

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 attack 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.

TECHNICAL PROCEDURE :-

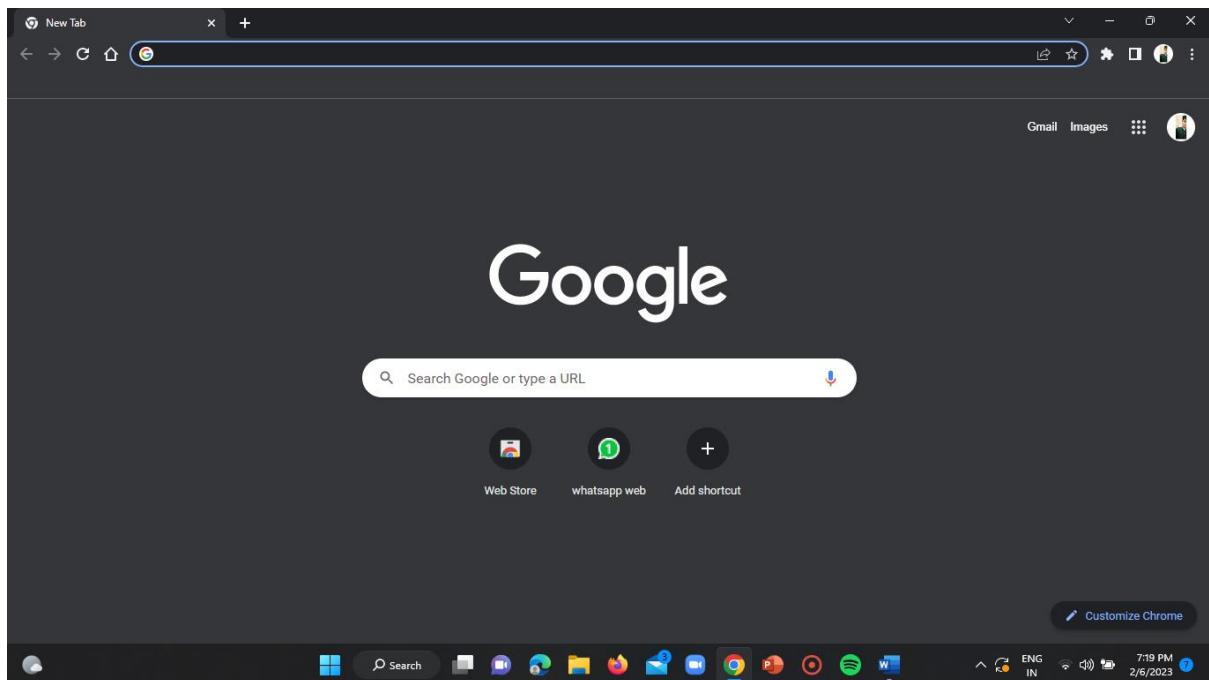
SOLUTION-1 :-

ADMIN LOGIN PAGES :-

TOOL USED:- “ GOOGLE DORKS ”

Step-1:

Open google chrome.

