Bug Bounty Tools

Recon

- Subdomain Enumeration
- Port Scanning
- Screenshots
- Technologies
- Content Discovery
- Links
- Parameters
- Fuzzing

Vulnerability Scanners

Exploitation

- Command Injection
- CORS Misconfiguration
- CRLF Injection
- CSRF Injection
- Directory Traversal
- File Inclusion
- GraphQL Injection
- Header Injection
- Insecure Deserialization
- Insecure Direct Object References
- Open Redirect
- Race Condition
- Request Smuggling
- Server Side Request Forgery
- SQL Injection
- XSS Injection
- XXE Injection

Miscellaneous

- Passwords
- Secrets
- Git
- Buckets
- CMS
- JSON Web Token
- postMessage
- Subdomain Takeover
- Uncategorized

Recon

Subdomain Enumeration

Sublist3r - Fast subdomains enumeration tool for penetration testers

https://github.com/aboul3la/Sublist3r

Amass - In-depth Attack Surface Mapping and Asset Discovery

https://github.com/OWASP/Amass

massdns - A high-performance DNS stub resolver for bulk lookups and reconnaissance (subdomain enumeration)

https://github.com/blechschmidt/massdns

Findomain - The fastest and cross-platform subdomain enumerator, do not waste your time.

https://github.com/Findomain/Findomain

Sudomy - Sudomy is a subdomain enumeration tool to collect subdomains and analyzing domains performing automated reconnaissance (recon) for bug hunting / pentesting

https://github.com/Screetsec/Sudomy

chaos-client - Go client to communicate with Chaos DNS API.

https://github.com/projectdiscovery/chaos-client

domained - Multi Tool Subdomain Enumeration

https://github.com/TypeError/domained

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

https://github.com/appsecco/bugcrowd-levelup-subdomain-enumeration

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

https://github.com/projectdiscovery/shuffledns

censys-subdomain-finder - Perform subdomain enumeration using the certificate transparency logs from Censys.

https://github.com/christophetd/censys-subdomain-finder

Turbolist3r - Subdomain enumeration tool with analysis features for discovered domains

https://github.com/fleetcaptain/Turbolist3r

censys-enumeration - A script to extract subdomains/emails for a given domain using SSL/TLS certificate dataset on Censys

https://github.com/0xbharath/censys-enumeration

tugarecon - Fast subdomains enumeration tool for penetration testers.

https://github.com/skynet0x01/tugarecon

as3nt - Another Subdomain ENumeration Tool

https://github.com/cinerieus/as3nt

Subra - A Web-UI for subdomain enumeration (subfinder)

https://github.com/si9int/Subra

Substr3am - Passive reconnaissance/enumeration of interesting targets by watching for SSL certificates being issued

https://github.com/nexxai/Substr3am

domain - enumall.py Setup script for Regon-ng

https://github.com/jhaddix/domain/

altdns - Generates permutations, alterations and mutations of subdomains and then resolves them

https://github.com/infosec-au/altdns

brutesubs - An automation framework for running multiple open sourced subdomain bruteforcing tools (in parallel) using your own wordlists via Docker Compose

https://github.com/anshumanbh/brutesubs

dns-parallel-prober - his is a parallelised domain name prober to find as many subdomains of a given domain as fast as possible.

https://github.com/lorenzog/dns-parallel-prober

dnscan - dnscan is a python wordlist-based DNS subdomain scanner.

https://github.com/rbsec/dnscan

knock - Knockpy is a python tool designed to enumerate subdomains on a target domain through a wordlist.

https://github.com/guelfoweb/knock

hakrevdns - Small, fast tool for performing reverse DNS lookups en masse.

https://github.com/hakluke/hakrevdns

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.

https://github.com/projectdiscovery/dnsx

subfinder - Subfinder is a subdomain discovery tool that discovers valid subdomains for websites.

https://github.com/projectdiscovery/subfinder

assetfinder - Find domains and subdomains related to a given domain

https://github.com/tomnomnom/assetfinder

crtndstry - Yet another subdomain finder

https://github.com/nahamsec/crtndstry

VHostScan - A virtual host scanner that performs reverse lookups

https://github.com/codingo/VHostScan

scilla - Information Gathering tool - DNS / Subdomains / Ports / Directories enumeration

https://github.com/edoardottt/scilla

sub3suite - A research-grade suite of tools for subdomain enumeration, intelligence gathering and attack surface mapping.

https://github.com/3nock/sub3suite

Port Scanning

masscan - TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.

https://github.com/robertdavidgraham/masscan

RustScan - The Modern Port Scanner

https://github.com/RustScan/RustScan

naabu - A fast port scanner written in go with focus on reliability and simplicity.

https://github.com/projectdiscovery/naabu

nmap - Nmap - the Network Mapper. Github mirror of official SVN repository.

https://github.com/nmap/nmap

sandmap - Nmap on steroids. Simple CLI with the ability to run pure Nmap engine, 31 modules with 459 scan profiles.

