ST#IS#4899

TASK – 2

TARGET:-

- **TARGET DOMAINS :-**

1) https://buruniv.ac.in/
2) https://stjosephsvizag.com/
3) https://gnauniversity.edu.in/
4) https://hindusthan.net/
5) http://coer.ac.in/

QUESTION-1 :-

Find admin login pages in the given websites using footprinting techniques (URL).

QUESTION-2 :-

A) **Gather 10 email addresses from any 3 given domains.**
Note: Domain/sub domain registered email IDs only.
B) **Find whether the mails have been breached and if breached provide the resource(download link) where you can get the database file**.

QUESTION-3 :-

Find 7 webcams which are connected in the open network and are live streaming i.e, when accessed you should be able to watch the live streaming(URL).

Note: All the webcams should be from one country only.

SYNOPSIS:-

Google dork is a search query. This uses advanced searching operations to find information that is not automatically available on a website. Google dorking is a passive attach that involves the use of custom code. Google dorking is also known as google hacking. It can return information difficult to locate through simple search queries.

ST#IS#4899

TECHNICAL PROCEDURE :-

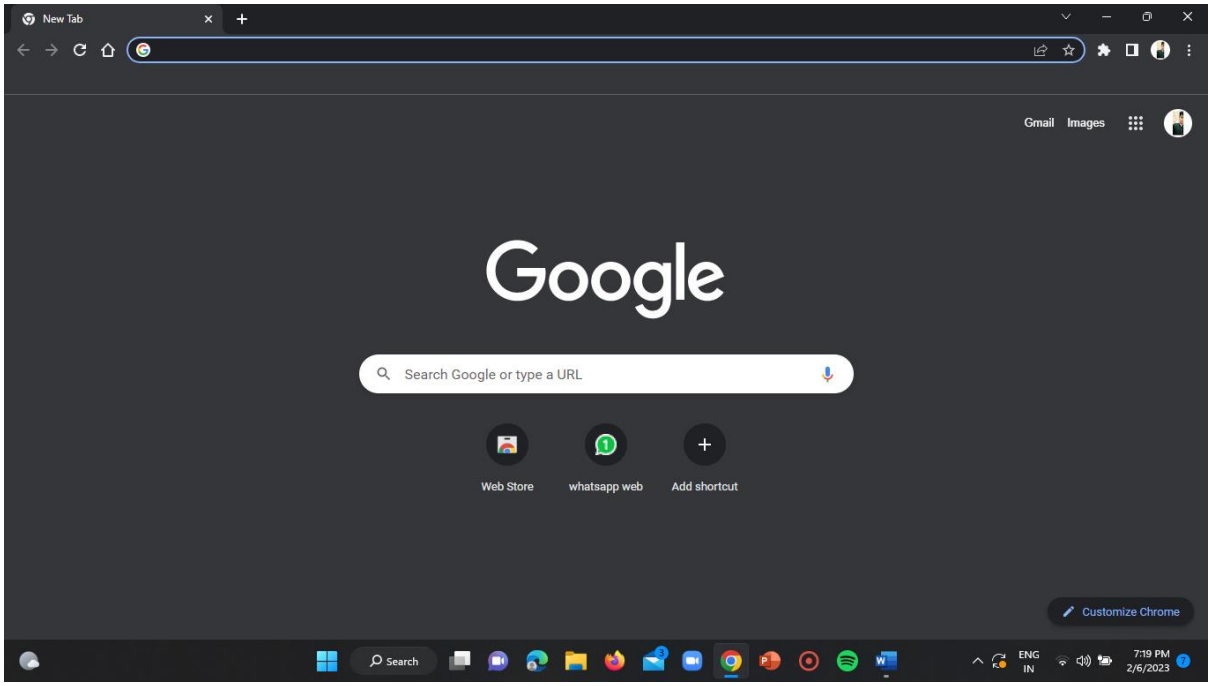
SOLUTION-1 :-

ADMIN LOGIN PAGES :-

TOOL USED:- “ GOOGLE DORKS ”

Step-1:

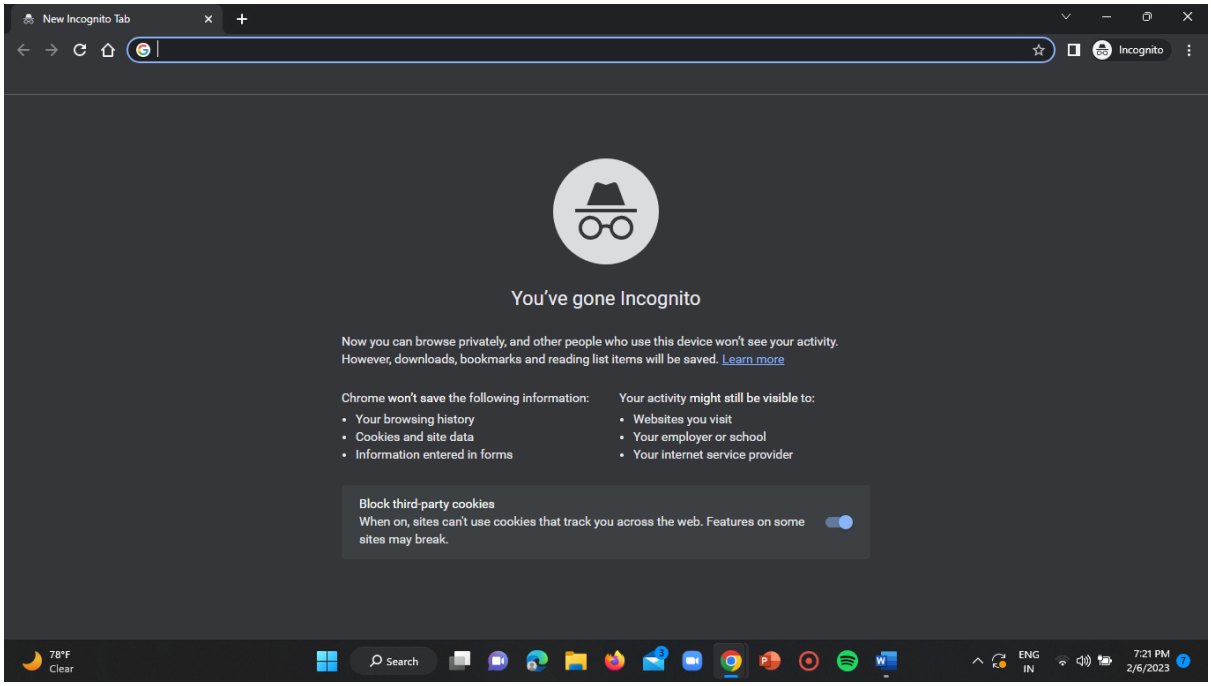
Open google chrome.



Step-2:

Open incognito window in your google manually or by using the below mentioned shortcut.

SHORTCUT = “ ctrl+shift+n ”



Step-3:

Start using several google dorks regarding the admin login page details.

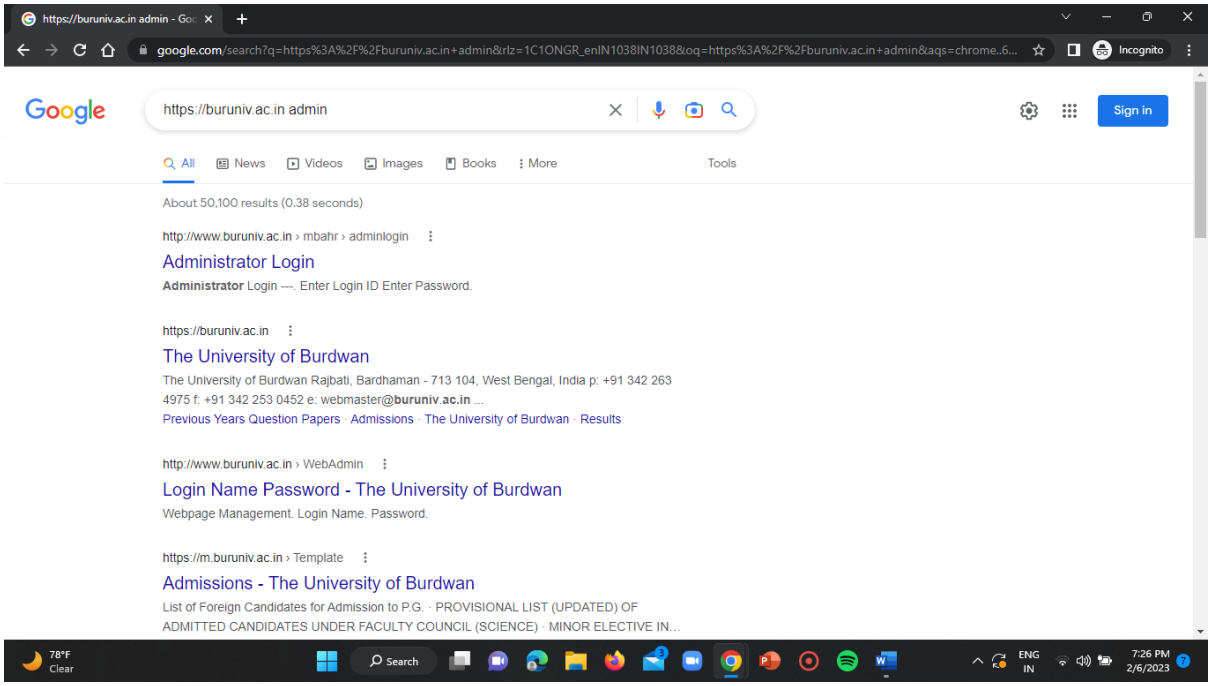
DOMAIN-1:

Step-4:

Use the "admin" dork for the very first domain.

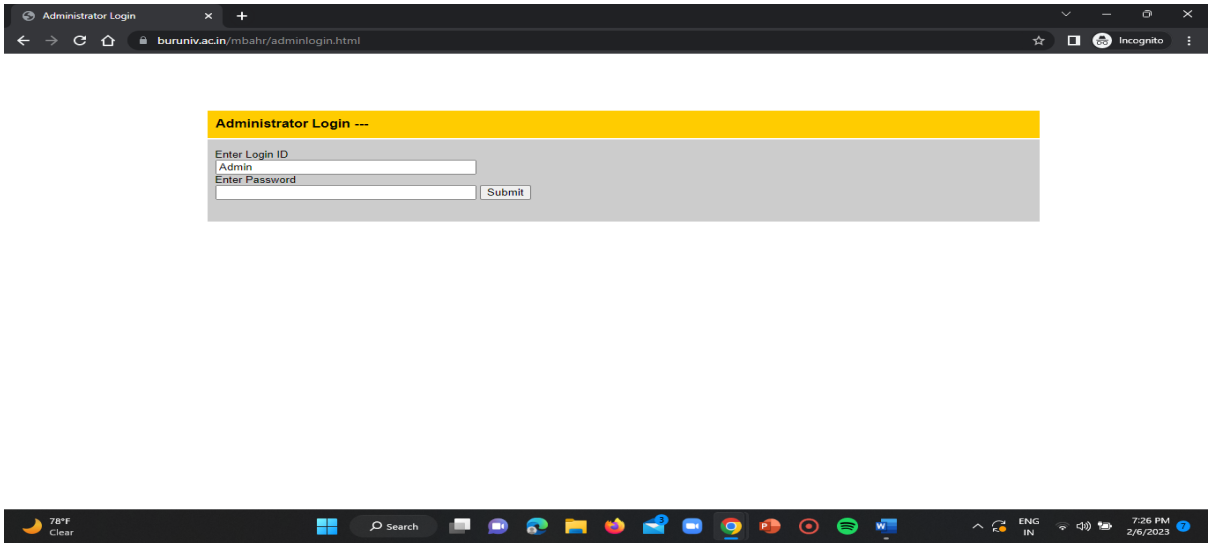
That is type " https://buruniv.ac.in admin "

ST#IS#4899



Step-5:

Now click on the very first blue link displayed on the home page is “Administrator login” page.



ADMIN PAGE LINK FOR THE FIRST TARGET DOMAIN:

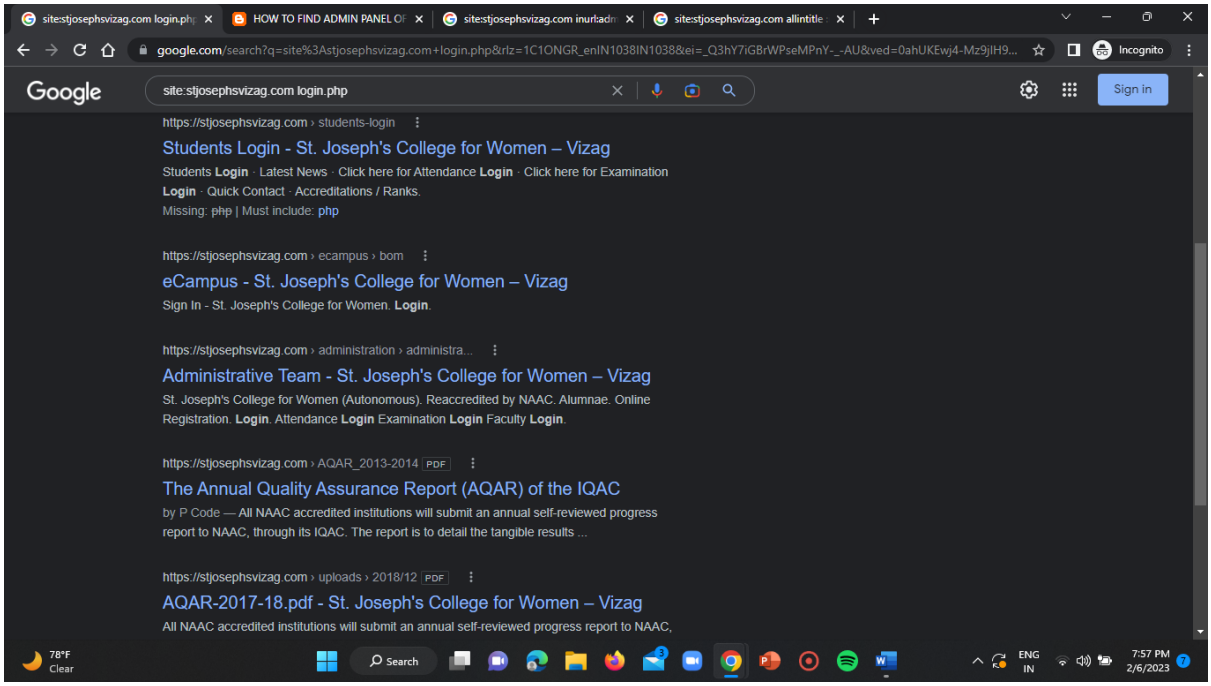
https://www.buruniv.ac.in/mbahr/adminlogin.html

DOMAIN-2:

Step-6:

In domain-2 use the google dork “site:stjosephsvizag.com login.php” and search it as it is in the search input section of the chrome page.

ST#IS#4899



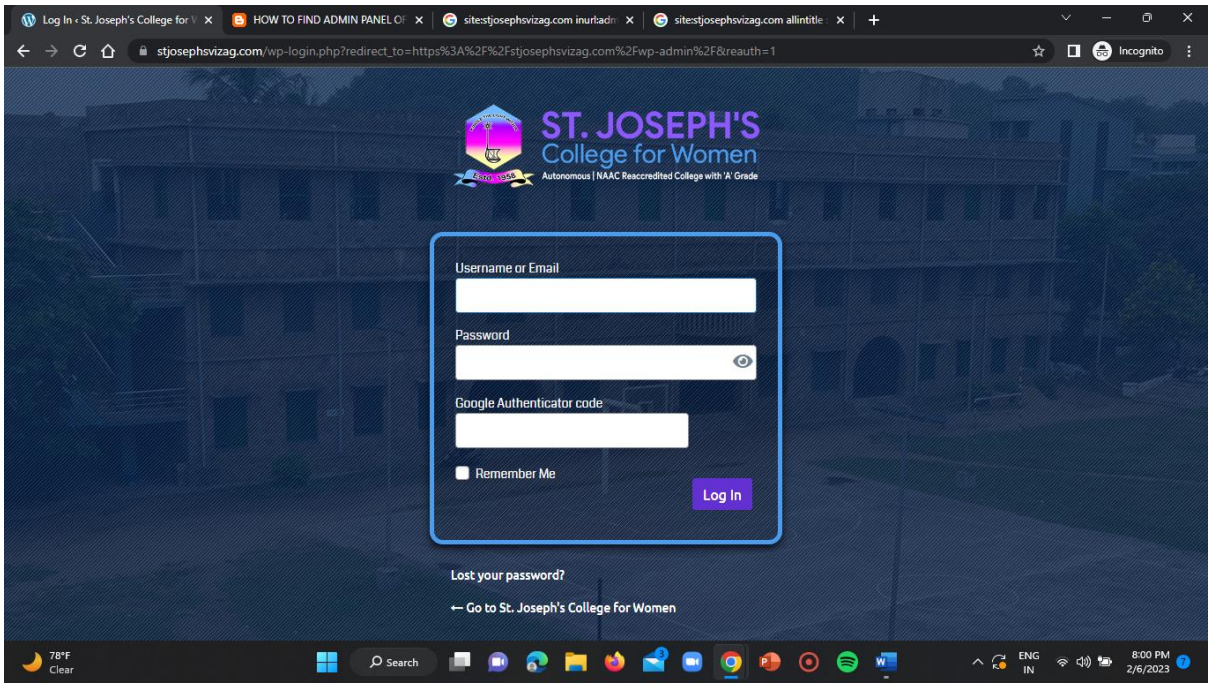
Step-7:

Now click on the blue link mentioning as “administrative team”.

The login page looks as follows.

ADMIN LOGIN PAGE LINK FOR THE SECOND TARGET DOMAIN:

https://stjosephsvizag.com/wp-login.php?redirect_to=https%3A%2F%2Fstjosephsvizag.com%2Fwp-admin%2F&reauth=1



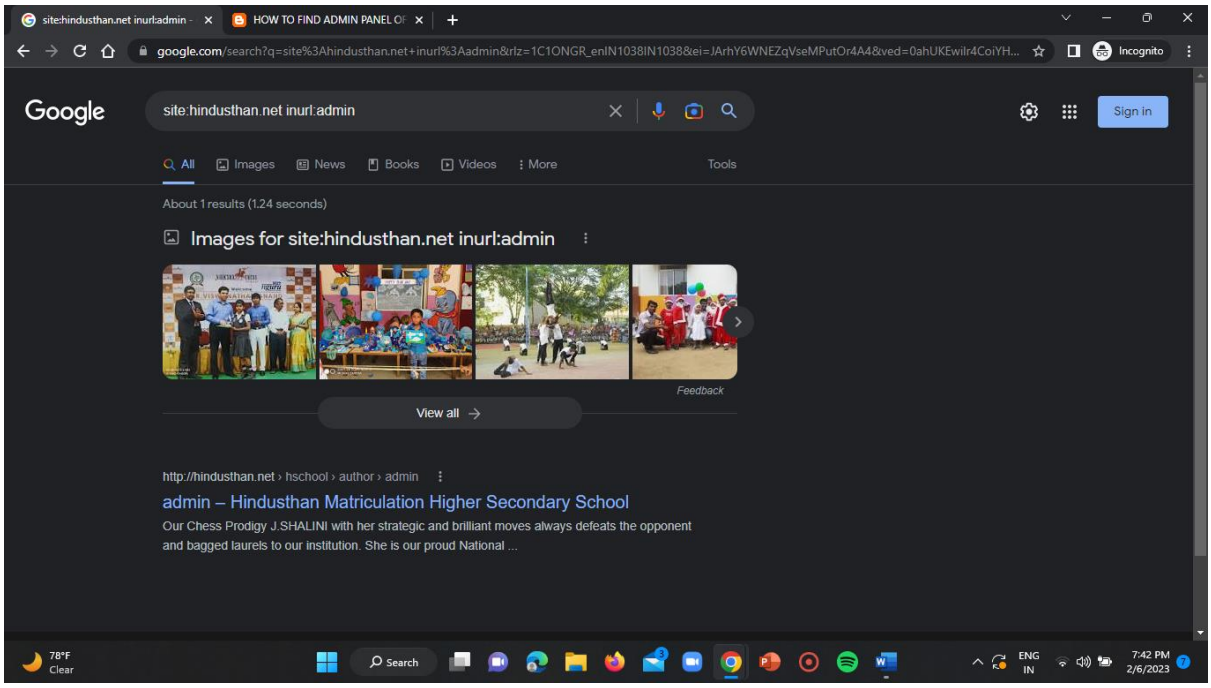
ST#IS#4899

DOMAIN-3:

Step-8:

In case of domain-3 use the google dork “site:hindusthan.net inurl:admin”

i.e search it on your chrome browser and wait for the results.



Step-9:

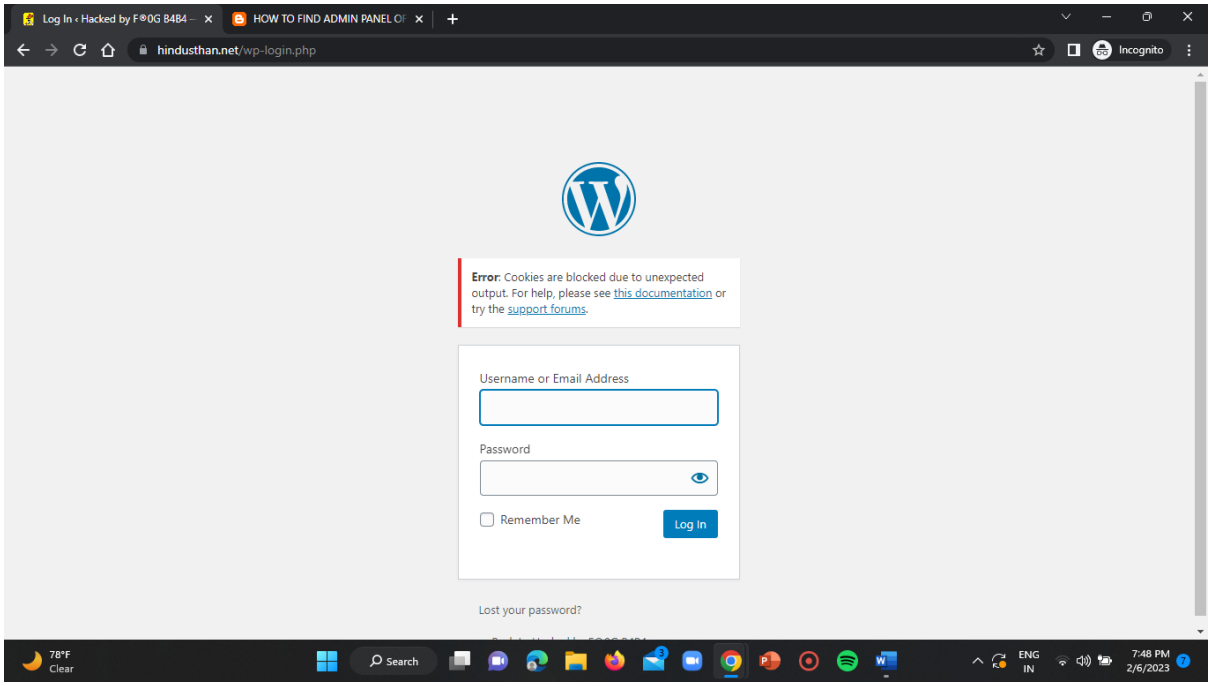
Now click on the blue link mentioning as “admin” on the displayed result page after searching.

Then the required admin portal i.e login page gets opened as shown below.

ADMIN LOGIN PAGE LINK FOR THE THIRD TARGET DOMAIN:

https://hindusthan.net/wp-login.php

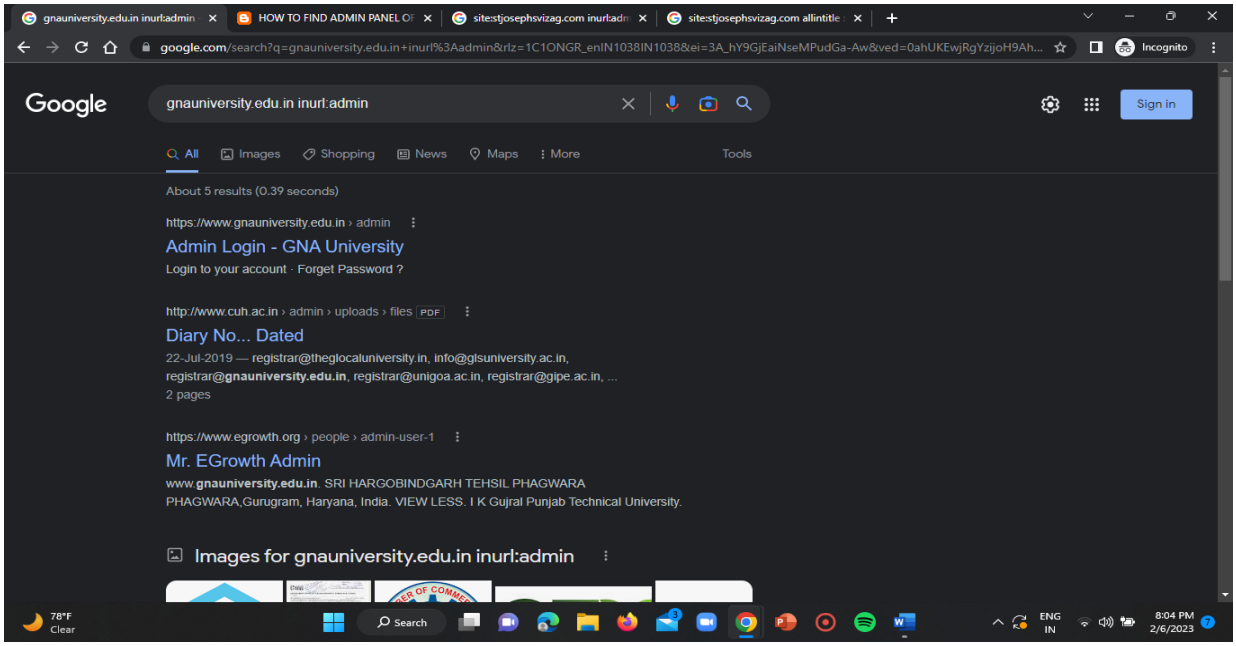
ST#IS#4899



DOMAIN-4:

Step-10:

For this fourth target domain use the “inurl:admin” google dork and search it on the chrome window followed by the domain link i.e as “gnauniversity.edu.in inurl:admin” .



