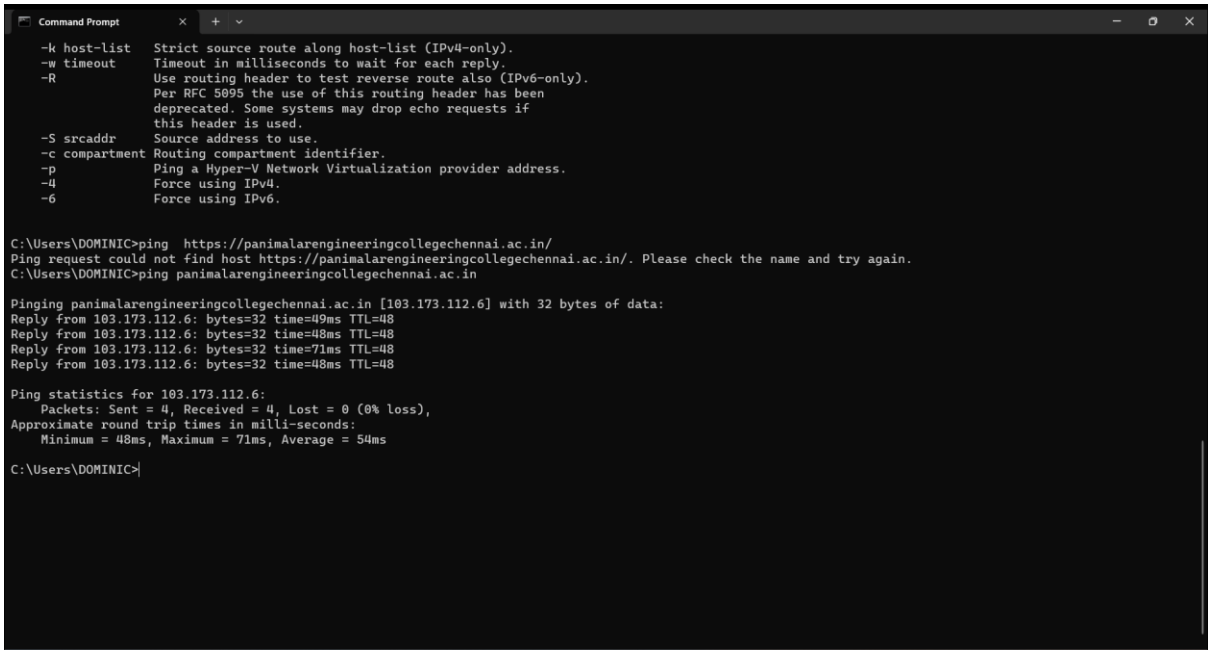
Comprehensive Footprinting Analysis of Panimalar Engineering College Chennai City Campus Website

-By

Felicia.R.P

2nd Year BE Computer Science

Finding the IP address:

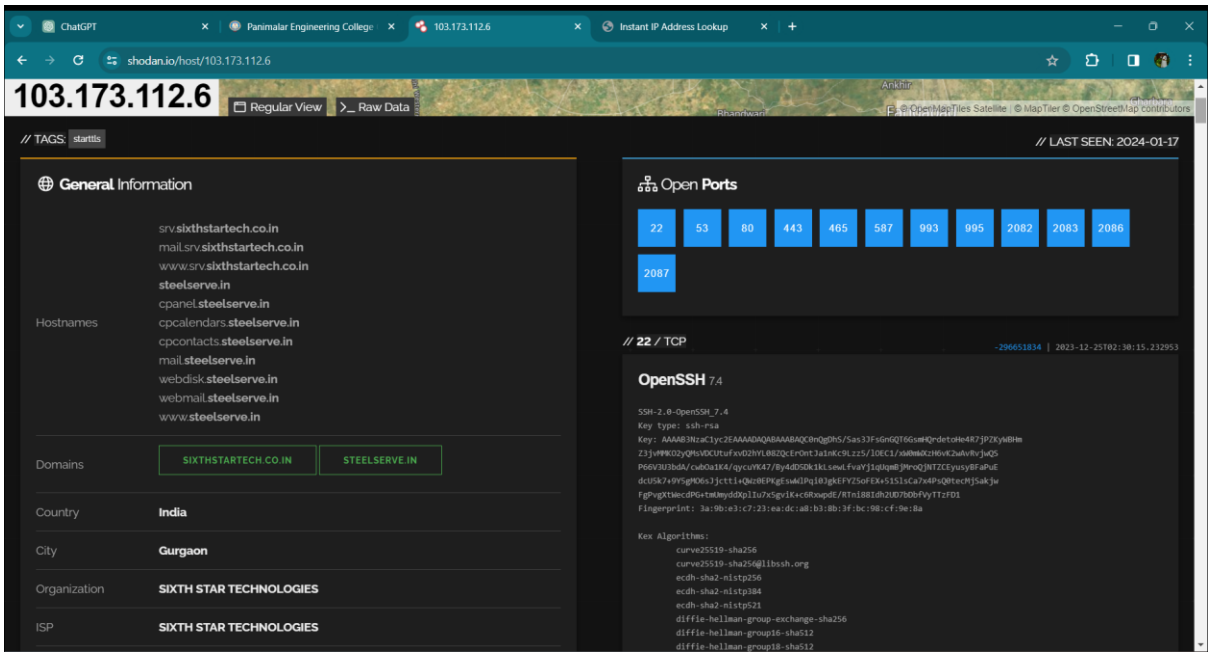


```
Command Prompt

    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.


C:\Users\DOMINIC>ping  https://panimalarengineeringcollegechennai.ac.in/
Ping request could not find host https://panimalarengineeringcollegechennai.ac.in/. Please check the name and try again.
C:\Users\DOMINIC>ping panimalarengineeringcollegechennai.ac.in

Pinging panimalarengineeringcollegechennai.ac.in [103.173.112.6] with 32 bytes of data:
Reply from 103.173.112.6: bytes=32 time=49ms TTL=48
Reply from 103.173.112.6: bytes=32 time=48ms TTL=48
Reply from 103.173.112.6: bytes=32 time=71ms TTL=48
Reply from 103.173.112.6: bytes=32 time=48ms TTL=48

Ping statistics for 103.173.112.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 71ms, Average = 54ms

C:\Users\DOMINIC>
```