https://github.com/trimstray/sandmap

ScanCannon - Combines the speed of masscan with the reliability and detailed enumeration of nmap

https://github.com/johnnyxmas/ScanCannon

Screenshots

EyeWitness - EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.

https://github.com/FortyNorthSecurity/EyeWitness

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.

https://github.com/michenriksen/aquatone

screenshoteer - Make website screenshots and mobile emulations from the command line.

https://github.com/vladocar/screenshoteer

gowitness - gowitness - a golang, web screenshot utility using Chrome Headless

https://github.com/sensepost/gowitness

WitnessMe - Web Inventory tool, takes screenshots of webpages using Pyppeteer (headless Chrome/Chromium) and provides some extra bells & whistles to make life easier.

https://github.com/byt3bl33d3r/WitnessMe

eyeballer - Convolutional neural network for analyzing pentest screenshots

https://github.com/BishopFox/eyeballer

scrying - A tool for collecting RDP, web and VNC screenshots all in one place

https://github.com/nccgroup/scrying

Depix - Recovers passwords from pixelized screenshots

https://github.com/beurtschipper/Depix

httpscreenshot - HTTPScreenshot is a tool for grabbing screenshots and HTML of large numbers of websites.

https://github.com/breenmachine/httpscreenshot/

Technologies

wappalyzer - Identify technology on websites.

https://github.com/wappalyzer/wappalyzer

webanalyze - Port of Wappalyzer (uncovers technologies used on websites) to automate mass scanning.

https://github.com/rverton/webanalyze

python-builtwith - BuiltWith API client

https://github.com/claymation/python-builtwith

whatweb - Next generation web scanner

https://github.com/urbanadventurer/whatweb

retire.js - scanner detecting the use of JavaScript libraries with known vulnerabilities

https://github.com/RetireJS/retire.js

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.

https://github.com/projectdiscovery/httpx

fingerprintx - fingerprintx is a standalone utility for service discovery on open ports that works well with other popular bug bounty command line tools.

https://github.com/praetorian-inc/fingerprintx

Content Discovery

gobuster - Directory/File, DNS and VHost busting tool written in Go

https://github.com/OJ/gobuster

recursebuster - rapid content discovery tool for recursively querying webservers, handy in pentesting and web application assessments

https://github.com/C-Sto/recursebuster

feroxbuster - A fast, simple, recursive content discovery tool written in Rust.

https://github.com/epi052/feroxbuster

dirsearch - Web path scanner

https://github.com/maurosoria/dirsearch

dirsearch - A Go implementation of dirsearch.

https://github.com/evilsocket/dirsearch

filebuster - An extremely fast and flexible web fuzzer

https://github.com/henshin/filebuster

dirstalk - Modern alternative to dirbuster/dirb

https://github.com/stefanoj3/dirstalk

dirbuster-ng - dirbuster-ng is C CLI implementation of the Java dirbuster tool

https://github.com/digination/dirbuster-ng

gospider - Gospider - Fast web spider written in Go

https://github.com/jaeles-project/gospider

hakrawler - Simple, fast web crawler designed for easy, quick discovery of endpoints and assets within a web application

https://github.com/hakluke/hakrawler

Links

LinkFinder - A python script that finds endpoints in JavaScript files

https://github.com/GerbenJavado/LinkFinder

JS-Scan - a .js scanner, built in php. designed to scrape urls and other info

https://github.com/zseano/JS-Scan

LinksDumper - Extract (links/possible endpoints) from responses & filter them via decoding/sorting

https://github.com/arbazkiraak/LinksDumper

GoLinkFinder - A fast and minimal JS endpoint extractor

https://github.com/0xsha/GoLinkFinder

BurpJSLinkFinder - Burp Extension for a passive scanning JS files for endpoint links.

https://github.com/InitRoot/BurpJSLinkFinder

urlgrab - A golang utility to spider through a website searching for additional links.

https://github.com/IAmStoxe/urlgrab

waybackurls - Fetch all the URLs that the Wayback Machine knows about for a domain

https://github.com/tomnomnom/waybackurls

gau - Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl.

https://github.com/lc/gau

getJS - A tool to fastly get all javascript sources/files

https://github.com/003random/getJS

linx - Reveals invisible links within JavaScript files

https://github.com/riza/linx

Parameters

parameth - This tool can be used to brute discover GET and POST parameters

https://github.com/maK-/parameth

param-miner - This extension identifies hidden, unlinked parameters. It's particularly useful for finding web cache poisoning vulnerabilities.

https://github.com/PortSwigger/param-miner

ParamPamPam - This tool for brute discover GET and POST parameters.

https://github.com/Bo0oM/ParamPamPam

Arjun - HTTP parameter discovery suite.

https://github.com/s0md3v/Arjun

ParamSpider - Mining parameters from dark corners of Web Archives

https://github.com/devanshbatham/ParamSpider

Fuzzing

wfuzz - Web application fuzzer

https://github.com/xmendez/wfuzz

ffuf - Fast web fuzzer written in Go

https://github.com/ffuf/ffuf

fuzzdb - Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.

