# Shodan: Exploring Past, Present, and Future Vulnerabilities

*Jonathan Roeseler*
jroes001@odu.edu

## Abstract

The fast evolution of the Internet, and technology in general, has led to an ever-increasing attack surface, with vulnerabilities emerging/existing in legacy and modern systems. Shodan, a hacker's dream search engine that looks at all systems, devices, and networks connected to the Internet, is a much-needed tool for identifying systems with certain vulnerabilities and ultimately painting a picture of what is connected and exposed to the Internet. This project explores Shodan: specifically, its current use cases in cybersecurity, and the potential future impact of its use. By examining past incidents, present vulnerabilities, and potential future attacks, this project aims to provide an overview of how Shodan can be leveraged to find vulnerabilities of all kinds.

## Background/Intro

Shodan is an incredible tool, used by both ethical and non-ethical hackers. Shodan stands out as a tool as it is able to grab all devices with a particular vulnerability (that are internet-connected), making it much easier to diagnose how much of the Internet is susceptible to a particular attack or vulnerability. Shodan's impact can be tremendous on cyber-systems, especially if used maliciously. As seen in my research, despite being an almost 8-year-old vulnerability, there are still about 4,000 devices susceptible to the popular Eternal Blue exploit(MS17-010). If an attacker were to make use of this information, all these devices could be compromised and used for malicious purpose, such as for a botnet, allowing for the DDoSing of arbitrary domains and sites.

## Objectives

i. Find popular vulnerabilities such as Eternal Blue
ii. Find recent vulnerabilities
    i. ex: CVE-2024
iii. Demonstrate how Shodan can be used to find brand new vulnerabilities (NO CVE)

## Methods

✓Searched for Eternal Blue vulnerability

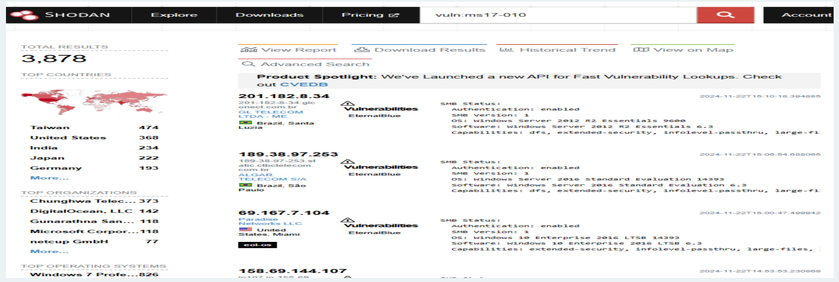
✓Searched for recent CVE

✓Found that Shodan can be used to help find devices with zero-days. For example, Let's say that it was just discovered a Cloudflare CDN in front of nginx servers are susceptible to HTTP Request Smuggling(HRS). To prove this attack works and it's not limited to the site being tested on, Shodan can be induced to show all systems using this configuration. By searching for both the Cloudflare and Nginx backend it allows for the easy finding of potentially vulnerable devices. In the screenshot to the right, all that was needed to search for this hypothetical attack is:

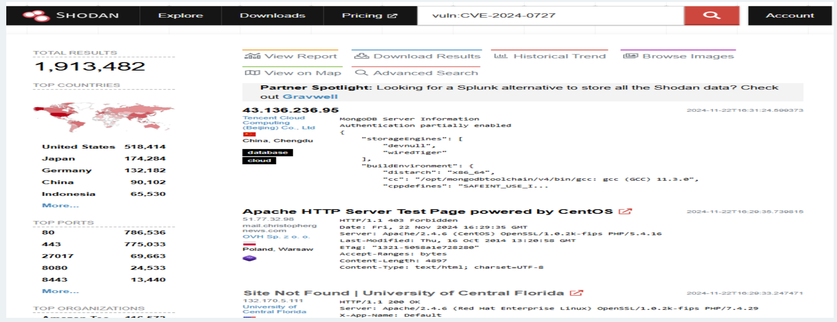
✓http.component: cloudfront AND http.component: nginx

## Results

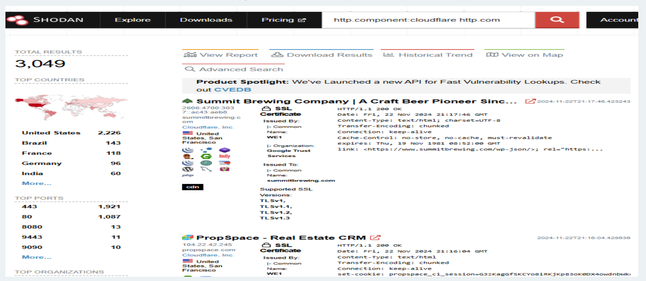
✓Found systems vulnerable to Eternal Blue




✓Found a very recent vulnerability (CVE-2024-0727)




✓Found "vulnerable" systems




## Conclusion

✓Shodan can be used to easily find old vulnerabilities

✓Shodan can be used to find newly reported vulnerabilities

✓Shodan can be used to discover potentially susceptible systems/0-days