Bug Bounty Tools

Uncategorized
- **JSONBee** — A ready to use JSONP endpoints/payloads to help bypass content security policy (CSP) of different websites.
- **CyberChef** — The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis
- **bountyplz** — Automated security reporting from markdown templates (HackerOne and Bugcrowd are currently the platforms supported)
- **PayloadsAllTheThings** — A list of useful payloads and bypass for Web Application Security and Pentest/CTF
- **bounty-targets-data** — This repo contains hourly-updated data dumps of bug bounty platform scopes (like Hackerone/Bugcrowd/Intigriti/etc) that are eligible for reports
- **android-security-awesome** — A collection of android security related resources
- **awesome-mobile-security** — An effort to build a single place for all useful android and iOS security related stuff.
- **awesome-vulnerable-apps** — Awesome Vulnerable Applications
- **XFFenum** — X-Forwarded-For [403 forbidden] enumeration
- **httpx** — httpx is a fast and multi-purpose HTTP toolkit allow to run multiple probers using retryablehttp library, it is designed to maintain the result reliability with increased threads.

Vulnerability Scanners
- **nuclei** — Nuclei is a fast tool for configurable targeted scanning based on templates offering massive extensibility and ease of use.
- **Sn1per** — Automated pentest framework for offensive security experts
- **metasploit-framework** — Metasploit Framework
- **nikto** — Nikto web server scanner
- **arachni** — Web Application Security Scanner Framework
- **jaeles** — The Swiss Army knife for automated Web Application Testing
- **retire.js** — scanner detecting the use of JavaScript libraries with known vulnerabilities
- **Osmedeus** — Fully automated offensive security framework for reconnaissance and vulnerability scanning
- **getsploit** — Command line utility for searching and downloading exploits
- **flan** — A pretty sweet vulnerability scanner
- **Findsploit** — Find exploits in local and online databases instantly
- **BlackWidow** — A Python based web application scanner to gather OSINT and fuzz for OWASP vulnerabilities on a target website.
- **backslash-powered-scanner** — inds unknown classes of injection vulnerabilities
- **Eagle** — Multithreaded Plugin based vulnerability scanner for mass detection of web-based applications vulnerabilities
- **OWASP ZAP** — World' s most popular free web security tools and is actively maintained by a dedicated international team of volunteers

Subdomain Takeover
- **subjack** — Subdomain Takeover tool written in Go
- **Subdomain-takeover** — Sub-Domain TakeOver Vulnerability Scanner
- **Sub0ver** — A Powerful Subdomain Takeover Tool
- **autoSubTakeover** — A tool used to check if a CNAME resolves to the scope address. If the CNAME resolves to a non-scope address it might be worth checking out if subdomain takeover is possible.
- **NSBrute** — Python utility to takeover domains vulnerable to AWS NS Takeover
- **can-i-take-over-xyz** — a list of services and how to claim (sub)domains with dangling DNS records
- **cnames** — take a list of resolved subdomains and output any corresponding CNAMES en masse.
- **subHijack** — Hijacking forgotten & misconfigured subdomains
- **tko-subs** — A tool that can help detect and takeover subdomains with dead DNS records
- **HostileSubBruteforcer** — This app will bruteforce for exisiting subdomains and provide information if the 3rd party host has been properly setup.
- **second-order** — Second-order subdomain takeover scanner
- **takeover** — A tool for testing subdomain takeover possibilities at a mass scale.
- **dnsReaper** — DNS Reaper is yet another sub-domain takeover tool, but with an emphasis on accuracy, speed and the number of signatures in our arsenal!

postMessage
- **postMessage-tracker** — A Chrome Extension to track postMessage usage (url, domain and stack) both by logging using CORS and also visually as an extension-icon
- **PostMessage_Fuzz_Tool** — WebDeveloper Tool

JSON Web Token
- **jwt_tool** — A toolkit for testing, tweaking and cracking JSON Web Tokens
- **c-jwt-cracker** — JWT brute force cracker written in C
- **jwt-heartbreaker** — The Burp extension to check JWT (JSON Web Tokens) for using keys from known from public sources
- **jwtear** — Modular command-line tool to parse, create and manipulate JWT tokens for hackers
- **jwt-key-id-injector** — Simple python script to check against hypothetical JWT vulnerability.
- **jwt-hack** — jwt-hack is tool for hacking / security testing to JWT.
- **jwt-cracker** — Simple HS256 JWT token brute force cracker

