MINI PROJECT REPORT ON RECONNAISSANCE

NAME : AMAN SAH

UGC : BCA 2ND SEM

COURSE : ACMEGRADE (CYBER SECURITY)

PLACE OF STUDY : ASSAM DON BOSCO UNIVERSITY SCHOOL OF TECHNOLOGY, AZARA, GUWAHATI, ASSAM

So, basically Reconnaissance or foot printing are of two types in which Hackers gather information. They are :

- BASIC RECONNAISSANCE: This are very basic things which a hacker usually does for gathering information. They are by:

1.Social Networking Sites: Through social networking sites one can gather a bunch of information required of a company for hacking into it.

2.Hacking Search Engines: It helps to get much deeper information

about a particular company that a normal search engines can't fetch just by coping the companies IP address and pasting in the hacking search engines. Some of it are Shodan, Censys, Notevil, Duckduckgo.

3.Google Dorks: It helps to search for a precise or a specific information that you are looking for.

- **ADVANCE RECONNAISSANCE** : This are some advance techniques which a hacker usually use for gathering information. They are by:

1. **Website Technology Extension** : This helps to find loop holes while developing websites. Some of it are “netcraft” and “wapplyzer”.

2. **Subdomains Of Websites** : This helps to find subdomains of all the main domains. Thus making easy for Hacker to find loop holes and get into the environment. “subdomain finder” finds the subdomains of all the domains.

3. **Hidden Links Of Website** : This helps to get all additional links that a particular website bears which are hidden from public. “link extractor” helps in doing so.

4. **Check Security Headers Of a Website** : This checks the packet information by “securityheaders.com”.

5. **SSL Test** : One can test their secure socket layers through “ssllabs.com” or “ssltest.com”.

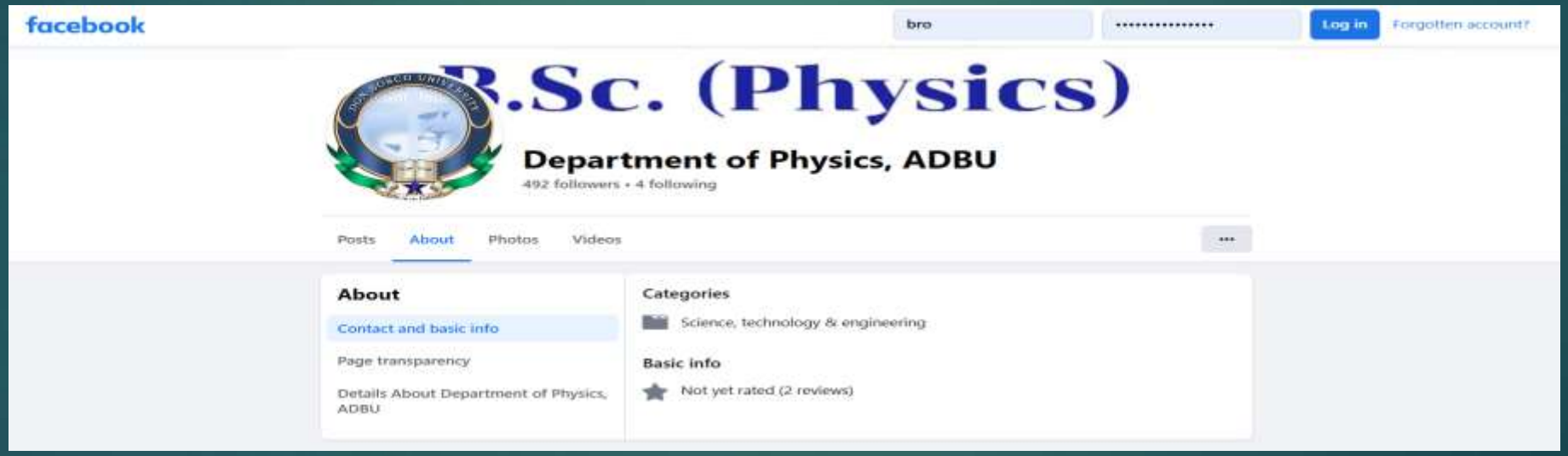
6. **IP Of a Website and Buffer Size** : One can search for IP address of a website through command prompt and the buffer size which is the maximum size of the packets.

7. **Time Travel Over a Website** : It is also called as time way back machine. It helps to gather some of the personal information about a particular website through travelling back in time when the particular website was developed.

“archive.org” helps in doing so.

So lets perform some Basic Reconnaissance in my university website.

- **Social Networking Sites** : Some information gathered through social networking sites of my university are as follows –



assamdonboscouniversity Follow

95 posts 575 followers 0 following

ADBU MEDIA
Department of Mass Communication, Assam Don Bosco University
www.dbuniversity.ac.in


Special Lectur...


