Bug Bounty & Web Vulnerability Testing Mastery Guide (Day 1-30)

This guide provides 100+ commands and techniques for ethical bug bounty hunting and web vulnerability testing, organized day-by-day for practice in authorized lab environments.

Day 1-5: Subdomain & Recon Enumeration

1. `sublist3r -d example.com` → Subdomain enumeration
2. `amass enum -d example.com` → DNS enumeration
3. `assetfinder --subs-only example.com` → Find subdomains
4. `crt.sh/?q=%.example.com` → Certificate transparency search
5. `dig subdomain.example.com` → DNS lookup
6. `whois example.com` → Domain registration info
7. `nslookup example.com` → Resolve domain IP
8. `nmap -sL example.com` → List hosts
9. `host example.com` → Check IP/DNS records
10. `theHarvester -d example.com -b all` → Emails & subdomains
11. `amass enum -brute -d example.com` → Bruteforce subdomain discovery
12. `subfinder -d example.com` → Fast subdomain enumeration
13. `findomain -t example.com` → Cross-platform subdomain discovery
14. `dig axfr example.com @ns.example.com` → Zone transfer attempt (lab only)
15. `dnsrecon -d example.com -t std` → Standard DNS enumeration
16. `dnsenum example.com` → Multi-method DNS enumeration
17. `fierce -dns example.com` → Find domains and misconfigurations
18. `amass viz -d example.com` → Visualize network of subdomains
19. `crtsh-subdomain -d example.com` → Extract subdomains from SSL certs
20. `shodan host example.com` → Check open ports and services

Day 6-10: Port Scanning & Service Enumeration

1. `nmap -sS example.com` → TCP SYN scan
2. `nmap -sU example.com` → UDP scan
3. `nmap -p 80,443 -A example.com` → Aggressive scan
4. `nmap -p- -T4 example.com` → Scan all ports
5. `nmap --script=vuln example.com` → NSE vulnerability scan
6. `nmap -sV -p 80,443 example.com` → Service version detection
7. `nikto -h example.com` → Web server vulnerabilities
8. `whatweb example.com` → Detect web technologies
9. `wappalyzer-cli https://example.com` → Detect CMS/frameworks
10. `sslscan example.com:443` → SSL/TLS assessment

11. `testssl.sh example.com` → Check TLS security
12. `nmap --script http-enum example.com` → Web service enumeration
13. `nmap --script http-title example.com` → Fetch page titles
14. `nmap --script http-methods example.com` → List allowed methods
15. `nmap --script http-headers example.com` → Review security headers
16. `masscan -p0-65535 example.com` → Ultra-fast port scanning
17. `unicornscan -Iv example.com` → Asynchronous scanning
18. `hping3 -S example.com -p 80` → TCP SYN probe
19. `curl -I example.com` → HTTP header inspection
20. `curl -X OPTIONS example.com -i` → Allowed HTTP methods

Day 11-20: Directory & File Enumeration

1. `gobuster dir -u https://example.com -w /usr/share/wordlists/dirb/common.txt`
2. `dirb https://example.com /usr/share/wordlists/dirb/common.txt`
3. `wfuzz -c -w common.txt --hc 404 https://example.com/FUZZ`
4. `ffuf -u https://example.com/FUZZ -w /usr/share/wordlists/dirb/common.txt`
5. `burpsuite` → Intercept & analyze requests
6. `zap.sh` → OWASP ZAP proxy
7. `curl -I https://example.com/admin` → Check headers of admin endpoints
8. `wget -r -l1 -A .php,.html https://example.com` → Recursive file download
9. `gitrob github_username` → Discover sensitive repos
10. `gitleaks detect` → Scan for secrets
11. `commix -u "https://example.com/vuln?id=1"` → Command injection testing
12. `ffuf -u https://example.com/?page=FUZZ -w common.txt` → Parameter fuzzing
13. `dirsearch -u https://example.com -e php,html,txt` → Web directory scanner
14. `subjack -w subdomains.txt -t 100 -o takeover.txt` → Subdomain takeover check
15. `dnsmap example.com` → Subdomain mapping
16. `eyeWitness -f urls.txt` → Screenshot web endpoints
17. `aquatone-discover -d example.com` → Recon & screenshots
18. `aquatone-scan -d example.com` → HTTP/S scanning & screenshot
19. `hakrawler -url https://example.com` → Crawl for URLs and parameters
20. `nmap --script http-vhosts example.com` → Detect virtual hosts

