

## Lab Instructions

### Step 0: What is Shodan?

What is Shodan?

Shodan is a search engine specializing in scanning the internet for connected devices all around the world, and providing a centralized location for publicly available information about these devices. Connected devices range from routers and servers such as:

Home security cameras

IoT (Internet of Things) such as home devices, intelligent refrigerators and smart door locks

Medical devices such as internet-connected heart monitors

Complex industrial IoT devices (which can include technology for supply chain and logistics processes, remote asset tracking, drone-based delivery and transportation devices)

How does Shodan work?

Shodan will search the internet for information using a crawler (please see the linked Authenticat8 article for how this crawler works). The crawler will regularly be scanning and updating the Shodan database with up-to-date information that it finds (the crawlers work daily to collect data from around the world in different countries). If a device is directly hooked up to the Internet then Shodan will be able to gather all sorts of valuable data about it.

The data is taken from the device's banners. Banners contain metadata about the services, the device's operating system and ports that are running on the individual device. Banner grabbing is the process of getting this information from the port scan.

Here are two examples of different banners:

220 [kcg.cz](http://kcg.cz) FTP server (Version 6.00LS) ready.

An FTP banner, from [Shodan.io](http://Shodan.io)

HTTP/1.0 200 OK

Date: Tue, 16 Feb 2010 10:03:04 GMT

Server: Apache/1.3.26 (Unix) AuthMySQL/2.20 PHP/4.1.2 mod\_gzip/1.3.19.1a  
mod\_ssl/2.8.9 OpenSSL/0.9.6g

Last-Modified: Wed, 01 Jul 1998 08:51:04 GMT

ETag: "135074-61-3599f878"

Accept-Ranges: bytes  
Content-Length: 97  
Content-Type: text/html  
An HTTP banner, from [Shodan.io](https://shodan.io)

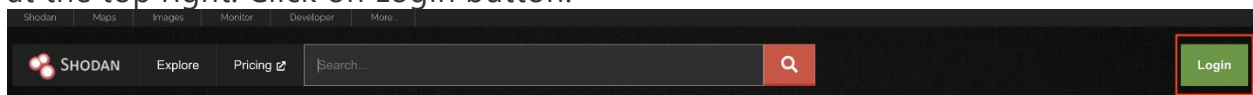
In the banner above, we are able to see that the device is running an Apache web server, along with the specific version of it (version 1.3.26). This might give further clues about vulnerabilities that can be exposed, as well as ways to find default login credentials and passwords for the devices and/or ways to access administrator consoles.

Other types of information that you might see in a banner could be:

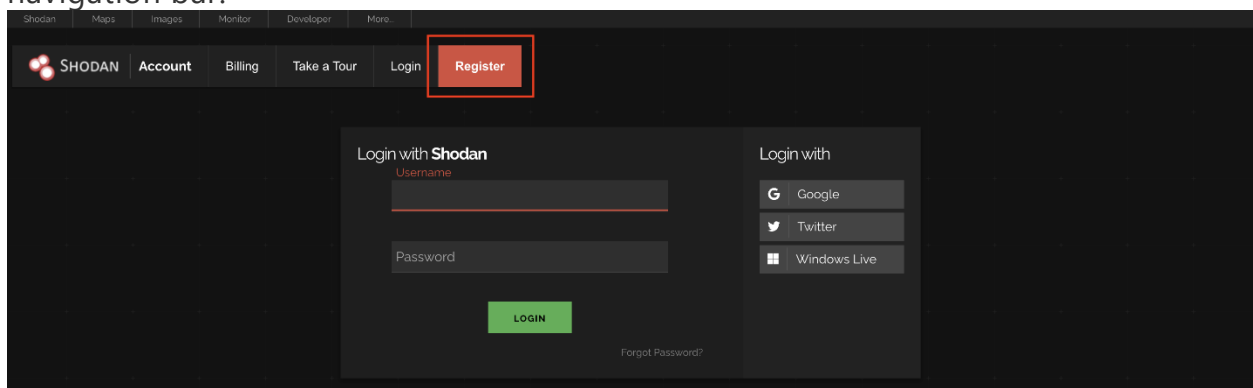
- Data about the service
- its IP address
- Port numbers that are in use
- The organization that the device belongs to
- The location / country where the device lives

Step 1: Create a Shodan account  
In this step, we'll setup an account in Shodan.