Special Days


Studio

Assam Don Bosco University, Guwahati, Assam

Carpe Diem! Life in its fullness!

Education Administration Programs · Guwahati, Assam · 911 followers

1 person from your school works here · 64 employees

✓ Following | Visit website | More

Home | About | Posts | Jobs | Alumni

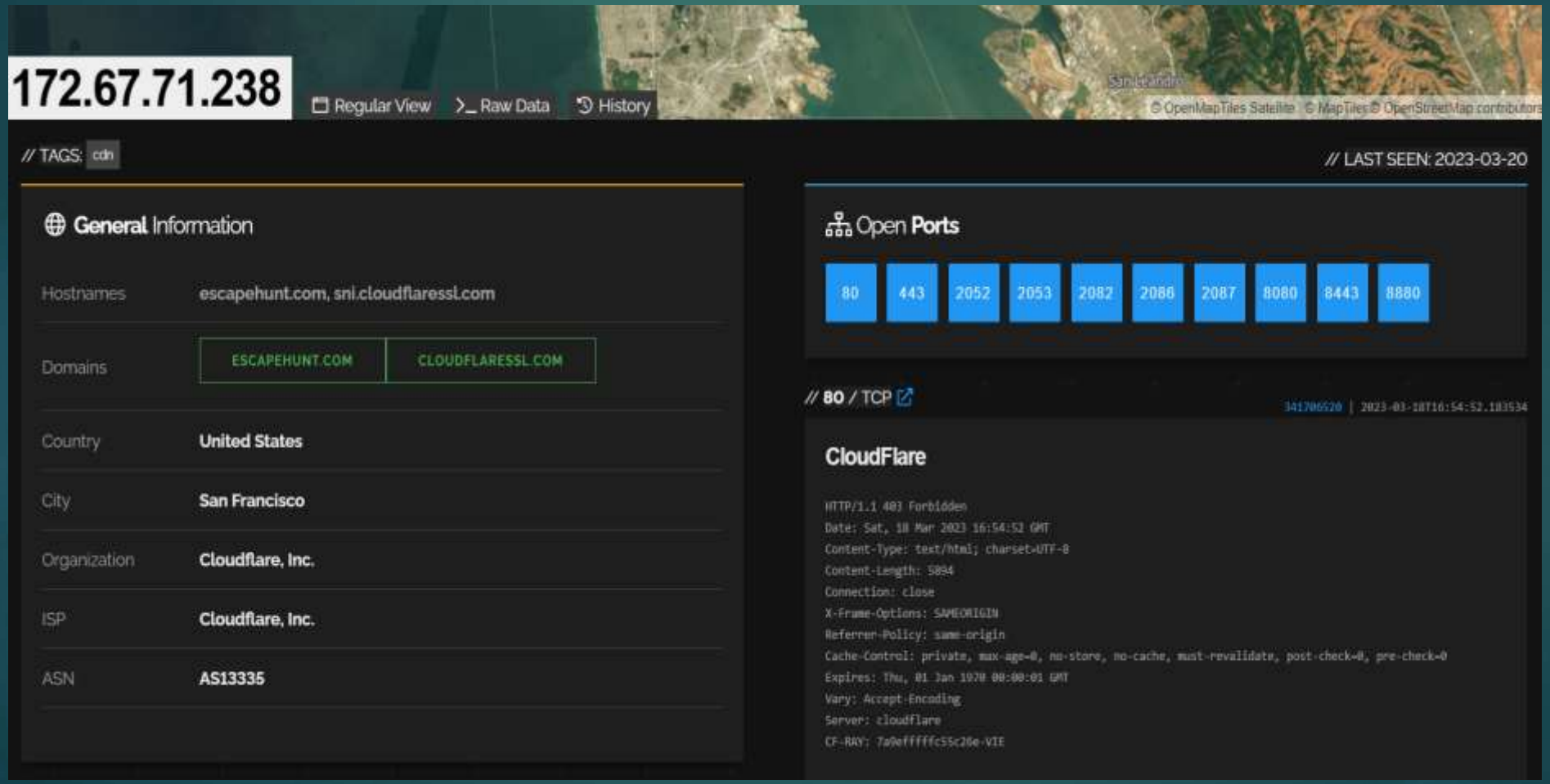
Overview

Assam Don Bosco University
Assam Don Bosco University (ADBU) is established as the first State University of Assam in the private sector on 29 March 2008, and set up by Don Bosco Society in response to the felt educational needs of the people of North-East India. In a little over 10 years, Assam Don Bosco University has become one of the best Universities in the Northeast and has the distinction of the only private University in Assam with an 'A' Grade from National Assessment and Accreditation Council (NAAC). The University has also been given a 12B status by the University Grants Commission, hence, becoming the first private University to attain this status in North East and the fourth in the country.

