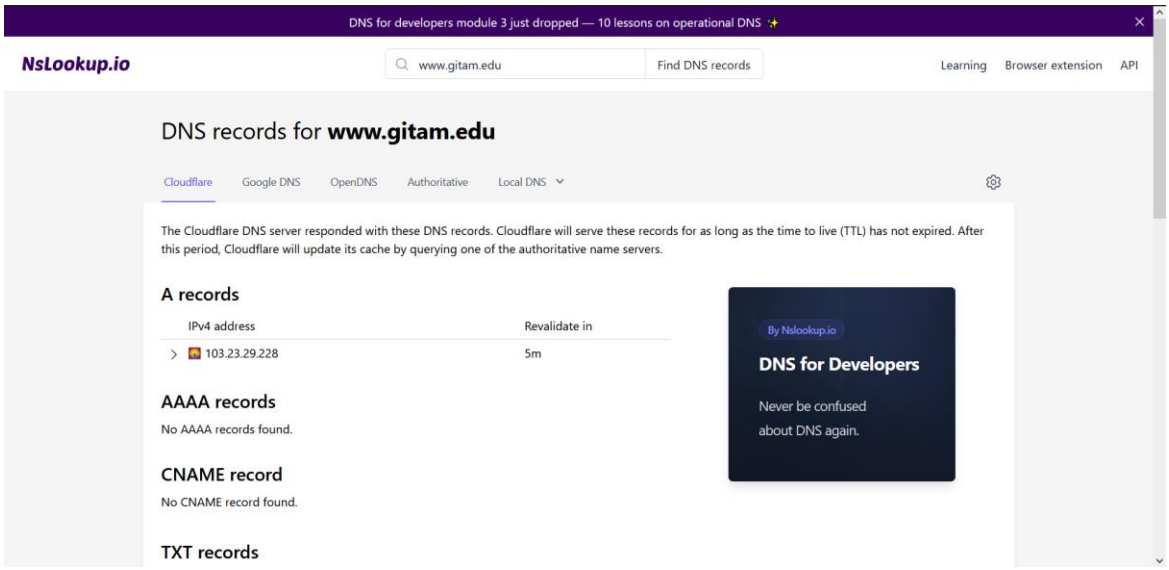
TASK 5

Overview

Select any website and collect footprint reconnaissance information about it. Do passive reconnaissance (nslookup.io , Nessus and Shodan).