CMS
- **wpscan** — WPScan is a free, for non-commercial use, black box WordPress security scanner
- **CMSeek** — CMS Detection and Exploitation suite - Scan WordPress, Joomla, Drupal and over 170 other CMSs
- **Droopescan** — A plugin-based scanner that aids security researchers in identifying issues with several CMSs, mainly Drupal & Silverstripe.
- **Drupwn** — Drupal enumeration & exploitation tool
- **WPSpider** — A centralized dashboard for running and scheduling WordPress scans powered by wpscan utility.
- **wprecon** — Wordpress Recon
- **CMSmap** — CMSmap is a python open source CMS scanner that automates the process of detecting security flaws of the most popular CMSs.
- **joomscan** — OWASP Joomla Vulnerability Scanner Project
- **pyfiscan** — Free web-application vulnerability and version scanner

Buckets
- **S3Scanner** — Scan for open AWS S3 buckets and dump the contents
- **AWSBucketDump** — Security Tool to Look For Interesting Files in S3 Buckets
- **CloudScraper** — CloudScraper: Tool to enumerate targets in search of cloud resources. S3 Buckets, Azure Blobs, Digital Ocean Storage Space.
- **s3viewer** — Publicly Open Amazon AWS S3 Bucket Viewer
- **festin** — S3 Bucket Weakness Discovery
- **s3reverse** — The format of various s3 buckets is convert in one format. for bugbounty and security testing.
- **mass-s3-bucket-tester** — This tests a list of s3 buckets to see if they have dir listings enabled or if they are uploadable
- **S3BucketList** — Firefox plugin that lists Amazon S3 Buckets found in requests
- **dirlstr** — Finds Directory Listings or open S3 buckets from a list of URLs
- **Burp-AnonymousCloud** — Burp extension that performs a passive scan to identify cloud buckets and then test them for publicly accessible vulnerabilities
- **kicks3** — S3 bucket finder from html,js and bucket misconfiguration testing tool
- **2tearsinabucket** — Enumerate s3 buckets for a specific target.
- **s3_objects_check** — Whitebox evaluation of effective S3 object permissions, to identify publicly accessible files.
- **s3tk** — A security toolkit for Amazon S3
- **CloudBrute** — Awesome cloud enumerator
- **s3cario** — This tool will get the CNAME first if it's a valid Amazon s3 bucket and if it's not, it will try to check if the domain is a bucket name.
- **S3Cruze** — All-in-one AWS S3 bucket tool for pentesters.

Git
- **GitTools** — A repository with 3 tools for pwn'ing websites with .git repositories available
- **gitjacker** — Leak git repositories from misconfigured websites
- **git-dumper** — A tool to dump a git repository from a website
- **GitHunter** — A tool for searching a Git repository for interesting content
- **dvcs-ripper** — Rip web accessible (distributed) version control systems: SVN/GIT/HG...

