[BUGITRIX]

FROM ZERO TO BUG BOUNTY HUNTER IN 90 DAYS

The Honest Roadmap — 2026 Edition

■ Beginner Friendly

■ Free Tools Only

■ Week-by-Week Plan

PHASE 1
Days 1–30
Foundation
& Tools

›

PHASE 2
Days 31–60
Learn Vulns
& Recon

›

PHASE 3
Days 61–90
Hunt, Report
& Earn

VIRAL SCORE 9.3 / 10 ■

REALISTIC INCOME TIMELINE

Month 1	Month 2–3	Month 4–6	Month 6–12	Year 2+
$0	$0–$150	$100–$500	$500–$2K/mo	$2K–$10K+/mo
Learning phase — completely normal	First reports, expect duplicates	Consistent hunting & skill building	Part-time hunter momentum	Expert-level consistent earnings

PLATFORM COMPARISON

Platform	Programs	Beginner?	Min Payout	Max Payout
HackerOne	2,000+	🟩 Yes	$50	$10,000+
Bugcrowd	1,500+	🟩 Yes	$50	$15,000+
Intigriti	800+	🟨 Moderate	$100	$20,000+
YesWeHack	600+	🟩 Yes	$50	$10,000+
Synack	500+	🟥 Advanced	$200	$50,000+

PRO TIP:

For 2026, start with HackerOne or Bugcrowd. Filter for new programs with wildcard scope — fewer competitors, more surface area, and faster triage response times. Smaller programs = bigger beginner opportunities.

■ BUILD YOUR FOUNDATION ■

WEEK 1–2

Internet & Web Basics

- How HTTP/HTTPS works
- Request & response cycle
- HTML, JS & browser basics
- Cookies, sessions & tokens
- DNS, IP & networking 101
- Install Burp Suite Community
- Set up Kali Linux on VirtualBox

GOAL: Complete TryHackMe Pre-Security path

WEEK 3–4

Top Vulnerability Types

- XSS — Cross-Site Scripting
- IDOR — Insecure Direct Object Ref
- SQL Injection basics
- CSRF & Open Redirects
- Broken Authentication
- Subdomain Takeover
- Info Disclosure

GOAL: Finish XSS + IDOR labs on PortSwigger

■ FREE RESOURCE STACK (Zero Cost)

Resource	Type	Cost	Best For
PortSwigger Web Security Academy	Labs	**FREE**	Hands-on vuln practice — best on the internet
TryHackMe	CTF/Labs	**FREE**	Beginner-friendly structured paths
HackTheBox	CTF	**FREE***	Intermediate real-world challenges
Burp Suite Community	Tool	**FREE**	Intercepting & manipulating web traffic
Kali Linux	OS	**FREE**	Full hacking toolkit pre-installed
crt.sh + Shodan + Wayback	Recon	**FREE**	Subdomain discovery, exposure, old endpoints
HackerOne Hacktivity	Reports	**FREE**	Read real disclosed bug reports

■ RECON IS 80% OF THE HUNT

WEEK 5–6

Master Recon Techniques

- Enumerate subdomains (crt.sh, Sublist3r)
- Find live hosts with httpx
- Wayback Machine for old endpoints
- Google Dorks for exposed data
- Read JS files for API keys & endpoints
- Shodan for exposed servers
- theHarvester for emails & IPs
- Map ALL entry points before touching

GOAL: Full recon on one real program — no bugs yet

WEEK 7–8

Your First Real Hunt

- Pick a beginner-friendly program
- Filter: new programs, wildcard scope
- Focus on IDOR & XSS first
- Test ALL user input fields
- Change object IDs (IDOR check)
- Look for open redirects in params
- Check HTTP responses for leaks
- Submit your FIRST report!

GOAL: Submit at least 1 report (valid or not — practice!)

■ TOP VULNERABILITIES TO HUNT (Beginner Priority)

Vulnerability	Difficulty	Avg Bounty	Frequency	Start Here?
XSS (Cross-Site Scripting)	🟩🟩 Easy	$50–$1,000	Very Common	🟩 YES
IDOR (Insecure Direct Object Ref)	🟩🟩 Easy	$100–$5,000	Very Common	🟩 YES
Open Redirect	🟩 Easy	$50–$300	Very Common	🟩 YES
Info Disclosure	🟩 Easy	$50–$500	Very Common	🟩 YES
CSRF	🟩🟩 Easy	$50–$500	Common	🟩 YES
SQL Injection	🟨🟨🟨 Med	$200–$10K	Common	🟨 Learn first
SSRF	🟥🟥🟥🟥 Hard	$500–$20K	Moderate	🟥 Later

■ WRITE REPORTS THAT GET PAID

WEEK 9–10

Report Writing Mastery

- Title: short, clear, specific
- Severity: honest CVSS rating
- Steps to Reproduce: numbered
- Proof of Concept: screenshots/video
- Impact: business-level consequences
- Read 10 disclosed reports on H1
- Practice with 3+ full write-ups

GOAL: Write 3 polished reports with full PoC

WEEK 11–12

Build Momentum

- Keep a daily hunting journal
- Track: tested, found, outcome, lesson
- Join Bugitrix community forum
- Every duplicate = right direction
- Every N/A = severity lesson
- Every Informational = impact lesson
- Pick 2–3 programs for next 90 days

GOAL: Submit 5+ reports & join the community

■ REPORT QUALITY = PAYOUT QUALITY

Report Quality	Typical Outcome
Vague report, no PoC	Informational / N/A — no payout
Clear description but incomplete PoC	Low bounty or request for more information
Clear, reproducible, full impact statement	Full bounty paid at rated severity
Exceptional write-up + business impact	Bonus awarded or higher triage rating + reputation boost

■ THE 5 PARTS OF A WINNING REPORT

1. TITLE
Short, clear, describes vuln + impact

2. SEVERITY
Honest CVSS — don't overrate

3. STEPS
Numbered, reproducible, clear

4. PoC
Show actual impact with evidence

5. IMPACT
Business consequences in plain English

🟥 7 BEGINNER MISTAKES TO AVOID

1. **Test without reading scope**
   Read every word of the program policy. Out-of-scope testing = platform ban.
2. **Jump between too many targets**
   Go DEEP on one target per week. Breadth is for experts. Depth builds skills.
3. **Ignore JavaScript files**
   2026's highest-paying bugs hide in .js files — API keys, endpoints, logic flaws.
4. **Not using Burp Suite**
   Testing without intercepting traffic means missing 70% of what's happening.
5. **Overrating severity**
   Calling a low-impact XSS 'Critical' destroys your reputation with triage teams.
6. **Quitting after first duplicate**
   Everyone gets duplicates. Even top hunters. It means you found a REAL bug.
7. **Skipping recon phase**
   The bug is in endpoint #847. Without recon, you'll keep testing the same 5 places.

🟩 YOUR 90-DAY CHECKLIST

WEEKS 1–2: Foundation

- □ Finish TryHackMe Pre-Security path
- □ Understand HTTP request/response cycle
- □ Install Burp Suite & set up Firefox proxy
- □ Set up Kali Linux on VirtualBox

WEEKS 3–4: Vulnerability Knowledge

- □ Complete XSS labs on PortSwigger
- □ Complete IDOR labs on PortSwigger
- □ Complete SQL Injection intro on PortSwigger
- □ Explain each vulnerability without looking it up

WEEKS 5–6: Recon Skills

- □ Enumerate subdomains using crt.sh
- □ Run Wayback Machine recon on a real target
- □ Build personal recon methodology checklist

WEEKS 7–8: First Hunt

- □ Create accounts on HackerOne and Bugcrowd
- □ Pick a beginner-friendly program
- □ Submit at least 1 report

WEEKS 9–12: Reports & Momentum

- □ Write 3+ reports with full PoC
- □ Study 10 disclosed reports on H1 Hacktivity
- □ Keep a hunting journal for 30+ days
- □ Join Bugitrix community

[BUGITRIX]

bugitrix.com

Don't Hunt Alone.

Join the Community. Accelerate Fast.

The best hunters aren't solo wolves they're part of networks

🟩 MORE VALUABLE CONTENT

Guides, tutorials, career resources
for ethical hackers & security pros

bugitrix.com

🟦 DAILY CYBER TIPS

Breaking news, CVE alerts, hacking
tricks delivered to your phone

t.me/bugitrix

🟨 HACKER COMMUNITY

Connect with hunters, share write-ups,
get feedback & grow together

bugitrix.com/forum/help-1

🟪 1-ON-1 MENTORSHIP

Accelerate your progress with
guidance from expert practitioners

bugitrix.com/mentorship-details

🟥 BUILD YOUR CYBERSECURITY RESUME WITH US

We help you craft a resume that reflects real hacking skills — built to land security roles

bugitrix.com › Resume Builder Form

Your 90 days start TODAY. The tools are free. The knowledge is free.

The only question is: are you going to do the work? 🟩