

DOMAIN SPECIFIC TASK

TOPIC: CYBERSECURITY

NAME: KARTHIKEYA

ROLL NO: 108124135

1 Level 1: Reconnaissance Objective

1.1 Task Overview

Objective: Understand the surface of a web application using reconnaissance tools and manual inspection.

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

Tools Used: nslookup, whois, nmap, whatweb, httpx, ffuf, dirsearch, subfinder, waybackurls, etc.

1.2 IP Address Discovery

Finding the IP address for a website is straightforward. We can use the **host** command in our terminal or use nikto command for more comprehensive information.

Command:

```
host testphp.vulnweb.com
```

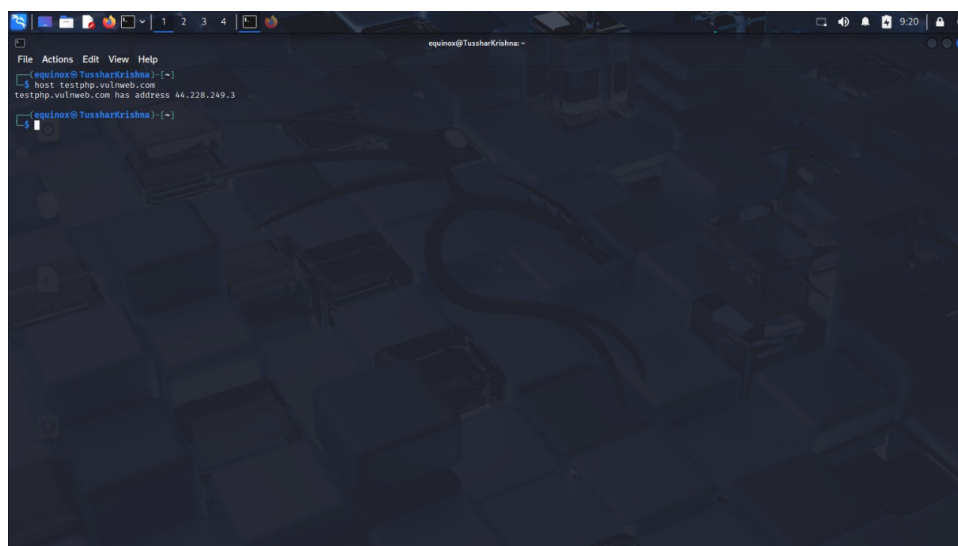


Figure 1: IP Address Discovery using host command

1.3 Subdomain Information

There are multiple methods to extract subdomain information:

1. Using reconnaissance tools like subfinder, sublist3r, amass
2. Online subdomain lookup websites like netcraft, dnsdumpster, **crt.sh (probably the best)**

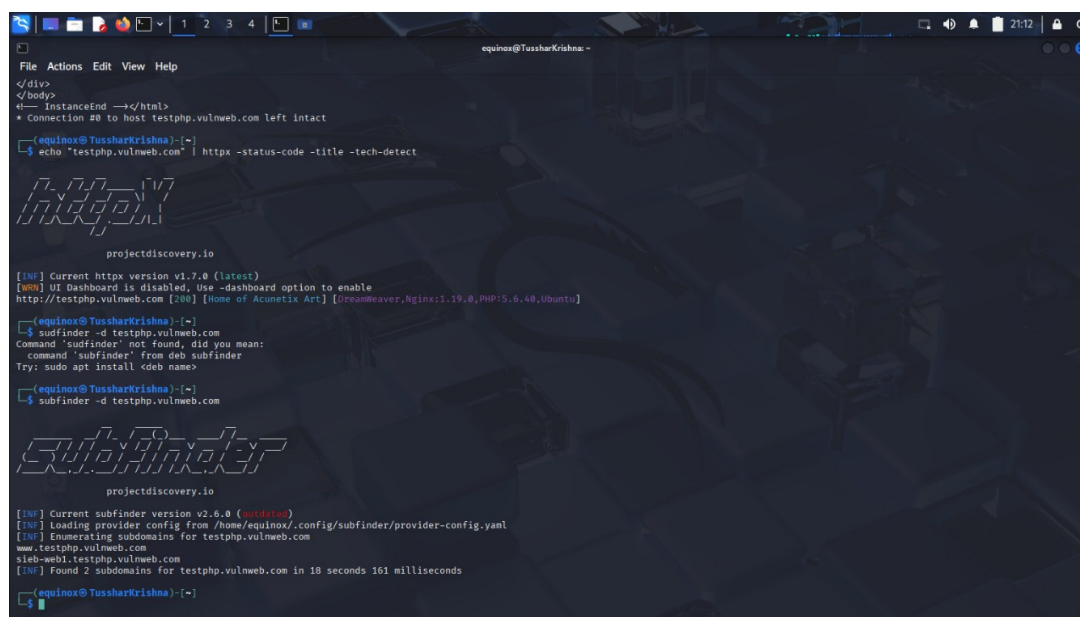
Each method has its advantages and disadvantages. We will perform multiple approaches to gather comprehensive information.