Secrets
- **git-secrets** — Prevents you from committing secrets and credentials into git repositories
- **gitleaks** — Scan git repos (or files) for secrets using regex and entropy
- **truffleHog** — Searches through git repositories for high entropy strings and secrets, digging deep into commit history
- **gitGraber** — gitGraber: monitor GitHub to search and find sensitive data in real time for different online services
- **talisman** — By hooking into the pre-push hook provided by Git, Talisman validates the outgoing changeset for things that look suspicious - such as authorization tokens and private keys.
- **GitGot** — Semi-automated, feedback-driven tool to rapidly search through troves of public data on GitHub for sensitive secrets.
- **git-all-secrets** — A tool to capture all the git secrets by leveraging multiple open source git searching tools
- **github-search** — Tools to perform basic search on GitHub.
- **git-vuln-finder** — Finding potential software vulnerabilities from git commit messages
- **commit-stream** — #OSINT tool for finding Github repositories by extracting commit logs in real time from the Github event API
- **gitrob** — Reconnaissance tool for GitHub organizations
- **repo-supervisor** — Scan your code for security misconfiguration, search for passwords and secrets.
- **GitMiner** — Tool for advanced mining for content on Github
- **shhgit** — Ah shhgit! Find GitHub secrets in real time
- **detect-secrets** — An enterprise friendly way of detecting and preventing secrets in code.
- **rusty-hog** — A suite of secret scanners built in Rust for performance. Based on TruffleHog
- **whispers** — Identify hardcoded secrets and dangerous behaviours
- **yar** — Yar is a tool for plunderin' organizations, users and/or repositories.
- **dufflebag** — Search exposed EBS volumes for secrets
- **secret-bridge** — Monitors Github for leaked secrets
- **earlybird** — EarlyBird is a sensitive data detection tool capable of scanning source code repositories for clear text password violations, PII, outdated cryptography methods, key files and more.
- **Trufflehog-Chrome-Extension**

Passwords
- **thc-hydra** — Hydra is a parallelized login cracker which supports numerous protocols to attack.
- **DefaultCreds-cheat-sheet** — One place for all the default credentials to assist the Blue/Red teamers activities on finding devices with default password
- **changeme** — A default credential scanner.
- **BruteX** — Automatically brute force all services running on a target.
- **patator** — Patator is a multi-purpose brute-forcer, with a modular design and a flexible usage.

XXE Injection
- **ground-control** — A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.
- **dtd-finder** — List DTDs and generate XXE payloads using those local DTDs.
- **docem** — Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids)
- **xxeserv** — A mini webserver with FTP support for XXE payloads
- **xxexploiter** — Tool to help exploit XXE vulnerabilities
- **B-XSSRF** — Toolkit to detect and keep track on Blind XSS, XXE & SSRF
- **XXEinjector** — Tool for automatic exploitation of XXE vulnerability using direct and different out of band methods.
- **oxml_xxe** — A tool for embedding XXE/XML exploits into different filetypes

XSS Injection
- **XSStrike** — Most advanced XSS scanner.
- **xssor2** — Hack with JavaScript.
- **xsscrapy** — 66/66 wavsep XSS detected
- **sleepy-puppy** — Sleepy Puppy XSS Payload Management Framework
- **ezXSS** — ezXSS is an easy way for penetration testers and bug bounty hunters to test (blind) Cross Site Scripting
- **xsshunter** — The XSS Hunter service - a portable version of XSSHunter.com
- **dalfox** — DalFox(Finder Of XSS) / Parameter Analysis and XSS Scanning tool based on golang
- **xsser** — Cross Site "Scripter" (aka XSSer) is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based applications.
- **XSpear** — Powerfull XSS Scanning and Parameter analysis tool&gem
- **weaponised-XSS-payloads** — XSS payloads designed to turn alert(1) into P1
- **tracy** — A tool designed to assist with finding all sinks and sources of a web application and display these results in a digestible manner.
- **ground-control** — A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.
- **xssValidator** — This is a burp intruder extender that is designed for automation and validation of XSS vulnerabilities.
- **JSShell** — An interactive multi-user web JS shell
- **bXSS** — bXSS is a utility which can be used by bug hunters and organizations to identify Blind Cross-Site Scripting.
- **docem** — Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids)
- **XSS-Radar** — XSS Radar is a tool that detects parameters and fuzzes them for cross-site scripting vulnerabilities.
- **BruteXSS** — BruteXSS is a tool written in python simply to find XSS vulnerabilities in web application.
- **findom-xss** — A fast DOM based XSS vulnerability scanner with simplicity.
- **domdig** — DOM XSS scanner for Single Page Applications
- **femida** — Automated blind-xss search for Burp Suite
- **B-XSSRF** — Toolkit to detect and keep track on Blind XSS, XXE & SSRF
- **domxssscanner** — DOMXSS Scanner is an online tool to scan source code for DOM based XSS vulnerabilities
- **xsshunter_client** — Correlated injection proxy tool for XSS Hunter
- **extended-xss-search -** — A better version of my xssfinder tool - scans for different types of xss on a list of urls.
- **xssmap** — XSSMap is a tool developed based on Python3 to detect XSS vulnerabilities
- **XSSCon** — Simple XSS Scanner tool
- **BitBlinder** — BurpSuite extension to inject custom cross-site scripting payloads on every form/request submitted to detect blind XSS vulnerabilities
- **XSSOauthPersistence** — Maintaining account persistence via XSS and Oauth
- **shadow-workers** — Shadow Workers is a free and open source C2 and proxy designed for penetration testers to help in the exploitation of XSS and malicious Service Workers (SW)
- **rexsser** — This is a burp plugin that extracts keywords from response using regexes and test for reflected XSS on the target scope.
- **xss-flare** — XSS hunter on cloudflare serverless workers.
- **Xss-Sql-Fuzz** — The burpsuite plugin automatically adds xss sql payload to fuzz all GP parameters (filtering special parameters) with one click
- **vaya-ciego-nen** — Detect, manage and exploit Blind Cross-site scripting (XSS) vulnerabilities.
- **dom-based-xss-finder** — Chrome extension that finds DOM based XSS vulnerabilities
- **XSSTerminal** — Develop your own XSS Payload using interactive typing
- **xss2png** — PNG IDAT chunks XSS payload generator
- **XSSwagger** — A simple Swagger-ui scanner that can detect old versions vulnerable to various XSS attacks