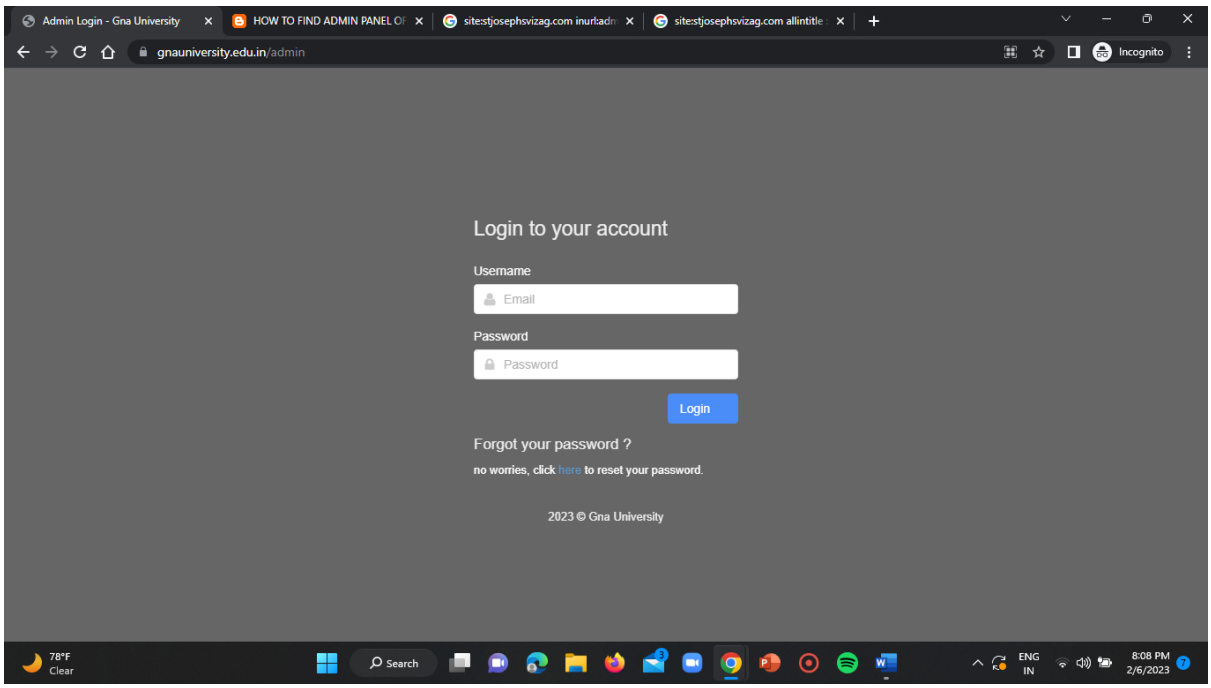
Step-11:

Now open the blue link which is displayed as “Admin Login” in the above result page of the chrome.

ST#IS#4899

ADMIN LOGIN PAGE LINK FOR THE FOURTH TARGET DOMAIN:

https://www.gnauniversity.edu.in/admin

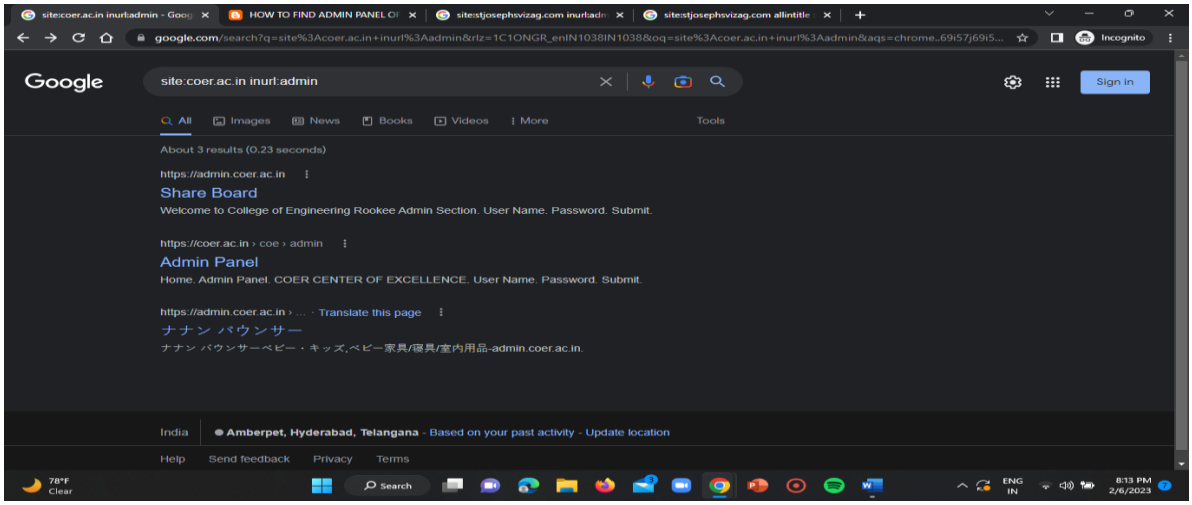


DOMAIN-5:

Step-12:

In case of fifth target domain use the “inurl:admin” google dork to obtain the admin login page for the target domain.

Search in the search bar as “site:coer.ac.in inurl:admin”



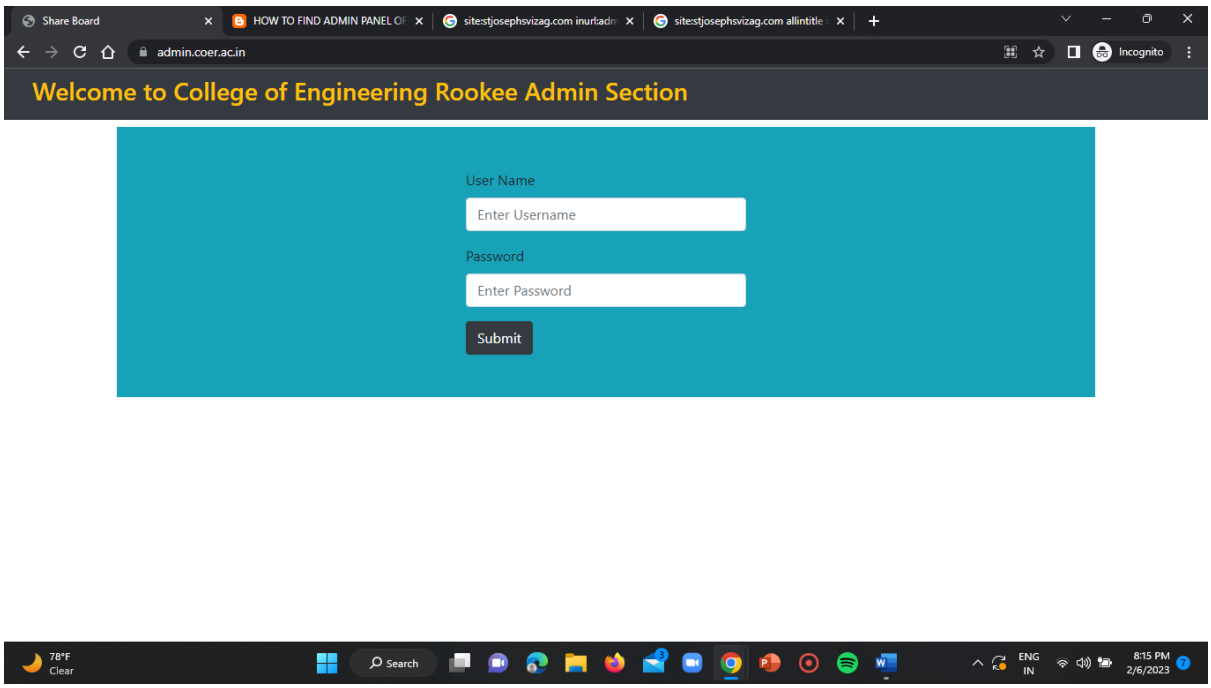
Step-13:

Now click on the first blue link displaying as “Share board”.

ST#IS#4899

ADMIN LOGIN PAGE LINK FOR THE FIFTH TARGET DOMAIN:

https://admin.coer.ac.in/



SOLUTION-2 :-

A-BIT :-

TOOL USED = “ HUNTER.IO **”**

DOMAIN-1 :

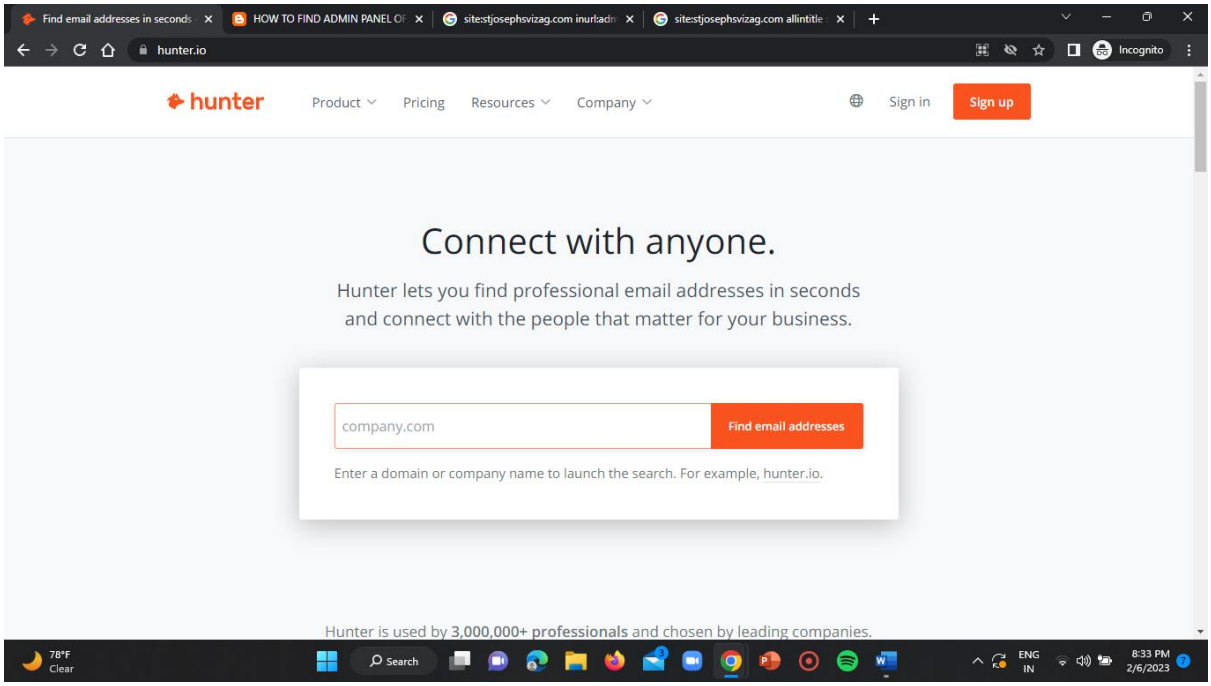
Step-1:

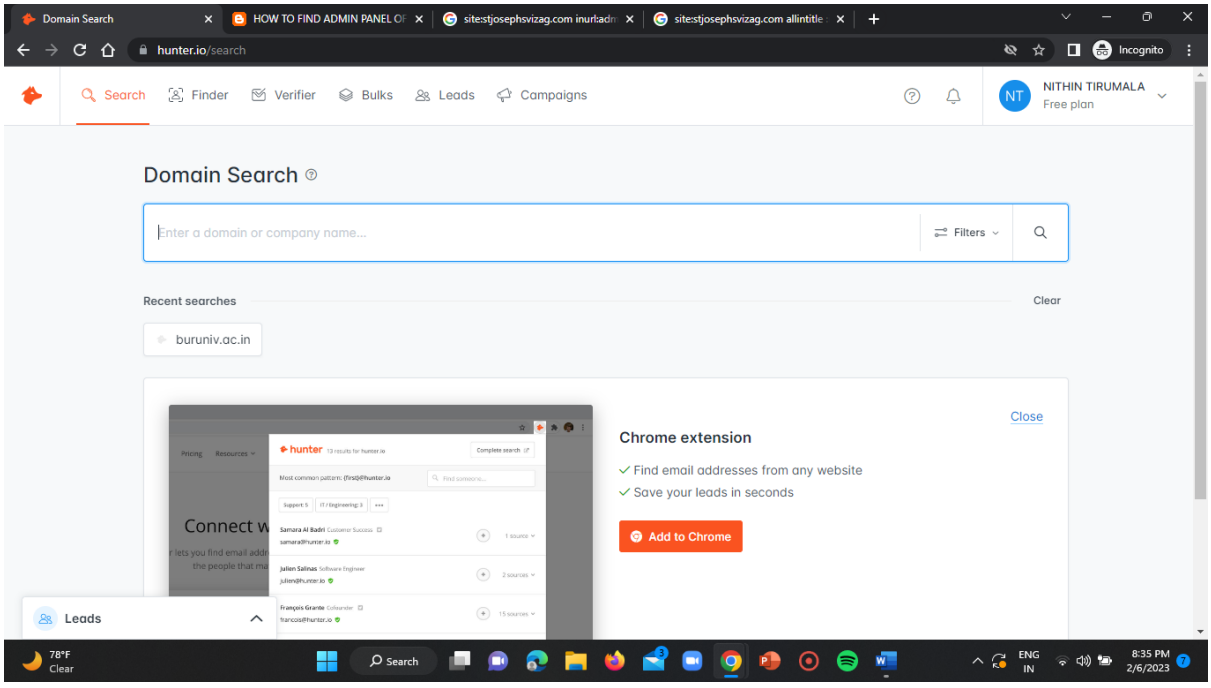
Open your google chrome and search for the hunter.io webpage using the below mentioned link.

LINK: https://hunter.io/

Note: For appropriate and accurate results you need to signup using an organisation/work email IDs i.e the college provided student accounts can also be used to create your accounts.

ST#IS#4899

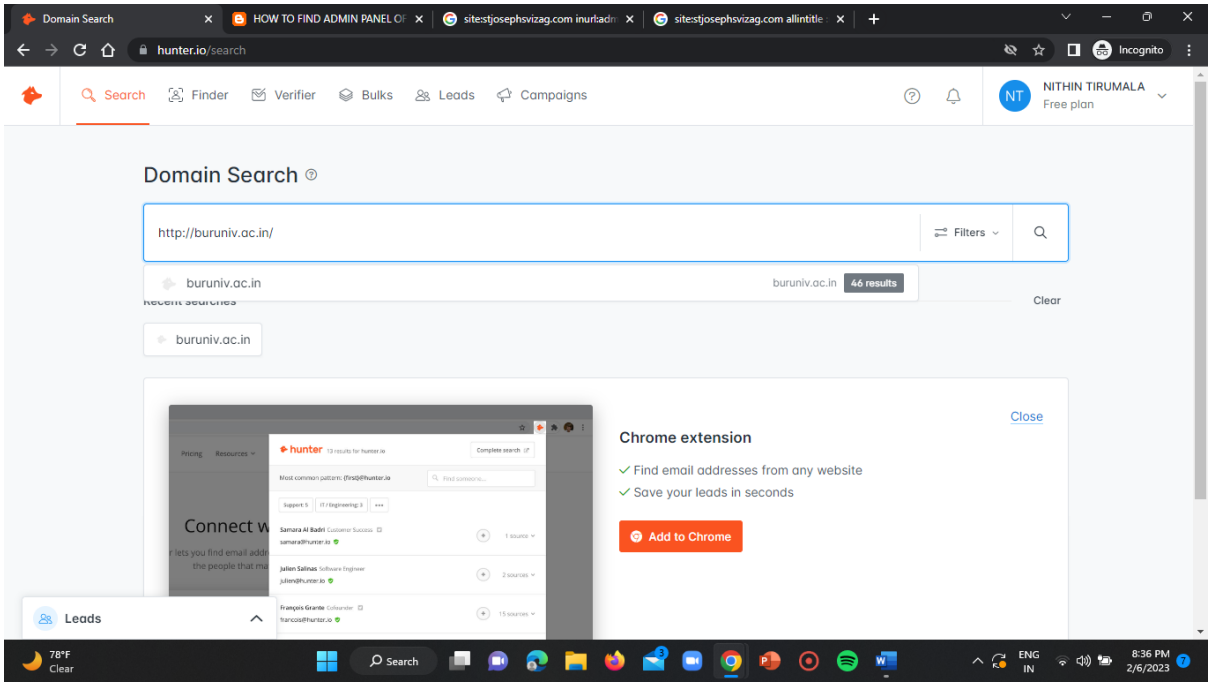




Step-2:

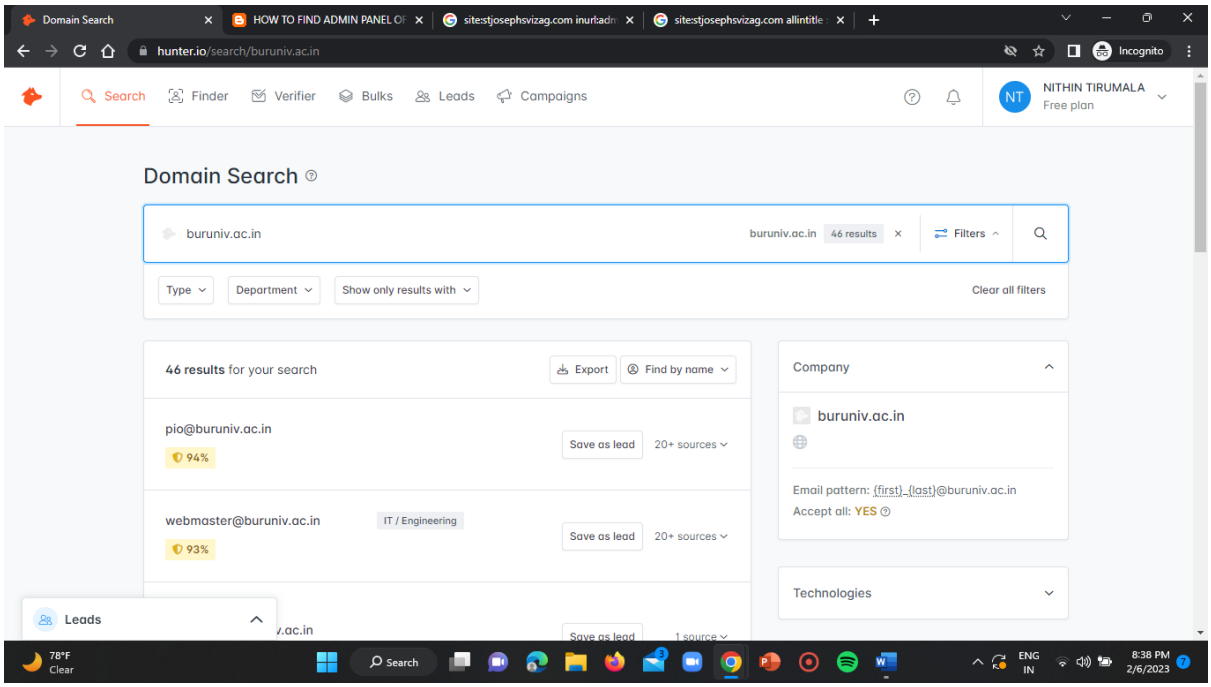
Enter the target domain name in the input bar of the hunter.io homepage and click on enter key.

ST#IS#4899



Step-3:

The result displaying the various email addresses of the target domain will be displayed as shown below.



E-MAIL ADDRESSES OF THE TARGET DOMAIN-1:

1) pio@buruniv.ac.in
2) webmaster@buruniv.ac.in
3) dean_arts@buruniv.ac.in
4) registrar@buruniv.ac.in

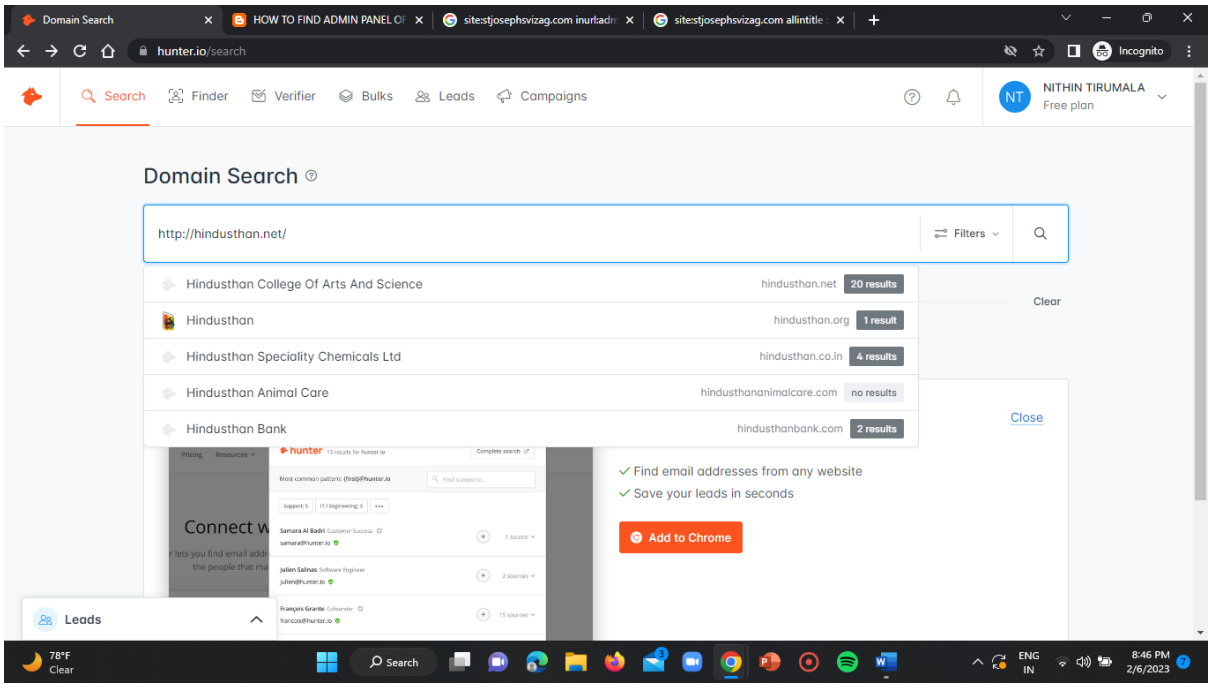
5) info@buruniv.ac.in
6) rect.mba@buruniv.ac.in
7) rect.chemistry@buruniv.ac.in
8) rect.sanskrit@buruniv.ac.in
9) rect.hindi@buruniv.ac.in
10) rect.education@buruniv.ac.in

STEP NOTE – Similarly do the same thing i.e follow the same steps for all the domains.

DOMAIN-4 :

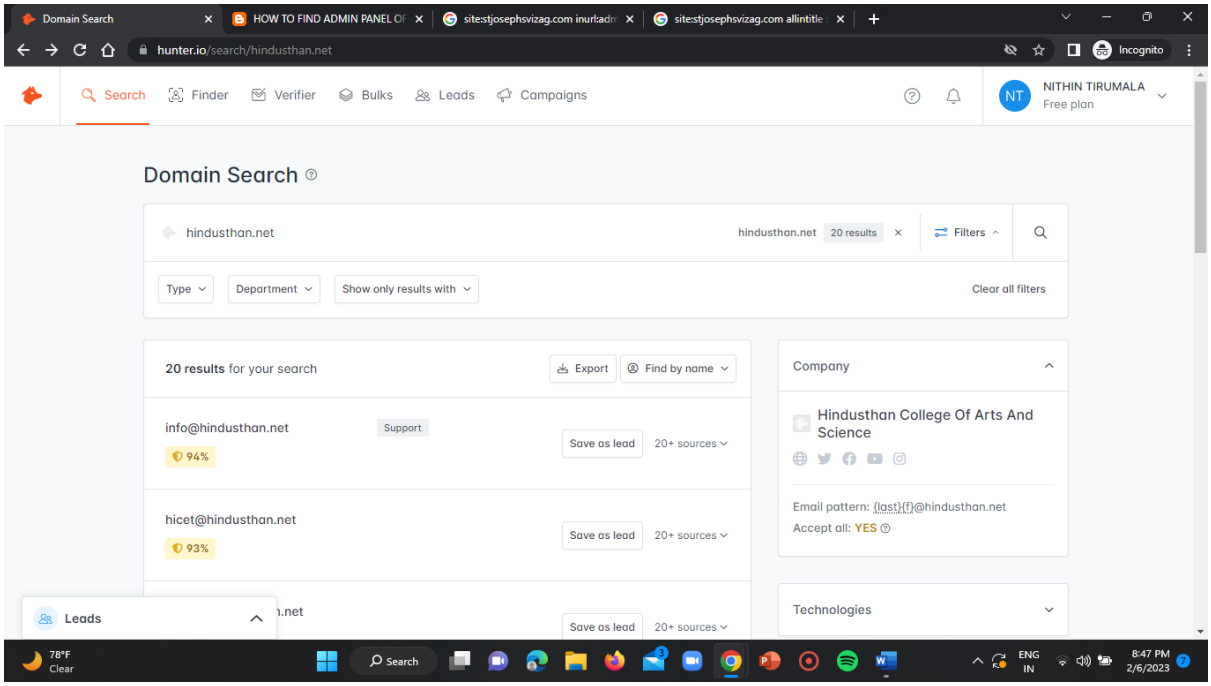
Step-5:

Give the target domain in the search bar of the hunter homepage and click on enter key.



