Week 1 - Recon phase

Objectives

The primary objectives of recon are to gather detailed `Sensitive in some cases` information about the target, identify potential vulnerabilities, and map the network and system structure and also identify potential entry points. This phase also involves understanding and knowing the technologies and configurations web-application uses. The information collected helps in the testing process by revealing weak points and entry opportunities for further exploration.

> Our target will be : https://newrelic.com/
>
> - it's a software analytics and performance monitoring platform.
> - New Relic provides tools for monitoring applications and infrastructure, allowing developers to track performance metrics, gain insights into user interactions, and optimize application performance.

Tools and word lists used in the recon phase

- Subfinder
- Sublist3r
- security-trails
- Shodan
- Google dorking
- Github dorking
- Gau
- uro

- WaybackUrls
- httpx
- Wappalyzer

Subdomain Enumeration process

```
cat target.txt | wc
19542    19542   825868
```

This **file** contains as showing +19K different subdomain, all of them could be used as an entry point

> after some investigation the most critical end-points could be start with to look for vulnerabilities in there are the subdomains that contains
>
> - new
> - relic
> - div
> - lab
> - docs
> - data
> - management
> - service
> - and others

Note: after using httpx on this list, there are around `2300` subdomain with the status code of "200", but still subdomains with status code `303,302` or even `404,403,401` could be used later in the directory discovery phase and some subdomains may include some sensitive information in them.

WaybackUrls

with these two commands:
- echo "newrelic.com" | gau --threads 5 --blacklist png,jpg,gif | tee waybackurls.txt
- echo "newrelic.com" | waybackurls | tee -a waybackurls.txt

```
cat waybackurls.txt| wc
37303   37304 3015758
```

> these +37K waybackurl could be used for finding Deprecated or forgotten Endpoints, locating sensitive Information, Identifying Attack Vectors for specific vulnerabilities like **LFI**, **RFI**, **SQLi** and **XSS**, Exploring old JavaScript Files and much more

---

Directory discovery

- We use this process to discover a hidden directories that could include sensitive information, hidden admin pages with weak/default credentials and also hidden end points that could have significant vulnerabilities due to no one had discovered or reached this end point before, so Directory enumeration is consider one of the most crucial and critical recon phase.
- This file contains +100 hidden directory could be checked in the exploitation process

```
(venv) ┌─[user@parrot]─[~/workspace/targets]
└──╼ $cat output.txt | wc
    104     375    5578
```