Day 21-40: Input Testing & Vulnerabilities

1. `sqlmap -u "https://example.com/page?id=1" --batch` → SQL injection
2. `xsser -u "https://example.com/search?q=test"` → XSS testing
3. `csrfscan https://example.com` → CSRF detection
4. `burpsuite intruder` → Form fuzzing
5. `ffuf -u https://example.com/FUZZ -w payloads.txt` → Fuzzing for params
6. `wfuzz -c -w common.txt -d "param=FUZZ" https://example.com` → Parameter fuzzing
7. `nmap --script http-sql-injection -p 80,443 example.com`
8. `nikto -h https://example.com -Tuning 9`
9. `wpscan --url https://example.com --enumerate u` → WordPress users

10. `wpscan --url https://example.com --enumerate p` → WordPress plugins
11. `joomscan -u https://example.com` → Joomla scanner
12. `droopescan scan drupal -u https://example.com` → Drupal scanner
13. `nuclei -t cves/ -u https://example.com` → Vulnerability templates
14. `commix -u "https://example.com/vuln?id=1"` → Command injection
15. `dalfox url.txt` → XSS scanning automation
16. `gobuster vhost -u https://example.com -w vhosts.txt` → Virtual host discovery
17. `ffuf -u https://example.com/admin/FUZZ -w common.txt` → Admin panel fuzzing
18. `crlfuzz -u https://example.com` → CRLF injection testing
19. `paramspider -d example.com` → Discover GET/POST parameters
20. `jaeles scan -u https://example.com` → Advanced automated scanning

Day 41-60: Automation, Reporting & Misc

1. `nmap -p 80,443 --script http-security-headers example.com` → Check security headers
2. `subjack -w subdomains.txt -t 100 -o takeover.txt` → Check for takeovers
3. `amass intel -org "Target Org"` → Discover related domains
4. `dnsrecon -d example.com -a` → Active enumeration
5. `fierce -dns example.com` → DNS brute-force
6. `massdns -r resolvers.txt -t A -o S -w output.txt example.com` → Fast DNS resolver
7. `aquatone-discover -d example.com` → Discover & screenshot
8. `aquatone-scan -d example.com` → Scan for HTTP/S issues
9. `nmap --script vuln -p- example.com` → NSE vulnerability scan
10. `subfinder -d example.com -o subs.txt` → Export subdomains
11. `hakrawler -u https://example.com -d` → Spider web app
12. `ffuf -w common.txt -u https://example.com/FUZZ` → Fuzz directories
13. `theHarvester -d example.com -b linkedin` → Gather emails
14. `waybackurls example.com > urls.txt` → Old endpoints from Wayback Machine
15. `gau example.com` → Get URLs from public archives
16. `linkfinder -i urls.txt -o links.txt` → Discover JS endpoints
17. `unfurl domains -u urls.txt` → Extract domains from URLs
18. `nuclei -l urls.txt -t cves/` → Scan multiple URLs
19. `gobuster dir -u https://example.com -w /usr/share/wordlists/raft-large-directories.txt` → Large wordlist scan
20. `eyewitness -f urls.txt -d screenshots/` → Generate screenshots for reporting

Note: Only test targets you own or are explicitly authorized to assess. Unauthorized scanning or exploitation is illegal. Always follow responsible disclosure practices.