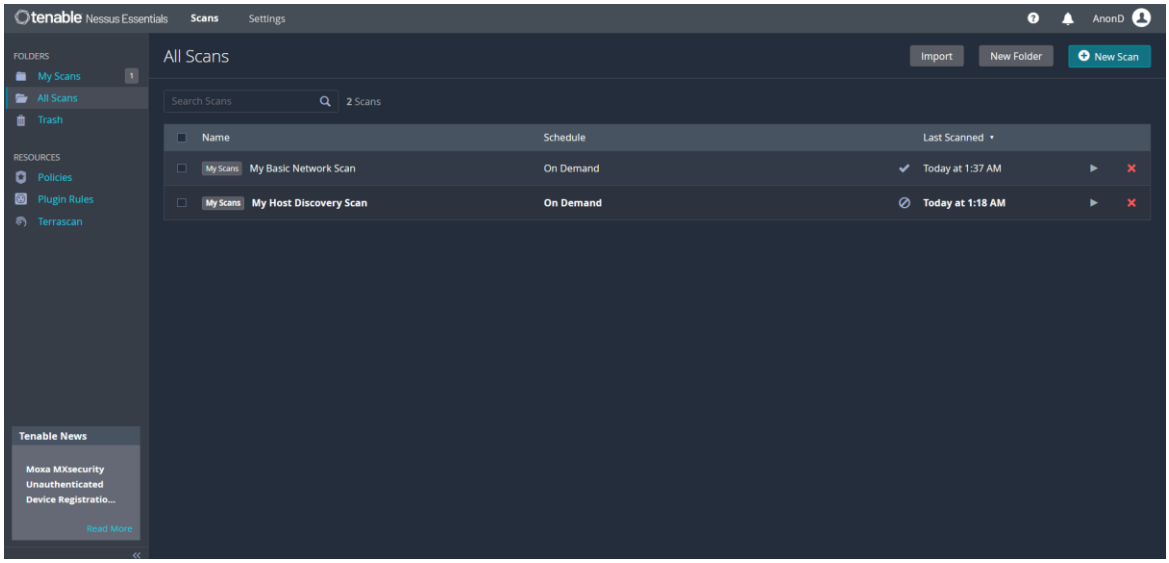
nslookup.io

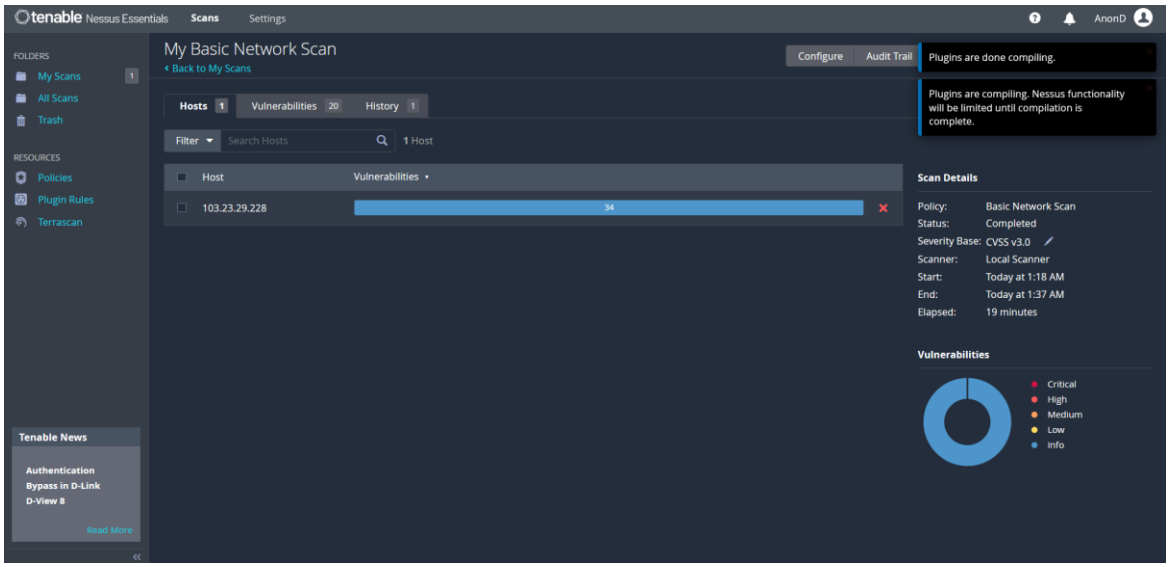
The nslookup.io is a web-based service that provides network-related information. It allows users to perform Domain Name System (DNS) lookups to obtain details about domain names and IP addresses. Users can enter a domain or an IP address to retrieve DNS records, including A (IPv4), AAAA (IPv6), MX (mail exchange), and TXT (text) records. This tool is valuable for network administrators and cybersecurity professionals as it aids in diagnosing DNS-related issues and verifying domain configurations.