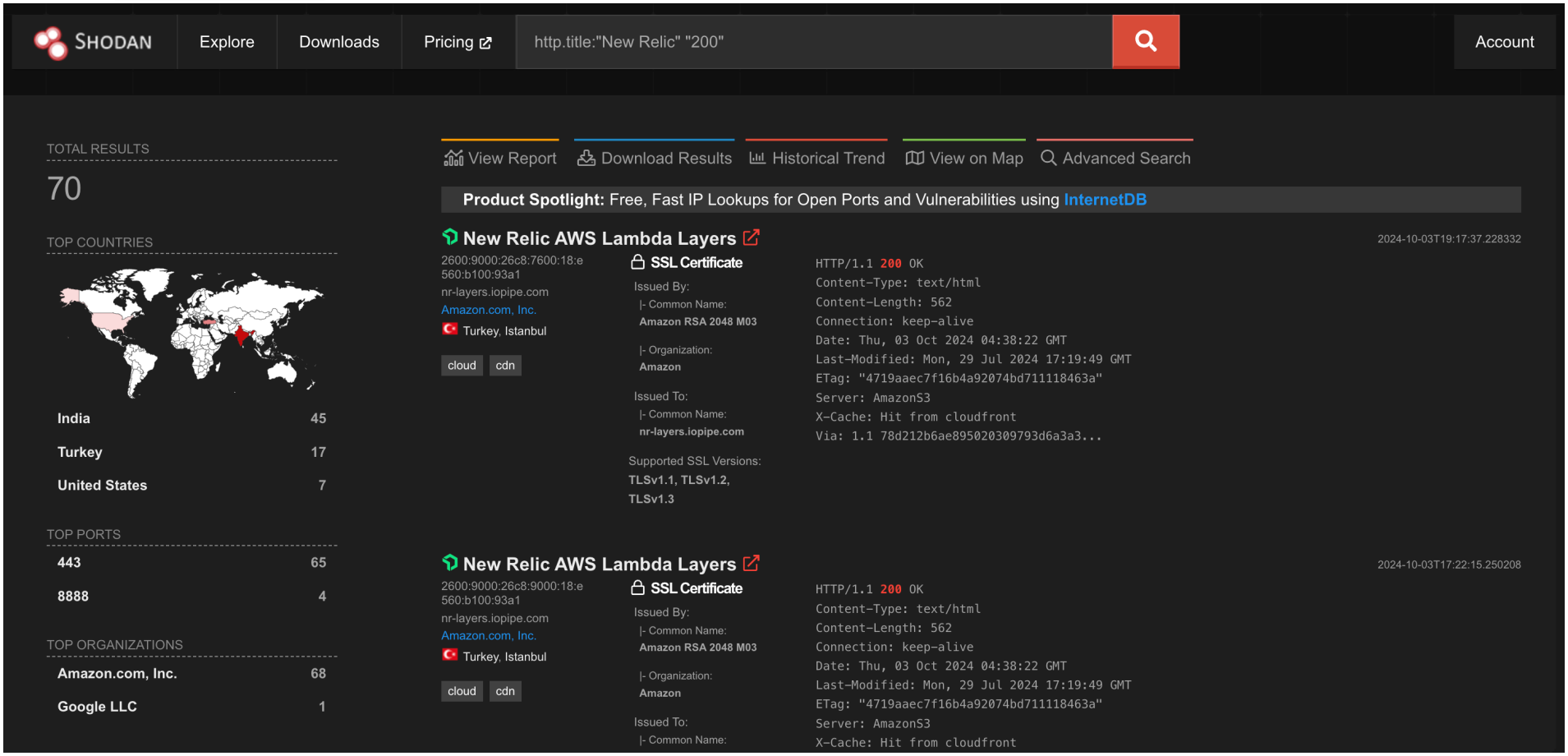
After this phase we could use a tool like aquatone to for visual and inspect the endpoints with status code `200"` or manual check them, also we as we performed a lot of semi-deep recon, we could use a tool like gf and dalfox to automate the scan of `XSS` vulnerability

