

[< Go to the original](#)

How To Find Your 1st Bug For Bug Bounty Hunters (Step-by-Step Guide) — Guaranteed Result

Are you staring at HackerOne or Bugcrowd dashboards wondering when you'll finally find your first bug? 🙄



Vipul Sonule

Follow

 InfoSec Write-ups androidstudio ~3 min read ·
June 15, 2025 (Updated: June 15, 2025) · Free: No

I've been there. Refreshing scope pages. Watching recon tools run. Questioning my life choices. But let me tell you — **your first bug is closer than you think, if you follow a smart system.** 🎯

Let's go from *zero to your first report*. ✓

🔍 Step 1: Choose the Right Platform (and Program)

Don't randomly jump on massive companies like Google or PayPal. Start with **new or less noisy** programs. Why? Because:

- Less competition
- More scope flexibility
- Easier targets

👉 I recommend checking:

- [HackerOne New Programs](#)
- [Bugcrowd Low Hanging Fruit](#)
- [Intigriti Programs with Zero Reports](#)

💡 *Look for programs with:* ✓ Wildcard subdomains ✓ Low submission volume ✓ Known tech stack like WordPress, Laravel, etc.

🧠 Step 2: Understand the Scope and Rules

Before touching anything, **read the scope. Twice**. Most new hunters ignore this and waste hours testing things that are out-of-scope.

📄 Example scope:

- *.example.com (includes all subdomains) ✓
- mobile app APIs (only iOS) ✓

 Avoid:





- Third-party services (like Salesforce) unless explicitly in scope
- Denial of Service tests
- Automated scanning without permission

Step 3: Set Up Your Toolkit (Minimalist Edition)

You don't need 50 tools. You need the *right* tools.

 Here's a beginner-friendly setup:

Recon Tools:

- Subfinder 
- httpx 
- Nuclei 
- Waybackurls 

Manual Testing Tools:

- Burp Suite (Community Edition is fine) 
- Firefox with extensions like Wappalyzer and HackBar 

Step 4: Recon and Map the Target

Now it's time to **map** the attack surface.

1. Run Subfinder to find subdomains:

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

```
cat subs.txt | httpx -status-code -title -o live.txt
```

1. Run Nuclei for common misconfigurations:

- `nuclei -l live.txt -t cves/ -o results.txt`

1. Explore the site manually. Visit every link. Look at every form.

✓ *Look for things like:*

- Login/Signup pages
- Contact forms
- Upload fields
- Parameters in the URL (`?id=123`)
- Forgotten subdomains (`dev.example.com` , `test.example.com`)

💣 Step 5: Focus on Easy & Common Bugs

Don't chase fancy RCEs on day one. Start with:

- 🐛 XSS (Cross-site Scripting)
- 🐛 IDOR (Insecure Direct Object Reference)
- 🐛 Open Redirects
- 🐛 Subdomain Takeover
- 🐛 Sensitive Data in JS files

🔧 Example: Visit `dev.example.com` , check for `robots.txt` , open `main.js` , and find hardcoded credentials. 💣 *Boom*, report-worthy.

Great resources to learn:

- [Web Security Academy by PortSwigger](#)



Step 6: Report It Like a Pro

Found something?

Here's how to write a clear, reproducible report:

- **Title:** Clear and specific *"Stored XSS on blog.example.com via comment box"*
- **Summary:** Explain what the bug is and its impact
- **Steps to Reproduce:**

1. Go to `blog.example.com` 2. Click on "Add Comment" 3. Submit
`<script>alert(1)</script>` 4. Refresh the page - XSS fires

- **Proof of Concept (PoC):** Screenshots, Burp logs, or videos
- **Impact:** Explain *why it matters* to the business.



Want help? Use this free tool: <https://hacktivitywriter.com>



Bonus Tip: Play CTFs & Bug Bounty Labs

To sharpen your real-world bug hunting skills, practice here:

- [TryHackMe Bug Bounty Path](#)
- [PortSwigger Labs](#)
- [HackerOne CTF](#)



Success Stories from Beginners

marketing subdomain of a big company.

And you can too.

Final Thoughts: Don't Give Up

Finding your first bug is **not about luck**, it's about:

✓ Being consistent ✓ Staying curious ✓ Testing smart, not hard

You might spend 10 days and find nothing. Then on day 11, you'll spot that forgotten endpoint or misconfigured subdomain and BAM — you're a bug bounty hunter with a payout. 💰

Let's Connect

Follow me for more:

- [Medium](#)
- [LinkedIn](#) 

 Drop your questions or thoughts in the comments! I love nerdy discussions. 

 **Thanks for reading!**

#hacking #bug-bounty #programming #technology #cybersecurity