FULL BUG BOUNTY HUNTING

📘 Xsploit Hackademy — Bug Bounty Hunting (Full Module)

(Complete Training Material PDF)

Covers: Foundations → Recon → Vulnerabilities → Automation → Reporting → Tools → Commands → Real Examples

---

MODULE 1 — Introduction to Bug Bounty Hunting

1.1 What is Bug Bounty?

A **bug bounty** is a legally authorized security testing program where companies pay you for finding vulnerabilities in their websites, apps, APIs, and systems.

Companies like Google, Meta, Microsoft, Apple, and 10,000+ others run bounty programs.

Bug bounty is NOT hacking illegally — it's:

✔ Authorized

✔ Reward-based

✔ Research-focused

✔ Safe and legal

1.2 Types of Bug Bounty Programs

1. Private Programs

Invite-only (HackerOne, Bugcrowd).

2. Public Programs

Anyone can join.

3. VDP – Vulnerability Disclosure Programs

No bounty, but safe to report.

4. Self-hosted Programs

Run on company's own site.

1.3 Skill Requirements

To be successful:

- Web Application Pentesting
- OWASP Top 10
- API Testing
- Network Recon
- DNS & Subdomain Enumeration
- Burp Suite Mastery
- Automation (Bash + Python)

MODULE 2 — Methodology Framework (VERY IMPORTANT)

Every bug bounty hunter follows a **fixed workflow**:

1. **Scope Understanding**
2. **Reconnaissance**
3. **Enumeration**
4. **Vulnerability Discovery**
5. **Exploitation**
6. **Automation**
7. **Reporting**

If you follow this exactly → You win.

MODULE 3 — Reconnaissance (Deep + With Commands)

This is the MOST important stage (50% of success).

3.1 Subdomain Enumeration

Tools & Commands

① Subfinder

```
subfinder -d target.com -o subs.txt
```

What it does:

Passive subdomain enumeration using public sources → fast, reliable.

---

② Assetfinder

```
assetfinder --subs-only target.com >> subs.txt
```

What it does:

Grabs subdomains from APIs like crt.sh, bufferover, threatcrowd.

---

③ Amass (Active + Passive)

```
amass enum -d target.com -o amass.txt
```

What it does:

Deep crawling + DNS brute force + ASN lookup.

---

④ Shuffle DNS (Fast bruteforce)

```
shuffledns -d target.com -w wordlist.txt -r resolvers.txt -o bruteforce.txt
```

What it does:

Uses massive wordlists to discover *hidden* subdomains.

Combine all

```
cat subs.txt amass.txt bruteforce.txt | sort -u > final_subdomains.txt
```

3.2 Probing Subdomains

httprobe

```
cat final_subdomains.txt | httprobe > alive.txt
```

Finds alive/working domains.

httpx (best tool)

```
httpx -l final_subdomains.txt -o alive.txt -title -sc -ip -cl
```

Shows:

- Status codes
- Titles
- Content length
- IP
- Tech stack

3.3 DNS Recon

DNSX

```
dnsx -l alive.txt -resp -a -aaaa -cname -o dns_records.txt
```

3.4 Discovering Technologies

Wappalyzer CLI

```
wappalyzer -u https://site.com
```

whatweb

```
whatweb https://target.com
```

MODULE 4 — Directory Enumeration (Deep)

Tools

Gobuster

```
gobuster dir -u https://target.com -w wordlist.txt -o dirs.txt
```

Feroxbuster

```
feroxbuster -u https://target.com -w wordlist.txt -t 50 -o ferox.txt
```

Dirsearch

```
python3 dirsearch.py -u https://target.com -e php,asp,js
```

MODULE 5 — Parameter Discovery

Paramspider

```
python3 paramspider.py -d target.com --exclude woff,css,png
```

GF Patterns (for vulnerabilities)

```
gf sqli
gf xss
gf ssrf
gf redirect
```

MODULE 6 — Vulnerability Finding (Full OWASP Top 10)

But here we focus on **Bug Bounty Style**, NOT textbook style.

6.1 SQL Injection (Bug Bounty Approach)

Using Burp Suite

Step 1: Capture Request

Send to Repeater

Add `'` after each parameter

Step 2: Look for errors

Examples:

- MySQL: `You have an error in your SQL syntax`
- MSSQL: `Unclosed quotation mark`
- Oracle: `ORA-00933`

Step 3: Boolean tests

```
?id=1 AND 1=1
?id=1 AND 1=2
```

Step 4: Time-based

```
?id=1' AND SLEEP(5)--+
```

6.2 XSS (Client-side bug)

Payloads

```
"><script>alert(1)</script>
```

For filters:

```
<svg/onload=alert(1)>
```

6.3 IDOR / BOLA (Most profitable)

Test

Change:

```
/api/user/120/orders
```

to

```
/api/user/119/orders
```

If data returns → $$ jackpot.

6.4 SSRF (High payout)

Test URL params:

```
url=http://127.0.0.1:80
url=file:///etc/passwd
```

Use Burp Collaborator for callbacks.

6.5 CSRF

(Already covered in previous module)

MODULE 7 — API Bug Bounty (VERY IMPORTANT)

Tools:

- Postman
- Burp
- Insomnia
- Swagger Parser
- Kiterunner

API endpoints:

```
/api/v1/users
/api/v1/auth/login
```

```
/api/v1/admin
```

Test:

- Auth bypass
- Rate limiting
- Mass assignment
- IDOR
- Unvalidated input

MODULE 8 — Automation for Bug Bounty

Bash Recon Automation

```
#!/bin/bash
domain=$1

subfinder -d $domain -o subs.txt
httpx -l subs.txt -o live.txt
nuclei -l live.txt -t cves/ -o results.txt
```

Nuclei (Hacker’s Weapon)

```
nuclei -l live.txt -t nuclei-templates -o output.txt
```

Detects:

- Misconfigurations
- CVEs
- APIs
- Tokens

- Exposed panels

MODULE 9 — Reporting (VERY IMPORTANT FOR PAYOUT)

Structure

1. Title
2. Severity
3. Description
4. Steps to Reproduce
5. Impact
6. Evidence (Burp request/response)
7. Fix Recommendation

Perfect report example

Title: IDOR in `/api/v1/account/` allows viewing any user's private data

Impact: Exposure of PII

Severity: High

Proof:

`/api/account?id=102` → returns victim data

MODULE 10 — Earning Strategies (How to Get Paid)

1. Hunt private programs (higher rewards)

2. Use automation to cover large scope

3. Focus on easy high-paid bugs:

- IDOR
- CSRF

- Access control
- Server misconfig
- Authentication bypass

4. Don’t go for XSS only

5. Specialize in API bugs

6. Report quickly (race matters)

MODULE 11 — Top Tools List (Full)

Recon

- Subfinder
- Amass
- Assetfinder
- httpx
- Hakrawler
- Gau
- Paramspider

Testing

- Burp Suite
- Postman
- ffuf
- Nuclei
- Dalfox (XSS)

Exploitation

- SQLmap
- XSStrike

- Kiterunner
- Smuggler
- JWT Toolkit

Reporting

- Hacktivity feed
- Burp Logger
- Dradis
- Obsidian

MODULE 12 — Real Bug Bounty Examples (Educational)

(Use safe examples, not sensitive)

Example 1: IDOR

Found in booking system

Payout: $2,000

URL changed from

`/api/bookings/1120` → `/api/bookings/1100`

Example 2: XSS

Parameter reflected → stored

Payout: $500

Example 3: SSRF

URL parameter exposed AWS metadata

Payout: $5,000

✅ All Useful Websites for Bug Bounty Hunters (Complete List)

(Organized Category-wise)

🔵 1. Bug Bounty Platforms (Where You Hunt & Earn)

- **HackerOne** – https://hackerone.com
- **Bugcrowd** – https://bugcrowd.com
- **Intigriti** – https://intigriti.com
- **YesWeHack** – https://yeswehack.com
- **Synack** – https://synack.com (private)
- **Open Bug Bounty** – https://openbugbounty.org
- **Federacy** – https://federacy.com
- **Hacktrophy** – https://hacktrophy.com
- **SafeHats** – https://safehats.com
- **Detectify Crowdsource** – https://detectify.com
- **Zerocopter** – https://www.zerocopter.com/

🔵 2. Recon & Asset Discovery Websites

- **crt.sh** – https://crt.sh
- **Shodan** – https://shodan.io
- **Censys** – https://search.censys.io
- **ZoomEye** – https://zoomeye.org
- **BinaryEdge** – https://app.binaryedge.io
- **FullHunt** – https://fullhunt.io
- **Hunter.io** – https://hunter.io

- **SecurityTrails** – https://securitytrails.com
- **Netlas** – https://netlas.io
- **DNSDumpster** – https://dnsdumpster.com
- **LeakIX** – https://leakix.net

🔵 3. URL/JS/API Discovery

- **Wayback Machine** – https://web.archive.org
- **Waybackurls Viewer** – https://urlscan.io
- **URLScan.io** – https://urlscan.io
- **JSFinder Web** – https://jsfinder.net
- **Swagger UI / API Docs** (usually: `/api/docs` or `/swagger`)

🔵 4. Vulnerability Checking / Online Scanners

(use only for allowed scope)

- **Pentest-Tools** – https://pentest-tools.com
- **Detectify scanner** – https://detectify.com
- **Wappalyzer Online** – https://www.wappalyzer.com/lookup
- **VirusTotal URL Scanner** – https://www.virustotal.com
- **Jira Scan Tools** – https://jira.nessus.org

🔵 5. Subdomain Enumeration (Online)

- **Findsubdomains** – https://findsubdomains.com
- **Raccoon Security** – https://raccoon.onyxbits.de
- **HackerTarget Subnet Finder** – https://hackertarget.com
- **Dnsdumpster** – https://dnsdumpster.com

- **Pentest-Tools Subdomain Finder** – https://pentest-tools.com/subdomain-discovery

🔵 6. Website Fingerprinting / Tech Stack Identification

- **BuiltWith** – https://builtwith.com
- **Wappalyzer Web** – https://www.wappalyzer.com
- **WhatWeb Online** – https://whatweb.net/online

🔵 7. Payload & Cheat Sheet Resources

- **PayloadsAllTheThings** – https://github.com/swisskyrepo/PayloadsAllTheThings
- **HackTricks** – https://book.hacktricks.xyz
- **OWASP Cheat Sheets** – https://cheatsheetseries.owasp.org
- **Cheat.sh** – https://cheat.sh
- **XSS Cheat Sheet** – https://portswigger.net/web-security/cross-site-scripting/cheat-sheet

🔵 8. Wordlists (Dictionaries for Bruteforce)

- **SecLists** – https://github.com/danielmiessler/SecLists
- **Assetnote Wordlists** – https://wordlists.assetnote.io
- **Kaonashi** – https://github.com/duyetdev/kaonashi
- **Dirbuster Wordlists** – https://github.com/daviddias/node-dirbuster

🔵 9. Learning & Practice Platforms

- **PortSwigger Academy** – https://portswigger.net/web-security

- **TryHackMe** – https://tryhackme.com
- **HackTheBox** – https://hackthebox.com
- **VulnHub** – https://vulnhub.com
- **RootMe** – https://root-me.org
- **CyberSecLabs** – https://cyberseclabs.co.uk
- **PentesterLab** – https://pentesterlab.com
- **Hacker101** – https://www.hacker101.com

🔵 10. Practice vulnerable labs for bug bounty

- **DVWA** – https://github.com/digininja/DVWA
- **bWAPP** – http://www.itsecgames.com
- **WebGoat** – https://owasp.org/www-project-webgoat
- **OWASP Juice Shop** – https://owasp.org/www-project-juice-shop
- **Hackazon** – https://github.com/rapid7/hackazon

🔵 11. Code Search & Leak Hunting

- **GitHub Search** – https://github.com/search
- **GitLab Search** – https://gitlab.com/search
- **DeHashed** – https://dehashed.com
- **LeakCheck** – https://leakcheck.io
- **PublicWWW** – https://publicwww.com

🔵 12. Public Disclosure Databases (for inspiration)

- **HackerOne Hacktivity** – https://hackerone.com/hacktivity
- **Bugcrowd Warrior Dashboard** – https://bugcrowd.com/leaderboard

- **Intigriti Leaderboard** – https://app.intigriti.com
- **Exploit-DB** – https://exploit-db.com

🔵 13. CVE & Exploit Analysis Websites

- **NVD (National Vulnerability Database)** – https://nvd.nist.gov
- **MITRE CVE Search** – https://cve.mitre.org
- **CIRCL CVE** – https://cve.circl.lu
- **PacketStorm** – https://packetstormsecurity.com

🔵 14. Developer & API Documentation (useful for API hacking)

- **Swagger Editor** – https://editor.swagger.io
- **Postman API Network** – https://www.postman.com/explore
- **RapidAPI Hub** – https://rapidapi.com
- **ProgrammableWeb** – https://www.programmableweb.com

🔵 15. Tools that run in the browser

- **JWT.io** – https://jwt.io (Decode JWT tokens)
- **CyberChef** – https://gchq.github.io/CyberChef
- **Regex101** – https://regex101.com
- **JSON Formatter** – https://jsonformatter.org
- **Base64 Decode** – https://www.base64decode.org

🔵 16. Online Encoders / Decoders / Hashing

- **MD5 Hash Generator** – https://md5hashing.net

- **SHA256 Tools** – https://emn178.github.io/online-tools/sha256.html
- **URL Encoder** – https://www.urlencoder.io

🔵 17. HTTP Tools + Request Builders

- **ReqBin** – https://reqbin.com
- **Hoppscotch** – https://hoppscotch.io
- **Postman Web** – https://postman.com
- **Curl Converter** – https://curlconverter.com

🔵 18. Writeups + Research Sites

- **Medium Security Writeups** – https://medium.com/tag/bug-bounty
- **Reddit /r/bugbounty** – https://reddit.com/r/bugbounty
- **PentesterLand** – https://pentester.land
- **ProjectDiscovery Blog** – https://blog.projectdiscovery.io

🔵 19. CDN, IP & DNS Analysis

- **Cloudflare Radar** – https://radar.cloudflare.com
- **IPinfo** – https://ipinfo.io
- **Whois Lookup** – https://who.is

🔵 20. Browser Extensions (Web)

- **Wappalyzer extension**
- **Cookie Editor**
- **ModHeader**
- **FoxyProxy**
- **HackTools**