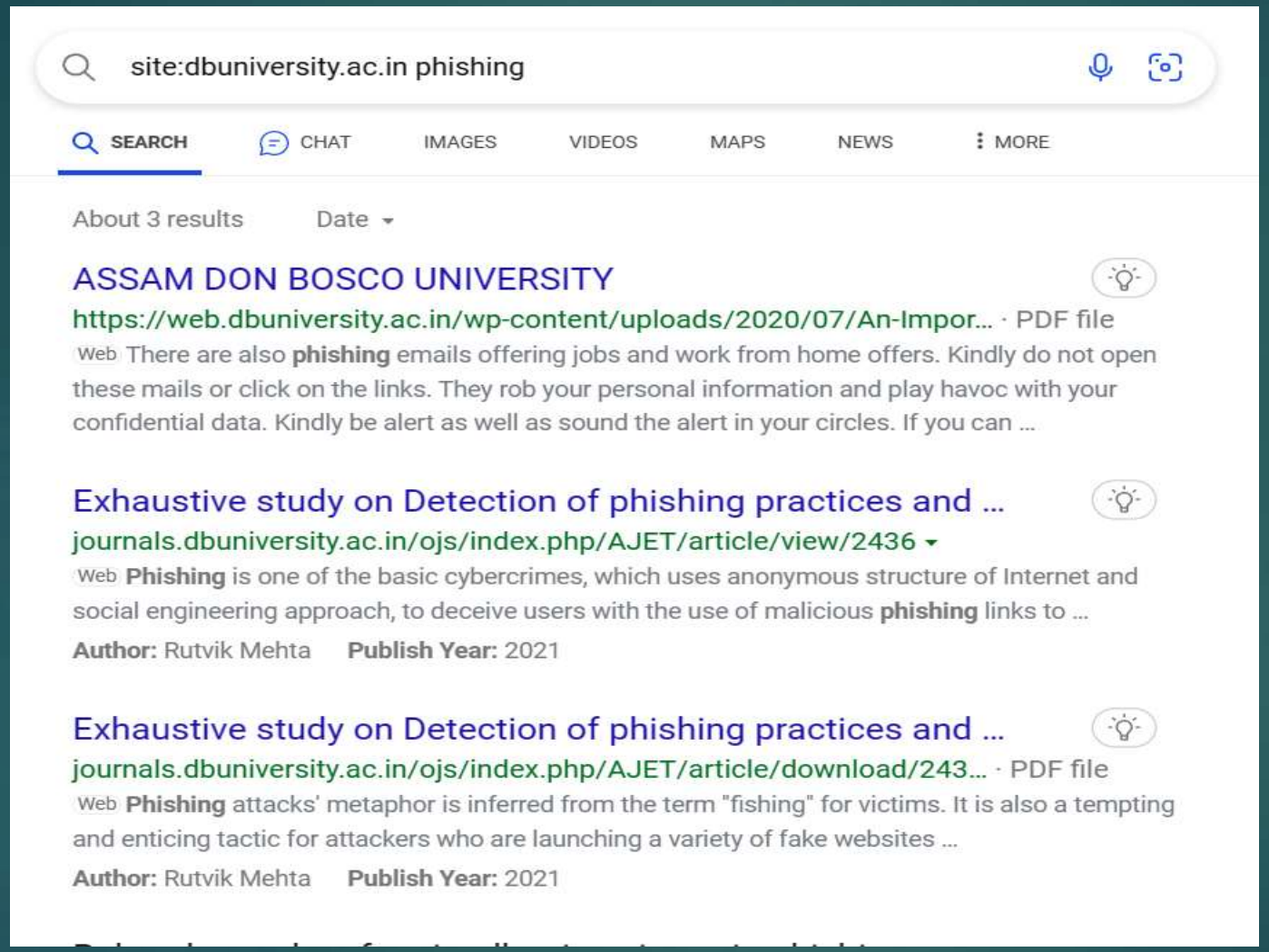
Website
http://www.dbuniversity.ac.in

- **Hacking Search Engines** : By the IP address of my university I can get much deeper information that normal search engines cant give.

By Using Shodan we can see the ports of my university that are open:

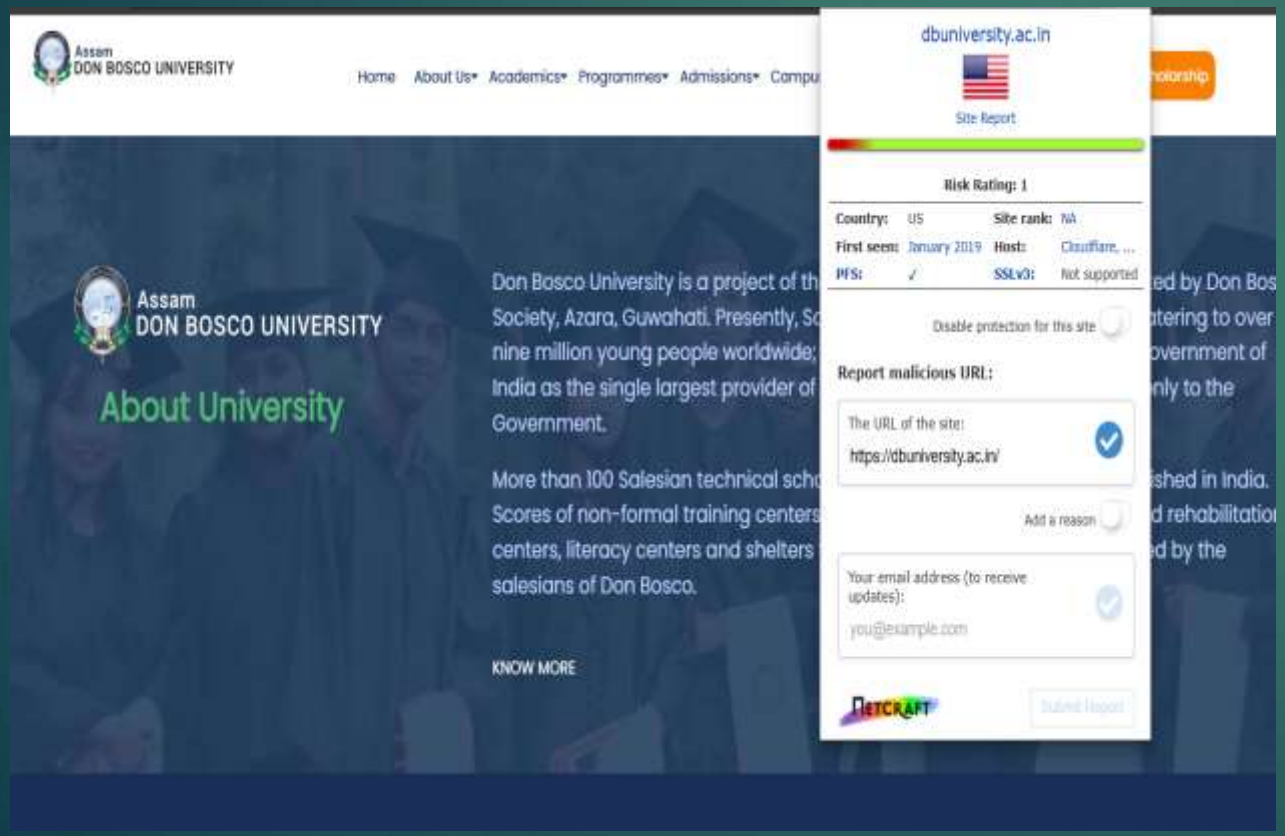


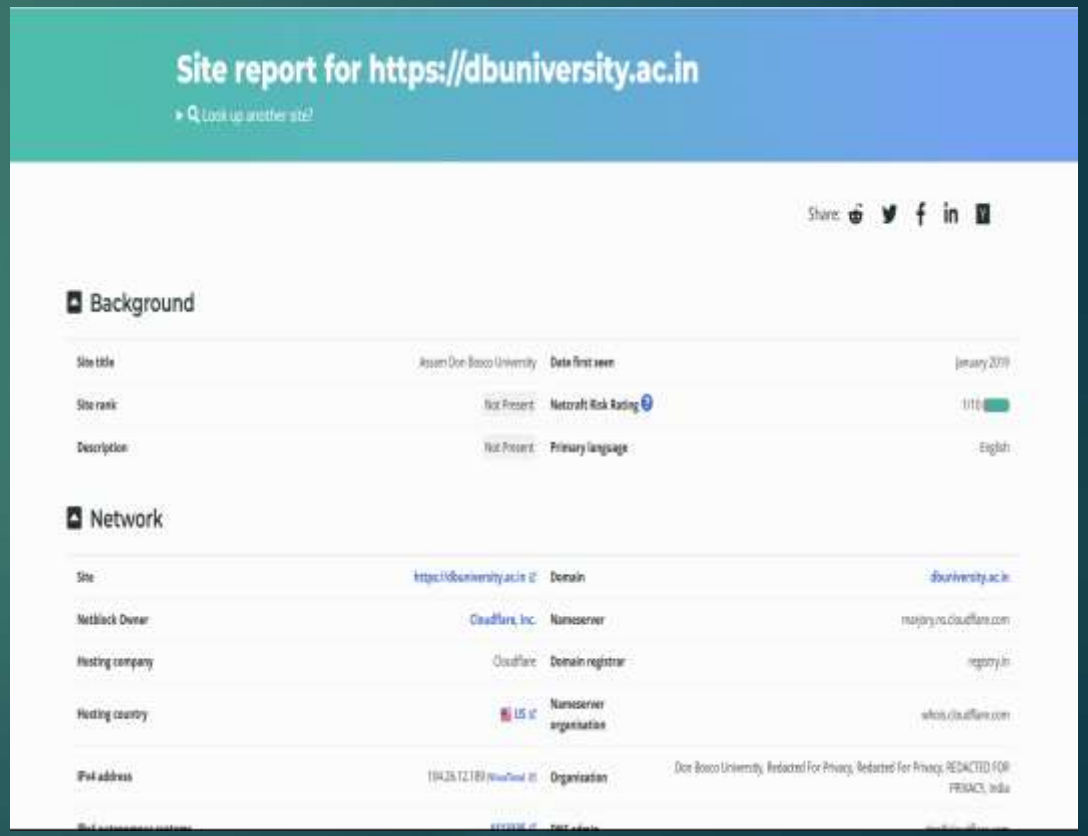
- **Google Dorks** : About a particular information related to my website :



So now lets see some Advance Reconnaissance in my university website.

- **Website Technology** : As by using Netcraft Extension I can find many information related to my university website.





IPv4 autonomous systems	AS13335	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:20:0:0:0:681a:cbd	Top Level Domain	India (.ac.in)
IPv6 autonomous systems	AS13335	DNS Security Extensions	unknown
Reverse DNS	unknown		

IP delegation

IPv4 address (104.26.12.189)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 104.26.12.189	United States	CLOUDFLARENET	Cloudflare, Inc.

IPv6 address (2606:4700:20:0:0:0:681a:cbd)

IP range	Country	Name	Description

IP delegation

IPv4 address (104.26.12.189)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 104.26.12.189	United States	CLOUDFLARENET	Cloudflare, Inc.

IPv6 address (2606:4700:20:0:0:0:681a:cbd)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inetbnum object
↳ 2600::/12	United States	NET6-2600	American Registry for Internet Numbers
↳ 2606:4700::/32	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 2606:4700:20:0:0:0:681a:cbd	United States	CLOUDFLARENET	Cloudflare, Inc.

SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	net.brahmaputra.dbuniversity.ac.in	Supported TLS Extensions	RFC8446 key share, RFC8446 supported versions, RFC4366 server name, RFC7301 application-layer protocol negotiation, RFC6962 signed certificate timestamp, RFC4366 status request

SSL/TLS

Assurance	Domain validation
Common name	net.brahmaputra.dbuniversity.ac.in
Organisation	Not Present
State	Not Present
Country	Not Present
Organisational unit	Not Present
Subject Alternative Name	dbuniversity.ac.in, net.brahmaputra.dbuniversity.ac.in
Validity period	From Feb 1 2023 to May 2 2023 (3 months)
Matches hostname	Yes
Server	cloudflare
Public key algorithm	id-ecPublicKey
Protocol version	TLSv1.3
Public key length	256

Perfect Forward Secrecy	Yes
Supported TLS Extensions	RFC8446 key share, RFC8446 supported versions, RFC4366 server name, RFC7301 application-layer protocol negotiation, RFC6962 signed certificate timestamp, RFC4366 status request
Application-Layer Protocol Negotiation	h2
Next Protocol Negotiation	Not Present
Issuing organisation	Let's Encrypt
Issuer common name	E1
Issuer unit	Not Present
Issuer location	Not Present
Issuer country	US
Issuer state	Not Present
Certificate Revocation Lists	Not Present
Certificate Hash	VsE1j4eHj6gSRt6Br8VmbpH5avw

Certificate check	ok
Signature algorithm	ecdsa-with-SHA384
Serial number	0x0478b3896e7ee83b5aebea8e7f92c75e0e54
Cipher	TLS_AES_256_GCM_SHA384
Version number	0x02

OCSP servers	http://e1.o.lencr.org - *100% uptime in the past 24 hours* Performance Graph
OCSP stapling response	Certificate valid
OCSP data generated	Mar 18 22:00:00 2023 GMT
OCSP data expires	Mar 25 21:59:58 2023 GMT

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Let's Encrypt Oak 2023 [illegible]	2023-02-01 04:26:38	Success
Certificate	Cloudflare Nimbus 2023 [illegible]	2023-02-01 04:26:38	Success

