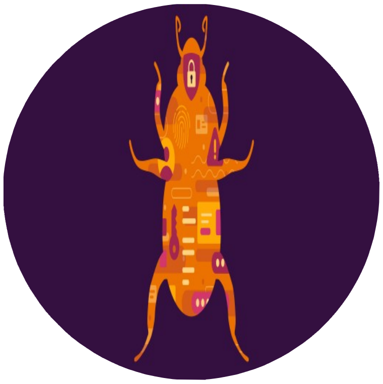

Awesome Bug Bounty Tools

Contents

Recon

Lorem ipsum dolor sit amet

Subdomain Enumeration

- Sublist3r (https://github.com/aboul3la/Sublist3r) - Fast subdomains enumeration tool for penetration testers
- Amass (https://github.com/OWASP/Amass) - In-depth Attack Surface Mapping and Asset Discovery
- massdns (https://github.com/blechschmidt/massdns) - A high-performance DNS stub resolver for bulk lookups and reconnaissance (subdomain enumeration)
- Findomain (https://github.com/Findomain/Findomain) - The fastest and cross-platform subdomain enumerator, do not waste your time.
- Sudomy (https://github.com/Screetsec/Sudomy) - Sudomy is a subdomain enumeration tool to collect subdomains and analyzing domains performing automated reconnaissance (recon) for bug hunting / pentesting
- chaos-client (https://github.com/projectdiscovery/chaos-client) - Go client to communicate with Chaos DNS API.
- domained (https://github.com/TypeError/domained) - Multi Tool Subdomain Enumeration
- bugcrowd-levelup-subdomain-enumeration (https://github.com/appsecco/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 (https://github.com/projectdiscovery/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 (https://github.com/christophetd/censys-subdomain-finder) - Perform subdomain enumeration using the certificate transparency logs from Censys.
- Turbolist3r (https://github.com/fleetcaptain/Turbolist3r) - Subdomain enumeration tool with analysis features for discovered domains
- censys-enumeration (https://github.com/0xbharath/censys-enumeration) - A script to extract subdomains/emails for a given domain using SSL/TLS certificate dataset on Censys

- tugarecon (https://github.com/LordNeoStark/tugarecon) - Fast subdomains enumeration tool for penetration testers.
- as3nt (https://github.com/cinerieus/as3nt) - Another Subdomain ENumeration Tool
- Subra (https://github.com/si9int/Subra) - A Web-UI for subdomain enumeration (subfinder)
- Substr3am (https://github.com/nexxai/Substr3am) - Passive reconnaissance/enumeration of interesting targets by watching for SSL certificates being issued
- domain (https://github.com/jhaddix/domain/) - enumall.py Setup script for Regon-ng
- altdns (https://github.com/infosec-au/altdns) - Generates permutations, alterations and mutations of subdomains and then resolves them
- brutesubs (https://github.com/anshumanbh/brutesubs) - An automation framework for running multiple open sourced subdomain bruteforcing tools (in parallel) using your own wordlists via Docker Compose
- dns-parallel-prober (https://github.com/lorenzog/dns-parallel-prober) - his is a parallelised domain name prober to find as many subdomains of a given domain as fast as possible.
- dnscan (https://github.com/rbsec/dnscan) - dnscan is a python wordlist-based DNS subdomain scanner.
- knock (https://github.com/guelfoweb/knock) - Knockpy is a python tool designed to enumerate subdomains on a target domain through a wordlist.
- hakrevdns (https://github.com/hakluke/hakrevdns) - Small, fast tool for performing reverse DNS lookups en masse.
- dnsx (https://github.com/projectdiscovery/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.
- subfinder (https://github.com/projectdiscovery/subfinder) - Subfinder is a subdomain discovery tool that discovers valid subdomains for websites.
- assetfinder (https://github.com/tomnomnom/assetfinder) - Find domains and subdomains related to a given domain
- crtndstry (https://github.com/nahamsec/crtndstry) - Yet another subdomain finder
- VHostScan (https://github.com/codingo/VHostScan) - A virtual host scanner that performs reverse lookups
- scilla (https://github.com/edoardottt/scilla) - Information Gathering tool - DNS / Subdomains / Ports / Directories enumeration
- sub3suite (https://github.com/3nock/sub3suite) - A research-grade suite of tools for subdomain enumeration, intelligence gathering and attack surface mapping.