> Most interesting directory as a beginning : https://newrelic.com/robots.txt

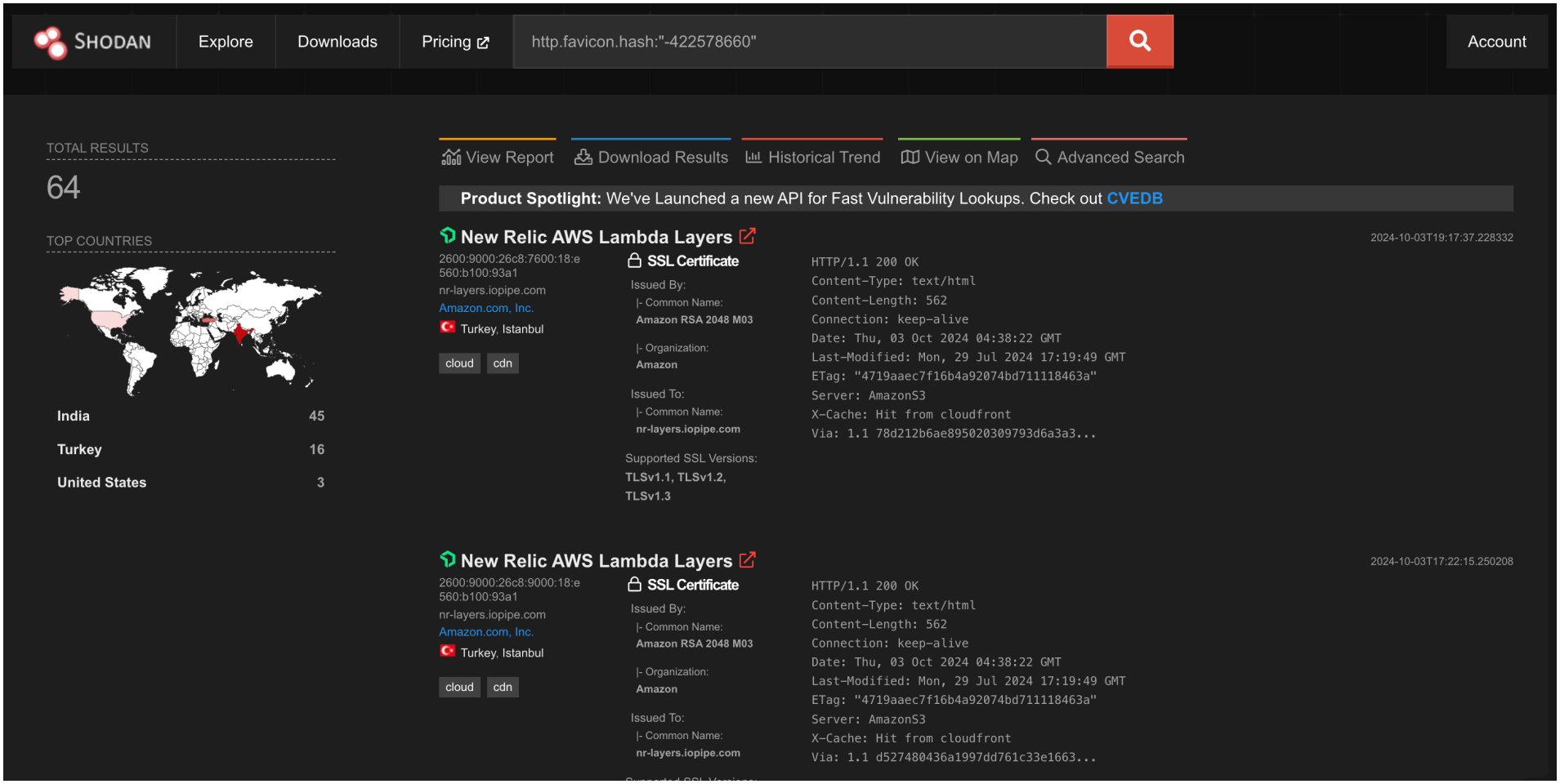
