Cheatography

Shodan.io Cheat Sheet

by j.johnson138 via cheatography.com/147102/cs/31937/

Common Commands

search	Searches Shodan and outputs results in a terminal-friendly manner
count	Returns the number of results for a search query
stats	Shows statistics using specified facets through a search query
version	Outputs the version of Shodan that is installed
host [ip]	Shows more information about the given host
myip	Shows your own IP address
download*	Downloads the results in JSON format
parse	Allows you to parse a JSON download
domain	Shows more information about the domain

*Only downloads the first 1000 results by default.

Common Flags

--limit	Limits the number of results
--fields	Comma-separated list of desired fields
--separator	Specifies the separator between fields
--facets	Used with **stats** command; comma-separated list of facets

Common Search Fields

ip_str	The IP address of the banner
asn	The ASN or "block" of IP addresses the banner belongs to
net	Specifies the network the banner belongs to
port	The port number of the banner
org	The organization logged in the banner
hostname	Hostname for the banner
os	The operating system
country	The country of the banner
city	The city of the banner

Common Facets

port	Sorts results by port number
org	Sorts results by organization
city	Sorts results by city
country	Sorts results by country
ip	Sorts results by IP address

Common Facets (cont)

domain	Sorts results by domain name
os	Sorts results by OS
state	Sorts results by state

Example Commands

shodan search --fields ip_str,port,org,hostnames microsoft iis 6.0	Displays results with the given columns for "microsoft iis 6.0"
shodan host 144.756.3-24.535	Displays information about the host
shodan count microsoft iis 6.0	Outputs the number of results
shodan download Data microsoft iis 6.0	Downloads results to a JSON file named "Data"
shodan parse --fields ip_str,port,org --separator , Data.json.gz	Analyzes the JSON file and outputs the columns with a comma as the separator
domain google.com	Shows information about the domain
shodan search --limit 100 hostname:my_computer	Searches for endpoints with the hostname "my_computer" and restricts to 100 results
shodan stats --facets port net:198.20/16	Searches for devices on the network and sorts results by port number

Common Shodan.io Website Search Filters

ip
asn
country
hostname
port
os
version
tag*
vuln*

Without any filters, Shodan.io only searches the *data* portion of a banner.

*requires premium Shodan subscription

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com