

INFORMATION GATHERING



TOOLS



CODELIVELY
LEARN CYBERSECURITY

GOOGLE HACKING DATABASE



The screenshot shows the 'Exploit Database' logo in the top left corner. The main heading is 'Google Hacking Database'. Below the heading is a 'Show' dropdown menu set to '15'. The table has two columns: 'Date Added' and 'Dork'. The table contains 15 rows of data, each with a date and a corresponding Google Dork query.

Date Added	Dork
2023-11-30	<code>inurl:typo3/index.php</code>
2023-11-30	<code>Submission of New Google Dork</code>
2023-11-30	<code>site:.edu intext:"robotics" inurl:/research</code>
2023-11-30	<code>site:*.edu.* filetype:template</code>
2023-11-30	<code>inurl:*.install.appcenter.ms/orgs/*</code>
2023-11-30	<code>site:*.ac.* filetype:template</code>
2023-11-29	<code>filetype:log intext:"Account Number"</code>
2023-11-27	<code>intitle:"WAMPSEVER Homepage"</code>
2023-11-27	<code>intext:"index of" "pins" site:*.com</code>
2023-11-27	<code>intitle:index.of /logs.txt</code>
2023-11-27	<code>inurl: /adminer.php</code>
2023-11-27	<code>site:*.com */admin.txt</code>
2023-11-24	<code>site:s3.amazonaws.com "index of /"</code>



CODELIVELY
LEARN CYBERSECURITY

SHODAN.IO

Shodan

Maps

Images

Monitor

Developer

More...

 SHODAN

Explore

Downloads

Pricing 



TOTAL RESULTS

307,417

TOP COUNTRIES



United States	305,406
Venezuela, Bolivarian Republic of	799
Mexico	493
Colombia	490
Costa Rica	226

More...

 View Report

 Browse Images

 View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out [everything](#)

103.224.182.253 

buyseo.shop
tripacvisor.com
cablemd.com
newzealandair.com
samsungappstore.com
[Trellian Pty. Limited](#)
 United States, San Diego

 **SSL Certificate**

Issued By:
[- Common Name:
R3

[- Organization:
Let's Encrypt

Issued To:
[- Common Name:
buyhostbd.xyz

Supported SSL Versions:
TLSv1.2, TLSv1.3

HTTP/1.1 302 Found
date: Thu, 30 Nov 2023 11:32:20 GMT
server: Apache
set-cookie: __tad=1701343940.6014026; expires=
location: http://ww16.4tivo.com/?sub1=20231130
content-length: 2
content-type: text/html; charset=...

64.87.23.194

64-87-23-194.ephost.com
[EPhost](#)
 United States, San Diego

9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.14
Resolver name: ep164.ephost.com

TOP PORTS

CODELIVLY
LEARN CYBERSECURITY

NETCRAFT

[Platform](#) ▾[Solutions](#) ▾[Why Netcraft](#)[Resources](#) ▾[Company](#) ▾[BOOK A DEMO](#)[Tools](#)

Research Tools

Use our tools to find out what infrastructure and technologies any site is using, which sites are the most popular, and how to stay safe on the internet.

Internet Research Tools



Site Report

Using results from our internet data mining, find out the technologies and infrastructure of any site.



Search DNS

Explore hostnames visited by users of the [Netcraft extensions](#). Search by domain or keyword.