It results the page with the required email addresses of the target domain as follows.

ST#IS#4899



E-MAIL ADDRESSES OF THE TARGET DOMAIN-4:

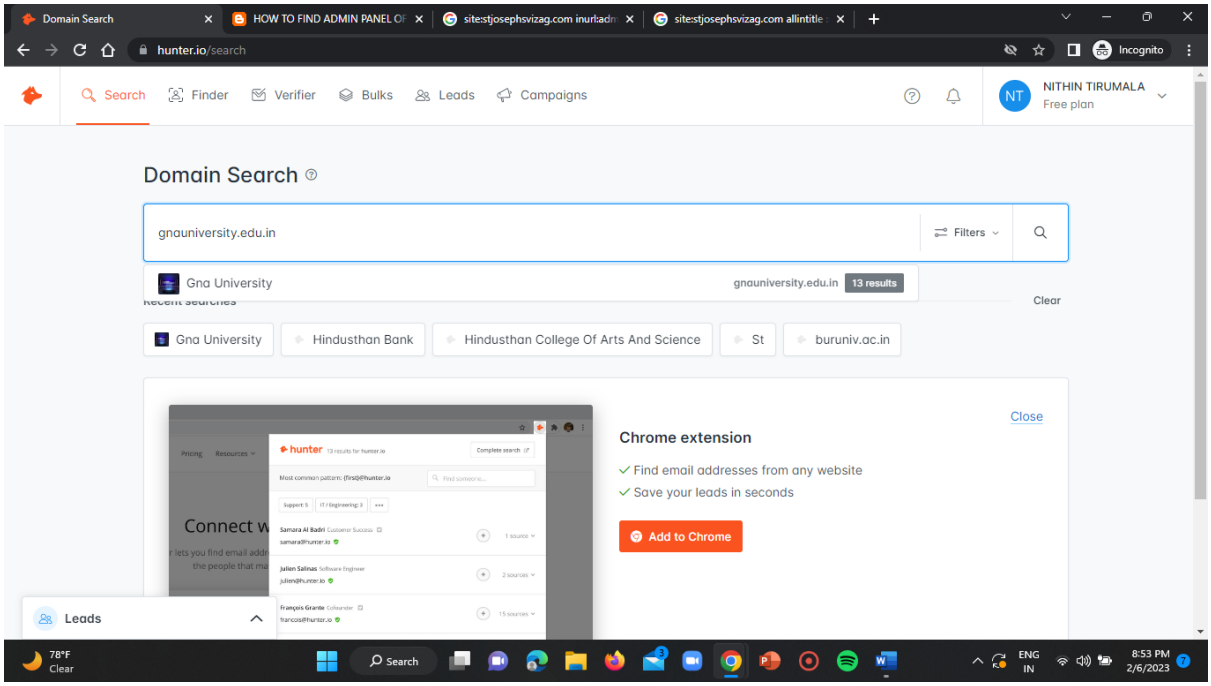
1) info@hindusthan.net
2) hicet@hindusthan.net
3) hitech@hindusthan.net
4) hitprincipal@hindusthan.net
5) hicas@hindusthan.net
6) barch@hindusthan.net
7) school@hindusthan.net
8) admission@hindusthan.net
9) ecampus@hindusthan.net
10) bed@hindusthan.net

DOMAIN-3 :

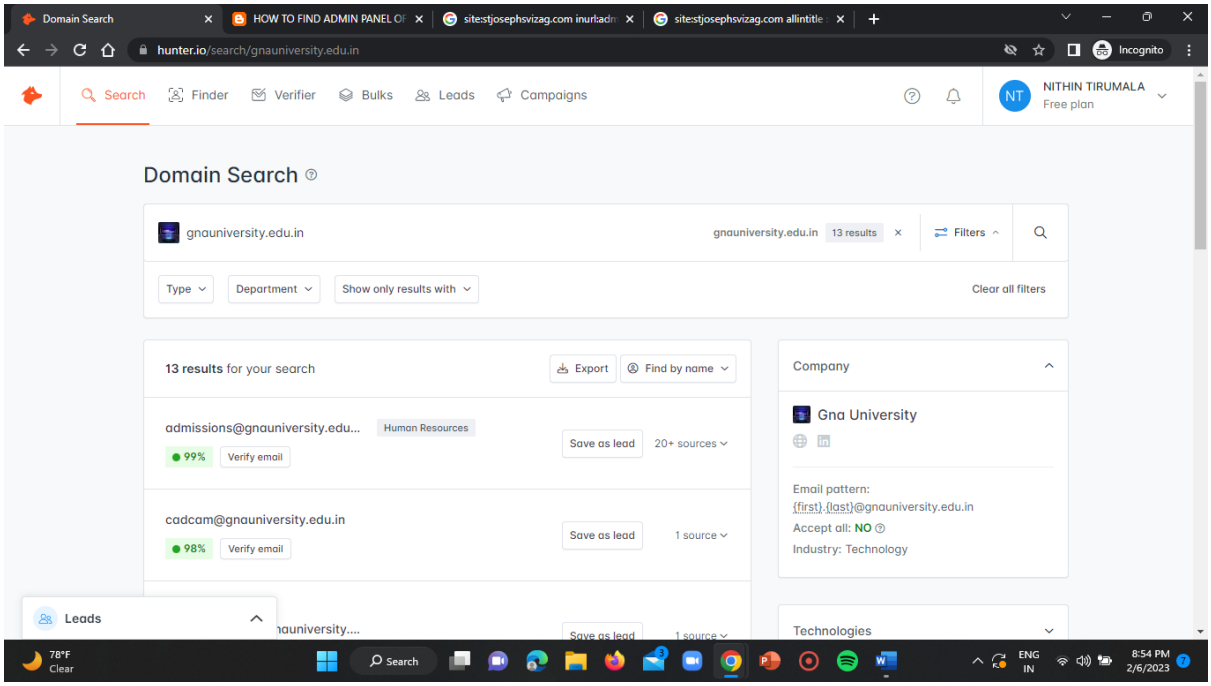
Step-6:

Enter the target domain in the search input bar of the hunter homepage.

ST#IS#4899



It results the page with the required email addresses of the target domain as follows.



E-MAIL ADDRESSES OF THE TARGET DOMAIN-3:

1) admissions@gnauniversity.edu.in
2) cadcam@gnauniversity.edu.in
3) sushant.anand@gnauniversity.edu.in
4) parveen.singh@gnauniversity.edu.in
5) info@gnauniversity.edu.in

6) icohost@gnauniversity.edu.in
7) iso@gnauniversity.edu.in
8) research@gnauniversity.edu.in
9) dean.foh@gnauniversity.edu.in
10) careers@gnauniversity.edu.in

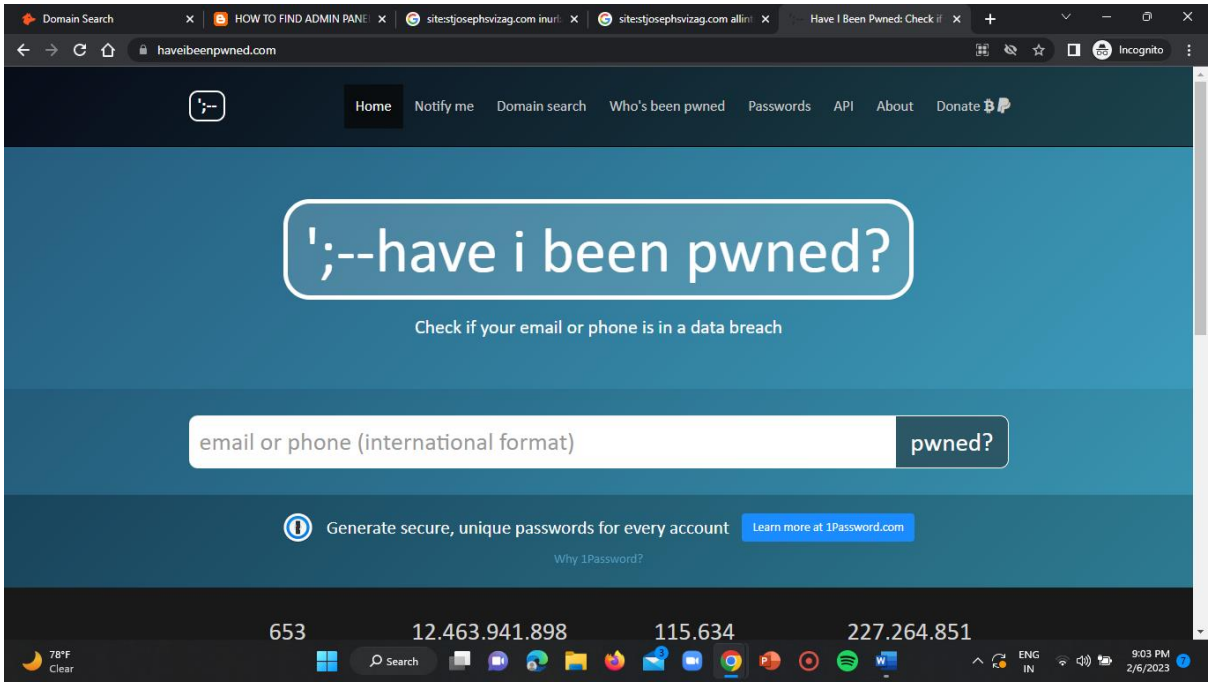
B – BIT:

TOOL USED = "HAVE I BEEN PWNED"

Link for the tool = https://haveibeenpwned.com/

Step-1:

Open your chrome incognito window in the browser and enter the above mentioned URL to get the access of "have I been pwned" tool.



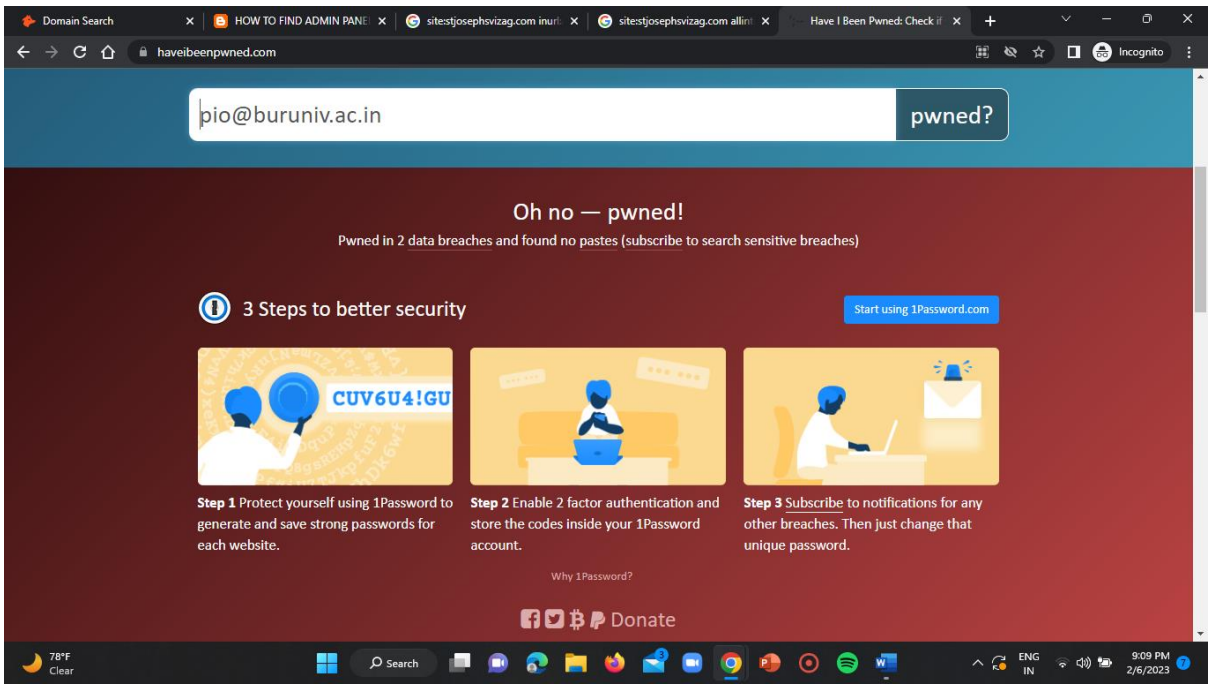
Step-2:

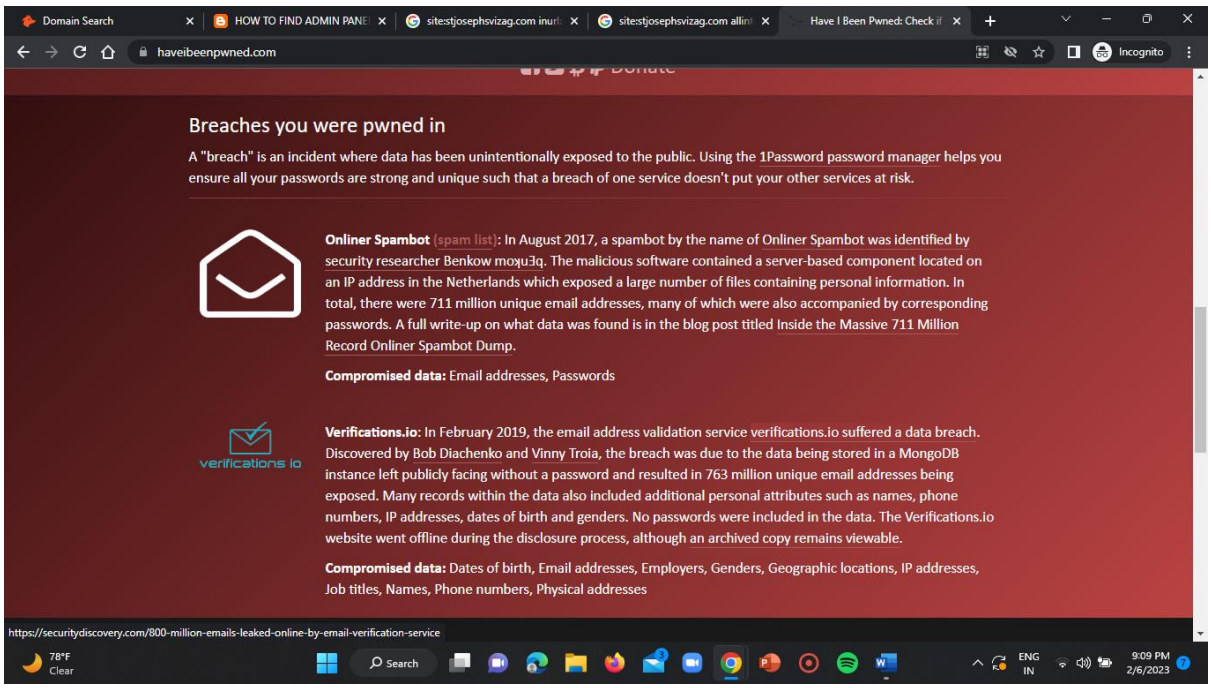
Paste all the target email addresses that you have found in the above A-BIT solution of the target domains in the input bar of the have I been pwned homepage to check whether the respective email addresses are breached are not.