SQL Injection
- **sqlmap** — Automatic SQL injection and database takeover tool
- **NoSQLMap** — Automated NoSQL database enumeration and web application exploitation tool.
- **SQLiScanner** — Automatic SQL injection with Charles and sqlmap api
- **SleuthQL** — Python3 Burp History parsing tool to discover potential SQL injection points. To be used in tandem with SQLmap.
- **mssqlproxy** — mssqlproxy is a toolkit aimed to perform lateral movement in restricted environments through a compromised Microsoft SQL Server via socket reuse
- **sqli-hunter** — SQLi-Hunter is a simple HTTP / HTTPS proxy server and a SQLMAP API wrapper that makes digging SQLi easy.
- **waybackSqliScanner** — Gather urls from wayback machine then test each GET parameter for sql injection.
- **ESC** — Evil SQL Client (ESC) is an interactive .NET SQL console client with enhanced SQL Server discovery, access, and data exfiltration features.
- **mssqli-duet** — SQL injection script for MSSQL that extracts domain users
- **burp-to-sqlmap** — Performing SQLInjection test on Burp Suite Bulk Requests using SQLMap
- **BurpSQLTruncSanner** — Messy BurpSuite plugin for SQL Truncation vulnerabilities.
- **andor** — Blind SQL Injection Tool with Golang
- **Blinder** — A python library to automate time-based blind SQL injection
- **sqliv** — massive SQL injection vulnerability scanner
- **nosqli** — NoSql Injection CLI tool, for finding vulnerable websites using MongoDB

Server Side Request Forgery
- **SSRFmap** — Automatic SSRF fuzzer and exploitation tool
- **Gopherus** — This tool generates gopher link for exploiting SSRF and gaining RCE in various servers
- **ground-control** — A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.
- **SSRFire** — An automated SSRF finder. Just give the domain name and your server and chill! ;) Also has options to find XSS and open redirects
- **httprebind** — Automatic tool for DNS rebinding-based SSRF attacks
- **ssrf-sheriff** — A simple SSRF-testing sheriff written in Go
- **B-XSSRF** — Toolkit to detect and keep track on Blind XSS, XXE & SSRF
- **extended-ssrf-search** — Smart ssrf scanner using different methods like parameter brute forcing in post and get...
- **gaussrf** — Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl and Filter Urls With OpenRedirection or SSRF Parameters.
- **ssrfDetector** — Server-side request forgery detector
- **grafana-ssrf** — Authenticated SSRF in Grafana
- **sentrySSRF** — Tool to searching sentry config on page or in javascript files and check blind SSRF
- **lorsrf** — Bruteforcing on Hidden parameters to find SSRF vulnerability using GET and POST Methods
- **singularity** — A DNS rebinding attack framework.
- **whonow** — A "malicious" DNS server for executing DNS Rebinding attacks on the fly (public instance running on rebind.network:53)
- **dns-rebind-toolkit** — A front-end JavaScript toolkit for creating DNS rebinding attacks.
- **dref** — DNS Rebinding Exploitation Framework
- **rbndr** — Simple DNS Rebinding Service
- **httprebind** — Automatic tool for DNS rebinding-based SSRF attacks
- **dnsFookup** — DNS rebinding toolkit

