**INTRO TO BUG HUNTING**

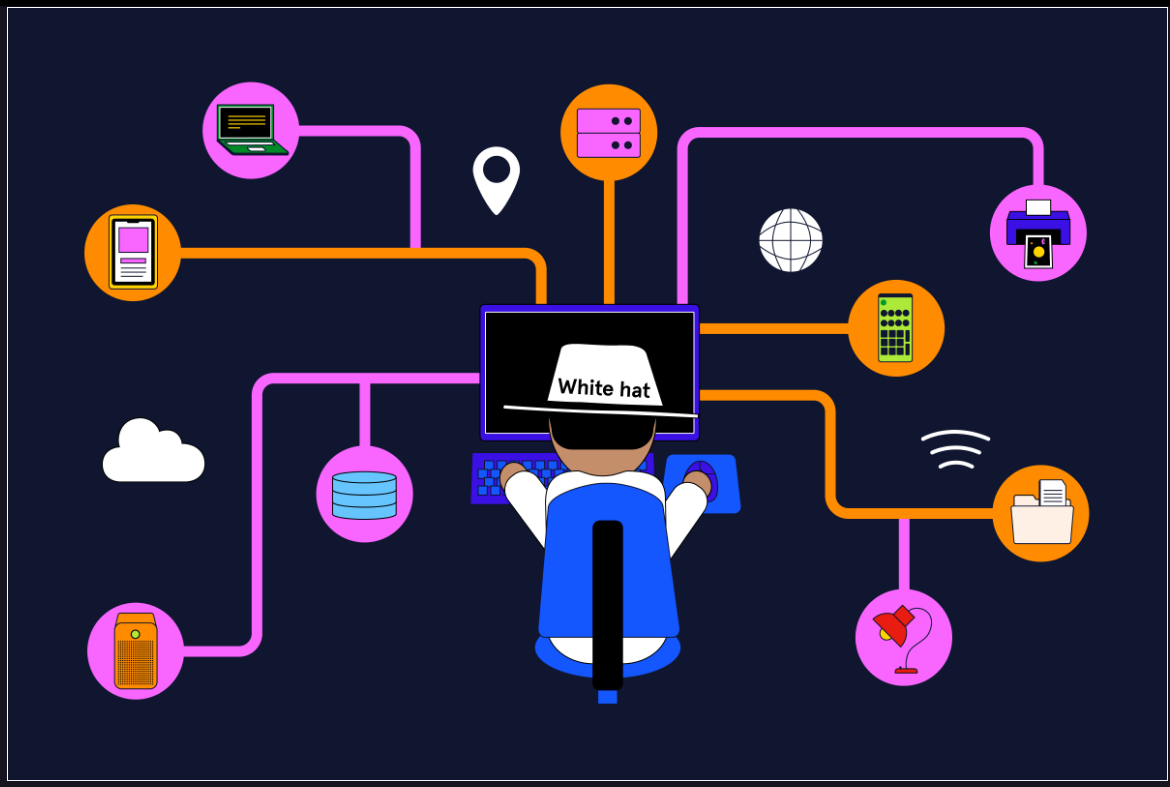
**Introduction**

Have you ever thought about a career in bug hunting?

Not hunting for little critters that roam outside your home or inside but hunting for software bugs, errors in the code, found in an application or service. Hackers that search, find, and report or eliminate bugs within an application or service are called bug hunters. The process of searching, identifying, and eliminating bugs in a system is bug hunting.

As an ethical hacker, one of your tasks is to search for and eliminate bugs in a system. Applications or services that have bugs are prone to vulnerabilities and since malicious actors can use vulnerabilities to gain access to a system, ethical hackers must act quickly to remove the bugs once identified.

In this lesson, you will learn and practice bug hunting. You will learn about the [hacking](https://www.codecademy.com/resources/docs/cybersecurity/hacking) process, ethical hacking tactics, and, lastly, how to be an effective bug hunter and ethical hacker. That said, let’s begin!



**The Hacking Process**

Before we go hunting, let’s learn about the [hacking](https://www.codecademy.com/resources/docs/cybersecurity/hacking) process. The hacking process is a combination of ethical hacking tactics for organizational defense. Having a list of tactics to ensure organizational defenses is a helpful resource for ethical hackers and bug hunters. Ethical hackers can use these tactics to ensure the security of a system and identify potential areas of vulnerabilities and software bugs.

The hacking process consists of the following:

* Footprinting
* Scanning
* Enumeration
* System Hacking
* Escalation of Privilege
* Planting Backdoors
* Covering Tracks

1. *Footprinting*, also known as the “Reconnaissance” phase, is passive information gathering of targets before active attack activities.
2. *Scanning* is an initial active/passive inspecting technique to gather technical information on target systems.
3. *Enumeration* is the consolidation and gathering of more detailed information on target systems and networks.
4. *System Hacking* is the planning and execution of attacks conducted based on the information gathered in Footprinting, Scanning, and Enumeration.
5. *Escalation of Privilege* is when an attacker is successful and can gain access to the systems/networks of the organization.
6. *Planting Backdoors* is leaving an entry point to a compromised system for easy access to further attack activities.
7. *Covering Tracks* is the act of removing or destroying signs of intrusion and activities performed on a system.

