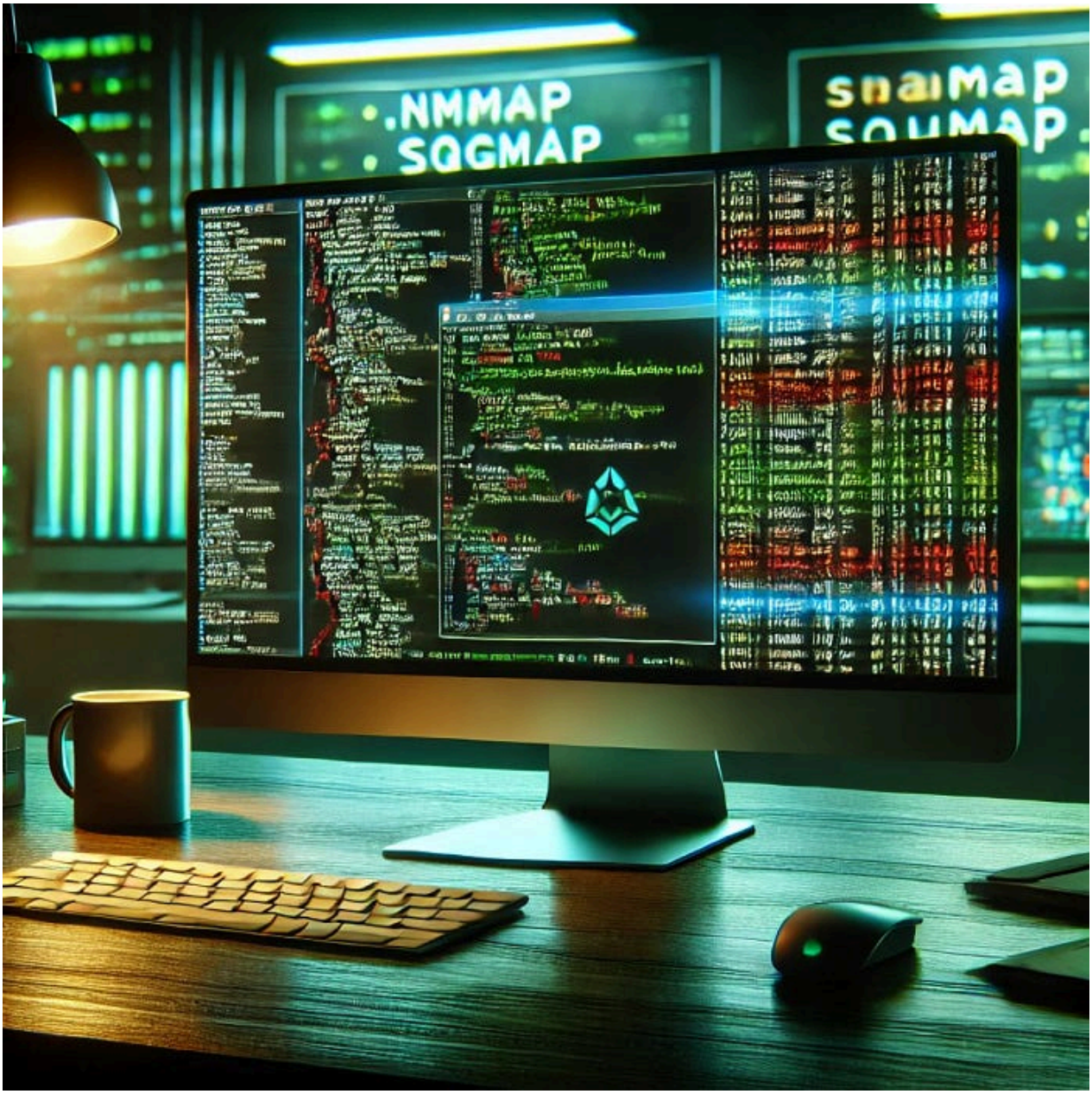
100 CLI Flags and Tricks Every Bug Bounty Hunter Should Know

16 April 2025 - Posted in tools (https://blog.hackxpert.com/category/tools) by The XSS Rat (https://blog.hackxpert.com/author/uncle rat)



Bug bounty hunting is an exciting yet challenging field that requires the mastery of numerous tools and techniques. While graphical interfaces can simplify tasks, the real power often lies in command-line interfaces (CLI). For bug bounty hunters, knowing the right CLI commands and flags can make the difference between success and failure.