1.3.1 Using Subfinder

Subfinder is a fast, passive subdomain enumeration tool. It gathers subdomains of a target domain by querying various public sources and APIs like VirusTotal, crt.sh, and Shodan. Since it uses passive methods, it doesn't interact directly with the target, making it stealthy and suitable for reconnaissance.

Command:

```
subfinder -d testphp.vulnweb.com
```



```
equinox@TussharKrishna:~$ subfinder -d testphp.vulnweb.com
projectdiscovery.io

[INF] Current subfinder version v2.6.0 (runner)
[INF] Loading provider config from /home/equinox/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for testphp.vulnweb.com
www.testphp.vulnweb.com
subweb1.testphp.vulnweb.com
[INF] Found 2 subdomains for testphp.vulnweb.com in 18 seconds 161 milliseconds
```

Figure 2: Subdomain enumeration using Subfinder

Note: Using tools like this won't always give perfect results, so it's good to use multiple methods and cross-verify.

Note: Subfinder is a passive reconnaissance tool.

1.3.2 Using Online Lookups

Using websites like crt.sh, we can find subdomains of the target.

Method: Simply search crt.sh and type in the target domain name.

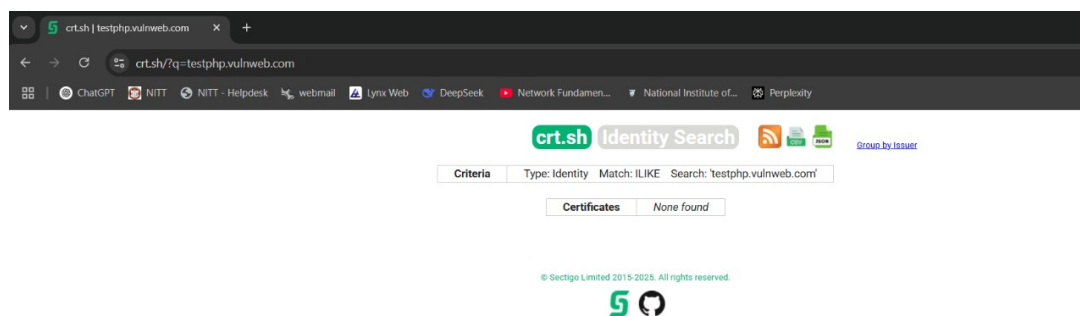


Figure 3: Subdomain lookup using crt.sh

Result: We didn't get any subdomains from crt.sh. However, we obtained 2 subdomains from subfinder. This is because subfinder is a passive recon tool that searches the web (subdomain dumps and public sources, public APIs) for subdomains. The subdomain might have been removed and crt.sh updated its database, while subfinder found the old subdomain from other resources.

