# Shodan Teacher Workout Instructions

### Introduction:

For this workout students will be using the Shodan API to view data on unprotected devices connected to the internet.

Shodan is a popular tool used that scans the internet for devices that aren't properly or securely configured and returns the information based upon the header response. While all of these devices could be found with a regular search on Google, a user might have to search through thousands of results to find one instance whereas Shodan makes this access easily accessible. Some security professionals use Shodan to help discover any vulnerable devices or servers that can be used to provide access to the client they are performing a security analysis for.

> When using Shodan, it is important to know that unless you have *explicit written consent from the owner of the device,* it is considered illegal *to act* upon any information found.

### Your Mission

To get started, in a new tab, go to the URL provided on your Cyber Gym Student landing page.

> For some of these questions, it can be helpful for the student to Google for information in order to help build the correct query. Example: to find Minecraft servers, it would be helpful to know what port they run on. Googling "*Minecraft default ports*" should return port 25565.

- **Task 1: Search for Minecraft servers in Dallas. What is the organization that owns the server of the 2nd result?**

  **Query**: `port:25565 city:"Dallas"`

- **Task 2: Search for companies that could be running pfSense in the United States. From the first result, what is the IP for the server? [IP format: 35.1.10.34]**

  Questions to ask: "What is pfSense?", "What system does it run on?"

  **Query**: `os:"FreeBSD" country:"US"`

- **Task 3: How many vulnerable Apache servers are there in Phoenix?**

  **Query:** `city:"Phoenix" "Apache"`

- **Task 4: How many servers are still vulnerable to Heartbleed?**

  Questions to ask: “What is Heartbleed?”

  **Query:** `vuln:"CVE-2014-0160”`

- **Task 5: Build your own query and submit a screenshot of your most interesting find!**

For even more information, students can dig through the raw data by clicking on the *view raw data* button. This could show anything from more details on any CVE’ s found on the page to HTML responses from the server.

> It isn’t recommended to follow any URL’s outside of Shodan or the Shodan API as some websites contain malware or adult content.

### Interesting Finds

This person was able to discover some pretty interesting finds with Shodan (Awesome-Shodan-Queries).