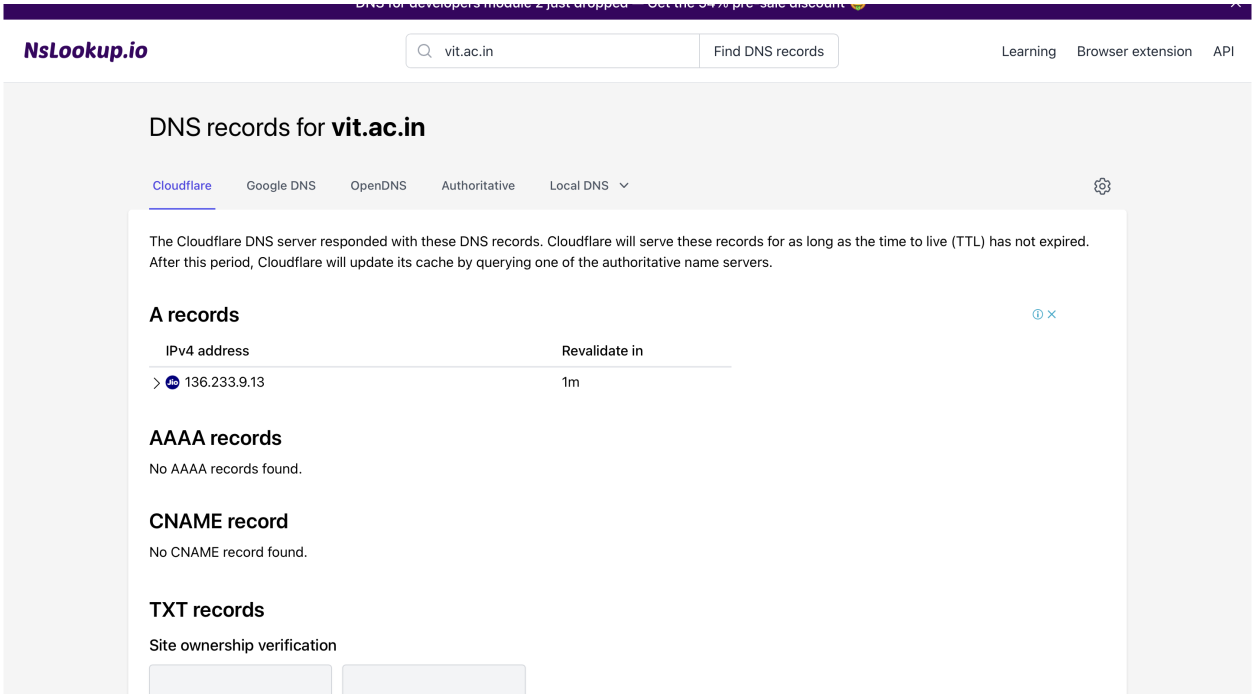
Assignment_3

Vulerabilities scan

Website: https://vit.ac.in

- Using NsLookup for DNS record:



DNS records for **vit.ac.in**

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
136.233.9.13	1m

AAAA records

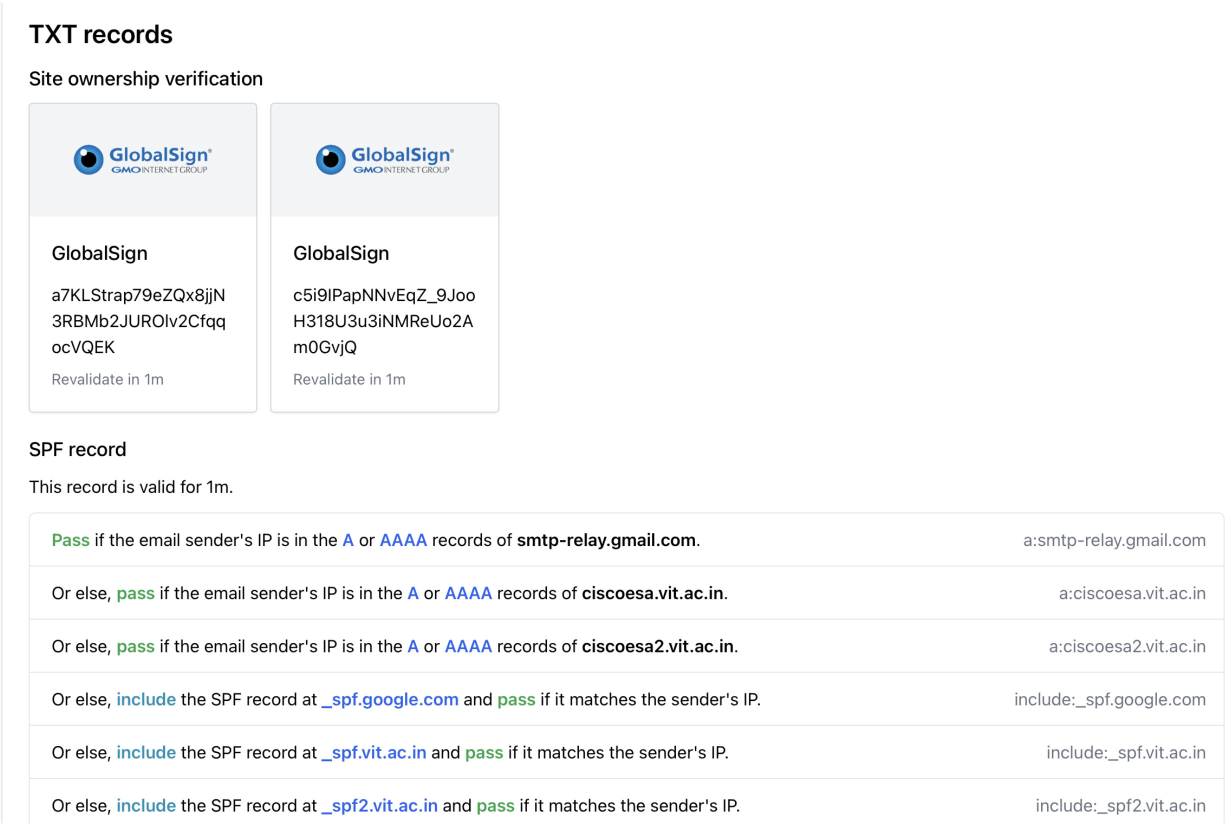
No AAAA records found.

CNAME record

No CNAME record found.

TXT records

Site ownership verification



TXT records

Site ownership verification

GlobalSign

a7KLStrap79eZQx8jjN3RBMb2JUROlv2CfqqocVQEK

Revalidate in 1m

GlobalSign

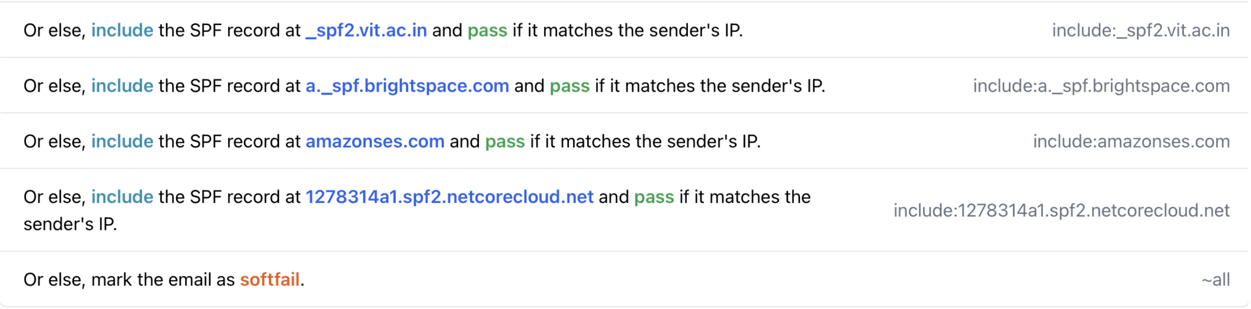
c5i9IPapNNvEqZ_9JooH318U3u3iNMReUo2Am0GvjQ

Revalidate in 1m

SPF record

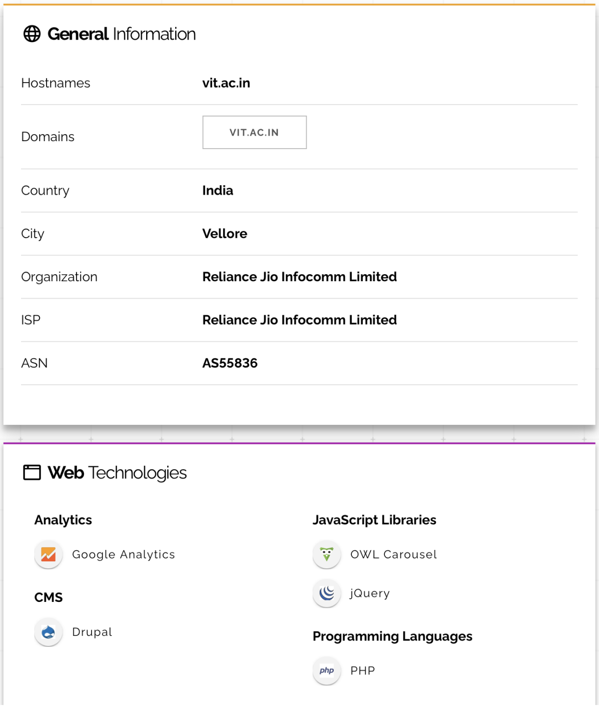
This record is valid for 1m.

Pass if the email sender's IP is in the A or AAAA records of **smtp-relay.gmail.com**.	a:smtp-relay.gmail.com
Or else, pass if the email sender's IP is in the A or AAAA records of **ciscoesa.vit.ac.in**.	a:ciscoesa.vit.ac.in
Or else, pass if the email sender's IP is in the A or AAAA records of **ciscoesa2.vit.ac.in**.	a:ciscoesa2.vit.ac.in
Or else, include the SPF record at _spf.google.com and pass if it matches the sender's IP.	include:_spf.google.com
Or else, include the SPF record at _spf.vit.ac.in and pass if it matches the sender's IP.	include:_spf.vit.ac.in
Or else, include the SPF record at _spf2.vit.ac.in and pass if it matches the sender's IP.	include:_spf2.vit.ac.in



Or else, include the SPF record at _spf2.vit.ac.in and pass if it matches the sender's IP.	include:_spf2.vit.ac.in
Or else, include the SPF record at a._spf.brightspace.com and pass if it matches the sender's IP.	include:a._spf.brightspace.com
Or else, include the SPF record at amazonses.com and pass if it matches the sender's IP.	include:amazonses.com
Or else, include the SPF record at 1278314a1.spf2.netcorecloud.net and pass if it matches the sender's IP.	include:1278314a1.spf2.netcorecloud.net
Or else, mark the email as softfail.	~all

- Using shodan.io:



General Information

Hostnames	vit.ac.in
Domains	VIT.AC.IN
Country	India
City	Vellore
Organization	Reliance Jio Infocomm Limited
ISP	Reliance Jio Infocomm Limited
ASN	AS55836

Web Technologies

Analytics

Google Analytics

CMS

Drupal

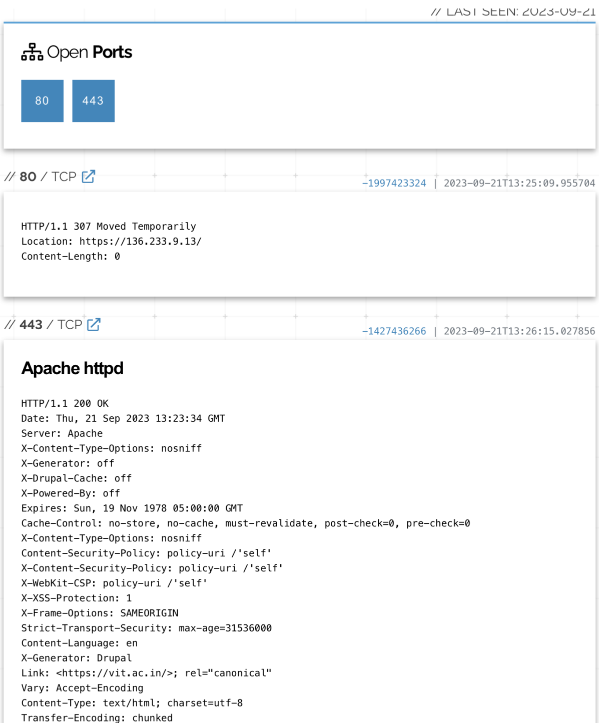
JavaScript Libraries

OWL Carousel

jQuery

Programming Languages

PHP



// LAST SEEN: 2023-09-21

Open Ports

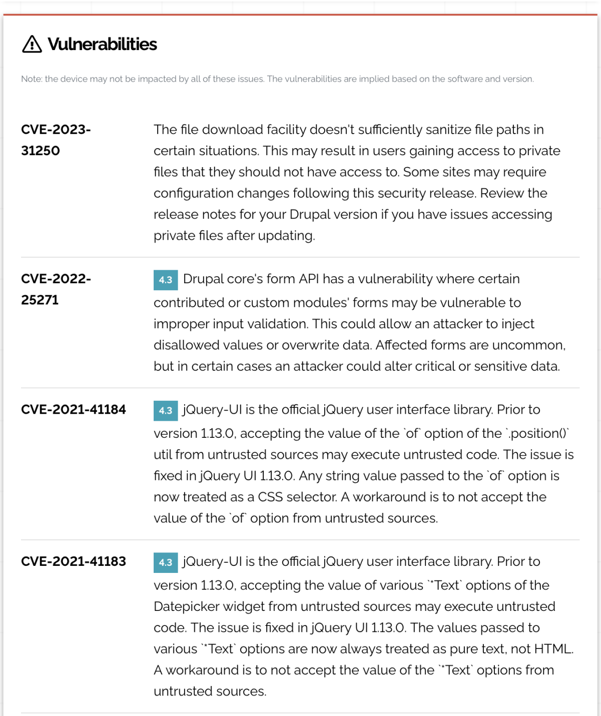
// **80** / TCP   -1997423324 | 2023-09-21T13:25:09.955704

```
HTTP/1.1 307 Moved Temporarily
Location: https://136.233.9.13/
Content-Length: 0
```

// **443** / TCP   -1427436266 | 2023-09-21T13:26:15.027856

Apache httpd

```
HTTP/1.1 200 OK
Date: Thu, 21 Sep 2023 13:23:34 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Generator: off
X-Drupal-Cache: off
X-Powered-By: off
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
X-Content-Type-Options: nosniff
Content-Security-Policy: policy-uri /'self'
X-Content-Security-Policy: policy-uri /'self'
X-WebKit-CSP: policy-uri /'self'
X-XSS-Protection: 1
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Content-Language: en
X-Generator: Drupal
Link: <https://vit.ac.in/>; rel="canonical"
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
```



Vulnerabilities

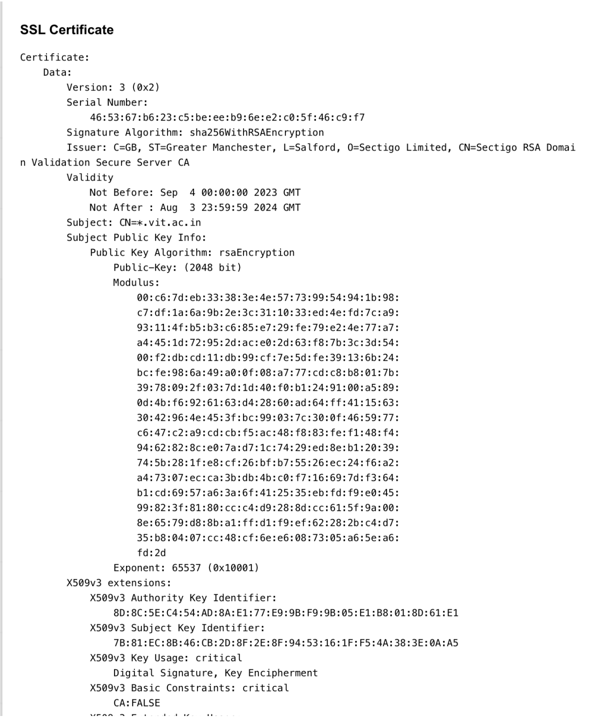
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-31250 The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.