We can verify this using amass:

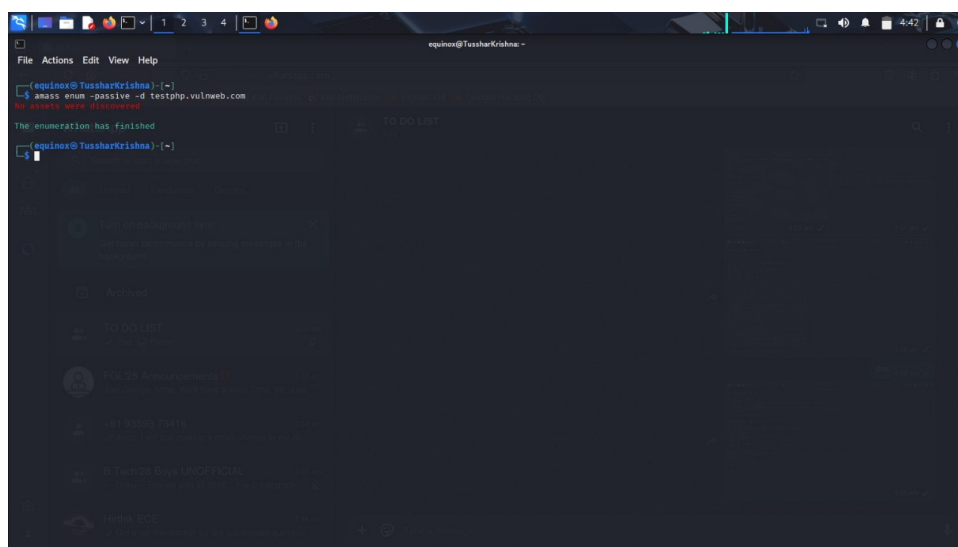


Figure 4: Verification using Amass

1.4 Tech Stack Information

1.4.1 What is Tech Stack?

Tech stack is the underlying software of a website, generally consisting of four parts:

- Web servers (e.g., Apache, Nginx)
- Backend frameworks (e.g., Django, Node.js)
- Databases (e.g., MySQL, MongoDB)
- Security tools (e.g., Cloudflare WAF)

In cybersecurity context, finding this crucial information can be advantageous for an attack. Various reconnaissance tools can be used:

1. curl
2. whatweb
3. httpx (and many more - each tool has its own advantages and disadvantages)

Commands used:

```
curl -v http://testphp.vulnweb.com
whatweb testphp.vulnweb.com
echo "testphp.vulnweb.com" | httpx -status-code -title -tech-detect
```