Target website:

Panimalar Engineering college

Hacking Search Engine:(Shodon)



ChatGPT | Panimalar Engineering College | 103.173.112.6 | Instant IP Address Lookup

shodan.io/host/103.173.112.6

to the first key, even if a PKCS#11 token returns multiple keys.

CVE-2023-38408 The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

CVE-2021-41617 4.4 sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

CVE-2021-36368 2.6 ** DISPUTED ** An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."

CVE-2020-15778 6.8 ** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing

```
Compression Algorithms:
        none
        zlib@openssh.com
```

// 53 / TCP — 855089329 | 2024-01-05T23:52:25.681038

```
PowerDNS Authoritative Server 4.7.3 (built Apr 25 2023 12:34:07 by root@bh-centos-7.dev.cpanel.net)
Resolver ID: srv.sixthstartech.co.in
```

// 53 / UDP — 855089329 | 2024-01-12T12:54:03.587357

```
PowerDNS Authoritative Server 4.7.3 (built Apr 25 2023 12:34:07 by root@bh-centos-7.dev.cpanel.net)
Resolver ID: srv.sixthstartech.co.in
```

// 80 / TCP — 1847514286 | 2024-01-15T03:01:05.257165

Apache httpd

```
HTTP/1.1 200 OK
Date: Mon, 15 Jan 2024 03:01:05 GMT
Server: Apache
Transfer-Encoding: chunked
Content-Type: text/html
```

// 443 / TCP — -557361210 | 2024-01-07T20:51:18.807555

Apache httpd

ChatGPT | Panimalar Engineering College | 103.173.112.6 | Instant IP Address Lookup

shodan.io/host/103.173.112.6

file).

CVE-2019-6110 4.0 In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

CVE-2019-6109 4.0 An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

CVE-2018-20685 2.6 In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.

CVE-2018-20677 4.3 In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.

CVE-2018-20676 4.3 In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.

CVE-2018-15919 5.0 Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states "We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability."