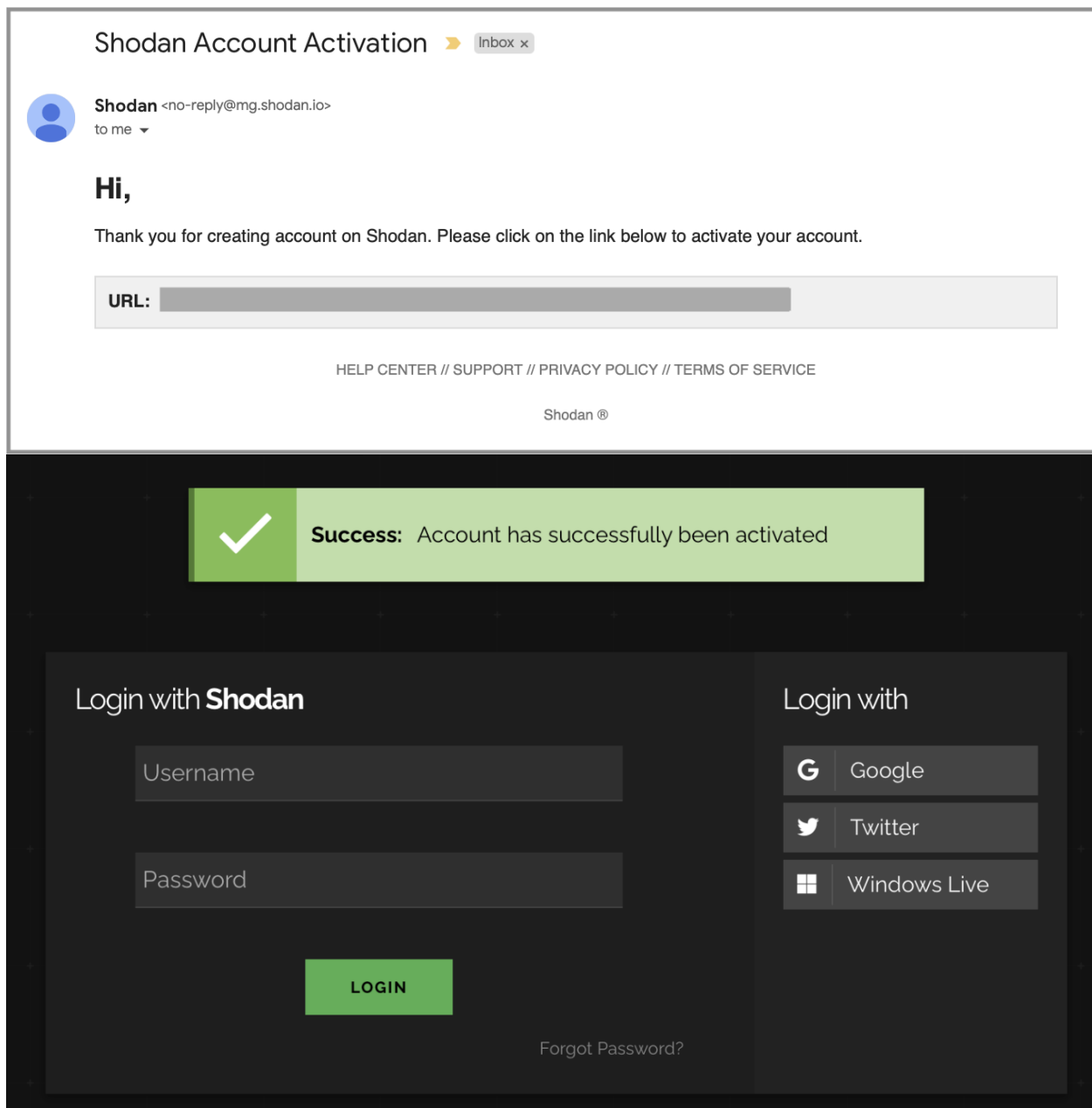
Go to the Shodan page, and there will be a navigation bar with a green Login button at the top right. Click on Login button.



You should be taken to a Login page. Click on the red Register button that is in the navigation bar.



After account is created. Go to your inbox and check the email sent from Shodan and activate your account.



⚠ If you use your Google, Twitter, or Windows Live account to register your Shodan account, you may not receive an activation email. Your account should still be successfully set up!