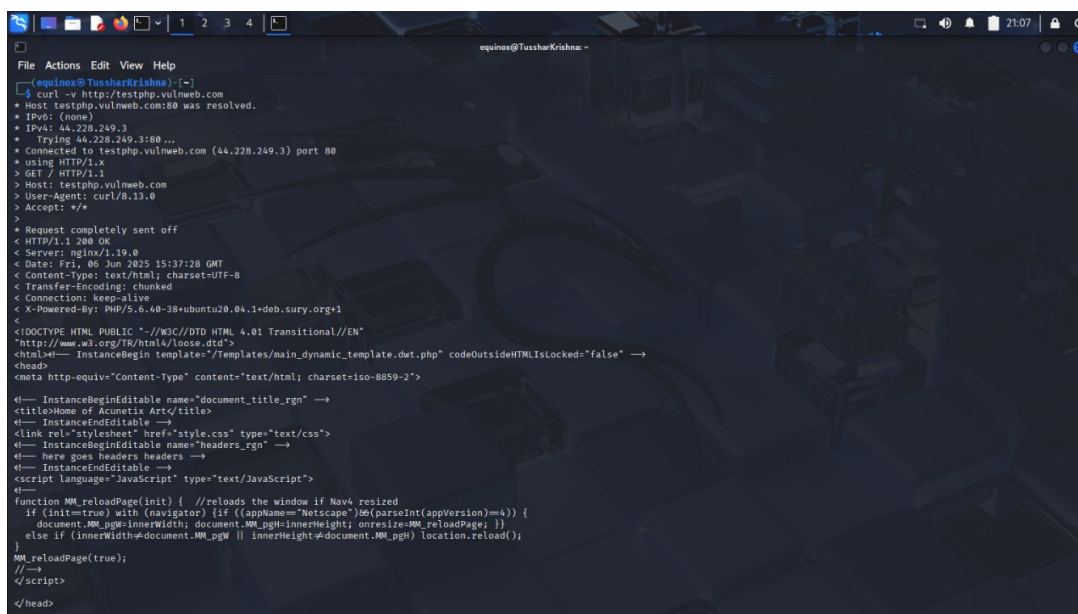


Figure 5: Tech stack analysis using multiple tools

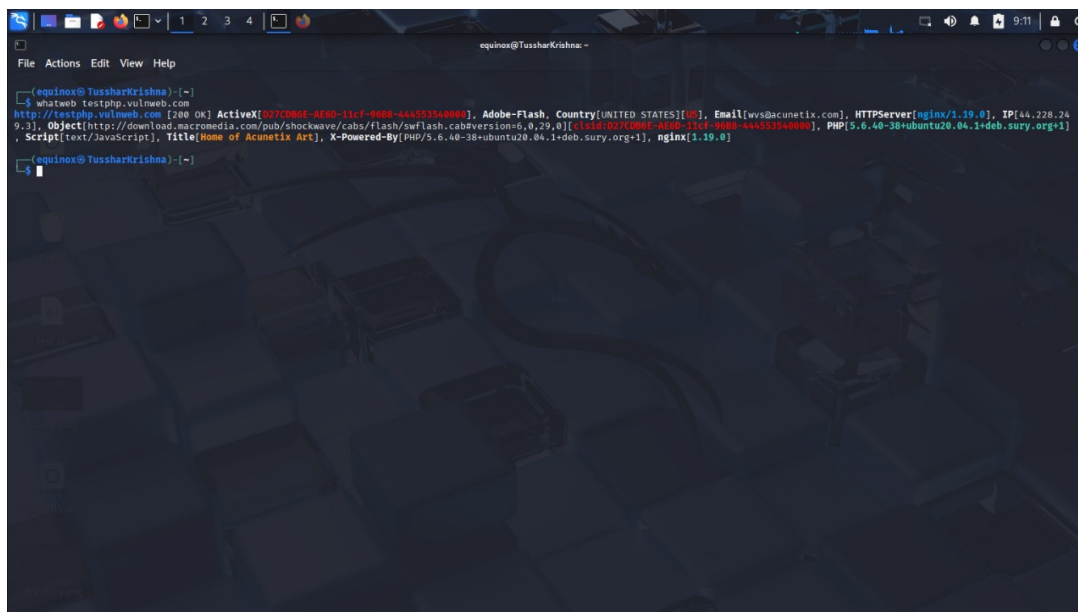


Figure 6: Additional tech stack information

1.4.2 Results of the Reconnaissance

Server

- Nginx 1.19.0 (Web server)

Backend

- PHP 5.0.40 (Outdated, insecure)

Database

- We can use nmap to find it: `nmap -p 3306,5432,1433,2707 -sV`

Frontend

- JavaScript (Client-side)
- Adobe Flash (Deprecated, insecure)

1.5 Open Ports and Services

To find open ports and services, we use the nmap tool with appropriate modes (-sS, -sV).

