DAY 4

DATE: 06/06/2025

Targeted Site: https://www.alagappauniversity.ac.in/homepage

Findings:

- Internet Protocol addresses and domain information of the targeted college site was collected using urlscan.io site. The College site has 13 IP addresses in 3 Countries. Their Autonomous system information has also been collected (an Autonomous System (AS) is a collection of interconnected IP networks and routers managed by a single administrative entity. This entity defines and controls a unified routing policy for the AS, ensuring coordinated data transmission) – Fig 01

- External and Internal links associated with the website was also collected using the same urlscan.io site and is listed on the figure no 02

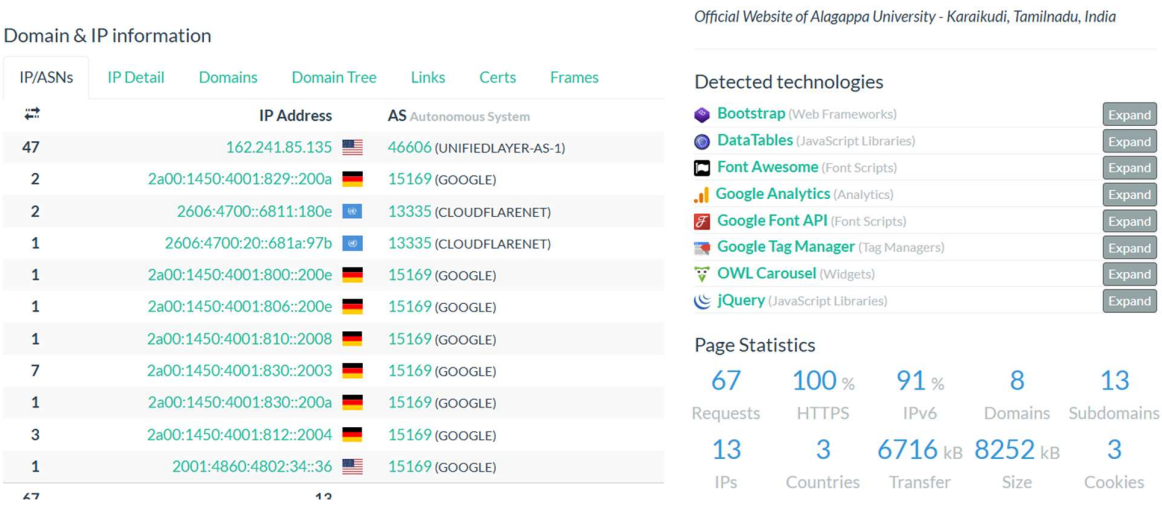

Fig no:01

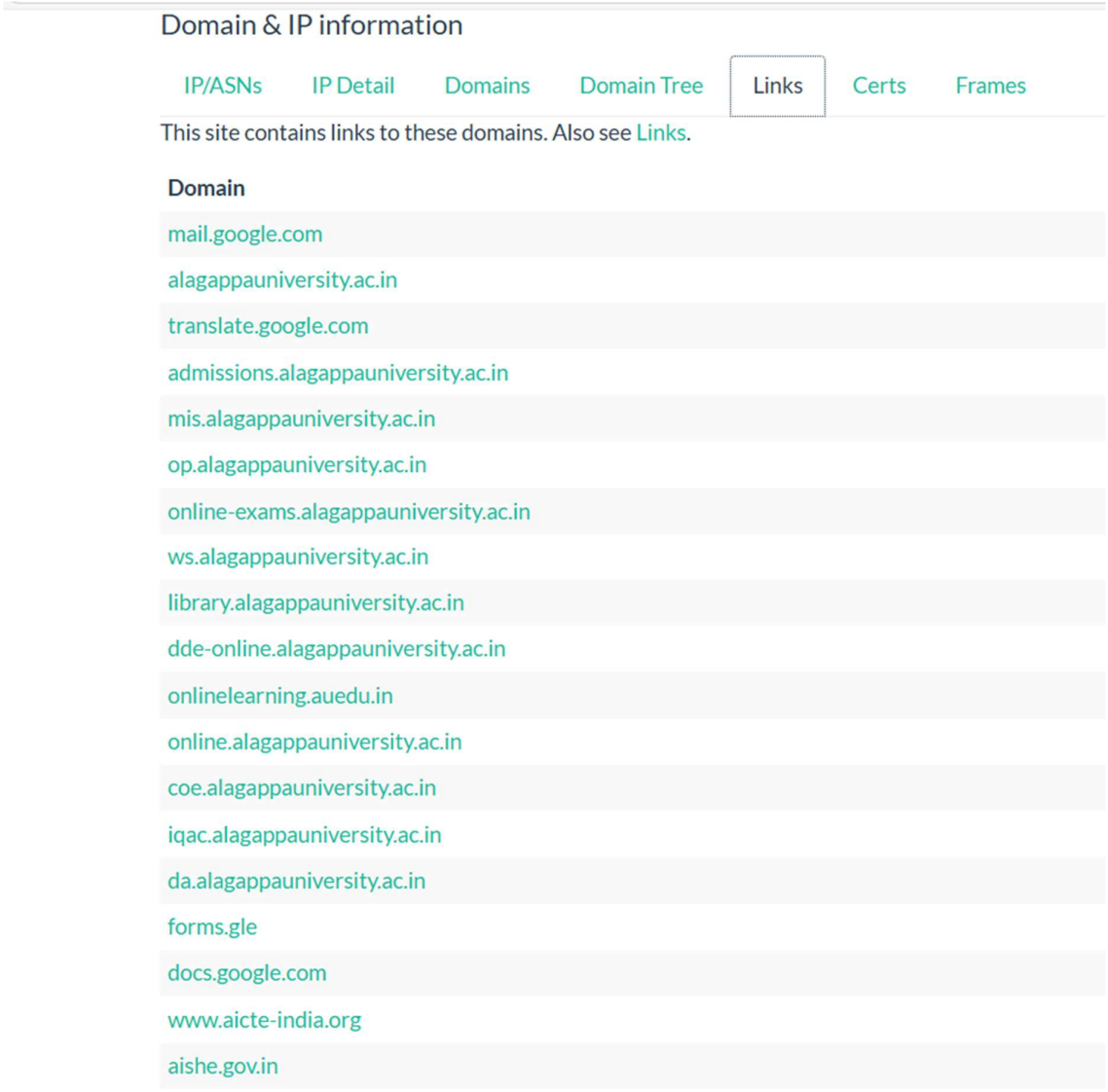

Fig no:02

- A Domain Name System (DNS) record is a set of instructions used to connect domain names with internet protocol (IP) addresses within DNS servers
- **A (Address) Record:** Maps a domain name to an IPv4 address.
- **AAAA (Quad A) Record:** Maps a domain name to an IPv6 address.
- **CNAME (Canonical Name) Record:** Aliases one domain name to another, directing traffic to a canonical domain.
- **MX (Mail Exchange) Record:** Specifies the mail server responsible for accepting email for a domain.
- **NS (Name Server) Record:** Indicates which DNS servers are authoritative for a domain.
- **SOA (Start of Authority) Record:** Contains administrative information about a domain, including the zone's serial number and contact information.

- The above-mentioned DNS record types were collected from Webcheck and nslookup.io shown in fig 3 and 4

Fig no:03

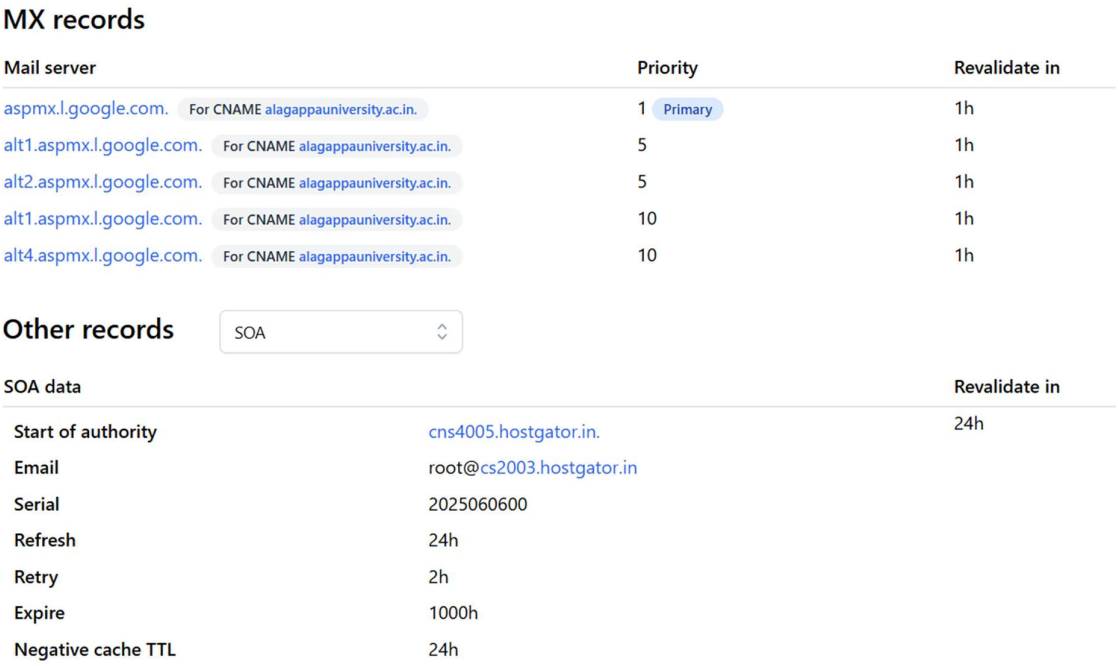

Fig no:04

- HSTS - HSTS (HTTP Strict Transport Security) is a web security policy mechanism that forces browsers to always connect to a website over HTTPS, even if the user attempts to access it via HTTP
- HSTS policy was found absent in the targeted college site which is shown in fig 05 in seo site checkup website

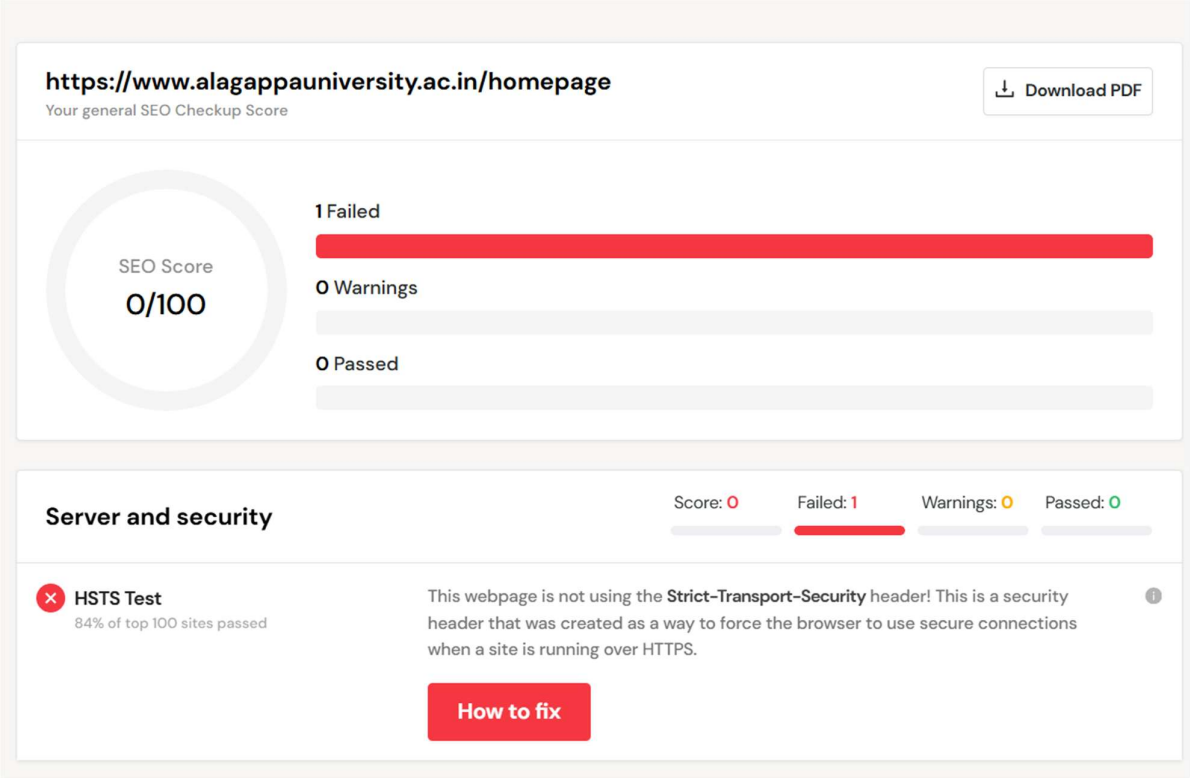

Fig no:05

- DNSSEC stands for Domain Name System Security Extensions. It's a suite of extensions to the Domain Name System (DNS) that uses cryptographic signatures to authenticate DNS responses. This ensures that data received by clients is genuine and hasn't been tampered with during transit.
- DNSSEC was found absent using Powdermac DNSSEC and DNSSEC Checker extension in fig no 6 and 7

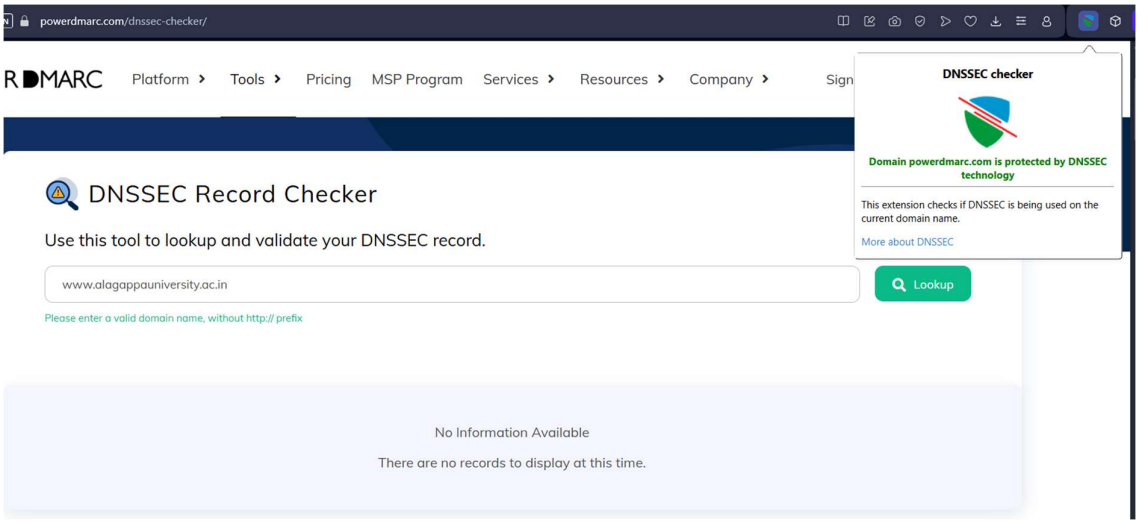

Fig no:06

Fig no:07

- HTTP security headers are those HTTP headers that are related specifically to security, exchanged between a client (like a web browser) and a server to define the security of HTTP communication. These include dedicated security headers and several others that can indirectly affect privacy and security.
- HTTP Security features were found absent in the targeted site using securityheaders website in fig no 8.

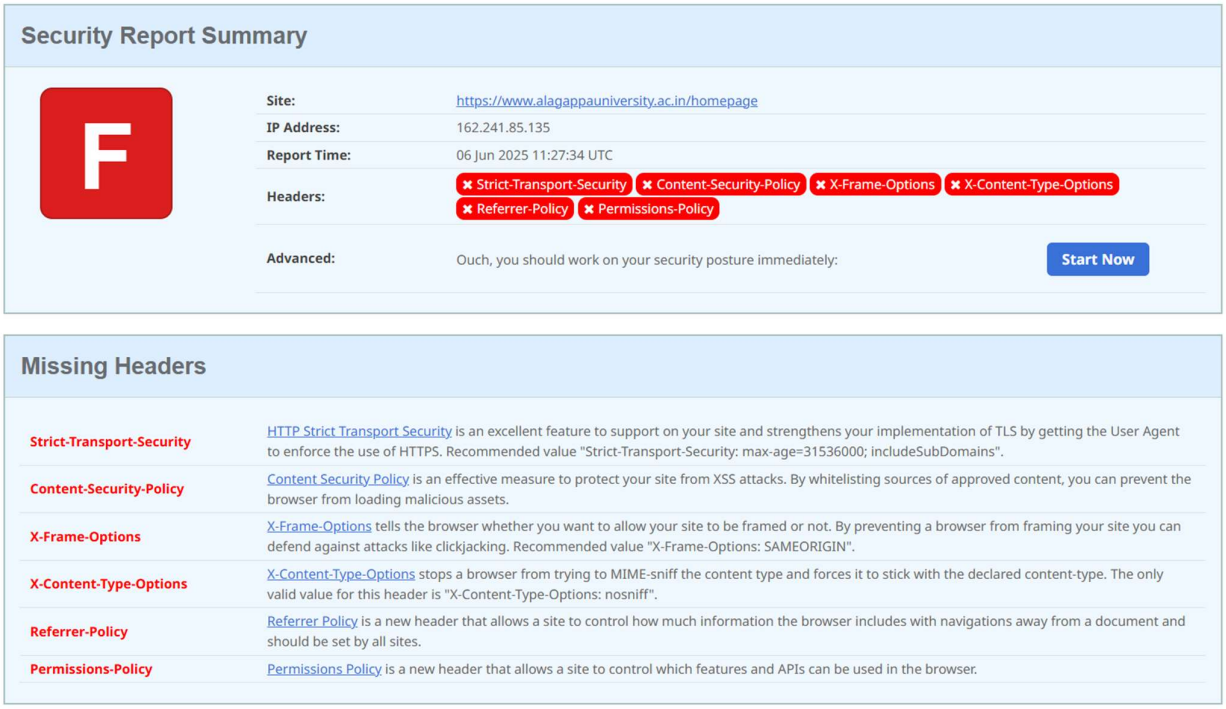

Fig no:08

- Operating system details of the targeted system were found using N-map in fig 9

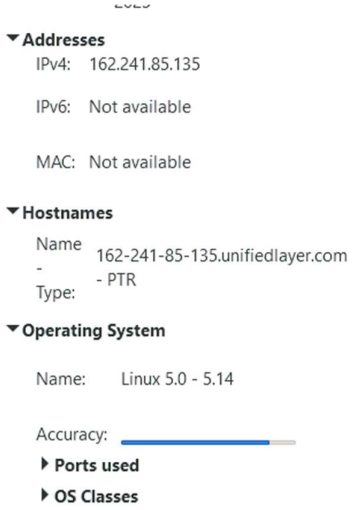

Fig no: 09