---

shodan dorking

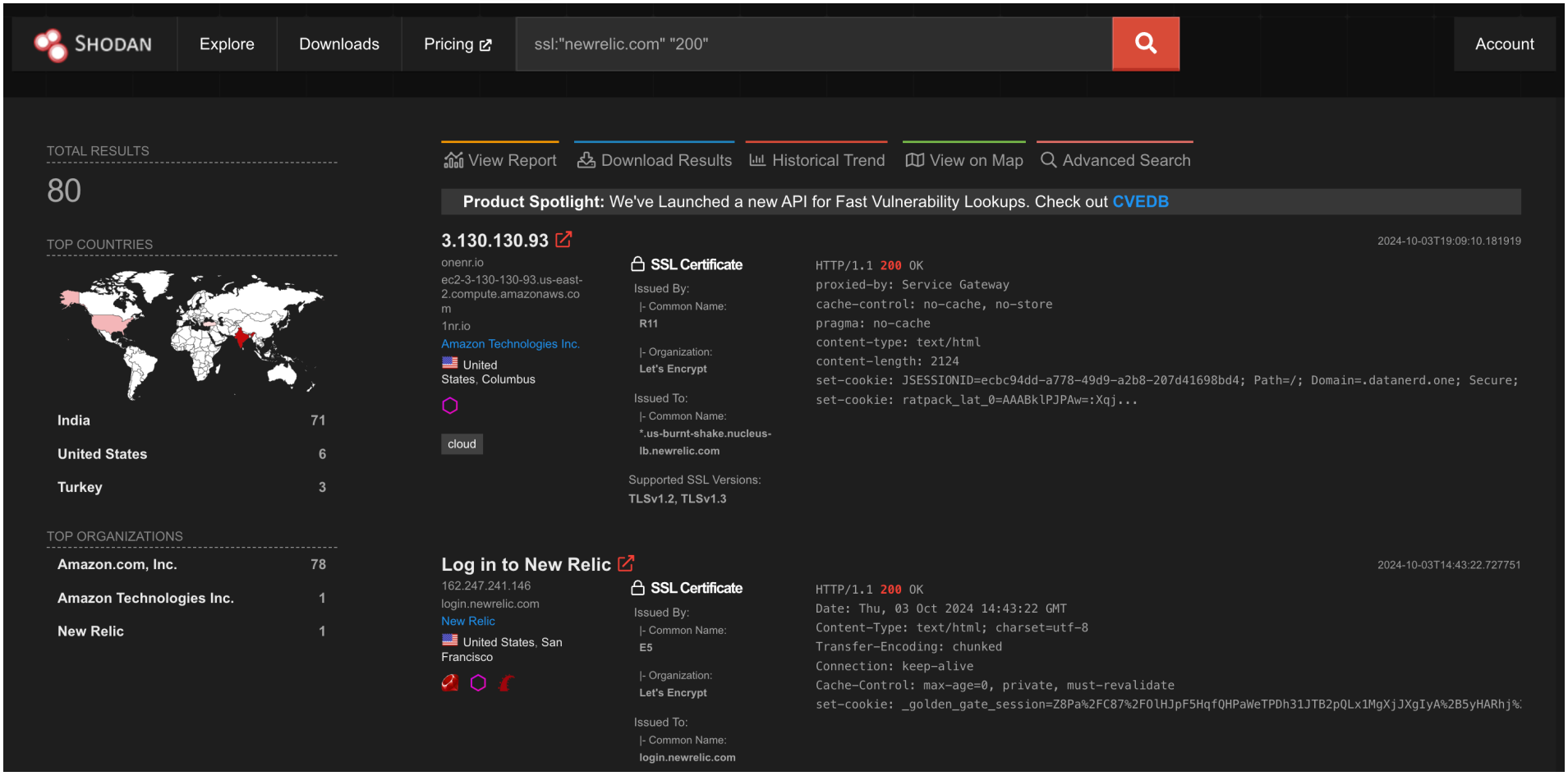
- http.title: `"New Relic.com"` --> 70 results



- http.favicon.hash:"-422578660" | use this website to get the favicon

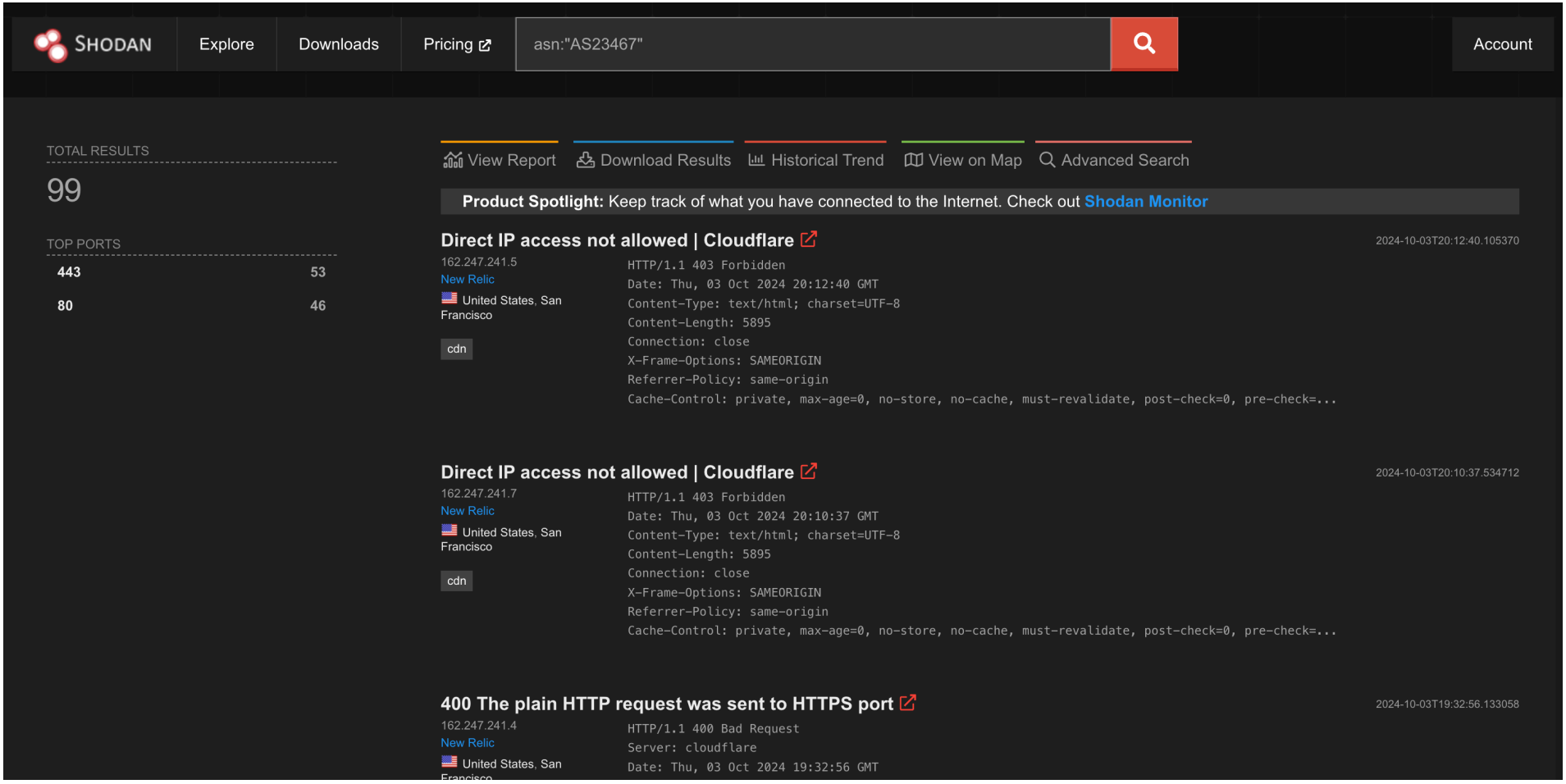


- ssl:"newrelic.com" --> 230 result --> use `"200"` to reduce the results



- ASN number
  - ASN number `Autonomous System Number` : is a unique identifier collect range of IP networks and routers under the control of the target organization
  - use this one, this one, and this one could be a great resources to get the ASN numbers for the target
  - some collected asn numbers : AS54078, AS395722, AS23467, AS206998 and AS60819

- then use this dork : asn:" `<ASN_Number>` " ex: asn:"AS54078"



Google dorking

- Here is some interesting potential hidden attack surface on the target using google dorking
  No.1

Google

site:newrelic.com inurl:api | site:*/rest | site:*/v1 | site:*/v2 | site:*/v3

New Relic API keys | New Relic...
New Relic Documentation

Explore the Public API Perform...
New Relic Documentation

New Relic API keys | New Relic...
New Relic Documentation

Show more images

New Relic Documentation
https://docs.newrelic.com › docs › apis › intro-apis › ne...

