**Report -Task -7 01-09-2023 Friday**

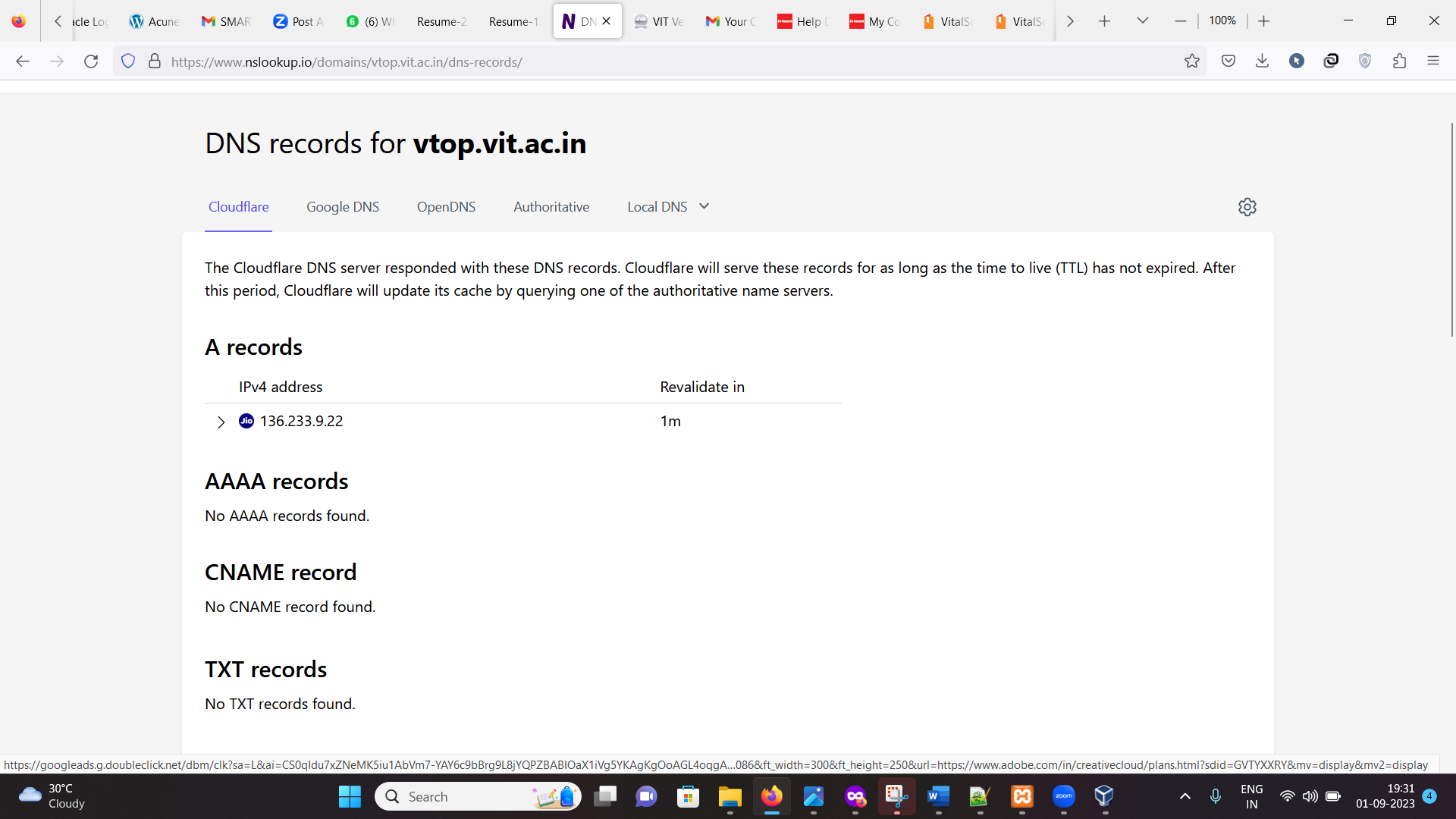
**By Sameer Chauhan 21BCE0999**

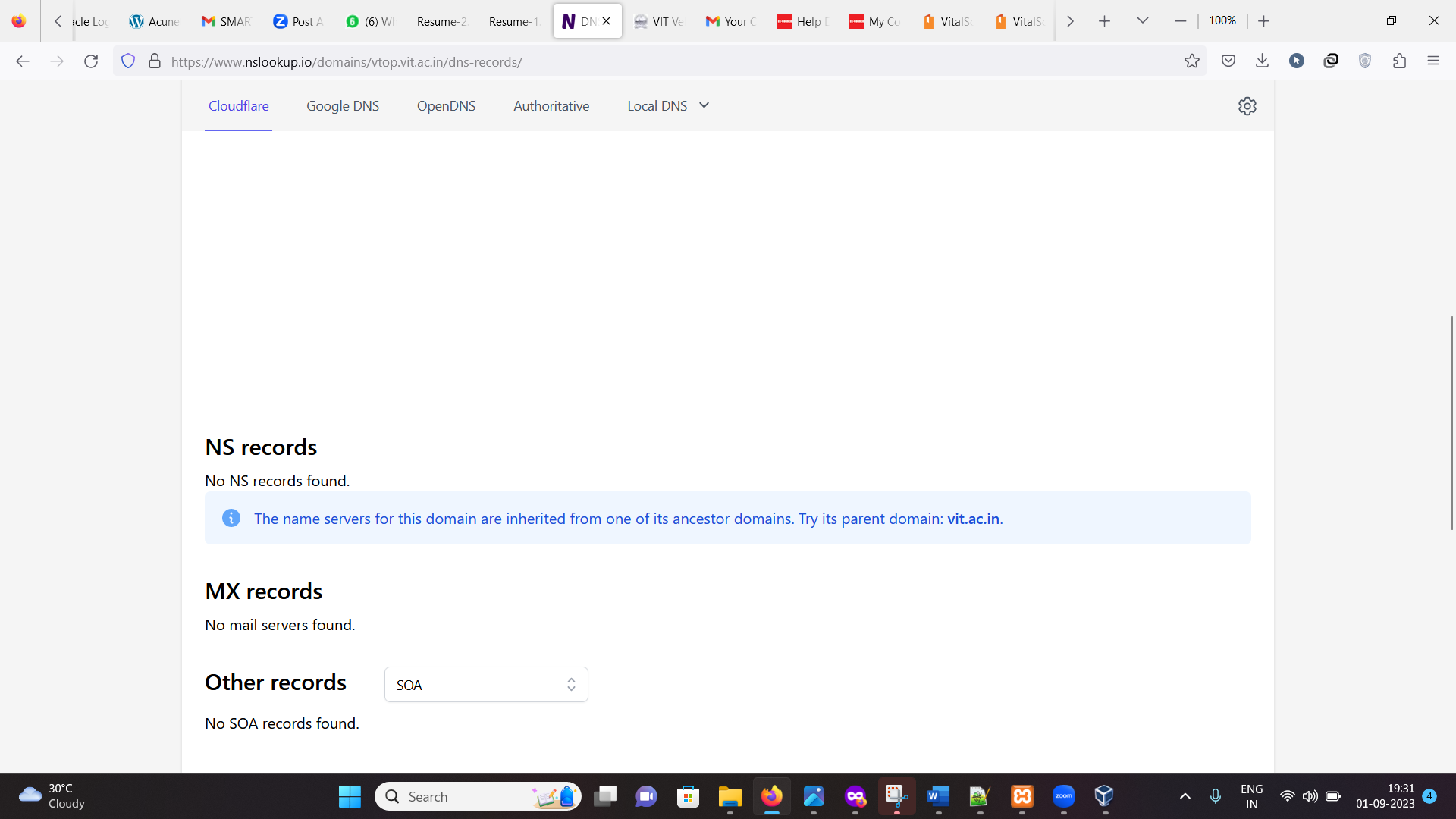
**Report Aim -We have to gather information of our own choice website and do passive Reconnaissance**

