

Cyber Threat Intelligence (CTI) Report: Walmart Inc.

Kayla Hodge | CYB3355-O | C202508-01

Contents

Introduction 3

Google Dork Findings 4

 Figure 1: Google Dork Search 4

Shodan and Censys Findings 5

 Figure 2: Shodan Top 10 IP Addresses for Walmart.com 5

 Figure 3: Shodan Top 10 Ports for Walmart.com 6

 Figure 4: Censys Certificates Found 7

Wayback Machine Findings.....8

 Figure 5: Walmart.com December 29, 1996 8

OSINT Reflection 9

References 10

Introduction

This investigation looked at Walmart.com using Open-Source Intelligence (OSINT) to see what kind of information is publicly available. The goal was to find anything that could be exposed online, without touching any private systems. Tools used included Google Dorks, Shodan, Censys, and the Wayback Machine.

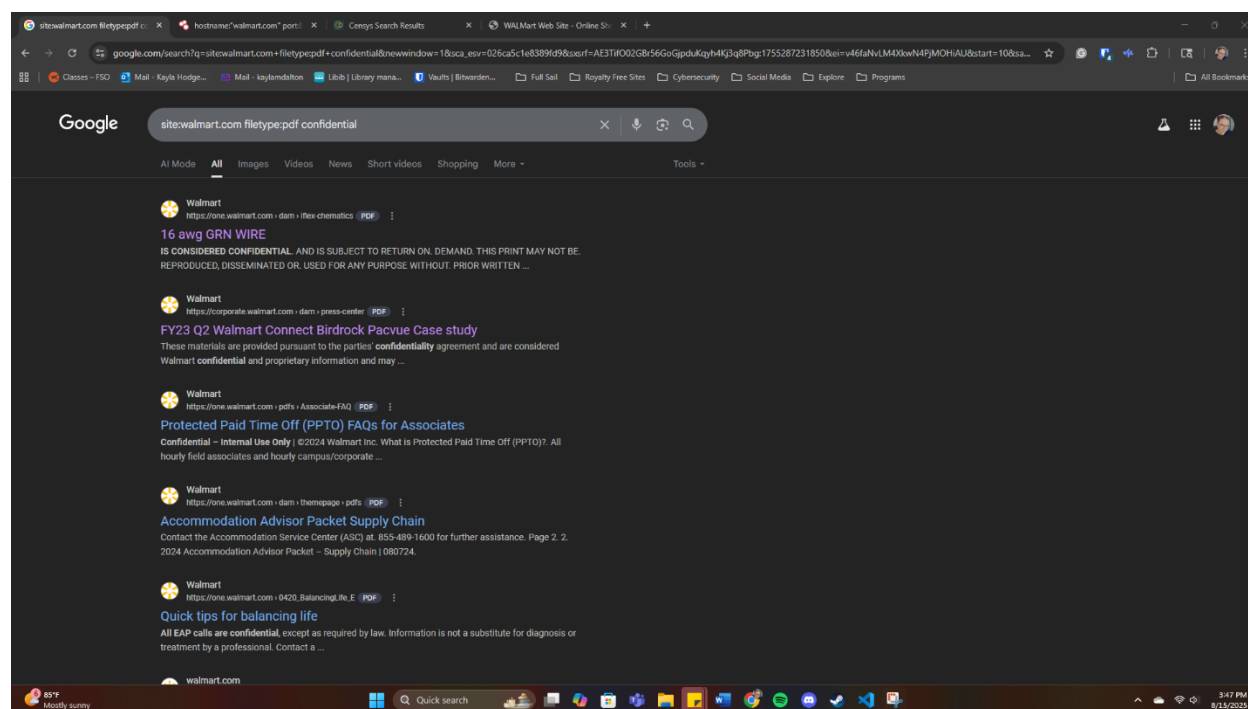
By checking directories, documents, servers, certificates, and website archives, it became clear that even large companies like Walmart have a lot of information floating around publicly. This shows how useful OSINT can be for getting a bigger picture of a company's digital footprint.

Google Dork Findings

Using Google Dorks to search Walmart.com started out rather ordinary, showing book indexes and general content anyone could find. Digging a bit deeper, though, uncovered some things that seemed meant for internal eyes only. For example, financial documents like the stock split for 2024 and Q4'21 earnings call results were visible. Employee resources also showed up, including HMO plans, benefits information for multiple years (2021–2023), and case study flyers marked for internal use only. There were also some technical documents like schematics for a wire, cluster analyses, and FAQs meant for employees only. No passwords or login credentials were found, but the amount of internal-use-only material was surprising.