This guide explores 100 essential CLI flags and tricks across popular tools for reconnaissance, scanning, exploitation, and post-exploitation. Whether you're just starting out or refining your skills, these commands will boost your efficiency and effectiveness.

Reconnaissance and OSINT Tools

Reconnaissance is the foundation of bug bounty hunting. These commands help you gather critical information about your targets:

1. `nmap -A` – Enable OS detection and version detection.
2. `nmap -sC` – Run default scripts for enumeration.
3. `nmap -sV` – Detect service versions.
4. `nmap --script vuln` – Run vulnerability detection scripts.

5. `nmap -Pn` – Disable host discovery and scan all targets.
6. `nmap -p-` – Scan all 65,535 ports.
7. `nmap --top-ports 100` – Scan top 100 ports.
8. `nmap -oN output.txt` – Save output in normal format.
9. `nmap -oX output.xml` – Save output in XML format for automation.
10. `nmap -iL targets.txt` – Input list of targets to scan.
11. `amass enum -d domain.com` – Enumerate subdomains.
12. `amass intel -whois -d domain.com` – Perform WHOIS-based reconnaissance.
13. `amass track -d domain.com` – Track subdomain changes over time.
14. `amass viz -d domain.com -o output.graphml` – Visualize enumeration results.
15. `subfinder -d domain.com` – Find subdomains quickly.
16. `subfinder -d domain.com -silent` – Silent mode for clean output.
17. `subfinder -d domain.com -o output.txt` – Save subdomains to file.
18. `assetfinder --subs-only domain.com` – Discover subdomains.
19. `waybackurls domain.com` – Fetch URLs from the Wayback Machine.
20. `gau domain.com` – Fetch archived URLs from multiple sources.
21. `httpx -silent` – Test HTTP/HTTPS services silently.
22. `httpx -status-code` – Include HTTP status codes in output.
23. `httpx -title` – Display page titles.
24. `httpx -tech-detect` – Detect technologies used on target.
25. `dnsx -d domain.com` – Perform DNS probing.

Scanning Tools

Use these commands to scan for open ports, directories, and vulnerabilities:

1. `masscan -p0-65535 target` – Fast scan for all ports.
2. `masscan --rate 1000 -p22,80 target` – Set rate limit for scanning.
3. `masscan -iL targets.txt` – Read targets from a file.
4. `ffuf -w wordlist.txt -u http://target/FUZZ` – Fuzz directories.
5. `ffuf -w wordlist.txt -u http://target/FUZZ -mc 200` – Match HTTP status 200 only.
6. `ffuf -c` – Use colors for better readability.
7. `ffuf -H "Authorization: Bearer TOKEN"` – Add headers to requests.
8. `ffuf -fs 4242` – Filter results by size.
9. `ffuf -recursion` – Enable directory recursion fuzzing.
10. `dirsearch -u http://target` – Directory brute-forcing.
11. `dirsearch -e php,html,js` – Add extensions to fuzzing.
12. `dirsearch --threads 50` – Set thread count.
13. `dirsearch -x 404` – Exclude 404 responses.
14. `gobuster dir -u http://target -w wordlist.txt` – Fuzz directories.
15. `gobuster dns -d domain.com -w wordlist.tx t` – Fuzz DNS subdomains.
16. `gobuster -k` – Ignore SSL certificate warnings.
17. `gobuster dir -o output.txt` – Save results to file.
18. `nikto -host http://target` – Scan for vulnerabilities.
19. `nikto -ssl` – Force SSL scanning.

20. `nikto -output output.txt` – Save scan results.

