Lab_6

1. Who is the domain registrar of www.manipal.edu?

Whois Identity for everyone Domains Hosting Servers Email Security Whois Deals

```
--------------------------------------------------------------

Domain Name: MANIPAL.EDU

Registrant:
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India

Administrative Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Technical Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu
```

2. What is the domain creation date?

DOMAIN AGE CHECKER

#	Value
Domain	Manipal.edu
Domain Age	25 Years, 144 Days
Domain Created Date	27th-Sep-1999
Domain Updated Date	21st-Oct-2024
Domain Expiry Date	31st-Jul-2025

3. What is the expiration date of the domain?

DOMAIN AGE CHECKER

#	Value
Domain	Manipal.edu
Domain Age	25 Years, 144 Days
Domain Created Date	27th-Sep-1999
Domain Updated Date	21st-Oct-2024
Domain Expiry Date	31st-Jul-2025

4. Identify the name servers associated with the domain.

```
Name Servers:
        NS1-36.AZURE-DNS.COM
        NS3-36.AZURE-DNS.ORG
        NS4-36.AZURE-DNS.INFO
        NS2-36.AZURE-DNS.NET

Domain record activated:    27-Sep-1999
Domain record last updated: 21-Oct-2024
Domain expires:             31-Jul-2025
```

5. Is there any contact email provided for administrative or technical support?

```
Administrative Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Technical Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu
```

6. What country is the domain registered in?

Whois Identity for everyone Domains Hosting Servers Email Security Whois Deals

```
--------------------------------------------------------------

Domain Name: MANIPAL.EDU

Registrant:
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India

Administrative Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Technical Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu
```

ANS: India

7. Run a WHOIS query for example.com and check if the registrant's details (name, address, email) are visible.

Whois Identity for everyone Domains Hosting Servers Email Security Whois Deals

```
The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

--------------------------------------------------------------

Domain Name: MANIPAL.EDU

Registrant:
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India

Administrative Contact:
        Domain Admin
        Manipal Academy of Higher Education
```

Whois Identity for everyone Domains Hosting Servers Email Security Whois Deals

```
Administrative Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Technical Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Name Servers:
        NS4-36.AZURE-DNS.INFO
        NS2-36.AZURE-DNS.NET
        NS3-36.AZURE-DNS.ORG
        NS1-36.AZURE-DNS.COM

Domain record activated:    27-Sep-1999
Domain record last updated: 21-Oct-2024
Domain expires:             31-Jul-2025
```

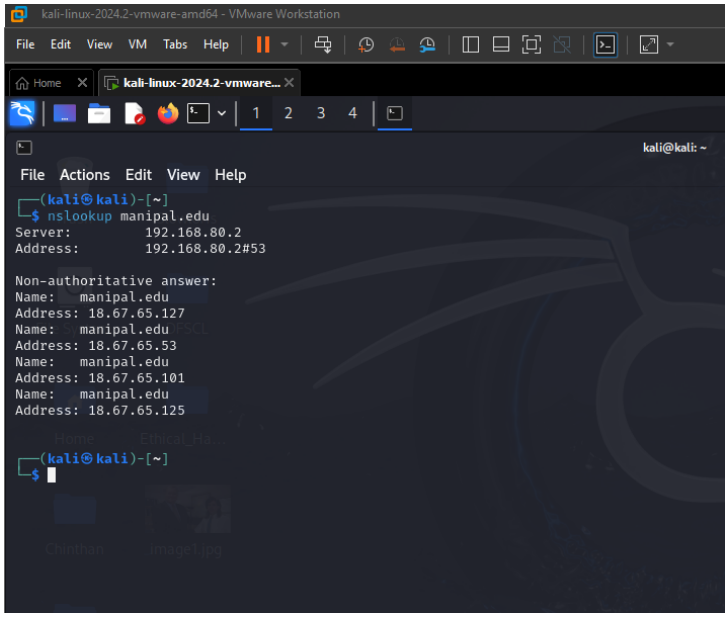
8. If privacy protection is enabled, what information is displayed instead of actual owner details?

   ANS: The actual registrant details (name, address, email, phone number) are replaced with generic or anonymized information provided by the domain registrar's privacy service.

9. What are the security implications of exposing or hiding data?

   ANS: Exposing WHOIS data increases risks like phishing, spam, and domain hijacking but improves transparency, while hiding it enhances privacy and security but may reduce trust and hinder cybercrime investigations.