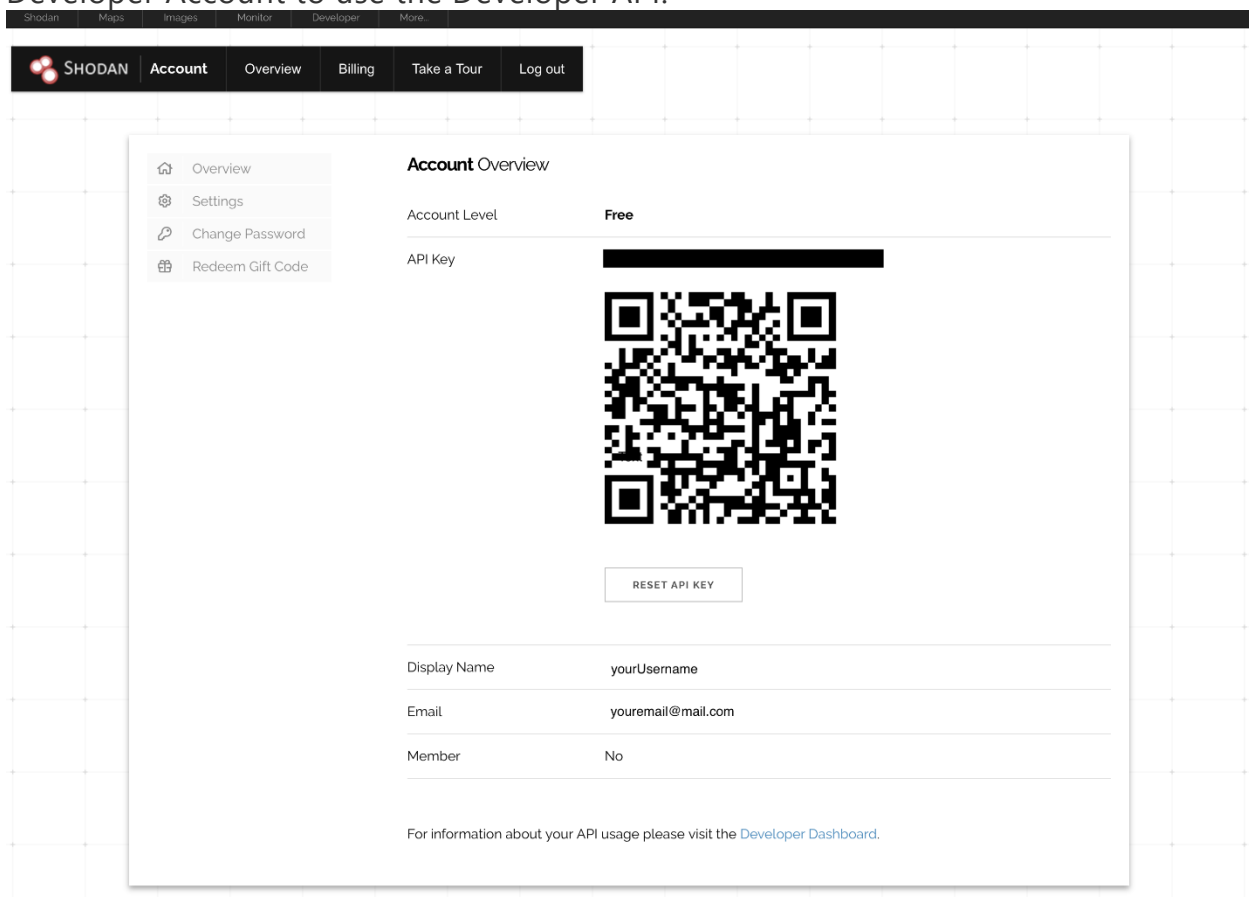
Step 2: Access Your Generated API key

After your account has been activated on Step 1, you should be able to login and access your Account page.

Go to your Account page by clicking Account on the [Shodan.io](https://shodan.io) homepage.

In the Account Overview, you'll see that it generated an API key automatically. You can also see more details about your account usage in the Developer Dashboard.

We will not be needing the API key for the queries we will be doing for this lab, yet it will be here for your reference and if you later decide to sign up for a paid Developer Account to use the Developer API.



🔑 Checkpoint 1: You've created an account on Shodan! Now you are ready to start exploring on the website.