ST#IS#4899

DATA BREACH VERIFICATION FOR ALL THE 30 EMAIL IDs :-

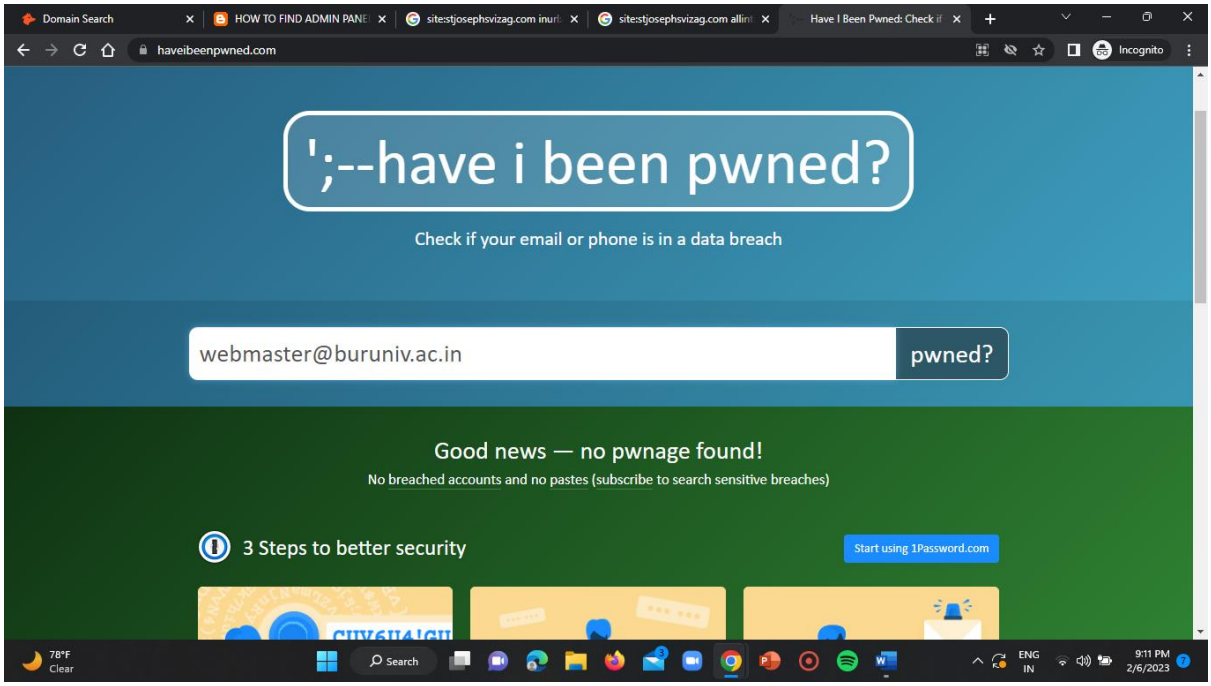
1) pio@buruniv.ac.in



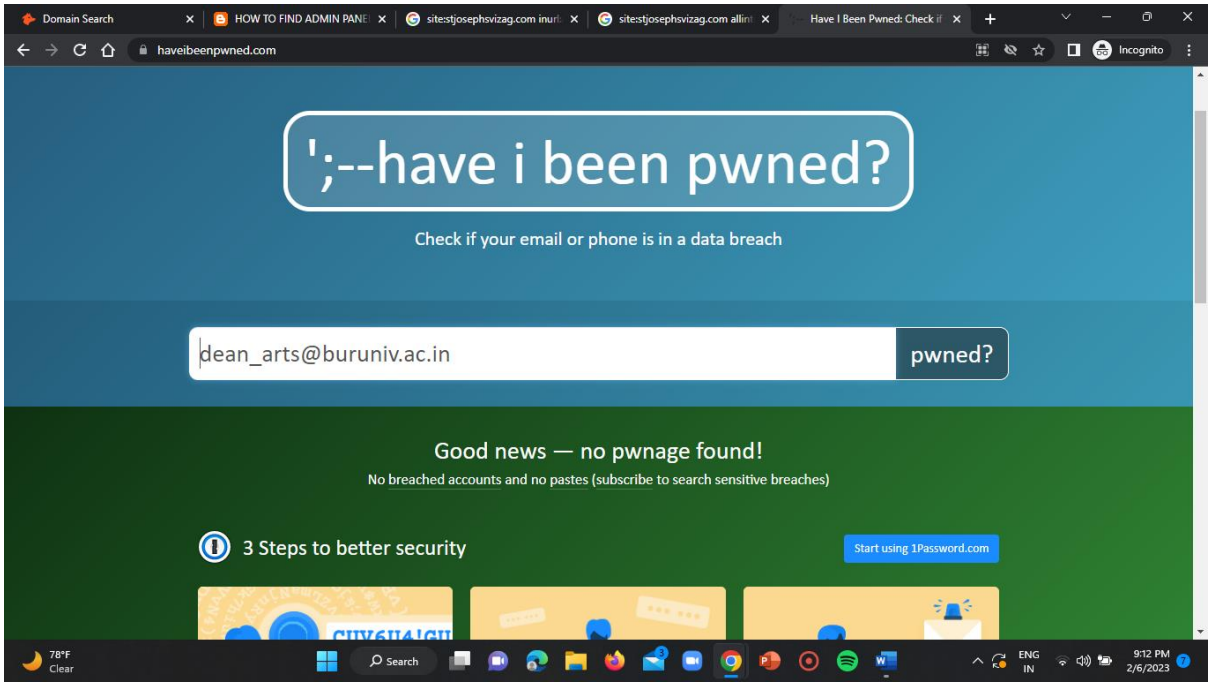


ST#IS#4899

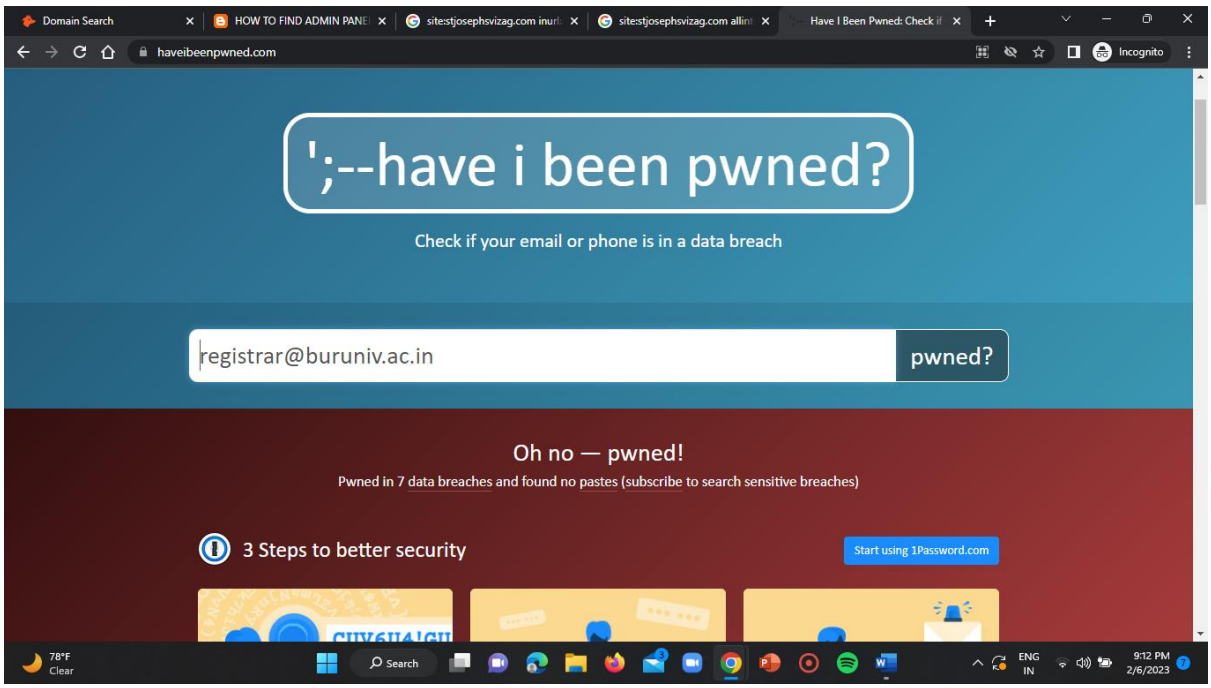
2) webmaster@buruniv.ac.in

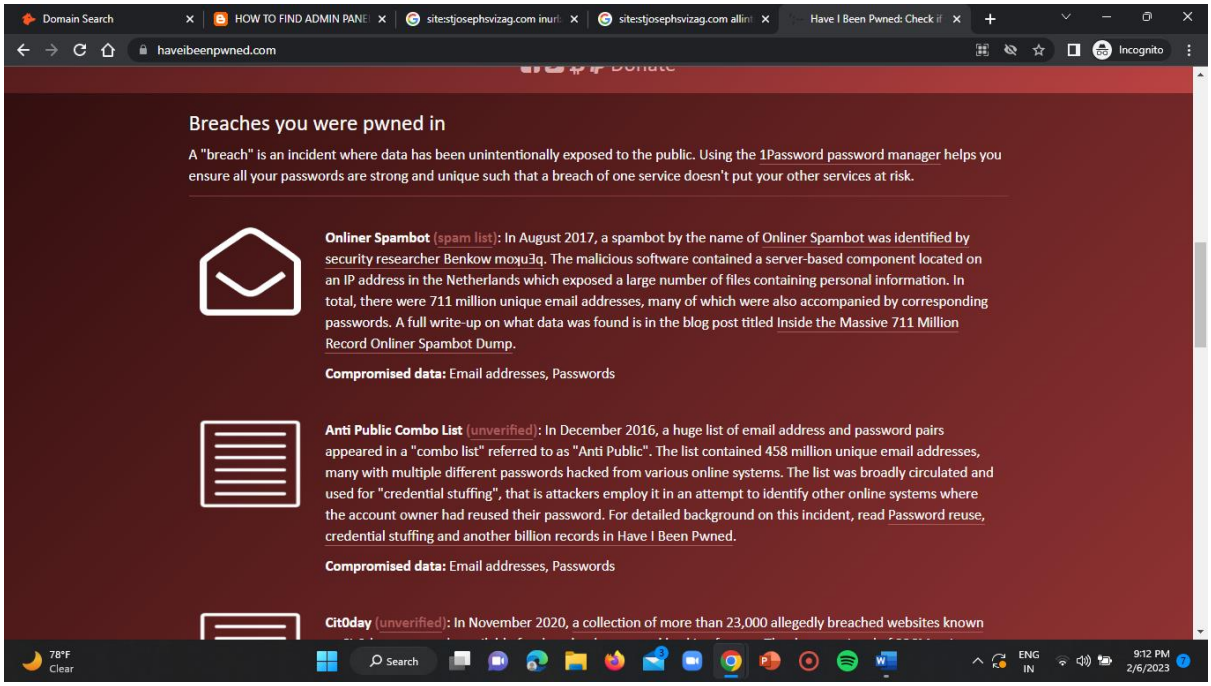


3) dean_arts@buruniv.ac.in

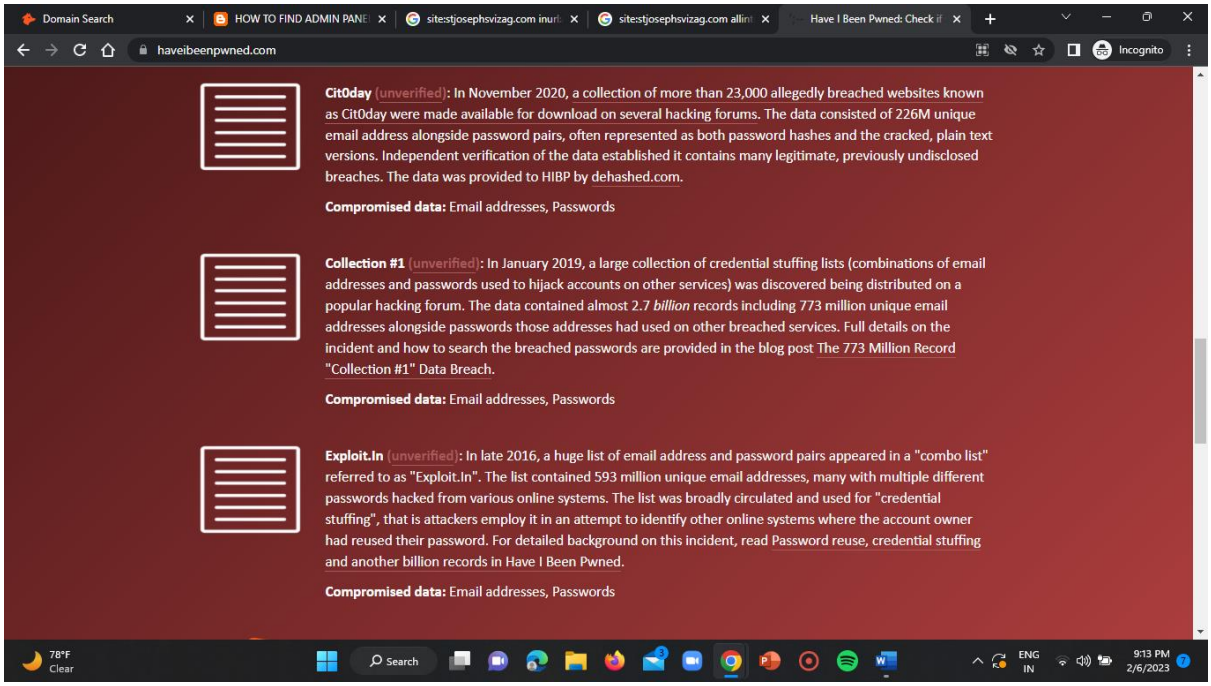


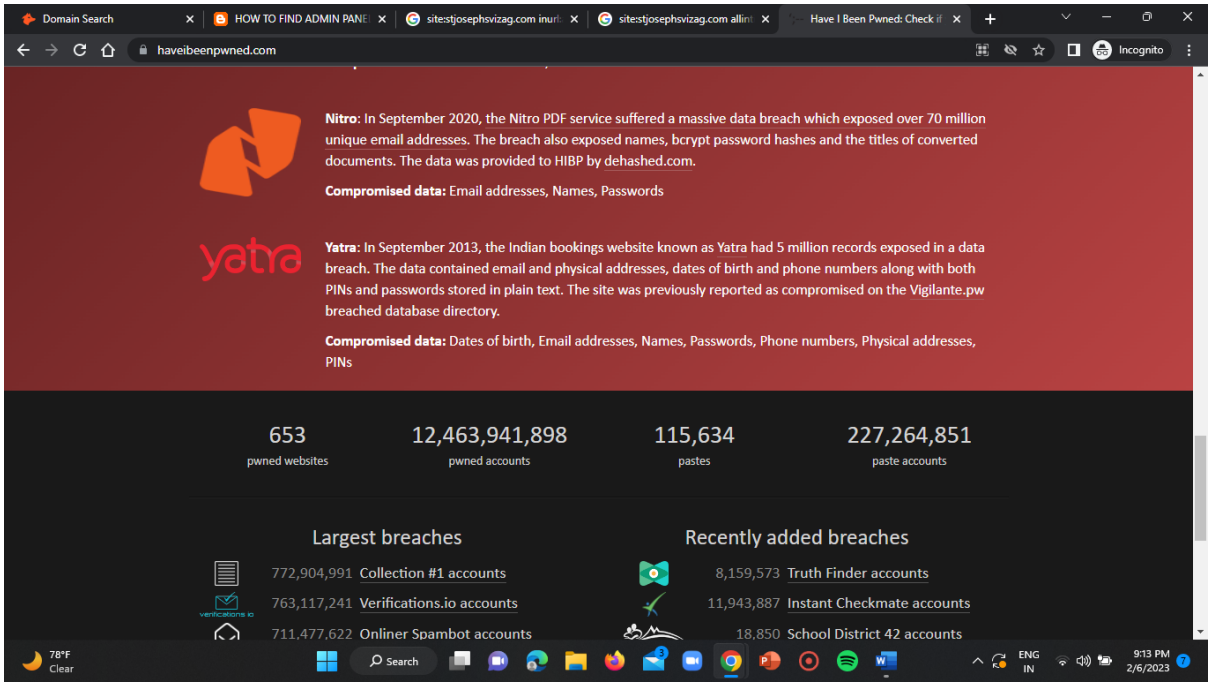
4) registrar@buruniv.ac.in



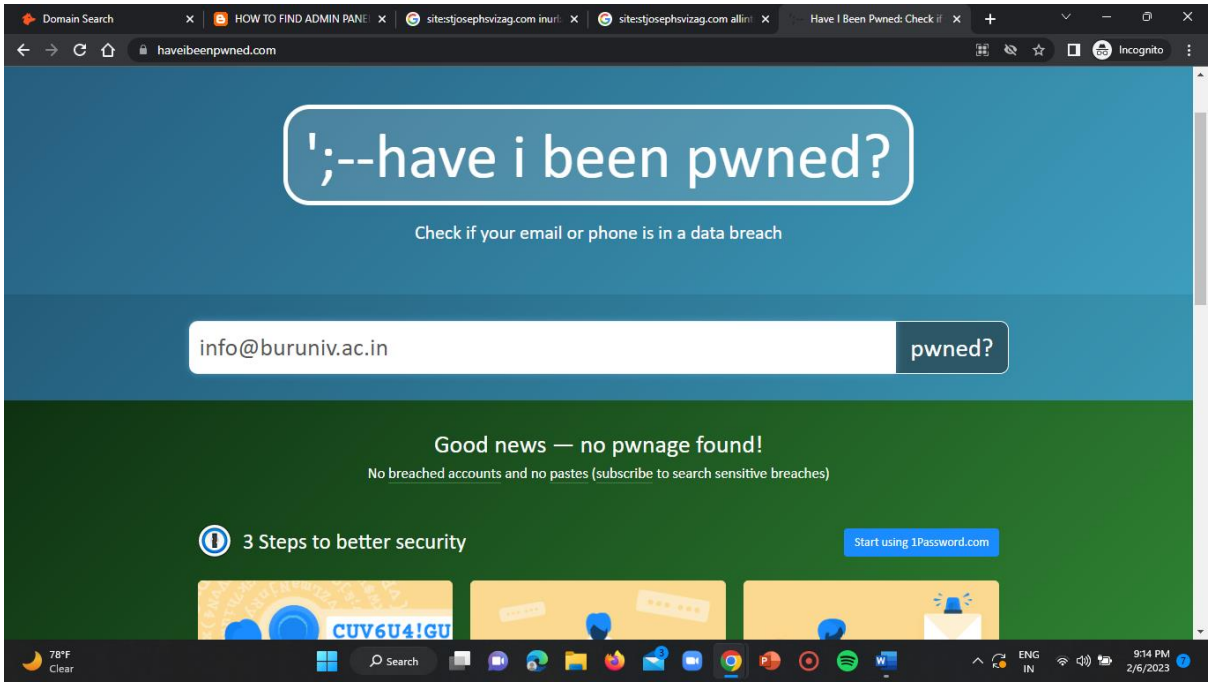


ST#IS#4899

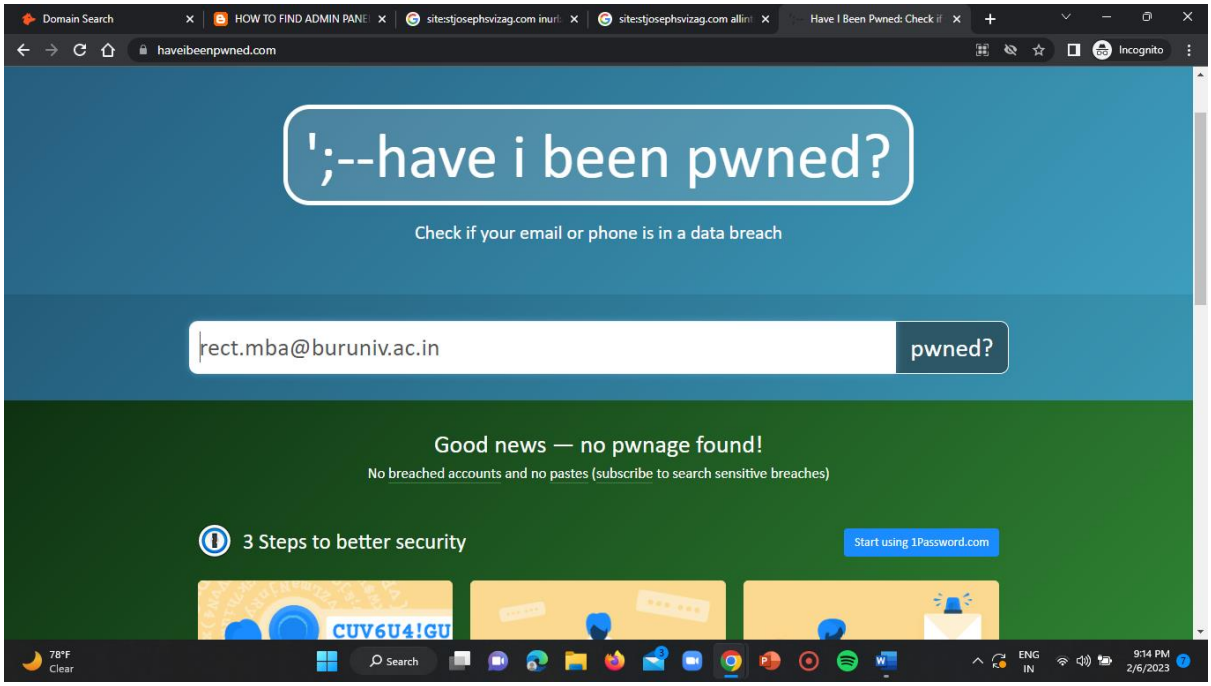

Domain Search
HOW TO FIND ADMIN PANE
site:stjosephsvizag.com inurl
site:stjosephsvizag.com allint
Have I Been Pwned: Check if
haveibeenpwned.com
Incognito
Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.
Compromised data: Email addresses, Passwords
Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.
Compromised data: Email addresses, Passwords
Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.
Compromised data: Email addresses, Passwords
78°F
Clear
Search
ENG
IN
9:13 PM
2/6/2023


Domain Search
HOW TO FIND ADMIN PANE
site:stjosephsvizag.com inurl
site:stjosephsvizag.com allint
Have I Been Pwned: Check if
haveibeenpwned.com
Incognito
Nitro: In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bcrypt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.
Compromised data: Email addresses, Names, Passwords
yatra
Yatra: In September 2013, the Indian bookings website known as Yatra had 5 million records exposed in a data breach. The data contained email and physical addresses, dates of birth and phone numbers along with both PINs and passwords stored in plain text. The site was previously reported as compromised on the Vigilante.pw breached database directory.
Compromised data: Dates of birth, Email addresses, Names, Passwords, Phone numbers, Physical addresses, PINs
653
pwned websites
12,463,941,898
pwned accounts
115,634
pastes
227,264,851
paste accounts
Largest breaches
772,904,991 Collection #1 accounts
763,117,241 Verifications.io accounts
711,477,622 Onliner Spambot accounts
Recently added breaches
8,159,573 Truth Finder accounts
11,943,887 Instant Checkmate accounts
18,850 School District 42 accounts
78°F
Clear
Search
ENG
IN
9:13 PM
2/6/2023