https://github.com/fuzzdb-project/fuzzdb

IntruderPayloads - A collection of Burpsuite Intruder payloads, BurpBounty payloads, fuzz lists, malicious file uploads and web pentesting methodologies and checklists.

https://github.com/1N3/IntruderPayloads

fuzz.txt - Potentially dangerous files

https://github.com/Bo0oM/fuzz.txt

fuzzilli - A JavaScript Engine Fuzzer

https://github.com/googleprojectzero/fuzzilli

fuzzapi - Fuzzapi is a tool used for REST API pentesting and uses API_Fuzzer gem

https://github.com/Fuzzapi/fuzzapi

qsfuzz - qsfuzz (Query String Fuzz) allows you to build your own rules to fuzz query strings and easily identify vulnerabilities.

https://github.com/ameenmaali/qsfuzz

vaf - very advanced (web) fuzzer written in Nim.

https://github.com/d4rckh/vaf

Vulnerability Scanners

nuclei - Nuclei is a fast tool for configurable targeted scanning based on templates offering massive extensibility and ease of use.

https://github.com/projectdiscovery/nuclei

Sn1per - Automated pentest framework for offensive security experts

https://github.com/1N3/Sn1per

metasploit-framework - Metasploit Framework

https://github.com/rapid7/metasploit-framework

nikto - Nikto web server scanner

https://github.com/sullo/nikto

arachni - Web Application Security Scanner Framework

https://github.com/Arachni/arachni

jaeles - The Swiss Army knife for automated Web Application Testing

https://github.com/jaeles-project/jaeles

retire.js - scanner detecting the use of JavaScript libraries with known vulnerabilities

https://github.com/RetireJS/retire.js

Osmedeus - Fully automated offensive security framework for reconnaissance and vulnerability scanning

https://github.com/j3ssie/Osmedeus

getsploit - Command line utility for searching and downloading exploits

https://github.com/vulnersCom/getsploit

flan - A pretty sweet vulnerability scanner

https://github.com/cloudflare/flan

Findsploit - Find exploits in local and online databases instantly

https://github.com/1N3/Findsploit

BlackWidow - A Python based web application scanner to gather OSINT and fuzz for OWASP vulnerabilities on a target website.

https://github.com/1N3/BlackWidow

backslash-powered-scanner - Finds unknown classes of injection vulnerabilities

https://github.com/PortSwigger/backslash-powered-scanner

Eagle - Multithreaded Plugin based vulnerability scanner for mass detection of web-based applications vulnerabilities

https://github.com/BitTheByte/Eagle

cariddi - Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, tokens and more.

https://github.com/edoardottt/cariddi

OWASP ZAP - World's most popular free web security tools and is actively maintained by a dedicated international team of volunteers

https://github.com/zaproxy/zaproxy

Exploitation

Command Injection

commix - Automated All-in-One OS command injection and exploitation tool.

https://github.com/commixproject/commix

CORS Misconfiguration

Corsy - CORS Misconfiguration Scanner

https://github.com/s0md3v/Corsy

CORStest - A simple CORS misconfiguration scanner

https://github.com/RUB-NDS/CORStest

cors-scanner - A multi-threaded scanner that helps identify CORS flaws/misconfigurations

https://github.com/laconicwolf/cors-scanner

CorsMe - Cross Origin Resource Sharing MisConfiguration Scanner

https://github.com/Shivangx01b/CorsMe

CRLF Injection

CRLFsuite - A fast tool specially designed to scan CRLF injection

https://github.com/Nefcore/CRLFsuite

crlfuzz - A fast tool to scan CRLF vulnerability written in Go

https://github.com/dwisiswant0/crlfuzz

CRLF-Injection-Scanner - Command line tool for testing CRLF injection on a list of domains.

https://github.com/MichaelStott/CRLF-Injection-Scanner

Injectus - CRLF and open redirect fuzzer

https://github.com/BountyStrike/Injectus

CSRF Injection

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

https://github.com/0xInfection/XSRFProbe

Directory Traversal

dotdotpwn - DotDotPwn - The Directory Traversal Fuzzer

https://github.com/wireghoul/dotdotpwn

FDsploit - File Inclusion & Directory Traversal fuzzing, enumeration & exploitation tool.

https://github.com/chrispetrou/FDsploit

off-by-slash - Burp extension to detect alias traversal via NGINX misconfiguration at scale.

https://github.com/bayotop/off-by-slash

liffier - tired of manually add dot-dot-slash to your possible path traversal? this short snippet will increment ../ on the URL.

