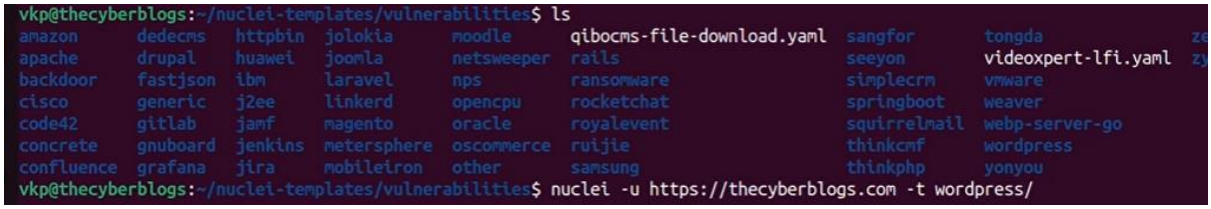
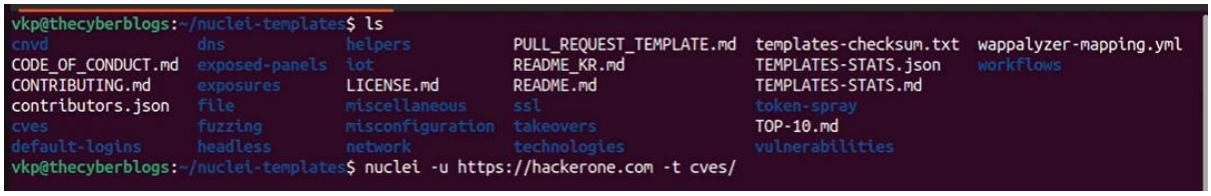
Attack Name	Tools
SubDomain	**SubFinder::** subfinder -d www.abc.xyz subfinder -dL target.txt subfinder -d hackerone.com -nW -silent > hackerone.txt subfinder -d hackerone.com -nW -silent | tee hackerone.txt **Sublist3r::** sublist3r -d hackerone.com -b amass enum -d hackerone.com assetfinder hackerone.com assetfinder hackerone.com > hackerone.txt **knockpy::** python3 knockpy.py hackerone.com python3 knockpy.py hackerone.com --no-http-code 404 500 530 **Anew::** cat 1.txt | anew 2.txt > 3.txt
Subdomain enumeration from tools	https://www.virustotal.com/gui/home/upload https://search.censys.io/ https://chaos.projectdiscovery.io/#/ crt.sh
Filtering live domains	cat * | sort -u | wc -l cat * | grep -E *.hackerone.com |sort -u | tee hackerone.com cat hackerone.com | wc -l cat hackerone.com | httpx cat hackerone.com | httpx -sc cat hackerone.com | httpx -ct cat hackerone.com | httpx -td cat hackerone.com | httpx -ip cat hackerone.com | httpx -title cat hackerone.com | httpx –cname
URL extraction from the internet	echo "www.hackerone.com" | gau echo "www.hackerone.com" | gau | tee hackerone.txt cat hackerone.txt | grep ? | tee hack.txt cat hackerone.txt | grep -E *[.]js gospider -s www.abc.xyz --subs --js --sitemap --robots -o abc.txt
Finding Paramtere	https://github.com/devanshbatham/ParamSpider python3 paramspider.py -d hackerone.com https://github.com/s0md3v/Arjun arjun -u hackerone.com
Finding Link from past	https://archive.org/web/ https://github.com/tomnomnom/waybackurls echo "hackerone.com" | waybackurls

sorting url	cat * | gf xss cat * | gf rce cat * | gf idor cat * | gf lfi cat * | gf sqli cat * | gf redirects
Automation for replacing parameters with Payloads	https://github.com/tomnomnom/qsreplace cat 1.txt | qsreplace "<script>alert(1)</script>"
Footprinting websites	https://github.com/urbanadventurer/WhatWeb whatweb hackerone.com whatweb hackerone.com -v netcraft, Security Headers, dnsdump, domaintools, mstoolbox, Osint, mulfrats
Browser Addons	Wappalyzer , retire.js , shodan , knoxx , Hack Tools
Waff Testing	wafw00f www.abc.xyz
Subdomain takeOver	https://github.com/nahamsec/HostileSubBruteforcer ruby sub_brute.rb --fast https://github.com/r3curs1v3-pr0xy/sub404 python3 sub404.py -h python3 sub404.py -f txtfilepath https://github.com/haccer/subjack apt install subjack subjack pathlist -v
Fuzzing	dirb www.abc.xyz dirb www.abc.xyz wordlist ffuf -u www.abc.xyz/FUZZ -w wordlistpath ffuf -u www.abc.xyz/FUZZ -w wordlistpath -mc 200,300 ffuf -u FUZZ.abc.xom -w subdomain.txt -mc 200,301
Port Scaning	nmap www.abc.xyz nmap www.abc.xyz -p1-100 nmap www.abc.xyz -p- nmap www.abc.xyz -p smtp,http nmap www.abc.xyz -F nmap www.abc.xyz --top-ports 2000 nmap www.abc.xyz -sV nmap www.abc.xyz -sV --version-intersity 8 nmap www.abc.xyz -sV --version-light nmap www.abc.xyz -sV --version-all nmap www.abc.xyz -O naabu -host www.abc.xyz naabu -host www.abc.xyz -silent

Vulnerability scanning	https://github.com/projectdiscovery/nuclei nuclei -h nuclei -u www.abc.xyz nuclei -u www.abc.xyz -t wordpress -v nuclei -u www.abc.xyz -t cevs/ -v wpscan --url www.abc.xyz -e u wpscan --url www.abc.xyz -e vp wpscan --url www.abc.xyz -e dbe wpscan --url www.abc.xyz -e cb wpscan --url www.abc.xyz -plugin-detection passsive –v





Source ::: Link