New Relic API keys

These keys allow only approved people in your organization to report data to New Relic, access that data, and configure features.

New Relic Documentation
https://docs.newrelic.com › apis › rest-api-v2 › get-started

How to use our REST API (v2)

New Relic's REST API lets you retrieve data from and push data to New Relic tools, as well as to configure features and perform delete operations.

New Relic Documentation
https://docs.newrelic.com › docs › distributed-tracing › i...

Introduction to the Trace API

Our Trace API is used to send distributed tracing data to New Relic: either in our own generic format or the Zipkin data format.

New Relic Documentation
https://docs.newrelic.com › docs › data-apis › ingest-apis

Incident event REST API

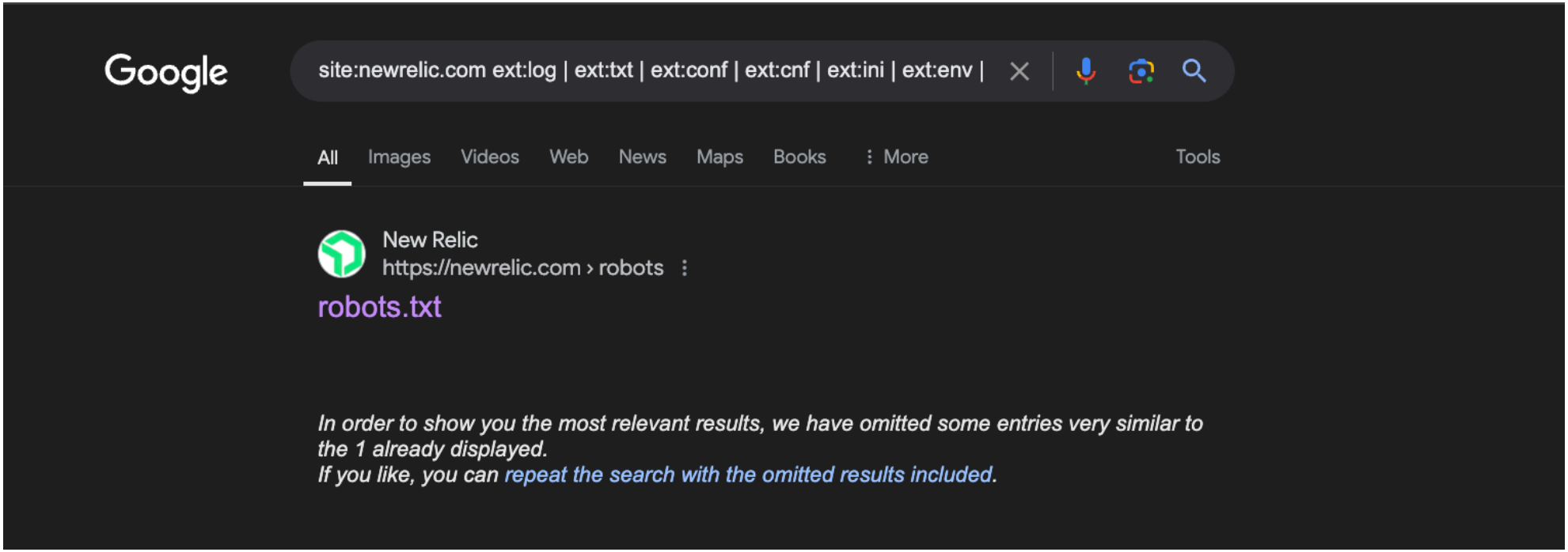
The API is an asynchronous endpoint. This means you can send a large volume of POSTS, reliably, with low-response latency. Using the API: an overview.