Step 3: Perform searches and share the results

In this step, we will be performing a series of interesting search queries and share back some of the results. We'll be using the Shodan search engine at <https://www.shodan.io>.

You'll be able to view:

General info, open ports and banner information from those ports

Known device vulnerabilities and issues based on the device's software and version

Web technologies that are in use

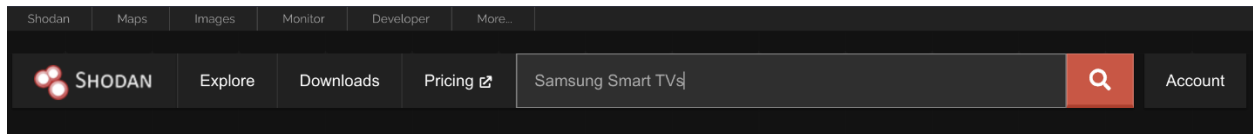
If connected to a webcam, a live preview of the device

📝 Note: A paid account is required to browse images, view raw data and history.

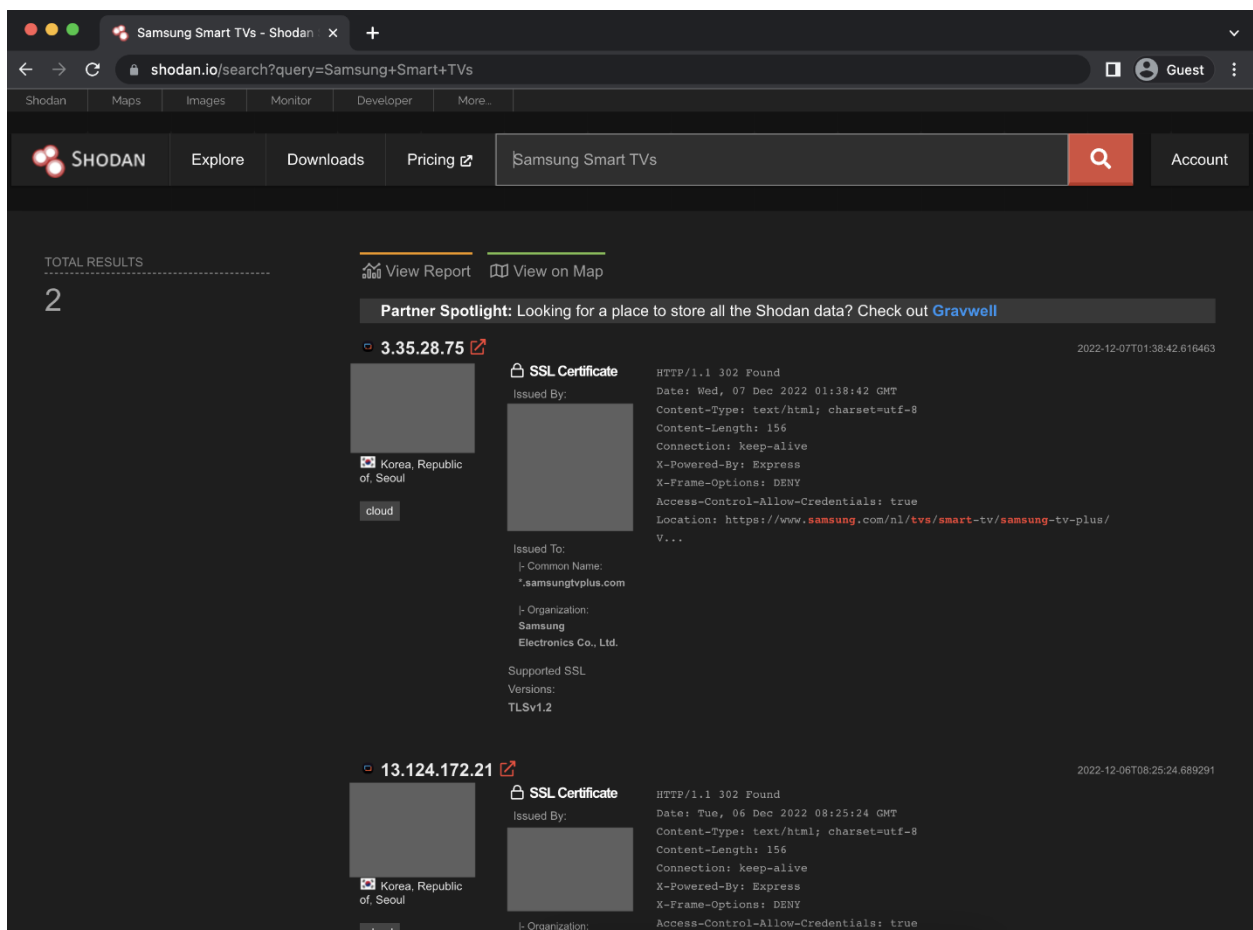
You will be able to see the information on the reports for the searches on the free plan.

## Search for Samsung Smart TVs

To perform a search, type the string you would like to search for in the search bar.



Hit the search button on the right. It should give you a list of results, like the one shown below:



Next, perform a search for websites that has been hacked and show who has hacked them. To use the filter, use the colon (:) between what you would like to filter for and the search term. For example, this uses the product filter to search Shodan for nginx type of web servers:

product:nginx

To search for a string in the banner, you can query for the filter and include the string in quotes. Here we are searching for devices in San Diego:

city:"San Diego"

Look in the Shodan Dashboard for examples of filters that can be used. There is one in this list that will help you find the sites that were hacked by someone.

Filters Cheat Sheet		
Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.		
Filter Name	Description	Example
city	Name of the city	<a href="#">Devices in San Diego</a>

Linked below are the:

Full list of filters on Shodan that we can use: [Filter Reference](#)

Examples of search queries and filters that can be used.


Once you give it a try, click this dropdown to check your work.

⚠ Warning: Be careful about running too many filters for this lab. Here are a few tips with using the free account:

Applying a filter will use up a query credit. We are only limited to 10 filters to use total for the month, so please use them sparingly.

Another tip is to stay on the first page of the query results. If you navigate to page 2 of any search, it will use up one of your query credits for the month.

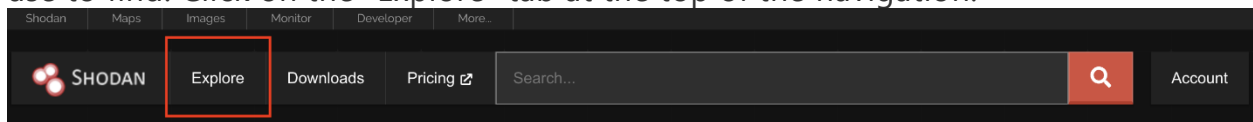
Queries are free (for instance, searching for "webcam" in the search engine will not use up any credits. However, searching for product:apache will use up an applied filter credit).

**Error:** Daily search usage limit reached. Please wait a bit before doing more searches or use the API.

Here is a link with a bit more details about the Shodan Credits.