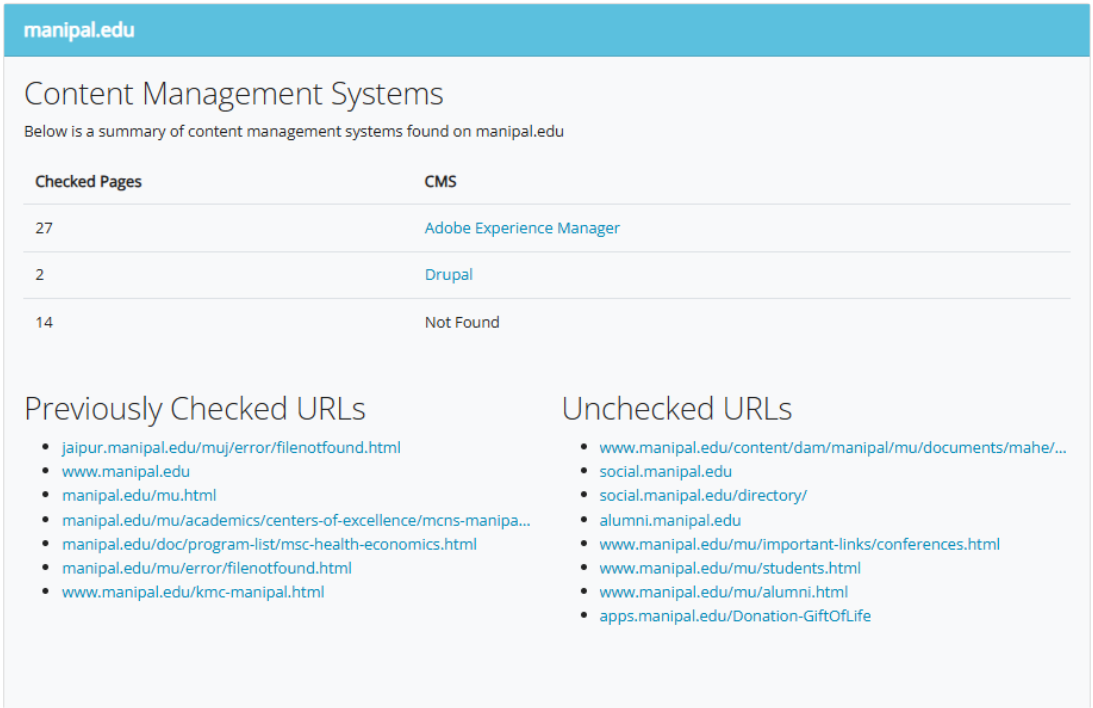
10. Look for Name Server (NS) records and associated domains.



11. what are the different methods to find the subdomain using both passive and active methods

    ANS: Passive methods like WHOIS lookup, Certificate Transparency Logs (crt.sh), and Google Dorking help find subdomains without directly interacting with the target. Active methods like Brute Force (Gobuster, Sublist3r), DNS Zone Transfer, and DNS Enumeration (dig, nslookup) involve direct queries to discover subdomains.

12. Identify CMS (WordPress, Joomla, etc.) and frameworks used.



manipal.edu

Content Management Systems

Below is a summary of content management systems found on manipal.edu

Checked Pages	CMS
27	Adobe Experience Manager
2	Drupal
14	Not Found

Previously Checked URLs

- jaipur.manipal.edu/muj/error/filenotfound.html
- www.manipal.edu
- manipal.edu/mu.html
- manipal.edu/mu/academics/centers-of-excellence/mcns-manipa...
- manipal.edu/doc/program-list/msc-health-economics.html
- manipal.edu/mu/error/filenotfound.html
- www.manipal.edu/kmc-manipal.html

Unchecked URLs

- www.manipal.edu/content/dam/manipal/mu/documents/mahe/...
- social.manipal.edu
- social.manipal.edu/directory/
- alumni.manipal.edu
- www.manipal.edu/mu/important-links/conferences.html
- www.manipal.edu/mu/students.html
- www.manipal.edu/mu/alumni.html
- apps.manipal.edu/Donation-GiftOfLife

✓ Success JSON

www.manipal.edu/mu.html uses

Category	Software	Version
Other CMS, CMS	Adobe Experience Manager	
Programming Language	Java	
CDN	Amazon CloudFront	
Web Server	Apache HTTP Server	

Social Media

Network	Profile	Url
Twitter	mahe_manipal	https://twitter.com/mahe_manipal
Facebook	mahemanipal	https://www.facebook.com/mahemanipal/
Instagram	mahe_manipal	http://www.instagram.com/mahe_manipal/

Help us improve these results

13. Compare whatweb and wappalyzer

ANS:

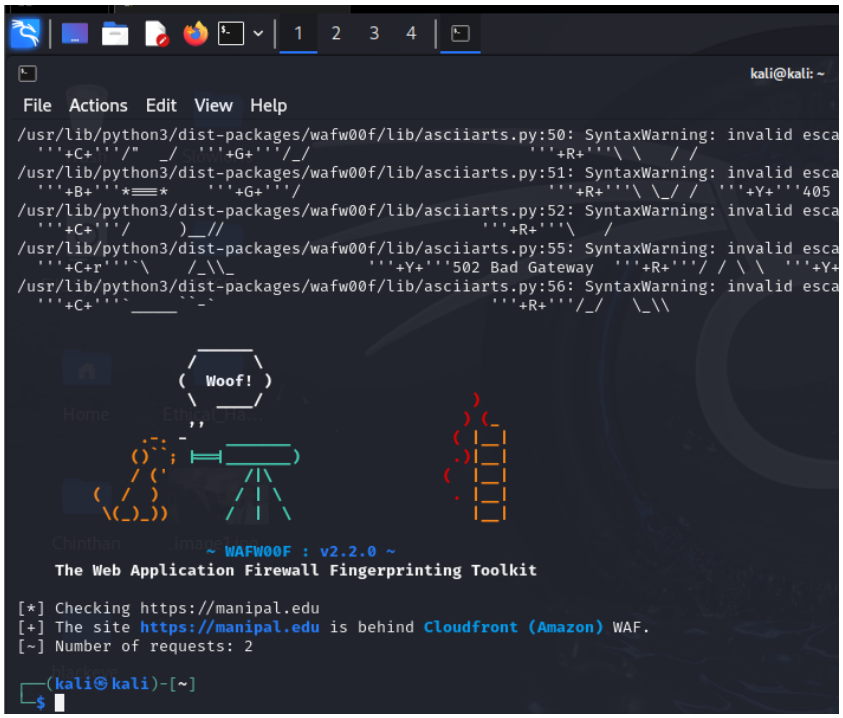
- **Purpose & Usage** – WhatWeb is designed for penetration testing and cybersecurity, while Wappalyzer is a user-friendly tool for general web technology identification.
- **Detection Method** – WhatWeb supports both active and passive scanning, whereas Wappalyzer is purely passive and does not interact with the target website.
- **Output & Analysis** – WhatWeb provides detailed technical data, including potential security risks, while Wappalyzer presents categorized, easy-to-read results suitable for research.

14. Fetch the HTTP Header (Many methods are available). Identify the tools used to find HTTP Header details

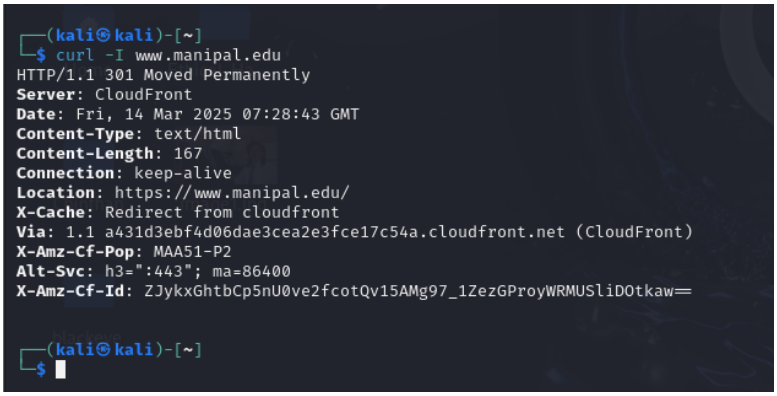
```
┌──(kali㉿kali)-[~]
└─$ curl -I www.manipal.edu
HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Fri, 14 Mar 2025 07:28:43 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
Location: https://www.manipal.edu/
X-Cache: Redirect from cloudfront
Via: 1.1 a431d3ebf4d06dae3cea2e3fce17c54a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: MAA51-P2
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: ZJykxGhtbCp5nU0ve2fcotQv15AMg97_1ZezGProyWRMUSliDOtkaw==

┌──(kali㉿kali)-[~]
└─$
```

15. Check whether domain have firewall installed or not



16. do they have load balancer



17. Search for exposed environment configuration files

ANS: curl -s -X GET http://<target>/.env

18. Look for log files that may contain sensitive information

ANS: find / -name "*.log" 2>/dev/null

19. Find database backup files

    ANS: **curl -s -X GET http://<target>/backup.sql**

20. Find live camera feeds

    ANS: **nmap -p 554 --script rtsp-url-brute <target>**

21. Search for open IoT device

    ANS: **nmap -p 23,554,81 --open <target>**