New Relic Documentation
https://docs.newrelic.com › log-api › introduction-log-api

Send your logging data with our Log API

Use our Log API so you can send your monitored log data directly to New Relic via HTTP input.

No.2


Google
site:newrelic.com ext:log | ext:txt | ext:conf | ext:cnf | ext:ini | ext:env |
All
Images
Videos
Web
News
Maps
Books
More
Tools
New Relic
https://newrelic.com › robots
robots.txt
In order to show you the most relevant results, we have omitted some entries very similar to the 1 already displayed.
If you like, you can repeat the search with the omitted results included.

No.3

Google

inurl:http | inurl:url= | inurl:path= | inurl:dest= | inurl:html= | inurl:data=

All Videos Images Books Web News Maps More Tools

New Relic
https://newrelic.com › mobile-monitoring › page=64

https://newrelic.com/mobile-monitoring?p1j641=&page=64

No information is available for this page.

Learn why

New Relic
https://newrelic.com › blog › search › page=4

Search Results

In diesem Blog-Post sehen wir uns an, wie die neue Integration von New Relic und Azure Monitor funktioniert und welche Vorteile Unternehmen aus den ...

In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.
If you like, you can repeat the search with the omitted results included.

Used Technologies & open ports

- after the process of port scanning the open ports are only : 80, 443
- used Technologies :
  - CMS : Drupal
  - databases : MariaDB "sqli"
  - Video players: Wistia
  - IaaS: Snowplow Analytics
  - Reverse proxies: Nginx
  - UI framworks: Tailwind CSS
  - Web servers: Nginx
  - Programming languages: Python & PHP
  - CDN: Fastly
  - Customer data platfrom: Segment

After some walking through the web application

- Here is the most critical and potential domains to find and exploit vulnerabilities

> trynewrelic.com
> newrelicone.com
> newrelic.co.in
> new-relic.com
> newrelic.one
> newrelic-external.com
> newrelicone.net
> newrelicobservability.com

> newrelicjobs.com
> newrelic.social
> newrelic.org
> new-relic.org
> newrelicgov.com
> newrelic.in
> wwwnewrelic.com
> staging-newrelic.com
> new-relic.one
> newrelicone.one
> new-relic.net
> newrelic.com

---

ip Ranges

- 64.251.192.0/20
- 152.38.128.0/19
- 162.247.240.0/24
- 162.247.241.0/24
- 212.32.0.0/20

--> use this shodan dork to classify these ranges : ip: `<ip range>` ex: **ip:162.247.240.0/24**

> 64.251.192.0/20 --> All hosts down
> 152.38.128.0/19 --> All hosts down
> 162.247.240.0/24 --> All hosts down

> 162.247.241.0/24 --> there are 95 hosts UP
> 212.32.0.0/20 --> All hosts down

SHODAN | Explore | Downloads | Pricing | ip:162.247.241.0/24 | Account

TOTAL RESULTS

99

TOP PORTS

443	53
80	46

View Report | Download Results | Historical Trend | View on Map | Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

400 The plain HTTP request was sent to HTTPS port 2024-10-03T20:16:07.743131

162.247.241.9
New Relic
United States, San Francisco
cdn

```
HTTP/1.1 400 Bad Request
Server: cloudflare
Date: Thu, 03 Oct 2024 20:16:07 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -
```

Direct IP access not allowed | Cloudflare 2024-10-03T20:12:40.105370

162.247.241.5
New Relic
United States, San Francisco
cdn

```
HTTP/1.1 403 Forbidden
Date: Thu, 03 Oct 2024 20:12:40 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
Connection: close
X-Frame-Options: SAMEORIGIN
Referrer-Policy: same-origin
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=...
```

Direct IP access not allowed | Cloudflare 2024-10-03T20:10:37.534712

162.247.241.7
New Relic
United States, San Francisco

```
HTTP/1.1 403 Forbidden
Date: Thu, 03 Oct 2024 20:10:37 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 5895
```