Most Popular Sites

Find out which sites are most visited globally or for any country, as determined by users of the [Netcraft](#)



CODELIVELY
LEARN CYBERSECURITY

THE HARVESTER

```
(root@kali)-[~]
└─$ theHarvester -h
*****
* theHarvester
*
* theHarvester 4.4.4
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-s START] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

options:
  -h, --help                show this help message and exit
  -d DOMAIN, --domain DOMAIN
                           Company name or domain to search.
  -l LIMIT, --limit LIMIT
                           Limit the number of search results, default=500.
  -s START, --start START
                           Start with result number X, default=0.
  -p, --proxies              Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan              Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                           Take screenshots of resolved domains specify output directory: --screenshot output_directory
  -v, --virtual-host         Verify host name via DNS resolution and search for virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                           DNS server to use for lookup.
  -t, --take-over           Check for takeovers.
  -r [DNS_RESOLVE], --dns-resolve [DNS_RESOLVE]
                           Perform DNS resolution on subdomains with a resolver list or passed in resolvers, default False.
  -n, --dns-lookup          Enable DNS server lookup, default False.
  -c, --dns-brute           Perform a DNS brute force on the domain.
  -f FILENAME, --filename FILENAME
                           Save the results to an XML and JSON file.
  -b SOURCE, --source SOURCE
                           anubis, baidu, bevigil, binaryedge, Bing, BingAPI, bufferoverrun, brave, censys, certspotter, criminalip, crtsh, dnsdumpster, duckduck
                           onyphe, otx, pentesttools, projectdiscovery, rapiddns, rocketreach, securityTrails, sitedossier, subdomaincenter, subdomainfinderC99,
```



CODELIVLY
LEARN CYBERSECURITY

SHERLOCK

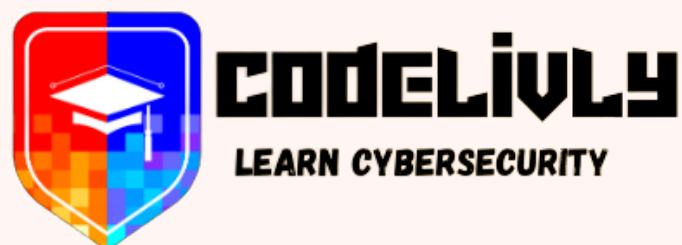
```
(root@kali)-[~]  
# sherlock venkatesh  
[*] Checking username venkatesh on:  
  
[+] 7Cups: https://www.7cups.com/@venkatesh  
[+] 8tracks: https://8tracks.com/venkatesh  
[+] 9GAG: https://www.9gag.com/u/venkatesh  
[+] About.me: https://about.me/venkatesh  
[+] Academia.edu: https://independent.academia.edu/venkatesh  
[+] Airlines: https://www.airliners.net/user/venkatesh/profile/photos  
[+] AllMyLinks: https://allmylinks.com/venkatesh  
[+] Amino: https://aminoapps.com/u/venkatesh  
[+] Anilist: https://anilist.co/user/venkatesh/  
[+] Apple Developer: https://developer.apple.com/forums/profile/venkatesh  
[+] Apple Discussions: https://discussions.apple.com/profile/venkatesh  
[+] Archive.org: https://archive.org/details/@venkatesh  
[+] Asciinema: https://asciinema.org/~venkatesh  
[+] AskFM: https://ask.fm/venkatesh  
[+] Audiojungle: https://audiojungle.net/user/venkatesh
```

workspaces



CODELIVELY
LEARN CYBERSECURITY

RECON-NG

[illegible]

RECON-DOG

```
(kali㉿kali)-[~/Tools/ReconDog]  
$ ./dog
```

```
ReconDog v2.0
```

1. Censys
2. NS lookup
3. Port scan
4. Detect CMS
5. Whois lookup
6. Detect honeypot
7. Find subdomains
8. Reverse IP lookup
9. Detect technologies
0. All

```
>> █
```



CODELIVELY
LEARN CYBERSECURITY

SUBLIST3R

```
(kali㉿kali)-[~/Tools/Sublist3r]
$ python sublist3r.py -d example.com

workspaces

Sublist3r

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for example.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
^X@sS[-] Total Unique Subdomains Found: 7
AS207960 Test Intermediate - example.com
www.example.com
dev.example.com
m.example.com
products.example.com
support.example.com
m.testexample.com
```



CODELIVELY
LEARN CYBERSECURITY