Who is the domain registrar of [www.manipal.edu](http://www.manipal.edu)?

The **registrar** information is not explicitly mentioned in the WHOIS data. However, since the domain **MANIPAL.EDU** has a **.EDU** extension, it is most likely registered through **Educause**, the exclusive registrar for **.EDU** domains.

Registrant:

Manipal Academy of Higher Education

Madhav Nagar

Manipal, Karnataka 576104

India

What is the domain creation date?

27-Sep-1999

What is the expiration date of the domain?

31-Jul-2025

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

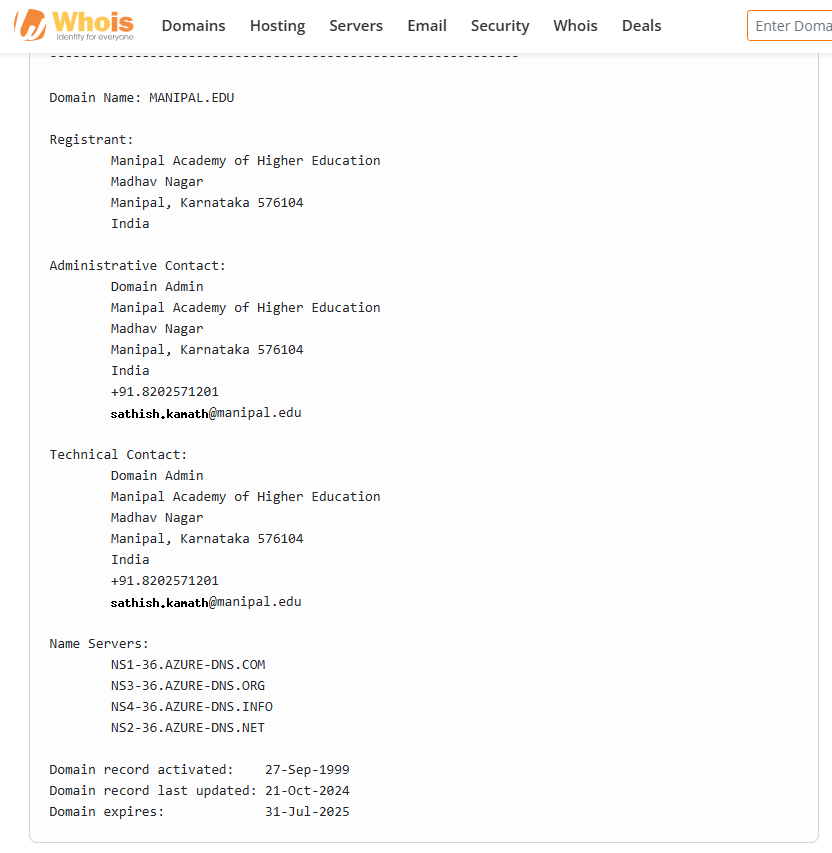
NS2-36.AZURE-DNS.NET

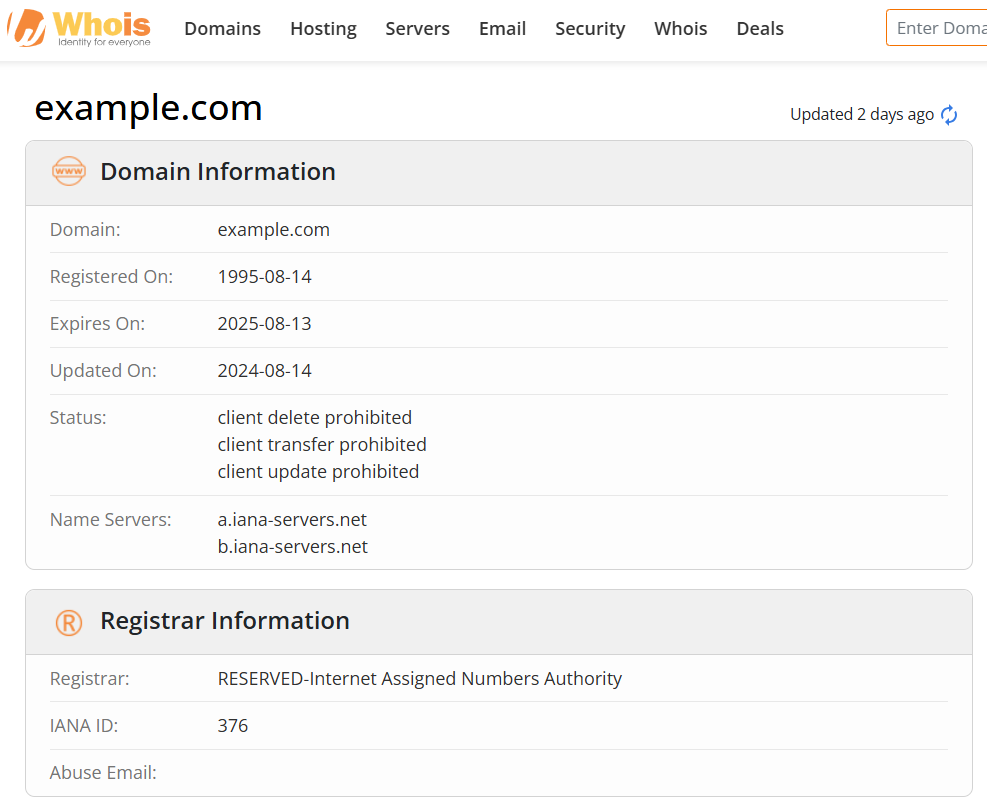
Is there any contact email provided for administrative or technical support?

sathish.kamath@manipal.edu

What country is the domain registered in?

India







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

The WHOIS output does not show any personal registrant details because **example.com** is a **reserved domain** managed by the **Internet Assigned Numbers Authority (IANA)**.

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

Since **example.com** is reserved, privacy protection is **not needed**. Instead of personal registrant details, the WHOIS entry lists **IANA** as the registrar.

**Registry Domain ID**: 2336799\_DOMAIN\_COM-VRSN

**Registrar:** RESERVED-Internet Assigned Numbers Authority

**Registrar WHOIS Server:** whois.iana.org

What are the security implications of exposing or hiding data?

**Exposing Data (No Privacy Protection)**

* Can **help with trust verification**
* Risk of **spam, phishing, and social engineering attacks** targeting the domain owner.

**Hiding Data (Privacy Protection Enabled)**

* Protects personal **identity and contact details**.
* Prevents **email spam and targeted cyber attacks**.
* Can obscure ownership, making it harder to verify legitimate control over a domain.