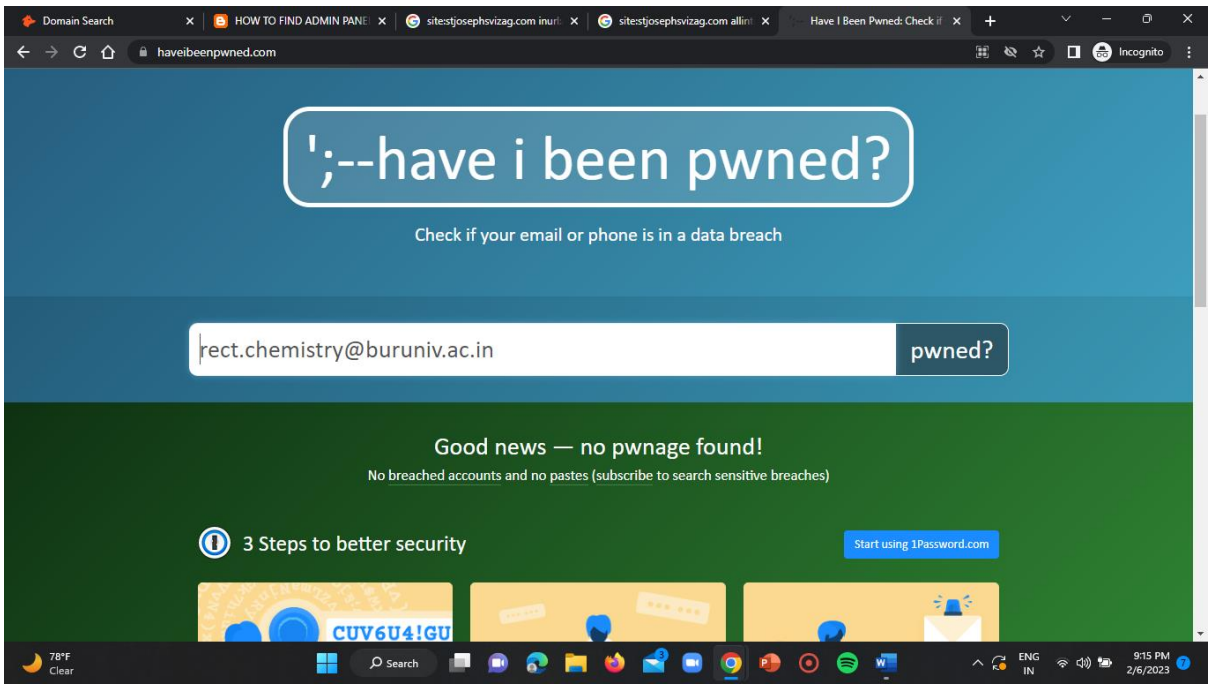
5) info@buruniv.ac.in



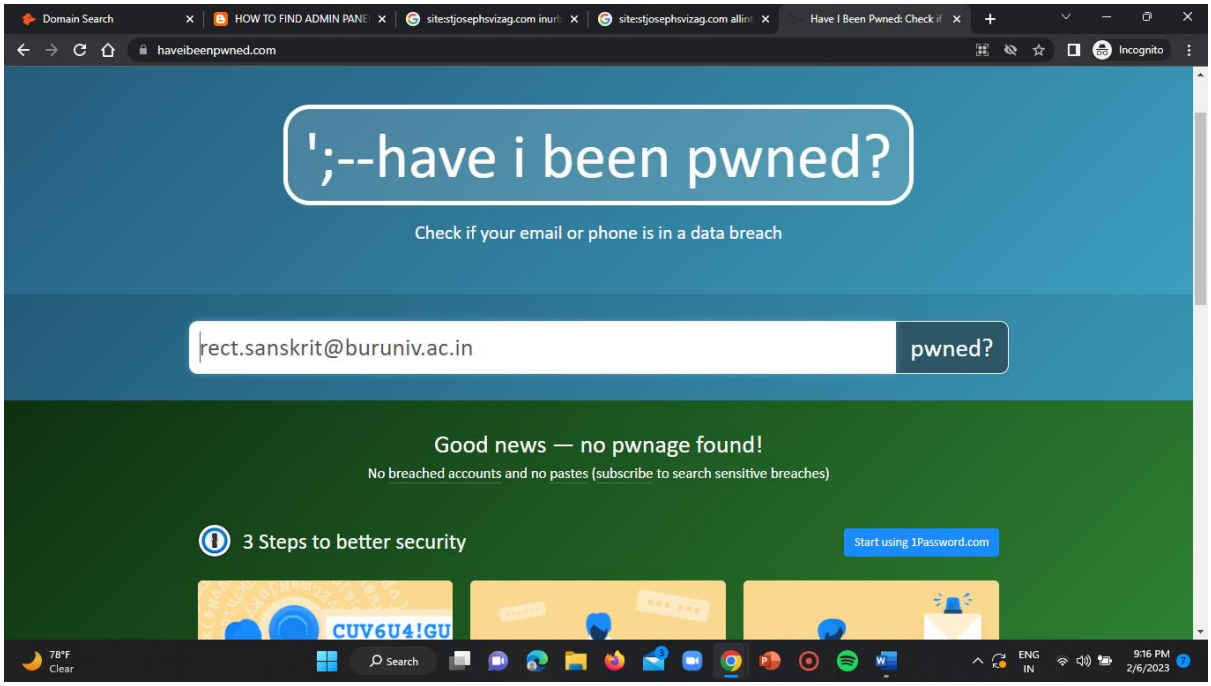
6) rect.mba@buruniv.ac.in



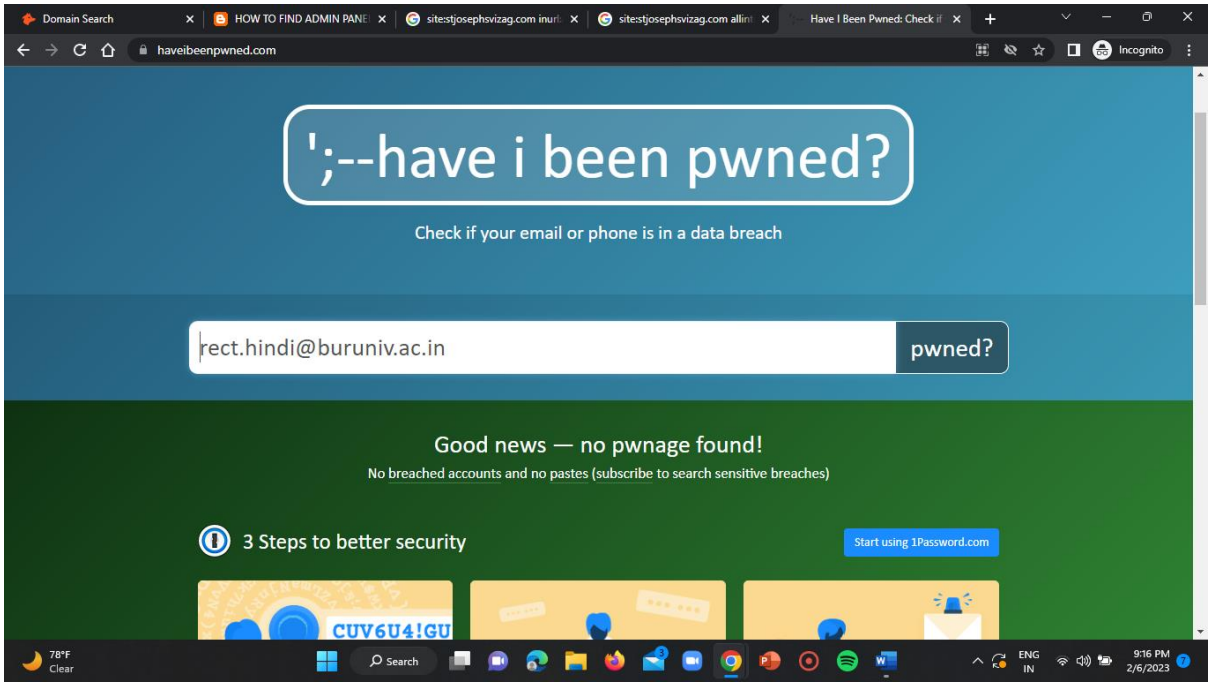
7) rect.chemistry@buruniv.ac.in



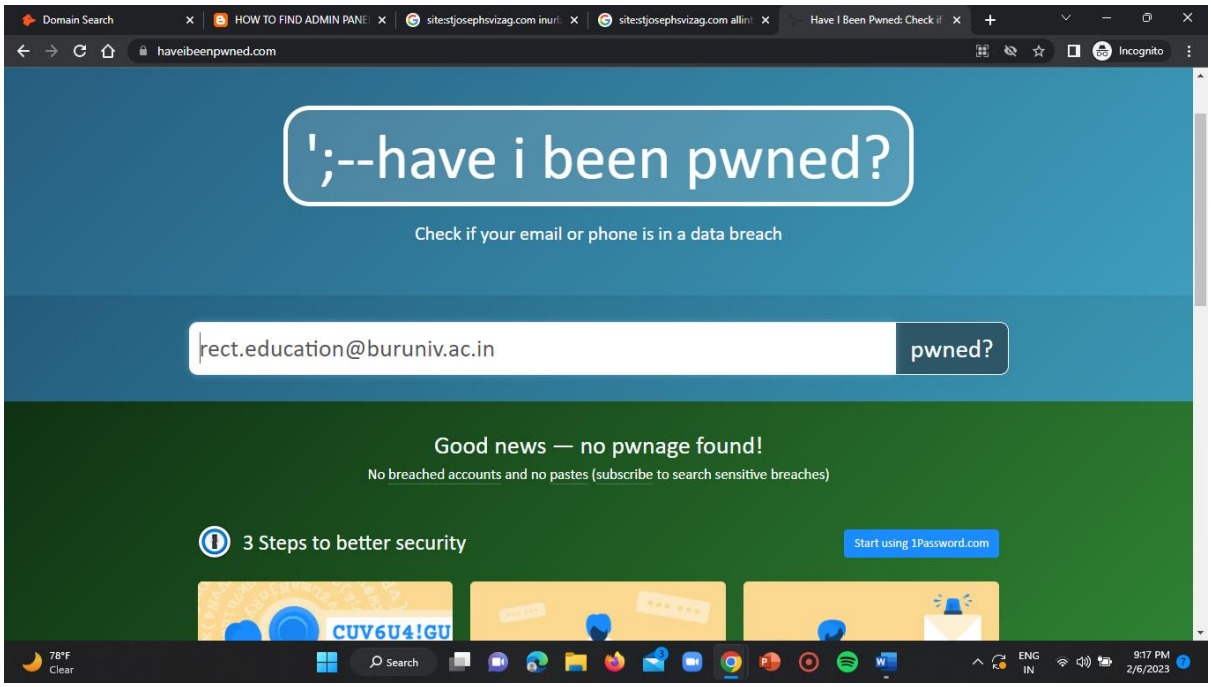
8) rect.sanskrit@buruniv.ac.in



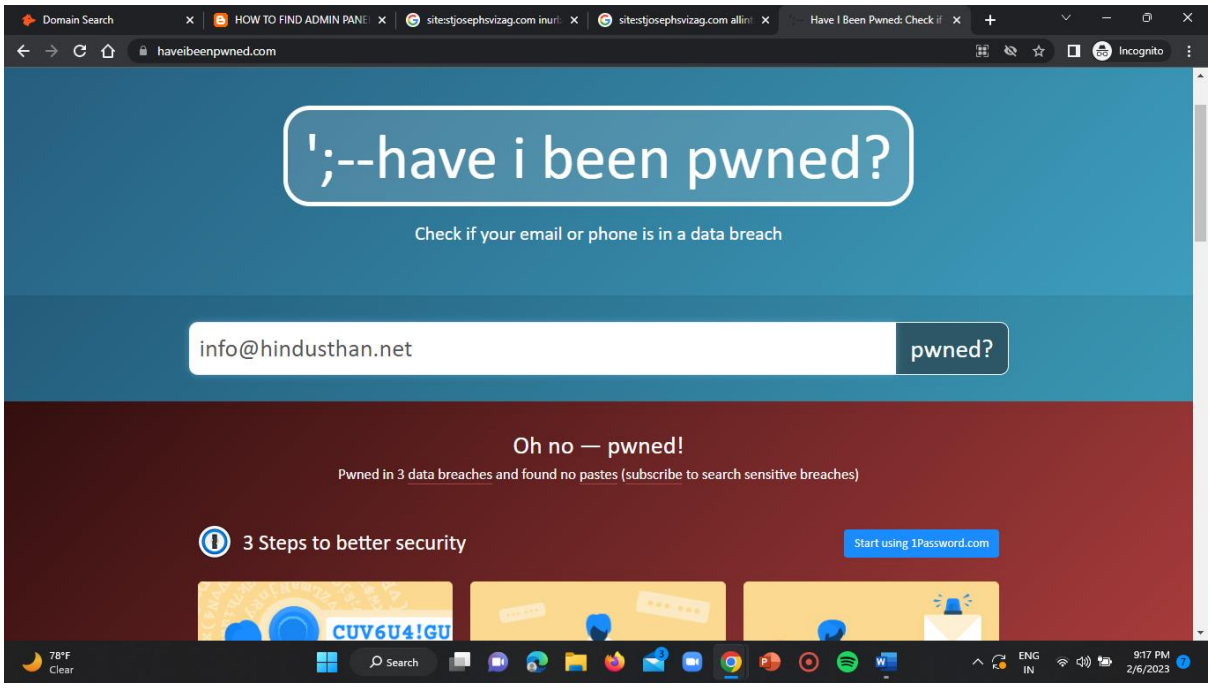
9) rect.hindi@buruniv.ac.in

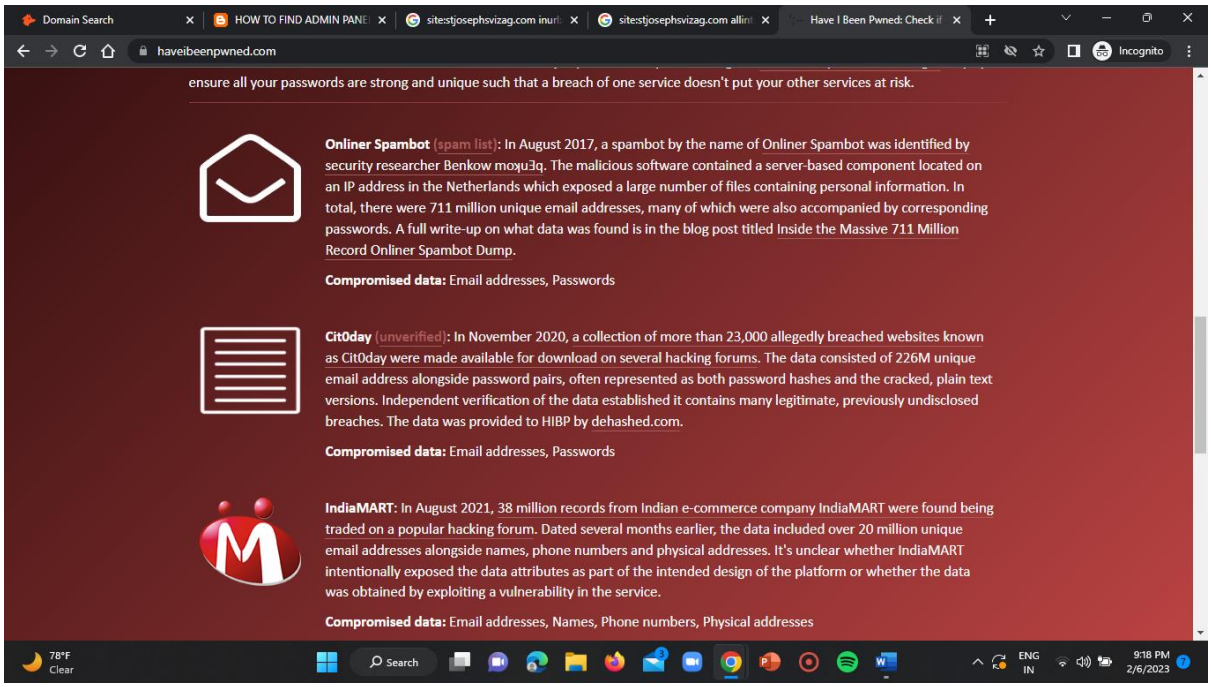


10) rect.education@buruniv.ac.in

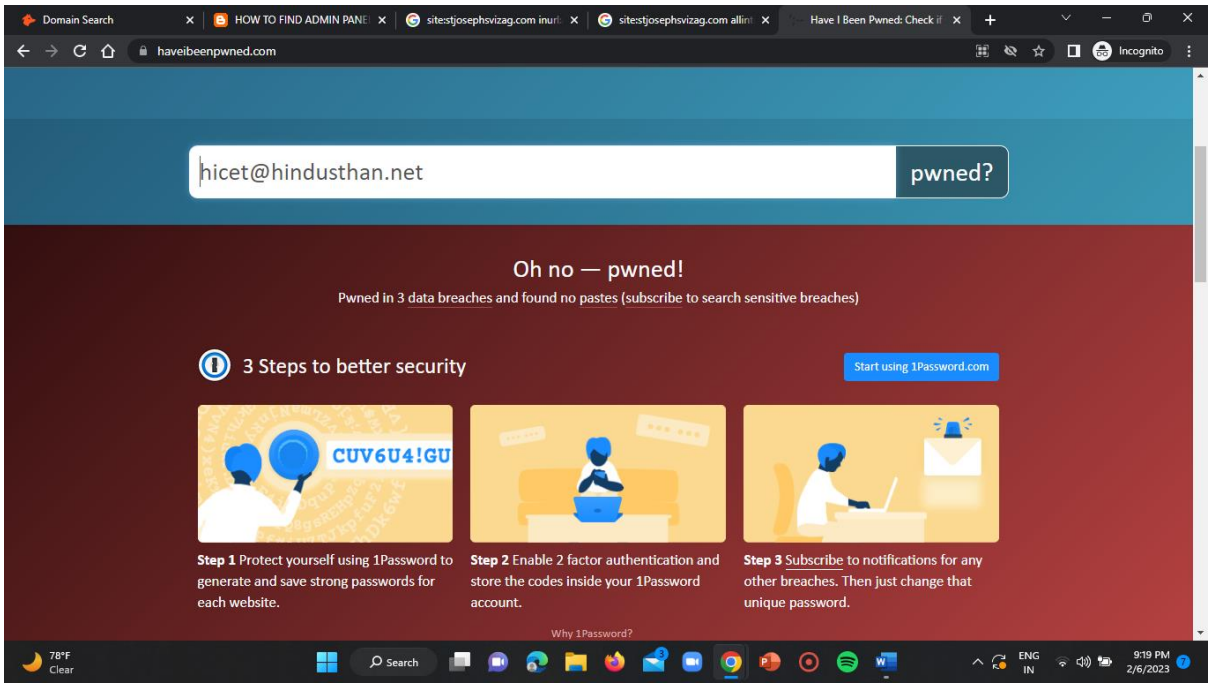


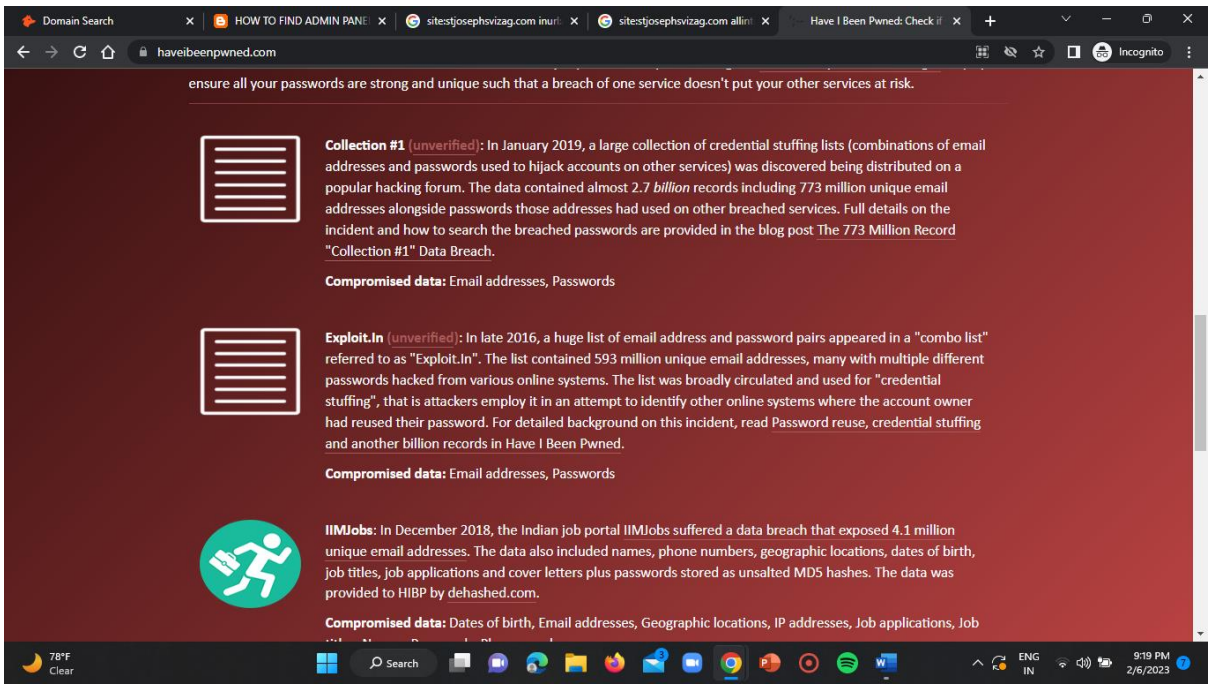
11) info@hindusthan.net



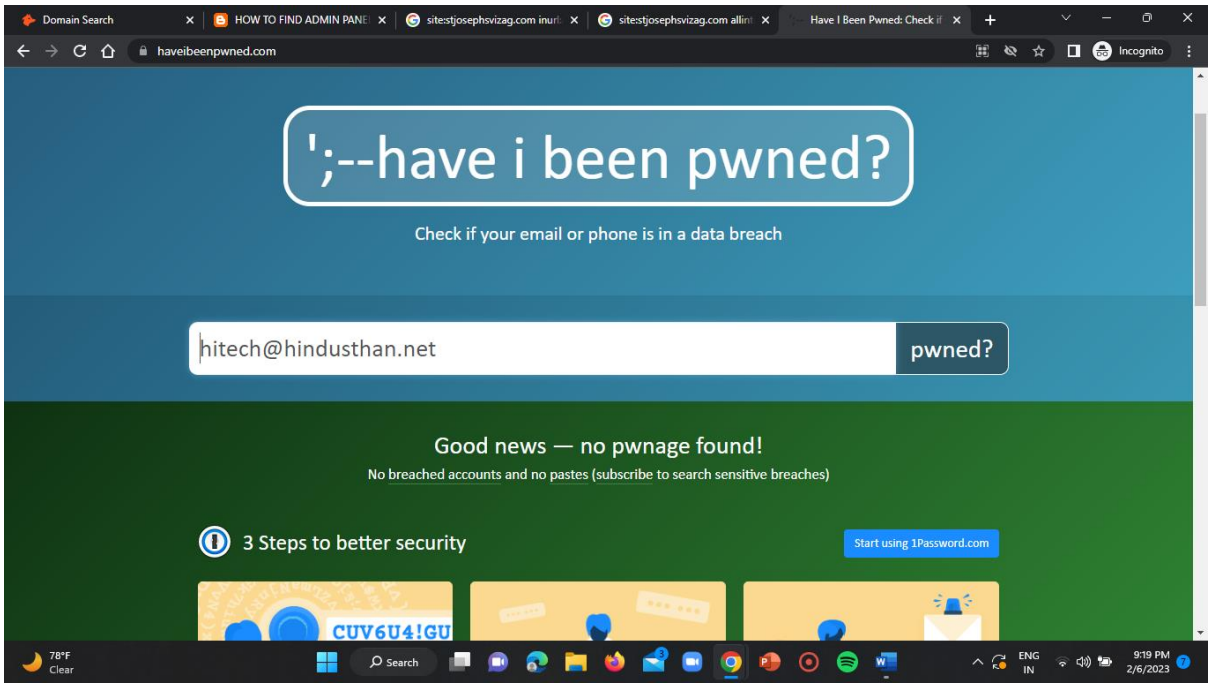


12) hicet@hindusthan.net

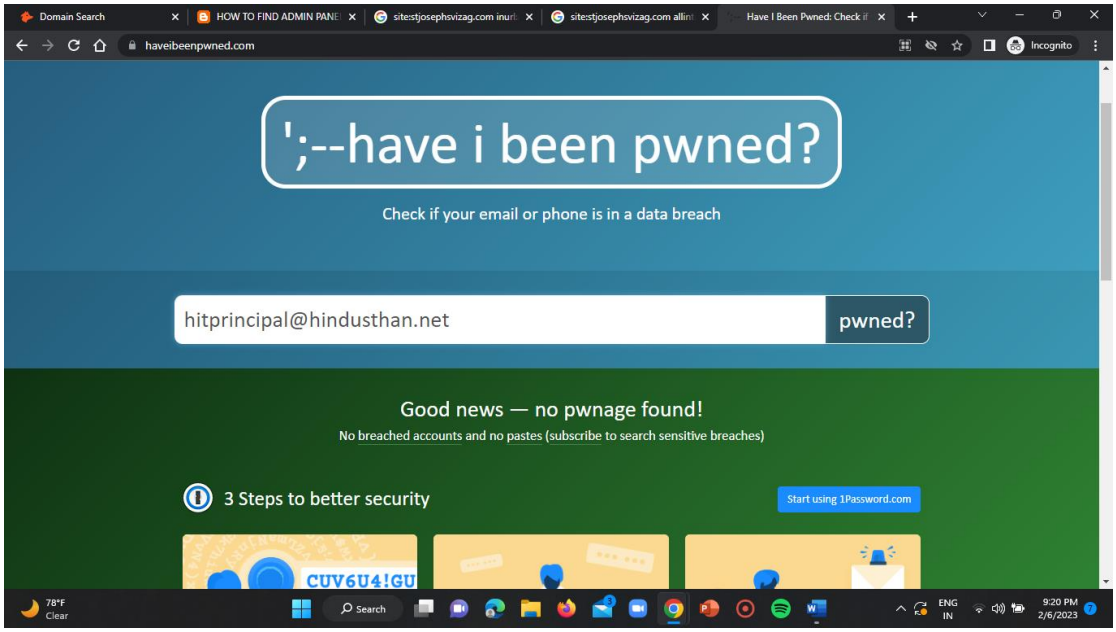




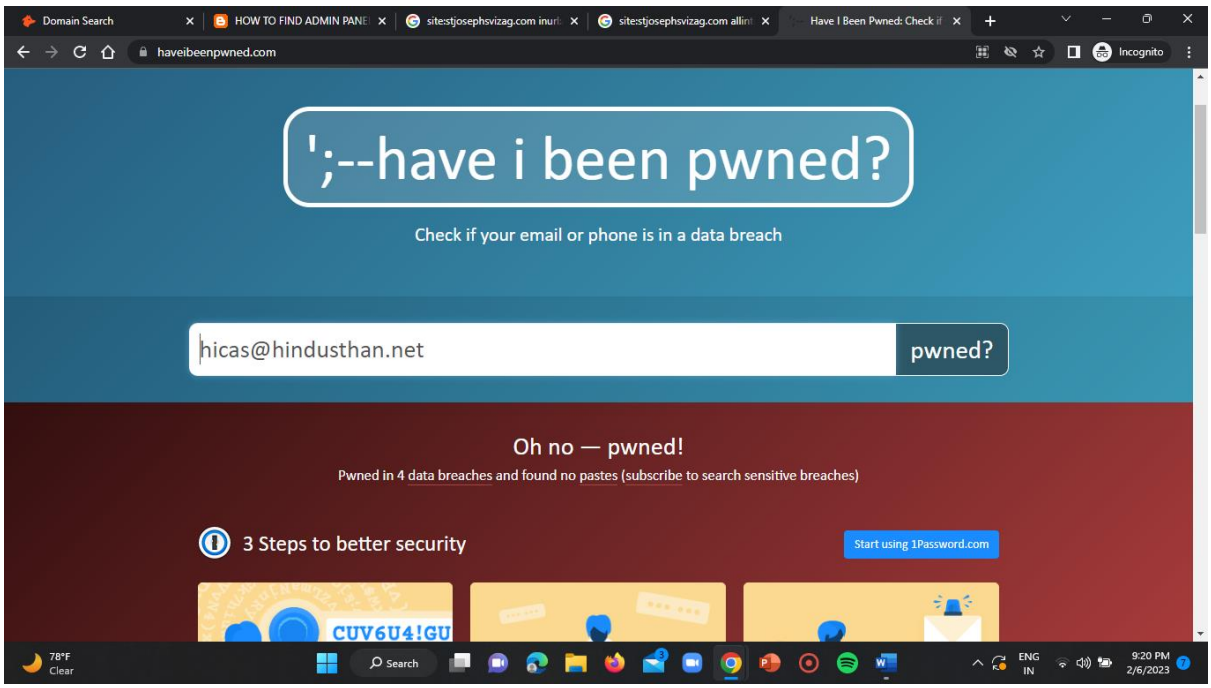
13) hitech@hindusthan.net

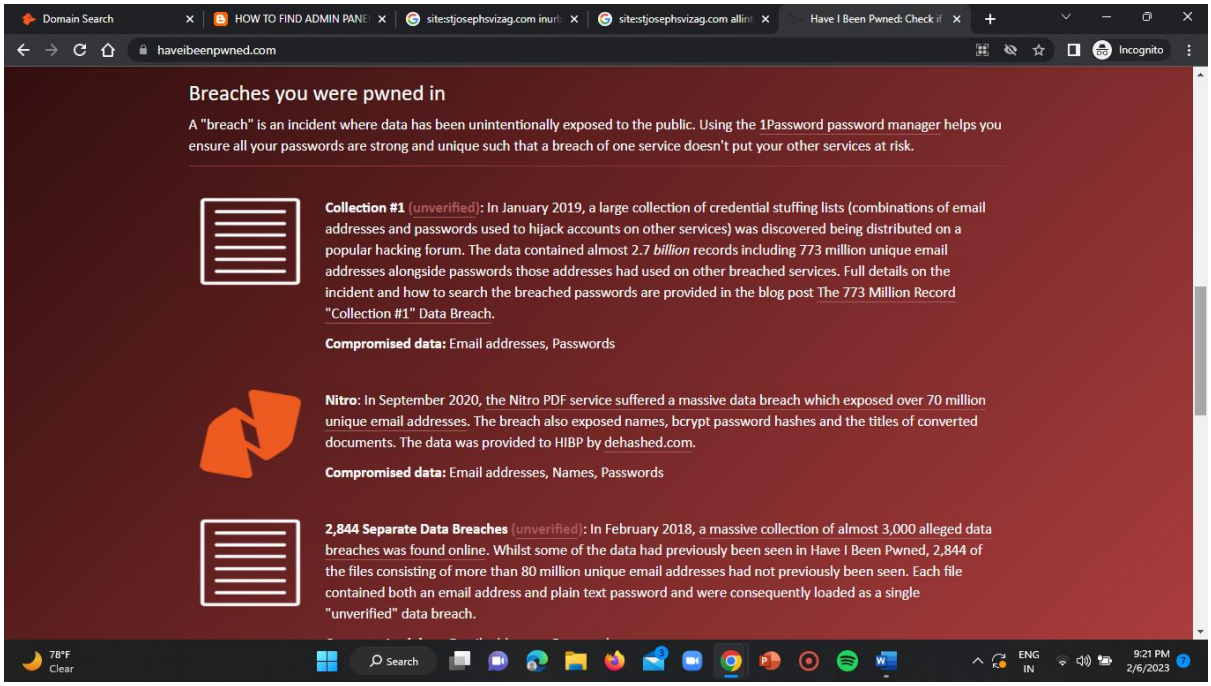


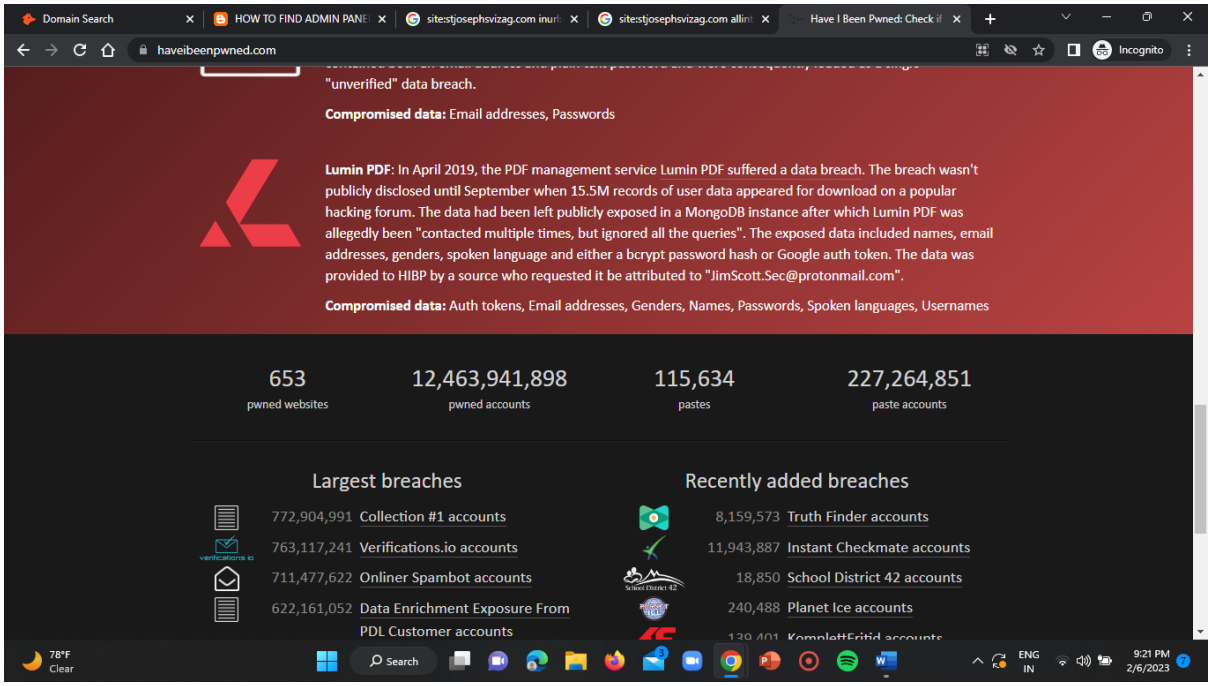