**I will choose my university website vtop.vit.ac.in**

**To have a better understanding of my college web framework and Security**

**I will use Nslookup.io firstly**





1- **A Records (IPv4 address)**:

* **IPv4 address: 136.233.9.13**
* **Revalidate in: 1 minute**
* **Hosted by Reliance Jio Info comm Limited**

**This indicates that the domain or website you're querying has an IPv4 address of 136.233.9.13. The "Revalidate in" value suggests that this DNS record should be rechecked or refreshed every 1 minute. It also mentions that the website is hosted by Reliance Jio Infocomm Limited.**

2- **AAAA Records (IPv6 address)**:

**"No AAAA records found."**

**This section indicates that there are no IPv6 (AAAA) records associated with this domain. IPv6 records are used for IPv6 addresses, but in this case, there are none.**

3-**CNAME Record**:

**"No CNAME record found."**

**This section suggests that there is no Canonical Name (CNAME) record associated with this domain. CNAME records are used to specify an alias for a domain (e.g., pointing one domain to another).**

4- **TXT Records**:

**"Site ownership verification"**

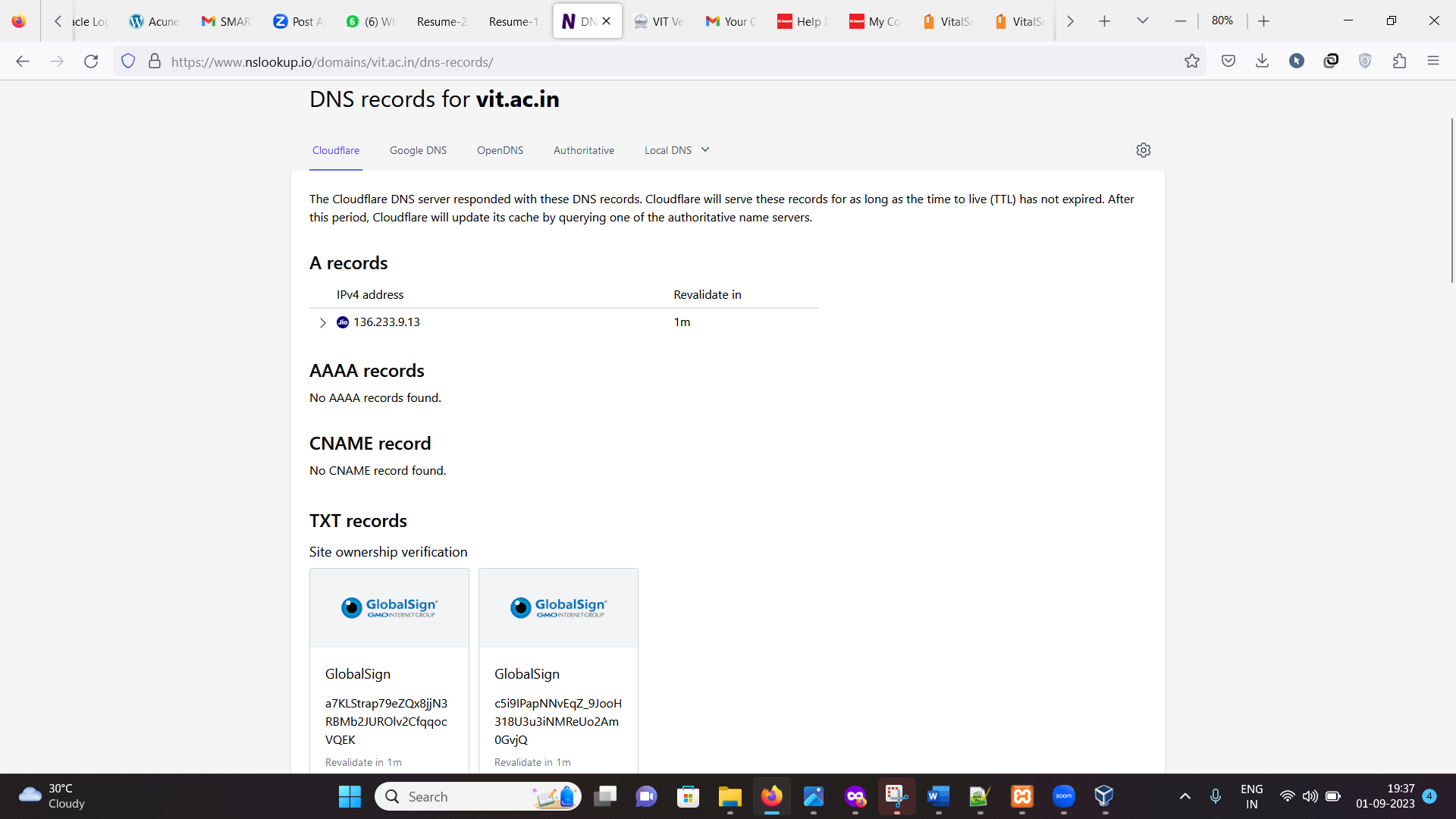
**This part indicates that there is at least one TXT (Text) record associated with the domain, and its content suggests it might be used for site ownership verification. TXT records are**

