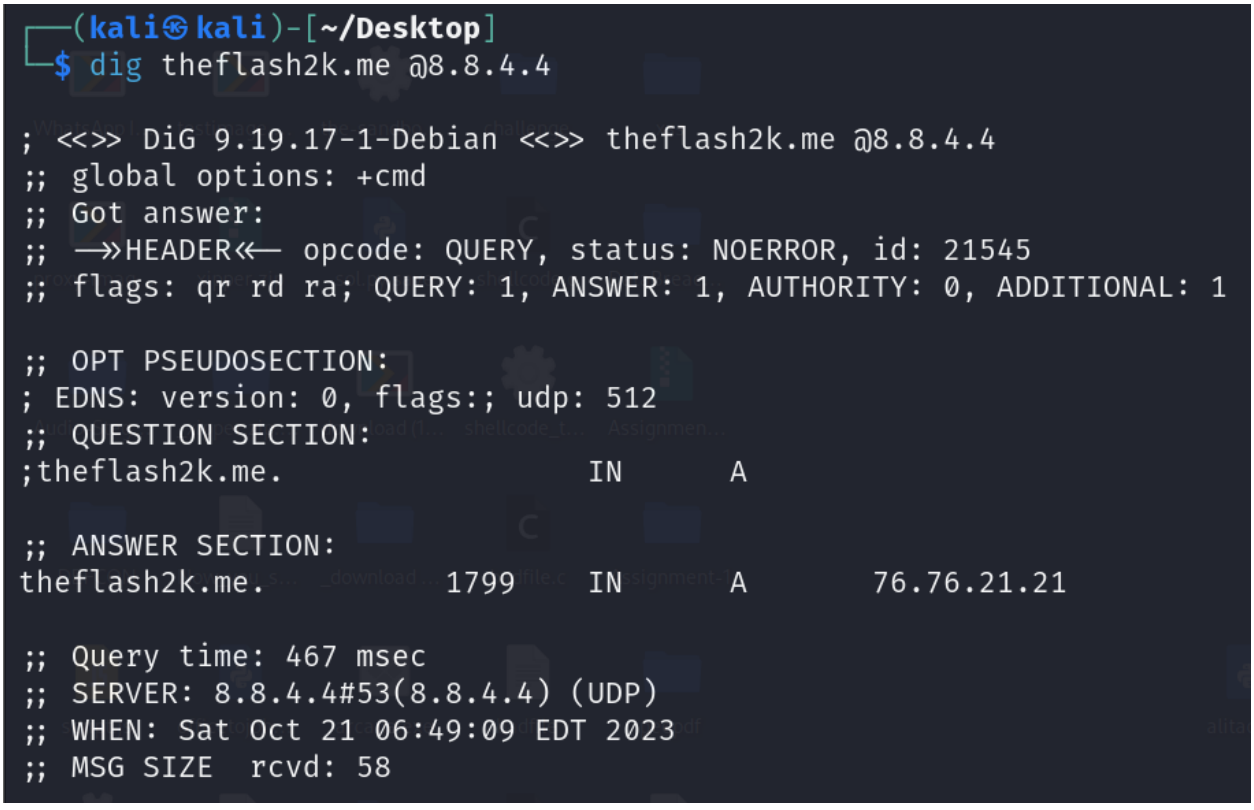
Lab Task 3

⇒ Passive Recon

Task - 1:

Using dig , and 8.8.4.4 as the dns, can you find the IP Address of theflash2k.me ?

```
dig theflash2k.me @8.8.4.4
```

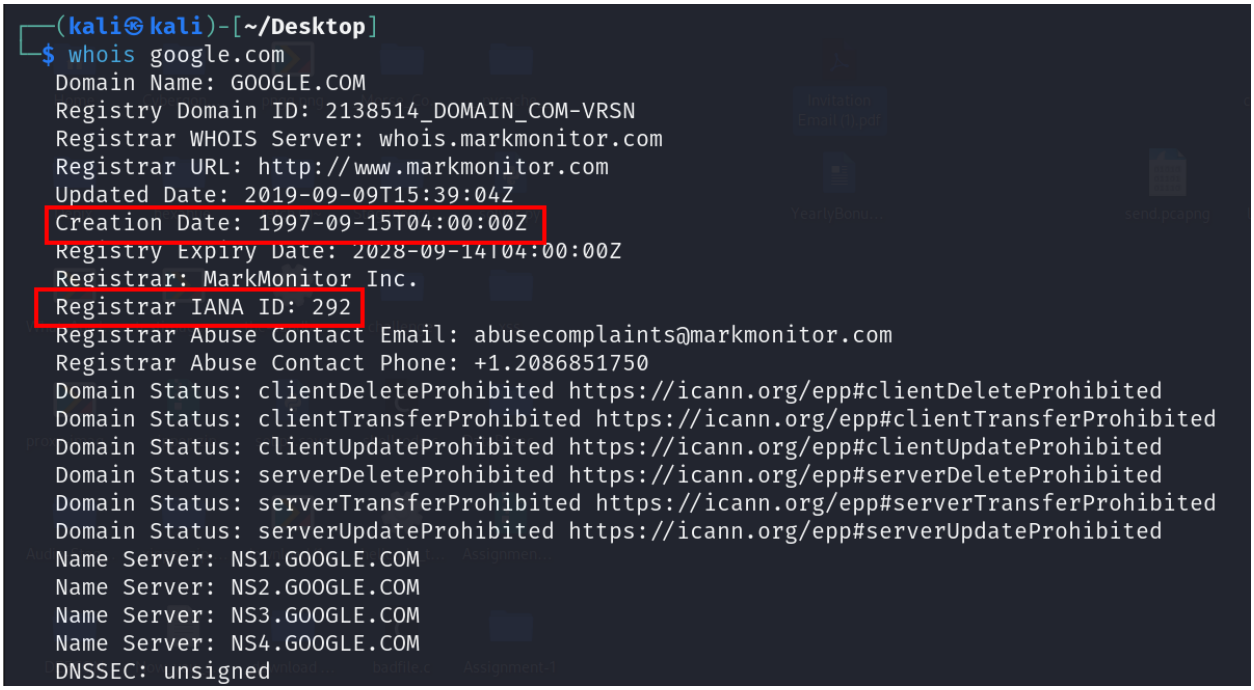


IP address: `76.76.21.21`

Task - 2:

Performing WHOIS Lookup on google.com , what is the Registrar's IANA ID and Creation Date?

```
whois google.com
```



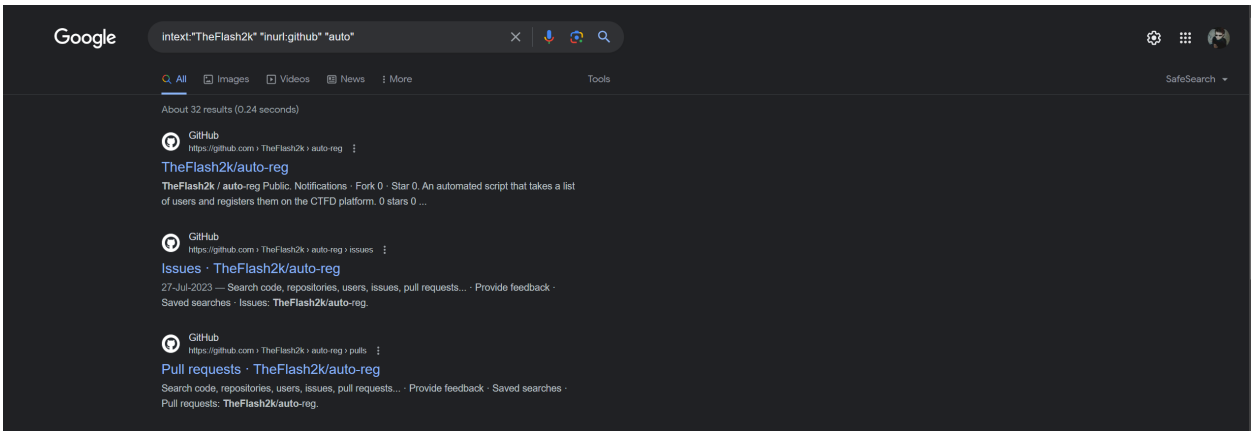
Creation Date: `1997-09-15T04:00:00Z`

Registrar IANA ID: `292`

Task - 3:

Using the following google dork: intext:"TheFlash2k" "inurl:github" , can you find the REPO that contains the word auto ? Modify the dork and answer with the updated dork, and the screenshot + url of the repository found.

```
intext:"TheFlash2k" "inurl:github" "auto"
```



Repository URL: `https://github.com/TheFlash2k/auto-reg`

⇒ Active Recon

Task - 4:

How many ports are open on theflash2k.me . Also, add a screenshot of the service and script scan that you ran against the open ports.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -T4 theflash2k.me
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 06:59 EDT
Nmap scan report for theflash2k.me (76.76.21.21)
Host is up (0.051s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.22 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -T4 theflash2k.me
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 06:59 EDT
Nmap scan report for theflash2k.me (76.76.21.21)
Host is up (0.051s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.22 seconds
```

Task - 5:

Find subdomains of shameerkashif.me

```
subfinder -d shameerkashif.me
```

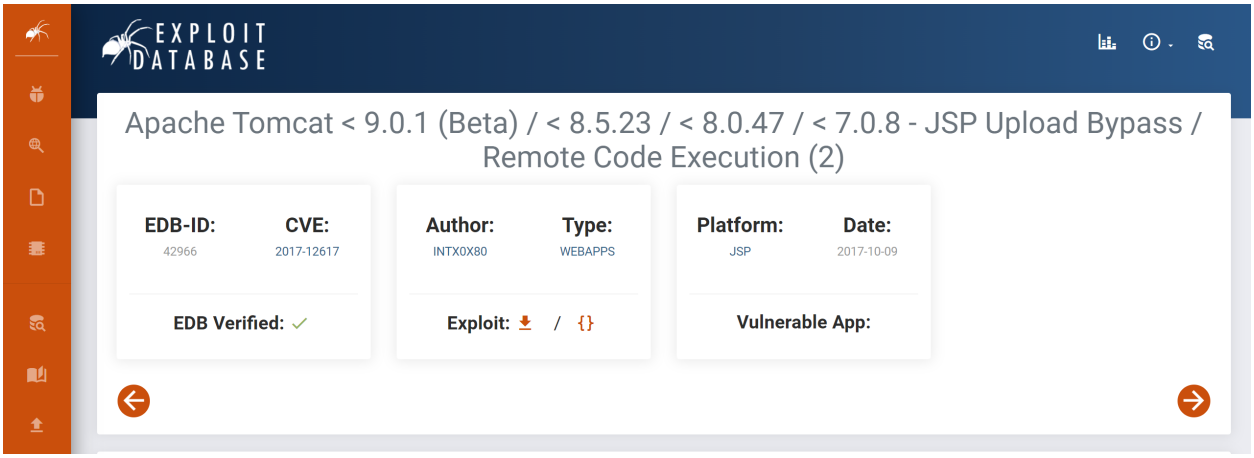
```
┌──(kali㉿kali)-[~/Desktop]
└─$ subfinder -d shameerkashif.me

                     __     _
   _____  __  _____/ /_   (_)___  ____/ /__  _____
  / ___/ / / / / __  / / / / __ \/ __  / _ \/ ___/
 (__  ) / /_/ / /_/ / / / / / / / /_/ /  __/ /
/____/  \__,_/\__,_/_/ /_/_/ /_/\__,_/\___/_/   v2

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Configuration file saved to /home/kali/.config/subfinder/config.yaml
[INF] Enumerating subdomains for shameerkashif.me
blog.shameerkashif.me
```

Subdomain found: `blog.shameerkashif.me`

Task - 6:

Using searchsploit, what is the exact CVE , the Exploit Title and Path for Apache Tomcat JSP Upload Bypass . Answer should be like: CVE-2023, Microsoft Shares < 9.0, jsp/webapps/91251.py

```
┌──(kali㉿kali)-[~/Desktop]
└─$ searchsploit --cve Apache Tomcat JSP Upload Bypass
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - .
------------------------------------------------------------------------
Shellcodes: No Results
```



CVE: `CVE-2017-12617`