SSLv3/POODLE

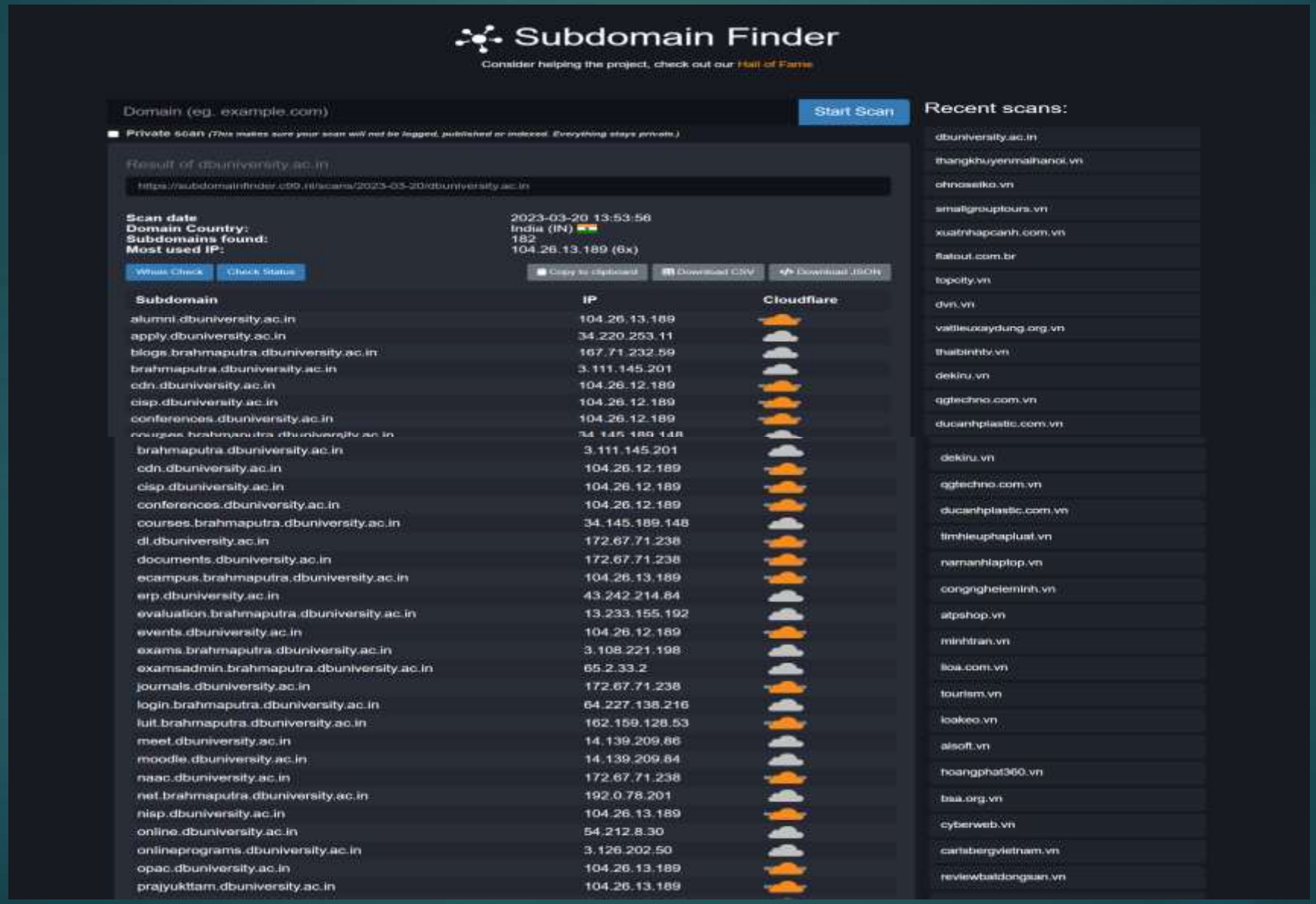
This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

- **Subdomains of Website** : As I can find many subdomains that my university domain bears through sub domain finder .

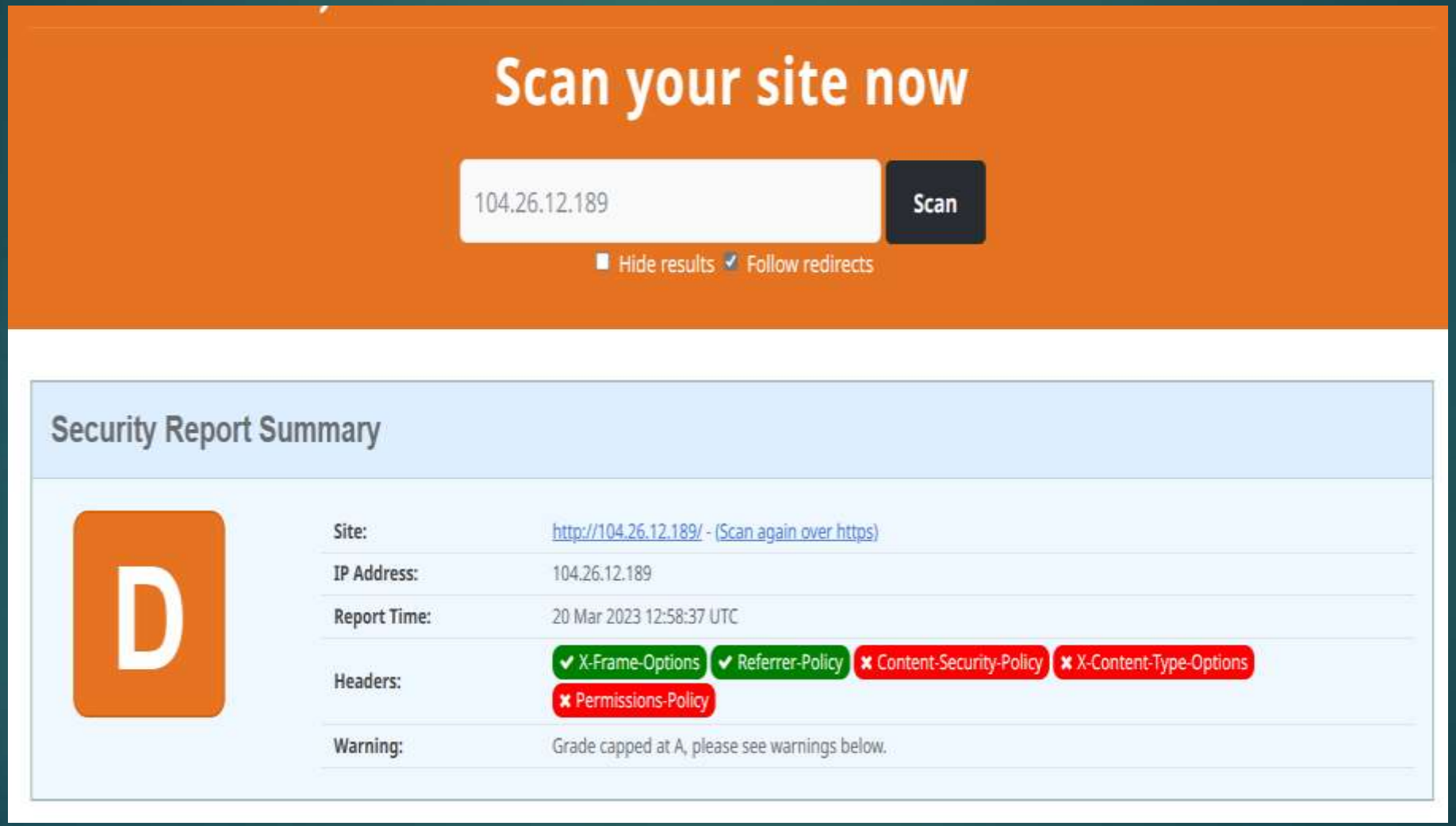


- **Finding hidden links of website** : I can find many hidden links of my university website through “linkextractor” .

URLs | Plain URLs | Internal Links Only | External Links Only

Sr#	URL	Anchor	Follow Status	Type
1	http://dbuniversity.ac.in/	A-	dofollow	Internal Link
2	http://dbuniversity.ac.in/index.php	Image	dofollow	Internal Link
3	http://dbuniversity.ac.in//cdn-cgi/l/email-protection		dofollow	Internal Link
4	https://www.youtube.com/user/ADBUGuwahati	Youtube	dofollow	External Link
5	https://twitter.com/DonBoscoUniv	Twitter	dofollow	External Link
6	https://www.facebook.com/AssamDonBoscoUniversity/	Facebook	dofollow	External Link
7	http://dbuniversity.ac.in//dbuglobal	Distance Education	dofollow	Internal Link
8	http://dbuniversity.ac.in/javascript:void(0)	about us	dofollow	Internal Link

- **Checking Security Headers of Website :** As you can see I can find many security Headers missing for my university website as I checked through “securityheaders.com”.



- **SSL Test :** As the certificates in each of the server of my university is fine and can be checked through “ssltest.com”.

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

SSL Report: dbuniversity.ac.in

Assessed on: Mon, 20 Mar 2023 13:18:30 UTC | Hide | Clear cache

Scan Another >>

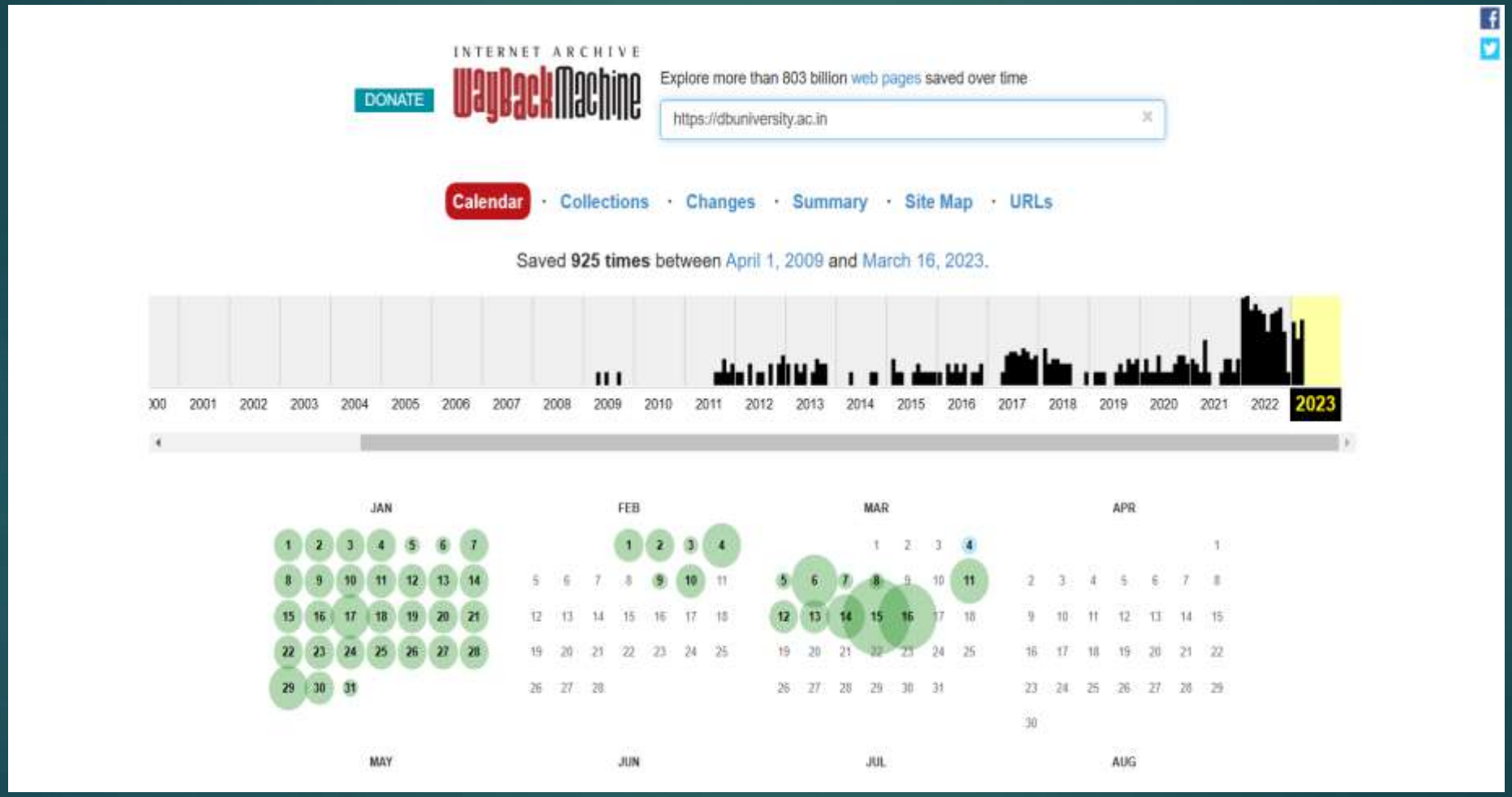
	Server	Test time	Grade
1	104.26.13.189 Ready	Mon, 20 Mar 2023 13:03:12 UTC Duration: 147.477 sec	A
2	104.26.12.189 Ready	Mon, 20 Mar 2023 13:05:39 UTC Duration: 146.809 sec	A
3	2606:4700:20:0:0:0:ac43:47ee Ready	Mon, 20 Mar 2023 13:08:06 UTC Duration: 147.16 sec	A
4	172.67.71.238 Ready	Mon, 20 Mar 2023 13:10:33 UTC Duration: 172.679 sec	A
5	2606:4700:20:0:0:0:681a:dbd Ready	Mon, 20 Mar 2023 13:13:26 UTC Duration: 157.335 sec	A
6	2606:4700:20:0:0:0:681a:cbd Ready	Mon, 20 Mar 2023 13:16:03 UTC Duration: 146.564 sec	A

SSL Report v2.1.10

- **IP Address and Buffer size** : I can get to know the buffer size through the command prompt.

```
C:\Users\Aman>ping -f -l 1470 104.26.12.189

Pinging 104.26.12.189 with 1470 bytes of data:
Reply from 104.26.12.189: bytes=1470 time=307ms TTL=56
Reply from 104.26.12.189: bytes=1470 time=214ms TTL=56
Reply from 104.26.12.189: bytes=1470 time=215ms TTL=56
Reply from 104.26.12.189: bytes=1470 time=217ms TTL=56

Ping statistics for 104.26.12.189:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 214ms, Maximum = 307ms, Average = 238ms

C:\Users\Aman>ping -f -l 1475 104.26.12.189

Pinging 104.26.12.189 with 1475 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 104.26.12.189:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- **Time Travelling** : I can also time travel on my university website and find some personal details there.



THANK YOU