https://github.com/momenbasel/liffier

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Directory%20Traversal

File Inclusion

liffy - Local file inclusion exploitation tool

https://github.com/mzfr/liffy

Burp-LFI-tests - Fuzzing for LFI using Burpsuite

https://github.com/Team-Firebugs/Burp-LFI-tests

LFI-Enum - Scripts to execute enumeration via LFI

https://github.com/mthbernardes/LFI-Enum

LFISuite - Totally Automatic LFI Exploiter (+ Reverse Shell) and Scanner

https://github.com/D35m0nd142/LFISuite

LFI-files - Wordlist to bruteforce for LFI

https://github.com/hussein98d/LFI-files

GraphQL Injection

inql - InQL - A Burp Extension for GraphQL Security Testing

https://github.com/doyensec/inql

GraphQLmap - GraphQLmap is a scripting engine to interact with a graphql endpoint for pentesting purposes.

https://github.com/swisskyrepo/GraphQLmap

shapeshifter - GraphQL security testing tool

https://github.com/szski/shapeshifter

graphql_beautifier - Burp Suite extension to help make Graphql request more readable

https://github.com/zidekmat/graphql_beautifier

clairvoyance - Obtain GraphQL API schema despite disabled introspection!

https://github.com/nikitastupin/clairvoyance

Header Injection

headi - Customisable and automated HTTP header injection.

https://github.com/mlcsec/headi

Insecure Deserialization

ysoserial - A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.

https://github.com/frohoff/ysoserial

GadgetProbe - Probe endpoints consuming Java serialized objects to identify classes, libraries, and library versions on remote Java classpaths.

https://github.com/BishopFox/GadgetProbe

ysoserial.net - Deserialization payload generator for a variety of .NET formatters

https://github.com/pwntester/ysoserial.net

phpggc - PHPGGC is a library of PHP unserialize() payloads along with a tool to generate them, from command line or programmatically.

https://github.com/ambionics/phpggc

Insecure Direct Object References

Autorize - Automatic authorization enforcement detection extension for burp suite written in Jython developed by Barak Tawily

https://github.com/Quitten/Autorize

Open Redirect

Oralyzer - Open Redirection Analyzer

https://github.com/r0075h3ll/Oralyzer

Injectus - CRLF and open redirect fuzzer

https://github.com/BountyStrike/Injectus

dom-red - Small script to check a list of domains against open redirect vulnerability

https://github.com/Naategh/dom-red

OpenRedireX - A Fuzzer for OpenRedirect issues

https://github.com/devanshbatham/OpenRedireX

Race Condition

razzer - A Kernel fuzzer focusing on race bugs

https://github.com/compsec-snu/razzer

racepwn - Race Condition framework

https://github.com/racepwn/racepwn

requests-racer - Small Python library that makes it easy to exploit race conditions in web apps with Requests.

https://github.com/nccgroup/requests-racer

turbo-intruder - Turbo Intruder is a Burp Suite extension for sending large numbers of HTTP requests and analyzing the results.

https://github.com/PortSwigger/turbo-intruder

race-the-web - Tests for race conditions in web applications. Includes a RESTful API to integrate into a continuous integration pipeline.

https://github.com/TheHackerDev/race-the-web

Request Smuggling

http-request-smuggling - HTTP Request Smuggling Detection Tool

https://github.com/anshumanpattnaik/http-request-smuggling

smuggler - Smuggler - An HTTP Request Smuggling / Desync testing tool written in Python 3

https://github.com/defparam/smuggler

h2csmuggler - HTTP Request Smuggling over HTTP/2 Cleartext (h2c)

https://github.com/BishopFox/h2csmuggler

tiscripts - These scripts I use to create Request Smuggling Desync payloads for CLTE and TECL style attacks.

https://github.com/defparam/tiscripts

Server Side Request Forgery

SSRFmap - Automatic SSRF fuzzer and exploitation tool

https://github.com/swisskyrepo/SSRFmap

Gopherus - This tool generates gopher link for exploiting SSRF and gaining RCE in various servers

https://github.com/tarunkant/Gopherus

ground-control - A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.

https://github.com/jobertabma/ground-control

SSRFire - An automated SSRF finder. Just give the domain name and your server and chill! ;) Also has options to find XSS and open redirects

https://github.com/ksharinarayanan/SSRFire

httprebind - Automatic tool for DNS rebinding-based SSRF attacks

https://github.com/daeken/httprebind

ssrf-sheriff - A simple SSRF-testing sheriff written in Go

https://github.com/teknogeek/ssrf-sheriff

B-XSSRF - Toolkit to detect and keep track on Blind XSS, XXE & SSRF

https://github.com/SpiderMate/B-XSSRF

extended-ssrf-search - Smart ssrf scanner using different methods like parameter brute forcing in post and get.

https://github.com/Damian89/extended-ssrf-search

gaussrf - Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl and Filter Urls With OpenRedirection or SSRF Parameters.