This just shows that even simple searches can reveal information companies may not realize is out there. It's a good reminder that keeping track of what's publicly visible can help prevent accidental exposure. Regular monitoring of a company's online footprint can make a big difference in identifying and addressing these risks early.

Figure 1: Google Dork Search



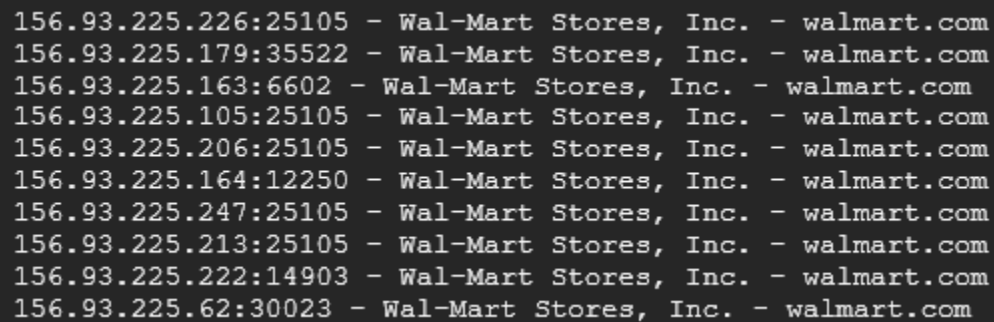
Google results for site: and filetype: Google Dorks used to investigate Walmart.com. Several “For Internal Use Only” files showed up in this filetype:pdf confidential search.

Shodan and Censys Findings

Looking at Walmart's external systems, Shodan provided a quick snapshot of the internet-facing IPs and ports currently in use. I pulled the top ten IP addresses from Shodan into a Word document, which are listed in Figure 2: Shodan Top 10 IP Addresses for Walmart.com. Port 443 appeared more frequently, which makes sense since it's used for secure web traffic, followed by port 80 for standard web traffic. A few other less common ports also appeared, as shown in Figure 3: Shodan Top 10 Ports for Walmart.com.

While nothing in the results jumped out as immediately exploitable, the presence of some older or less-used ports is a reminder that regular security checks are still important. Even from the outside looking in, you can see how large and distributed Walmart's network is, and it's easy to imagine how much effort it must take to manage and secure all of it.

Figure 2: Shodan Top 10 IP Addresses for Walmart.com



```
156.93.225.226:25105 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.179:35522 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.163:6602 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.105:25105 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.206:25105 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.164:12250 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.247:25105 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.213:25105 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.222:14903 - Wal-Mart Stores, Inc. - walmart.com
156.93.225.62:30023 - Wal-Mart Stores, Inc. - walmart.com
```

Shodan scan results showing the top 10 IP addresses associated with Walmart.com. This data highlights the company's internet-facing infrastructure, including key ports and services that are publicly accessible.