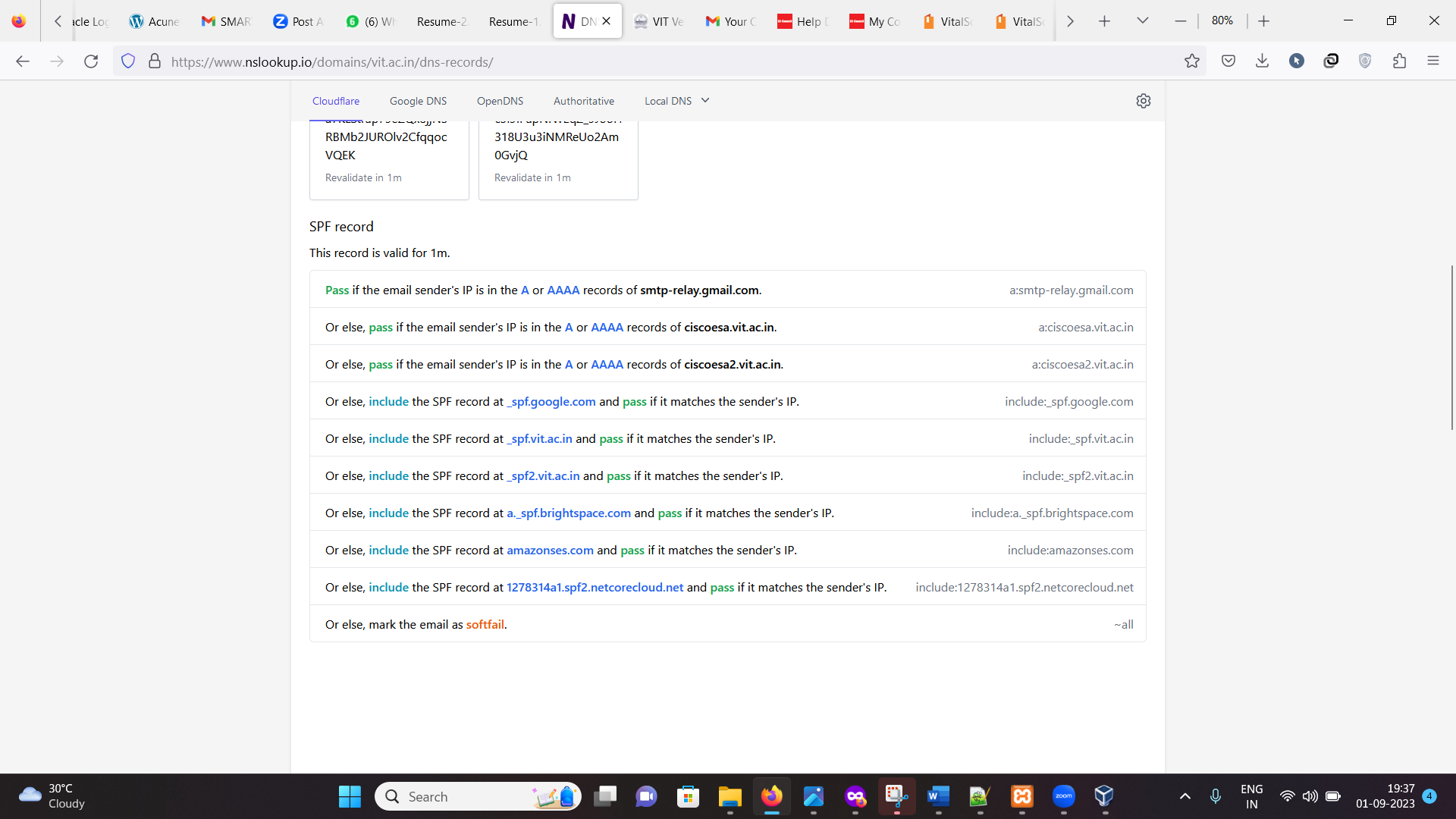
**5- SPF RECORDS**

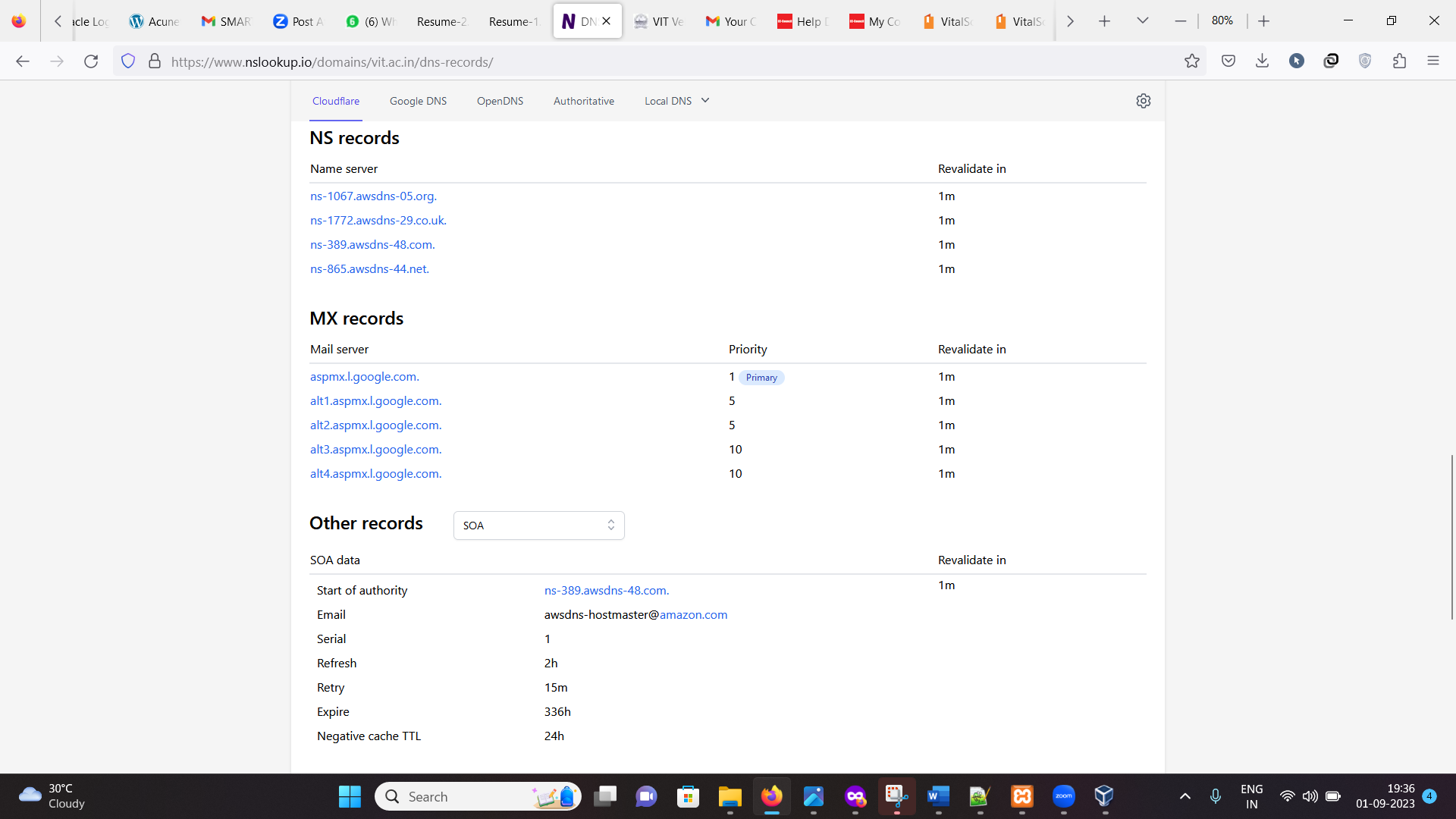
:**The SPF (Sender Policy Framework) record provided specifies the conditions under which incoming email messages claiming to be sent from your domain will be considered legitimate. In this case, the SPF record allows email messages to pass as legitimate if the email sender's IP address is found in the A or AAAA records of "smtp-relay.gmail.com," and it specifies the TTL (Time To Live) of 1 minute for this record.**

**Usage:** **SPF records are used to help prevent email spoofing and phishing by specifying which mail servers are authorized to send emails on behalf of a domain. In this case, it appears that you have authorized "smtp-relay.gmail.com" to send emails on behalf of your domain.**

**We will check further records by inheriting our site previous domain-**







**NS records-** **This information provided is DNS (Domain Name System) NS (Name Server) records for a domain. These NS records specify the authoritative name servers responsible for handling DNS queries for the domain.**

1. **ns-1067.awsdns-05.org.:This NS record points to the name server "ns-1067.awsdns-05.org."The "Revalidate in" value is set to 1 minute. This means that the DNS resolver should recheck this NS record every 1 minute.**
2. **ns-1772.awsdns-29.co.uk.:This NS record points to the name server "ns-1772.awsdns-29.co.uk."Like the previous record, it has a "Revalidate in" value of 1 minute.**
3. **ns-389.awsdns-48.com.:This NS record points to the name server "ns-389.awsdns-48.com."It also has a "Revalidate in" value of 1 minute.**
4. **ns-865.awsdns-44.net.:This NS record points to the name server "ns-865.awsdns-44.net."Similar to the others, it has a "Revalidate in" value of 1 minute**.