Request Smuggling
- **http-request-smuggling** — HTTP Request Smuggling Detection Tool
- **smuggler** — An HTTP Request Smuggling / Desync testing tool written in Python 3
- **h2csmuggler** — HTTP Request Smuggling over HTTP/2 Cleartext (h2c)
- **tiscripts** — These scripts I use to create Request Smuggling Desync payloads for CLTE and TECL style attacks.

Race Condition
- **razzer** — A Kernel fuzzer focusing on race bugs
- **racepwn** — Race Condition framework
- **requests-racer** — Small Python library that makes it easy to exploit race conditions in web apps with Requests.
- **turbo-intruder** — Turbo Intruder is a Burp Suite extension for sending large numbers of HTTP requests and analyzing the results.
- **race-the-web** — Tests for race conditions in web applications. Includes a RESTful API to integrate into a continuous integration pipeline. / Request Smuggling

Open Redirect
- **Oralyzer** — Open Redirection Analyzer
- **Injectus** — CRLF and open redirect fuzzer
- **dom-red** — Small script to check a list of domains against open redirect vulnerability
- **OpenRedireX** — A Fuzzer for OpenRedirect issues

Insecure Direct Object References
- **Autorize** — Automatic authorization enforcement detection extension for burp suite written in Jython developed by Barak Tawily

Insecure Deserialization
- **ysoserial** — A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.
- **GadgetProbe** — Probe endpoints consuming Java serialized objects to identify classes, libraries, and library versions on remote Java classpaths.
- **ysoserial.net** — Deserialization payload generator for a variety of .NET formatters
- **phpggc** — PHPGGC is a library of PHP unserialize() payloads along with a tool to generate them, from command line or programmatically.

Header Injection
- **headi** — Customisable and automated HTTP header injection.

GraphQL Injection
- **inql** — A Burp Extension for GraphQL Security Testing
- **GraphQLmap** — GraphQLmap is a scripting engine to interact with a graphql endpoint for pentesting purposes.
- **shapeshifter** — GraphQL security testing tool
- **graphql_beautifier** — Burp Suite extension to help make Graphql request more readable
- **clairvoyance** — Obtain GraphQL API schema despite disabled introspection!

File Inclusion
- **liffy** — Local file inclusion exploitation tool
- **Burp-LFI-tests** — Fuzzing for LFI using Burpsuite
- **LFI-Enum** — Scripts to execute enumeration via LFI
- **LFISuite** — Totally Automatic LFI Exploiter (+ Reverse Shell) and Scanner
- **LFI-files** — Wordlist to bruteforce for LFI

Wordlists
- **cewl** — CeWL (Custom Word List generator) is a ruby app which spiders a given URL, up to a specified depth, and returns a list of words which can then be used for password crackers such as John the Ripper.
- **cUPP** — CUPP tool is an automated script written in the python language that interacts with the user and answers some fundamental questions about the victim like Name, Company Name, Partner's Name, etc.
- **crunch** — Crunch is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists.
- **pydictor** — A powerful and useful hacker dictionary builder for a brute-force attack
- **rsmangler** — RSMangler will take a wordlist and perform various manipulations on it similar to those done by John the Ripper the main difference being that it will first take the input words and generate all permutations and the acronym of the words (in order they appear in the file) before it applies the rest of the mangles.
- **rockyou.txt** — Kali Linux provides this dictionary file as part of its standard installation.
- **seclists** — SecLists is 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.
- **Assetnote Wordlists** — wordlists.assetnote.io

Google Cloud Storage
- **GCPBucketBrute** — A script to enumerate Google Storage buckets, determine what access you have to them, and determine if they can be privilege escalated.

