Task 2: Shodan Dorks for Reconnaissance

Maheshwar Anup

July 13, 2025

Contents

1 Task 2

To use Shodan dorks to find login pages and other juicy stuff.

2 Steps

2.1 Used Kali GPT (Chat GPT) to generate Shodan dorks.

♦ Basic Syntax Recap

```
keyword filter:value
```

Listing 1: Basic Shodan Dork Syntax

Common filters:

- `port:`
- `country:`
- `org:`
- `os:`
- `product:`
- `hostname:`
- `title:`
- `http.html:`
- `ssl:`
- `before:`
- `after:`

♦ 1. Unprotected Devices and Databases

Exposed MongoDB:

```
product:"MongoDB" port:27017 -authentication
```

Open Elasticsearch (no auth):

```
port:9200 json
```

Redis with no auth:

```
product:"Redis" port:6379
```

CouchDB exposed with Fauxton:

```
"Welcome to Fauxton" port:5984
```

Kibana dashboards (elastic):

```
title:"Kibana" port:5601
```

MySQL with root access:

```
product:"MySQL" port:3306
```

♦ 2. Open Cameras / Surveillance
General webcams (MJPEG streams):

```
port:554 has_screenshot:true
```

Axis IP cameras:

```
"Server: Boa/0.94.13" "200 OK"
```

AvTech DVRs (often default creds):

```
port:80 title:"VideoWebServer"
```

RTSP live stream cameras:

```
port:554 state:"open"
```

♦ 3. Login Portals with Weak Configs
Web login panels over HTTP:

```
http.title:"Login" http.html:"password" port:80
```

Admin panels:

```
http.title:"Admin" OR http.title:"Dashboard"
```

PHPMyAdmin interfaces:

```
http.favicon.hash:-293242991
```

Jenkins dashboards (CI/CD):

```
http.title:"Dashboard [Jenkins]"
```

♦ 4. Cloud Storage & Git Exposure
Exposed Git repositories:

```
"Index of /.git"
```

AWS S3 buckets (misconfigured):

```
http.title:"Amazon S3" http.status:200
```

Open FTP servers:

```
port:21 "220" anonymous
```

♦ 5. Industrial Control Systems (ICS)
SCADA HMI interfaces:

```
title:"HMI" port:8080
```

Modbus TCP (danger zone):

```
port:502
```

Hikvision NVR/DVRs:

```
port:8000 Hikvision
```

♦ 6. Miscellaneous Goldmines
Printers leaking documents:

```
port:80 product:"HP" title:"Printer"
```

VOIP phone interfaces:

```
port:80 title:"Cisco IP Phone"
```

VPN gateways (often brute-forceable):

```
title:"GlobalProtect Portal"
```

Apache status pages (info leak):

```
title:"Apache Status" "Server Status"
```

Ethics Reminder

✓ Only use these dorks on assets you own or have explicit permission to test.
✗ Unauthorized access or exploitation is illegal and against ethical guidelines.

2.2 Used the dorks to search on Shodan.

Even though I couldn't find any juicy stuff, I did find some interesting results including login pages.
Here is an example:

```
"Server: Boa/0.94.13" "200 OK" has_screenshot:true
```

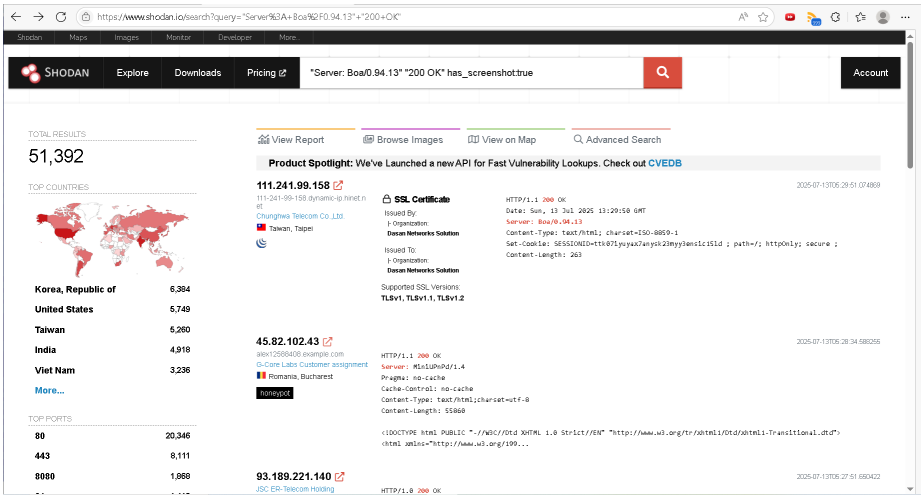

Figure 1: Shodan Search Result Example

Login page:

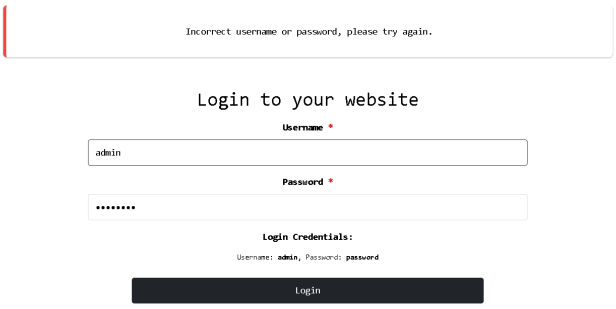

Figure 2: Login Page Example

2.3 Basic Brute Force

- Try using `hydra` or `medusa` to brute force the login page (AT YOUR OWN RISK!!).
- I tried default credentials like `admin:admin`, `root:root`, etc. but it didn't work.

2.4 BONUS

Finally just randomly searching for `"robots.txt"` on Shodan gives some interesting results.

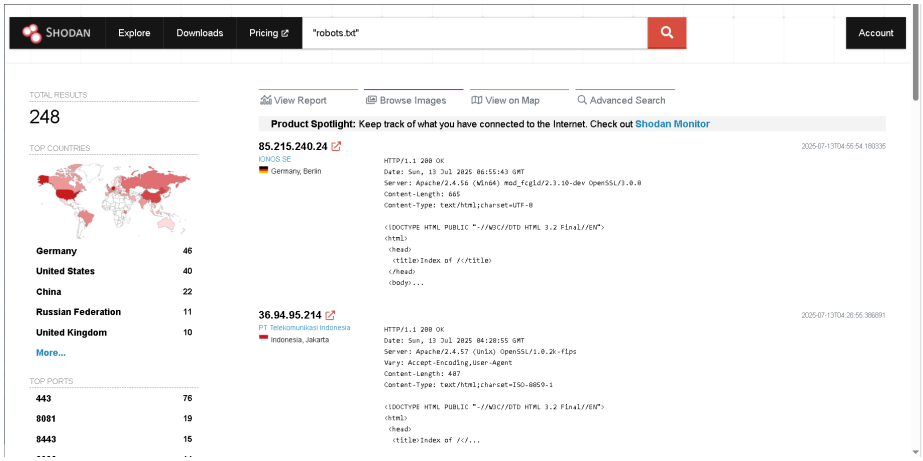

Figure 3: Shodan Search for robots.txt

Got log files:

Figure 4: Log Files Found

Lets see whats inside the log file:

3 Conclusion

This task was a great way to learn about Shodan dorks and how to use them to find interesting stuff on the internet. I learned how to use Shodan dorks to

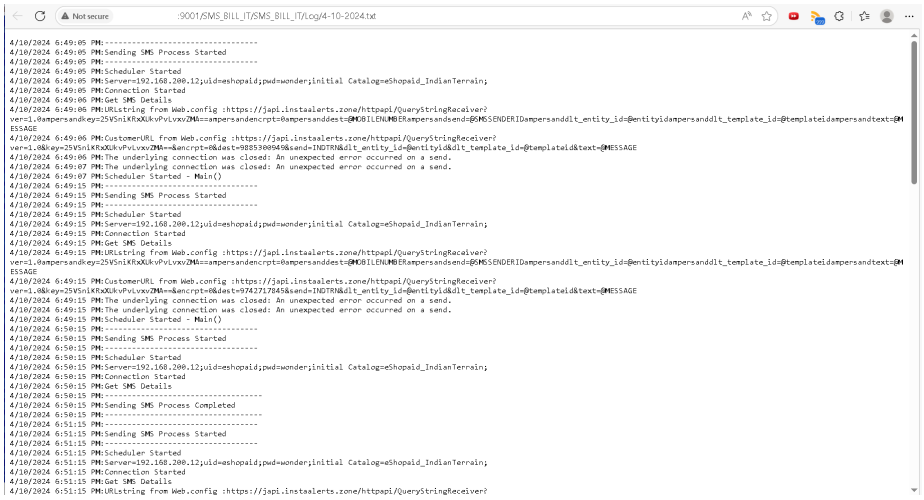

Figure 5: Content of Log File

find login pages, unprotected devices, and other juicy stuff. I also learned how to use hydra and medusa to brute force login pages. Finally, I learned how to search for `robots.txt` files on Shodan and found some interesting results.