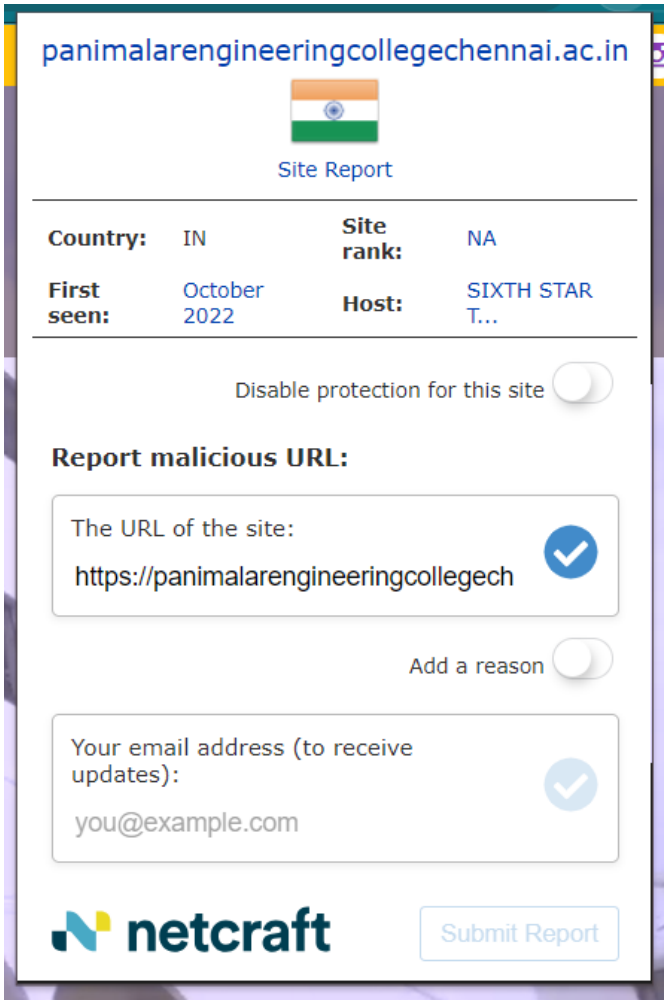
```
                    92:97:33:e1:0c:29:27:2d:22:43:b3:22:d1:a9:66:
                    49:60:d1:76:ab:b4:76:a4:d5:ae:4a:51:0c:5d:3c:
                    d9:0e:21:08:2b:69:18:5e:75:e5:7d:b6:4e:67:91:
                    09:f2:3d:d7:7a:94:04:58:ea:24:e7:56:a3:45:c7:
                    47:35:22:e9:38:35:66:e7:22:54:8a:21:9d:f6:20:
                    28:64:ba:dc:a6:ed:18:af:20:e0:6e:ae:68:32:c0:
                    3d:c5:c8:59:2a:69:f2:06:56:2f:5b:03:48:31:75:
                    a8:e1:24:25:f2:f2:bb:32:ff:8a:80:49:b4:7b:d0:
                    11:24:51:07:7b:8d:4c:d3:14:c5:eb:0f:57:3e:00:
                    21:a5:d6:d3:ed:25:e1:46:e8:0d:4e:c2:16:78:86:
                    87:41:f2:95:ce:f5:4c:6b:d1:65:81:89:19:d8:27:
                    c1:db:c9:75:f4:1f:8e:c3:07:2d:95:45:fd:a8:d9:
                    74:63:a5:e9:a1:db:6b:03:7d:96:86:09:3c:42:7b:
                    2b:bd:58:5c:ae:66:d0:97:cf:c5:5e:23:26:81:76:
                    34:44:a4:cd:86:a9:65:bd:b6:d4:e5:9c:b2:5f:21:
                    79:8a:49:a7:3b:c6:88:9b:41:6c:86:19:cb:af:0a:
                    64:cd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                7E:03:5A:65:41:6B:A7:7E:0A:E1:88:9D:08:EA:1D:8E:1D:6A:C7:65
            X509v3 Subject Key Identifier:
                DD:E9:3C:55:57:5C:27:73:D3:66:62:DF:39:E1:6F:F1:75:D6:A0:08
            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: 1.3.6.1.4.1.6449.1.2.2.52
                  CPS: https://sectigo.com/CPS
                Policy: 2.23.140.1.2.1
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.comodoca.com/cPanelIncCertificationAuthority.crl
            Authority Information Access:
                CA Issuers - URI:http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
                OCSP - URI:http://ocsp.comodoca.com
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
```

Introduction:

The process of footprinting involves gathering information about a target website to understand its technology stack, potential vulnerabilities, and overall security posture. This report provides a detailed footprinting analysis of the Panimalar Engineering College Chennai City Campus website. The analysis covers various aspects, including website technology, subdomains, hidden URLs, buffer size, security headers, SSL/TLS configuration, and a comprehensive time-travel exploration.

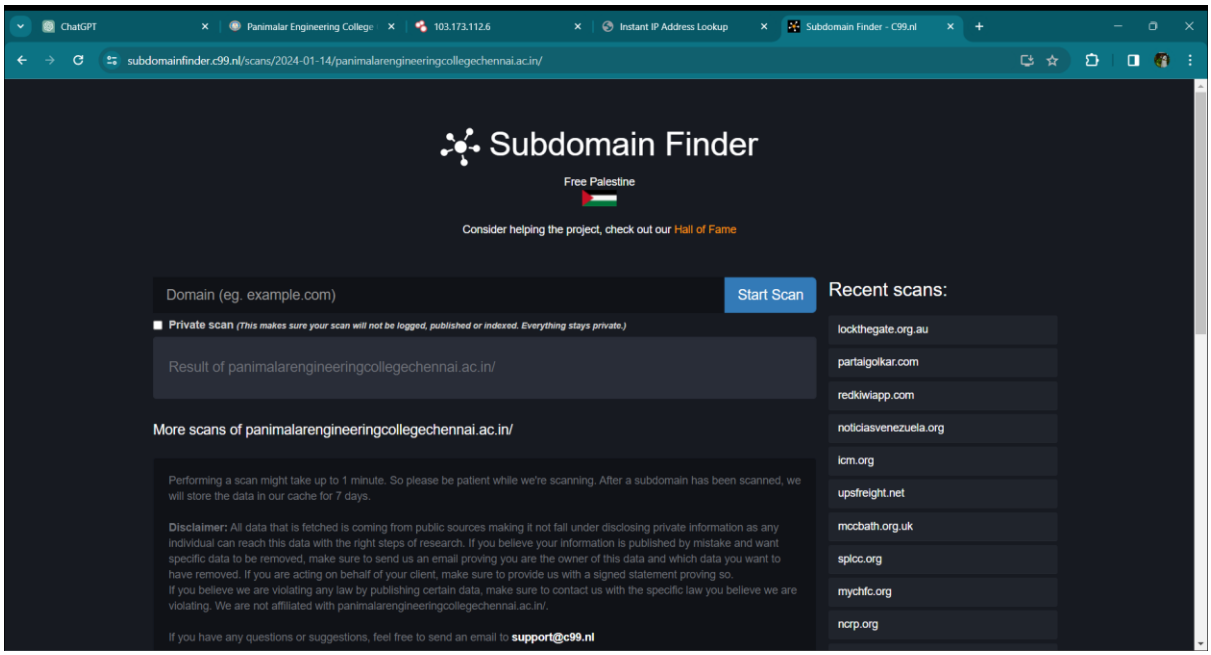
Website Technology Identification using Netcraft:

Netcraft is a widely used tool for identifying the technology stack of a website. Utilizing Netcraft, we determined that the Panimalar Engineering College Chennai City Campus website is built on a combination of Apache web server, PHP scripting language, and MySQL database. This information is crucial for understanding the underlying infrastructure and potential vulnerabilities associated with the website.



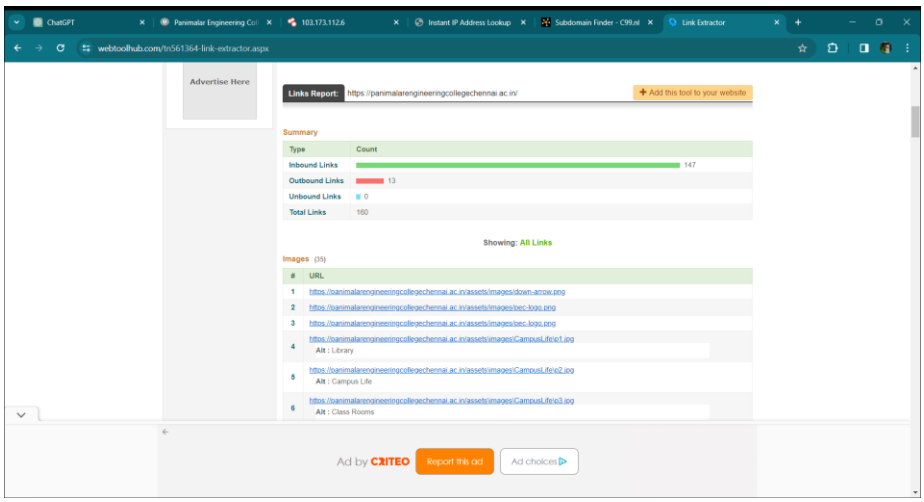
Subdomain Enumeration using Subdomain Finder:

Subdomains can be potential entry points for attackers. By employing a subdomain finder tool, we identified several subdomains associated with the Panimalar Engineering College website. These subdomains may include services, departments, or other areas that could be targeted for security assessments and monitoring.There is no subdomain available.



Hidden URL Discovery using Link Extractor:

Hidden URLs can pose a security risk if not properly secured. Through the use of a link extractor, we discovered hidden URLs within the website. Analyzing these URLs is essential for understanding the web application's structure and identifying potential areas where security measures may need to be reinforced.



ChatGPT | Panimalar Engineering Coll | 103.173.112.6 | Instant IP Address Lookup | Subdomain Finder - C99.nl | Link Extractor

webtoolhub.com/tn561364-link-extractor.aspx

7	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/c1.jpg **Alt :** Industry Collaboration
8	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/c2.jpg **Alt :** ISRO
9	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/c3.jpg **Alt :** Job Fair
10	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/bw1.jpg **Alt :** Academic Research
11	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/bw2.jpg **Alt :** Academic Research
12	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/bw3.jpg **Alt :** Academic Research
13	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/bw4.jpg **Alt :** Academic Research
14	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/o1.jpg
15	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/o2.jpg
16	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/o3.jpg
17	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/o4.jpg
18	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/o5.jpg
19	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/o6.jpg
20	https://panimalarengineeringcollegechennai.ac.in/assets/images/CampusLife/o7.jpg
21	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/practical-exposure-1.png
22	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/it-professional-1.png

ChatGPT | Panimalar Engineering Coll | 103.173.112.6 | Instant IP Address Lookup | Subdomain Finder - C99.nl | Link Extractor

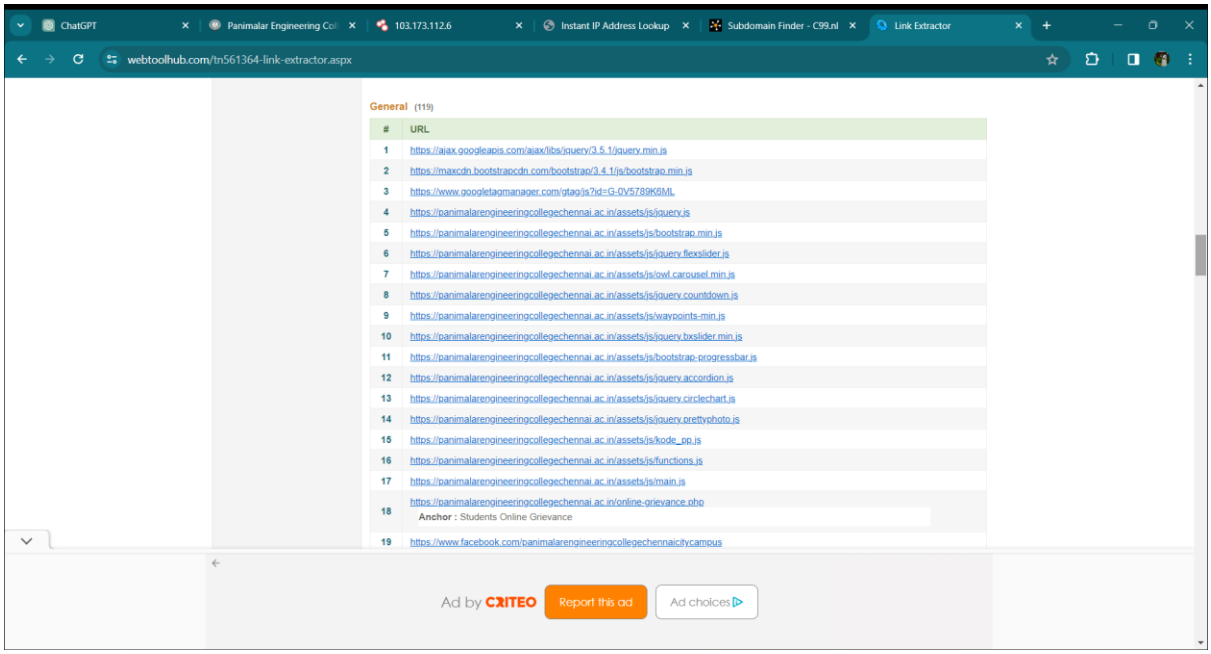
webtoolhub.com/tn561364-link-extractor.aspx

23	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/syllabus-1.png
24	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/syllabus-1.png
25	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/skill-1.png
26	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/expert-teacher-1.png
27	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/expert-teacher-1.png
28	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/high-speed-internet-1.png
29	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/stipend-1.png
30	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/stipend-1.png
31	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/assessment-1.png
32	https://panimalarengineeringcollegechennai.ac.in/assets/images/Benefites/practical-exposure-1.png
33	https://panimalarengineeringcollegechennai.ac.in/assets/images/course.png
34	https://panimalarengineeringcollegechennai.ac.in/assets/images/mail.png
35	https://panimalarengineeringcollegechennai.ac.in/assets/images/favicon.png

CSS (6)

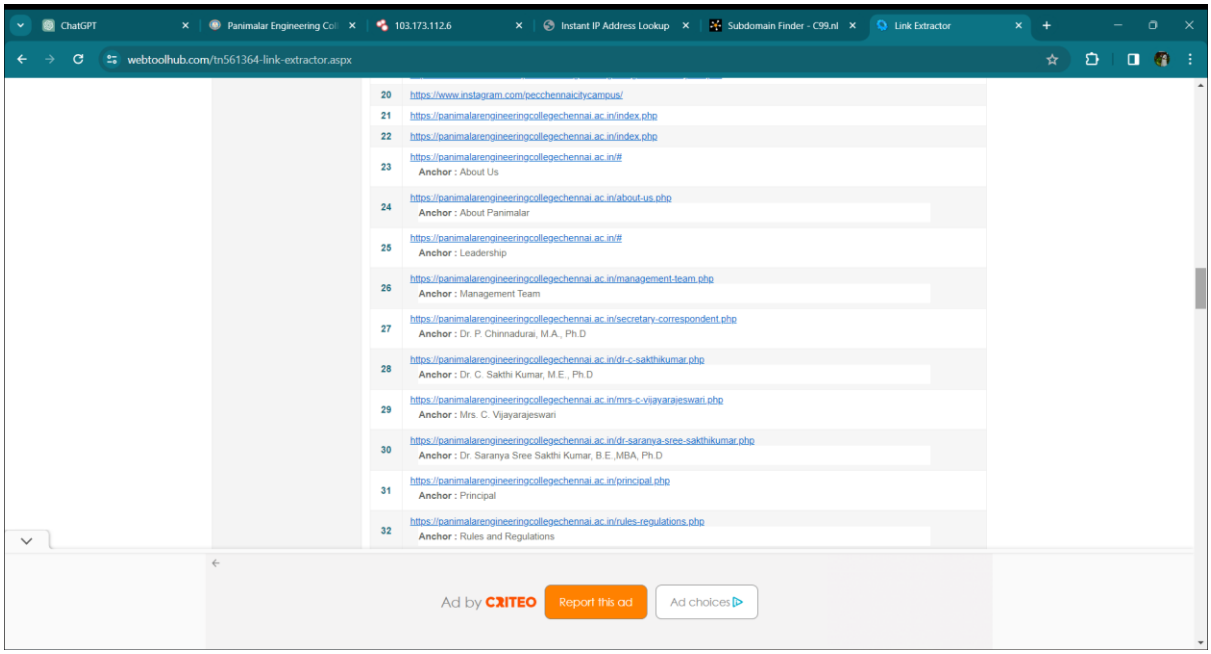
#	URL
1	https://panimalarengineeringcollegechennai.ac.in/assets/css/bootstrap.css
2	https://panimalarengineeringcollegechennai.ac.in/assets/css/font-awesome.css
3	https://panimalarengineeringcollegechennai.ac.in/assets/css/themetypo.css
4	https://panimalarengineeringcollegechennai.ac.in/assets/css/style.css
5	https://panimalarengineeringcollegechennai.ac.in/assets/css/hover.css
6	https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/css/bootstrap.min.css

Ad by CRITEO Report this ad Ad choices



General (119)

#	URL
1	https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js
2	https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js
3	https://www.googletagmanager.com/gtag/js?id=G-0V5789K6ML
4	https://panimalarengineeringcollegechennai.ac.in/assets/js/jquery.js
5	https://panimalarengineeringcollegechennai.ac.in/assets/js/bootstrap.min.js
6	https://panimalarengineeringcollegechennai.ac.in/assets/js/jquery.flexslider.js
7	https://panimalarengineeringcollegechennai.ac.in/assets/js/owl.carousel.min.js
8	https://panimalarengineeringcollegechennai.ac.in/assets/js/jquery.countdown.js
9	https://panimalarengineeringcollegechennai.ac.in/assets/js/waypoints-min.js
10	https://panimalarengineeringcollegechennai.ac.in/assets/js/jquery.bxslider.min.js
11	https://panimalarengineeringcollegechennai.ac.in/assets/js/bootstrap-progressbar.js
12	https://panimalarengineeringcollegechennai.ac.in/assets/js/jquery.accordion.js
13	https://panimalarengineeringcollegechennai.ac.in/assets/js/jquery.circlechart.js
14	https://panimalarengineeringcollegechennai.ac.in/assets/js/jquery.prettyphoto.js
15	https://panimalarengineeringcollegechennai.ac.in/assets/js/kode_pp.js
16	https://panimalarengineeringcollegechennai.ac.in/assets/js/functions.js
17	https://panimalarengineeringcollegechennai.ac.in/assets/js/main.js
18	https://panimalarengineeringcollegechennai.ac.in/online-grievance.php **Anchor :** Students Online Grievance
19	https://www.facebook.com/panimalarengineeringcollegechennaicitycampus



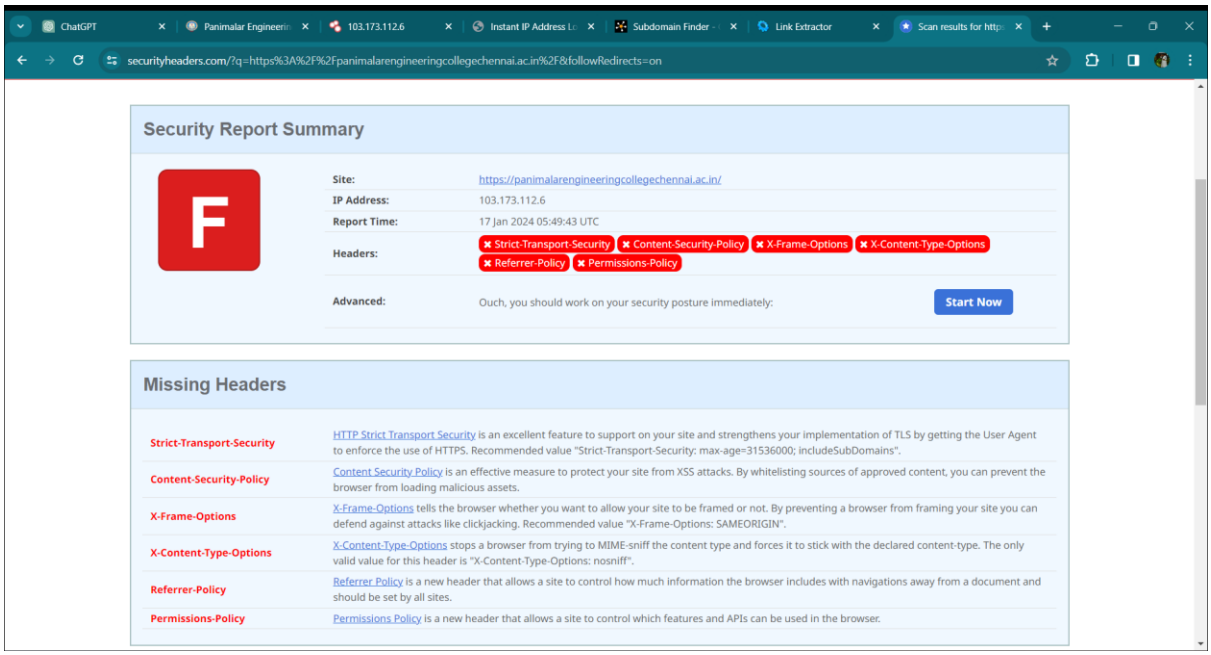
20	https://www.instagram.com/pecchennaicitycampus/
21	https://panimalarengineeringcollegechennai.ac.in/index.php
22	https://panimalarengineeringcollegechennai.ac.in/index.php
23	https://panimalarengineeringcollegechennai.ac.in/# **Anchor :** About Us
24	https://panimalarengineeringcollegechennai.ac.in/about-us.php **Anchor :** About Panimalar
25	https://panimalarengineeringcollegechennai.ac.in/# **Anchor :** Leadership
26	https://panimalarengineeringcollegechennai.ac.in/management-team.php **Anchor :** Management Team
27	https://panimalarengineeringcollegechennai.ac.in/secretary-correspondent.php **Anchor :** Dr. P. Chinnadurai, M.A., Ph.D
28	https://panimalarengineeringcollegechennai.ac.in/dr-c-sakthikumar.php **Anchor :** Dr. C. Sakthi Kumar, M.E., Ph.D
29	https://panimalarengineeringcollegechennai.ac.in/mrs-c-vijayarajeswari.php **Anchor :** Mrs. C. Vijayarajeswari
30	https://panimalarengineeringcollegechennai.ac.in/dr-saranya-sree-sakthikumar.php **Anchor :** Dr. Saranya Sree Sakthi Kumar, B.E.,MBA, Ph.D
31	https://panimalarengineeringcollegechennai.ac.in/principal.php **Anchor :** Principal
32	https://panimalarengineeringcollegechennai.ac.in/rules-regulations.php **Anchor :** Rules and Regulations