Command used:

```
nmap -sV testphp.vulnweb.com
```

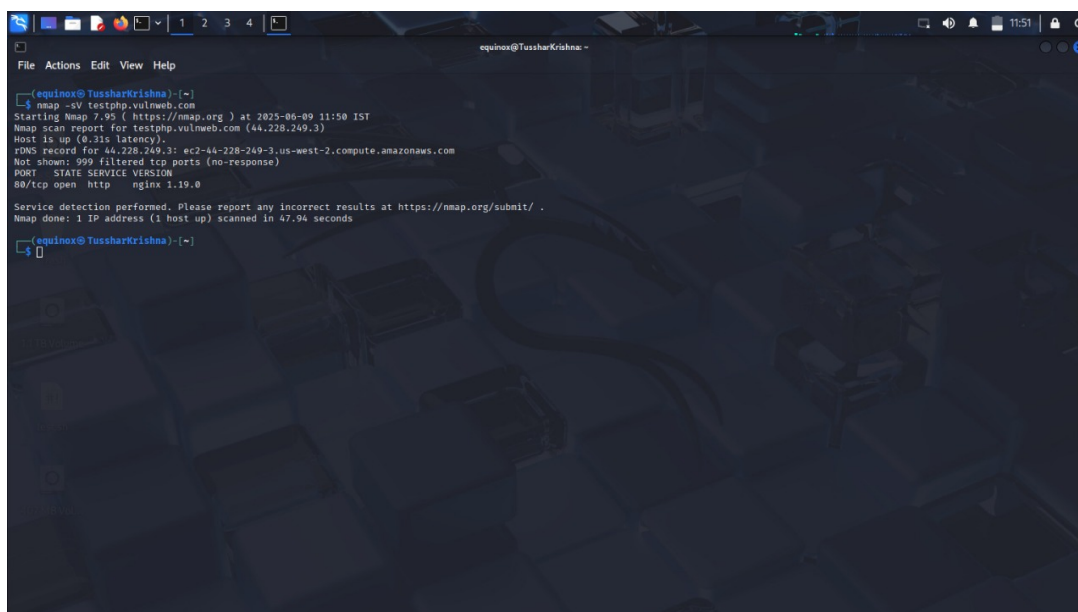


Figure 7: Port scanning results using nmap

1.6 Directory Structure

To find the directory structure, we use the ffuf tool, which is an active reconnaissance tool using brute force techniques.

Command used:

```
ffuf -u http://testphp.vulnweb.com/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-lowercase.txt
```

