Footprinting

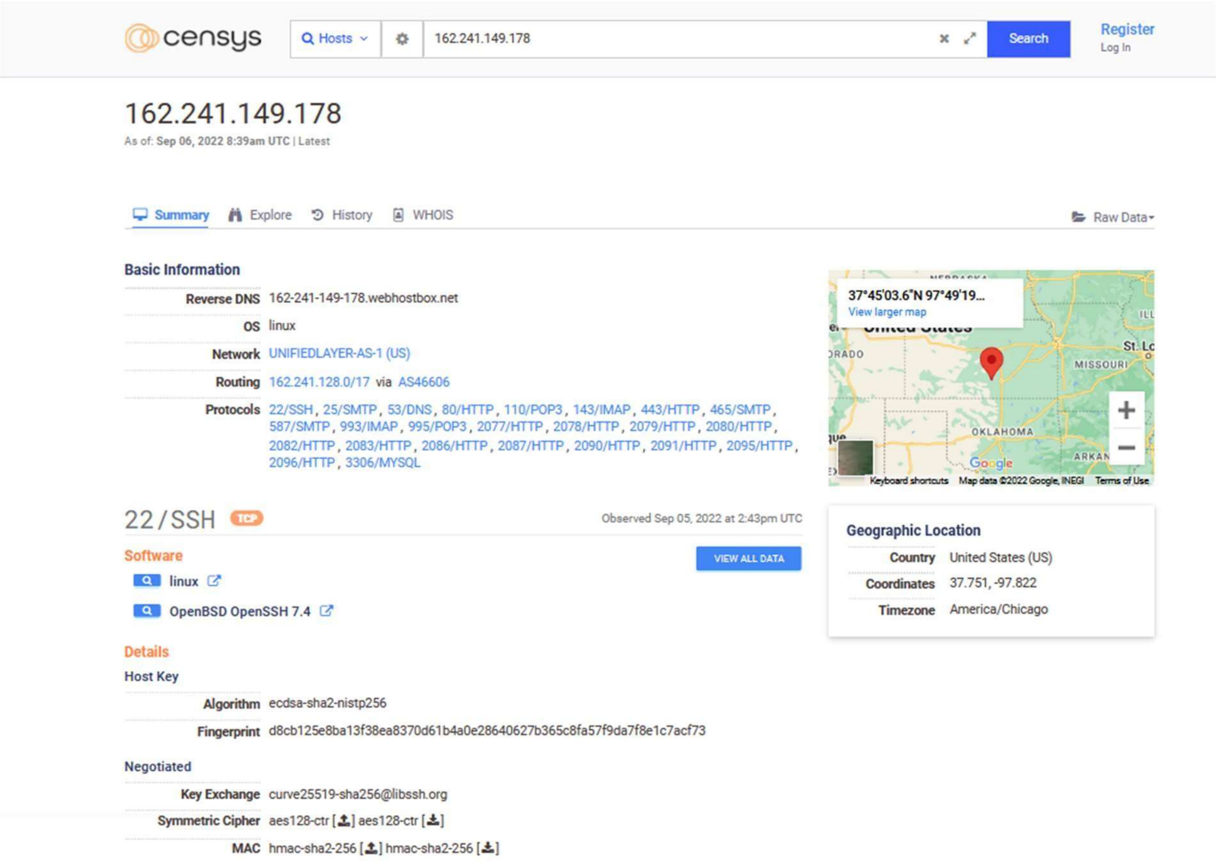
Target: Thadomal Shahani Engineering College

Basic Footprinting:

1] Hacking Website:

The search engines used to search vulnerabilities. It helps to find all the data related to the website.

Censys.io



Search: 162.241.149.178

162.241.149.178

As of: Sep 06, 2022 8:39am UTC | Latest

Basic Information

Reverse DNS	162-241-149-178.webhostbox.net
OS	linux
Network	UNIFIEDLAYER-AS-1 (US)
Routing	162.241.128.0/17 via AS46606
Protocols	22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 143/IMAP, 443/HTTP, 465/SMTP, 587/SMTP, 993/IMAP, 995/POP3, 2077/HTTP, 2078/HTTP, 2079/HTTP, 2080/HTTP, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2090/HTTP, 2091/HTTP, 2095/HTTP, 2096/HTTP, 3306/MYSQL

Geographic Location

Country	United States (US)
Coordinates	37.751, -97.822
Timezone	America/Chicago

22 / SSH TCP

Observed Sep 05, 2022 at 2:43pm UTC

Software

- linux
- OpenBSD OpenSSH 7.4

Details

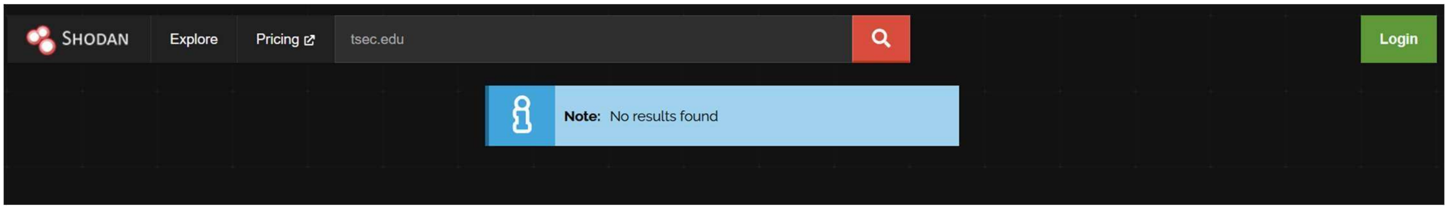
Host Key

Algorithm	ecdsa-sha2-nistp256
Fingerprint	d8cb125e8ba13f38ea8370d61b4a0e28640627b365c8fa57f9da7f8e1c7acf73