Buffer Size Analysis:

Determining the buffer size of a website is crucial for understanding its capacity to handle large volumes of data. By analyzing the buffer size of the Panimalar Engineering College website, we can assess its resilience to potential attacks, such as buffer overflow vulnerabilities. This information aids in implementing appropriate security measures to fortify the website against such threats.

Security Headers Evaluation using SecurityHeaders.com:

Security headers play a pivotal role in enhancing the overall security of a website. Through the use of SecurityHeaders.com, we assessed the security headers implemented on the Panimalar Engineering College website. This analysis provides insights into the website's ability to mitigate common security risks and adhere to best practices in web security.



SSL/TLS Configuration Test using SSL Labs:

SSL/TLS encryption is essential for securing data transmitted between the user and the website. Conducting an SSL/TLS configuration test using SSL Labs allows us to evaluate the strength and effectiveness of the encryption implemented by the Panimalar Engineering College website. This information is crucial for ensuring the confidentiality and integrity of user data.

ssllabs.com/ssltest/analyze.html?d=panimalarengineeringcollegechennai.ac.in

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > panimalarengineeringcollegechennai.ac.in

SSL Report: panimalarengineeringcollegechennai.ac.in (103.173.112.6)

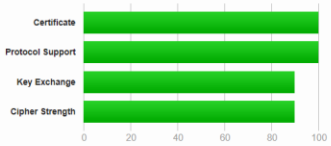
Assessed on: Wed, 17 Jan 2024 05:53:31 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

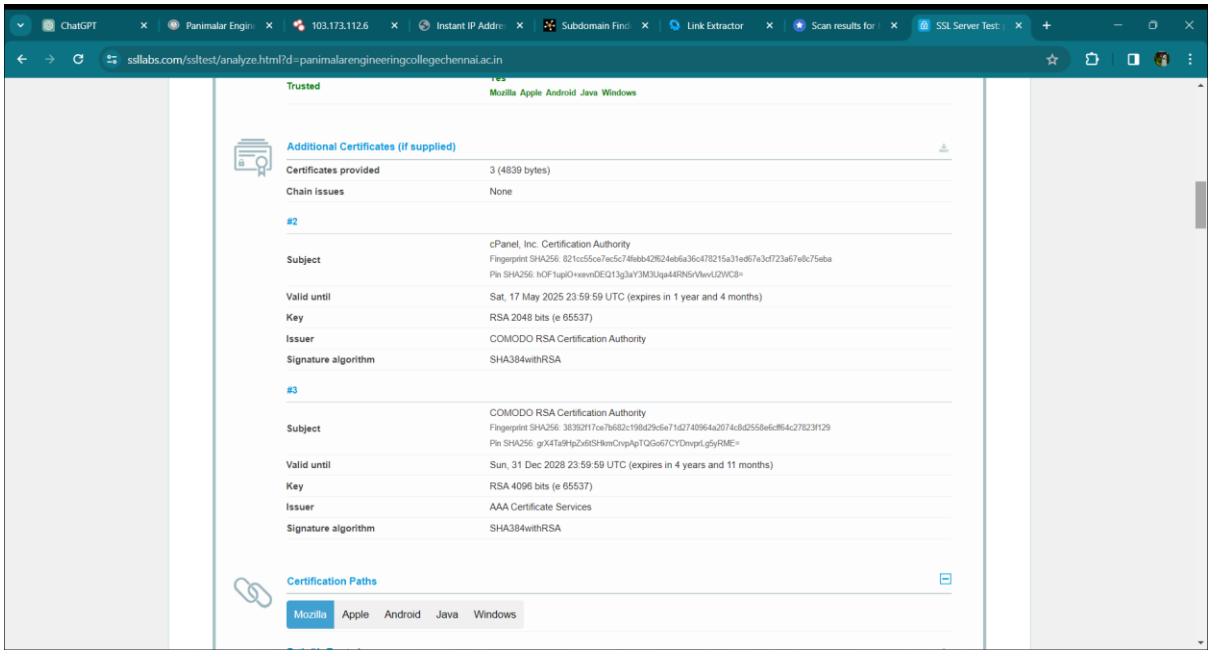
Certificate #1: RSA 2048 bits (SHA256withRSA)

ssllabs.com/ssltest/analyze.html?d=panimalarengineeringcollegechennai.ac.in

Certificate #1: RSA 2048 bits (SHA256withRSA)

