=PLO-h_HEvT1ysKxfLkI-uk3_vxzxoUHCD7) - Critical Thinking Bug Bounty Podcast.

Other resources

Tools

- [Nmap Cheat Sheet](https://github.com/ByteSnipers/awesome-pentest-cheat-sheets/blob/main/docs/nmap.md)
- [SQLmap Cheat Sheet](https://github.com/ByteSnipers/awesome-pentest-cheat-sheets/blob/main/docs/sqlmap-cheatsheet-1.0-SDB.pdf)
- [SQLmap Tamper Scripts](https://forum.bugcrowd.com/t/sqlmap-tamper-scripts-sql-injection-and-waf-bypass/423) - SQLmap Tamper Scripts General/MSSQL/MySQL.
- [VIM Cheatsheet](https://i.imgur.com/YLInLlY.png)
- [Wireshark Display Filters](https://github.com/ByteSnipers/awesome-pentest-cheat-sheets/blob/main/docs/Wireshark_Display_Filters.pdf) - Filters for the best sniffing tool.

Tools Online

- [revshells.com](https://www.revshells.com) - Reverse shell payload generator ([Source code](https://github.com/0dayCTF/reverse-shell-generator)).
- [Segfault](https://www.thc.org/segfault) - Segfault: Free disposable root servers (by [@THC](https://www.thc.org/)).
- suip.biz - Various free online pentesting tools like nmap, wpscan, sqlmap.
- [XSS'OR Encoder/Decoder](http://xssor.io/#ende) - Online Decoder/Encoder for testing purposes (@evilcos).
- [WebGun](https://brutelogic.com.br/webgun/) - WebGun, XSS Payload Creator (@brutelogic).
- [Hackvertor](https://hackvertor.co.uk) - Tool to convert various encodings and generate attack vectors (@garethheyes).
- [JSFiddle](https://jsfiddle.net) - Test and share XSS payloads, [Example PoC](https://jsfiddle.net/xqjpsh65/).

Payloads

- [Fuzzdb](https://github.com/fuzzdb-project/fuzzdb) - Dictionary of attack patterns and primitives for black-box application testing Polyglot Challenge with submitted solutions.
- [SecList](https://github.com/danielmiessler/SecLists) - A collection of multiple types of lists used during security assessments. List types include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads, and many more.

Write-Ups

- [Bug Bounty Reference](https://github.com/ngalongc/bug-bounty-reference) - Huge list of bug bounty write-up that is categorized by the bug type (SQLi, XSS, IDOR, etc.).
- [Write-Ups for CTF challenges](https://ctftime.org/writeups)
- [Facebook Bug Bounties](https://www.facebook.com/notes/phwd/facebook-bug-bounties/707217202701640) - Categorized Facebook Bug Bounties write-ups.

Wireless Hacking

Tools

- [wifite2](https://github.com/coreb1t/wifite2) - Full automated WiFi security testing script .

Defence Topics

- [Docker Security Cheat Sheet](https://container-solutions.com/content/uploads/2015/06/15.06.15_DockerCheatSheet_A2.pdf) - The following tips should help you to secure a container based system [(PDF version)](docs/DockerCheatSheet.pdf).
- [Windows Domain Hardening](https://github.com/PaulSec/awesome-windows-domain-hardening) - A curated list of awesome Security Hardening techniques for Windows.

Programming

- [JavaScript Cheat Sheet](https://github.com/coodict/javascript-in-one-pic) - Learn JavaScript in one picture [(Online version)](https://git.io/Js-pic) [(PNG version)](docs/js-in-one-pic.png).
- [Python Cheat Sheet #1](https://github.com/siyuanzhao/python3-in-one-pic) - Learn python3 in one picture [(PNG version)](docs/python-3-in-one-pic.png).
- [Python Cheat Sheet #2](https://github.com/coodict/python3-in-one-pic) - Learn python3 in one picture [Online version](https://git.io/Coo-py3) [PNG version](docs/py3-in-one-pic.png).
- [Python Snippets Cheat Sheet](https://github.com/ByteSnipers/awesome-pentest-cheat-sheets/blob/main/docs/python-snippets.md) - List of helpful re-usable code snippets in Python.