Figure 3: Shodan Top 10 Ports for Walmart.com

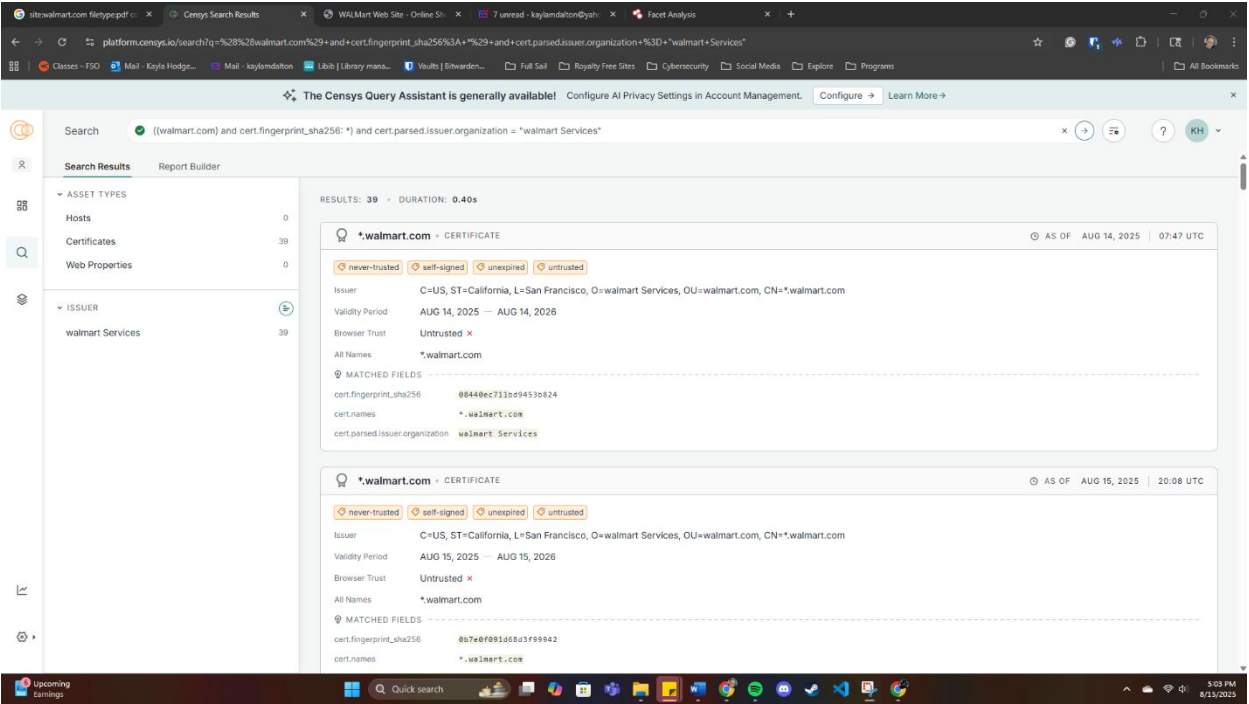


This chart shows the ten most common open ports found during the Shodan scan of Walmart.com’s network. Ports 443 and 80 appear the most.

I also used Censys to dig into Walmart’s certificates and host details, offering another layer of insight into their public infrastructure. The search revealed multiple TLS certificates spread across different servers, which points to a mix of encrypted web traffic and secure VPN endpoints. This kind of information doesn’t necessarily indicate vulnerability, but it does give a glimpse into the technologies Walmart relies on to secure its external connections.

It was especially interesting to see how these certificates are distributed, which can hint at different services, geographic locations, or backup systems. Even without uncovering anything risky, tools like Censys make it clear how much can be learned about a network just by examining what it openly shares with the internet.

Figure 4: Censys Certificates Found



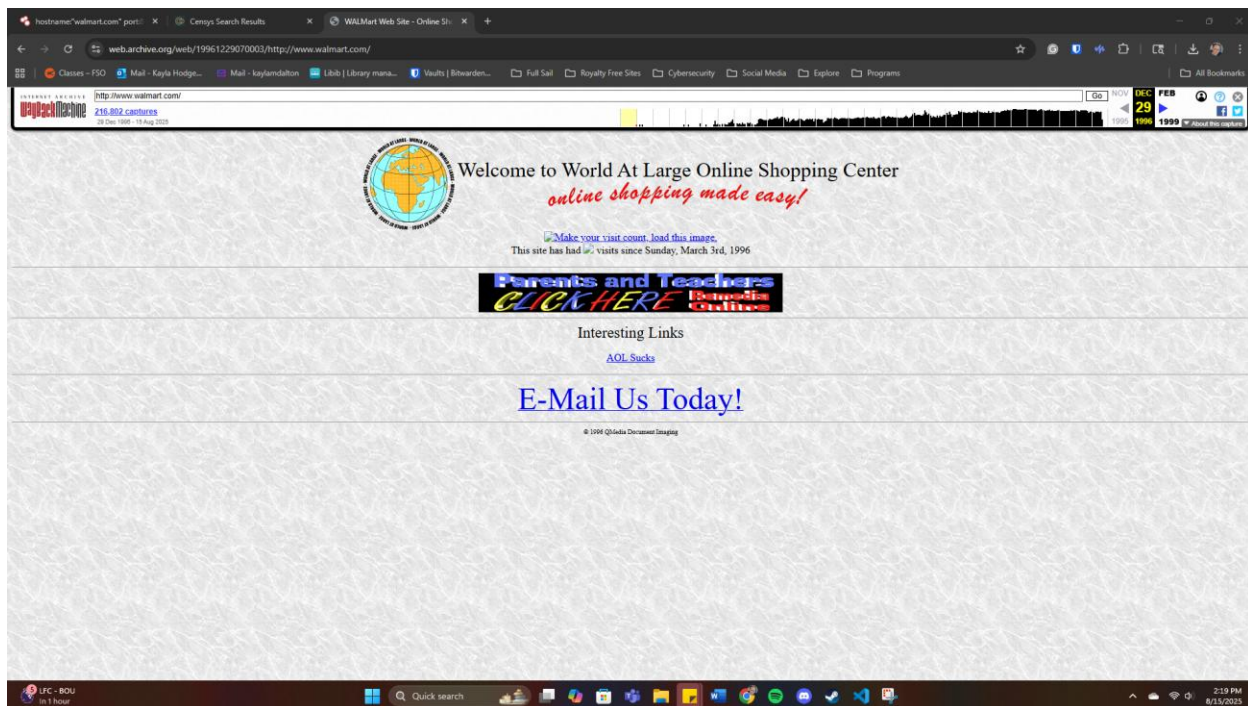
Censys search results displaying SSL/TLS certificates linked to Walmart.com. These certificates provide insight into the domains and subdomains actively using encrypted connections.