CVE-2022-25271 4.3 Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.

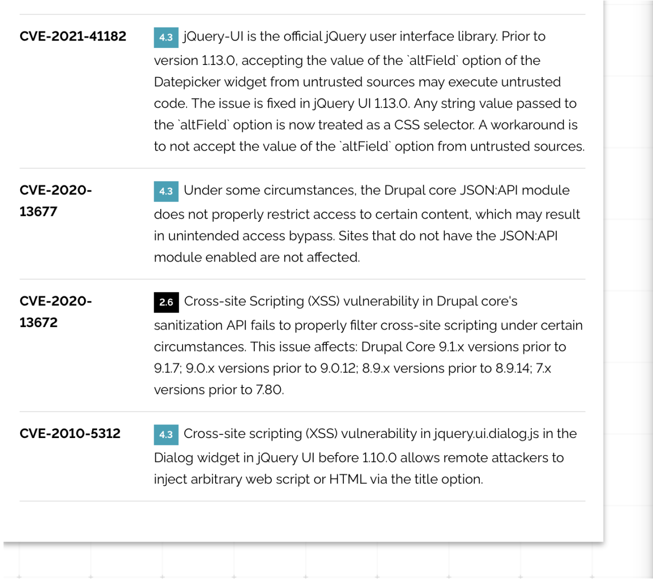
CVE-2021-41184 4.3 jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

CVE-2021-41183 4.3 jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.

