

Assignment-2

Bharath Prabhakar

B.Tech

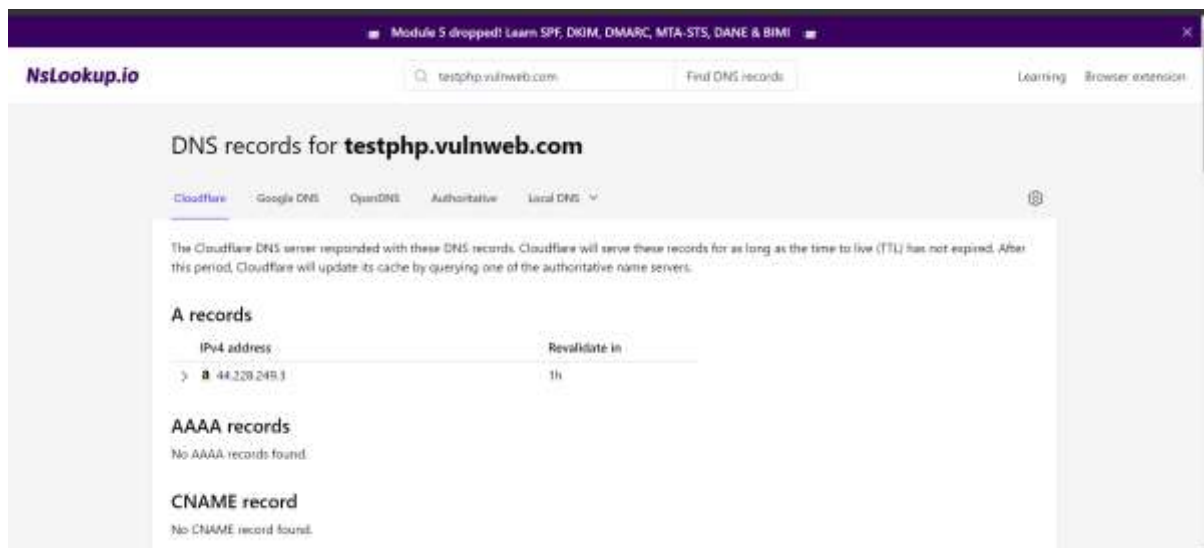
RCEE

Website: <http://testphp.vulnweb.com/>

Step-1: Finding ip address of the website

To find the ip address we can use the NSLOOKUP website

Enter the website url in the search bar of nslook up website then we get

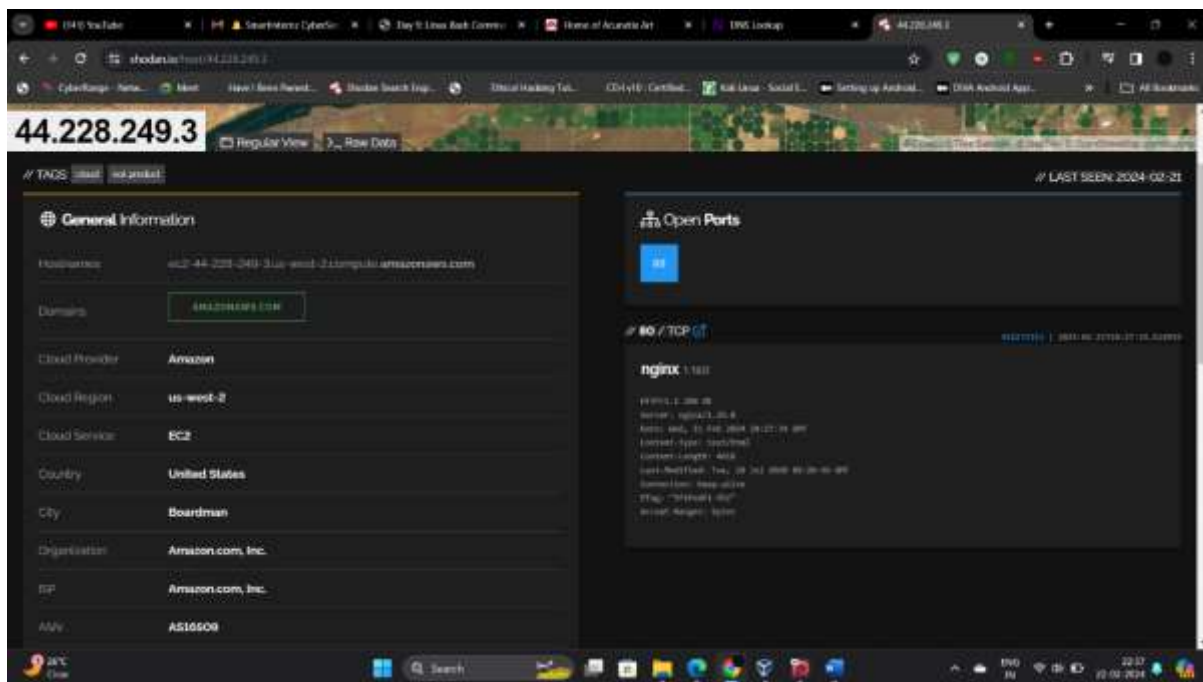


Here we got the ip address of the website that is

Ip: 44.228.249.3

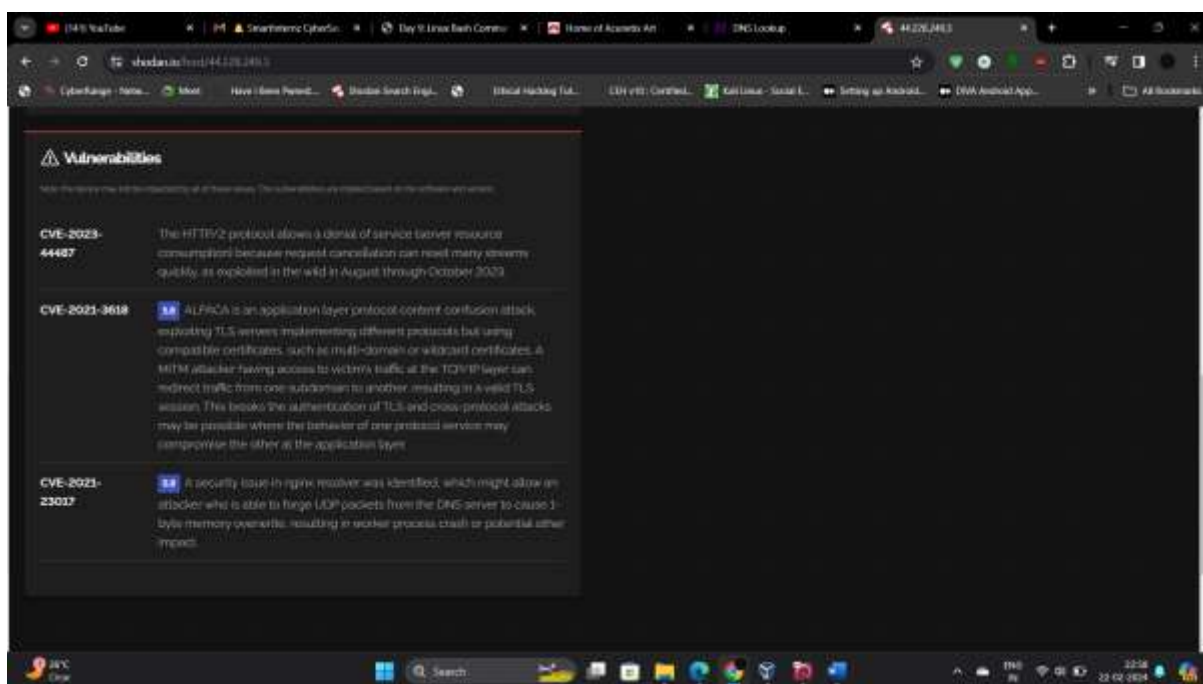
Step-2: To find the information about the website we use the Shodan website

Enter the ip address in the search bar in the shodan then we get



In the above picture we can see the open ports which is

Port: 80



In this picture we can find the vulnerabilities that are in the website

Using Nmap for more information about the website:

Scanning Host in nmap

```
(root@kali)~[/home/bharath]
# nmap -sL 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 07:57 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Nmap done: 1 IP address (0 hosts up) scanned in 12.76 seconds
```

Scanning services or versions in nmap

```
(root@kali)~[/home/bharath]
# nmap -sV 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 07:58 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.048s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.10 seconds
```

Scanning operating system in nmap

```
(root@kali)~[/home/bharath]
# nmap -O 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 08:01 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.033s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.21 seconds
```

Scanning ports in nmap

```
(root@kali)~[/home/bharath]
# nmap -p80 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 08:42 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0085s latency). Close

PORT      STATE SERVICE
80/tcp    filtered http

Nmap done: 1 IP address (1 host up) scanned in 11.63 seconds
```