https://github.com/KathanP19/gaussrf

ssrfDetector - Server-side request forgery detector

https://github.com/JacobReynolds/ssrfDetector

grafana-ssrf - Authenticated SSRF in Grafana

https://github.com/RandomRobbieBF/grafana-ssrf

sentrySSRF - Tool to searching sentry config on page or in javascript files and check blind SSRF

https://github.com/xawdxawdx/sentrySSRF

lorsrf - Bruteforcing on Hidden parameters to find SSRF vulnerability using GET and POST Methods

https://github.com/knassar702/lorsrf

singularity - A DNS rebinding attack framework.

https://github.com/nccgroup/singularity

whonow - A "malicious" DNS server for executing DNS Rebinding attacks on the fly (public instance running on rebind.network:53)

https://github.com/brannondorsey/whonow

dns-rebind-toolkit - A front-end JavaScript toolkit for creating DNS rebinding attacks.

https://github.com/brannondorsey/dns-rebind-toolkit

dref - DNS Rebinding Exploitation Framework

https://github.com/FSecureLABS/dref

rbndr - Simple DNS Rebinding Service

https://github.com/taviso/rbndr

httprebind - Automatic tool for DNS rebinding-based SSRF attacks

https://github.com/daeken/httprebind

dnsFookup - DNS rebinding toolkit

https://github.com/makuga01/dnsFookup

SQL Injection

sqlmap - Automatic SQL injection and database takeover tool

https://github.com/sqlmapproject/sqlmap

NoSQLMap - Automated NoSQL database enumeration and web application exploitation tool.

https://github.com/codingo/NoSQLMap

SQLiScanner - Automatic SQL injection with Charles and sqlmap api

https://github.com/0xbug/SQLiScanner

SleuthQL - Python3 Burp History parsing tool to discover potential SQL injection points. To be used in tandem with SQLmap.

https://github.com/RhinoSecurityLabs/SleuthQL

mssqlproxy - mssqlproxy is a toolkit aimed to perform lateral movement in restricted environments through a compromised Microsoft SQL Server via socket reuse

https://github.com/blackarrowsec/mssqlproxy

sqli-hunter - SQLi-Hunter is a simple HTTP / HTTPS proxy server and a SQLMAP API wrapper that makes digging SQLi easy.

https://github.com/zt2/sqli-hunter

waybackSqliScanner - Gather urls from wayback machine then test each GET parameter for sql injection.

https://github.com/ghostlulzhacks/waybackSqliScanner

ESC - Evil SQL Client (ESC) is an interactive .NET SQL console client with enhanced SQL Server discovery, access, and data exfiltration features.

https://github.com/NetSPI/ESC

mssqli-duet - SQL injection script for MSSQL that extracts domain users from an Active Directory environment based on RID bruteforcing

https://github.com/Keramas/mssqli-duet

burp-to-sqlmap - Performing SQLInjection test on Burp Suite Bulk Requests using SQLMap

https://github.com/Miladkhoshdel/burp-to-sqlmap

BurpSQLTruncSanner - Messy BurpSuite plugin for SQL Truncation vulnerabilities.

https://github.com/InitRoot/BurpSQLTruncSanner

andor - Blind SQL Injection Tool with Golang

https://github.com/sadicann/andor

Blinder - A python library to automate time-based blind SQL injection

https://github.com/mhaskar/Blinder

sqliv - massive SQL injection vulnerability scanner

https://github.com/the-robot/sqliv

nosqli - NoSql Injection CLI tool, for finding vulnerable websites using MongoDB.

https://github.com/Charlie-belmer/nosqli

XSS Injection

XSStrike - Most advanced XSS scanner.

https://github.com/s0md3v/XSStrike

xssor2 - XSS'OR - Hack with JavaScript.

https://github.com/evilcos/xssor2

xsscrapy - XSS spider - 66/66 wavsep XSS detected

https://github.com/DanMcInerney/xsscrapy

sleepy-puppy - Sleepy Puppy XSS Payload Management Framework

https://github.com/Netflix-Skunkworks/sleepy-puppy

ezXSS - ezXSS is an easy way for penetration testers and bug bounty hunters to test (blind) Cross Site Scripting.

https://github.com/ssl/ezXSS

xsshunter - The XSS Hunter service - a portable version of XSSHunter.com

https://github.com/mandatoryprogrammer/xsshunter

dalfox - DalFox(Finder Of XSS) / Parameter Analysis and XSS Scanning tool based on golang

https://github.com/hahwul/dalfox

xsser - Cross Site "Scripter" (aka XSSer) is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based applications.

https://github.com/epsylon/xsser

XSpear - Powerfull XSS Scanning and Parameter analysis tool&gem

https://github.com/hahwul/XSpear

weaponised-XSS-payloads - XSS payloads designed to turn alert(1) into P1

https://github.com/hakluke/weaponised-XSS-payloads

tracy - A tool designed to assist with finding all sinks and sources of a web application and display these results in a digestible manner.

https://github.com/nccgroup/tracy

ground-control - A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.

https://github.com/jobertabma/ground-control

xssValidator - This is a burp intruder extender that is designed for automation and validation of XSS vulnerabilities.