Digital Ocean
- **spaces-finder** — A tool to hunt for publicly accessible DigitalOcean Spaces

Command Injection
- **Commix** — Automated All-in-One OS command injection and exploitation tool.
- **SQLi sqlmap** — Automatic SQL injection and database takeover tool http://sqlmap.org
- **Sqliv** — massive SQL injection vulnerability scanner
- **Sqlmate** — A friend of SQLmap which will do what you always expected from SQLmap.

XSS
- **XSStrike** — Most advanced XSS scanner.
- **XSS-keylogger** — A keystroke logger to exploit XSS vulnerabilities in a site

API
- **Secretx** — Extracting api keys and secrets by requesting each url in your list.

AWS 53 Bucket
- **s3brute** — s3 brute force tool
- **S3-bucket-finder** — Find aws 53 buckets and extract datas
- **bucket-stream** — Find interesting Amazon 53 Buckets by watching certificate
- **slurp** — Enumerate $3 buckets via certstream, domain, or keywords.
- **lazys3** — A Ruby script to bruteforce for AWS s3 buckets using different permutations
- **cred scanner** — A simple file-based scanner to look for potential AWS access and secret keys in files
- **DumpsterDiver** — A tool used to analyze big volumes of various file types in search of harcoded secrets like keys (AWS Access Key, Azure Share Key or SSH keys) or passwords.
- **S3Scanner** — Scan for open AWS S3 buckets and dump the contents

Inspecting JS Files
- **JSParser** — A python 2.7 script using Tornado and JSBeautifier to parse relative URLs from JavaScript files.
- **relative-url-extractor** — A small tool that extracts relative URLS from a file.
- **sub.js** — A tool to get javascript files from a list of URLS or subdomains
- **LinkFinder** — A python script that finds endpoints in JavaScript files

Code Audit
- **Cobra** — Source Code Security Audit
- **Crawler** — Crawl website extract links
- **waybackMachine** — Use wayback Machine data to pull a list of paths
- **meg** — Fetch many paths for many hosts - without killing the hosts
- **hakrawler** — Simple, fast web crawler designed for easy, quick discovery of endpoints and assets within a web application
- **igoturls** — WaybackURLS + OtxURLS + CommonCrawl

Frameworks
- **Sniper** — Automated pentest framework for offensive security experts
- **XRay** — XRay is a tool for recon, mapping and OSINT gathering from public networks
- **Datasploit** — An #OSINT Framework to perform various recon techniques on Companies, People, Phone Number, Bitcoin Addresses, etc., aggregate all the raw data, and give data in multiple formats
- **Osmedeus** — Fully automated offensive security framework for reconnaissance and vulnerability scanning
- **TIDoS-Framework** — The Offensive Manual Web Application Penetration Testing Framework
- **discover** — Custom bash scripts used to automate various penetration testing tasks including recon, scanning, parsing, and creating malicious payloads and listeners with Metasploit
- **lazyrecon** — This script is intended to automate your reconnaissance process in an organized fashion
- **003Recon** — Some tools to automate recon - 003random
- **Vulmap** — Vulmap is a web vulnerability scanning and verification tool that can scan webapps for vulnerabilities and has a vulnerability verification function