Wayback Machine Findings

Checking Walmart.com on the Wayback Machine was interesting. The first capture was on December 29, 1996, and there have been 216,802 captures through August 15, 2025. It was quite shocking to see it go back that far, as well as gaining the knowledge that WAL stood for World at Large.

Some older pages included internal guidance or resources that aren't public anymore. While nothing sensitive showed up, it was fascinating to see how the website has changed over time. Looking at older versions can give insight into how a company presents itself online and how its public content has evolved.

Figure 5: Walmart.com December 29, 1996



Archived snapshot of Walmart.com from December 29, 1996. This early version of the site shows the company's original online presence and design style.

OSINT Reflection

Going through this investigation highlighted how much we can learn from public information alone, without ever accessing anything private or restricted. Even with basic searches and scanning tools, it's possible to uncover financial documents, internal-looking employee resources, server details, and years-old archived content that companies may have forgotten was still online.

This kind of exposure is exactly what makes OSINT so valuable. It maps out a company's digital footprint and often reveals areas that might otherwise be overlooked. For security teams, these findings can act as an early warning system, pointing them toward accidental exposures or outdated systems before they become problematic. It's a strong reminder that monitoring what's already out there is just as critical as locking down what's inside the network, because attackers often start with what's easiest to find.

References

Shodan (n.d.). Retrieved August 15, 2025, from

<https://www.shodan.io/search/facet?query=hostname%3A%22walmart.com%22&facet=port>

Censys (n.d.). Retrieved August 15, 2025, from

<https://platform.censys.io/certificates/14ef0eb3658595110cce9212b21b43c15c0a0a3d491a23cb62434818bb31fbc6>

Wayback Machine (n.d.). Retrieved August 15, 2025, from

<https://web.archive.org/web/19961229070003/http://www.walmart.com/>

Lee, C. (2025, July 15). *Google Dorks Cheat Sheet 2025: How to Hack Using Google*.

StationX. <https://www.stationx.net/google-dorks-cheat-sheet/>

OffSec Services Limited (n.d.). *Google Hacking Database*. Exploit Database. Retrieved

August 15, 2025, from <https://www.exploit-db.com/google-hacking-database>

Google Dorks used **site:walmart.com intitle:"index of" and filetype:pdf confidential**

https://www.google.com/search?q=site:walmart.com+filetype:pdf+confidential&newwindow=1&sca_esv=026ca5c1e8389fd9&sxsrf=AE3TifO02GBr56GoGjpduKqyh4Kj3q8Pbg:1755287231850&ei=v46faNvLM4XkwN4PjMOHiAU&start=10&sa=N&sstk=Ac65TH72RkjOiiQ_wJ7vYEd5UO35X0LljwXpn-4cA8tygdPd4vGXZ19KDBRaDFoXiV5Qnuxx21m7Vke-gyyYJlM1hRSasS3rmDKdJZaNqnWSt_Rni0OPp62hanQGinjJOxcHylmmPmwdV5MzXmM8czpHH81kiF6hASt164MeRl8mICG-GZkjV5Cat6cMXGqaoPketlvCklffhDiore7wSlw7oAqtqUth&ved=2ahUKEwibp7u_yo2PAxUFMtAFHYzhAVE4KBDy0wN6BAgHEAY&biw=1920&bih=911&dpr=1