Port Scanning

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

Screenshots

- EyeWitness (https://github.com/FortyNorthSecurity/EyeWitness) - EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.
- aquatone (https://github.com/michenriksen/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 (https://github.com/vladocar/screenshoteer) - Make website screenshots and mobile emulations from the command line.
- gowitness (https://github.com/sensepost/gowitness) - gowitness - a golang, web screenshot utility using Chrome Headless
- WitnessMe (https://github.com/byt3bl33d3r/WitnessMe) - Web Inventory tool, takes screenshots of webpages using Pyppeteer (headless Chrome/Chromium) and provides some extra bells & whistles to make life easier.
- eyeballer (https://github.com/BishopFox/eyeballer) - Convolutional neural network for analyzing pentest screenshots
- scrying (https://github.com/nccgroup/scrying) - A tool for collecting RDP, web and VNC screenshots all in one place
- Depix (https://github.com/beurtschipper/Depix) - Recovers passwords from pixelized screenshots
- httpscreenshot (https://github.com/breenmachine/httpscreenshot/) - HTTPScreenshot is a tool for grabbing screenshots and HTML of large numbers of websites.

Technologies

- wappalyzer (https://github.com/AliasIO/wappalyzer) - Identify technology on websites.
- webanalyze (https://github.com/rverton/webanalyze) - Port of Wappalyzer (uncovers technologies used on websites) to automate mass scanning.
- python-builtwith (https://github.com/claymation/python-builtwith) - BuiltWith API client
- whatweb (https://github.com/urbanadventurer/whatweb) - Next generation web scanner
- retire.js (https://github.com/RetireJS/retire.js) - scanner detecting the use of JavaScript libraries with known vulnerabilities
- httpx (https://github.com/projectdiscovery/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 (https://github.com/praetorian-inc/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 (https://github.com/OJ/gobuster) - Directory/File, DNS and VHost busting tool written in Go
- recursebuster (https://github.com/C-Sto/recursebuster) - rapid content discovery tool for recursively querying webservers, handy in pentesting and web application assessments
- feroxbuster (https://github.com/epi052/feroxbuster) - A fast, simple, recursive content discovery tool written in Rust.
- dirsearch (https://github.com/maurosoria/dirsearch) - Web path scanner
- dirsearch (https://github.com/evilsocket/dirsearch) - A Go implementation of dirsearch.
- filebuster (https://github.com/henshin/filebuster) - An extremely fast and flexible web fuzzer

- dirstalk (https://github.com/stefanoj3/dirstalk) - Modern alternative to dirbuster/dirb
- dirbuster-ng (https://github.com/digination/dirbuster-ng) - dirbuster-ng is C CLI implementation of the Java dirbuster tool
- gospider (https://github.com/jaeles-project/gospider) - Gospider - Fast web spider written in Go
- hakrawler (https://github.com/hakluke/hakrawler) - Simple, fast web crawler designed for easy, quick discovery of endpoints and assets within a web application
- crawley (https://github.com/s0rg/crawley) - fast, feature-rich unix-way web scraper/crawler written in Golang.

Links

- LinkFinder (https://github.com/GerbenJavado/LinkFinder) - A python script that finds endpoints in JavaScript files
- JS-Scan (https://github.com/zseano/JS-Scan) - a .js scanner, built in php. designed to scrape urls and other info
- LinksDumper (https://github.com/arbazkiraak/LinksDumper) - Extract (links/possible endpoints) from responses & filter them via decoding/sorting
- GoLinkFinder (https://github.com/0xsha/GoLinkFinder) - A fast and minimal JS endpoint extractor
- BurpJSLinkFinder (https://github.com/InitRoot/BurpJSLinkFinder) - Burp Extension for a passive scanning JS files for endpoint links.
- urlgrab (https://github.com/IAmStoxe/urlgrab) - A golang utility to spider through a website searching for additional links.
- waybackurls (https://github.com/tomnomnom/waybackurls) - Fetch all the URLs that the Wayback Machine knows about for a domain
- gau (https://github.com/lc/gau) - Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl.
- getJS (https://github.com/003random/getJS) - A tool to fastly get all javascript sources/files
- linx (https://github.com/riza/linx) - Reveals invisible links within JavaScript files

Parameters

- parameth (https://github.com/maK-/parameth) - This tool can be used to brute discover GET and POST parameters
- param-miner (https://github.com/PortSwigger/param-miner) - This extension identifies hidden, unlinked parameters. It's particularly useful for finding web cache poisoning vulnerabilities.
- ParamPamPam (https://github.com/Bo0oM/ParamPamPam) - This tool for brute discover GET and POST parameters.
- Arjun (https://github.com/s0md3v/Arjun) - HTTP parameter discovery suite.
- ParamSpider (https://github.com/devanshbatham/ParamSpider) - Mining parameters from dark corners of Web Archives.
- x8 (https://github.com/Sh1Yo/x8) - Hidden parameters discovery suite written in Rust.