14) hitprincipal@hindusthan.net



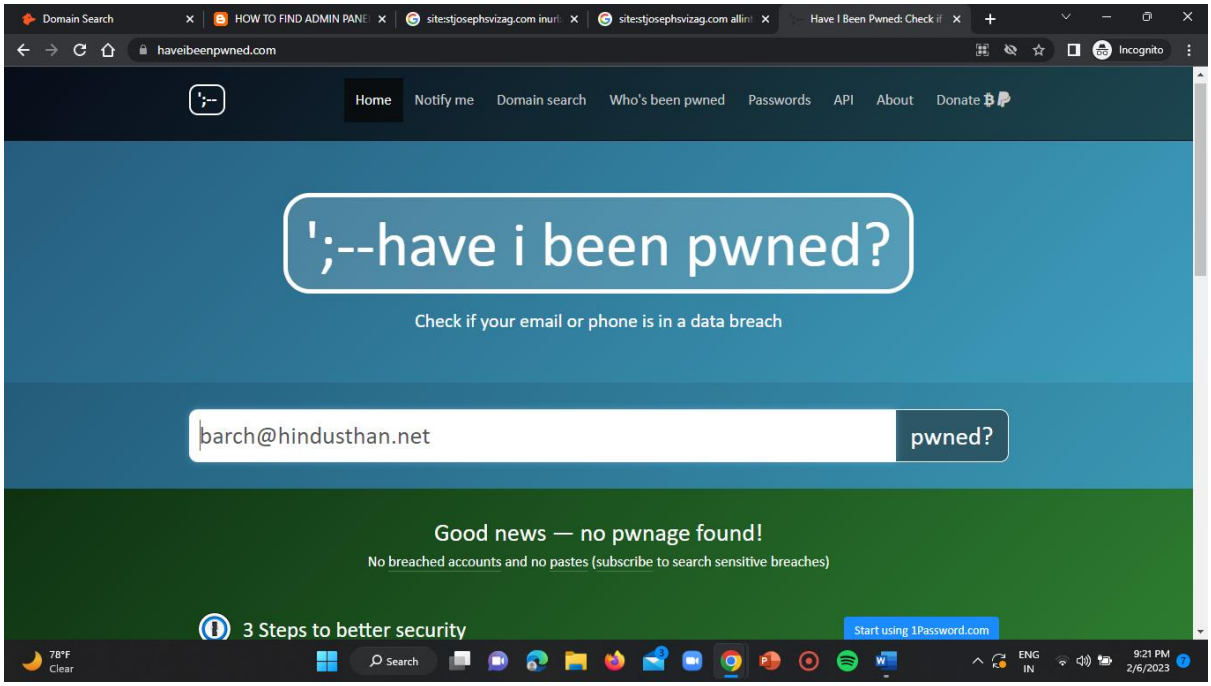
15) hicas@hindusthan.net





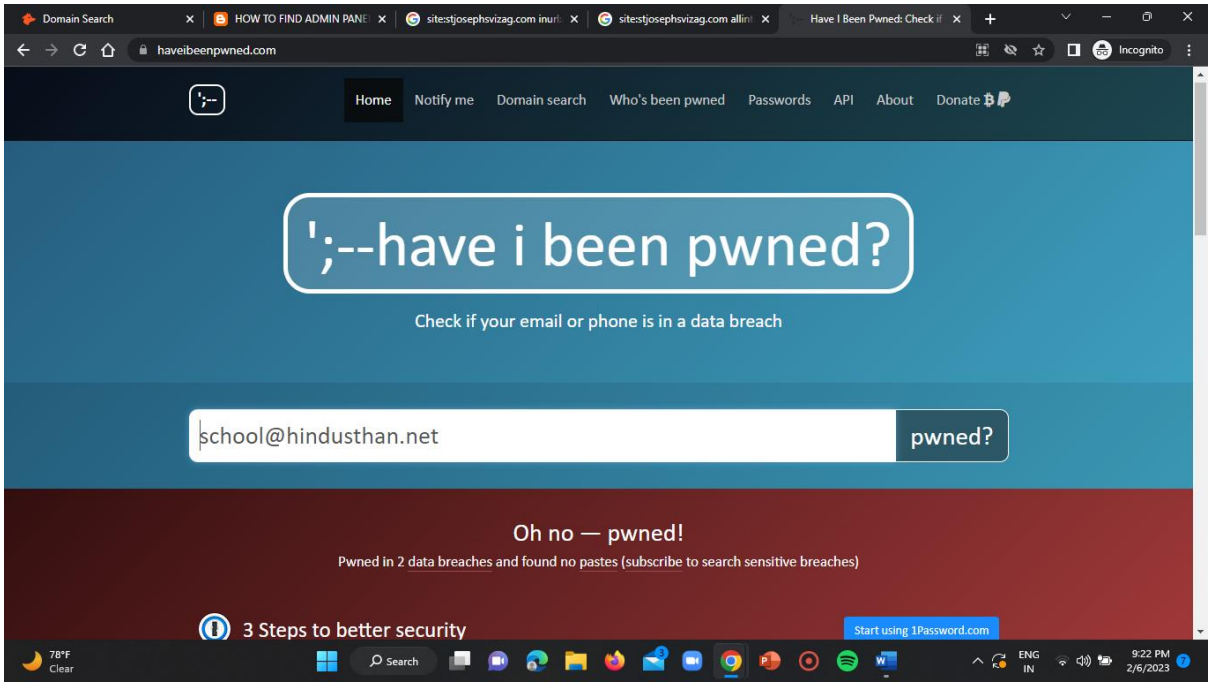


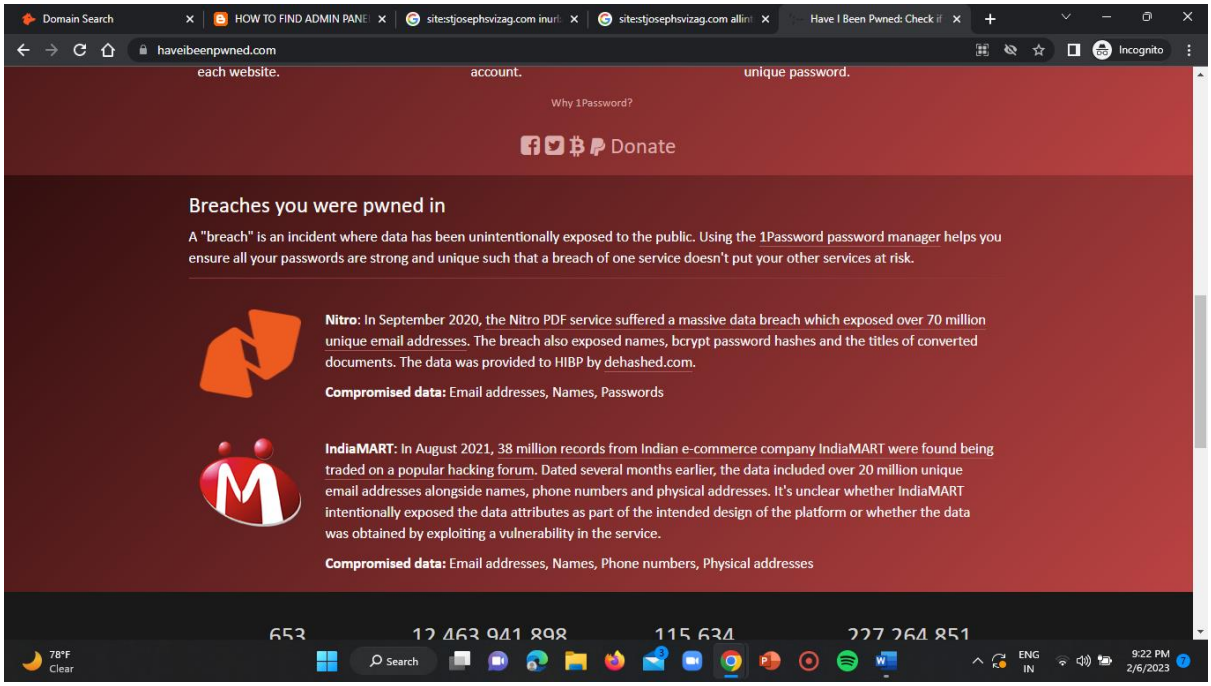
16) barch@hindusthan.net



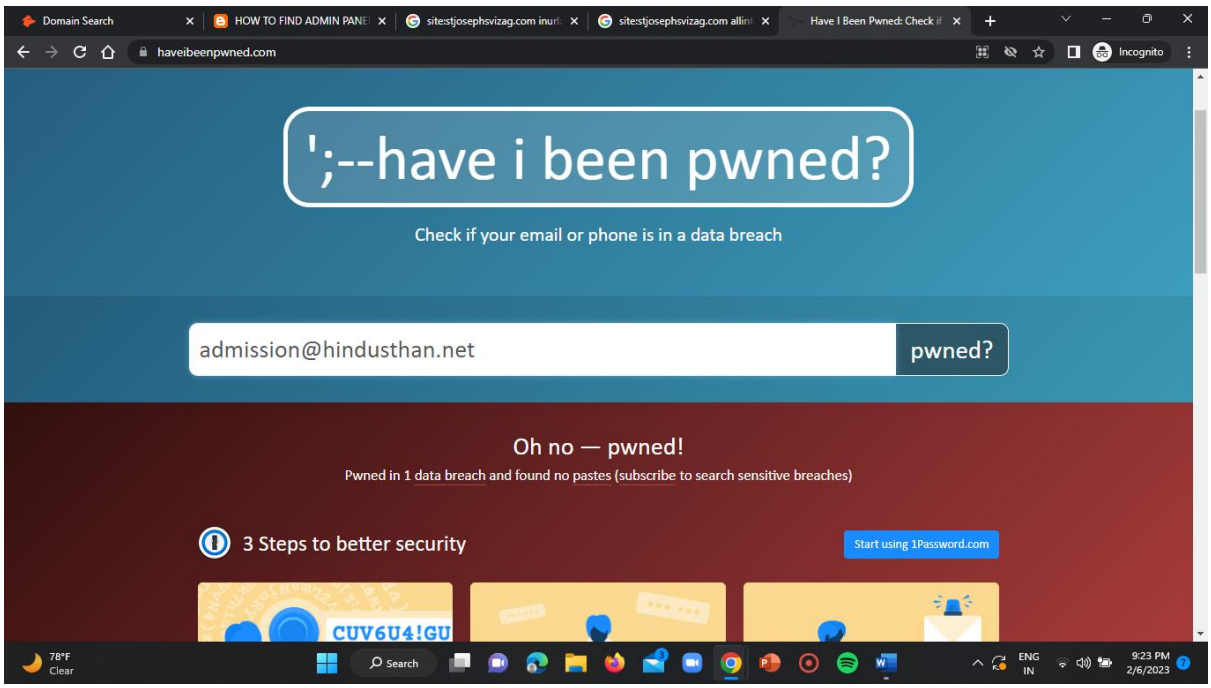
ST#IS#4899

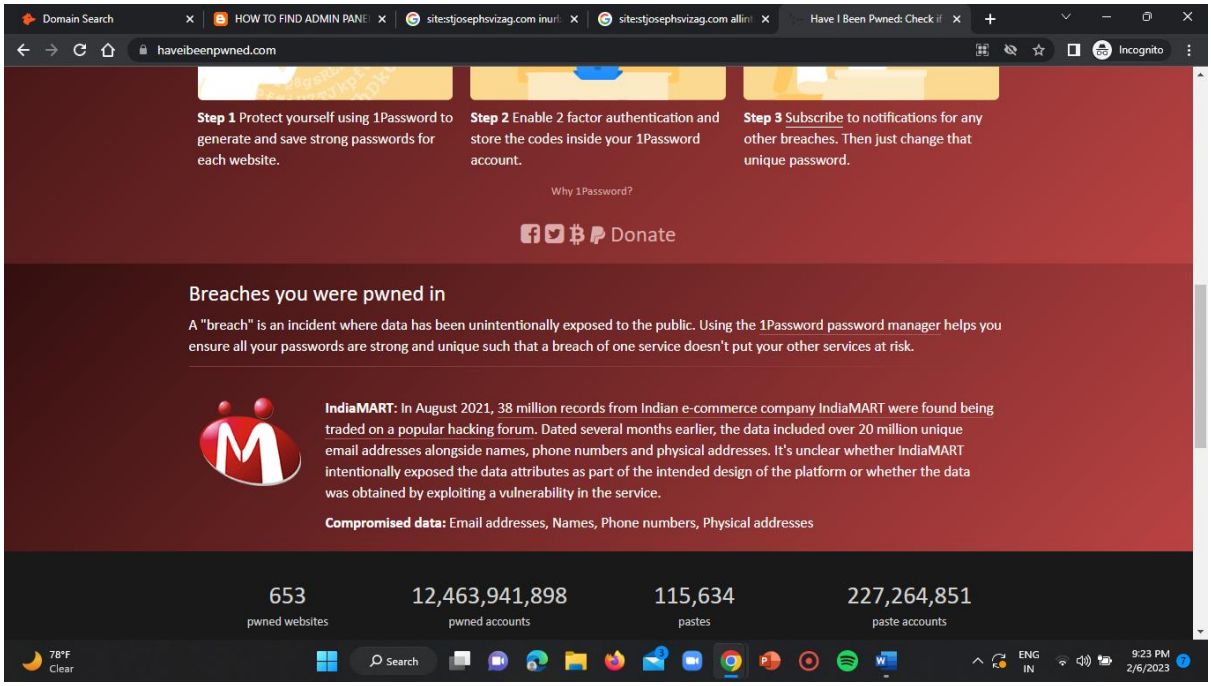
17) school@hindusthan.net



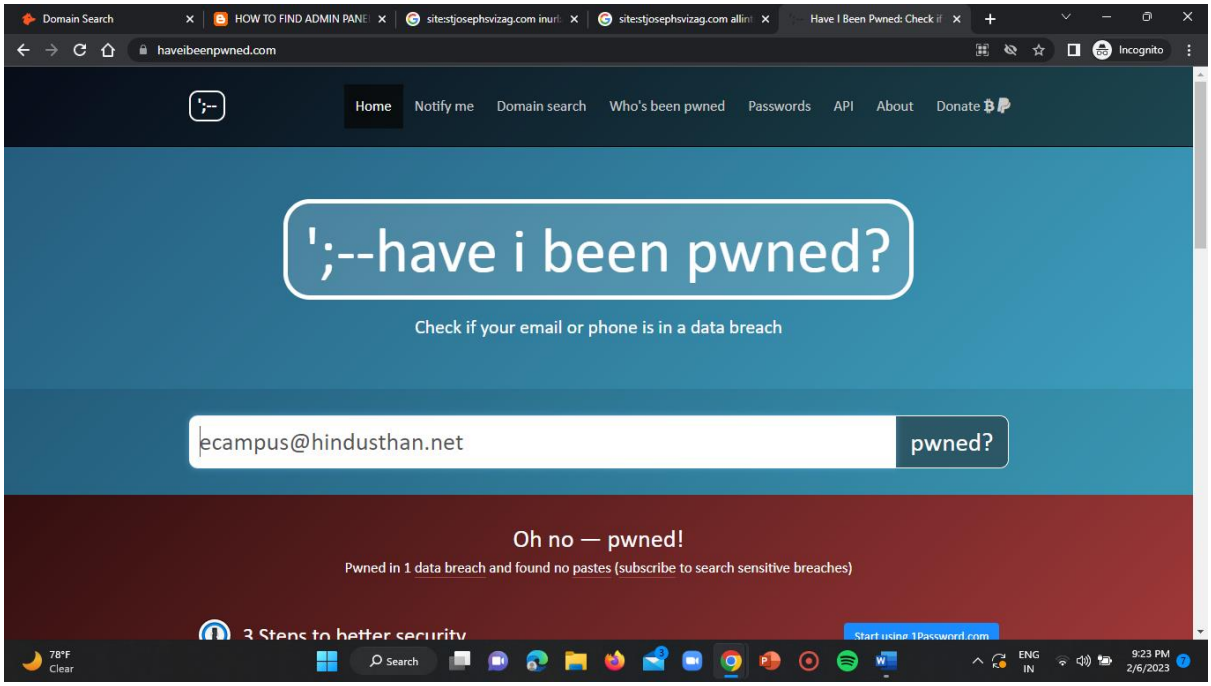


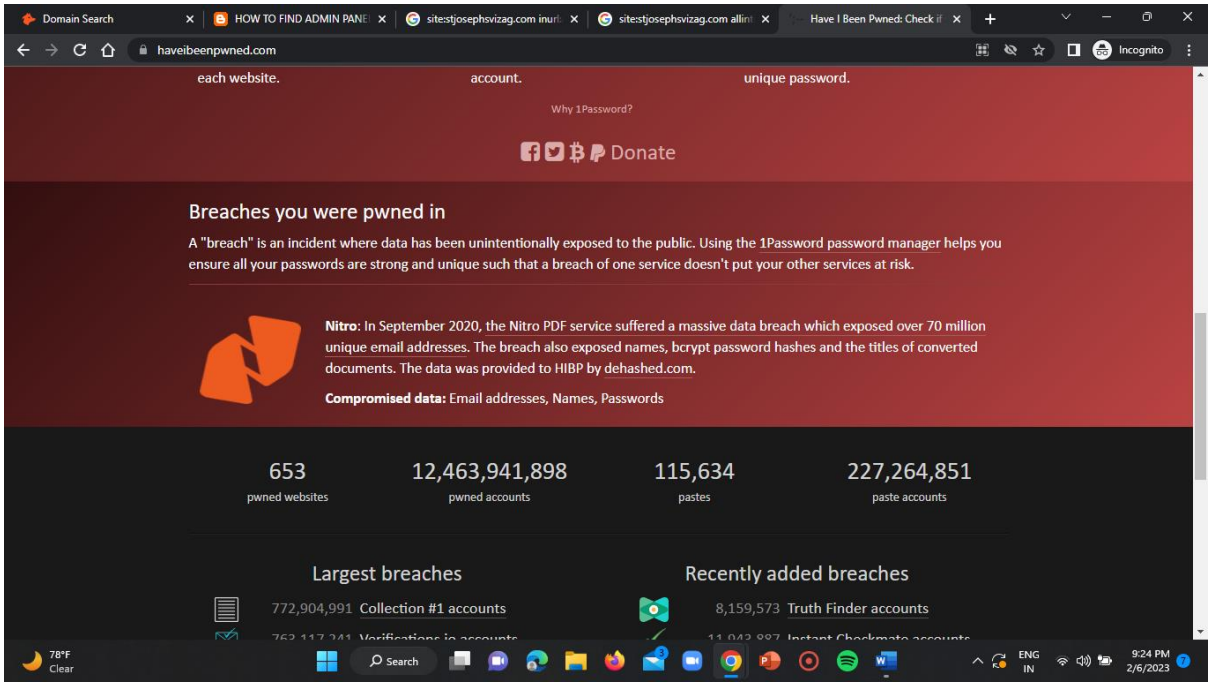
18) admission@hindusthan.net



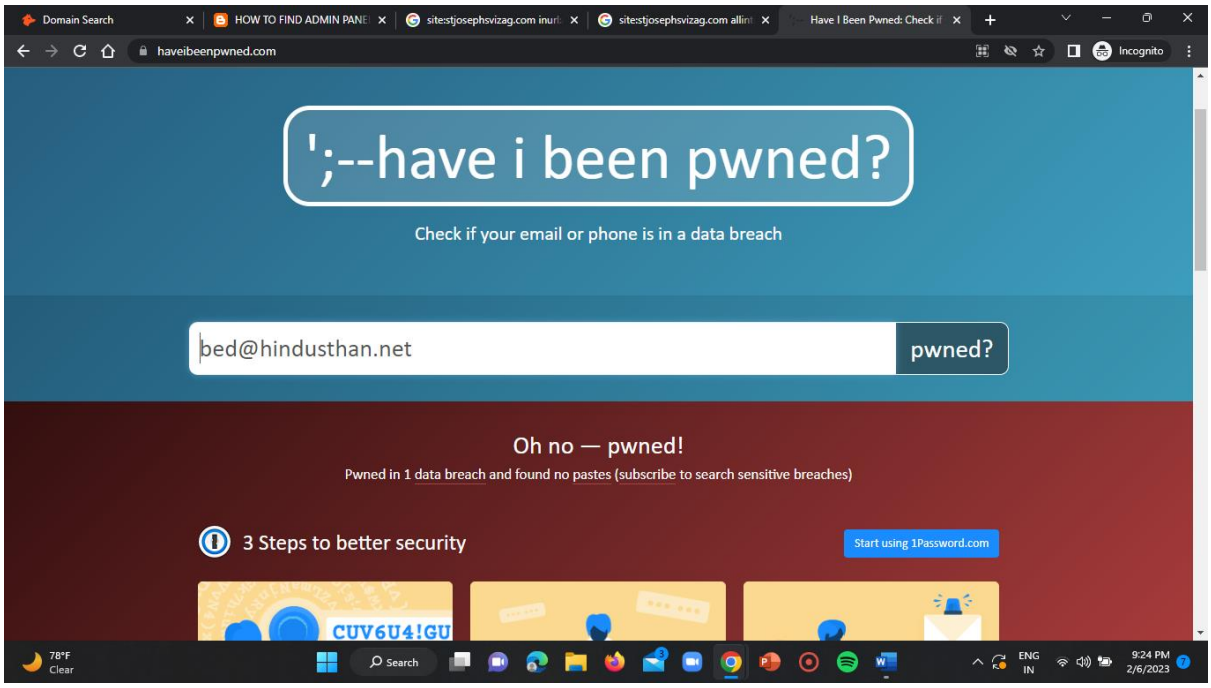


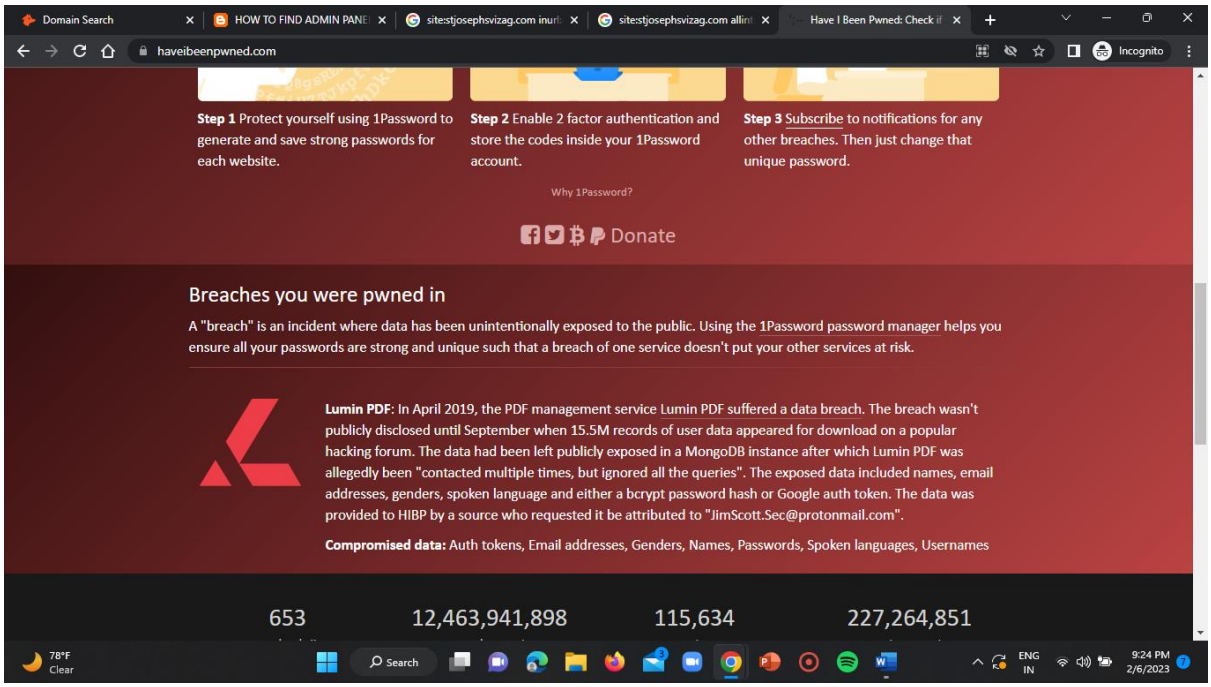
19) ecampus@hindusthan.net



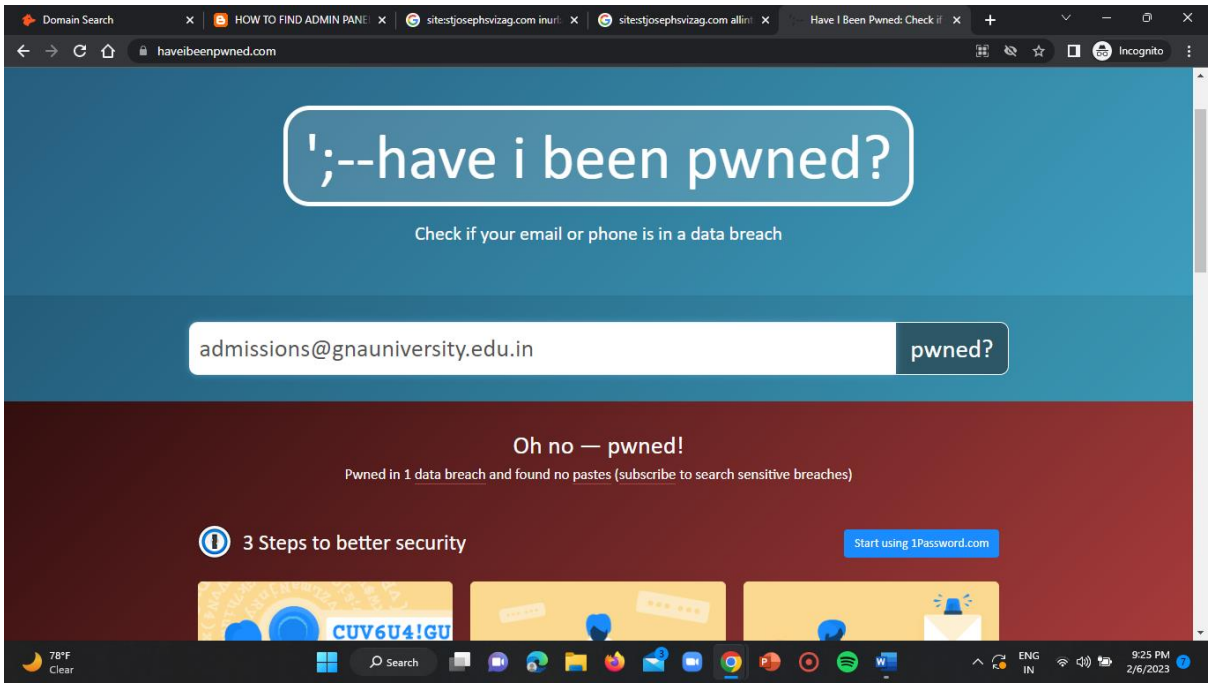


20) bed@hindusthan.net

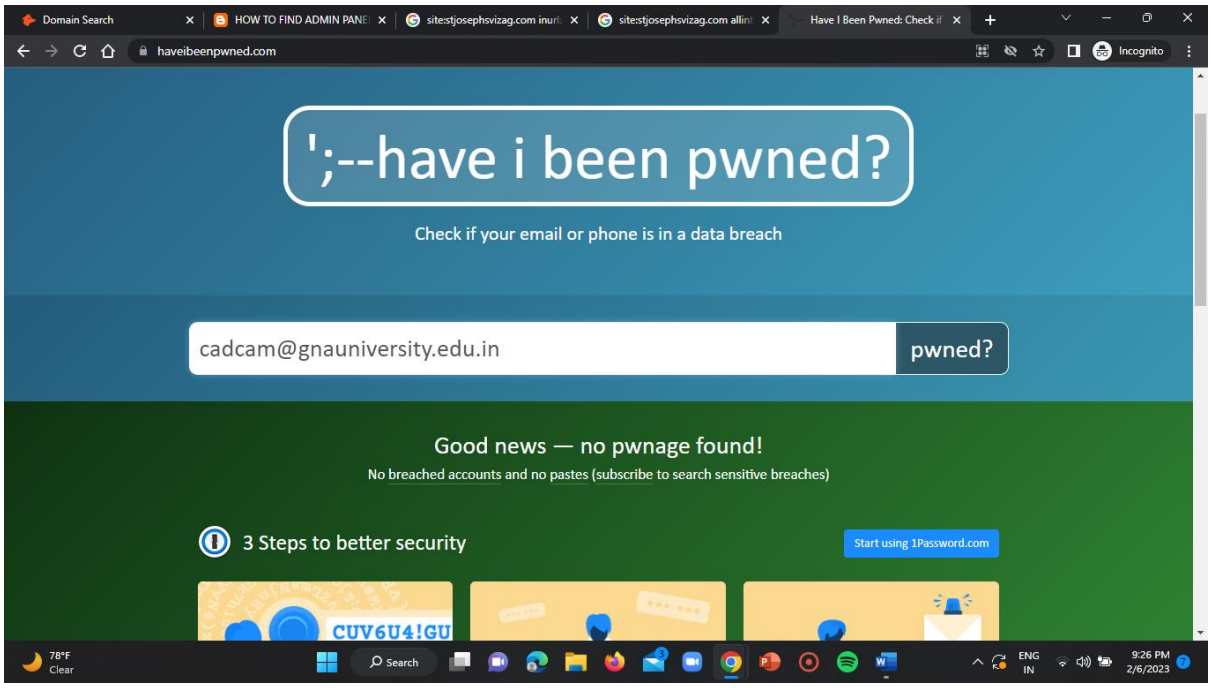




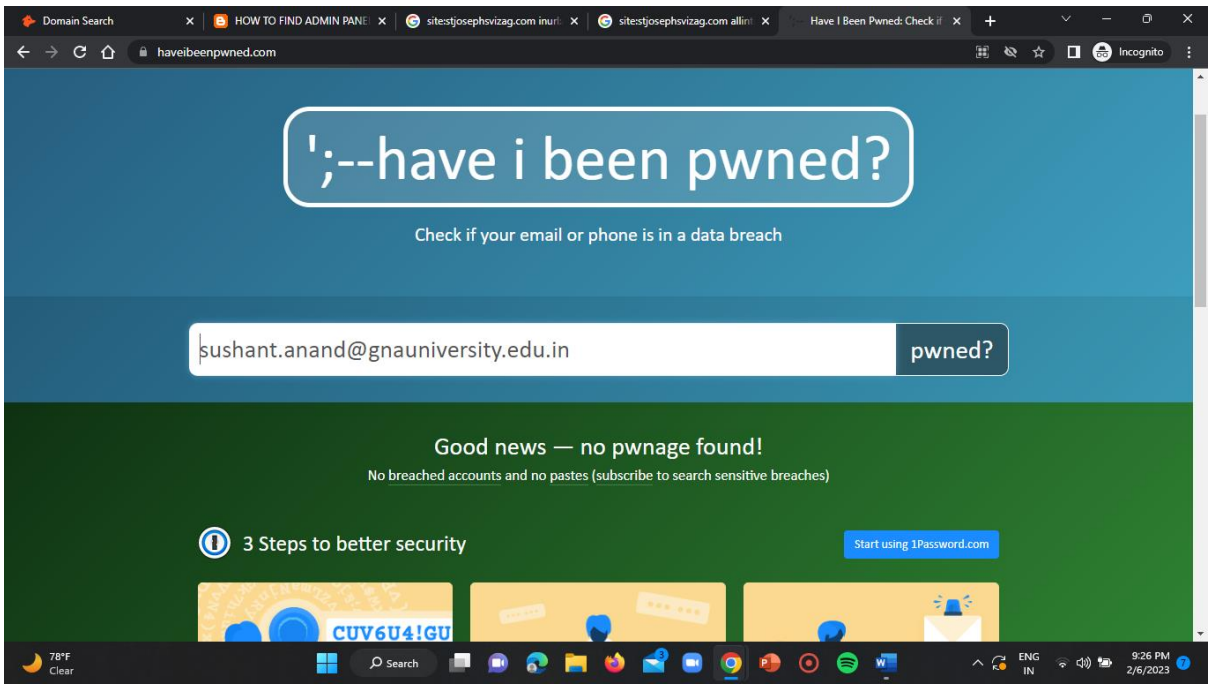
21) admissions@gnauniversity.edu.in