Exploitation Tools

Once reconnaissance and scanning are complete, these tools help you exploit discovered vulnerabilities:

1. `sqlmap -u http://target --dbs` – Enumerate databases.
2. `sqlmap -u http://target -D dbname --tables` – List tables in a database.
3. `sqlmap -u http://target -D dbname -T table --columns` – List columns.
4. `sqlmap -u http://target -D dbname -T table -C column --dump` – Dump data.
5. `sqlmap --batch` – Run in non-interactive mode.
6. `sqlmap --risk 3 --level 5` – Increase testing depth.
7. `hydra -l admin -P passwords.txt target http-post-form "/login:username=^USER^&password=^PASS^:F=Invalid"` – Brute-force
8. `hydra -t 16 -L users.txt -P passwords.txt ssh://target` – SSH brute-forcing.
9. `metasploit (msfconsole)` – Launch the Metasploit framework.
10. `searchsploit software` – Search for exploits in Exploit-DB.
11. `msfvenom -p payload -f exe > shell.exe` – Generate payloads.
12. `xssstrike -u http://target` – Scan for XSS vulnerabilities.
13. `wfuzz -w wordlist.txt -u http://target/FUZZ` – Fuzzing tool.
14. `wfuzz -z range,1-100` – Use numeric range for fuzzing.
15. `rescope -r scope.txt` – Restrict scanning to in-scope domains.

Post-Exploitation Tools

After gaining access, these tools help you analyze and maintain your foothold:

1. `john --wordlist=passwords.txt hash.txt` – Crack hashes with wordlists.
2. `hashcat -m 0 hash.txt passwords.txt` – Use GPU for cracking hashes.
3. `hashcat --show -m 0 hash.txt` – Display cracked passwords.
4. `sshuttle -r user@host 0/0` – Create a quick VPN-like tunnel.
5. `proxychains tool` – Route tools through a proxy.
6. `socat -d -d TCP-LISTEN:4444 STDOUT` – Create reverse shells.
7. `netcat -lvnp 4444` – Set up a listener for reverse shells.
8. `curl -I http://targe t` – Fetch HTTP headers.
9. `curl -X POST -d "param=value" http://target` – Test POST requests.
10. `curl -H "Authorization: Bearer TOKEN"` – Add headers to requests.

Miscellaneous Tricks

Expand your flexibility with these handy tricks:

1. `git clone https://github.com/repo.git` – Clone a Git repository.
2. `git log -p` – Check for sensitive changes in Git history.
3. `git grep 'password'` – Search for sensitive keywords in Git repositories.

4. `strings binary` – Extract strings from a binary file.
5. `hexdump -C file` – View file in hex format.
6. `exiftool file.jpg` – Extract metadata from files.
7. `jq '.' file.json` – Pretty-print JSON output.
8. `sed 's/old/new/g' file` – Replace text in files.
9. `awk '{print $1}' file` – Extract specific fields from files.
10. `sort file | uniq -c` – Count unique lines.
11. `base64 -d encoded.txt` – Decode base64 strings.
12. `openssl s_client -connect host:443` – Test SSL/TLS connections.
13. `openssl enc -d -aes-256-cbc -in encrypted.txt` – Decrypt files with OpenSSL.
14. `pspy64` – Monitor processes without root.
15. `strace -p PID` – Trace system calls.
16. `lsof -i :80` – List processes using a specific port.

Network and System Tools

Finish with these powerful network and system utilities:

1. `tcpdump -i eth0 port 80` – Capture packets on a specific port.
2. `wireshark` – Analyze network traffic.
3. `nc -zv host 1-1000` – Scan ports with netcat.
4. `iptables -L` – List firewall rules.
5. `traceroute target` – Trace network paths.
6. `dig domain.com` – Query DNS records.
7. `nslookup domain.com` – Resolve domain names.
8. `host domain.com` – Fetch DNS records.
9. `arp -a` – Display ARP table.
10. `whois domain.com` – Fetch domain ownership details.
11. `wget --mirror -p --convert-links -P ./target http://site` – Mirror a website.
12. `scp file user@host:/path` – Securely copy files.
13. `ssh user@host` – SSH into a target machine.
14. `tmux` – Use terminal multiplexer for managing multiple sessions.

