

Forum:[Hack Forums](#)

Thread: [How to Identify Potentially Vulnerable Systems Using Shodan \(2024 Perspective\)](#)

R5N3T - December 14, 2025, 9:58 pm

Tutorial on Finding System Vulnerabilities Using Shodan

To carry out the hacking process, we indeed need some sensitive and specific information to construct an attack. Therefore, the Shodan tool is able to provide clues to start an attack because it can collect various important information and data. Below is how to use Shodan:

1. Create a Shodan Account

The first step is to create a Shodan account by visiting [shodanhq.com](#). The registration process is free and does not require any additional payment to use the features available on the platform.

2. Search Process

After completing the registration, we can start performing specific searches by going directly to the Search Directory section. There, you will see several recent searches, and you can choose according to your needs or preferences.

3. Searching for Unsecured Webcams

In Shodan searches, there are many webcams that are not password-protected or lack proper security, making them easy to find and access. In this experiment, we found a home CCTV system, allowing it to be accessed remotely without a password.

4. Testing Traffic Light or Red Light CCTV Cameras

Using Shodan, we can find thousands of CCTV cameras, including those installed at road intersections, allowing us to view live conditions directly. This is because Shodan can search for and automatically discover devices that are vulnerable.

5. Testing the Search for Vulnerable Routers

Besides searching for active CCTV cameras, Shodan can also find thousands of routers connected to the internet that are not properly secured. We can access these routers using the default username and password, usually "admin."

Inside an unprotected router, we can change the DNS or other settings, which can later be redirected to phishing websites or fake pages to collect important information and data, such as login credentials from users connected to the router's Wi-Fi network.

6. Searching for SCADA Systems

Among the many types of searches, one of the most dangerous is searching for SCADA systems, which have the potential to cause serious damage and pose significant risks. This is because SCADA systems are widely connected to and control critical infrastructure such as electricity power grids, water installations, and other essential services.

SCADA devices themselves are often used by hackers to terrorize their victims and are considered

one form of cybercrime terrorism, as they can create chaos within a country by disabling power grids, electrical installations, and other critical infrastructure.

7. Searching for Default Passwords

In addition to features that can search for vulnerable devices, Shodan can also find passwords that are widely available on the internet. Simply by searching on Google for “default password,” Shodan will display a complete list of default credentials, including the username and password combinations.

Shodan is a powerful search engine tool for finding system vulnerabilities around the world. In addition, Shodan has several advanced and unique features that can be used to identify login types, such as web logins, ports, accurate geographic locations, and more.

Therefore, Shodan is a search engine tool that hackers must use to find things that cannot be found on Google, as Google has many limitations in place to protect privacy.

The tutorial above is shared strictly for educational and learning purposes only. It is not intended to encourage or support any illegal activities. Any information provided should be used responsibly, ethically, and only on systems you own or have explicit permission to test. [warn]