Subdomain Enumeration
- **Findomain** — The fastest and cross-platform subdomain enumerator, do not waste your time
- **chaos-client** — Go client to communicate with Chaos DNS API
- **domained** — Multi Tool Subdomain Enumeration
- **bugcrowd-levelup-subdomain-enumeration** — This repository contains all the material from the talk "Esoteric sub-domain enumeration techniques" given at Bugcrowd LevelUp 2017 virtual conference
- **shuffledns** — shuffleDNS is a wrapper around massdns written in go that allows you to enumerate valid subdomains using active bruteforce as well as resolve subdomains with wildcard handling and easy input-output
- **censys-subdomain-finder** — Perform subdomain enumeration using the certificate transparency logs from Censys.
- **Turbolist3r** — Subdomain enumeration tool with analysis features for discovered domains
- **censys-enumeration** — A script to extract subdomains/emails for a given domain using SSL/TLS certificate dataset on Censys
- **tugarecon** — Fast subdomains enumeration tool for penetration testers
- **as3nt** — Another Subdomain ENumeration Tool
- **Subra** — A Web-UI for subdomain enumeration (subfinder)
- **Substr3am** — Passive reconnaissance/enumeration of interesting targets by watching for SSL certificates being issued
- **domain** — enumall.py Setup script for Regon-ng
- **altdns** — Generates permutations, alterations and mutations of subdomains and then resolves them
- **brutesubs** — An automation framework for running multiple open sourced subdomain bruteforcing tools (in parallel) using your own wordlists via Docker Compose
- **dns-parallel-prober** — This is a parallelised domain name prober to find as many subdomains of a given domain as fast as possible
- **dnscan** — dnscan is a python wordlist-based DNS subdomain scanner
- **hakrevdns** — Small, fast tool for performing reverse DNS lookups en masse
- **dnsx** — Dnsx is a fast and multi-purpose DNS toolkit allow to run multiple DNS queries of your choice with a list of user-supplied resolvers
- **crtndstry** — Yet another subdomain finder
- **VHostScan** — A virtual host scanner that performs reverse lookups
- **scilla** — Information Gathering tool - DNS / Subdomains / Ports / Directories enumeration
- **sub3suite** — A research-grade suite of tools for subdomain enumeration, intelligence gathering and attack surface mapping.
- **Aquatone** — A Tool for Domain Flyovers
- **Knockpy** — Knockpy is a python tool designed to enumerate subdomains on a target domain through a wordlist.
- **subbrute** — A DNS meta-query spider that enumerates DNS records, and subdomains
- **Assetfinder** — Find domains and subdomains related to a given domain
- **Rsdl** — Subdomain Scan with the Ping Method
- **Massdns** — A high-performance DNS stub resolver for bulk lookups and reconnaissance (subdomain enumeration)
- **Subfinder** — Subfinder is a subdomain discovery tool that discovers valid subdomains for websites. Designed as a passive framework to be useful for bug bounties and safe for penetration testing
- **Amass** — In-depth Attack Surface Mapping and Asset Discovery
- **Sub.sh** — Online Subdomain Detect Script
- **Sublist3r** — Fast subdomains enumeration tool for penetration testers
- **Sudomy** — Sudomy is a subdomain enumeration tool to collect subdomains and analyzing domains performing automated reconnaissance (recon) for bug hunting / pentesting
- **dnsenum** — Multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks

Port Scanning
- **masscan** — TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
- **RustScan** — The Modern Port Scanner
- **naabu** — A fast port scanner written in go with focus on reliability and simplicity.
- **nmap** — Nmap - the Network Mapper. Github mirror of official SVN repository
- **sandmap** — Nmap on steroids. Simple CLI with the ability to run pure Nmap engine, 31 modules with 459 scan profiles.
- **ScanCannon** — Combines the speed of masscan with the reliability and detailed enumeration of nmap

Screenshots
- **EyeWitness** — EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.
- **aquatone** — Aquatone is a tool for visual inspection of websites across a large amount of hosts and is convenient for quickly gaining an overview of HTTP-based attack surface.
- **screenshoteer** — Make website screenshots and mobile emulations from the command line.
- **gowitness** — a golang, web screenshot utility using Chrome Headless
- **WitnessMe** — Web Inventory tool, takes screenshots of webpages using Pyppeteer (headless Chrome/Chromium) and provides some extra bells & whistles to make life easier
- **eyeballer** — Convolutional neural network for analyzing pentest screenshots
- **scrying** — A tool for collecting RDP, web and VNC screenshots all in one place
- **Depix** — Recovers passwords from pixelized screenshots
- **httpscreenshot** — HTTPScreenshot is a tool for grabbing screenshots and HTML of large numbers of websites

Technologies
- **wappalyzer** — Identify technology on websites.
- **webanalyze** — Port of Wappalyzer (uncovers technologies used on websites) to automate mass scanning.
- **python-builtwith** — BuiltWith API client
- **whatweb** — Next generation web scanner
- **retire.js** — scanner detecting the use of JavaScript libraries with known vulnerabilities
- **httpx** — httpx is a fast and multi-purpose HTTP toolkit allows to run multiple probers using retryablehttp library, it is designed to maintain the result reliability with increased threads.
- **fingerprintx** — fingerprintx is a standalone utility for service discovery on open ports that works well with other popular bug bounty command line tools.