**Ms records-** **This information is related to the MX (Mail Exchanger) records for a domain. MX records specify the mail servers responsible for receiving email messages on behalf of the domain.**

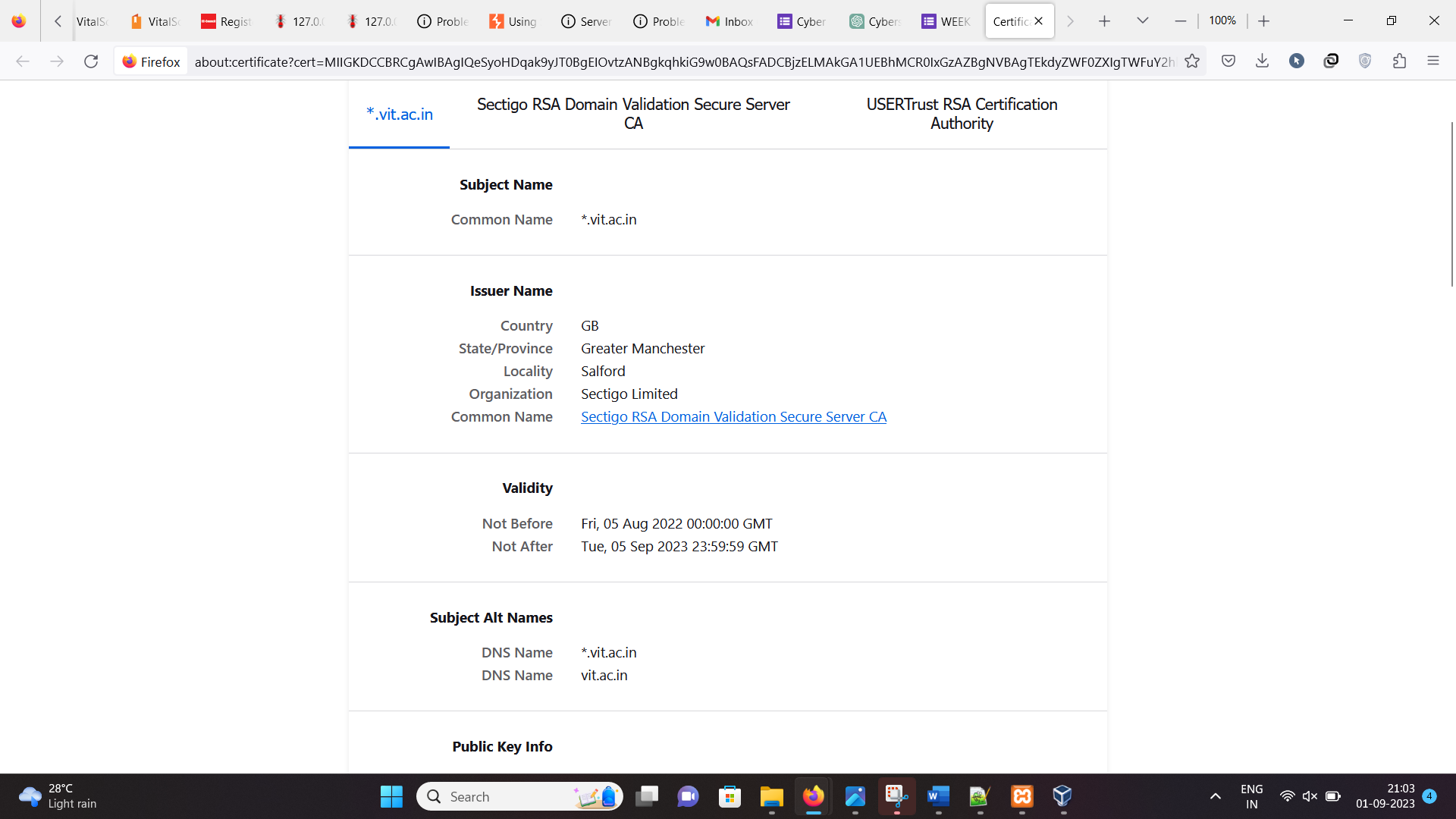
**1- aspmx.l.google.com.:**

**Mail server: aspmx.l.google.com**

**Priority: 1 (Primary Revalidate in: 1 minute**

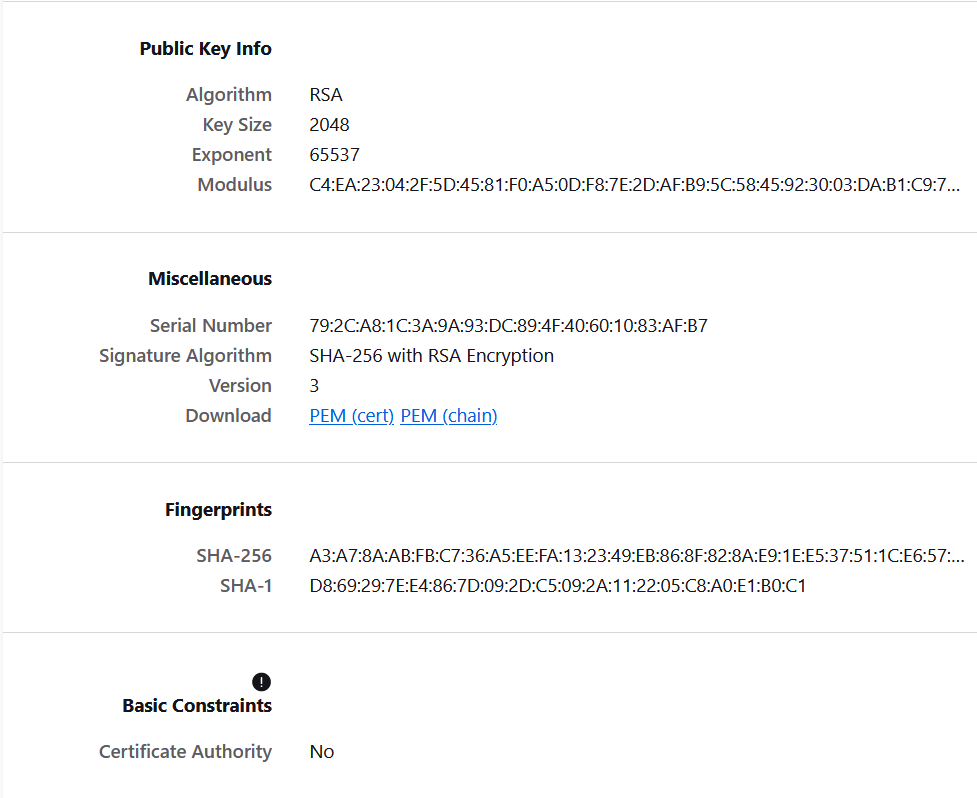
1. **alt1.aspmx.l.google.com.:**
   * **Mail server: alt1.aspmx.l.google.com**
   * **Priority: 5**
   * **Revalidate in: 1 minute**
2. **alt2.aspmx.l.google.com.:**
   1. **Mail server: alt2.aspmx.l.google.com**
   2. **Priority: 5**
   3. **Revalidate in: 1 minute**
3. **alt3.aspmx.l.google.com.:**
   1. **Mail server: alt3.aspmx.l.google.com**
   2. **Priority: 10**
   3. **Revalidate in: 1 minute**
4. **alt4.aspmx.l.google.com.:**
   1. **Mail server: alt4.aspmx.l.google.com**
   2. **Priority: 10**
   3. **Revalidate in: 1 minute**