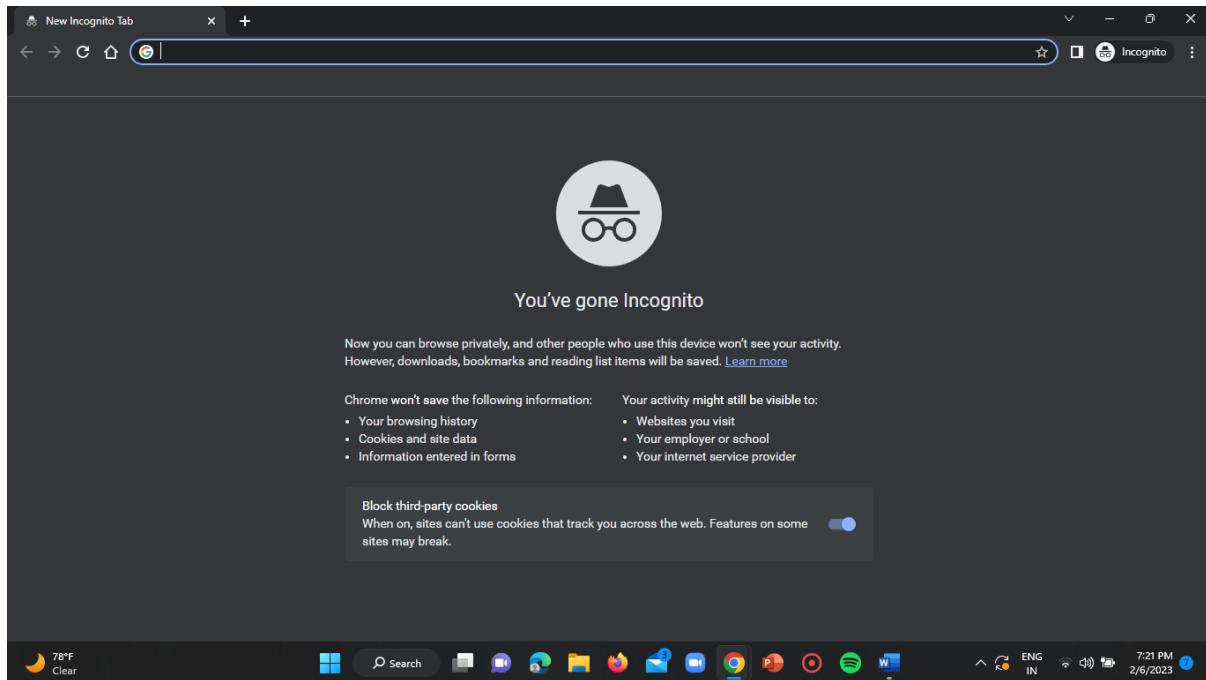


Step-2:

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

SHORTCUT = “ ctrl+shift+n ”

ST#IS#4899



Step-3:

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

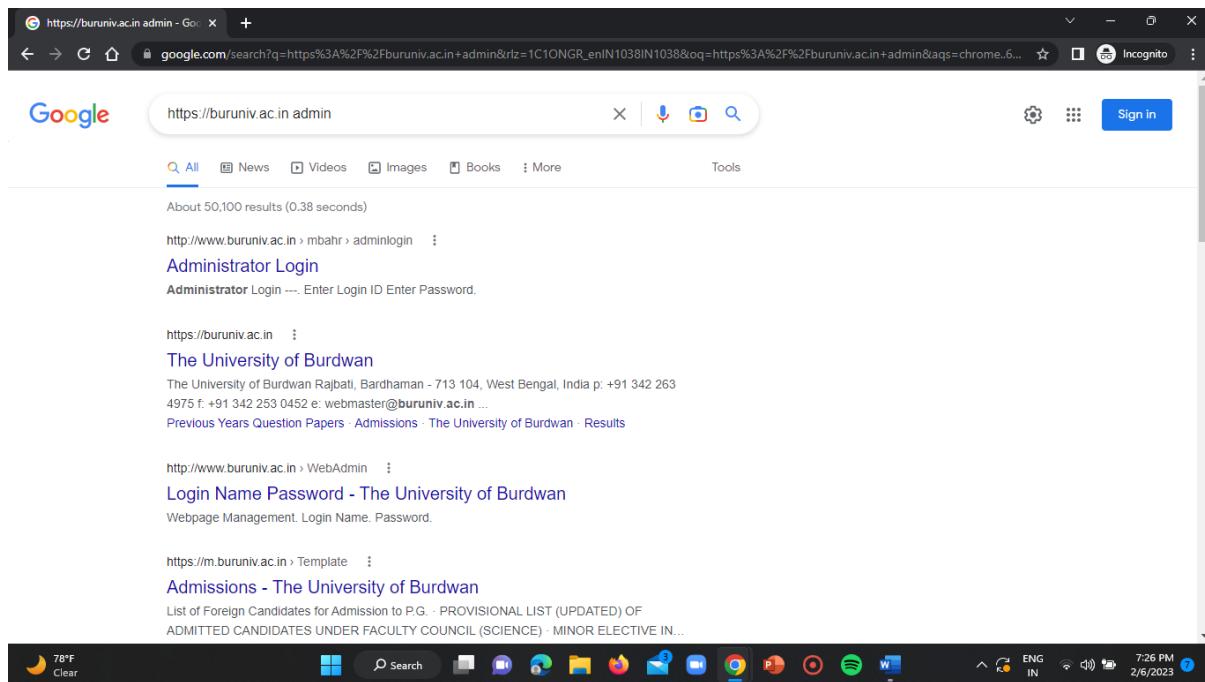
DOMAIN-1:

Step-4:

Use the “admin” dork for the very first domain.

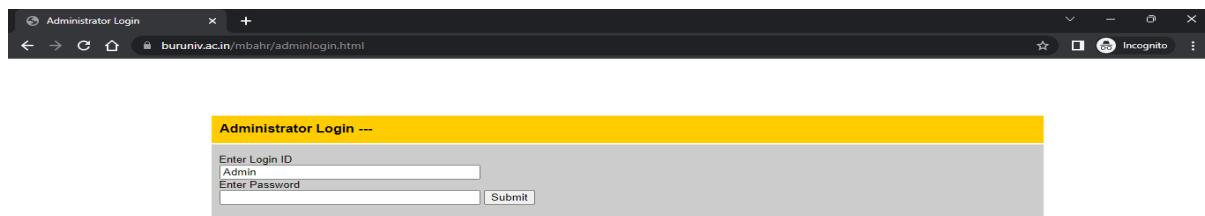
That is type “ <https://buruniv.ac.in/admin> ”

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

The screenshot shows a Google search results page with the query "site:stjosephsvizag.com login.php". The top result is a link to "Students Login - St. Joseph's College for Women – Vizag". Below it are links to "eCampus - St. Joseph's College for Women – Vizag", "Administrative Team - St. Joseph's College for Women – Vizag", and "The Annual Quality Assurance Report (AQAR) of the IQAC". The search bar at the top contains "site:stjosephsvizag.com login.php". The bottom of the screen shows a taskbar with various icons and system status.