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

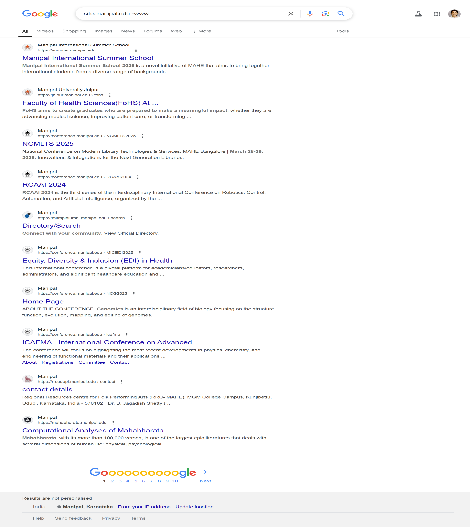
**NS records**: A.IANA-SERVERS.NET, B.IANA-SERVERS.NET



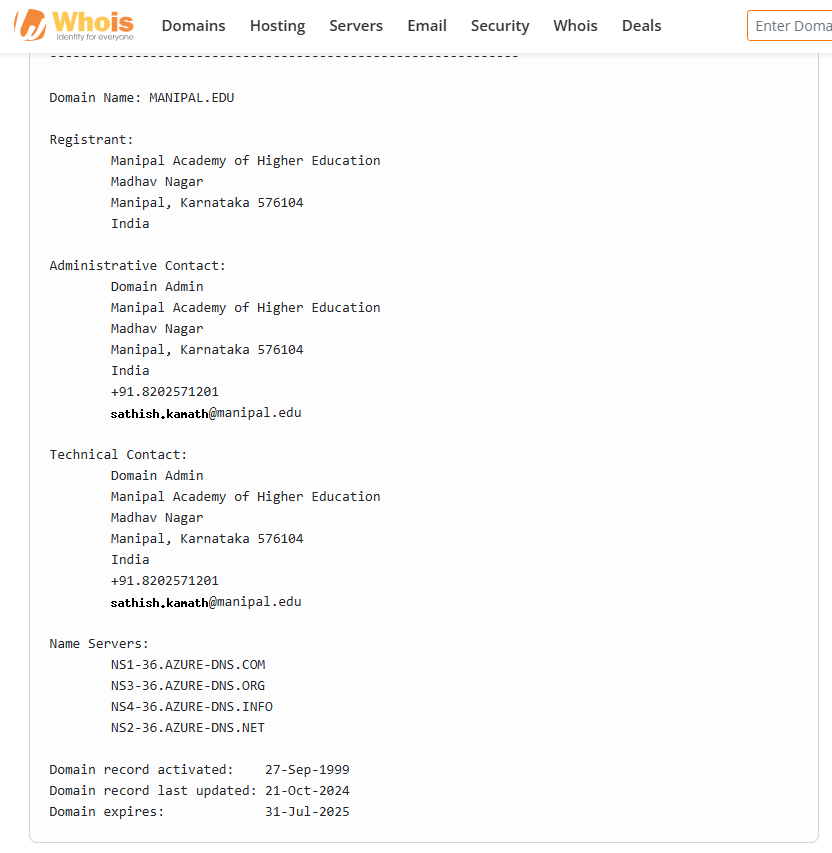
what are the different methods to find the subdomain using both passive and active methods

Passive:

1. Google Dorks



1. WhoIs lookup



1. DNS Dumpster

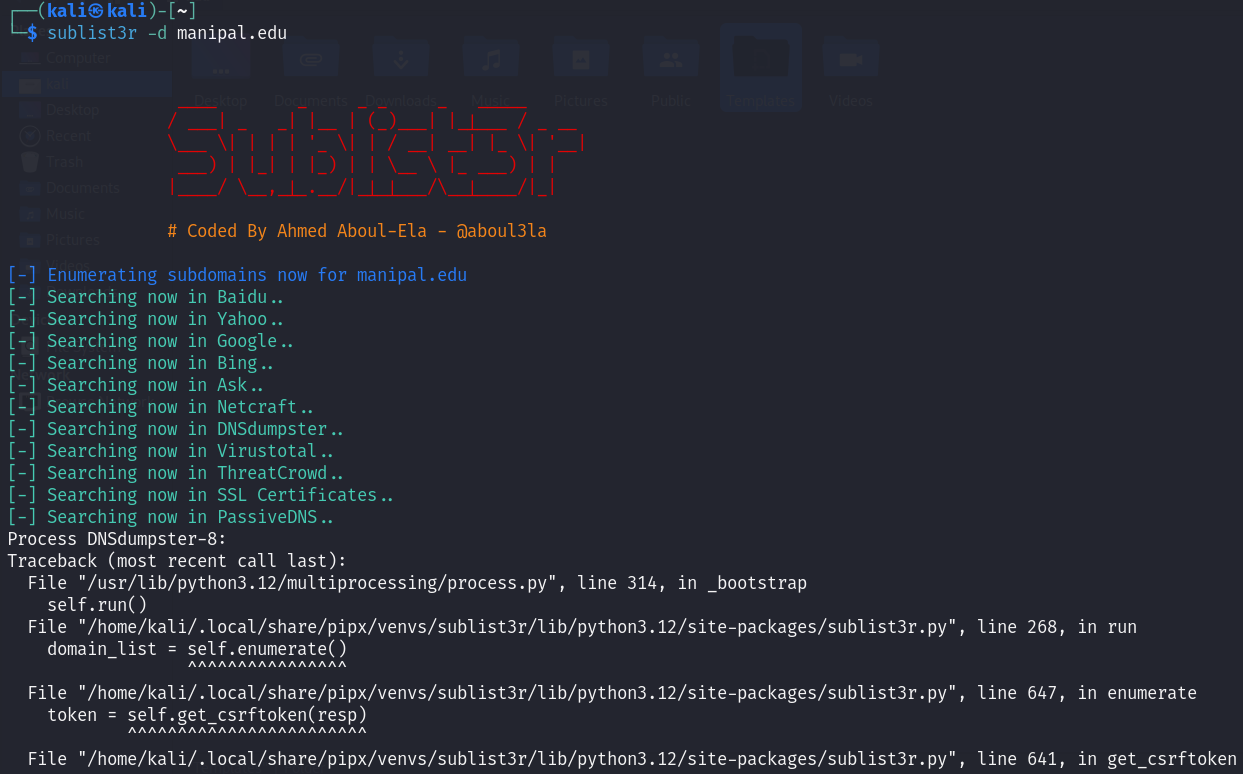


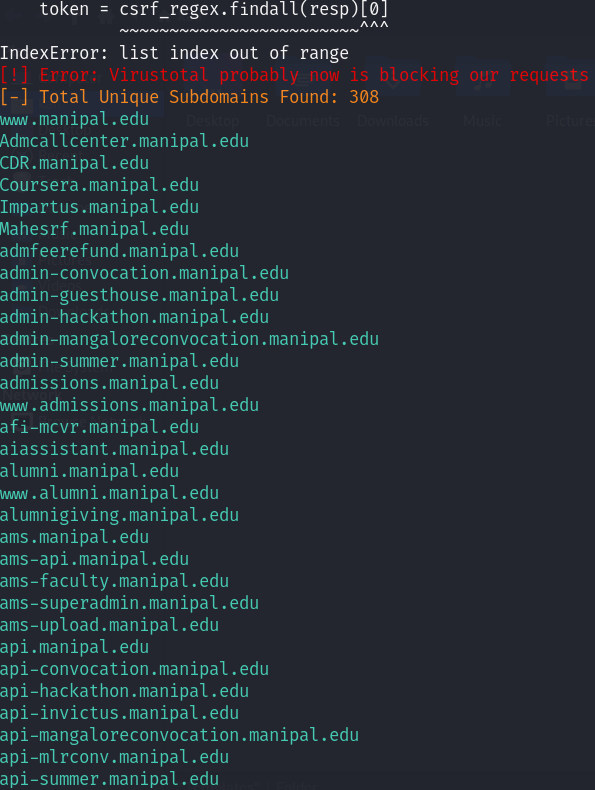
A Records (subdomains from dataset)

| **Host** | **IP** | **ASN** | **ASN Name** | **Open Services (from DB)** | **RevIP** |  |
| --- | --- | --- | --- | --- | --- | --- |
| admin-convocation.manipal.edu | 43.204.60.118 ec2-43-204-60-118.ap-south-1.compute.amazonaws.com | ASN:16509 43.204.0.0/15 | AMAZON-02 India | http: nginx/1.18.0 (Ubuntu) title: Welcome to nginx tech: Ubuntu Nginx:1.18.0 https: nginx title: Convocation MAHE cn: admin-convocation.manipal.edu tech: Bootstrap Nginx | 4 | ⋮ |
| admin-summer.manipal.edu | 65.1.193.164 ec2-65-1-193-164.ap-south-1.compute.amazonaws.com | ASN:16509 65.0.0.0/14 | AMAZON-02 India | http: nginx/1.18.0 (Ubuntu) title: Welcome to nginx tech: Nginx:1.18.0 Ubuntu https: nginx/1.18.0 (Ubuntu) title: MAHE Summer School cn: admin-summer.manipal.edu tech: Semantic UI Bootstrap Nginx:1.18.0 Ubuntu | 5 | ⋮ |
| afi-mcvr.manipal.edu | 1.186.28.84 | ASN:8075 1.186.0.0/16 | MICROSOFT-CORP-MSN-AS-BLOCK United Kingdom |  | 1 | ⋮ |
| alumni.manipal.edu | 52.74.41.140 ec2-52-74-41-140.ap-southeast-1.compute.amazonaws.com | ASN:16509 52.74.0.0/16 | AMAZON-02 Singapore | http: Apache title: Test Page for the Apache HTTP Server tech: Apache HTTP Server https: Apache cn: aagceslm.com tech: Apache HTTP Server | 137 | ⋮ |
| www.alumni.manipal.edu | 52.74.41.140 ec2-52-74-41-140.ap-southeast-1.compute.amazonaws.com | ASN:16509 52.74.0.0/16 | AMAZON-02 Singapore | http: Apache title: Test Page for the Apache HTTP Server tech: Apache HTTP Server https: Apache cn: aagceslm.com tech: Apache HTTP Server | 137 | ⋮ |
| alumnievent.manipal.edu | 45.112.150.155 | ASN:45769 45.112.150.0/24 | DVOIS-IN D-Vois Broadband Pvt Ltd, IN India |  | 27 | ⋮ |
| alumnigiving.manipal.edu | 45.112.150.155 | ASN:45769 45.112.150.0/24 | DVOIS-IN D-Vois Broadband Pvt Ltd, IN India |  | 27 | ⋮ |
| api.manipal.edu | 43.205.223.7 ec2-43-205-223-7.ap-south-1.compute.amazonaws.com | ASN:16509 43.204.0.0/15 | AMAZON-02 India | http: nginx/1.18.0 (Ubuntu) title: Welcome to nginx tech: Ubuntu Nginx:1.18.0 https: nginx cn: api.manipal.edu tech: Nginx |  |  |
|  |  |  |  |  |  |  |

Active Methods

* **Sublist3r**



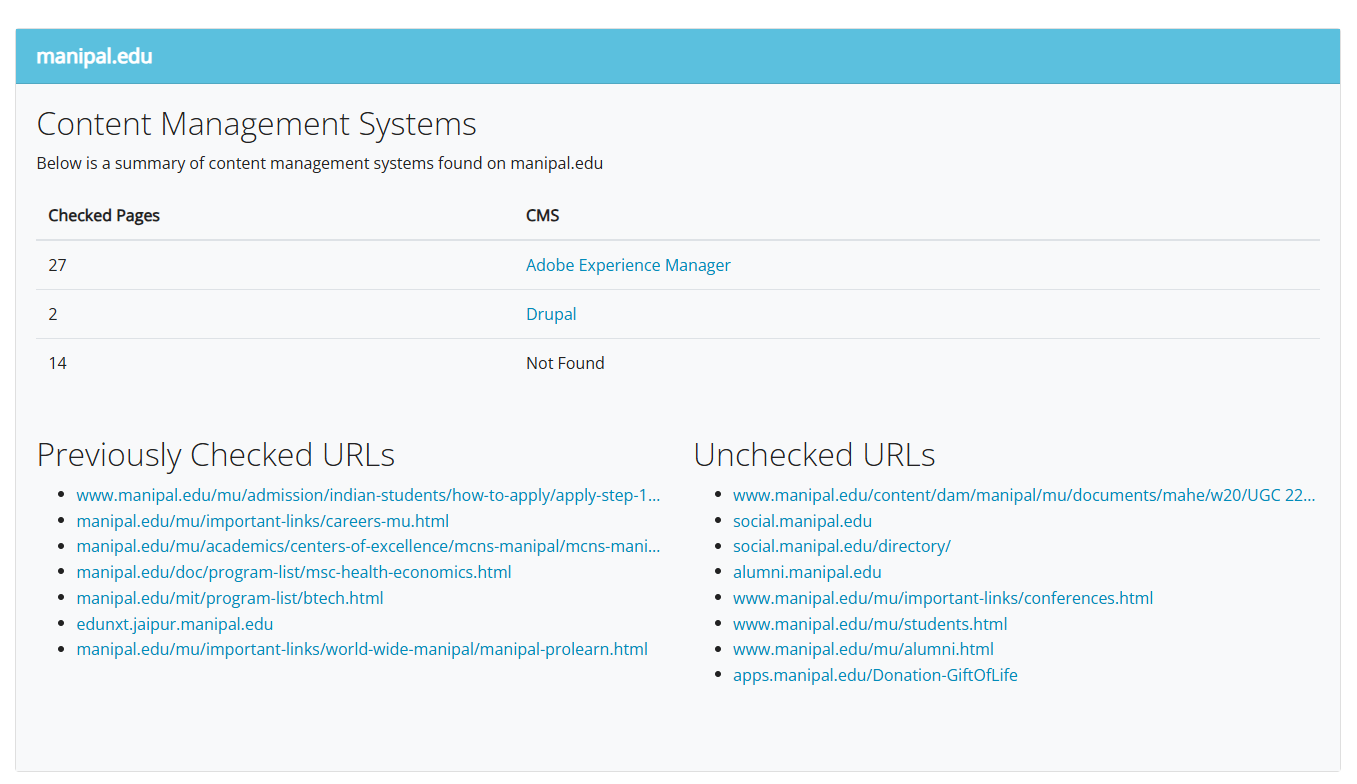


* **Web crawling**

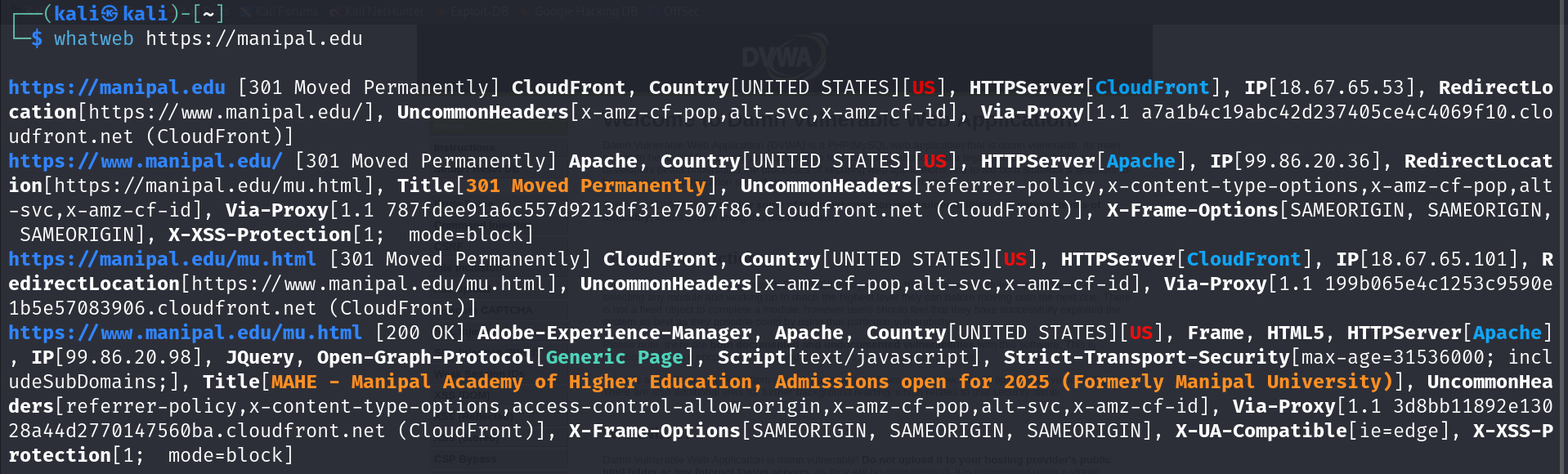
****

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

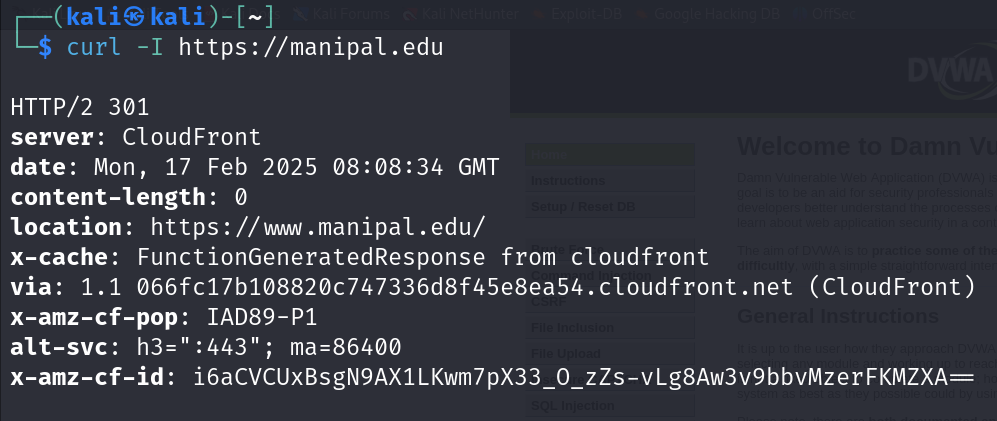
Whatcms tool:



Whatweb tool:



To check HTTP header and response:

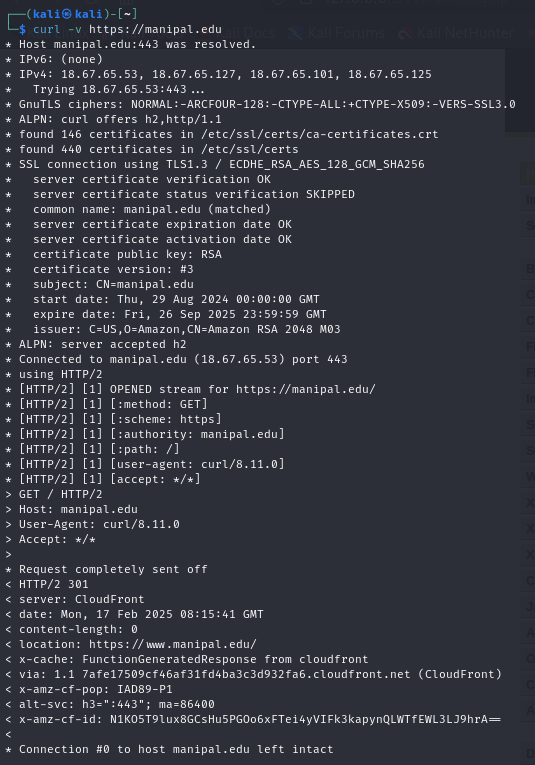


compare whatweb and wappalyzer

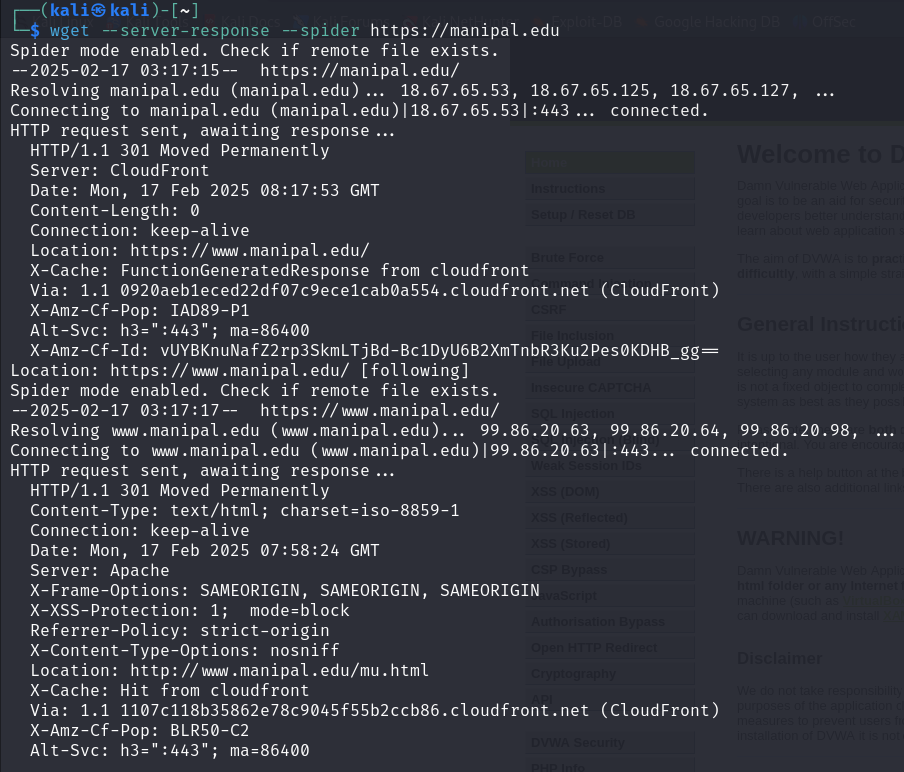
| **Feature** | **WhatWeb** | **Wappalyzer** |
| --- | --- | --- |
| Purpose | Web fingerprinting & reconnaissance | Detects CMS, libraries, and technologies |
| Usage Mode | CLI-based | CLI & browser extension |
| Accuracy | Fast & broad detection, may include false positives | More refined results but slower |
| Installation | Pre-installed in Kali Linux | Needs npm install -g wappalyzer-cli |
| Customization | Supports plugins for extended capabilities | Limited customization |

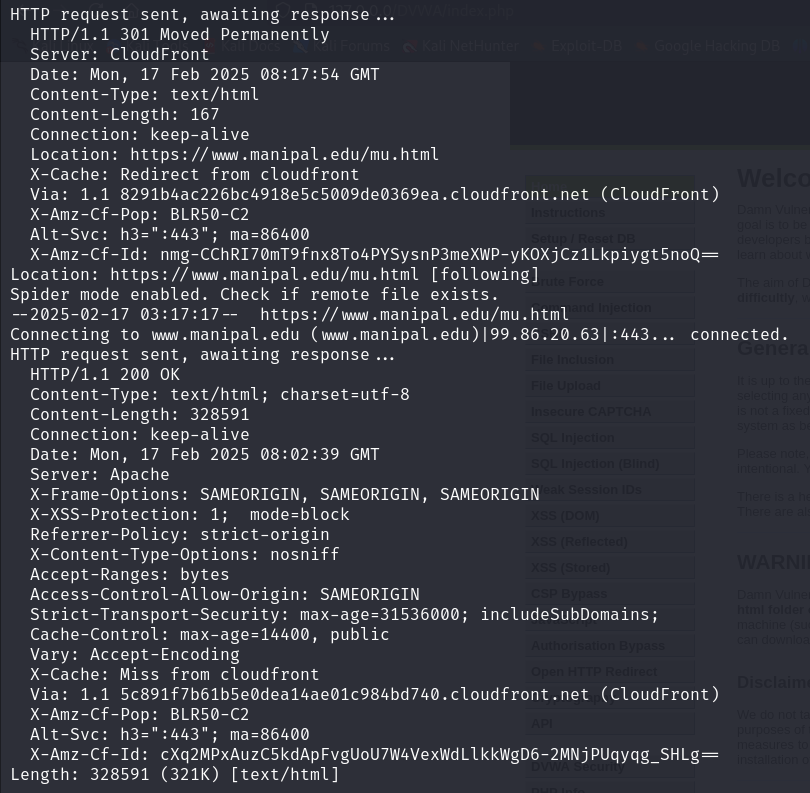
Fetch the HTTP Header ( Many methods are available). Identify the tools used to find HTTP Header details

Curl command:

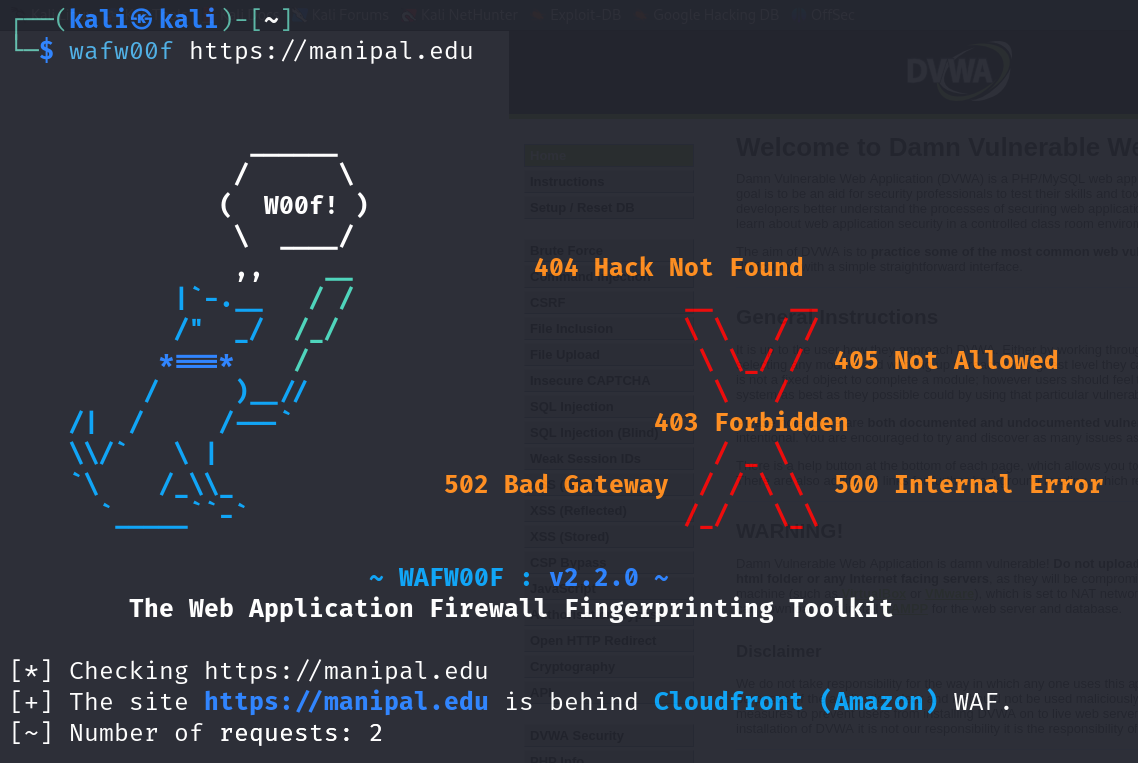


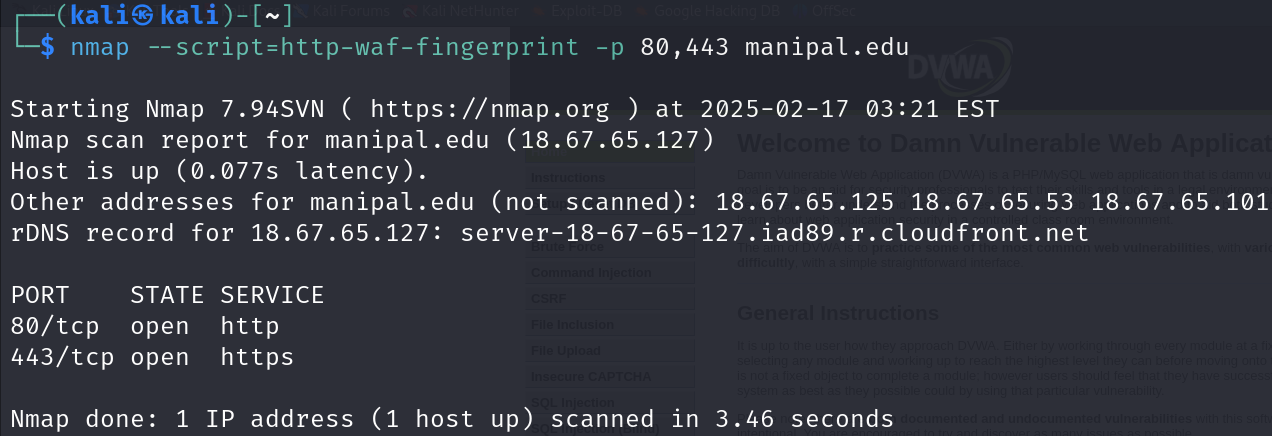
Wget:



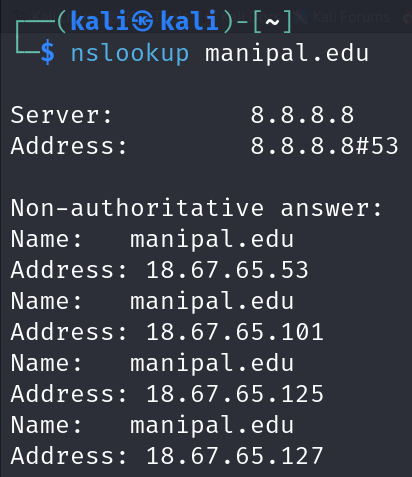


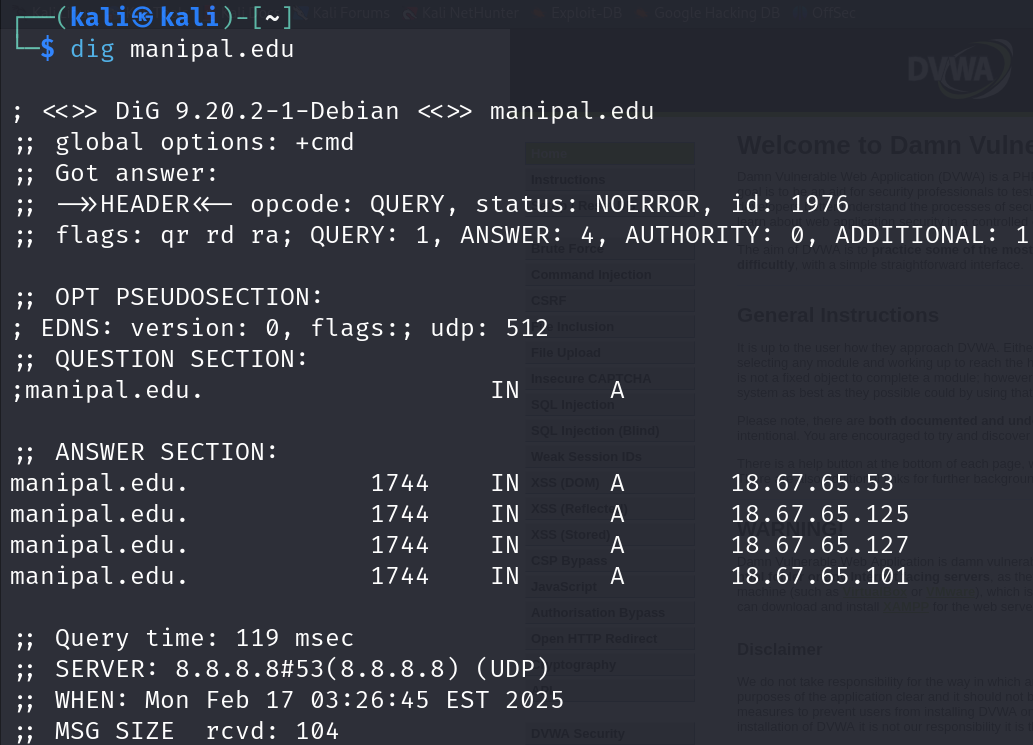
Check whether domain have firewall installed or not





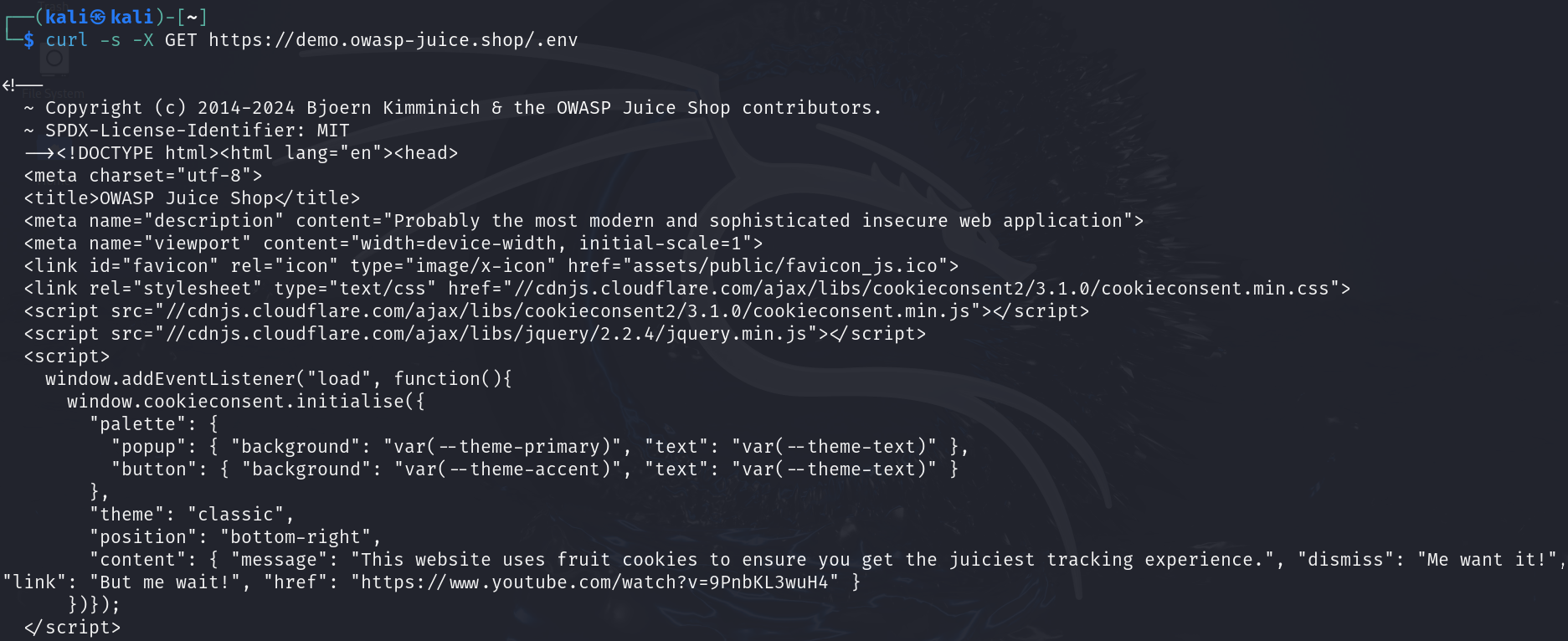
do they have load balancer

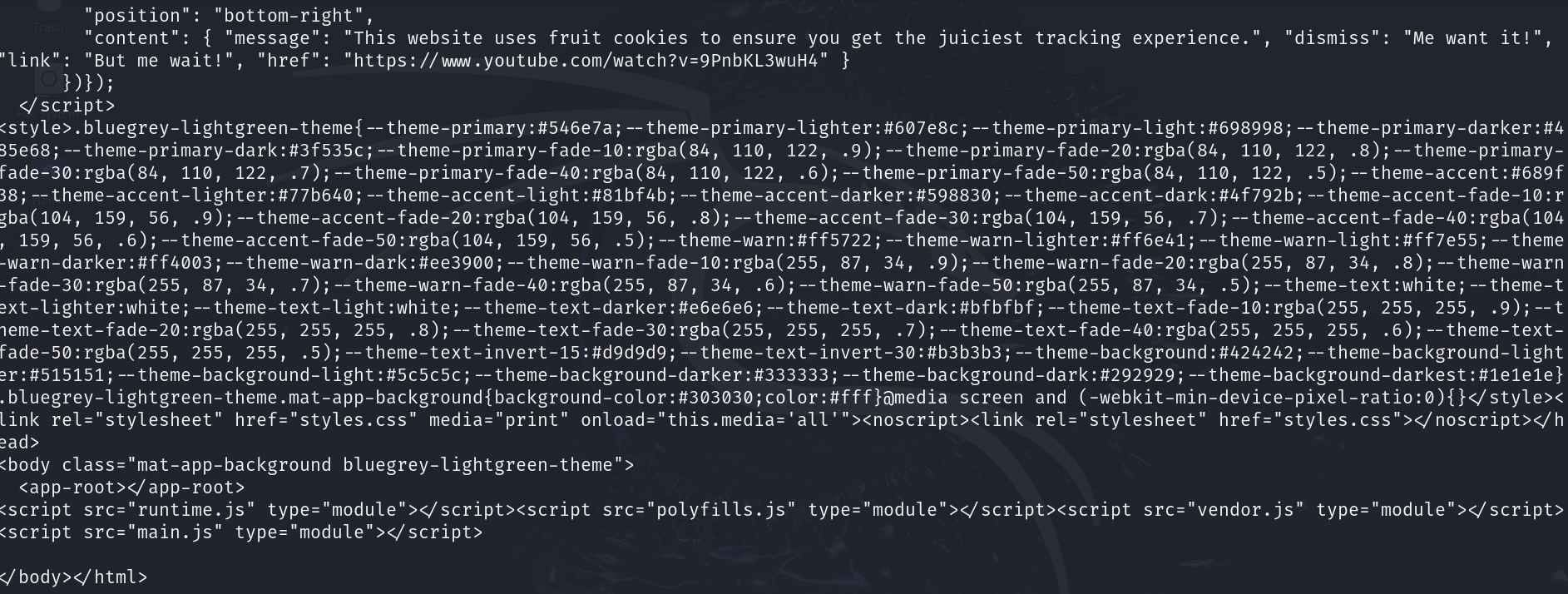




as domain has multiple IP addresses, it likely uses a load balancer.

Search for exposed environment configuration files

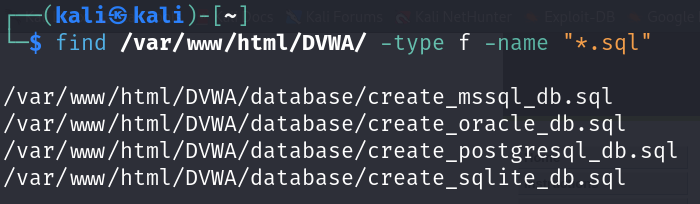




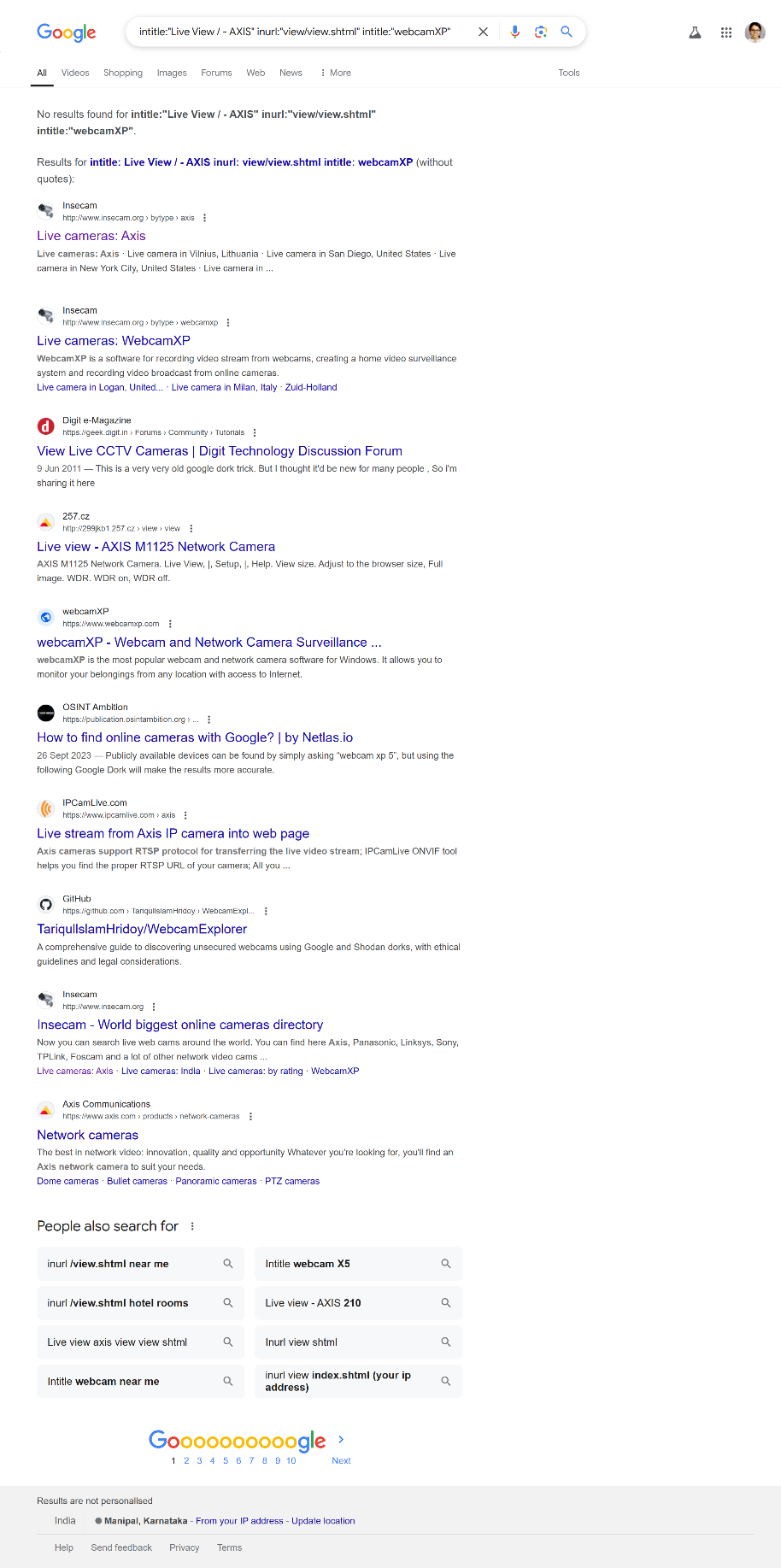
Look for log files that may contain sensitive information

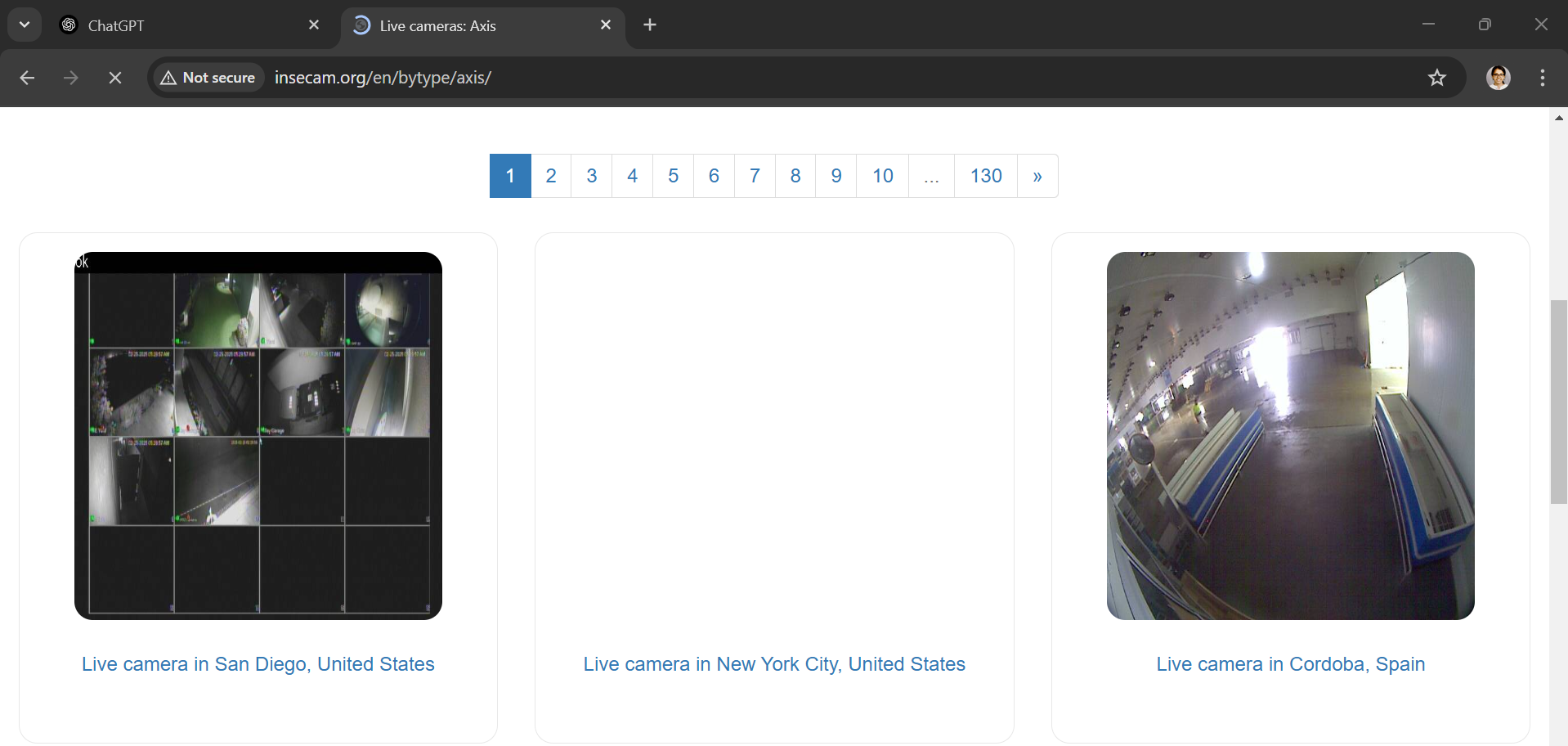


Find database backup files



Find live camera feeds





Search for open IoT device

