Shodan Cheat Sheet

by sir_slammington via cheatography.com/147122/cs/31955/

Common General Search Filters

ip:	Filter results by specific IP address.
asn:	Filter results by specific ASN ID.
hostname:	Filter results by specific hostname.
port:	Filter results by specific port number of service.
net:	Filter results from specified CIDR block.
isp:	Filter results by devices assigned a particular address (space) from a specified ISP.
city:	Filter results by specific city.
country:	Filter results by specific two-digit country code.
os:	Filter results by particular OS.
product:	Filter results by particular software.
version:	Filter results by specified version of software.

Common Premium API Search Filters

vuln:	Filter results by particular vulnerability ID (commonly CVE).
tag:	Filter results by tags on device.

HTTP Filters

http.component:	Filter results by a particular web technology.
http.status:	Filter results by specific status code.
http.html:	Filter results by strings found in HTML of files served.
http.title:	Filter results by string found in title of web pages served.

Common CLI Commands

count	Returns the number of results for a search.
domain	View all available information for a domain.
download	Download search results and save them in a compressed JSON file.
honeyscore	Check whether the IP is a honeypot or not.
host	View all available information for an IP address.
parse	Extract information out of compressed JSON files.
scan	Scan an IP/ netblock using Shodan.
search	Search the Shodan database.

Common CLI Search Fields

ip_str

port

org

hostnames

os

country

city

These will display their values upon a search, but won't provide statistics.

Common CLI Stats Facets

asn

city

country

cloud.provider

cloud.service

device

domain

ip

org

os

Common CLI Stats Facets (cont)

version

These will return statistical information about a given series of devices found on the public facing Internet. For example, it could be used to return the most common version found among devices running MariaDB in a particular ASN.

Use Case Examples

host: 8.8.8.8	**shodan host 8.8.8.8**	Display information about a Google's public DNS.
asn:15169 product:mysql	**shodan stats asn:15169 product:mysql**	Show information about devices within Google's ASN that run MySQL.
microsoft iis 6.0	**shodan search --fields ip_str,port,org,hostnames microsoft iis 6.0**	Detect IIS servers running on 6.0.
Navigate to https://honeyscore.shodan.io/ and enter target IP.	**shodan honeyscore [TARGET]**	Detect if given target is a honeypot or not.

Column one is the search you would perform in the Web UI. Column two is the search you would perform using the CLI utility, and the third column is an explanation of the search.

By **sir_slammington**
cheatography.com/sir-slammington/

Published 2nd May, 2022.
Last updated 2nd May, 2022.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com