Fuzzing

- wfuzz (https://github.com/xmendez/wfuzz) - Web application fuzzer
- ffuf (https://github.com/ffuf/ffuf) - Fast web fuzzer written in Go

- fuzzdb (https://github.com/fuzzdb-project/fuzzdb) - Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.
- IntruderPayloads (https://github.com/1N3/IntruderPayloads) - A collection of Burpsuite Intruder payloads, BurpBounty payloads, fuzz lists, malicious file uploads and web pentesting methodologies and checklists.
- fuzz.txt (https://github.com/Bo0oM/fuzz.txt) - Potentially dangerous files
- fuzzilli (https://github.com/googleprojectzero/fuzzilli) - A JavaScript Engine Fuzzer
- fuzzapi (https://github.com/Fuzzapi/fuzzapi) - Fuzzapi is a tool used for REST API pentesting and uses API_Fuzzer gem
- qsfuzz (https://github.com/ameenmaali/qsfuzz) - qsfuzz (Query String Fuzz) allows you to build your own rules to fuzz query strings and easily identify vulnerabilities.
- vaf (https://github.com/d4rckh/vaf) - very advanced (web) fuzzer written in Nim.

Exploitation

Lorem ipsum dolor sit amet

Command Injection

- commix (https://github.com/commixproject/commix) - Automated All-in-One OS command injection and exploitation tool.

CORS Misconfiguration

- Corsy (https://github.com/s0md3v/Corsy) - CORS Misconfiguration Scanner
- CORStest (https://github.com/RUB-NDS/CORStest) - A simple CORS misconfiguration scanner
- cors-scanner (https://github.com/laconicwolf/cors-scanner) - A multi-threaded scanner that helps identify CORS flaws/misconfigurations
- CorsMe (https://github.com/Shivangx01b/CorsMe) - Cross Origin Resource Sharing MisConfiguration Scanner

CRLF Injection

- CRLFsuite (https://github.com/Nefcore/CRLFsuite) - A fast tool specially designed to scan CRLF injection
- crlfuzz (https://github.com/dwisiswant0/crlfuzz) - A fast tool to scan CRLF vulnerability written in Go
- CRLF-Injection-Scanner (https://github.com/MichaelStott/CRLF-Injection-Scanner) - Command line tool for testing CRLF injection on a list of domains.
- Injectus (https://github.com/BountyStrike/Injectus) - CRLF and open redirect fuzzer

CSRF Injection

- XSRFProbe (https://github.com/0xInfection/XSRFProbe) -The Prime Cross Site Request Forgery (CSRF) Audit and Exploitation Toolkit.

Directory Traversal

- dotdotpwn (https://github.com/wireghoul/dotdotpwn) - DotDotPwn - The Directory Traversal Fuzzer
- FDsploit (https://github.com/chrispetrou/FDsploit) - File Inclusion & Directory Traversal fuzzing, enumeration & exploitation tool.
- off-by-slash (https://github.com/bayotop/off-by-slash) - Burp extension to detect alias traversal via NGINX misconfiguration at scale.
- liffier (https://github.com/momenbasel/liffier) - tired of manually add dot-dot-slash to your possible path traversal? this short snippet will increment ../ on the URL.

File Inclusion

- liffy (https://github.com/mzfr/liffy) - Local file inclusion exploitation tool
- Burp-LFI-tests (https://github.com/Team-Firebugs/Burp-LFI-tests) - Fuzzing for LFI using Burpsuite
- LFI-Enum (https://github.com/mthbernardes/LFI-Enum) - Scripts to execute enumeration via LFI
- LFISuite (https://github.com/D35m0nd142/LFISuite) - Totally Automatic LFI Exploiter (+ Reverse Shell) and Scanner
- LFI-files (https://github.com/hussein98d/LFI-files) - Wordlist to bruteforce for LFI

GraphQL Injection

- inql (https://github.com/doyensec/inql) - InQL - A Burp Extension for GraphQL Security Testing
- GraphQLmap (https://github.com/swisskyrepo/GraphQLmap) - GraphQLmap is a scripting engine to interact with a graphql endpoint for pentesting purposes.
- shapeshifter (https://github.com/szski/shapeshifter) - GraphQL security testing tool
- graphql_beautifier (https://github.com/zidekmat/graphql_beautifier) - Burp Suite extension to help make Graphql request more readable
- clairvoyance (https://github.com/nikitastupin/clairvoyance) - Obtain GraphQL API schema despite disabled introspection!