Content Discovery
- **gobuster** — Directory/File, DNS and VHost busting tool written in Go
- **Feroxbuster** — A fast, simple, recursive content discovery tool written in Rust.
- **Ffuf** — Fast web fuzzer written in Go
- **dirsearch** — Web path scanner
- **recursebuster** — rapid content discovery tool for recursively querying webservers, handy in pentesting and web application assessments
- **filebuster** — An extremely fast and flexible web fuzzer
- **dirstalk** — An extremely fast and flexible web fuzzer
- **dirbuster-ng** — An extremely fast and flexible web fuzzer
- **gospider** — Gospider - Fast web spider written in Go
- **hakrawler** — Simple, fast web crawler designed for easy, quick discovery of endpoints and assets within a web application
- **crawley** — fast, feature-rich unix-way web scraper/crawler written in Golang.

Links
- **LinkFinder** — A python script that finds endpoints in JavaScript files
- **JS-Scan** — a .js scanner, built in php. designed to scrape urls and other info
- **LinksDumper** — Extract (links/possible endpoints) from responses & filter them via decoding/sorting
- **GoLinkFinder** — A fast and minimal JS endpoint extractor
- **BurpJSLinkFinder** — Burp Extension for a passive scanning JS files for endpoint links.
- **urlgrab** — A golang utility to spider through a website searching for additional links.
- **waybackurls** — Fetch all the URLs that the Wayback Machine knows about for a domain
- **getJS** — A tool to fastly get all javascript sources/files
- **linx** — Reveals invisible links within JavaScript files

Parameters
- **parameth** — This tool can be used to brute discover GET and POST parameters
- **param-miner** — This extension identifies hidden, unlinked parameters. It's particularly useful for finding web cache poisoning vulnerabilities.
- **ParamPamPam** — This tool for brute discover GET and POST parameters.
- **Arjun** — HTTP parameter discovery suite.
- **ParamSpider** — Mining parameters from dark corners of Web Archives.

Fuzzing
- **wfuzz** — Web application fuzzer
- **ffuf** — Fast web fuzzer written in Go
- **fuzzdb** — Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.
- **IntruderPayloads** — A collection of Burpsuite Intruder payloads, BurpBounty payloads, fuzz lists, malicious file uploads and web pentesting methodologies and checklists.
- **fuzz.txt** — Potentially dangerous files
- **fuzzilli** — A JavaScript Engine Fuzzer
- **fuzzapi** — Fuzzapi is a tool used for REST API pentesting and uses API_Fuzzer gem
- **vaf** — very advanced (web) fuzzer written in Nim.

CORS Misconfiguration
- **Corsy** — CORS Misconfiguration Scanner
- **CORStest** — A simple CORS misconfiguration scanner
- **cors-scanner** — A multi-threaded scanner that helps identify CORS flaws/misconfigurations
- **CorsMe** — Cross Origin Resource Sharing MisConfiguration Scanner

CRLF Injection
- **CRLFsuite** — A fast tool specially designed to scan CRLF injection
- **crlfuzz** — A fast tool to scan CRLF vulnerability written in Go
- **CRLF-Injection-Scanner** — Command line tool for testing CRLF injection on a list of domains.
- **Injectus** — CRLF and open redirect fuzzer

CSRF Injection
- **XSRFProbe** — The Prime Cross Site Request Forgery (CSRF) Audit and Exploitation Toolkit.

Directory Traversal
- **dotdotpwn** — The Directory Traversal Fuzzer
- **FDsploit** — File Inclusion & Directory Traversal fuzzing, enumeration & exploitation tool.
- **off-by-slash** — Burp extension to detect alias traversal via NGINX misconfiguration at scale.
- **liffier** — tired of manually add dot-dot-slash to your possible path traversal? this short snippet will increment ../ on the URL.

@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles