

Forum:[Hack Forums](#)

Thread: [How to Start Bug Hunting and Get Paid to Hack Websites](#)

Chorozon - March 10, 2025, 7:02 am

What's Bug Hunting, Anyway?

Bug hunting, also known as ethical hacking, is the practice of finding vulnerabilities, or “bugs,” in websites, apps, or online systems. When you find a vulnerability, you report it to the company, and if they verify it, they'll reward you with a bounty.

These bounties can vary widely depending on the severity of the bug. For example, a simple cross-site scripting (XSS) vulnerability might earn you a couple hundred bucks, but a critical authentication bypass could net you thousands of dollars. It's a really cool way to make money while learning about cybersecurity and helping companies fix security issues before they get exploited by malicious hackers.

How Bug Bounty Programs Work

Companies run bug bounty programs on platforms like HackerOne, Bugcrowd, and others. These platforms host a variety of programs where you, as a security researcher or hacker, can test a company's website or app for vulnerabilities.

Each program typically has:

- A scope: What parts of the website or app you're allowed to test (e.g., you can test for XSS on certain pages but not the admin panel).

- A reward structure: The platform details how much you'll be paid based on the severity of the bug (e.g., \$500 for a medium-level bug, \$2,000 for a critical one).

- A disclosure policy: Once you report the bug, the company may take time to fix it. In the meantime, you should never publicly disclose the vulnerability until it's been addressed to avoid putting users at risk.

You submit your findings, and if the company agrees that the bug is valid, they'll pay you. It's that simple!

Finding Bug Bounties to Start With

Okay, so how do you actually find bounties to hunt? Where do you start? Here's a step-by-step process to help you discover the best bug bounty programs to focus on as a beginner.

1. Sign Up for Bug Bounty Platforms

The first step to getting started is to sign up for bug bounty platforms. These platforms host a variety of bug bounty programs from different companies, and they're the easiest place to find bounties to start working on.

Some of the most popular platforms are:

- HackerOne: One of the biggest platforms with hundreds of active programs from major companies.

- Bugcrowd: Another large platform with a mix of public and private programs. It's great for beginners because it offers a lot of resources and training.

Synack: Synack has a private bug bounty program, so you'll need to get invited to participate. However, it's known for its lucrative rewards.

Cobalt: A platform that offers private bug bounty programs, with a focus on high-quality researchers.

Open Bug Bounty: A community-driven platform with an open-source approach.

Once you've signed up, you'll have access to a dashboard where you can browse available programs. Some platforms also have a "new researcher" section to guide you through your first bounty!

2. Look for Programs You're Interested In

Once you're on a platform, take some time to browse through the available programs. Many platforms categorize programs by the type of system or website you'll be testing. Some categories might include:

- Web applications
- Mobile apps
- IoT (Internet of Things) devices
- Infrastructure testing

You'll want to focus on web application security in the beginning because it's the most accessible and beginner-friendly area. Web apps often have common vulnerabilities like SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF), which are perfect for newer bug hunters to look for.

Check out the program scope to see which areas of the website you're allowed to test. Some programs will explicitly mention that you can test for things like SQLi, XSS, and CSRF. Others might limit you to specific functionality or pages (e.g., you might not be able to test login pages or payment sections).

3. Start with Low-Hanging Fruit Programs

Some programs are specifically designed to help new researchers get started. These programs often have lower-level vulnerabilities but are still rewarding to find. These types of programs tend to have a lot of documentation to help beginners understand the types of bugs they should be looking for.

On platforms like HackerOne, look for programs labeled as "beginner-friendly" or "low-risk." These are ideal for your first bounty hunting experience.

4. Use the Bug Bounty Platform's Resources

Many platforms offer training and resources to help you get started. For example:

HackerOne offers a Hacker101 course, which is perfect for beginners and teaches you how to find common vulnerabilities.

Bugcrowd has a Bugcrowd University, which provides a range of tutorials and walkthroughs.

OWASP (the Open Web Application Security Project) has amazing resources for understanding common vulnerabilities.

These resources will help you get familiar with the kinds of bugs you should be hunting for and how to submit them properly.

5. Join Bug Hunting Communities

One of the best ways to accelerate your bug hunting journey is by joining bug hunting communities. There are a ton of online forums, Discord channels, and Reddit communities where ethical hackers share tips, tools, and resources. These are great places to ask questions, discuss bugs you've found, and get feedback from more experienced hunters.

Some great communities to check out:

- Reddit's /r/bugbounty
- Bugcrowd's community forum
- HackerOne's community forum
- Discord servers (many platforms have their own servers dedicated to bug bounty hunting)

You'll learn from others, and sometimes, more experienced hackers can point you in the direction of easy-to-find bugs!

Tools You'll Need to Start Bug Hunting

While you don't need to be a cybersecurity expert to get started, you'll want to use the right tools to help you find vulnerabilities faster and more efficiently. Here are some beginner-friendly tools to start with:

Burp Suite: This tool is the gold standard for web application security testing. The free version is packed with useful features like an intercepting proxy, scanner, and more.

OWASP ZAP: A great free alternative to Burp Suite, it's open-source and designed for beginners to test for common vulnerabilities.

XSSStrike: Perfect for testing and exploiting XSS vulnerabilities. It's beginner-friendly and super powerful once you get the hang of it.

Nikto: A great scanner for quickly checking a web server for vulnerabilities like outdated software, misconfigurations, and more.

Gobuster: A handy tool for finding hidden directories and subdomains on a website. Sometimes, a simple scan like this can uncover a goldmine of bugs.

Submitting Your Findings

Once you find a vulnerability, you'll need to report it to the company through the platform you're using. Make sure your report is clear, well-documented, and includes steps to reproduce the bug. The more details you provide, the easier it is for the company to verify the issue and get it fixed.

If they confirm that the bug is valid, they'll pay you the bounty. Keep in mind that the payouts can range from small amounts for low-severity bugs to thousands of dollars for critical vulnerabilities.

Why Bug Hunting is a good hobby

Learn and Earn: Bug hunting is one of the best ways to learn about cybersecurity while getting paid. As you find more bugs, you'll improve your skills and knowledge.

Flexibility: You can work on your own time. There's no boss, no deadlines—just you, the bugs, and your curiosity.

Big Money: Some hackers make a lot of money. If you get good at finding high-severity bugs, you could end up earning thousands of dollars in bounties. Plus, there are top-tier hackers making six figures a year just from bug bounties.

HerrWinston - May 9, 2025, 1:34 am

Very interesting, although until i am able to start bug hunting i gotta understand what types there are, keeping this in mind tho thanks for uploading