Ultimate Bug Bounty Mastery Guide (200+ Commands, 30-Day Roadmap)

This guide is a comprehensive resource for ethical bug bounty hunters, combining **200+ commands, tips, daily exercises, and ethical guidelines** for authorized testing environments.

Day 1-5: Reconnaissance & Subdomain Enumeration

Commands: 1. `sublist3r -d example.com` 2. `amass enum -d example.com` 3. `assetfinder --subs-only example.com` 4. `crt.sh/?q=%.example.com` 5. `dig subdomain.example.com` 6. `whois example.com` 7. `nslookup example.com` 8. `nmap -sL example.com` 9. `host example.com` 10. `theHarvester -d example.com -b all` 11. `amass enum -brute -d example.com` 12. `subfinder -d example.com` 13. `findomain -t example.com` 14. `dig axfr example.com @ns.example.com` 15. `dnsrecon -d example.com -t std` 16. `dnsenum example.com` 17. `fierce -dns example.com` 18. `amass viz -d example.com` 19. `crtsh-subdomain -d example.com` 20. `shodan host example.com`

Tips: - Combine multiple recon tools. - Use historical archives for forgotten endpoints. - Enumerate staging, dev, and admin subdomains.

Day 6-10: Port Scanning & Service Enumeration

Commands: 21. `nmap -sS example.com` 22. `nmap -sU example.com` 23. `nmap -p 80,443 -A example.com` 24. `nmap -p- -T4 example.com` 25. `nmap --script=vuln example.com` 26. `nmap -sV -p 80,443 example.com` 27. `nikto -h example.com` 28. `whatweb example.com` 29. `wappalyzer-cli https://example.com` 30. `sslscan example.com:443` 31. `testssl.sh example.com` 32. `nmap --script http-enum example.com` 33. `nmap --script http-title example.com` 34. `nmap --script http-methods example.com` 35. `nmap --script http-headers example.com` 36. `masscan -p0-65535 example.com` 37. `unicornscan -Iv example.com` 38. `hping3 -S example.com -p 80` 39. `curl -I example.com` 40. `curl -X OPTIONS example.com -i`

Day 11-20: Directory & File Enumeration

Commands: 41. `gobuster dir -u https://example.com -w /usr/share/wordlists/dirb/common.txt` 42. `dirb https://example.com /usr/share/wordlists/dirb/common.txt` 43. `wfuzz -c -w common.txt --hc 404 https://example.com/FUZZ` 44. `ffuf -u https://example.com/FUZZ -w /usr/share/wordlists/dirb/common.txt` 45. `burpsuite` 46. `zap.sh` 47. `curl -I https://example.com/admin` 48. `wget -r -l1 -A .php,.html https://example.com` 49. `gitrob github_username` 50. `gitleaks detect` 51. `commix -u "https://example.com/vuln?id=1"` 52. `ffuf -u https://example.com/?page=FUZZ -w common.txt` 53. `dirsearch -u `https://example.com -e php,html,txt` 54. `subjack -w subdomains.txt -t 100 -o takeover.txt` 55. `dnsmap example.com` 56. `eyeWitness -f urls.txt` 57. `aquatone-discover -d example.com` 58. `aquatone-scan -d example.com` 59. `hakrawler -url https://example.com` 60. `nmap --script http-vhosts example.com`

Day 21-40: Input Testing & Vulnerabilities

Commands: 61. `sqlmap -u "https://example.com/page?id=1" --batch` 62. `xsser -u "https://example.com/search?q=test"` 63. `csrfscan https://example.com` 64. `burpsuite intruder` 65. `ffuf -u https://example.com/FUZZ -w payloads.txt` 66. `wfuzz -c -w common.txt -d "param=FUZZ" https://example.com` 67. `nmap --script http-sql-injection -p 80,443 example.com` 68. `nikto -h https://example.com -Tuning 9` 69. `wpscan --url https://example.com --enumerate u` 70. `wpscan --url https://example.com --enumerate p` 71. `joomscan -u https://example.com` 72. `droopescan scan drupal -u https://example.com` 73. `nuclei -t cves/ -u https://example.com` 74. `commix -u "https://example.com/vuln?id=1"` 75. `dalfox url.txt` 76. `gobuster vhost -u https://example.com -w vhosts.txt` 77. `ffuf -u https://example.com/admin/FUZZ -w common.txt` 78. `crlfuzz -u https://example.com` 79. `paramspider -d example.com` 80. `jaeles scan -u https://example.com`

Day 41-60: Automation, Reporting & Misc

Commands: 81. `nmap -p 80,443 --script http-security-headers example.com` 82. `subjack -w subdomains.txt -t 100 -o takeover.txt` 83. `amass intel -org "Target Org"` 84. `dnsrecon -d example.com -a` 85. `fierce -dns example.com` 86. `massdns -r resolvers.txt -t A -o S -w output.txt example.com` 87. `aquatone-discover -d example.com` 88. `aquatone-scan -d example.com` 89. `nmap --script vuln -p- example.com` 90. `subfinder -d example.com -o subs.txt` 91. `hakrawler -u https://example.com -d` 92. `ffuf -w common.txt -u https://example.com/FUZZ` 93. `theHarvester -d example.com -b linkedin` 94. `waybackurls example.com > urls.txt` 95. `gau example.com` 96. `linkfinder -i urls.txt -o links.txt` 97. `unfurl domains -u urls.txt` 98. `nuclei -l urls.txt -t cves/` 99. `gobuster dir -u https://example.com -w /usr/share/wordlists/raft-large-directories.txt` 100. `eyewitness -f urls.txt -d screenshots/`

Day 61-200: Advanced Recon, API, Mobile, Exploitation, Logic Bugs, Automation

Commands: - 101–220: See previous messages with **advanced recon, API testing, SSRF, RCE, IDOR, LFI, business logic testing, payload automation, and reporting commands**

Tips & Best Practices: - Always stay within scope. - Prioritize sensitive endpoints and business-critical flows. - Document everything: payloads, steps, screenshots, and results. - Automate repetitive tasks with scripts or `ffuf`, `wfuzz`, `nuclei`, etc. - Stay updated with CVEs, Bugcrowd/HackerOne reports, and security blogs.

- Combine minor bugs for major impact. - Test responsibly: avoid destructive actions and protect sensitive data.

Ethical Guidelines: - Only test authorized targets. - Use VPN/proxies if allowed. - Follow program disclosure rules. - Never publicly share vulnerabilities before reporting.

This PDF is the **ultimate 200+ command Bug Bounty Mastery Guide** with a structured 30-day learning roadmap for reconnaissance, scanning, exploitation, and reporting in legal, ethical environments.