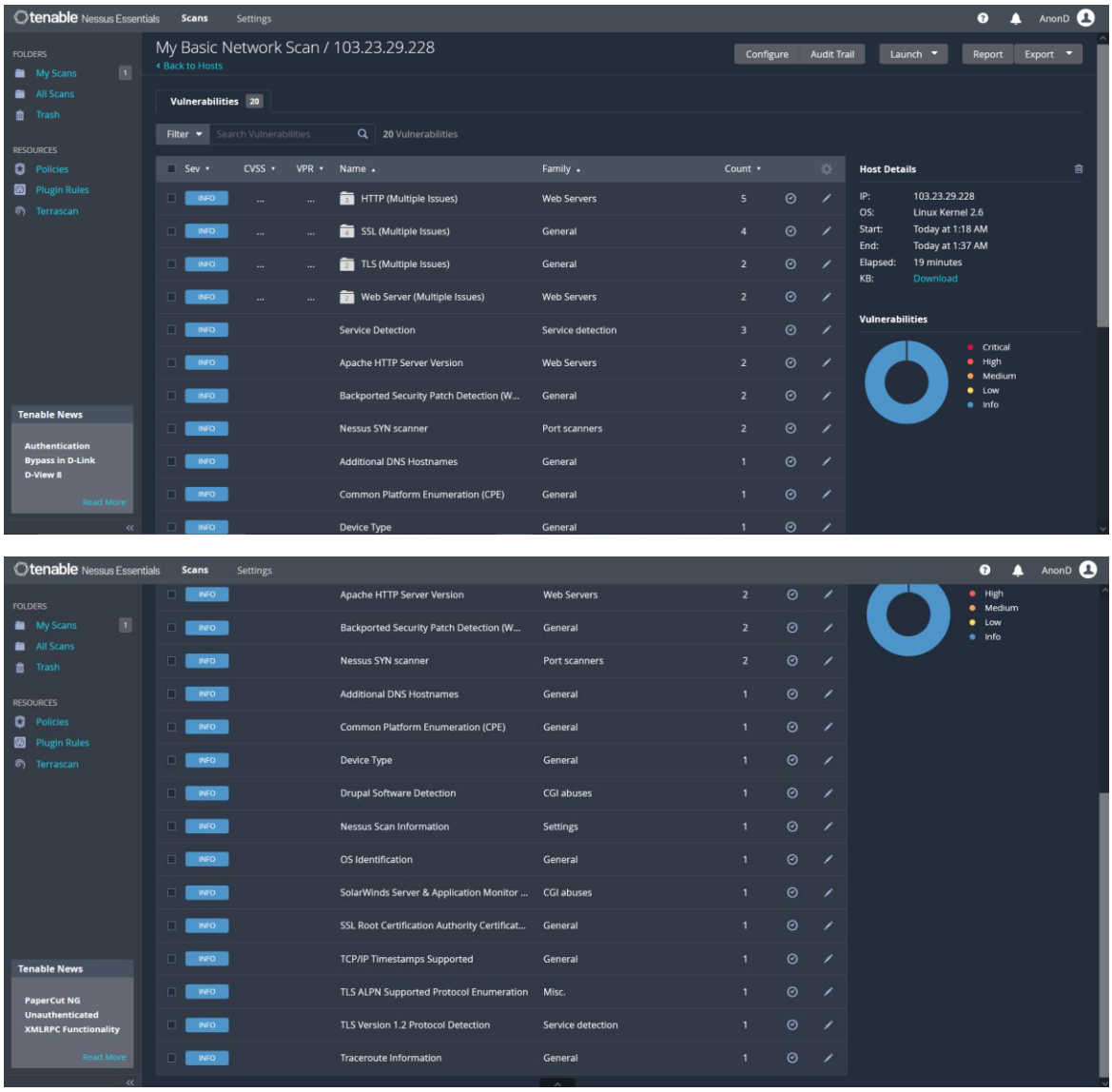


Nessus

Nessus is a widely used vulnerability scanner and assessment tool. It is designed to identify security vulnerabilities in systems and networks. Nessus scans for a wide range of issues, including software vulnerabilities, misconfigurations, and security weaknesses. It provides detailed reports to help organizations improve their security posture. Nessus is commonly employed by cybersecurity professionals to conduct security assessments and prioritize remediation efforts.