Header Injection

- headi (https://github.com/mlcsec/headi) - Customisable and automated HTTP header injection.

Insecure Deserialization

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

Insecure Direct Object References

- Autorize (https://github.com/Quitten/Autorize) - Automatic authorization enforcement detection extension for burp suite written in Jython developed by Barak Tawily

Open Redirect

- Oralyzer (https://github.com/r0075h3ll/Oralyzer) - Open Redirection Analyzer
- Injectus (https://github.com/BountyStrike/Injectus) - CRLF and open redirect fuzzer
- dom-red (https://github.com/Naategh/dom-red) - Small script to check a list of domains against open redirect vulnerability
- OpenRedireX (https://github.com/devanshbatham/OpenRedireX) - A Fuzzer for OpenRedirect issues

Race Condition

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

Request Smuggling

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

Server Side Request Forgery

- SSRFmap (https://github.com/swisskyrepo/SSRFmap) - Automatic SSRF fuzzer and exploitation tool
- Gopherus (https://github.com/tarunkant/Gopherus) - This tool generates gopher link for exploiting SSRF and gaining RCE in various servers
- ground-control (https://github.com/jobertabma/ground-control) - A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.
- SSRFire (https://github.com/micha3lb3n/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 (https://github.com/daeken/httprebind) - Automatic tool for DNS rebinding-based SSRF attacks
- ssrf-sheriff (https://github.com/teknogeek/ssrf-sheriff) - A simple SSRF-testing sheriff written in Go

- B-XSSRF (https://github.com/SpiderMate/B-XSSRF) - Toolkit to detect and keep track on Blind XSS, XXE & SSRF
- extended-ssrf-search (https://github.com/Damian89/extended-ssrf-search) - Smart ssrf scanner using different methods like parameter brute forcing in post and get...
- gaussrf (https://github.com/KathanP19/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 (https://github.com/JacobReynolds/ssrfDetector) - Server-side request forgery detector
- grafana-ssrf (https://github.com/RandomRobbieBF/grafana-ssrf) - Authenticated SSRF in Grafana
- sentrySSRF (https://github.com/xawdxawdx/sentrySSRF) - Tool to searching sentry config on page or in javascript files and check blind SSRF
- lorsrf (https://github.com/knassar702/lorsrf) - Bruteforcing on Hidden parameters to find SSRF vulnerability using GET and POST Methods
- singularity (https://github.com/nccgroup/singularity) - A DNS rebinding attack framework.
- whonow (https://github.com/brannondorsey/whonow) - A "malicious" DNS server for executing DNS Rebinding attacks on the fly (public instance running on rebind.network:53)
- dns-rebind-toolkit (https://github.com/brannondorsey/dns-rebind-toolkit) - A front-end JavaScript toolkit for creating DNS rebinding attacks.
- dref (https://github.com/FSecureLABS/dref) - DNS Rebinding Exploitation Framework
- rbndr (https://github.com/taviso/rbndr) - Simple DNS Rebinding Service
- httprebind (https://github.com/daeken/httprebind) - Automatic tool for DNS rebinding-based SSRF attacks
- dnsFookup (https://github.com/makuga01/dnsFookup) - DNS rebinding toolkit

SQL Injection

- sqlmap (https://github.com/sqlmapproject/sqlmap) - Automatic SQL injection and database takeover tool
- NoSQLMap (https://github.com/codingo/NoSQLMap) - Automated NoSQL database enumeration and web application exploitation tool.
- SQLiScanner (https://github.com/0xbug/SQLiScanner) - Automatic SQL injection with Charles and sqlmap api
- SleuthQL (https://github.com/RhinoSecurityLabs/SleuthQL) - Python3 Burp History parsing tool to discover potential SQL injection points. To be used in tandem with SQLmap.
- mssqlproxy (https://github.com/blackarrowsec/mssqlproxy) - mssqlproxy is a toolkit aimed to perform lateral movement in restricted environments through a compromised Microsoft SQL Server via socket reuse
- sqli-hunter (https://github.com/zt2/sqli-hunter) - SQLi-Hunter is a simple HTTP / HTTPS proxy server and a SQLMAP API wrapper that makes digging SQLi easy.
- waybackSqliScanner (https://github.com/ghostlulzhacks/waybackSqliScanner) - Gather urls from wayback machine then test each GET parameter for sql injection.
- ESC (https://github.com/NetSPI/ESC) - Evil SQL Client (ESC) is an interactive .NET SQL console client with enhanced SQL Server discovery, access, and data exfiltration features.
- mssqli-duet (https://github.com/Keramas/mssqli-duet) - SQL injection script for MSSQL that extracts domain users from an Active Directory environment based on RID bruteforcing
- burp-to-sqlmap (https://github.com/Miladkhoshdel/burp-to-sqlmap) - Performing SQLInjection test on Burp Suite Bulk Requests using SQLMap
- BurpSQLTruncSanner (https://github.com/InitRoot/BurpSQLTruncSanner) - Messy BurpSuite plugin for SQL Truncation vulnerabilities.

- andor (https://github.com/sadicann/andor) - Blind SQL Injection Tool with Golang
- Blinder (https://github.com/mhaskar/Blinder) - A python library to automate time-based blind SQL injection
- sqliv (https://github.com/the-robot/sqliv) - massive SQL injection vulnerability scanner
- nosqli (https://github.com/Charlie-belmer/nosqli) - NoSql Injection CLI tool, for finding vulnerable websites using MongoDB.

XSS Injection

- XSStrike (https://github.com/s0md3v/XSStrike) - Most advanced XSS scanner.
- xssor2 (https://github.com/evilcos/xssor2) - XSS'OR - Hack with JavaScript.
- xsscrapy (https://github.com/DanMcInerney/xsscrapy) - XSS spider - 66/66 wavsep XSS detected
- sleepy-puppy (https://github.com/Netflix-Skunkworks/sleepy-puppy) - Sleepy Puppy XSS Payload Management Framework
- ezXSS (https://github.com/ssl/ezXSS) - ezXSS is an easy way for penetration testers and bug bounty hunters to test (blind) Cross Site Scripting.
- xsshunter (https://github.com/mandatoryprogrammer/xsshunter) - The XSS Hunter service - a portable version of XSSHunter.com
- dalfox (https://github.com/hahwul/dalfox) - DalFox(Finder Of XSS) / Parameter Analysis and XSS Scanning tool based on golang
- xsser (https://github.com/epsylon/xsser) - Cross Site "Scripter" (aka XSSer) is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based applications.
- XSpear (https://github.com/hahwul/XSpear) - Powerfull XSS Scanning and Parameter analysis tool&gem
- weaponised-XSS-payloads (https://github.com/hakluke/weaponised-XSS-payloads) - XSS payloads designed to turn alert(1) into P1
- tracy (https://github.com/nccgroup/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 (https://github.com/jobertabma/ground-control) - A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.
- xssValidator (https://github.com/nVisium/xssValidator) - This is a burp intruder extender that is designed for automation and validation of XSS vulnerabilities.
- JSShell (https://github.com/Den1al/JSShell) - An interactive multi-user web JS shell
- bXSS (https://github.com/LewisArdern/bXSS) - bXSS is a utility which can be used by bug hunters and organizations to identify Blind Cross-Site Scripting.
- docem (https://github.com/whitel1st/docem) - Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids)
- XSS-Radar (https://github.com/bugbountyforum/XSS-Radar) - XSS Radar is a tool that detects parameters and fuzzes them for cross-site scripting vulnerabilities.
- BruteXSS (https://github.com/rajeshmajumdar/BruteXSS) - BruteXSS is a tool written in python simply to find XSS vulnerabilities in web application.
- findom-xss (https://github.com/dwisiswant0/findom-xss) - A fast DOM based XSS vulnerability scanner with simplicity.
- domdig (https://github.com/fcavallarin/domdig) - DOM XSS scanner for Single Page Applications
- femida (https://github.com/wish-i-was/femida) - Automated blind-xss search for Burp Suite

- B-XSSRF (https://github.com/SpiderMate/B-XSSRF) - Toolkit to detect and keep track on Blind XSS, XXE & SSRF
- domxssscanner (https://github.com/yaph/domxssscanner) - DOMXSS Scanner is an online tool to scan source code for DOM based XSS vulnerabilities
- xsshunter_client (https://github.com/mandatoryprogrammer/xsshunter_client) - Correlated injection proxy tool for XSS Hunter
- extended-xss-search (https://github.com/Damian89/extended-xss-search) - A better version of my xssfinder tool - scans for different types of xss on a list of urls.
- xssmap (https://github.com/Jewel591/xssmap) - XSSMap 是一款基于 Python3 开发用于检测 XSS 漏洞的工具
- XSSCon (https://github.com/menkrep1337/XSSCon) - XSSCon: Simple XSS Scanner tool
- BitBlinder (https://github.com/BitTheByte/BitBlinder) - BurpSuite extension to inject custom cross-site scripting payloads on every form/request submitted to detect blind XSS vulnerabilities
- XSSOauthPersistence (https://github.com/dxa4481/XSSOauthPersistence) - Maintaining account persistence via XSS and Oauth
- shadow-workers (https://github.com/shadow-workers/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 (https://github.com/profmoriarity/rexsser) - This is a burp plugin that extracts keywords from response using regexes and test for reflected XSS on the target scope.
- xss-flare (https://github.com/EgeBalci/xss-flare) - XSS hunter on cloudflare serverless workers.
- Xss-Sql-Fuzz (https://github.com/jiangsir404/Xss-Sql-Fuzz) - burpsuite 插件对GP所有参数(过滤特殊参数)一键自动添加xss sql payload 进行fuzz
- vaya-ciego-nen (https://github.com/hipotermia/vaya-ciego-nen) - Detect, manage and exploit Blind Cross-site scripting (XSS) vulnerabilities.
- dom-based-xss-finder (https://github.com/AsaiKen/dom-based-xss-finder) - Chrome extension that finds DOM based XSS vulnerabilities
- XSSTerminal (https://github.com/machinexa2/XSSTerminal) - Develop your own XSS Payload using interactive typing
- xss2png (https://github.com/vavkamil/xss2png) - PNG IDAT chunks XSS payload generator
- XSSwagger (https://github.com/vavkamil/XSSwagger) - A simple Swagger-ui scanner that can detect old versions vulnerable to various XSS attacks

XXE Injection

- ground-control (https://github.com/jobertabma/ground-control) - A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.
- dtd-finder (https://github.com/GoSecure/dtd-finder) - List DTDs and generate XXE payloads using those local DTDs.
- docem (https://github.com/whitel1st/docem) - Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids)
- xxeserv (https://github.com/staaldraad/xxeserv) - A mini webserver with FTP support for XXE payloads
- xxexploiter (https://github.com/luisfontes19/xxexploiter) - Tool to help exploit XXE vulnerabilities
- B-XSSRF (https://github.com/SpiderMate/B-XSSRF) - Toolkit to detect and keep track on Blind XSS, XXE & SSRF

- XXEinjector (https://github.com/enjoiz/XXEinjector) - Tool for automatic exploitation of XXE vulnerability using direct and different out of band methods.
- oxml_xxe (https://github.com/BuffaloWill/oxml_xxe) - A tool for embedding XXE/XML exploits into different filetypes
- metahttp (https://github.com/vp777/metahttp) - A bash script that automates the scanning of a target network for HTTP resources through XXE

Miscellaneous

Lorem ipsum dolor sit amet

Passwords

- thc-hydra (https://github.com/vanhauser-thc/thc-hydra) - Hydra is a parallelized login cracker which supports numerous protocols to attack.
- DefaultCreds-cheat-sheet (https://github.com/ihebski/DefaultCreds-cheat-sheet) - One place for all the default credentials to assist the Blue/Red teamers activities on finding devices with default password
- changeme (https://github.com/ztgrace/changeme) - A default credential scanner.
- BruteX (https://github.com/1N3/BruteX) - Automatically brute force all services running on a target.
- patator (https://github.com/lanjelot/patator) - Patator is a multi-purpose brute-forcer, with a modular design and a flexible usage.

Secrets

- git-secrets (https://github.com/awslabs/git-secrets) - Prevents you from committing secrets and credentials into git repositories
- gitleaks (https://github.com/zricethezav/gitleaks) - Scan git repos (or files) for secrets using regex and entropy
- truffleHog (https://github.com/dxa4481/truffleHog) - Searches through git repositories for high entropy strings and secrets, digging deep into commit history
- gitGraber (https://github.com/hisxo/gitGraber) - gitGraber: monitor GitHub to search and find sensitive data in real time for different online services
- talisman (https://github.com/thoughtworks/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 (https://github.com/BishopFox/GitGot) - Semi-automated, feedback-driven tool to rapidly search through troves of public data on GitHub for sensitive secrets.
- git-all-secrets (https://github.com/anshumanbh/git-all-secrets) - A tool to capture all the git secrets by leveraging multiple open source git searching tools
- github-search (https://github.com/gwen001/github-search) - Tools to perform basic search on GitHub.
- git-vuln-finder (https://github.com/cve-search/git-vuln-finder) - Finding potential software vulnerabilities from git commit messages
- commit-stream (https://github.com/x1sec/commit-stream) - #OSINT tool for finding Github repositories by extracting commit logs in real time from the Github event API

- gitrob (https://github.com/michenriksen/gitrob) - Reconnaissance tool for GitHub organizations
- repo-supervisor (https://github.com/auth0/repo-supervisor) - Scan your code for security misconfiguration, search for passwords and secrets.
- GitMiner (https://github.com/UnkL4b/GitMiner) - Tool for advanced mining for content on Github
- shhgit (https://github.com/eth0izzle/shhgit) - Ah shhgit! Find GitHub secrets in real time
- detect-secrets (https://github.com/Yelp/detect-secrets) - An enterprise friendly way of detecting and preventing secrets in code.
- rusty-hog (https://github.com/newrelic/rusty-hog) - A suite of secret scanners built in Rust for performance. Based on TruffleHog
- whispers (https://github.com/Skyscanner/whispers) - Identify hardcoded secrets and dangerous behaviours
- yar (https://github.com/nielsing/yar) - Yar is a tool for plunderin' organizations, users and/or repositories.
- dufflebag (https://github.com/BishopFox/dufflebag) - Search exposed EBS volumes for secrets
- secret-bridge (https://github.com/duo-labs/secret-bridge) - Monitors Github for leaked secrets
- earlybird (https://github.com/americanexpress/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 (https://github.com/trufflesecurity/Trufflehog-Chrome-Extension) - Trufflehog-Chrome-Extension

Git

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

Buckets

- S3Scanner (https://github.com/sa7mon/S3Scanner) - Scan for open AWS S3 buckets and dump the contents
- AWSBucketDump (https://github.com/jordanpotti/AWSBucketDump) - Security Tool to Look For Interesting Files in S3 Buckets
- CloudScraper (https://github.com/jordanpotti/CloudScraper) - CloudScraper: Tool to enumerate targets in search of cloud resources. S3 Buckets, Azure Blobs, Digital Ocean Storage Space.
- s3viewer (https://github.com/SharonBrizinov/s3viewer) - Publicly Open Amazon AWS S3 Bucket Viewer
- festin (https://github.com/cr0hn/festin) - FestIn - S3 Bucket Weakness Discovery
- s3reverse (https://github.com/hahwul/s3reverse) - The format of various s3 buckets is convert in one format. for bugbounty and security testing.
- mass-s3-bucket-tester (https://github.com/random-robbie/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 (https://github.com/AlecBlance/S3BucketList) - Firefox plugin that lists Amazon S3 Buckets found in requests

- dirlstr (https://github.com/cybercdh/dirlstr) - Finds Directory Listings or open S3 buckets from a list of URLs
- Burp-AnonymousCloud (https://github.com/codewatchorg/Burp-AnonymousCloud) - Burp extension that performs a passive scan to identify cloud buckets and then test them for publicly accessible vulnerabilities
- kicks3 (https://github.com/abuvanth/kicks3) - S3 bucket finder from html,js and bucket misconfiguration testing tool
- 2tearsinabucket (https://github.com/Revenant40/2tearsinabucket) - Enumerate s3 buckets for a specific target.
- s3_objects_check (https://github.com/nccgroup/s3_objects_check) - Whitebox evaluation of effective S3 object permissions, to identify publicly accessible files.
- s3tk (https://github.com/ankane/s3tk) - A security toolkit for Amazon S3
- CloudBrute (https://github.com/0xsha/CloudBrute) - Awesome cloud enumerator
- s3cario (https://github.com/0xspade/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 (https://github.com/JR0ch17/S3Cruze) - All-in-one AWS S3 bucket tool for pentesters.

CMS

- wpscan (https://github.com/wpscanteam/wpscan) - WPScan is a free, for non-commercial use, black box WordPress security scanner
- WPSpider (https://github.com/cyc10n3/WPSpider) - A centralized dashboard for running and scheduling WordPress scans powered by wpscan utility.
- wprecon (https://github.com/blackcrw/wprecon) - Wordpress Recon
- CMSmap (https://github.com/Dionach/CMSmap) - CMSmap is a python open source CMS scanner that automates the process of detecting security flaws of the most popular CMSs.
- joomscan (https://github.com/OWASP/joomscan) - OWASP Joomla Vulnerability Scanner Project
- pyfiscan (https://github.com/fgeek/pyfiscan) - Free web-application vulnerability and version scanner

JSON Web Token

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

postMessage

- postMessage-tracker (https://github.com/fransr/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 (https://github.com/kiranreddyrebel/PostMessage_Fuzz_Tool) - #BugBounty #BugBounty Tools #WebDeveloper Tool

Subdomain Takeover

- subjack (https://github.com/haccer/subjack) - Subdomain Takeover tool written in Go
- SubOver (https://github.com/Ice3man543/SubOver) - A Powerful Subdomain Takeover Tool
- autoSubTakeover (https://github.com/JordyZomer/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 (https://github.com/shivsahni/NSBrute) - Python utility to takeover domains vulnerable to AWS NS Takeover
- can-i-take-over-xyz (https://github.com/EdOverflow/can-i-take-over-xyz) - "Can I take over XYZ?" — a list of services and how to claim (sub)domains with dangling DNS records.
- cnames (https://github.com/cybercdh/cnames) - take a list of resolved subdomains and output any corresponding CNAMES en masse.
- subHijack (https://github.com/vavkamil/old-repos-backup/tree/master/subHijack-master) - Hijacking forgotten & misconfigured subdomains
- tko-subs (https://github.com/anshumanbh/tko-subs) - A tool that can help detect and takeover subdomains with dead DNS records
- HostileSubBruteforcer (https://github.com/nahamsec/HostileSubBruteforcer) - This app will bruteforce for exisiting subdomains and provide information if the 3rd party host has been properly setup.
- second-order (https://github.com/mhmdiaa/second-order) - Second-order subdomain takeover scanner
- takeover (https://github.com/mzfr/takeover) - A tool for testing subdomain takeover possibilities at a mass scale.
- dnsReaper (https://github.com/punk-security/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!

Vulnerability Scanners

- nuclei (https://github.com/projectdiscovery/nuclei) - Nuclei is a fast tool for configurable targeted scanning based on templates offering massive extensibility and ease of use.
- Sn1per (https://github.com/1N3/Sn1per) - Automated pentest framework for offensive security experts
- metasploit-framework (https://github.com/rapid7/metasploit-framework) - Metasploit Framework
- nikto (https://github.com/sullo/nikto) - Nikto web server scanner
- arachni (https://github.com/Arachni/arachni) - Web Application Security Scanner Framework
- jaeles (https://github.com/jaeles-project/jaeles) - The Swiss Army knife for automated Web Application Testing
- retire.js (https://github.com/RetireJS/retire.js) - scanner detecting the use of JavaScript libraries with known vulnerabilities
- Osmedeus (https://github.com/j3ssie/Osmedeus) - Fully automated offensive security framework for reconnaissance and vulnerability scanning
- getsploit (https://github.com/vulnersCom/getsploit) - Command line utility for searching and downloading exploits
- flan (https://github.com/cloudflare/flan) - A pretty sweet vulnerability scanner
- Findsploit (https://github.com/1N3/Findsploit) - Find exploits in local and online databases instantly

- BlackWidow (https://github.com/1N3/BlackWidow) - A Python based web application scanner to gather OSINT and fuzz for OWASP vulnerabilities on a target website.
- backslash-powered-scanner (https://github.com/PortSwigger/backslash-powered-scanner) - Finds unknown classes of injection vulnerabilities
- Eagle (https://github.com/BitTheByte/Eagle) - Multithreaded Plugin based vulnerability scanner for mass detection of web-based applications vulnerabilities
- cariddi (https://github.com/edoardottt/cariddi) - Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, tokens and more...
- OWASP ZAP (https://github.com/zaproxy/zaproxy) - World's most popular free web security tools and is actively maintained by a dedicated international team of volunteers

Uncategorized

- JSONBee (https://github.com/zigoo0/JSONBee) - A ready to use JSONP endpoints/payloads to help bypass content security policy (CSP) of different websites.
- CyberChef (https://github.com/gchq/CyberChef) - The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis
- () -
- bountyplz (https://github.com/fansr/bountyplz) - Automated security reporting from markdown templates (HackerOne and Bugcrowd are currently the platforms supported)
- PayloadsAllTheThings (https://github.com/swisskyrepo/PayloadsAllTheThings) - A list of useful payloads and bypass for Web Application Security and Pentest/CTF
- bounty-targets-data (https://github.com/arkadiyt/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 (https://github.com/ashishb/android-security-awesome) - A collection of android security related resources
- awesome-mobile-security (https://github.com/vaib25vicky/awesome-mobile-security) - An effort to build a single place for all useful android and iOS security related stuff.
- awesome-vulnerable-apps (https://github.com/vavkamil/awesome-vulnerable-apps) - Awesome Vulnerable Applications
- XFFenum (https://github.com/vavkamil/XFFenum) - X-Forwarded-For [403 forbidden] enumeration
- httpx (https://github.com/projectdiscovery/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.