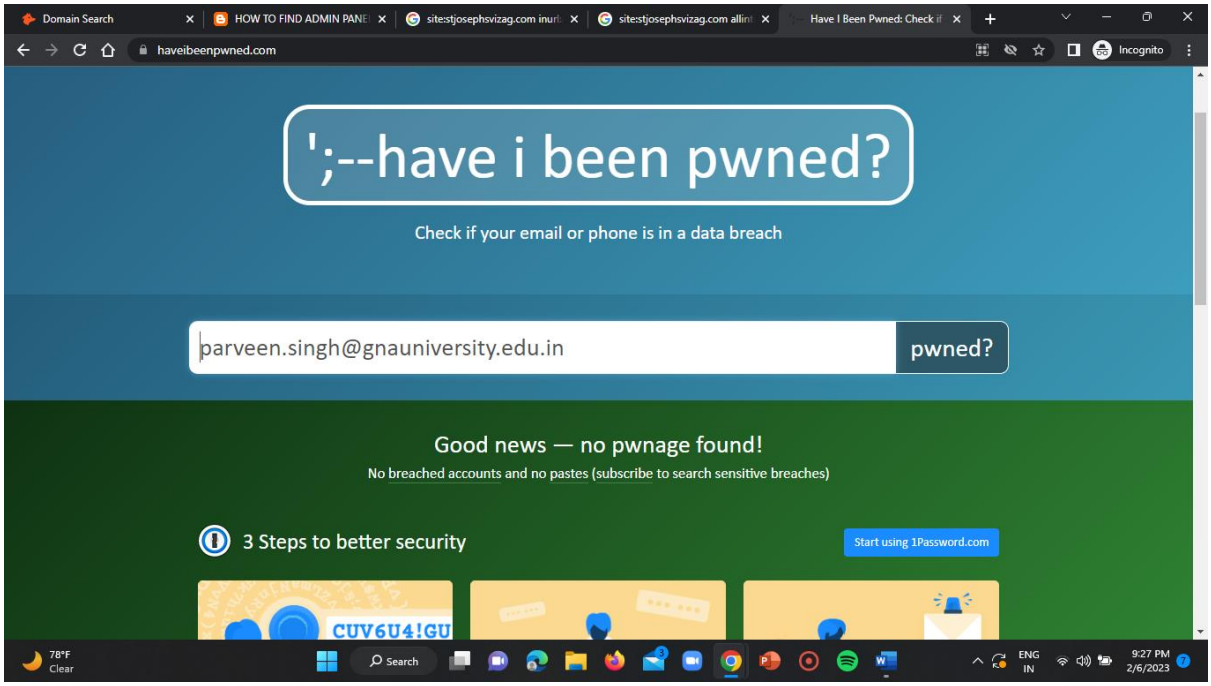
22) cadcam@gnauniversity.edu.in



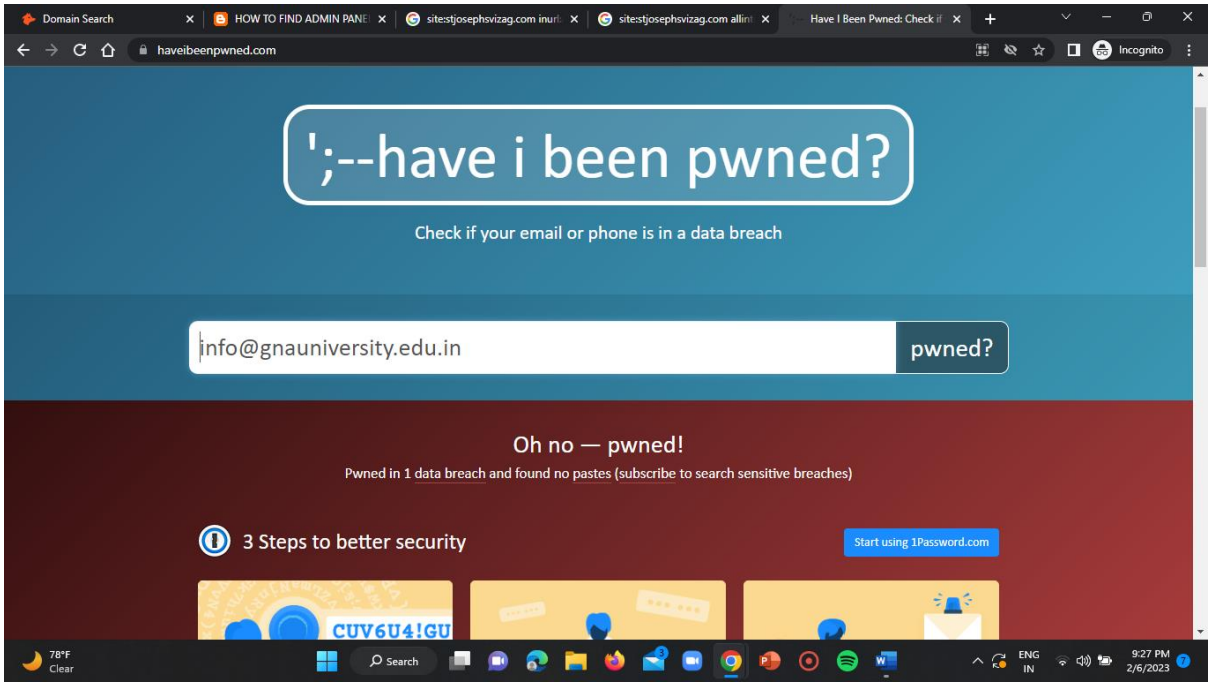
23) sushant.anand@gnauniversity.edu.in

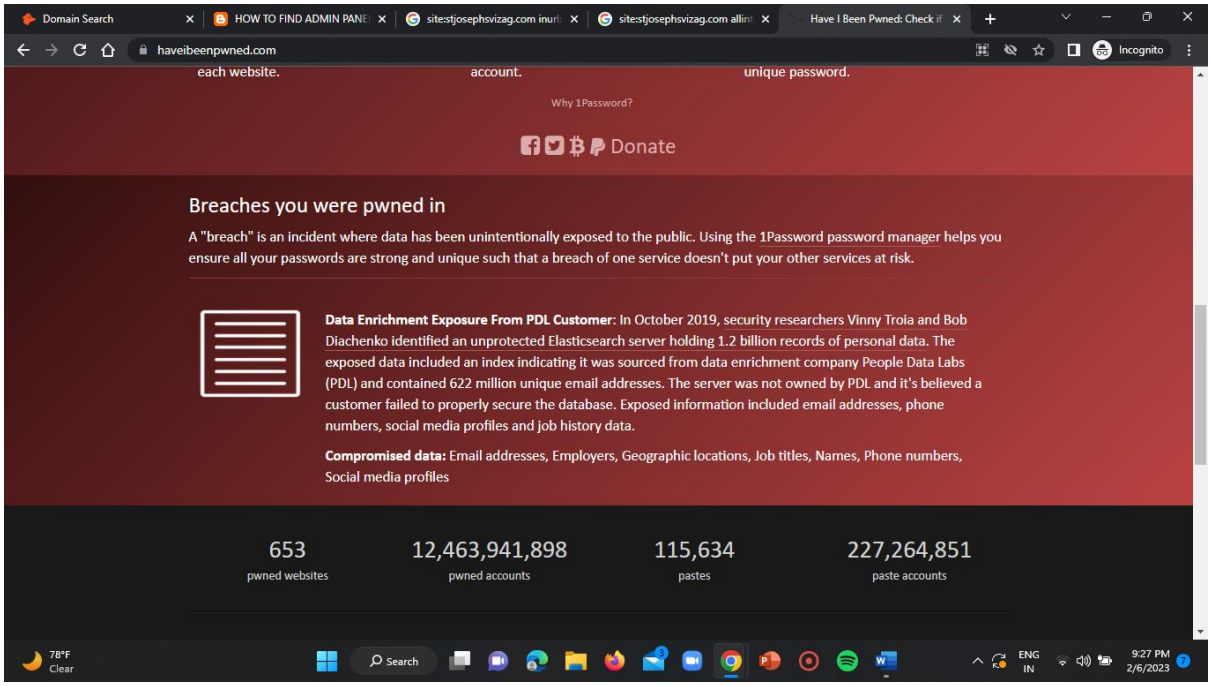


24) parveen.singh@gnauniversity.edu.in

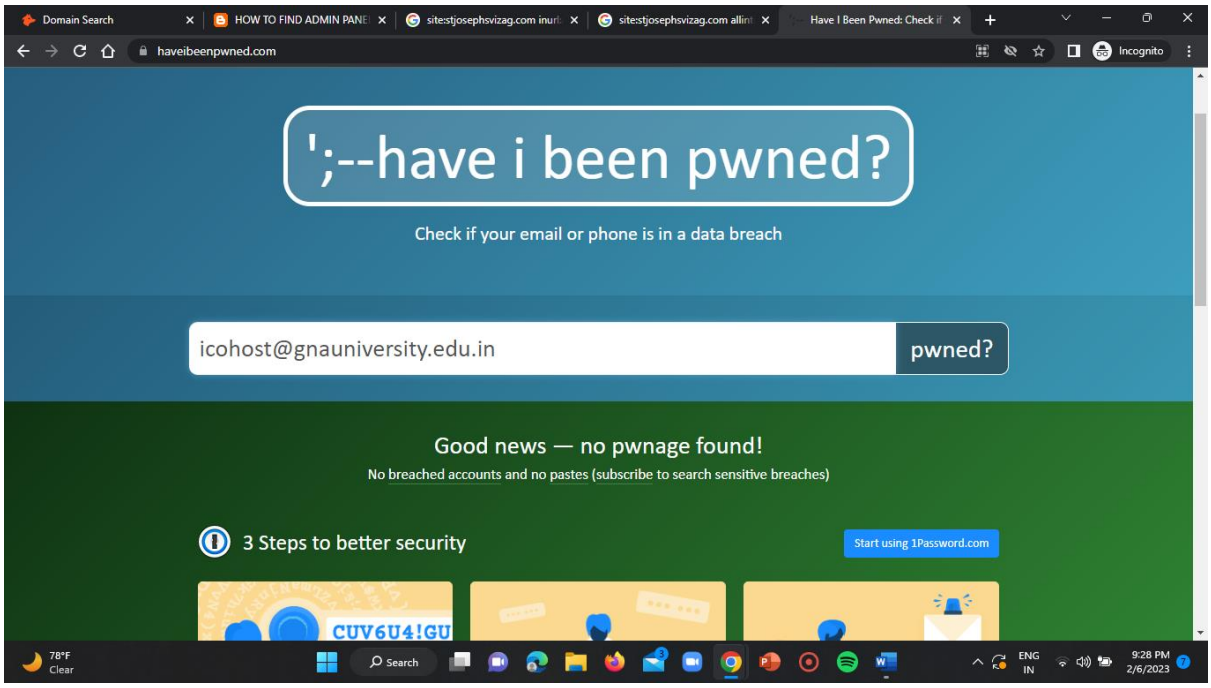


25) info@gnauniversity.edu.in

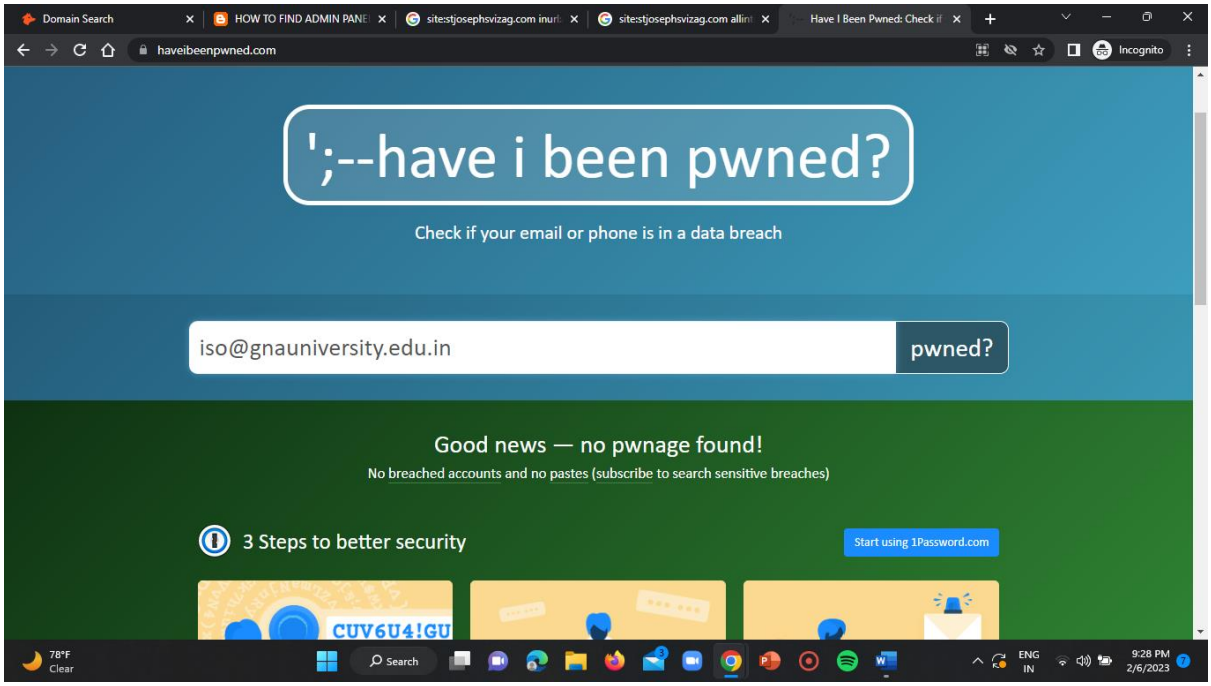




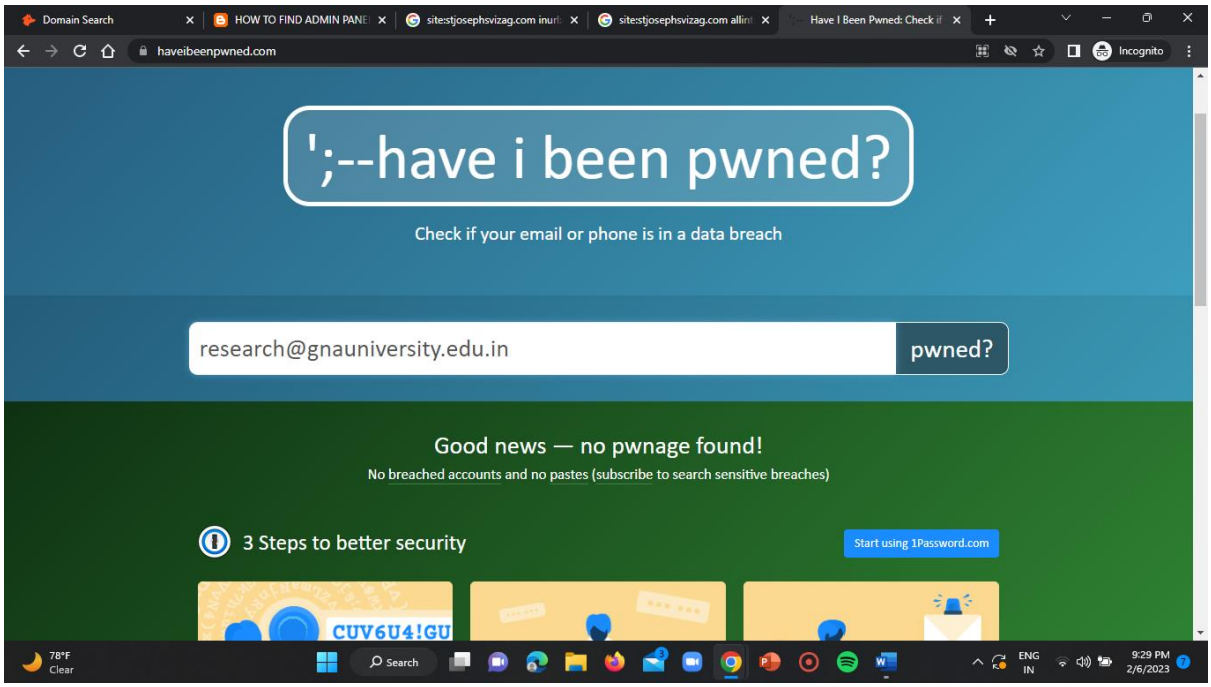
26) icohost@gnauniversity.edu.in



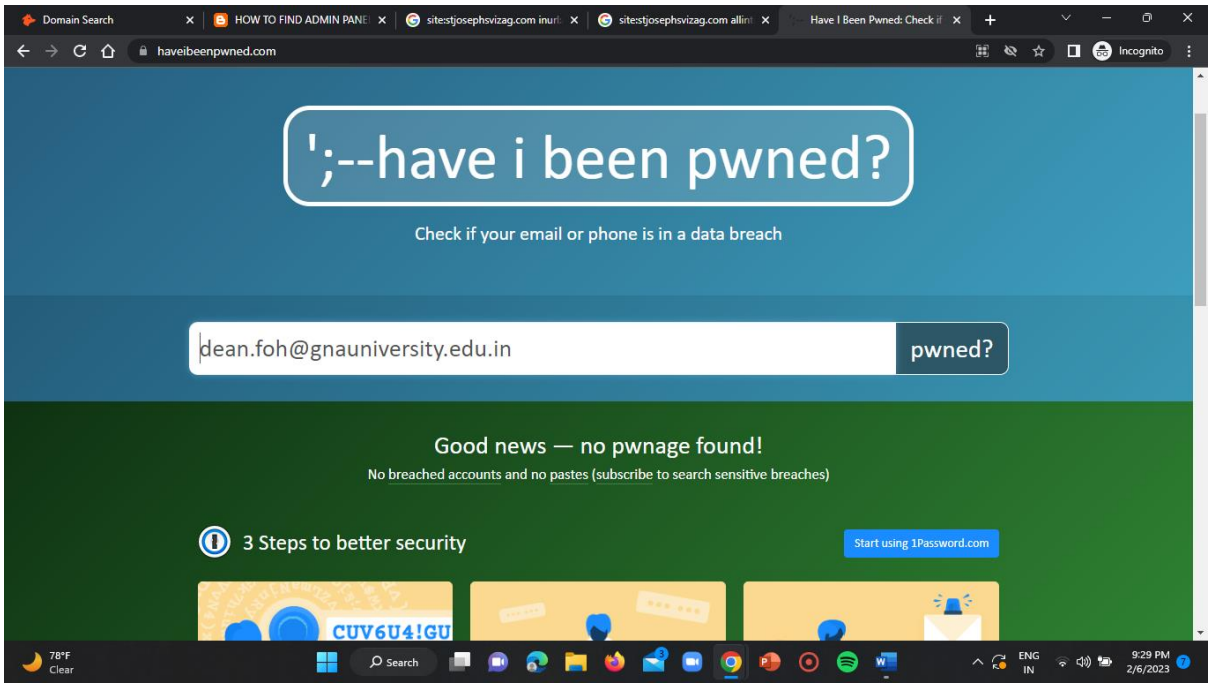
27) iso@gnauniversity.edu.in



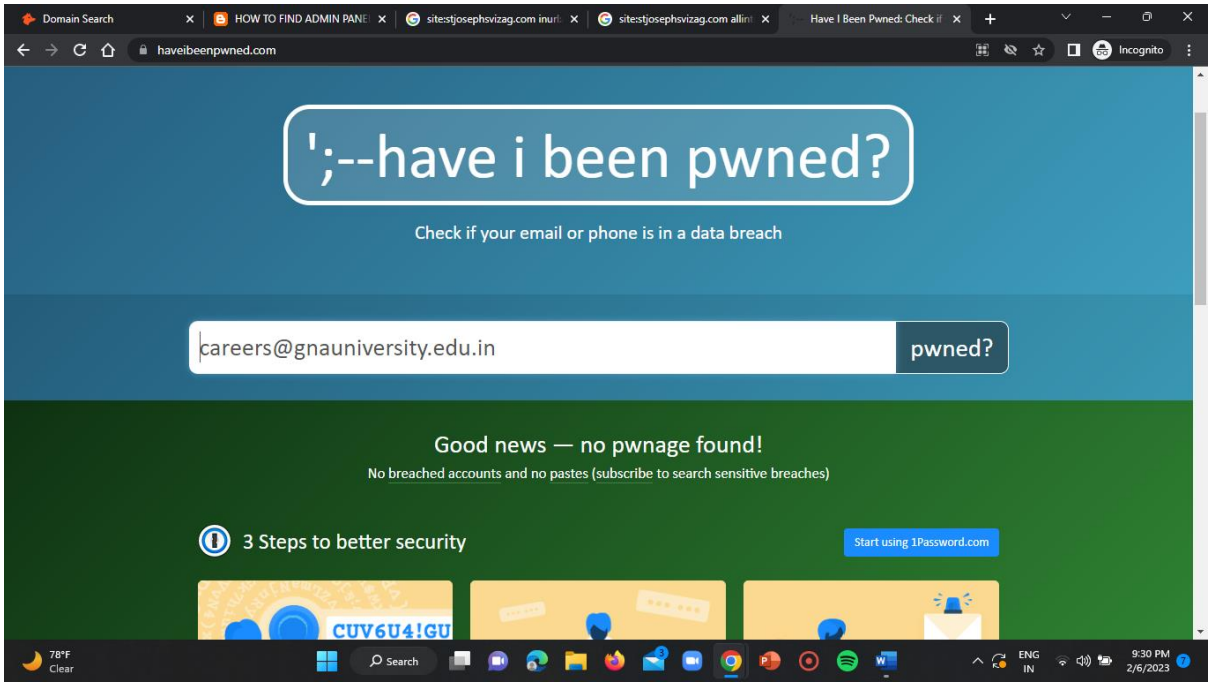
28) research@gnauniversity.edu.in



29) dean.foh@gnauniversity.edu.in



30) careers@gnauniversity.edu.in

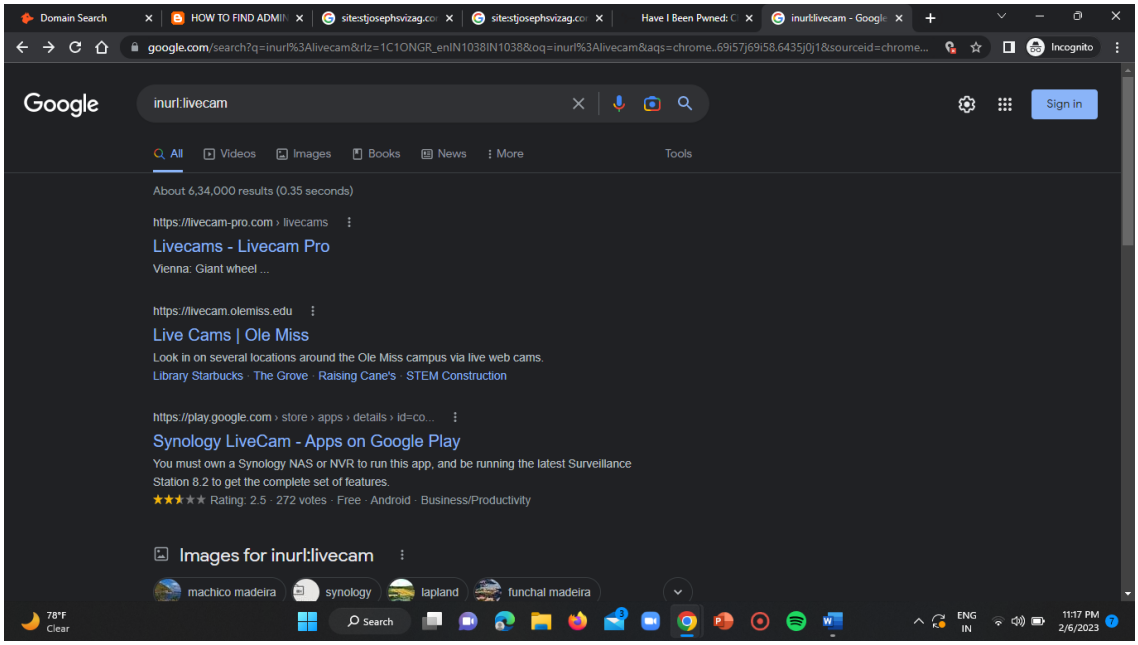


SOLUTION-3 :-

WEB CAMS WHICH ARE CONNECTED IN PUBLIC NETWORK AND WHICH ARE ALSO FROM A SINGLE COUNTRY:

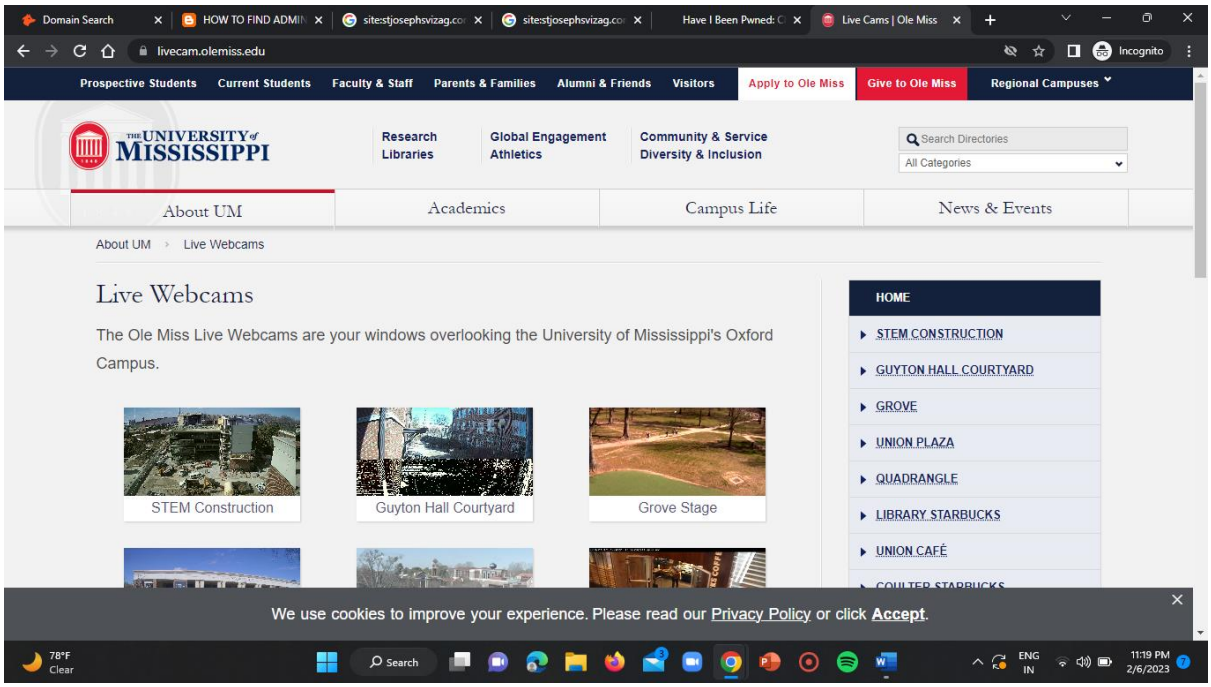
Step-1:

Open the incognito chrome window in your web browser and use the google dork “inurl:livecam” and enter it in the search input bar of the homepage.



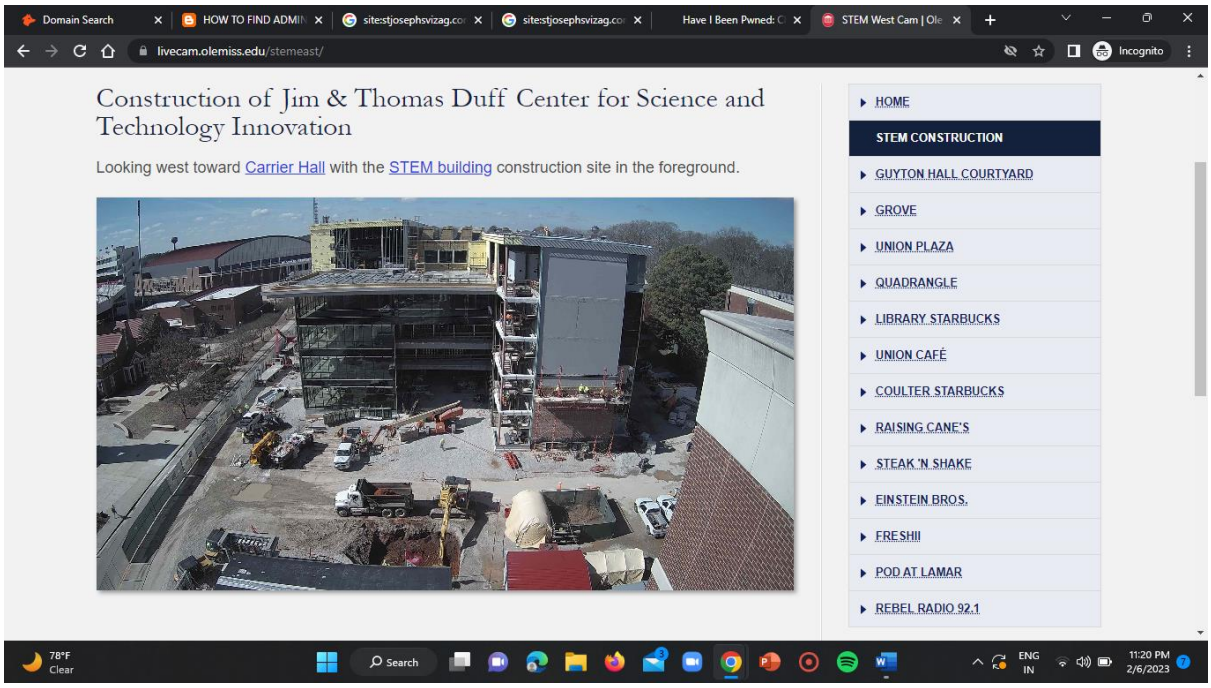
Step-2:

Open the second blue link mentioning as “Live Cams | Ole Miss” then you get displayed all the publicly available live streaming cams.



CAM-1:

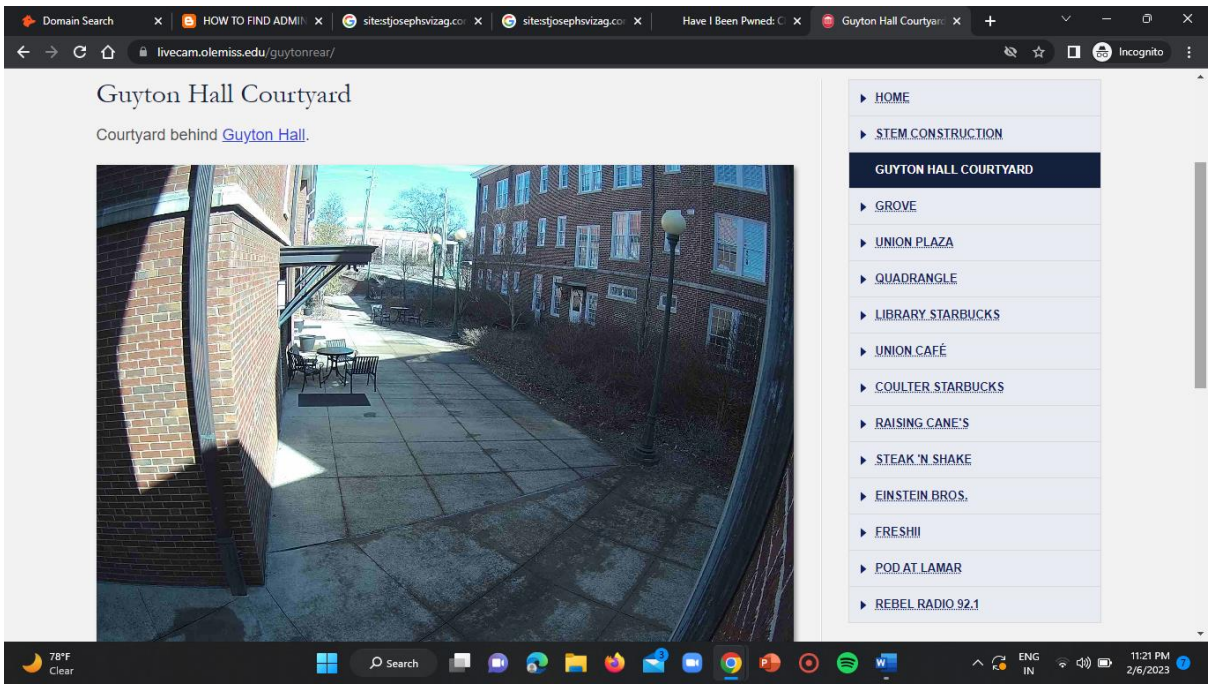
LINK = https://livecam.olemiss.edu/stemeast/



ST#IS#4899

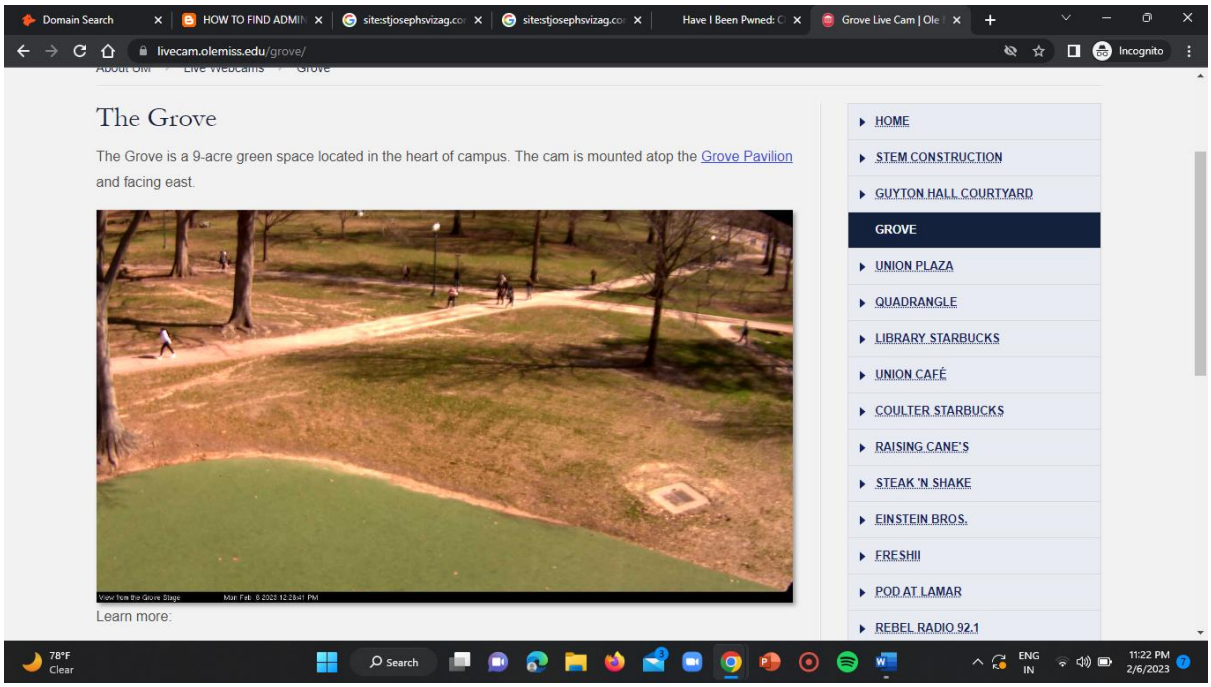
CAM-2:

LINK = https://livecam.olemiss.edu/guytonrear/



CAM-3:

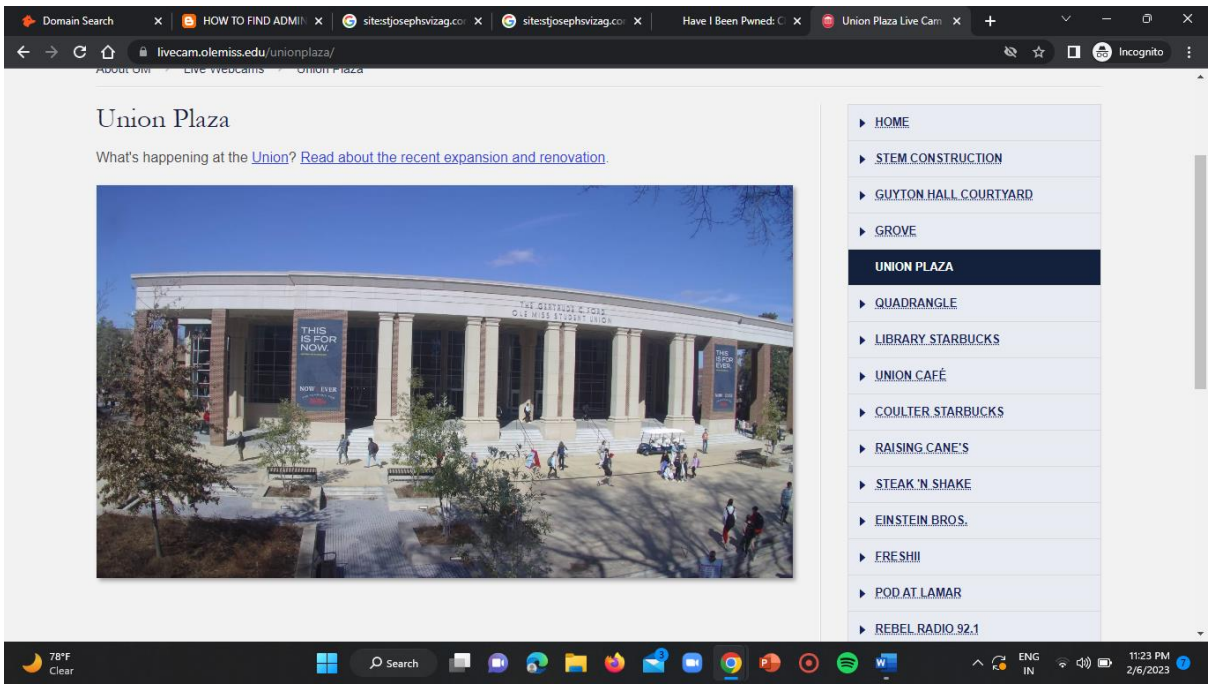
LINK = https://livecam.olemiss.edu/grove/



ST#IS#4899

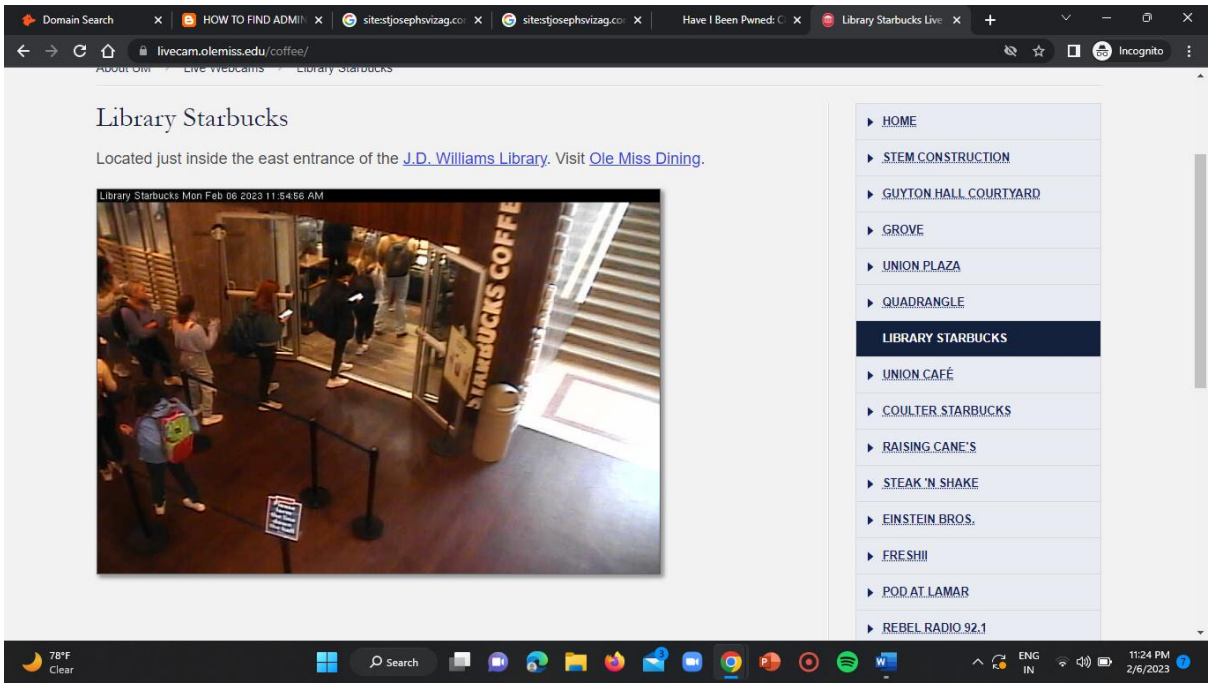
CAM-4:

LINK = https://livecam.olemiss.edu/unionplaza/



CAM-5:

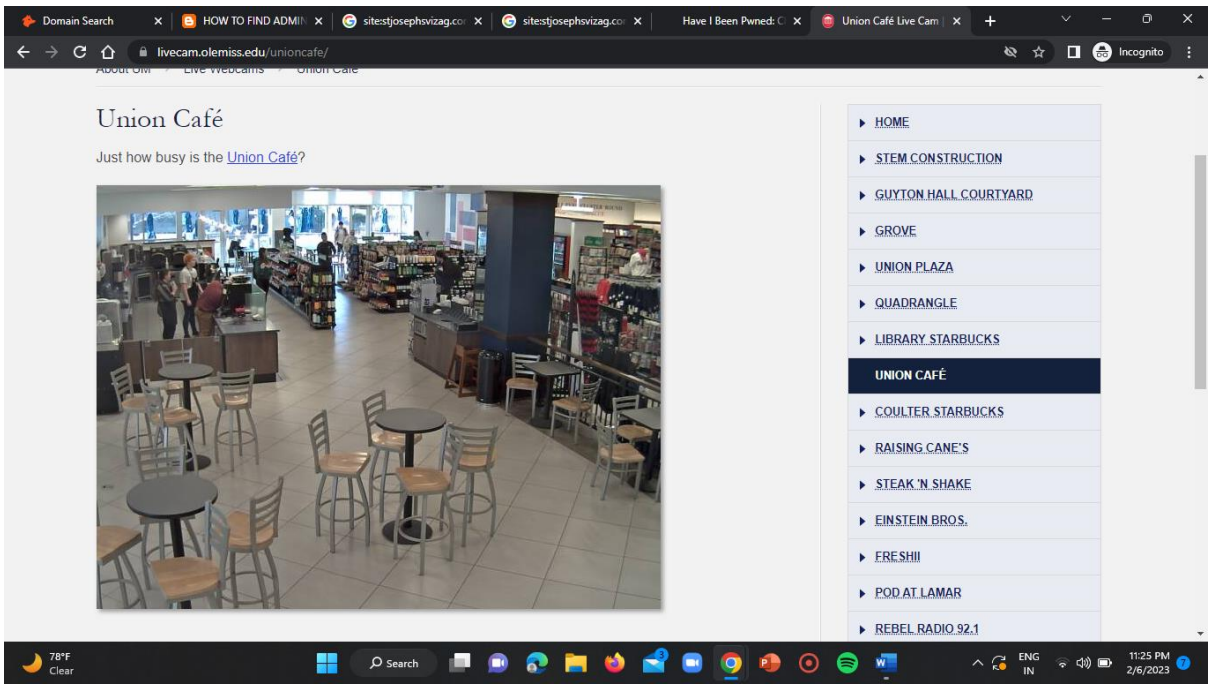
LINK = https://livecam.olemiss.edu/coffee/



ST#IS#4899

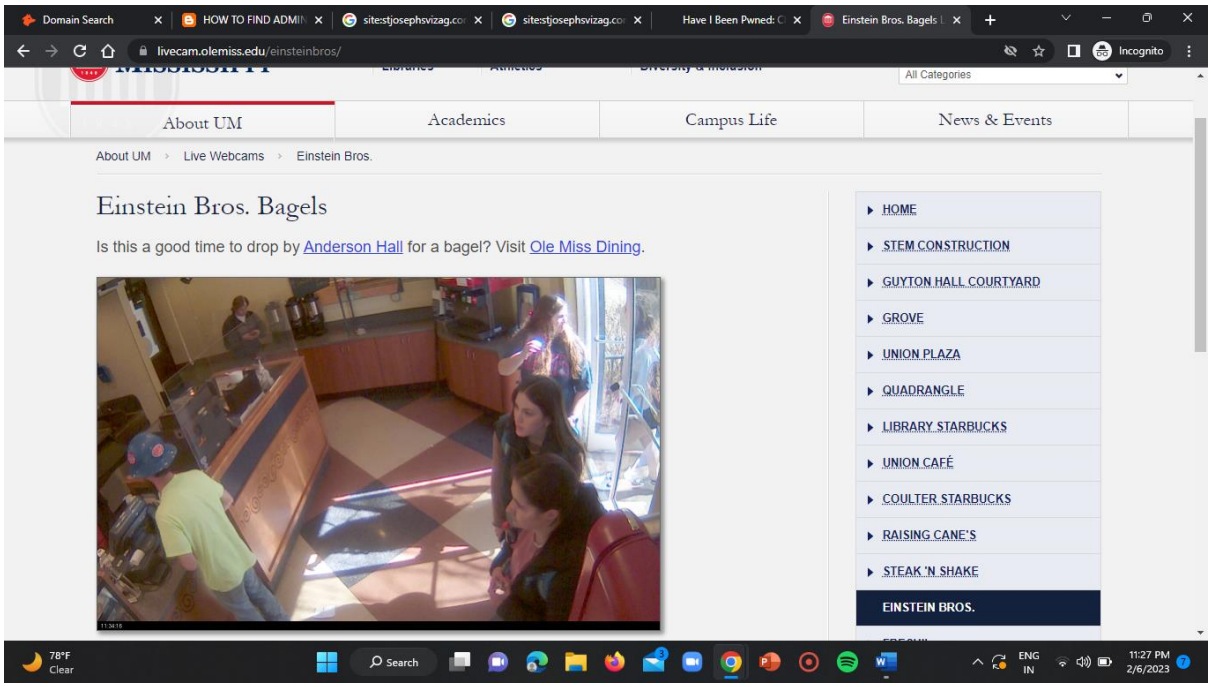
CAM-6:

LINK = https://livecam.olemiss.edu/unioncafe/



CAM-7:

LINK = https://livecam.olemiss.edu/einsteinbros/



CONCLUSION:-

So finally in this task segment we found the admin login pages of the given websites using footprinting technique. And we also gathered the 10 email addresses associated with any three of the given target domains and also we checked for the data breaches for all the emails we found in those domains. The last section of our task is about finding 7 webcams which are publicly available and connected to open networks and are live streaming and we successfully found then using the footprinting technique.