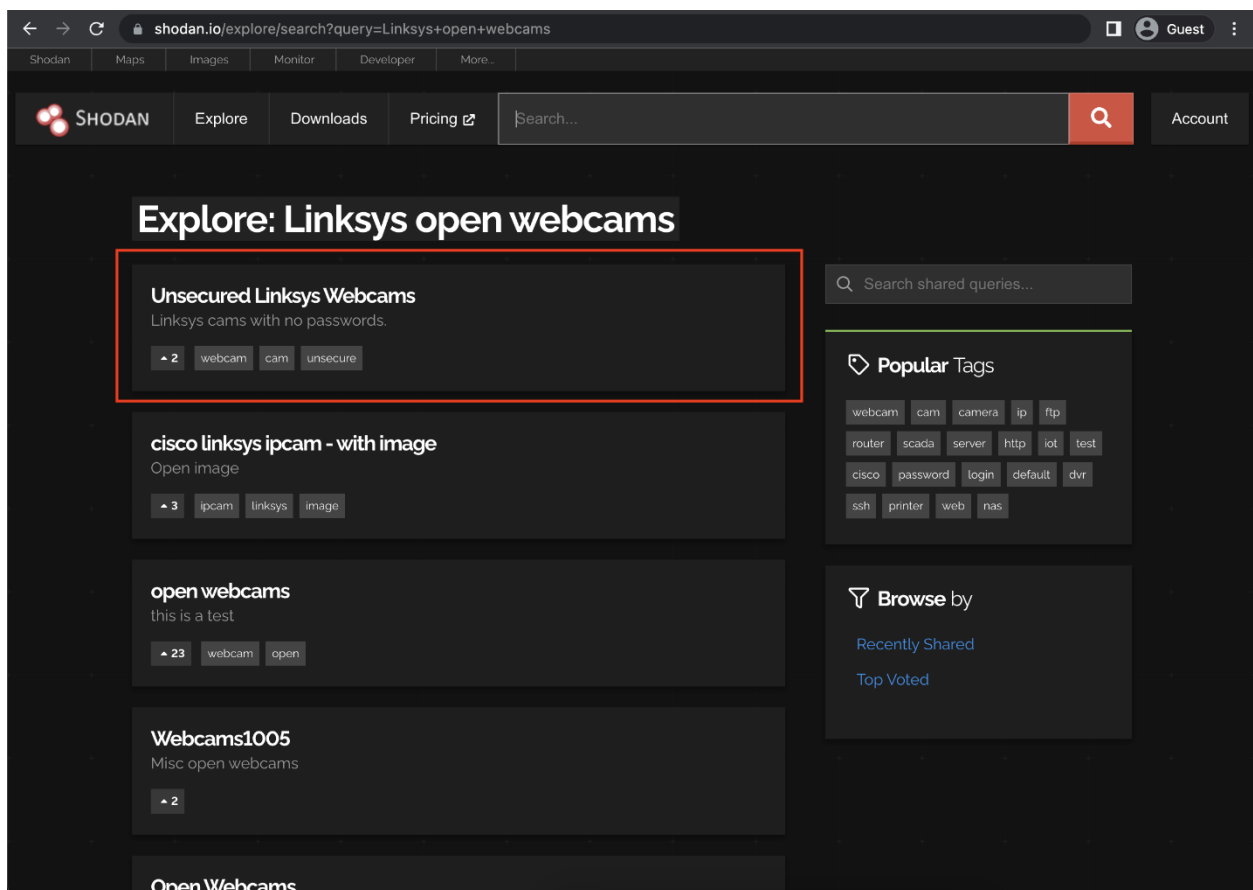
List Linksys Video Cameras with no passwords

Next, we will go explore some popular tags that people have created for others to use to find. Click on the "Explore" tab at the top of the navigation:

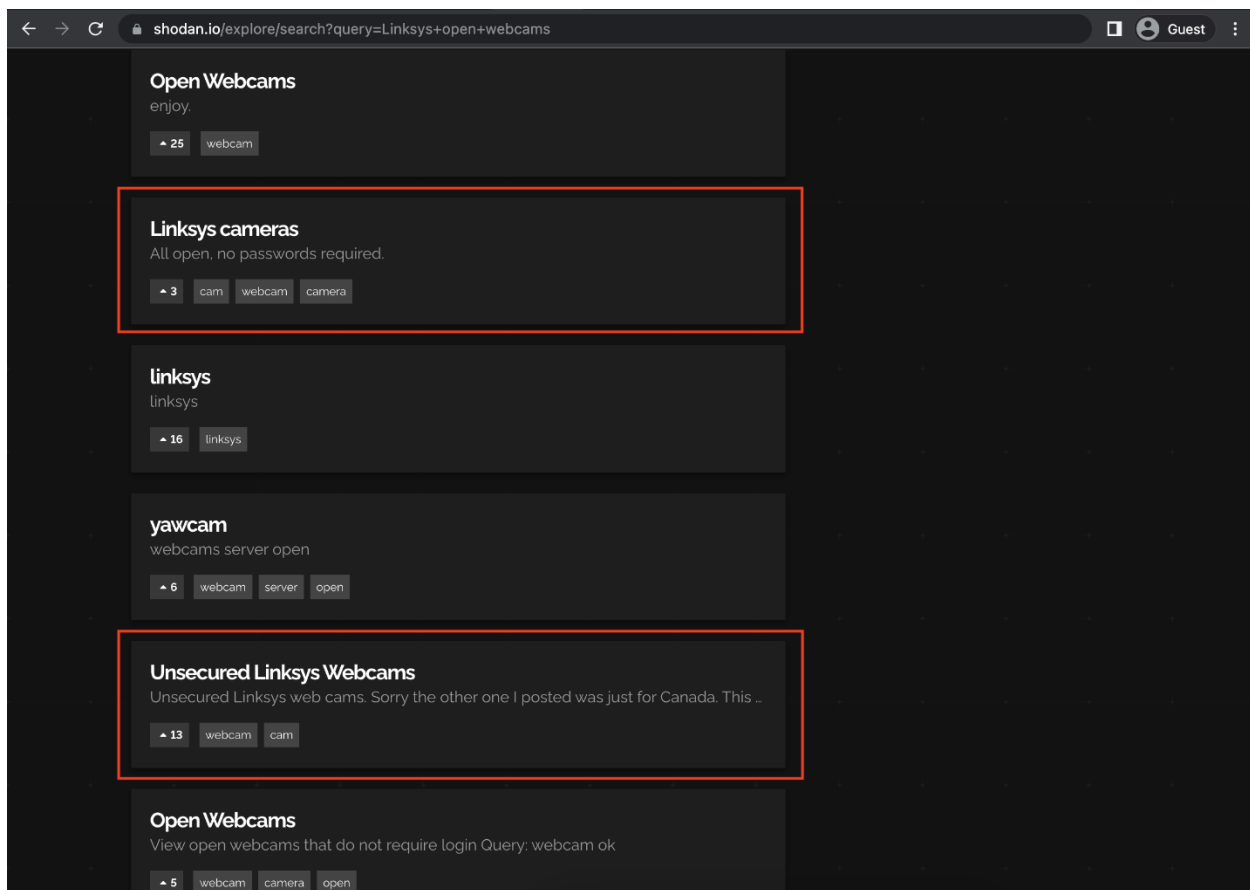


Search for "Linksys open webcams" using the "Browse Search Directory" search bar.

You will get a list of results back, such as the ones below. You can click on any of these options to view the query for it:



Here are the search results for Linksys cameras. You should find something similar to the search below:





shodan.io/search?query=title%3A"Linksys+Compact+Wireless"

Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing [title:"Linksys Compact Wireless"](#) Account

TOTAL RESULTS  
44

View Report View on Map


Partner Spotlight: Looking for a place to store all the Shodan data? Check out [Gravwell](#)


TOP COUNTRIES


United States 15  
France 7  
Canada 4  
Argentina 2  
Australia 2  
[More...](#)


TOP PORTS

1024 18  
1025 11  
80 7  
8001 2  
82 1  
[More...](#)

Linksys Compact Wireless-G Internet Video Camera [View Report](#) 2022-12-19T01:26:30.132871  
  
 HTTP/1.0 200 OK  
 Date: Sun, 18 Dec 2022 21:26:18 GMT  
 Server: Boa/0.94.13  
 Connection: close  
 Content-type: text/html  
 Canada, Toronto

Linksys Compact Wireless-G Internet Video Camera [View Report](#) 2022-12-18T18:59:50.728344  
  
 HTTP/1.0 200 OK  
 Date: Mon, 19 Dec 2022 04:59:40 GMT  
 Server: Boa/0.94.13  
 Connection: close  
 Content-type: text/html  
 Australia, Melbourne

Linksys Compact Wireless-G Internet Video Camera [View Report](#) 2022-12-16T11:24:27.684490  
  
 HTTP/1.0 200 OK  
 Date: Fri, 16 Dec 2022 13:24:14 GMT  
 Server: Boa/0.94.13  
 Connection: close  
 Content-type: text/html  
 France, Saint-Etienne

Linksys Compact Wireless-G Internet Video Camera [View Report](#) 2022-12-16T03:54:58.766847  
  
 HTTP/1.0 200 OK  
 Date: Fri, 16 Dec 2022 00:54:49 GMT  
 Server: Boa/0.94.13

Step 4: Generate some basic information about CodePath

How many hosts does CodePath have registered?

How many of those hosts are running OpenSSH?

Where are those hosts generally located?

Where are the SSH servers located?

What does the full report look like?

🔗 Checkpoint 2: On the search queries asked above, provide a screenshot on each of them and highlight the information that was asked.

🎉 Congratulations, you've completed your lab! 🎉

If you have time left over, continue on to the stretch features to improve your knowledge further!


## Stretch Features

Step 5: Craft your own queries

By now, you have already get to know Shodan and have learned what sorts of information we can retrieve from the site.

In this step, you are free to craft your own custom queries.

Perform a custom query of your own and share back the results!

 Congratulations, you've completed your lab AND stretch goals! 

[Expand all](#)[Back to top](#)[Go to bottom](#)

Select a repo