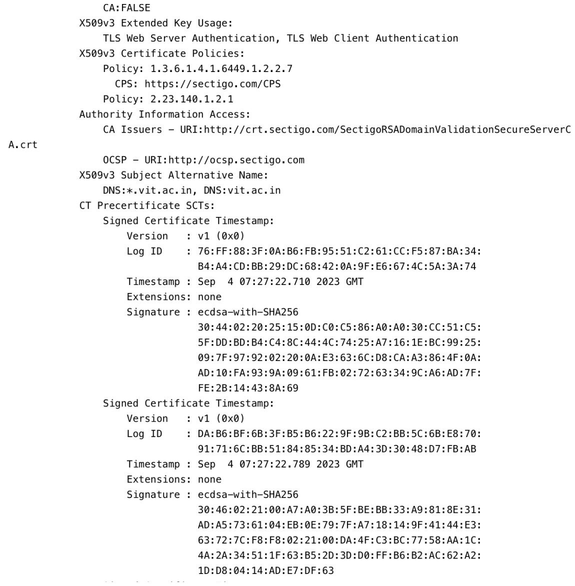


SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            46:53:67:b6:23:c5:be:ee:b9:6e:e2:c0:5f:46:c9:f7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domai
n Validation Secure Server CA
        Validity
            Not Before: Sep  4 00:00:00 2023 GMT
            Not After : Aug  3 23:59:59 2024 GMT
        Subject: CN=*.vit.ac.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c6:7d:eb:33:38:3e:4e:57:73:99:54:94:1b:98:
                    c7:df:1a:6a:9b:2e:3c:31:10:33:ed:4e:fd:7c:a9:
                    93:11:4f:b5:b3:c6:85:e7:29:fe:79:e2:4e:77:a7:
                    a4:45:1d:72:95:2d:ac:e0:2d:63:f8:7b:3c:3d:54:
                    00:f2:db:cd:11:db:99:cf:7e:5d:fe:39:13:6b:24:
                    bc:fe:98:6a:49:a0:0f:08:a7:77:cd:c8:b8:01:7b:
                    39:78:09:2f:03:7d:1d:40:f0:b1:24:91:00:a5:89:
                    0d:4b:f6:92:61:63:d4:28:60:ad:64:ff:41:15:63:
                    30:42:96:4e:45:3f:bc:99:03:7c:30:0f:46:59:77:
                    c6:47:c2:a9:cd:cb:f5:ac:48:f8:83:fe:f1:48:f4:
                    94:62:82:8c:e0:7a:d7:1c:74:29:ed:8e:b1:20:39:
                    74:5b:28:1f:e8:cf:26:bf:b7:55:26:ec:24:f6:a2:
                    a4:73:07:ec:ca:3b:db:4b:c0:f7:16:69:7d:f3:64:
                    b1:cd:69:57:a6:3a:6f:41:25:35:eb:fd:f9:e0:45:
                    99:82:3f:81:80:cc:c4:d9:28:8d:cc:61:5f:9a:00:
                    8e:65:79:d8:8b:a1:ff:d1:f9:ef:62:28:2b:c4:d7:
                    35:b8:04:07:cc:48:cf:6e:e6:08:73:05:a6:5e:a6:
                    fd:2d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1
            X509v3 Subject Key Identifier:
                7B:81:EC:8B:46:CB:2D:8F:2E:8F:94:53:16:1F:F5:4A:38:3E:0A:A5
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints: critical
                CA:FALSE
```



CVE-2021-41182	4.3 jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.
CVE-2020-13677	4.3 Under some circumstances, the Drupal core JSON:API module does not properly restrict access to certain content, which may result in unintended access bypass. Sites that do not have the JSON:API module enabled are not affected.
CVE-2020-13672	2.6 Cross-site Scripting (XSS) vulnerability in Drupal core's sanitization API fails to properly filter cross-site scripting under certain circumstances. This issue affects: Drupal Core 9.1.x versions prior to 9.1.7; 9.0.x versions prior to 9.0.12; 8.9.x versions prior to 8.9.14; 7.x versions prior to 7.80.
CVE-2010-5312	4.3 Cross-site scripting (XSS) vulnerability in jquery.ui.dialog.js in the Dialog widget in jQuery UI before 1.10.0 allows remote attackers to inject arbitrary web script or HTML via the title option.



```
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.6449.1.2.2.7
                  CPS: https://sectigo.com/CPS
                Policy: 2.23.140.1.2.1
            Authority Information Access:
                CA Issuers - URI:http://crt.sectigo.com/SectigoRSADomainValidationSecureServerC
A.crt
                OCSP - URI:http://ocsp.sectigo.com
            X509v3 Subject Alternative Name:
                DNS:*.vit.ac.in, DNS:vit.ac.in
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 76:FF:88:3F:0A:B6:FB:95:51:C2:61:CC:F5:87:BA:34:
                                B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74
                    Timestamp : Sep  4 07:27:22.710 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:44:02:20:25:15:0D:C0:C5:86:A0:A0:30:CC:51:C5:
                                5F:DD:BD:B4:C4:8C:44:4C:74:25:A7:16:1E:BC:99:25:
                                09:7F:97:92:02:20:0A:E3:63:6C:D8:CA:A3:86:4F:0A:
                                AD:10:FA:93:9A:09:61:FB:02:72:63:34:9C:A6:AD:7F:
                                FE:2B:14:43:8A:69
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70:
                                91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB
                    Timestamp : Sep  4 07:27:22.789 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:A7:A0:3B:5F:BE:BB:33:A9:81:8E:31:
                                AD:A5:73:61:04:EB:0E:79:7F:A7:18:14:9F:41:44:E3:
                                63:72:7C:F8:F8:02:21:00:DA:4F:C3:BC:77:58:AA:1C:
                                4A:2A:34:51:1F:63:B5:2D:3D:D0:FF:B6:B2:AC:62:A2:
                                1D:D8:04:14:AD:E7:DF:63
```