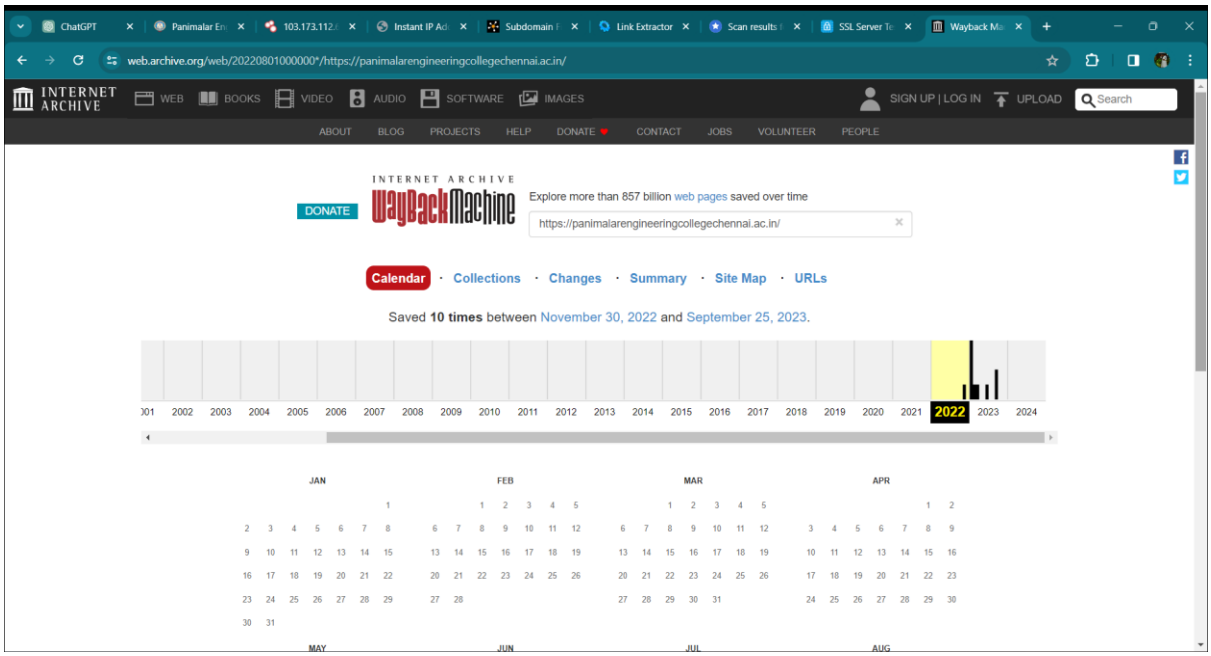
Server Key and Certificate #1

Subject	panimalarengineeringcollegechennai.ac.in Fingerprint SHA256: 28e398144d984bb472aca3d021697de7df11342b432a35156263b3be76497754 Pin SHA256: Y7YwLuKzbzabC7Y2YxKLlJiaJaLtfUm+zOfXdv+t0QHWU=
Common names	panimalarengineeringcollegechennai.ac.in
Alternative names	panimalarengineeringcollegechennai.ac.in cpanel.panimalarengineeringcollegechennai.ac.in cpcalendars.panimalarengineeringcollegechennai.ac.in cpcontacts.panimalarengineeringcollegechennai.ac.in mail.panimalarengineeringcollegechennai.ac.in webdisk.panimalarengineeringcollegechennai.ac.in webmail.panimalarengineeringcollegechennai.ac.in www.panimalarengineeringcollegechennai.ac.in
Serial Number	00e8b4668c853b9b0546f1280f01896540
Valid from	Tue, 21 Nov 2023 00:00:00 UTC
Valid until	Mon, 19 Feb 2024 23:59:59 UTC (expires in 1 month and 2 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	cPanel, Inc. Certification Authority AIA: http://crt.comodoca.com/cPanelIncCertificationAuthority.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crt.comodoca.com/cPanelIncCertificationAuthority.crl OCSP: http://ocsp.comodoca.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)



Time Travel Exploration:

Time travel across the website involves navigating through historical versions to identify changes, updates, or potential security incidents. This analysis helps in understanding the evolution of the website and identifying any vulnerabilities that may have been addressed or introduced over time. The time-travel exploration provides a holistic perspective on the website's security history.



Conclusion:

In conclusion, this comprehensive footprinting analysis of the Panimalar Engineering College Chennai City Campus website provides valuable insights into its technology stack, subdomains, hidden URLs, buffer size, security headers, SSL/TLS configuration, and historical changes. The information gathered can be instrumental in implementing targeted security measures to enhance the overall resilience and security posture of the website. Regular monitoring and updates based on the findings of this analysis will contribute to the ongoing security efforts of Panimalar Engineering College.