Fingerprint Web Server

A web server is software like Apache, Nginx, IIS, Lighttpd that delivers web pages when you visit a website. Fingerprinting = finding out which server & version is running.

Why is this important?

- If the server is old, it may have known vulnerabilities (CVEs).
- Example: Apache 2.4.49 had a Remote Code Execution bug (CVE-2021-41773).
- If we know the version, we can look up exploits.

How do we fingerprint?

We ask the server questions and watch how it responds:

1. **Banner grabbing** → "What server are you?" (sometimes it answers directly).
2. **Header ordering** → If it hides its name, we check the order of response headers.
3. **Malformed requests** → We send broken requests and check the error page style (different servers show different error pages).
4. **Tools** → Instead of doing everything manually, tools like Nmap, Nikto, Httprint, Httprecon do this automatically.

Manual Testing Step-by-Step

Step 1: Banner Grabbing

Run:

curl -I http://target.com

- If you see: Server: Apache/2.4.41 → server = Apache 2.4.41.
- If Server: is missing → go to next steps.
- -I means "only get headers, not full page."

Step 2: Using Telnet

Connect manually:

1) telnet target.com 80

2) GET / HTTP/1.1

Host: www.irisflorists.com

Press enter twice

- Server will send back headers (same idea as curl, but raw).

- Connect directly to the website using **telnet**.
- You type an HTTP request yourself to see **raw headers**.
- The website sends headers back.
- You can see **Server**, **Content-Type**, **Date**, etc.
- Helps when `curl` doesn't show server info.

Step 3: HTTPS Servers

If the site uses HTTPS:

For **HTTPS websites**, telnet can't connect directly.

Use **OpenSSL** to connect securely and read headers.

You see headers like server: LiteSpeed.

Confirms the server type even on **secure websites**.

1)openssl s_client -connect target.com:443

2) GET / HTTP/1.1

Host: www.irisflorists.com

Step 4: Malformed Requests (Error Response Check)

What it is:

Send a wrong or broken request to see how the server responds.

- The server shows an error page.
- Different servers show different styles of error pages:
    - LiteSpeed → 400 Bad Request
    - Nginx → 404 page with nginx/x.x
    - Apache → 400 Bad Request with Apache info

Why it's useful:

- Even if the server hides its type in headers, the error page style can give clues.

Command:

telnet www.irisflorists.com 80

Type an invalid request:

GET / INVALID/1.1

Host: www.irisflorists.com

Automated Testing Step-by-Step

Step 1: Nmap

```
nmap -sV -p 80,443 target.com
```

- Tells you service + version.
- Example: Apache httpd 2.4.41 ((Ubuntu)).

Step 2: Nikto

```
nikto -h http://target.com
```

- Shows server version + lists known vulnerabilities.

Step 3: Httprint

```
httprint -h http://target.com -s signatures.txt
```

- Uses header ordering + signatures to identify server.

Step 5: Desenmascarame (online)

Enter the target URL → detects the real server even if headers are fake.

```
https://desenmascarame.org/
```

Step 6: Netcraft (online)

Enter domain → shows web server type, OS, and history.

```
https://www.netcraft.com/
```