https://github.com/nVisium/xssValidator

JSShell - An interactive multi-user web JS shell

https://github.com/Den1al/JSShell

bXSS - bXSS is a utility which can be used by bug hunters and organizations to identify Blind Cross-Site Scripting.

https://github.com/LewisArdern/bXSS

docem - Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids)

https://github.com/whitel1st/docem

XSS-Radar - XSS Radar is a tool that detects parameters and fuzzes them for cross-site scripting vulnerabilities.

https://github.com/bugbountyforum/XSS-Radar

BruteXSS - BruteXSS is a tool written in python simply to find XSS vulnerabilities in web application.

https://github.com/rajeshmajumdar/BruteXSS

findom-xss - A fast DOM based XSS vulnerability scanner with simplicity.

https://github.com/dwisiswant0/findom-xss

domdig - DOM XSS scanner for Single Page Applications

https://github.com/fcavallarin/domdig

femida - Automated blind-xss search for Burp Suite

https://github.com/wish-i-was/femida

B-XSSRF - Toolkit to detect and keep track on Blind XSS, XXE & SSRF

https://github.com/SpiderMate/B-XSSRF

domxssscanner - DOMXSS Scanner is an online tool to scan source code for DOM based XSS vulnerabilities

https://github.com/yaph/domxssscanner

xsshunter_client - Correlated injection proxy tool for XSS Hunter

https://github.com/mandatoryprogrammer/xsshunter_client

extended-xss-search - A better version of my xssfinder tool - scans for different types of xss on a list of urls.

https://github.com/Damian89/extended-xss-search

xssmap - XSSMap 是一款基于 Python3 开发用于检测 XSS 漏洞的工具

https://github.com/Jewel591/xssmap

XSSCon - XSSCon: Simple XSS Scanner tool

https://github.com/menkrep1337/XSSCon

BitBlinder - BurpSuite extension to inject custom cross-site scripting payloads on every form/request submitted to detect blind XSS vulnerabilities

https://github.com/BitTheByte/BitBlinder

XSSOauthPersistence - Maintaining account persistence via XSS and Oauth

https://github.com/dxa4481/XSSOauthPersistence

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)

https://github.com/shadow-workers/shadow-workers

rexsser - This is a burp plugin that extracts keywords from response using regexes and test for reflected XSS on the target scope.

https://github.com/profmoriarity/rexsser

xss-flare - XSS hunter on cloudflare serverless workers.

https://github.com/EgeBalci/xss-flare

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

https://github.com/jiangsir404/Xss-Sql-Fuzz

vaya-ciego-nen - Detect, manage and exploit Blind Cross-site scripting (XSS) vulnerabilities.

https://github.com/hipotermia/vaya-ciego-nen

dom-based-xss-finder - Chrome extension that finds DOM based XSS vulnerabilities

https://github.com/AsaiKen/dom-based-xss-finder

XSSTerminal - Develop your own XSS Payload using interactive typing

https://github.com/machinexa2/XSSTerminal

xss2png - PNG IDAT chunks XSS payload generator

https://github.com/vavkamil/xss2png

XSSwagger - A simple Swagger-ui scanner that can detect old versions vulnerable to various XSS attacks

https://github.com/vavkamil/XSSwagger

XXE Injection

ground-control - A collection of scripts that run on my web server. Mainly for debugging SSRF, blind XSS, and XXE vulnerabilities.

https://github.com/jobertabma/ground-control

dtd-finder - List DTDs and generate XXE payloads using those local DTDs.

https://github.com/GoSecure/dtd-finder

docem - Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids)

https://github.com/whitel1st/docem

xxeserv - A mini webserver with FTP support for XXE payloads

https://github.com/staaldraad/xxeserv

xxexploiter - Tool to help exploit XXE vulnerabilities

https://github.com/luisfontes19/xxexploiter

B-XSSRF - Toolkit to detect and keep track on Blind XSS, XXE & SSRF

https://github.com/SpiderMate/B-XSSRF

XXEinjector - Tool for automatic exploitation of XXE vulnerability using direct and different out of band methods.

https://github.com/enjoiz/XXEinjector

oxml_xxe - A tool for embedding XXE/XML exploits into different filetypes

https://github.com/BuffaloWill/oxml_xxe

metahttp - A bash script that automates the scanning of a target network for HTTP resources through XXE

https://github.com/vp777/metahttp

Miscellaneous

Passwords

thc-hydra - Hydra is a parallelized login cracker which supports numerous protocols to attack.

https://github.com/vanhauser-thc/thc-hydra

DefaultCreds-cheat-sheet - One place for all the default credentials to assist the Blue/Red teamers activities on finding devices with default password

https://github.com/ihebski/DefaultCreds-cheat-sheet

changeme - A default credential scanner.

https://github.com/ztgrace/changeme

BruteX - Automatically brute force all services running on a target.

https://github.com/1N3/BruteX

patator - Patator is a multi-purpose brute-forcer, with a modular design and a flexible usage.