**Further we collected information regarding various certificates of the website server –**



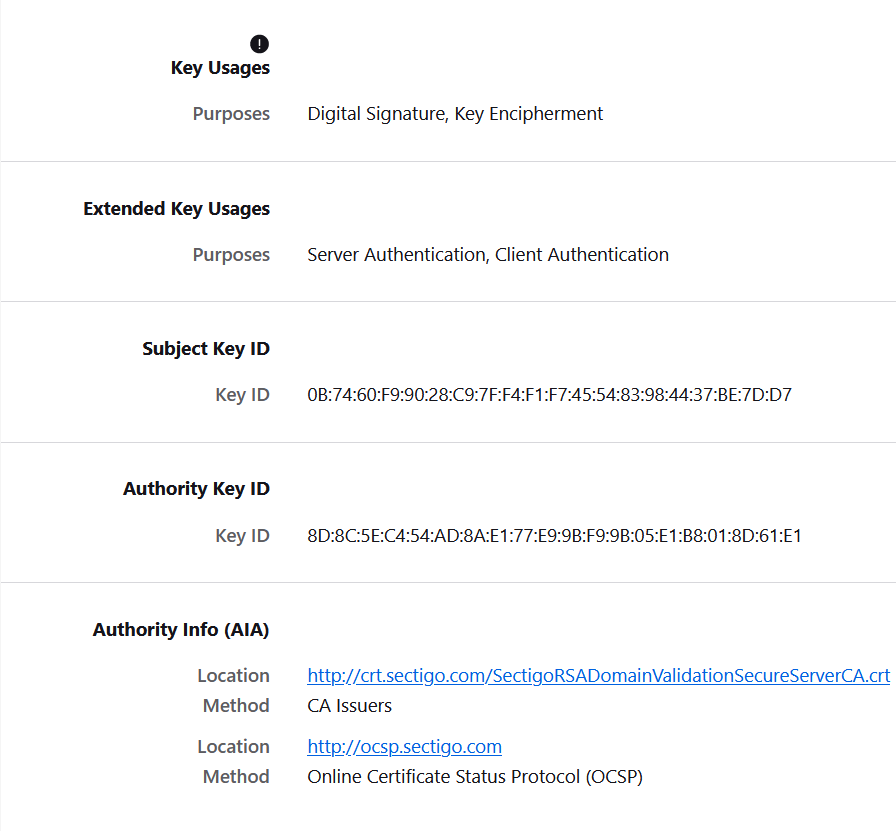
**Inference-The above information shows subject name of domain,issuer details such as country,locality,org**

**Validity of the Certificate,Subject Alternative Names (SANs) are an extension to the X.509 specification that allows users to specify additional host names for a single SSL certificate.**

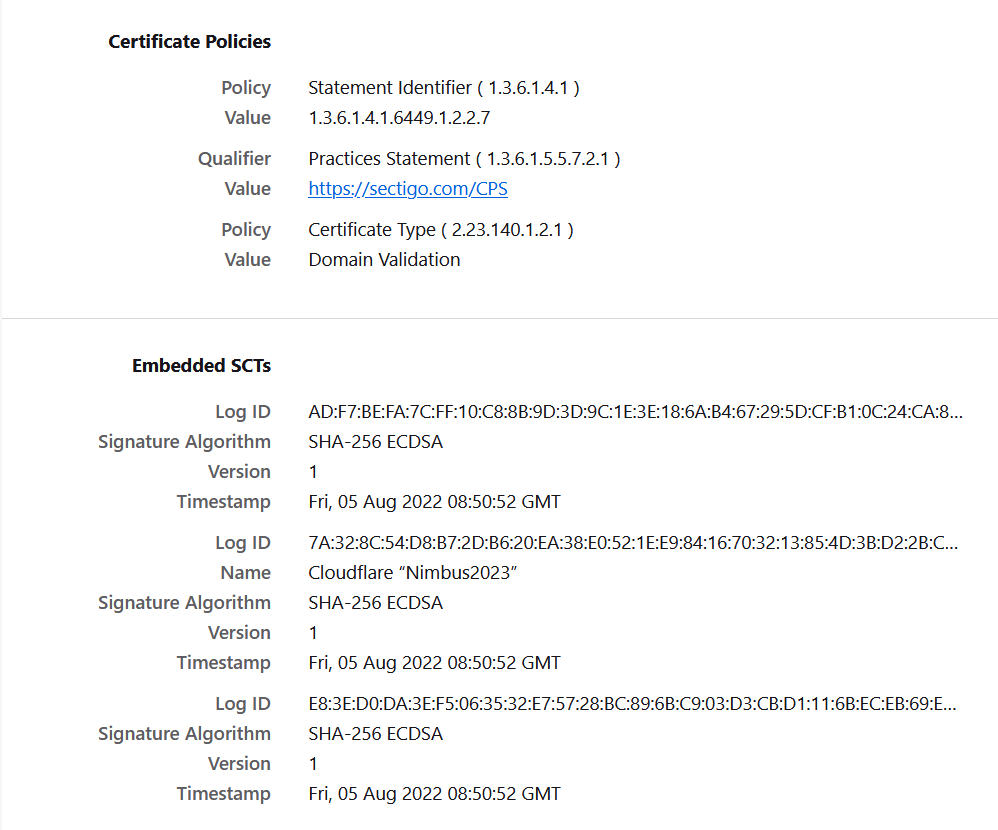
****

**Inference-Here we can see public key cryptography, the "modulus" is a critical component of the public key. It is an essential part of the public key's mathematical structure and plays a fundamental role in encryption and digital signature processes.**

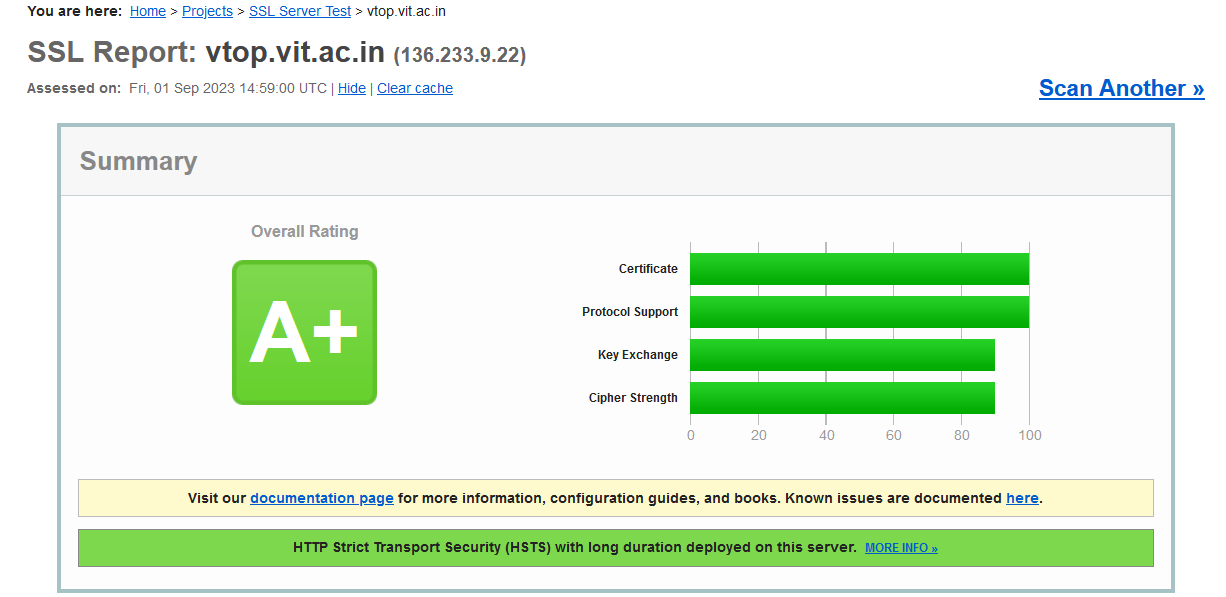
**We can see Fingerprinting, in a cybersecurity context, typically involves generating a unique representation (a "fingerprint") of data using cryptographic hash functions like SHA.**

****

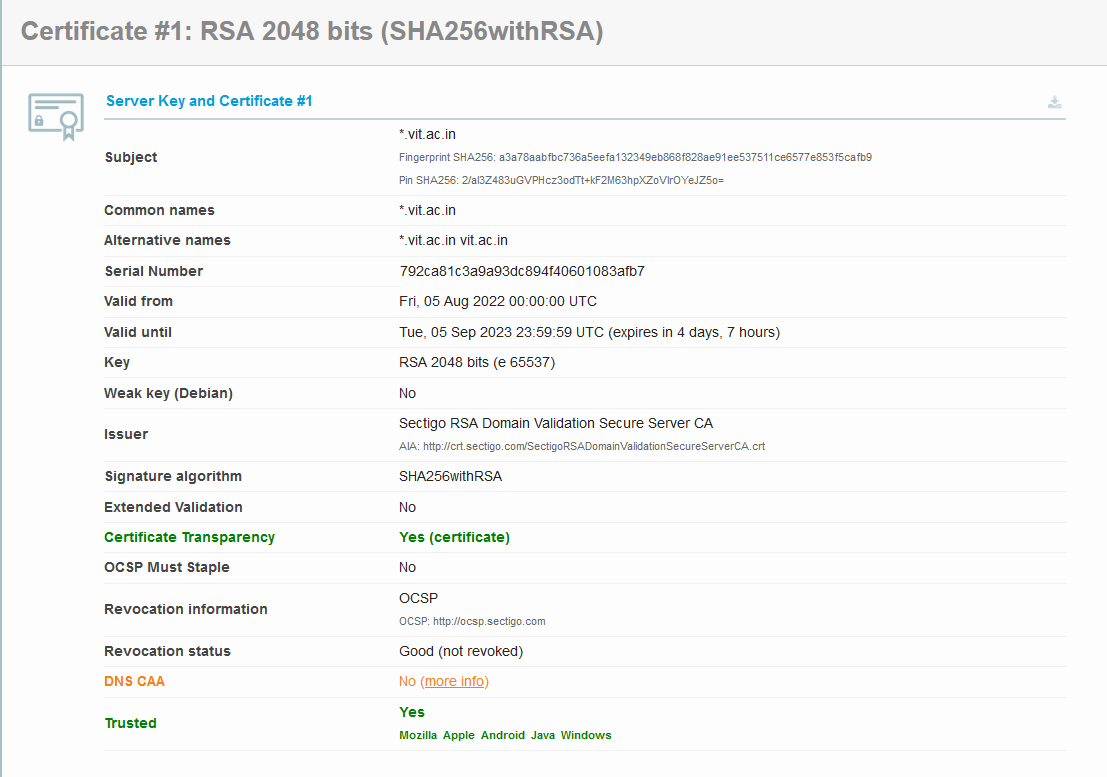
**Inference -key usages for digital signature,extended key usages purposes like client,server authentication, The Subject Key Identifier (SKI) and Authority Key Identifier (AKI) are two fields commonly found in X.509 digital certificates, which are used in various security protocols, including SSL/TLS for secure web communication and public key infrastructure (PKI) for authentication and encryption.**