Negotiated

Key Exchange	curve25519-sha256@libssh.org
Symmetric Cipher	aes128-ctr [⬆] aes128-ctr [⬇]
MAC	hmac-sha2-256 [⬆] hmac-sha2-256 [⬇]

Shodan.io



Search: tsec.edu

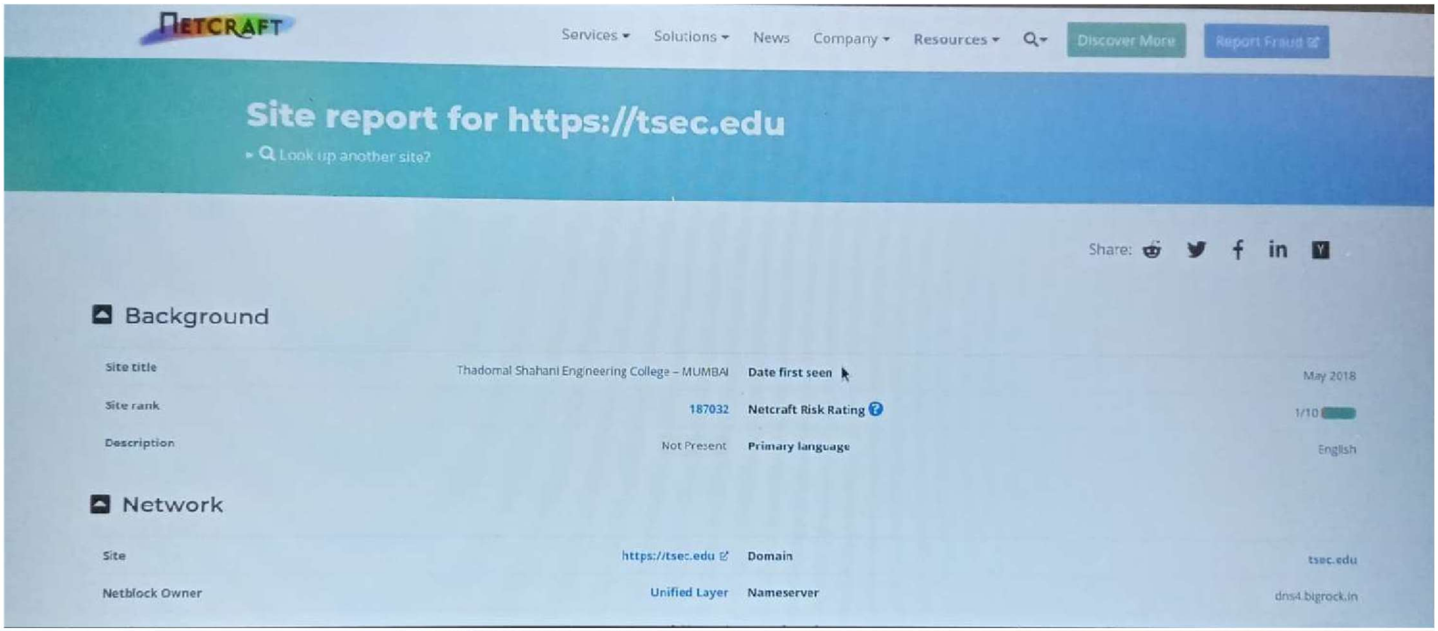
Note: No results found

Advance Footprinting:

1] Website Technology:

This helps to get the idea about technology used and if any vulnerabilities then which one more suitable for entering in the network.

NetCraft



Site report for https://tsec.edu

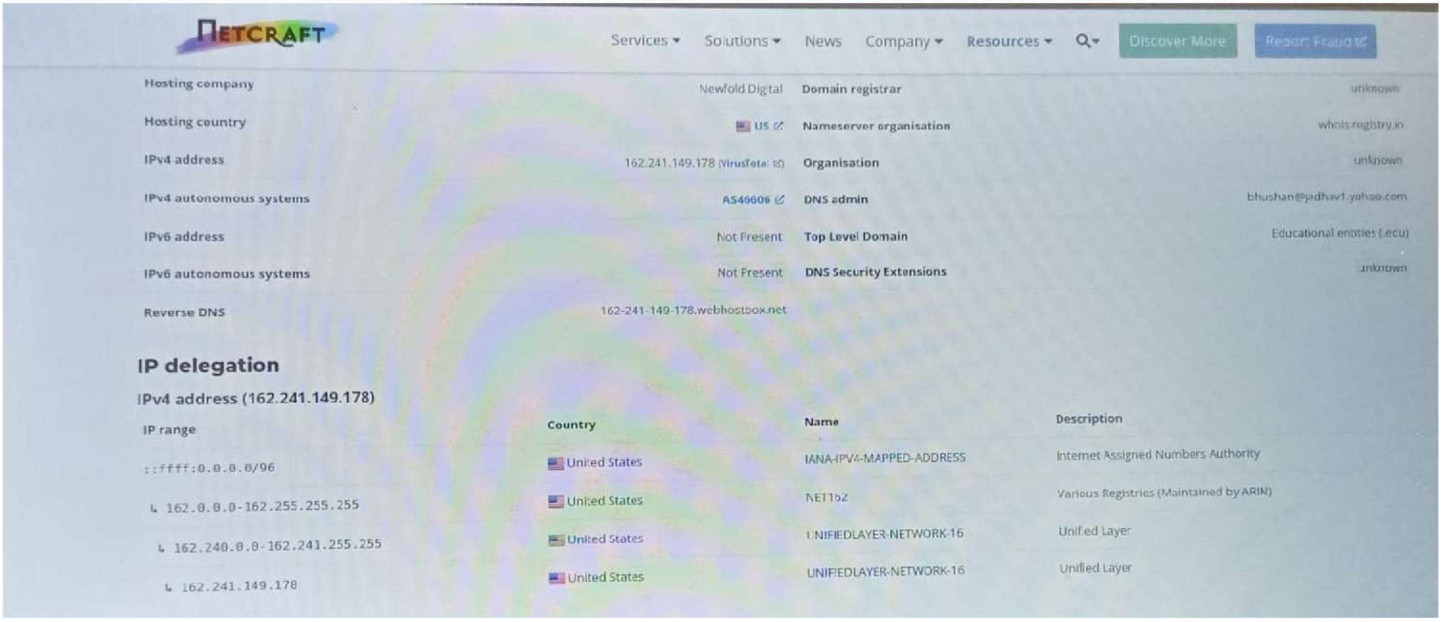
Look up another site?

Background

Site title	Thadomal Shahani Engineering College – MUMBAI	Date first seen	May 2018
Site rank	187032	Netcraft Risk Rating	1/10
Description	Not Present	Primary language	English

Network

Site	https://tsec.edu	Domain	tsec.edu
Netblock Owner	Unified Layer	Nameserver	dns4.bigrock.in



Hosting company	Newfold Digital	Domain registrar	unknown
Hosting country	US	Nameserver organisation	whois.registry.in
IPv4 address	162.241.149.178 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS46606	DNS admin	bhushan@jadhav1.yahoo.com
IPv6 address	Not Present	Top Level Domain	Educational entities (.edu)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	162-241-149-178.webhostbox.net		

IP delegation

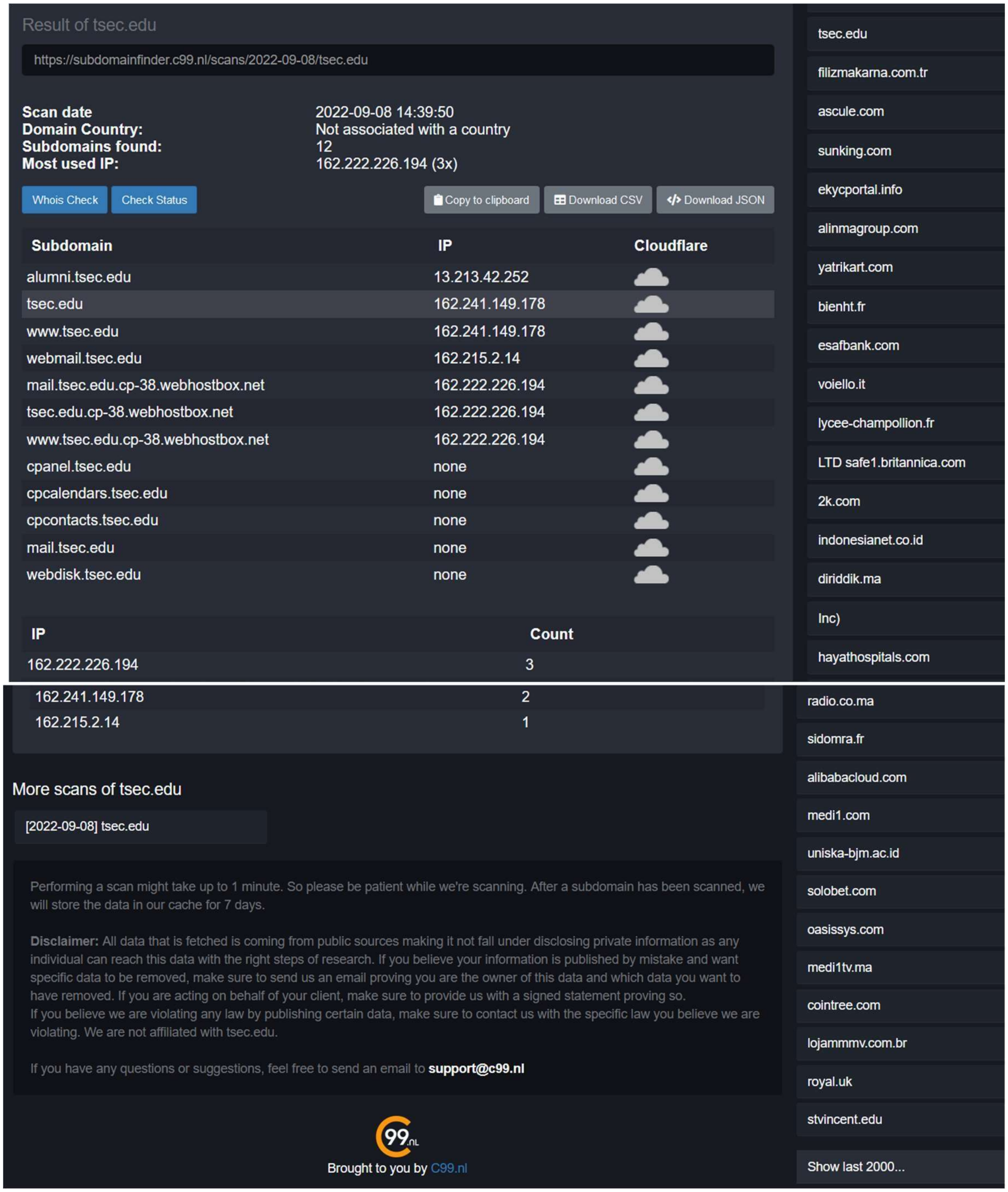
IPv4 address (162.241.149.178)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 162.0.0.0-162.255.255.255	United States	NET162	Various Registries (Maintained by ARIN)
↳ 162.240.0.0-162.241.255.255	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer
↳ 162.241.149.178	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer

2] Find Sub Domain:

This finds the data of internal subdomains of the website. If there is vulnerability in subdomain then we can enter the site using it and not the main domain.

Subdomainfinder.c99nl



Result of tsec.edu

https://subdomainfinder.c99.nl/scans/2022-09-08/tsec.edu

Scan date 2022-09-08 14:39:50
Domain Country: Not associated with a country
Subdomains found: 12
Most used IP: 162.222.226.194 (3x)

Subdomain	IP	Cloudflare
alumni.tsec.edu	13.213.42.252	☁
tsec.edu	162.241.149.178	☁
www.tsec.edu	162.241.149.178	☁
webmail.tsec.edu	162.215.2.14	☁
mail.tsec.edu.cp-38.webhostbox.net	162.222.226.194	☁
tsec.edu.cp-38.webhostbox.net	162.222.226.194	☁
www.tsec.edu.cp-38.webhostbox.net	162.222.226.194	☁
cpanel.tsec.edu	none	☁
cpcalendars.tsec.edu	none	☁
cpcontacts.tsec.edu	none	☁
mail.tsec.edu	none	☁
webdisk.tsec.edu	none	☁

IP	Count
162.222.226.194	3
162.241.149.178	2
162.215.2.14	1

More scans of tsec.edu

[2022-09-08] tsec.edu

Performing a scan might take up to 1 minute. So please be patient while we're scanning. After a subdomain has been scanned, we will store the data in our cache for 7 days.

Disclaimer: All data that is fetched is coming from public sources making it not fall under disclosing private information as any individual can reach this data with the right steps of research. If you believe your information is published by mistake and want specific data to be removed, make sure to send us an email proving you are the owner of this data and which data you want to have removed. If you are acting on behalf of your client, make sure to provide us with a signed statement proving so.
If you believe we are violating any law by publishing certain data, make sure to contact us with the specific law you believe we are violating. We are not affiliated with tsec.edu.

If you have any questions or suggestions, feel free to send an email to **support@c99.nl**

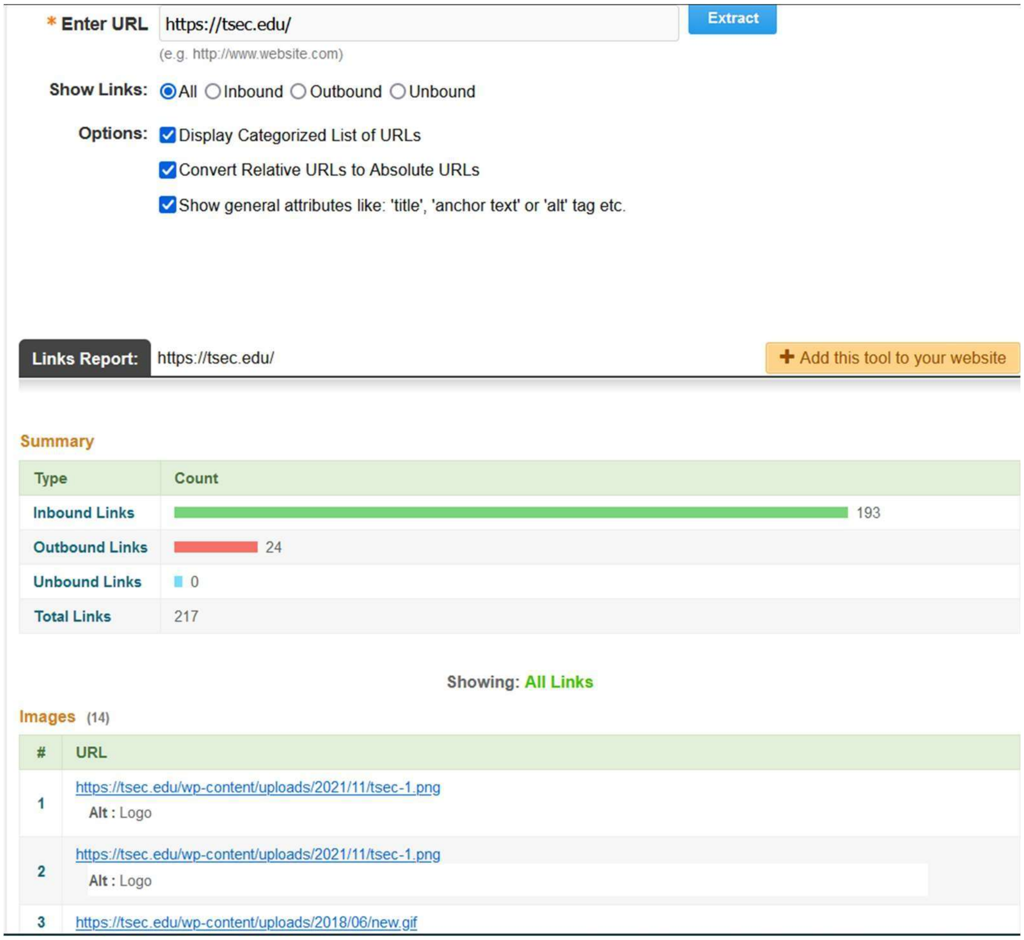
Brought to you by C99.nl

tsec.edu
filizmakarna.com.tr
ascule.com
sunking.com
ekycportal.info
alinmagroup.com
yatrikart.com
bienht.fr
esafbank.com
voiello.it
lycee-champollion.fr
LTD safe1.britannica.com
2k.com
indonesianet.co.id
diriddik.ma
Inc)
hayathospitals.com
radio.co.ma
sidomra.fr
alibabacloud.com
medi1.com
uniska-bjm.ac.id
solobet.com
oasissys.com
medi1tv.ma
cointree.com
lojammmv.com.br
royal.uk
stvincent.edu
Show last 2000...

3] Hidden Link:

It segregates the links used in website, whether it be inbound or outbound links. This information is helpful for MITM, sql injection or XSS attacks.

linkextractor:(webtoolhub.com)



* Enter URL https://tsec.edu/ Extract

(e.g. http://www.website.com)

Show Links: ● All ○ Inbound ○ Outbound ○ Unbound

Options: ☑ Display Categorized List of URLs

☑ Convert Relative URLs to Absolute URLs

☑ Show general attributes like: 'title', 'anchor text' or 'alt' tag etc.

Links Report: https://tsec.edu/ + Add this tool to your website

Summary

Type	Count
Inbound Links	193
Outbound Links	24
Unbound Links	0
Total Links	217

Showing: All Links

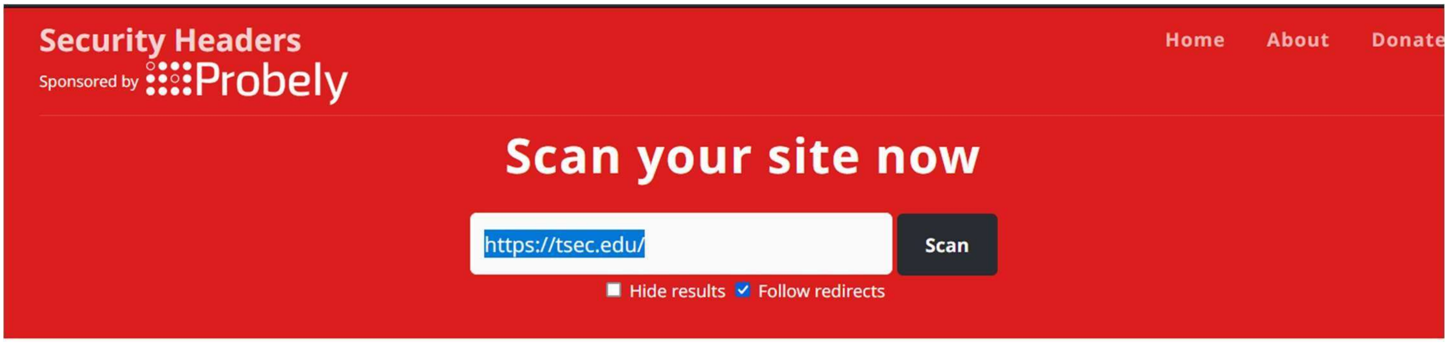
Images (14)

#	URL
1	https://tsec.edu/wp-content/uploads/2021/11/tsec-1.png Alt : Logo
2	https://tsec.edu/wp-content/uploads/2021/11/tsec-1.png Alt : Logo
3	https://tsec.edu/wp-content/uploads/2018/06/new.gif

4] check Security Header:

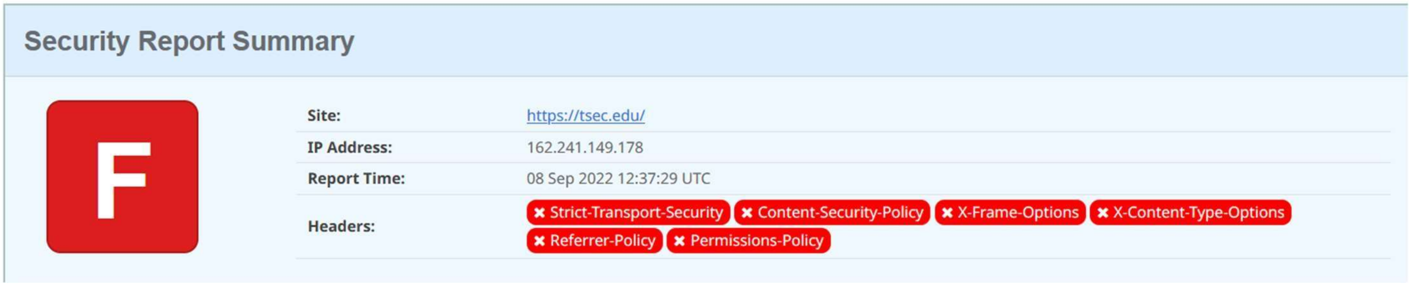
Header gives the instruction to the packets. It is in the transport layer of OSI model.

<u>Securityheaders.com</u>



https://tsec.edu/

□ Hide results ☑ Follow redirects

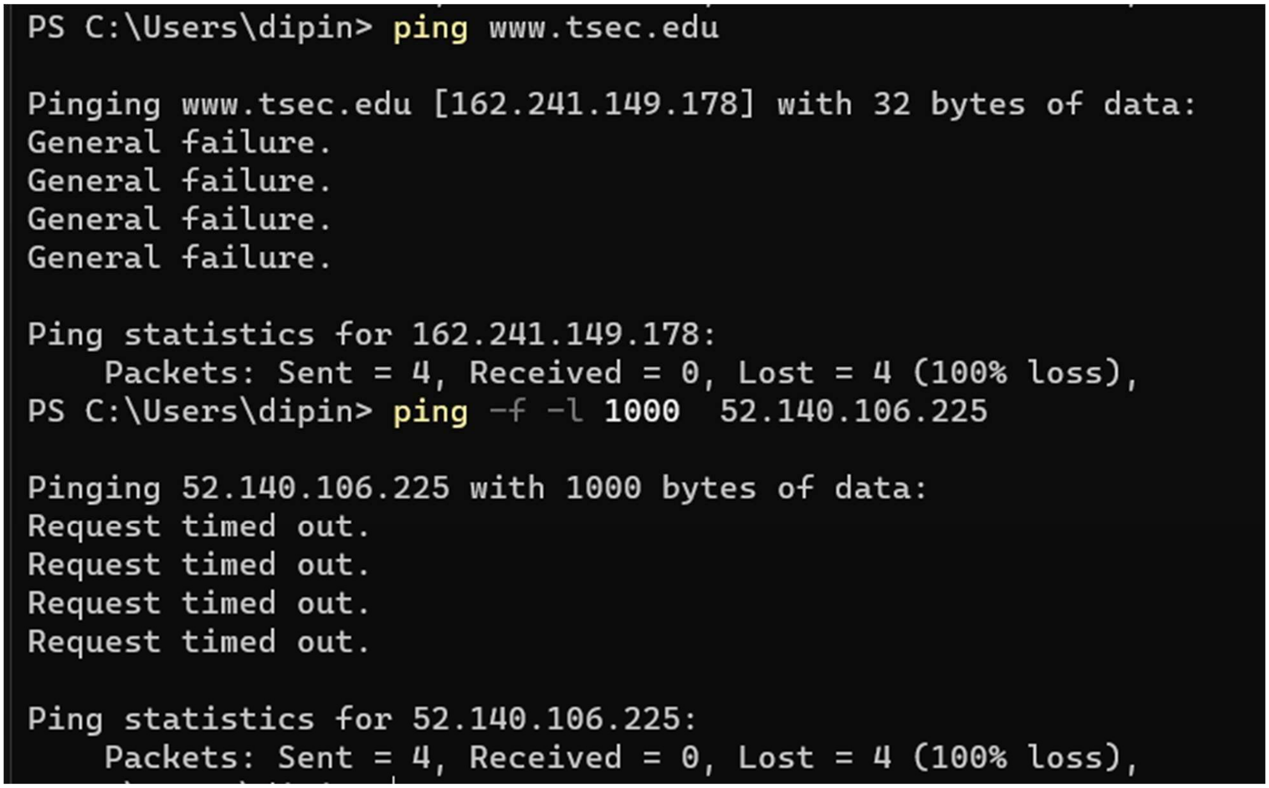


Security Report Summary

Site:	https://tsec.edu/
IP Address:	162.241.149.178
Report Time:	08 Sep 2022 12:37:29 UTC
Headers:	✖ Strict-Transport-Security ✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy

5] IP address & Buffer size:

It gives the IP address of the website also we find out the buffer size to send the data.

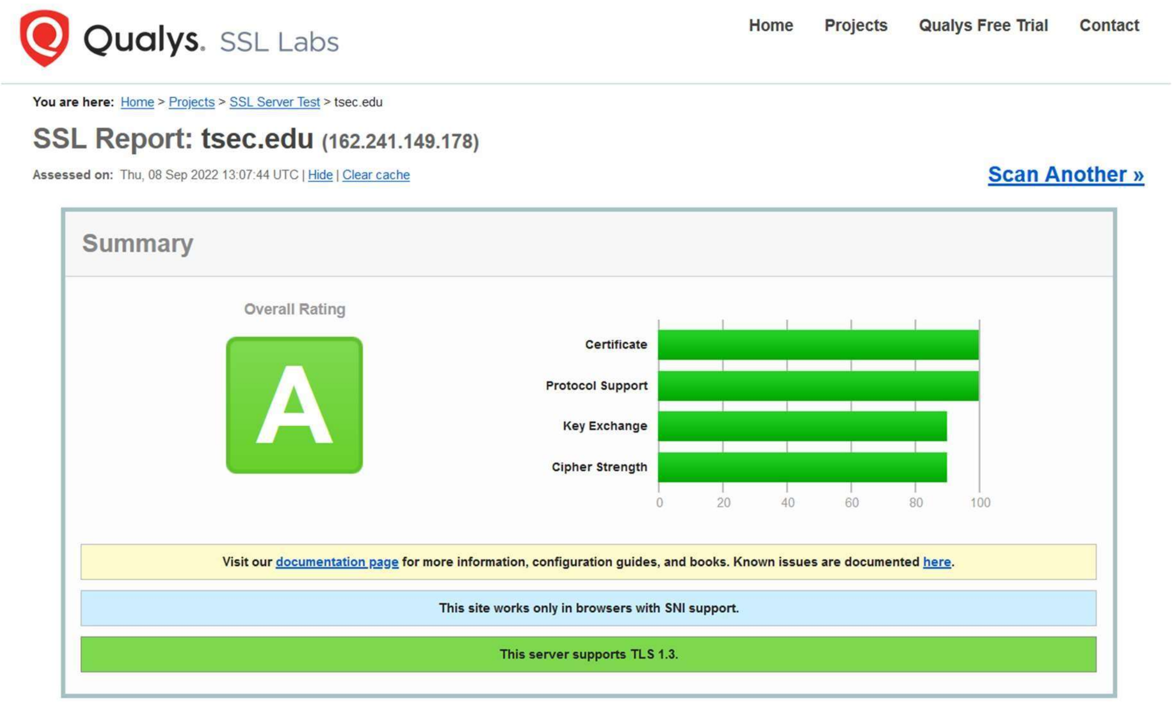


```
PS C:\Users\dipin> ping www.tsec.edu

Pinging www.tsec.edu [162.241.149.178] with 32 bytes of data:
General failure.
General failure.
General failure.
General failure.

Ping statistics for 162.241.149.178:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\dipin> ping -f -l 1000  52.140.106.225

Pinging 52.140.106.225 with 1000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 52.140.106.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

6] SSL:

SSL helps to encrypt the TLS packet, i.e., it provides security to packets.

ssllabs.com:



You are here: Home > Projects > SSL Server Test > tsec.edu

SSL Report: tsec.edu (162.241.149.178)

Assessed on: Thu, 08 Sep 2022 13:07:44 UTC | Hide | Clear cache

Scan Another »

Summary

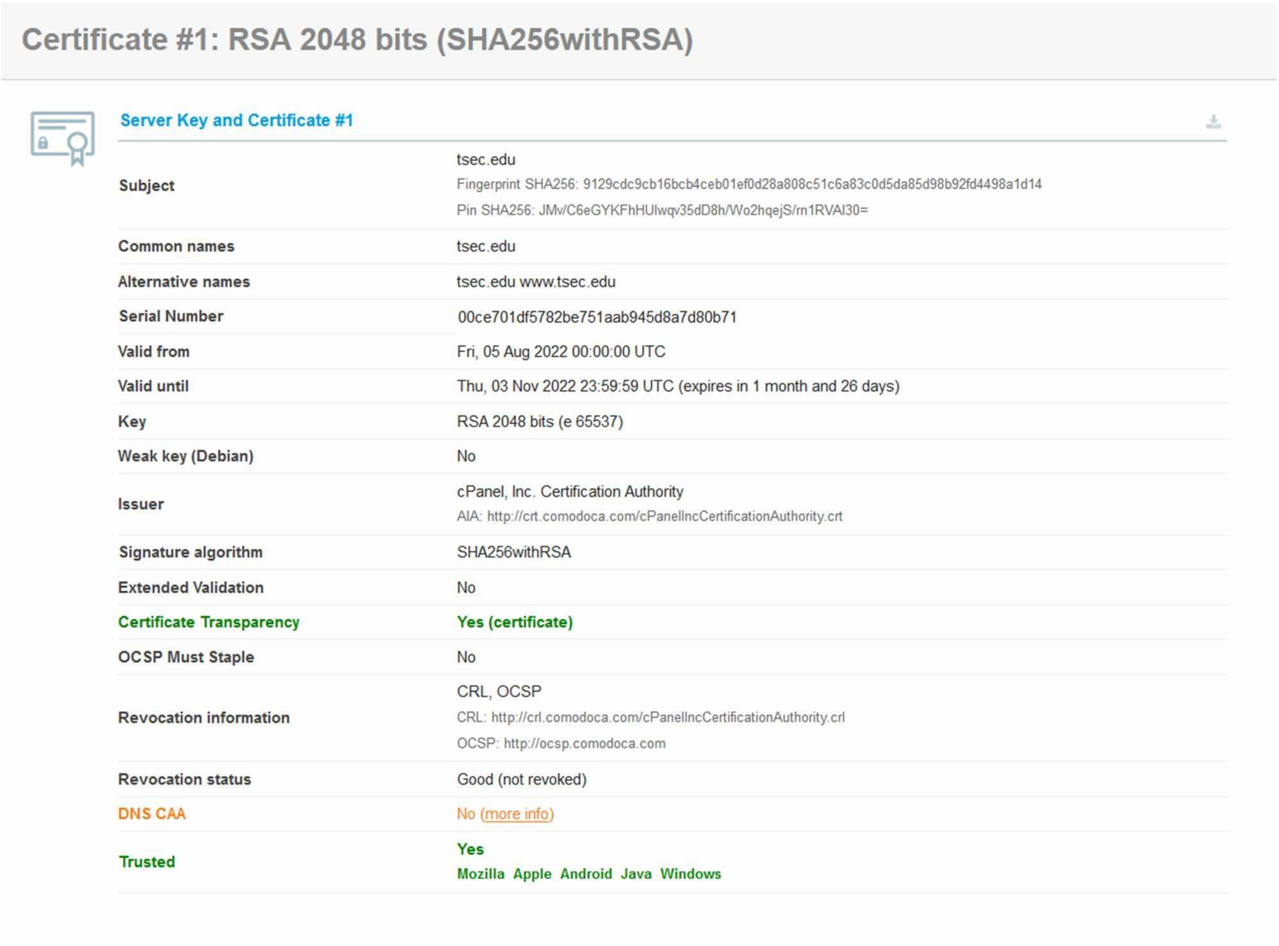
Overall Rating

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)

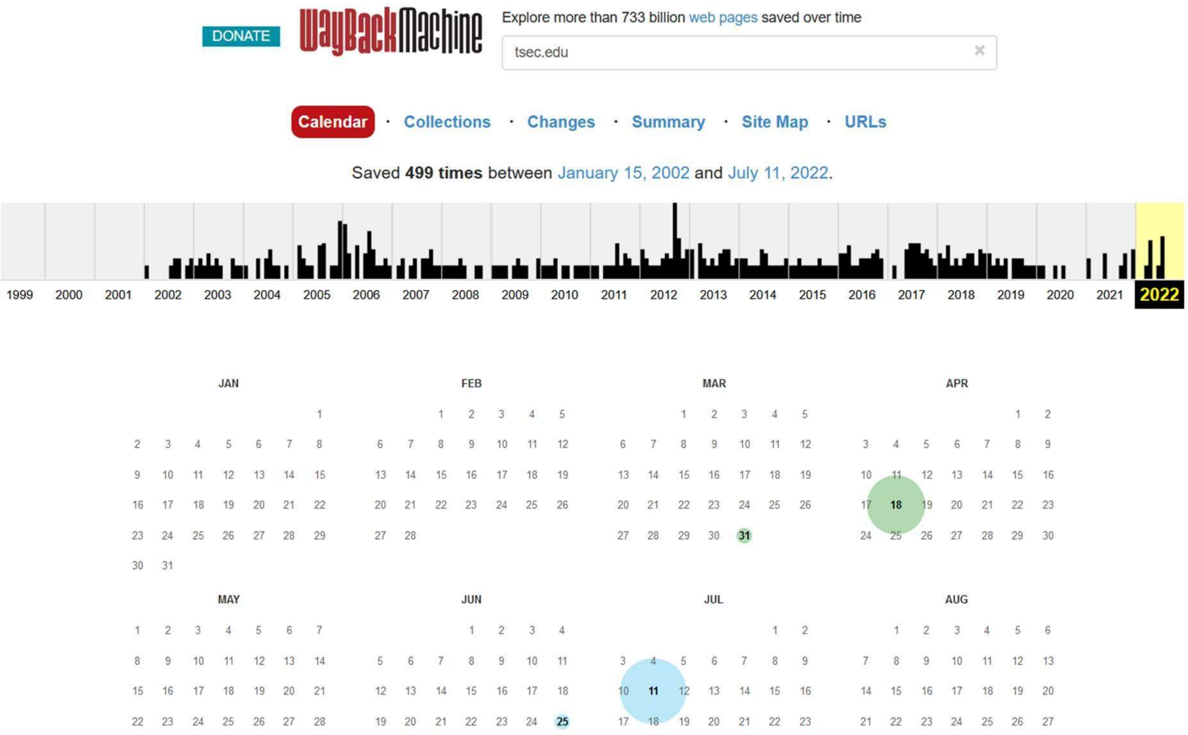
Server Key and Certificate #1

Subject	tsec.edu Fingerprint SHA256: 9129cdc9cb16bcb4ceb01ef0d28a808c51c6a83c0d5da85d98b92fd4498a1d14 Pin SHA256: JMv/C6eGYKFhHUlwqv35dD8h/Wo2hqejS/rn1RVAI30=
Common names	tsec.edu
Alternative names	tsec.edu www.tsec.edu
Serial Number	00ce701df5782be751aab945d8a7d80b71
Valid from	Fri, 05 Aug 2022 00:00:00 UTC
Valid until	Thu, 03 Nov 2022 23:59:59 UTC (expires in 1 month and 26 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://crl.comodoca.com/cPanelIncCertificationAuthority.crl OCSP: http://ocsp.comodoca.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

7] Way Back Machine:

It shows when the website was made and when all in past was it modified.

Archive.org:



Explore more than 733 billion web pages saved over time

tsec.edu

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved **499 times** between January 15, 2002 and July 11, 2022.

JAN

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

FEB

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28					

MAR

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	**31**		

APR

					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	**18**	19	20	21	22	23
24	25	26	27	28	29	30

MAY

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

JUN

			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	**25**

JUL

					1	2
3	4	5	6	7	8	9
10	**11**	12	13	14	15	16
17	18	19	20	21	22	23

AUG

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27