https://github.com/lanjelot/patator

Secrets

git-secrets - Prevents you from committing secrets and credentials into git repositories

https://github.com/awslabs/git-secrets

gitleaks - Scan git repos (or files) for secrets using regex and entropy

https://github.com/zricethezav/gitleaks

truffleHog - Searches through git repositories for high entropy strings and secrets, digging deep into commit history

https://github.com/trufflesecurity/trufflehog

gitGraber - gitGraber: monitor GitHub to search and find sensitive data in real time for different online services

https://github.com/hisxo/gitGraber

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.

https://github.com/thoughtworks/talisman

GitGot - Semi-automated, feedback-driven tool to rapidly search through troves of public data on GitHub for sensitive secrets.

https://github.com/BishopFox/GitGot

git-all-secrets - A tool to capture all the git secrets by leveraging multiple open source git searching tools

https://github.com/anshumanbh/git-all-secrets

github-search - Tools to perform basic search on GitHub.

https://github.com/gwen001/github-search

git-vuln-finder - Finding potential software vulnerabilities from git commit messages

https://github.com/cve-search/git-vuln-finder

commit-stream - #OSINT tool for finding Github repositories by extracting commit logs in real time from the Github event API

https://github.com/x1sec/commit-stream

gitrob - Reconnaissance tool for GitHub organizations

https://github.com/michenriksen/gitrob

repo-supervisor - Scan your code for security misconfiguration, search for passwords and secrets.

https://github.com/auth0/repo-supervisor

GitMiner - Tool for advanced mining for content on Github

https://github.com/UnkL4b/GitMiner

shhgit - Ah shhgit! Find GitHub secrets in real time

https://github.com/eth0izzle/shhgit

detect-secrets - An enterprise friendly way of detecting and preventing secrets in code.

https://github.com/Yelp/detect-secrets

rusty-hog - A suite of secret scanners built in Rust for performance. Based on TruffleHog

https://github.com/newrelic/rusty-hog

whispers - Identify hardcoded secrets and dangerous behaviours

https://github.com/Skyscanner/whispers

yar - Yar is a tool for plunderin' organizations, users and/or repositories.

https://github.com/nielsing/yar

dufflebag - Search exposed EBS volumes for secrets

https://github.com/BishopFox/dufflebag

secret-bridge - Monitors Github for leaked secrets

https://github.com/duo-labs/secret-bridge

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.

https://github.com/americanexpress/earlybird

Trufflehog-Chrome-Extension - Trufflehog-Chrome-Extension

https://github.com/trufflesecurity/Trufflehog-Chrome-Extension

Git

GitTools - A repository with 3 tools for pwn'ing websites with .git repositories available

https://github.com/internetwache/GitTools

gitjacker - Leak git repositories from misconfigured websites

https://github.com/liamg/gitjacker

git-dumper - A tool to dump a git repository from a website

https://github.com/arthaud/git-dumper

GitHunter - A tool for searching a Git repository for interesting content

https://github.com/digininja/GitHunter

dvcs-ripper - Rip web accessible (distributed) version control systems: SVN/GIT/HG...

https://github.com/kost/dvcs-ripper

Buckets

S3Scanner - Scan for open AWS S3 buckets and dump the contents

https://github.com/sa7mon/S3Scanner

AWSBucketDump - Security Tool to Look For Interesting Files in S3 Buckets

https://github.com/jordanpotti/AWSBucketDump

CloudScraper - CloudScraper: Tool to enumerate targets in search of cloud resources. S3 Buckets, Azure Blobs, Digital Ocean Storage Space.

https://github.com/jordanpotti/CloudScraper

s3viewer - Publicly Open Amazon AWS S3 Bucket Viewer

https://github.com/SharonBrizinov/s3viewer

festin - FestIn - S3 Bucket Weakness Discovery

https://github.com/cr0hn/festin

s3reverse - The format of various s3 buckets is convert in one format. for bugbounty and security testing.

https://github.com/hahwul/s3reverse

mass-s3-bucket-tester - This tests a list of s3 buckets to see if they have dir listings enabled or if they are uploadable

https://github.com/random-robbie/mass-s3-bucket-tester

S3BucketList - Firefox plugin that lists Amazon S3 Buckets found in requests

https://github.com/AlecBlance/S3BucketList

dirlstr - Finds Directory Listings or open S3 buckets from a list of URLs

https://github.com/cybercdh/dirlstr

Burp-AnonymousCloud - Burp extension that performs a passive scan to identify cloud buckets and then test them for publicly accessible vulnerabilities

https://github.com/codewatchorg/Burp-AnonymousCloud

kicks3 - S3 bucket finder from html,js and bucket misconfiguration testing tool

https://github.com/abuvanth/kicks3

2tearsinabucket - Enumerate s3 buckets for a specific target.

https://github.com/Revenant40/2tearsinabucket

s3_objects_check - Whitebox evaluation of effective S3 object permissions, to identify publicly accessible files.