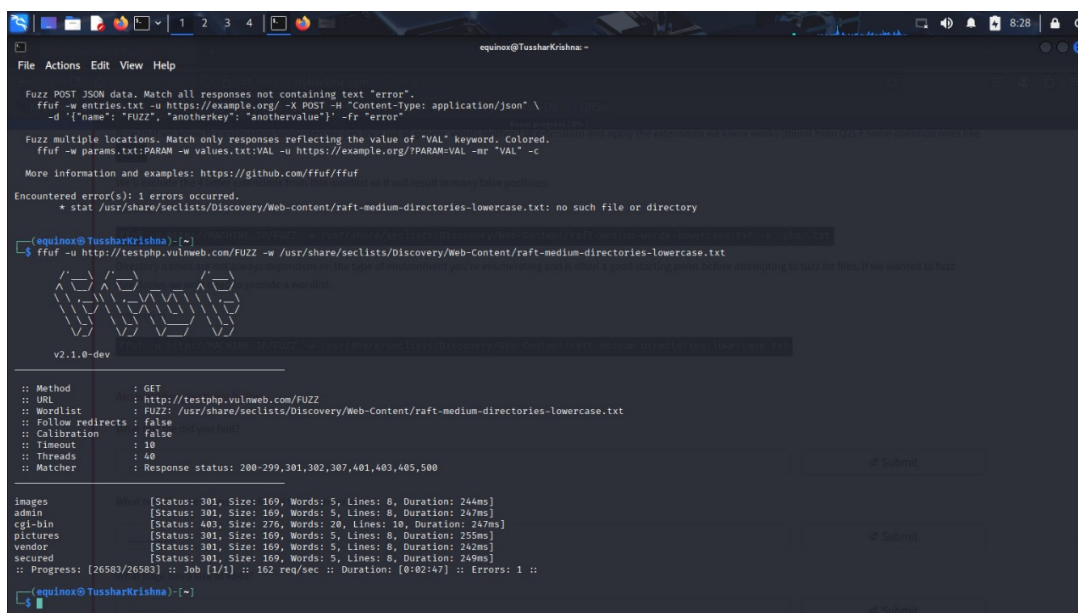


Figure 8: Directory enumeration using ffuf

Reference: TryHackMe ffuf module

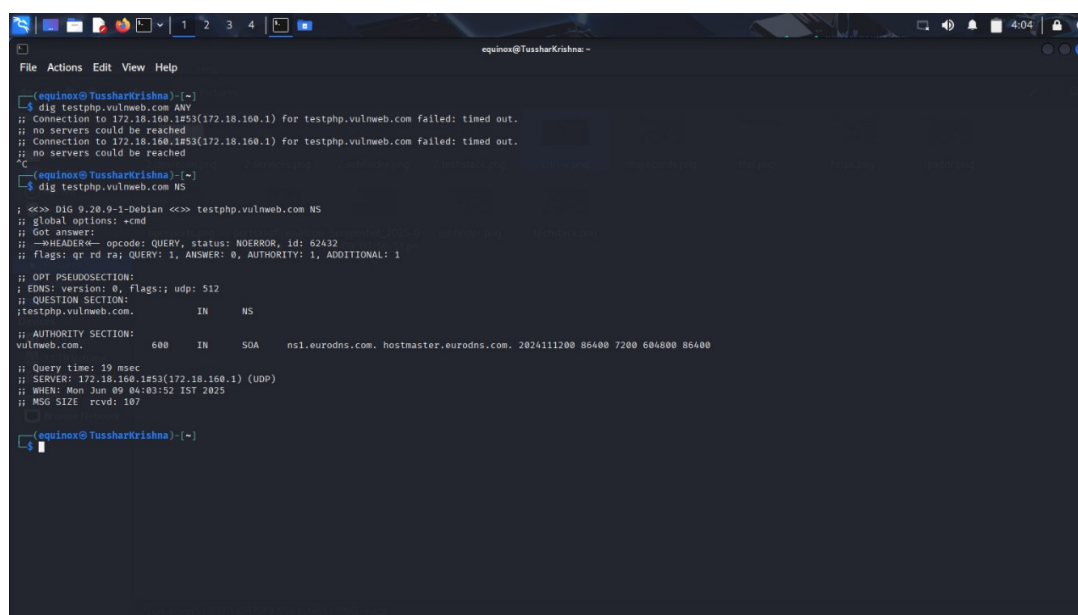
1.7 DNS Information

We can find DNS information using tools like `dnsrecon` and `dig` (passive recon tools). There are also active recon tools like `fierce`, which work on a combination of zone transfer exploitation and subdomain brute forcing.

1.7.1 Zone Transfer

In layman terms, DNS servers request other DNS servers for their database to maintain consistency across all DNS servers. **If the DNS servers are not AXFR restricted, we can request the DNS server for the data!**

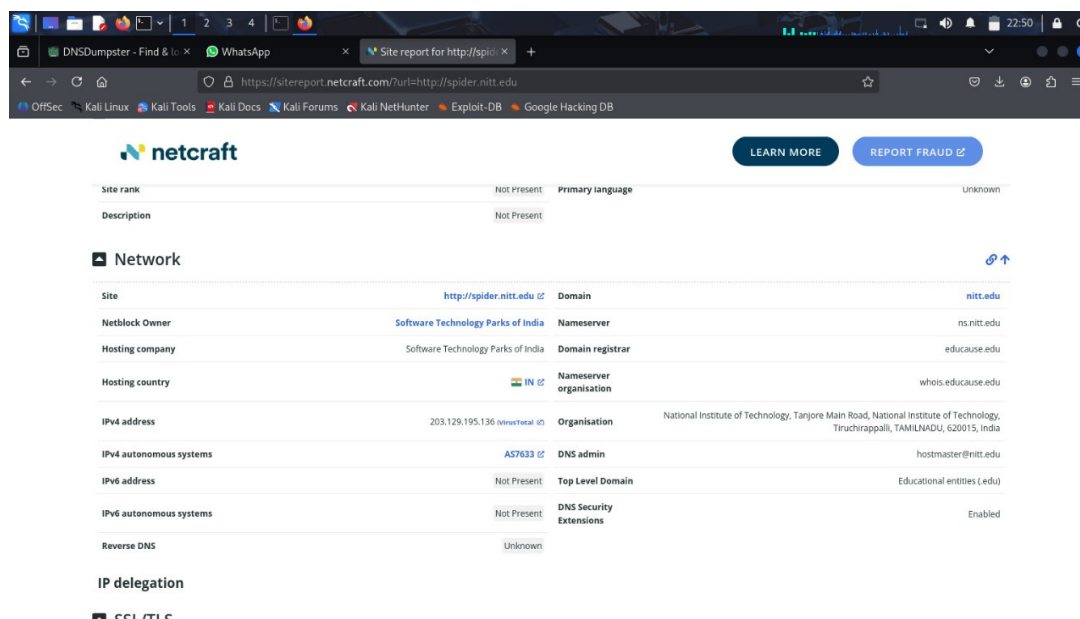
We use this vulnerability to get DNS records:

A screenshot of a terminal window titled 'equinox@TussharKrishna: ~'. The user has entered the command 'dig testphp.vulnweb.com ANY'. The output shows connection failures to 172.18.160.1 and 172.18.160.153. Then, the user enters 'dig testphp.vulnweb.com NS'. The output shows a successful query to 172.18.160.153, returning NS records for 'ns1.eurodns.com' and 'hostmaster.eurodns.com'.

```
equinox@TussharKrishna: ~  
$ dig testphp.vulnweb.com ANY  
;; Connection to 172.18.160.153(172.18.160.1) for testphp.vulnweb.com failed: timed out.  
;; no servers could be reached  
;; Connection to 172.18.160.153(172.18.160.1) for testphp.vulnweb.com failed: timed out.  
;; no servers could be reached  
^C  
equinox@TussharKrishna: ~  
$ dig testphp.vulnweb.com NS  
; <<>> DIG 9.20.9-1-Debian <<> testphp.vulnweb.com NS  
;; global options: +cmd  
;; Got answer:  
;; --HEADER-- opcode: QUERY, status: NOERROR, id: 62432  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
; testphp.vulnweb.com.      IN      NS  
  
;; AUTHORITY SECTION:  
vulnweb.com.      600     IN      SOA     ns1.eurodns.com. hostmaster.eurodns.com. 2024111200 86400 7200 604800 86400  
  
;; Query time: 19 msec  
;; SERVER: 172.18.160.153(172.18.160.1) (UDP)  
;; WHEN: Mon Jun 09 04:03:52 IST 2025  
;; MSG SIZE rcvd: 107  
equinox@TussharKrishna: ~
```

Figure 9: DNS zone transfer attempt

We can also use online DNS lookup tools like `netcraft` and `dnsdumpster` to see more about the DNS servers and their underlying structure:



netcraft		LEARN MORE	REPORT FRAUD
Site rank	NOT PRESENT	Primary language	Unknown
Description	Not Present		
Network			
Site	http://spider.nitt.edu	Domain	nitt.edu
Netblock Owner	Software Technology Parks of India	Nameserver	ns.nitt.edu
Hosting company	Software Technology Parks of India	Domain registrar	educase.edu
Hosting country	IN	Nameserver organisation	whois.educase.edu
IPv4 address	203.129.195.136	Organisation	National Institute of Technology, Tanjore Main Road, National Institute of Technology, Tiruchrappali, TAMILNADU, 620015, India
IPv4 autonomous systems	AS7633	DNS admin	hostmaster@nitt.edu
IPv6 address	Not Present	Top Level Domain	Educational entities (.edu)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled
Reverse DNS	Unknown		
IP delegation			

Figure 10: DNS information from online tools

1.8 Difference Between Active and Passive Reconnaissance

Active and passive reconnaissance are two approaches used in information gathering during cybersecurity assessments:

- **Active Reconnaissance:** Involves directly interacting with the target system, such as sending requests or probing ports, which can be detected by the target (e.g., using **Nmap** to scan open ports).
- **Passive Reconnaissance:** Gathers information without directly engaging with the target, often using third-party sources or public data (e.g., using **crt.sh** to find subdomains).

While active recon provides more detailed data, passive recon is stealthier and less likely to trigger alarms.

2 Level 3: Reconnaissance on the Spider Server

2.1 Task Overview

Apply knowledge from Level 1 & 2 on the Spider Server.