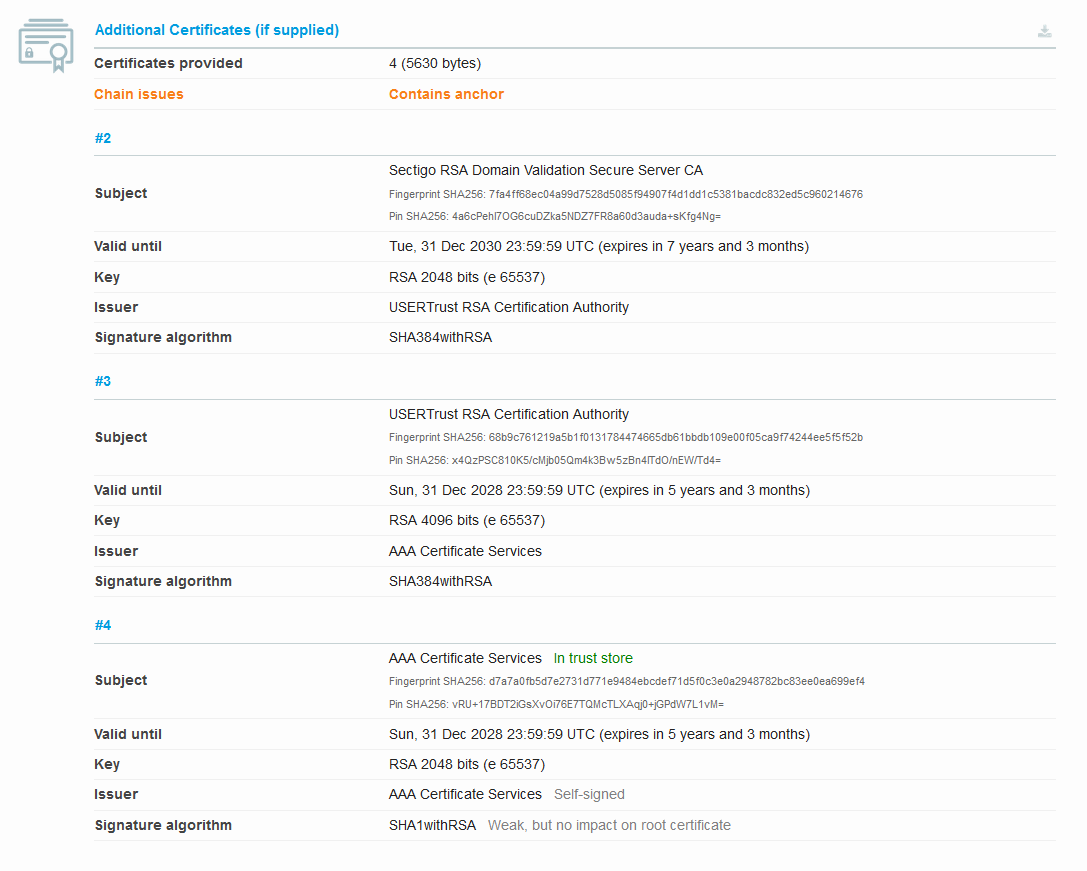
****

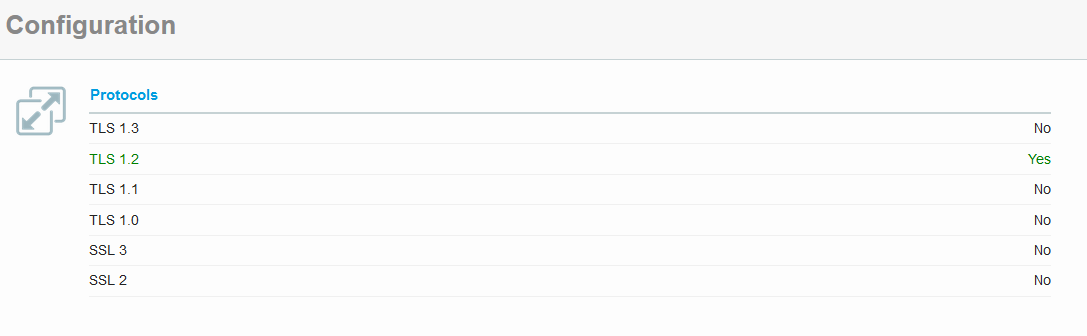
**Now we will test the Server of the site and some detailed certifications (generated report by SSL LABS)**

****

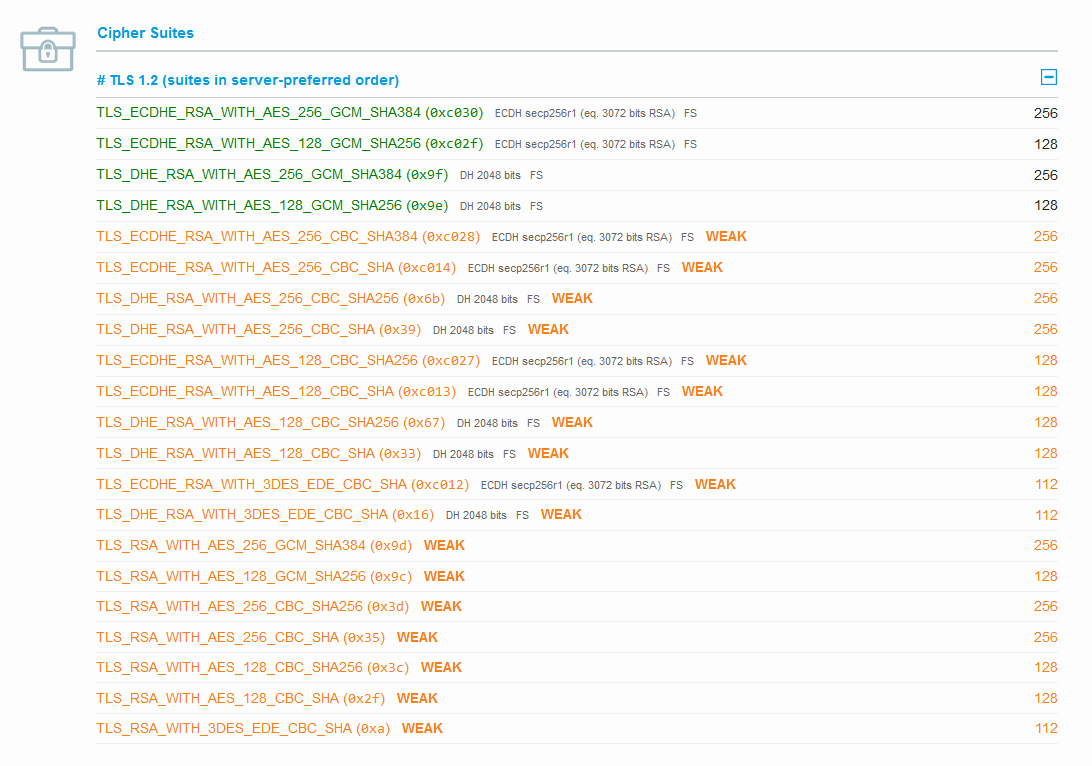
**The grade A+ shows very strong level of protection but still that doesn’t confirm it has 0 vulnerability.**

****

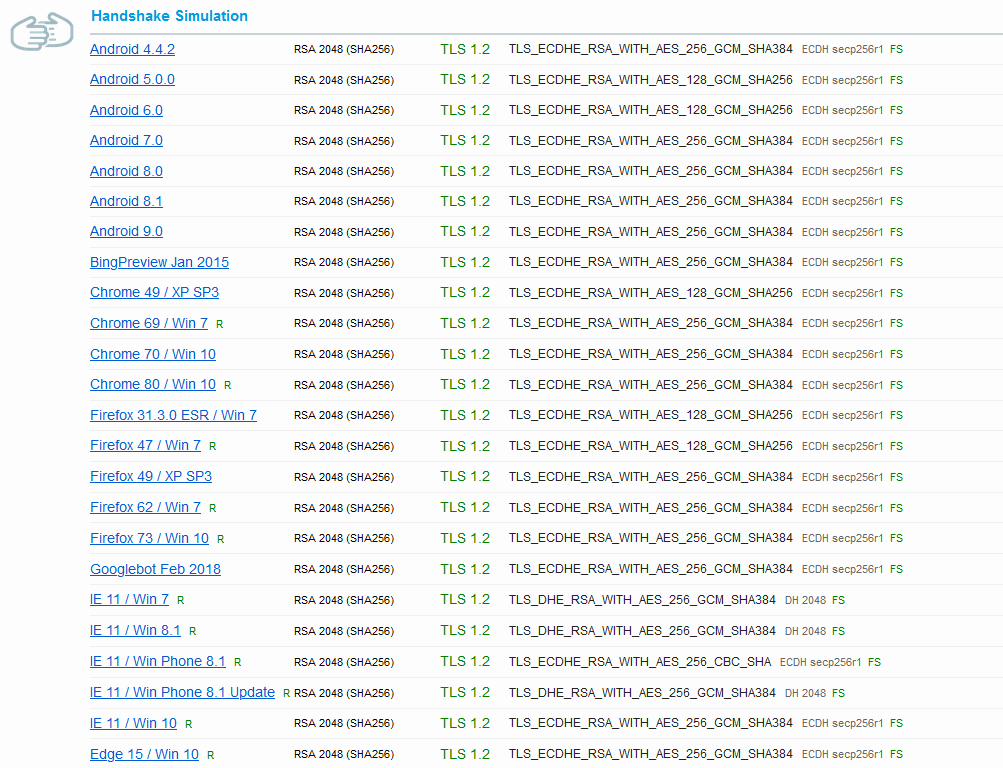
****

****

**As we can see our site is using only latest TLS transport layer security config earlier versions are disabled which ensures protection and no entry points**