https://github.com/nccgroup/s3_objects_check

s3tk - A security toolkit for Amazon S3

https://github.com/ankane/s3tk

CloudBrute - Awesome cloud enumerator

https://github.com/0xsha/CloudBrute

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.

https://github.com/0xspade/s3cario

S3Cruze - All-in-one AWS S3 bucket tool for pentesters.
https://github.com/JR0ch17/S3Cruze

CMS

wpscan - WPScan is a free, for non-commercial use, black box WordPress security scanner
https://github.com/wpscanteam/wpscan

WPSpider - A centralized dashboard for running and scheduling WordPress scans powered by wpscan utility.
https://github.com/cyc10n3/WPSpider

wprecon - Wordpress Recon
https://github.com/AngraTeam/wprecon

CMSmap - CMSmap is a python open source CMS scanner that automates the process of detecting security flaws of the most popular CMSs.
https://github.com/Dionach/CMSmap

joomscan - OWASP Joomla Vulnerability Scanner Project
https://github.com/OWASP/joomscan

pyfiscan - Free web-application vulnerability and version scanner
https://github.com/fgeek/pyfiscan

JSON Web Token

jwt_tool - A toolkit for testing, tweaking and cracking JSON Web Tokens
https://github.com/ticarpi/jwt_tool

c-jwt-cracker - JWT brute force cracker written in C
https://github.com/brendan-rius/c-jwt-cracker

jwt-heartbreaker - The Burp extension to check JWT (JSON Web Tokens) for using keys from known from public sources

https://github.com/wallarm/jwt-heartbreaker

jwtear - Modular command-line tool to parse, create and manipulate JWT tokens for hackers

https://github.com/KINGSABRI/jwtear

jwt-key-id-injector - Simple python script to check against hypothetical JWT vulnerability.

https://github.com/dariusztytko/jwt-key-id-injector

jwt-hack - jwt-hack is tool for hacking / security testing to JWT.

https://github.com/hahwul/jwt-hack

jwt-cracker - Simple HS256 JWT token brute force cracker

https://github.com/lmammino/jwt-cracker

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

https://github.com/fransr/postMessage-tracker

PostMessage_Fuzz_Tool - #BugBounty #BugBounty Tools #WebDeveloper Tool

https://github.com/kiranreddyrebel/PostMessage_Fuzz_Tool

Subdomain Takeover

subjack - Subdomain Takeover tool written in Go

https://github.com/haccer/subjack

SubOver - A Powerful Subdomain Takeover Tool

https://github.com/Ice3man543/SubOver

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.

https://github.com/JordyZomer/autoSubTakeover

NSBrute - Python utility to takeover domains vulnerable to AWS NS Takeover

https://github.com/shivsahni/NSBrute

can-i-take-over-xyz - "Can I take over XYZ?" — a list of services and how to claim (sub)domains with dangling DNS records.

https://github.com/EdOverflow/can-i-take-over-xyz

cnames - take a list of resolved subdomains and output any corresponding CNAMES en masse.

https://github.com/cybercdh/cnames

subHijack - Hijacking forgotten & misconfigured subdomains

https://github.com/vavkamil/old-repos-backup/tree/master/subHijack-master

tko-subs - A tool that can help detect and takeover subdomains with dead DNS records

https://github.com/anshumanbh/tko-subs

HostileSubBruteforcer - This app will bruteforce for exisiting subdomains and provide information if the 3rd party host has been properly setup.

https://github.com/nahamsec/HostileSubBruteforcer

second-order - Second-order subdomain takeover scanner

https://github.com/mhmdiaa/second-order

takeover - A tool for testing subdomain takeover possibilities at a mass scale.

https://github.com/mzfr/takeover

https://github.com/Ice3man543/SubOver

Uncategorized

JSONBee - A ready to use JSONP endpoints/payloads to help bypass content security policy (CSP) of different websites.

https://github.com/zigoo0/JSONBee

CyberChef - The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis

https://github.com/gchq/CyberChef

bountyplz - Automated security reporting from markdown templates (HackerOne and Bugcrowd are currently the platforms supported)

https://github.com/fransr/bountyplz

PayloadsAllTheThings - A list of useful payloads and bypass for Web Application Security and Pentest/CTF

https://github.com/swisskyrepo/PayloadsAllTheThings

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

https://github.com/arkadiyt/bounty-targets-data

android-security-awesome - A collection of android security related resources

https://github.com/ashishb/android-security-awesome

awesome-mobile-security - An effort to build a single place for all useful android and iOS security related stuff.

https://github.com/vaib25vicky/awesome-mobile-security

awesome-vulnerable-apps - Awesome Vulnerable Applications

https://github.com/vavkamil/awesome-vulnerable-apps

XFFenum - X-Forwarded-For [403 forbidden] enumeration

https://github.com/vavkamil/XFFenum

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.

https://github.com/projectdiscovery/httpx