Search Skills

Learn to efficiently search the Internet and use specialized search engines and technical docs.

Search Engines
Google
Bing
DuckDuckGo

"exact phrase": Double quotes indicate that you are looking for pages with the exact word or phrase

site:: This operator lets you specify the domain name to which you want to limit your search.

-: The minus sign allows you to omit search results that contain a particular word or phrase. For example, you might be interested in learning about the pyramids, but you don't want to view tourism websites; one approach is to search for or .pyramids -tourism-tourism pyramids

filetype:: This search operator is indispensable for finding files instead of web pages. Some of the file types you can search for using Google are Portable Document Format (PDF), Microsoft Word Document (DOC), Microsoft Excel Spreadsheet (XLS), and Microsoft PowerPoint Presentation (PPT)

Shodan
a search engine for devices connected to the Internet. It allows you to search for specific types and versions of servers, networking equipment, industrial control systems, and IoT devices.

Censys

At first glance, Censys appears similar to Shodan. However, Shodan focuses on Internet-connected devices and systems, such as servers, routers, webcams, and IoT devices. Censys, on the other hand, focuses on Internet-connected hosts, websites, certificates, and other Internet assets. Some of its use cases include enumerating domains in use, auditing open ports and services, and discovering rogue assets within a network

VirusTotal
VirusTotal is an online website that provides a virus-scanning service for files using multiple antivirus engines. It allows users to upload files or provide URLs to scan them against numerous antivirus engines and website scanners in a single operation. They can even input file hashes to check the results of previously uploaded files.

Have I Been Pwned
Have I Been Pwned (HIBP) does one thing; it tells you if an email address has appeared in a leaked data breach. Finding one's email within leaked data indicates leaked private information and, more importantly, passwords. Many users use the same password across multiple platforms, if one platform is breached, their password on other platforms is also exposed. Indeed, passwords are usually stored in encrypted format; however, many passwords are not that complex and can be recovered using a variety of attacks.

CVE
We can think of the Common Vulnerabilities and Exposures (CVE) program as a dictionary of vulnerabilities. It provides a standardized identifier for vulnerabilities and

security issues in software and hardware products

Exploit Database
There are many reasons why you would want to exploit a vulnerable application; one would be assessing a company's security as part of its red team. Needless to say, we should not try to exploit a vulnerable system unless we are given permission, usually via a legally binding agreement.

GitHub

a web-based platform for software development, can contain many tools related to CVEs, along with proof-of-concept (PoC) and exploit codes. To demonstrate this idea, check the screenshot below of search results on GitHub that are related to the Heartbleed vulnerability.