****

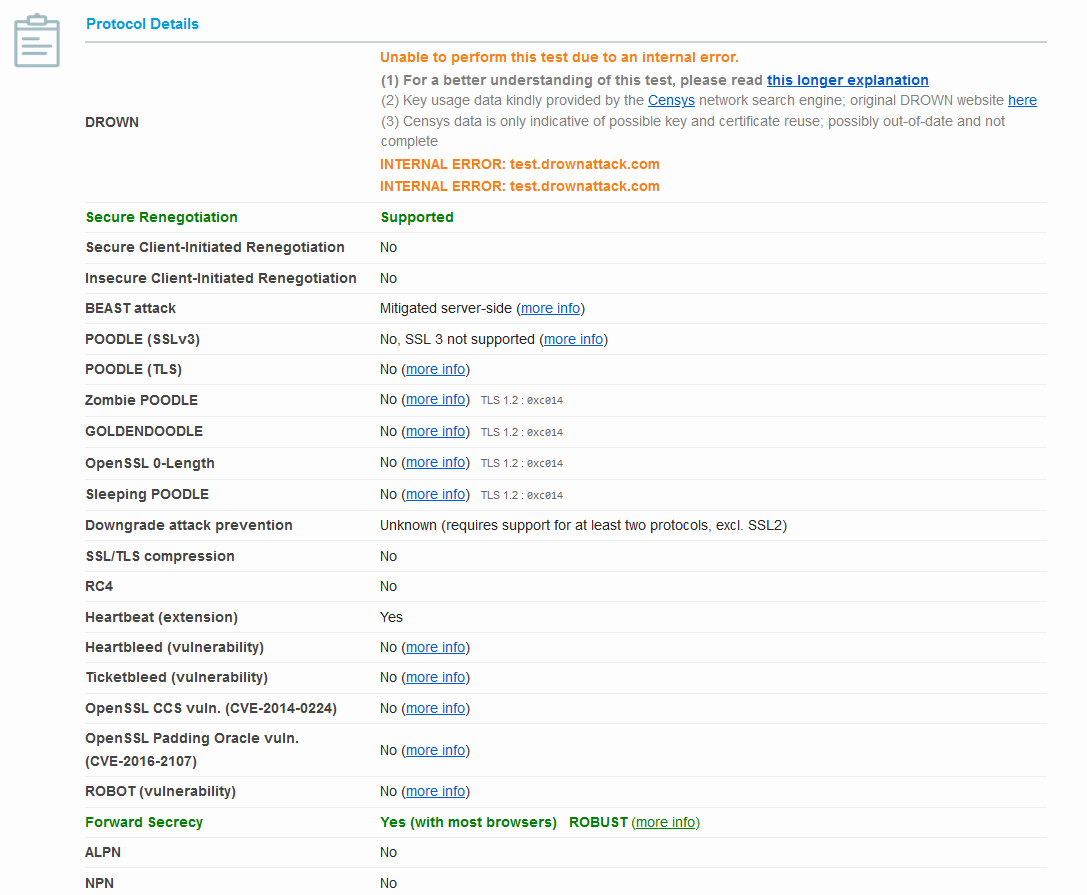
**Here the "WEAK" tag suggests that this cipher suite may be considered weak by modern security standards. In particular, using a 128-bit key for AES encryption is generally considered weaker than using a 256-bit key.**

****

**Lets understand 1 field**

**For example- Handshake Simulation Android 4.4.2 RSA 2048 (SHA256) TLS 1.2 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 ECDH secp256r1 FS**

**The provided information describes a handshake simulation for establishing a secure TLS 1.2 connection using the "TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384" cipher suite with the ECDH key exchange mechanism and Forward Secrecy (FS). This handshake simulation is for an Android 4.4.2 device:**

****

**LETS dissect Some of above listed protocols and safety features-**

1. **Secure Renegotiation Supported :This indicates that the server supports secure renegotiation, which means that it can establish a new encryption session securely after the initial handshake. Secure renegotiation is an important security feature to protect against certain attacks.**
2. **Secure Client-Initiated Renegotiation :This states that the client-initiated renegotiation is not supported, which is generally a good security practice. Client-initiated renegotiation has been a source of security vulnerabilities in the past, and many servers disable it.**
3. **Insecure Client-Initiated Renegotiation :This indicates that insecure client-initiated renegotiation is not supported, which is a positive security measure. Insecure client-initiated renegotiation can potentially be exploited by attackers.**
4. **BEAST attack Mitigated server-side :The BEAST (Browser Exploit Against SSL/TLS) attack is mentioned as being mitigated server-side. This means that the server has taken measures to protect against the BEAST attack. The BEAST attack is a cryptographic vulnerability related to the use of certain block ciphers in TLS. Mitigation measures are necessary to prevent this attack.**
5. **POODLE (SSLv3) :It indicates that the server does not support SSL 3, which is good from a security perspective. The POODLE (Padding Oracle On Downgraded Legacy Encryption) attack is a vulnerability in SSL 3. Since SSL 3 is not supported, the server is not vulnerable to this attack through that protocol.**
6. **POODLE (TLS):It states that the server is not vulnerable to the POODLE attack in the context of TLS. The POODLE attack in TLS is different from the SSL 3 version and also poses a security risk. The fact that it's not supported or vulnerable in TLS is a positive security aspect.**

****

**The HTTP request listed indicates an HTTP GET request made to the URL "**[**https://vtop.vit.ac.in/**](https://vtop.vit.ac.in/)**," and the server has responded with an HTTP/1.1 302 status code.**

# We will try to gain some more passive information by using new tool known as whois tool-Passive Reconnaissance-

# 

# 

# As we can see we only have some information only like domain name,Registrar name,state,country,email is also not provided

# 

# 

# Here we tried to collect some information but only get few such as domain id,creation date,expiry date,domain status the rest all are mentioned as redacted for privacy- in place of a phone number or some other contact information. This is a common practice to protect sensitive information when sharing or displaying it publicly which is a very good thing.

# Shodan report-This shows us some open ports,location which domain is accessed ,technology,protocol versions,products and vulnerability which are not yet reported or identified publically

# 

# 

# 

# Inference-again it is noticed that any sensitive information or vulnerability is not yet mentioned

# Censys Search- Censys is a search engine and online service that specializes in Internet-wide scanning and searching for information about devices, networks, and services on the internet. It's commonly used for security research, network monitoring, and asset discovery.

# 

# Here we got some basic information like network, routing, protocols ,location time zone,details of 80/HTTP type,response body hashes

# 

# Trust chart of browsers

# 

# Browser trust, public key info ,fingerprint .

# 

# 

# Here first time in our info collection we get some info like mobile number,address of the registrant

# 

**We got some contacts and address of administrative ,technical of the registrant**

**SUMMARY OF THE REPORT-**

**Summary of Passive Reconnaissance Report on VIT Vellore Website:**

1. **Secure Configuration: The website is configured securely with best practices in place. The web server, database server, and other infrastructure components are well-configured to resist common attacks.**
2. **No Sensitive Information Leakage: The passive reconnaissance did not reveal any sensitive information being inadvertently disclosed by the website. This includes not finding any exposed login credentials, personal data, or confidential documents.**
3. **No Obvious Vulnerabilities: There were no obvious vulnerabilities detected in the website's public-facing components. This indicates that the website's software and plugins are up to date and not susceptible to known vulnerabilities.**
4. **Limited Attack Surface: The website has a limited attack surface, meaning that there are fewer entry points or potential vulnerabilities exposed to external attackers.**
5. **Protection Against Scraping: The website may have measures in place to prevent data scraping or information harvesting by malicious actors.**
6. **Robust Privacy Practices: The website seems to follow robust privacy practices by not disclosing sensitive information about its users or internal systems.**
7. **Security Awareness: The organization behind the website appears to have a good level of security awareness and has taken steps to protect its online assets.**
8. **Continuous Monitoring: It's important to note that the security posture of a website can change over time. Regular monitoring and security assessments are necessary to ensure ongoing protection.**