Objectives:

- Find IP address, OS, and tech stack
- Identify services in use
- Discover hidden subdomains
- Find one subdomain that hosts an intentionally vulnerable app and attempt exploitation

2.2 IP Address, OS and Tech Stack

Using nikto for comprehensive information on IP address and more:

Command used:

```
nikto -h spider.nitt.edu
```

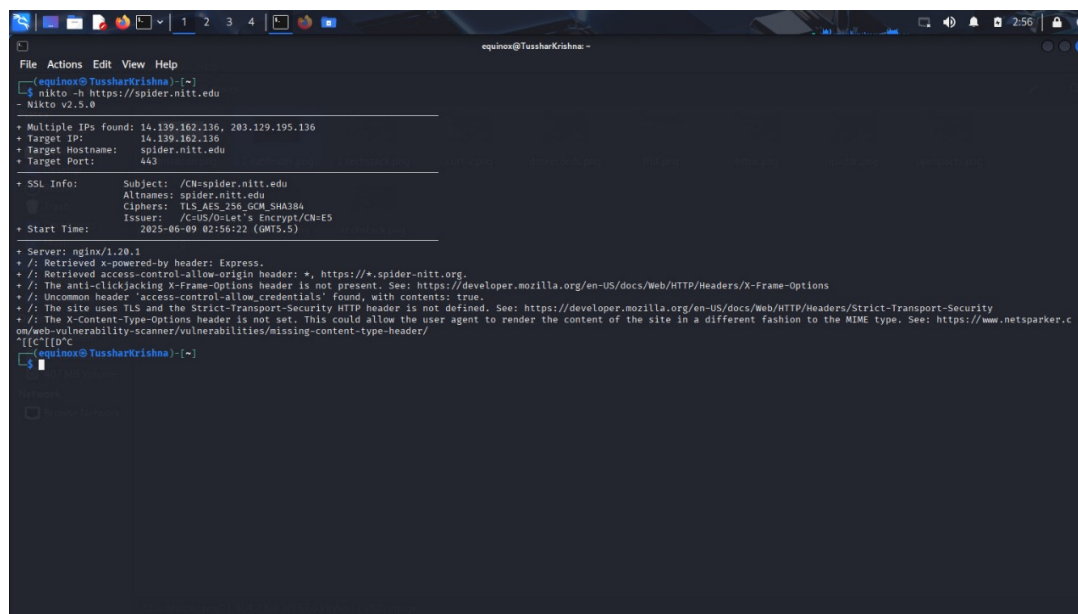


Figure 11: Nikto scan results for spider.nitt.edu

2.3 OS and Tech Stack Analysis

Using whatweb and netcraft for DNS information:

Command used:

```
whatweb -v spider.nitt.edu
```

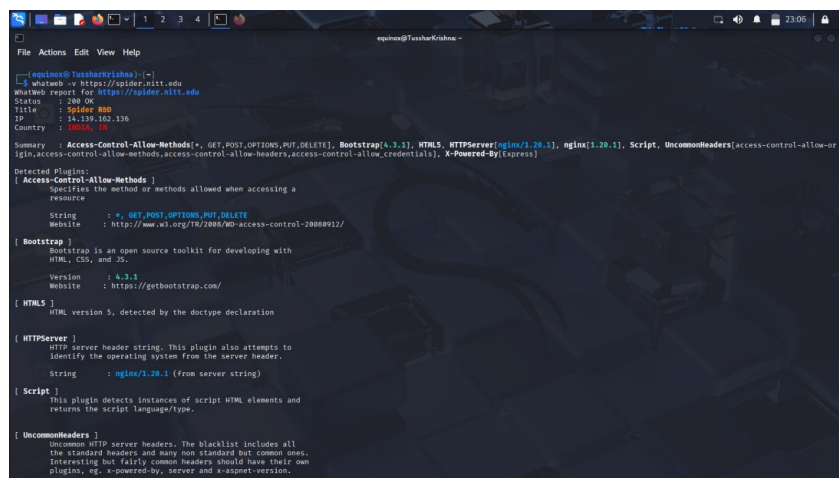


Figure 12: Comprehensive tech stack analysis using whatweb