Conclusion

Mastering these 100 CLI flags and tricks will greatly enhance your bug bounty hunting skills. Whether you're gathering reconnaissance data, scanning for vulnerabilities, or performing exploitation and post-exploitation tasks, the right CLI commands can save time and uncover hidden weaknesses. Happy hunting!

cli (https://blog.hackxpert.com/tag/cli)

(https://www.facebook.com/sharer.php?u=https://blog.hackxpert.com/2025/04/100-cli-flags-and-tricks-every-bug-bounty-hunter-should-know&t=100 CLI Flags and Tricks Every Bug Bounty Hunter Should Know)

(https://twitter.com/share?url=https://blog.hackxpert.com/2025/04/100-cli-flags-and-tricks-every-bug-bounty-hunter-should-know&text=100 CLI Flags and Tricks Every Bug Bounty Hunter Should Know)

← Next Post (https://blog.hackxpert.com/2025/04/how-to-get-into-bug-bounties-with-no-experience)
Previous Post → (https://blog.hackxpert.com/2025/01/optimizing-burp-suite-and-zap-for-hunting-business-logic-access-control-bac-vulnerabilities)

Related Posts

The top 25 ways an ethical... (https://blog.hackxpert.com/2024/05/the-top-25-ways-an-ethical-hacker-can-use-ai-in-their-day-to-day-work)

In today's rapidly evolving digital landscape, the role of... more (https://blog.hackxpert.com/2024/05/the-top-25-ways-an-ethical-hacker-can-use-ai-in-their-day-to-day-work)

Using ANY.RUN for Identifying... (https://blog.hackxpert.com/2024/11/using-anyrun-for-identifying-executable-files-that-download-additional-payloads-a-dynamic-approach)

In today's cybersecurity landscape, detecting and analyzing... more (https://blog.hackxpert.com/2024/11/using-anyrun-for-identifying-executable-files-that-download-additional-payloads-a-dynamic-approach)

Nikto - An overview (https://blog.hackxpert.com/2023/09/nikto-an-overview)

Nitko Scanner Nikto is an open-source web server scanner... more (https://blog.hackxpert.com/2023/09/nikto-an-overview)

About

Hackxpert (https://hackxpert.com)
Hackxpert Labs (https://labs.hackxpert.com)
The Cheese Shop (https://cheese-shop.be)
Our Courses (https://thexssrat.com)

Resources

XSS - BruteLogic (https://brutelogic.com.br/blog/)

Recent Posts

How to Get Into Bug Bounties with No Experience (https://blog.hackxpert.com/2025/04/how-to-get-into-bug-bounties-with-no-experience)

Introduction The world of bug bounties is growing, with companies offering...

Read more (https://blog.hackxpert.com/2025/04/how-to-get-into-bug-bounties-with-no-experience)

100 CLI Flags and Tricks Every Bug Bounty Hunter Should Know (https://blog.hackxpert.com/2025/04/100-cli-flags-and-tricks-every-bug-bounty-hunter-should-know)

Bug bounty hunting is an exciting yet challenging field that requires the...

Read more (https://blog.hackxpert.com/2025/04/100-cli-flags-and-tricks-every-bug-bounty-hunter-should-know)

Optimizing Burp Suite and ZAP for Hunting Business Logic... (https://blog.hackxpert.com/2025/01/optimizing-burp-suite-and-zap-for-hunting-business-logic-access-control-bac-vulnerabilities)

Optimizing Burp Suite and ZAP for Hunting Business Logic Access Control...

Read more (https://blog.hackxpert.com/2025/01/optimizing-burp-suite-and-zap-for-hunting-business-logic-access-control-bac-vulnerabilities)

How to become an amazing hacker - in 10 years or less (https://blog.hackxpert.com/2024/11/how-to-become-an-amazing-hacker-in-10-years-or-less)

Introduction Yesterday i wrote the story of how i became an amazing hacker...