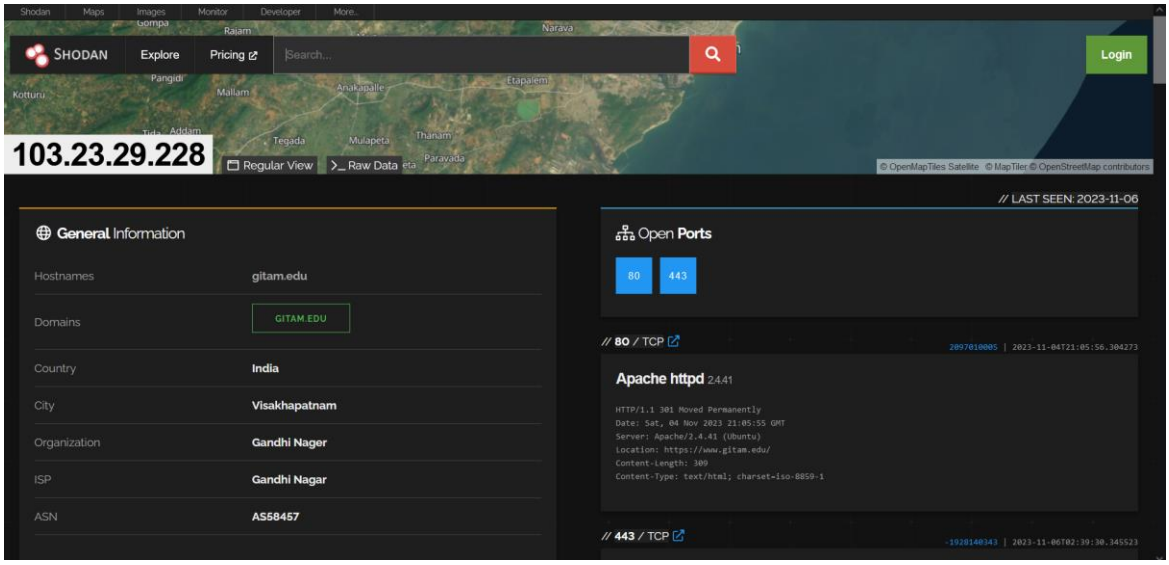


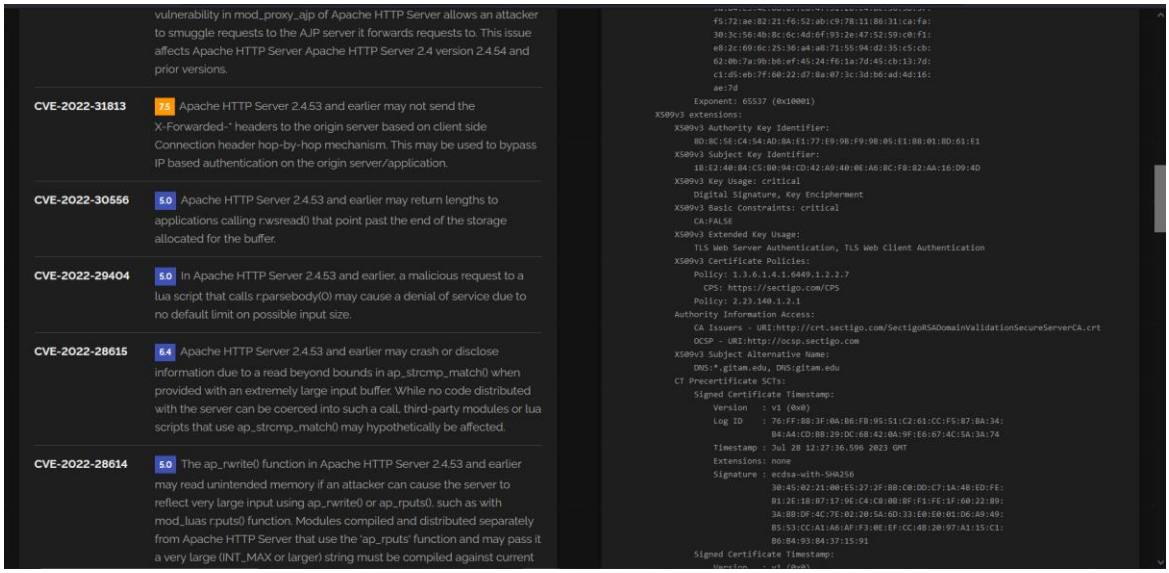


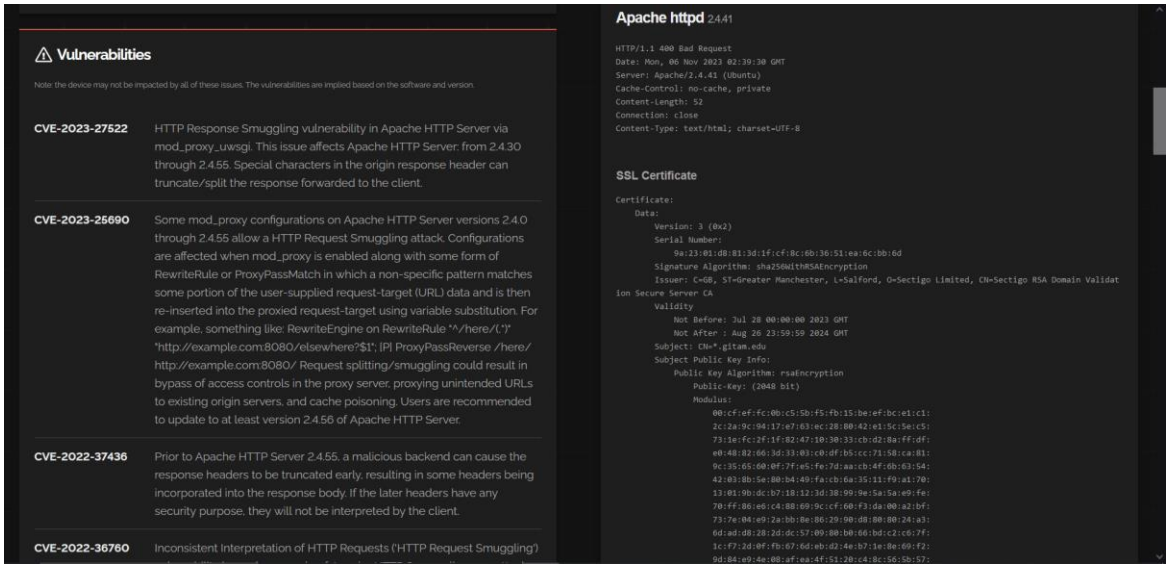


Shodan

Shodan is a specialized search engine that scans the internet for connected devices and services. It helps users discover exposed, potentially vulnerable systems and devices. Shodan can search for specific types of devices, open ports, and other characteristics, making it useful for cybersecurity researchers, penetration testers, and even malicious actors seeking to identify potential targets. While Shodan has legitimate uses, it underscores the importance of securing devices and services exposed to the internet to avoid exploitation by malicious actors.


Shodan
Maps
Images
Monitor
Developer
More..
SHODAN
Explore
Pricing
Search...
Login
103.23.29.228
Regular View
Raw Data
© OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors
// LAST SEEN: 2023-11-06
General Information
Hostnames gitam.edu
Domains GITAM.EDU
Country India
City Visakhapatnam
Organization Gandhi Nager
ISP Gandhi Nagar
ASN AS58457
Open Ports
80
443
// 80 / TCP
2097010005 | 2023-11-04T21:05:56.304273
Apache httpd 2.4.41
HTTP/1.1 301 Moved Permanently
Date: Sat, 04 Nov 2023 21:05:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: https://www.gitam.edu/
Content-Length: 309
Content-Type: text/html; charset=iso-8859-1
// 443 / TCP
-1920140343 | 2023-11-06T02:39:30.345523


vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
CVE-2022-31813 7.5 Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2022-30556 5.0 Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
CVE-2022-29404 5.0 In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-28615 6.4 Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
CVE-2022-28614 5.0 The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current
f5:72:ae:82:21:f6:52:ab:c9:78:11:86:31:ca:fa:
30:3c:56:4b:8c:6c:4d:6f:93:2e:47:52:59:c0:f1:
e8:2c:69:6c:25:36:a4:a8:71:55:94:d2:35:c5:cb:
62:0b:7a:9b:b6:ef:45:24:f6:1a:7d:45:cb:13:7d:
c1:d5:eb:7f:60:22:d7:8a:07:3c:3d:b6:ad:4d:16:
ae:7d
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Authority Key Identifier:
BD:BC:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:88:01:BD:61:E1
X509v3 Subject Key Identifier:
10:E2:40:84:C5:B0:94:CD:42:A9:40:0E:A6:BC:FB:82:AA:16:D9:4D
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Basic Constraints: critical
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/SectigoRSADomainValidationSecureServerCA.crt
OCSP - URI:http://ocsp.sectigo.com
X509v3 Subject Alternative Name:
DNS:*.gitam.edu, DNS:gitam.edu
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 : Jul 28 12:27:36.596 2023 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:02:21:00:E5:27:2F:BB:C0:DD:C7:1A:48:ED:FE:
B1:2E:18:B7:17:9E:C4:C8:00:BF:F1:FE:1F:60:22:89:
3A:BB:DF:4C:7E:02:20:5A:6D:33:E0:E0:01:D6:A9:49:
B5:53:CC:A1:A6:AF:F3:0E:EF:CC:4B:20:97:A1:15:C1:
B6:B4:93:84:37:15:91
Signed Certificate Timestamp:


Vulnerabilities
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.
CVE-2023-27522 HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.
CVE-2023-25690 Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
CVE-2022-37436 Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
CVE-2022-36760 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')
Apache httpd 2.4.41
HTTP/1.1 400 Bad Request
Date: Mon, 06 Nov 2023 02:39:30 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, private
Content-Length: 52
Connection: close
Content-Type: text/html; charset=UTF-8
SSL Certificate
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
9a:23:01:d8:81:3d:1f:cf:8c:6b:36:51:ea:6c:bb:6d
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Validity
Not Before: Jul 28 00:00:00 2023 GMT
Not After : Aug 26 23:59:59 2024 GMT
Subject: CN=*.gitam.edu
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:cf:ef:fc:0b:c5:5b:f5:fb:15:be:ef:bc:e1:c1:
2c:2a:9c:94:17:e7:63:ec:28:80:42:e1:5c:5e:c5:
73:1e:fc:2f:1f:82:47:10:30:33:cb:d2:8a:ff:df:
e0:48:02:66:3d:33:03:c0:df:b5:cc:71:58:ca:81:
9c:35:65:60:0f:7f:e5:fe:7d:aa:cb:4f:6b:63:54:
42:03:8b:5e:80:b4:49:fa:cb:6a:35:11:f9:a1:70:
13:01:9b:dc:b7:18:12:3d:38:09:9e:5a:5a:e9:fe:
70:ff:86:e6:c4:88:69:9c:cf:60:f3:da:00:a2:bf:
73:7e:04:e9:2a:bb:8e:86:29:90:d8:80:80:24:a3:
6d:ad:d8:28:2d:dc:57:09:80:b0:66:bd:c2:c6:7f:
1c:f7:2d:0f:fb:67:6d:eb:d2:4e:b7:1e:8e:69:f2:
9d:84:e9:4e:08:af:ea:4f:51:20:c4:8c:56:5b:57: