

Attack Name	Tools
SubDomain	<b>SubFinder::</b> 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  <b>Sublist3r::</b> sublist3r -d hackerone.com -b amass enum -d hackerone.com assetfinder hackerone.com assetfinder hackerone.com > hackerone.txt  <b>knockpy::</b> python3 knockpy.py hackerone.com python3 knockpy.py hackerone.com --no-http-code 404 500 530  <b>Anew::</b> cat 1.txt   anew 2.txt > 3.txt
Subdomain enumeration from tools	<a href="https://www.virustotal.com/gui/home/upload">https://www.virustotal.com/gui/home/upload</a> <a href="https://search.censys.io/">https://search.censys.io/</a> <a href="https://chaos.projectdiscovery.io/#/">https://chaos.projectdiscovery.io/#/</a> 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	<a href="https://github.com/devanshbatham/ParamSpider">https://github.com/devanshbatham/ParamSpider</a> python3 paramspider.py -d hackerone.com  <a href="https://github.com/s0md3v/Arjun">https://github.com/s0md3v/Arjun</a> arjun -u hackerone.com
Finding Link from past	<a href="https://archive.org/web/">https://archive.org/web/</a>  <a href="https://github.com/tomnomnom/waybackurls">https://github.com/tomnomnom/waybackurls</a> echo "hackerone.com"   waybackurls

<b>sorting url</b>	cat *   gf xss cat *   gf rce cat *   gf idor cat *   gf lfi cat *   gf sqli cat *   gf redirects
<b>Automation for replacing parameters with Payloads</b>	https://github.com/tomnomnom/qsreplace cat 1.txt   qsreplace "<script>alert(1)</script>"
<b>Footprinting websites</b>	https://github.com/urbanadventurer/WhatWeb whatweb hackerone.com whatweb hackerone.com -v  <a href="#">netcraft</a> , <a href="#">Security Headers</a> , <a href="#">dnsdump</a> , <a href="#">domaintools</a> , <a href="#">mstoolbox</a> , <a href="#">Osint</a> , <a href="#">mulfrats</a>
<b>Browser Addons</b>	<a href="#">Wappalyzer</a> , <a href="#">retire.js</a> , <a href="#">shodan</a> , <a href="#">knoxx</a> , <a href="#">Hack Tools</a>
<b>Waff Testing</b>	wafw00f www.abc.xyz
<b>Subdomain takeOver</b>	https://github.com/naamsec/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
<b>Fuzzing</b>	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
<b>Port Scanning</b>	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-intensity 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

<b>Vulnerability scanning</b>	<p><a href="https://github.com/projectdiscovery/nuclei">https://github.com/projectdiscovery/nuclei</a></p> <p>nuclei -h</p> <p>nuclei -u www.abc.xyz</p> <p>nuclei -u www.abc.xyz -t wordpress -v</p> <p>nuclei -u www.abc.xyz -t cve/ -v</p> <p>wpscan --url www.abc.xyz -e u</p> <p>wpscan --url www.abc.xyz -e vp</p> <p>wpscan --url www.abc.xyz -e db</p> <p>wpscan --url www.abc.xyz -e cb</p> <p>wpscan --url www.abc.xyz -plugin-detection passive -v</p>

```

vkp@the cyberblogs:~/nuclei-templates/vulnerabilities$ ls
amazon      dedecms     httpbin     jolokia     moodle      qibocms-file-download.yaml  sangfor      tongda      ze
apache      drupal      huawei       joomla      netsweeper  rails                seeyon       videexpert-lfi.yaml  zy
backdoor    fastjson    ibm         laravel     nps         ransomware          simplecrn    vmware
cisco       generic     j2ee        linkerd     opencpu     rocketchat          springboot   weaver
code42      gitlab      jamf        magento     oracle      royalevent          squirrelmail  webp-server-go
concrete    gnuboard    jenkins     metersphere oscommerce  ruijie              thinkcmf     wordpress
confluence  grafana     jira        mobileiron  other        samsung              thinkphp     yonyou
vkp@the cyberblogs:~/nuclei-templates/vulnerabilities$ nuclei -u https://the cyberblogs.com -t wordpress/

vkp@the cyberblogs:~/nuclei-templates$ ls
cnvd        dns          helpers      PULL_REQUEST_TEMPLATE.md  templates-checksum.txt  wappalyzer-mapping.yml
CODE_OF_CONDUCT.md  exposed-panels  iot          README_KR.md              TEMPLATES-STATS.json   workflows
CONTRIBUTING.md    exposures      LICENSE.md   README.md                  TEMPLATES-STATS.md
contributors.json    file           miscellaneous  ssl                        token-spray
cves              fuzzing        misconfiguration  takeovers                 TOP-10.md
default-logins     headless       network          technologies               vulnerabilities
vkp@the cyberblogs:~/nuclei-templates$ nuclei -u https://hackerone.com -t cves/

```

Source ::: [Link](#)