Shodan:

A search engine for IoT and Internet connected devices

Shodan is a search engine that specializes in indexing Internet-connected devices and systems. Unlike traditional search engines that index web pages, Shodan searches for devices connected to the Internet, such as servers, routers, webcams, industrial control systems, and other Internet of Things (IoT) devices.

Search parameters

Shodan uses search parameters to help you narrow down your search, the following sections will offer some of the most useful parameters.

General Query Terms

city:”[city name]”	Devices in a specific city.
org:”[organization name]”	Devices related to a certain organization.
country:”[country]”	Devices in a specified country.
region:”[region]”	Devices in a specific region.
postal:”[postal code]”	Devices in a specific postal code.
latitude:”[latitude]” longitude:”[longitude]”	Devices at specific coordinates.
os:”[operating system]”	Devices running a specific OS.
net:”[IP range]”	Devices within a certain IP range.
port:”[port number]”	Devices open on a specific port.

IoT Search Terms

“smart tv”	Searches for internet-connected smart TVs.
“IP camera” “default login”	IP cameras with default login credentials.

These are general terms that are suggested ways to target certain types of devices and should be used with other modifiers to narrow down the information.

Applications and Services

product:”[product name]”	Devices running a specific product.
version:”[version]”	Devices with a specific version number.
“X-Powered-By: PHP/[version]”	PHP version-specific servers.
“server: Apache”	Finds Apache web servers.
iis:[version number]	Servers running Microsoft IIS.
“server: nginx”	Devices running Nginx server.

Security and Vulnerability Terms

“Cisco IOS” “http auth”	Cisco IOS devices with HTTP authentication.
“default login” “router”	Routers with default login credentials.
vuln:”[CVE-ID]”	Searches for vulnerabilities with a specific CVE ID.
“Server: Apache” -“mod_ssl” -“OpenSSL”	Apache servers potentially without SSL encryption.
“heartbleed” vuln	Searches for vulnerabilities related to Heartbleed.
“EternalBlue” vuln	Devices vulnerable to EternalBlue.

These are general terms that are suggested ways to target certain types of services and should be used with other modifiers to narrow down the information.