Read more (https://blog.hackxpert.com/2024/11/how-to-become-an-amazing-hacker-in-10-years-or-less)

Using ANY.RUN for Identifying Executable Files that... (https://blog.hackxpert.com/2024/11/using-anyrun-for-identifying-executable-files-that-download-additional-payloads-a-dynamic-approach)

In today's cybersecurity landscape, detecting and analyzing malware is...

🔗 Read more (https://blog.hackxpert.com/2024/11/using-anyrun-for-identifying-executable-files-that-download-additional-payloads-a-dynamic-approach)

Archive

▼ 2025 (https://blog.hackxpert.com/archive/2025) (3)
  April (https://blog.hackxpert.com/archive/2025-04) (2)
  January (https://blog.hackxpert.com/archive/2025-01) (1)
► 2024 (https://blog.hackxpert.com/archive/2024) (33)
► 2023 (https://blog.hackxpert.com/archive/2023) (22)

Category

- API (https://blog.hackxpert.com/category/api)
- Bug bounties (https://blog.hackxpert.com/category/bug-bounties)
- Business logic (https://blog.hackxpert.com/category/business-logic)
- CWE (https://blog.hackxpert.com/category/cwe)
- hacking (https://blog.hackxpert.com/category/hacking)
- tools (https://blog.hackxpert.com/category/tools)
- Uncategorized (https://blog.hackxpert.com/category/uncategorized)
- XSS (https://blog.hackxpert.com/category/xss)

Tags

active directory (https://blog.hackxpert.com/tag/active-directory) AD (https://blog.hackxpert.com/tag/ad) AI (https://blog.hackxpert.com/tag/ai) API (https://blog.hackxpert.com/tag/api) auth (https://blog.hackxpert.com/tag/auth) authentication (https://blog.hackxpert.com/tag/authentication) authorisation (https://blog.hackxpert.com/tag/authorisation) automation (https://blog.hackxpert.com/tag/automation) bac (https://blog.hackxpert.com/tag/bac) bb (https://blog.hackxpert.com/tag/bb) breaches (https://blog.hackxpert.com/tag/breaches) Bug Bounty (https://blog.hackxpert.com/tag/bug-bounty) burnout (https://blog.hackxpert.com/tag/burnout) Burp suite (https://blog.hackxpert.com/tag/burp-suite) business logic (https://blog.hackxpert.com/tag/business-logic) career (https://blog.hackxpert.com/tag/career) cheat sheet (https://blog.hackxpert.com/tag/cheat-sheet) checklist (https://blog.hackxpert.com/tag/checklist) cli

(https://blog.hackxpert.com/tag/cli) coding (https://blog.hackxpert.com/tag/coding) csrf (https://blog.hackxpert.com/tag/csrf) CWE (https://blog.hackxpert.com/tag/cwe) cyber security (https://blog.hackxpert.com/tag/cyber-security) Cybersecurity for Beginners (https://blog.hackxpert.com/tag/cybersecurity-for-beginners) Ethical Hacking (https://blog.hackxpert.com/tag/ethical-hacking) file system (https://blog.hackxpert.com/tag/file-system) hacking (https://blog.hackxpert.com/tag/hacking) IDOR (https://blog.hackxpert.com/tag/idor) injection (https://blog.hackxpert.com/tag/injection) javascript (https://blog.hackxpert.com/tag/javascript) linux (https://blog.hackxpert.com/tag/linux) list (https://blog.hackxpert.com/tag/list) lists (https://blog.hackxpert.com/tag/lists) network (https://blog.hackxpert.com/tag/network) recon (https://blog.hackxpert.com/tag/recon) Security (https://blog.hackxpert.com/tag/security) tools (https://blog.hackxpert.com/tag/tools) vulnerabilities (https://blog.hackxpert.com/tag/vulnerabilities) XSS (https://blog.hackxpert.com/tag/xss) zap (https://blog.hackxpert.com/tag/zap)