# Bug bounty Tool Mindmap

read above all answers, analyse it and help me making my technologies.sh file . Update my technologies.sh file and make it more better, more efficient and more useful according to main.sh file scenario and structure.

bug\_bounty\_automation/

main.sh

modules/

subdomain\_enumeration.sh

port\_scanning.sh

screenshots.sh

technologies.sh

content\_discovery.sh

links.sh

parameters.sh

fuzzing.sh

command\_injection.sh

cors\_misconfiguration.sh

crlf\_injection.sh

csrf\_injection.sh

directory\_traversal.sh

file\_inclusion.sh

graphql\_injection.sh

header\_injection.sh

insecure\_deserialization.sh

insecure\_direct\_object\_references.sh

open\_redirect.sh

race\_condition.sh

request\_smuggling.sh

server\_side\_request\_forgery.sh

sql\_injection.sh

xss\_injection.sh

xxe\_injection.sh

passwords.sh

secrets.sh

git.sh

buckets.sh

cms.sh

json\_web\_token.sh

post\_message.sh

subdomain\_takeover.sh

vulnerability\_scanners.sh

# Tools Category Division

* Subdomain Enumeration

• Port Scanning

• Screenshots

• Technologies

• Content Discovery

• Links

• Parameters

• Fuzzing

• 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

• Passwords

• Secrets

• Git

• Buckets

• CMS

• JSON Web Token

• postMessage

• Subdomain Takeover

• Vulnerability Scanners

# Tools Names Total

Subdomain Enumeration: Sublist3r, Amass, subfinder, assetfinder, massdns, Findomain,

Port Scanning: masscan, nmap

Screenshots: EyeWitness, aquatone

Technologies: wappalyzer, webanalyze,

Content Discovery: gobuster, feroxbuster, dirsearch, dirsearch (Go implementation), gospider, hakrawler,

Links: LinkFinder, JS-Scan, waybackurls, gau,

Parameters: parameth, Arjun, x8

Fuzzing: wfuzz, ffuf, fuzzdb,

Command Injection: commix

CORS Misconfiguration: Corsy, CORStest,

CRLF Injection: CRLFsuite, crlfuzz,

CSRF Injection: XSRFProbe

Directory Traversal: dotdotpwn, FDsploit, off-by-slash,

File Inclusion: liffy, Burp-LFI-tests, LFI-Enum,

GraphQL Injection: inql, GraphQLmap, shapeshifter,

Header Injection: headi

Insecure Deserialization: ysoserial, GadgetProbe, ysoserial.net,

Insecure Direct Object References: Autorize

Open Redirect: Oralyzer, Injectus, dom-red,

Request Smuggling: http-request-smuggling, smuggler, h2csmuggler,

Server Side Request Forgery: SSRFmap, Gopherus, ground-control, SSRFire,

SQL Injection: sqlmap, NoSQLMap, SQLiScanner,

XSS Injection: XSStrike, xssor2, dalfox, BruteXSS

XXE Injection: ground-control, dtd-finder,

Passwords: thc-hydra,

Secrets: git-secrets, gitleaks, truffleHog,

Git: GitTools, gitjacker, git-dumper,

Buckets: S3Scanner, AWSBucketDump,

CMS: wpscan, WPSpider, wprecon,

JSON Web Token: jwt\_tool, c-jwt-cracker,

postMessage: postMessage-tracker, PostMessage\_Fuzz\_Tool

Subdomain Takeover: subjack, SubOver, autoSubTakeover, NSBrute, can-i-take-over-xyz,

Vulnerability Scanners: nuclei, Sn1per,