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

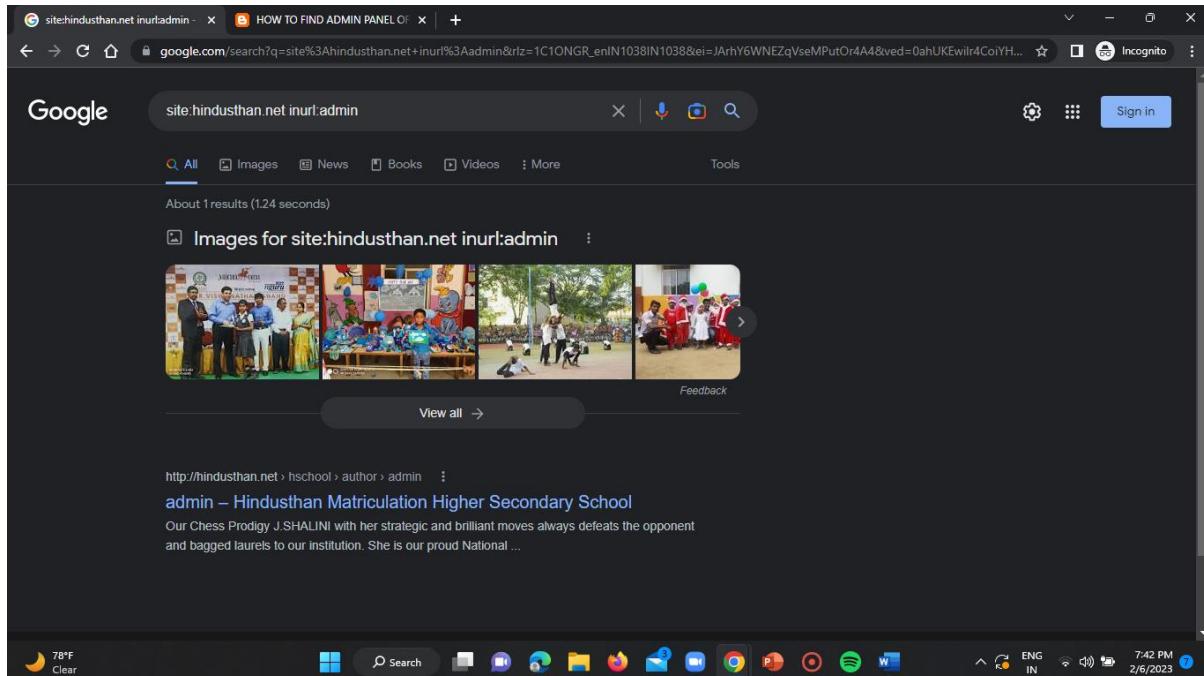
The screenshot shows the login page for St. Joseph's College for Women. The page features a logo with a pink and yellow design and the text "ST. JOSEPH'S College for Women" above a banner that reads "Autonomous | NAAC Reaccredited College with 'A' Grade". Below the banner is a large input form containing fields for "Username or Email", "Password", and "Google Authenticator code", along with a "Remember Me" checkbox and a "Log In" button. At the bottom of the form are links for "Lost your password?" and "← Go to St. Joseph's College for Women". The bottom of the screen shows a taskbar with various icons and system status.

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:

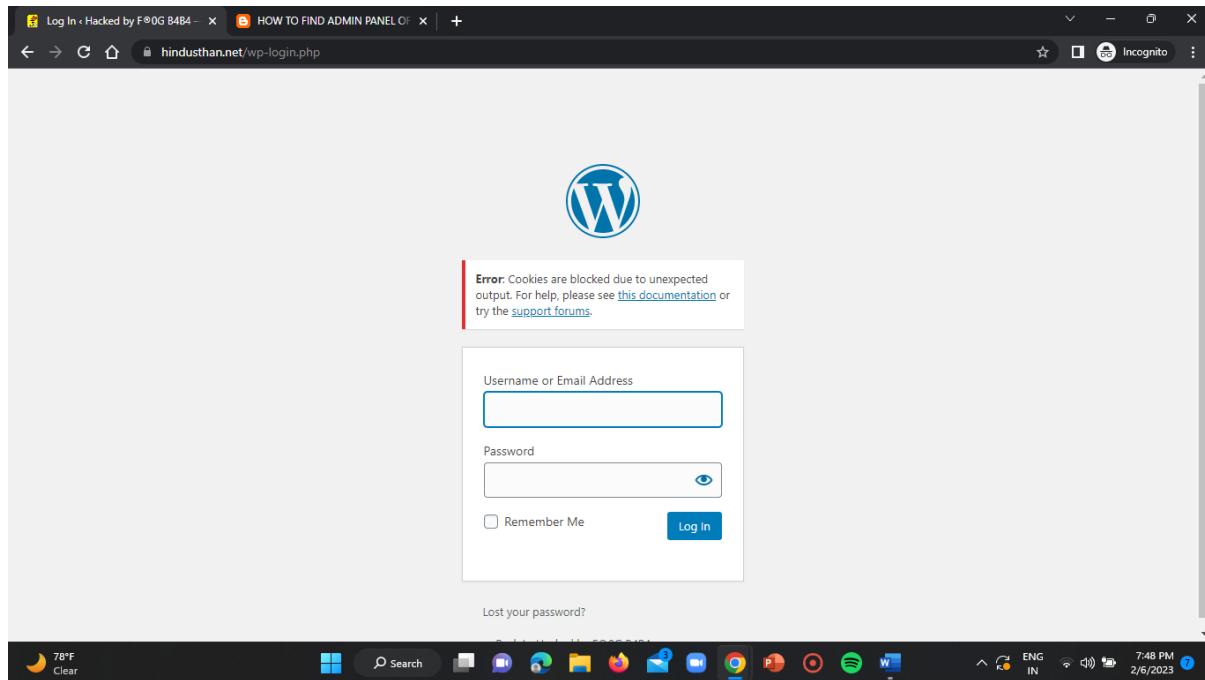
Now click on the blue link mentioning as “admin” on the displayed result page after searching.

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>

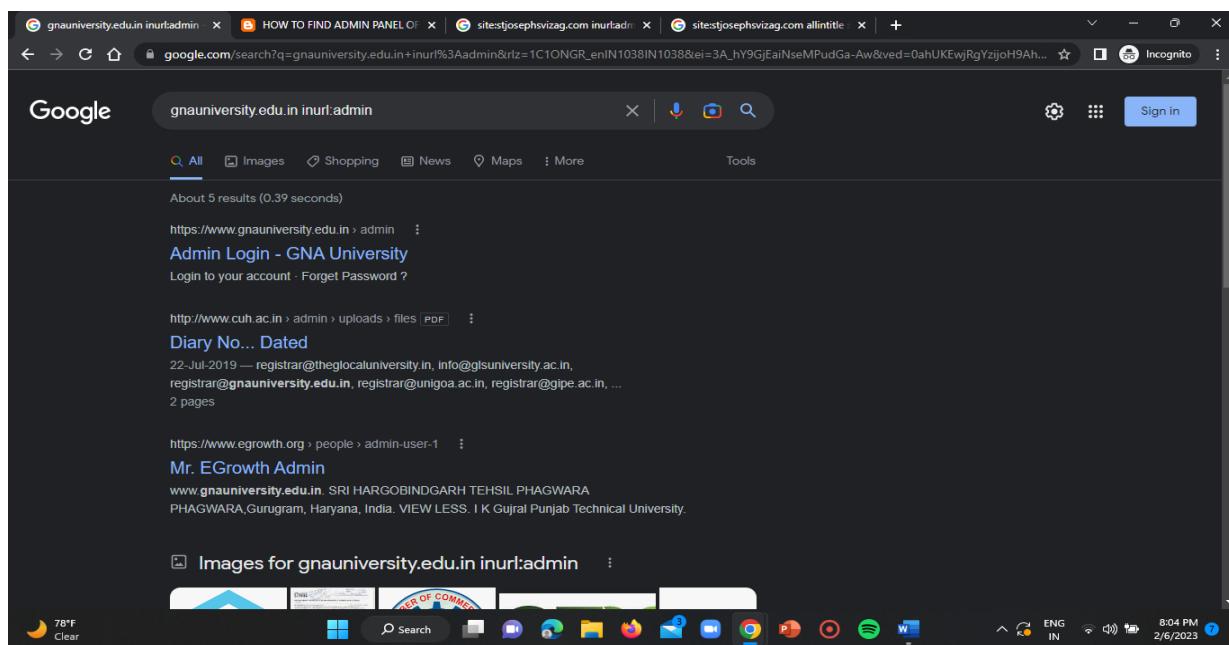
ST#IS#4899



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” .



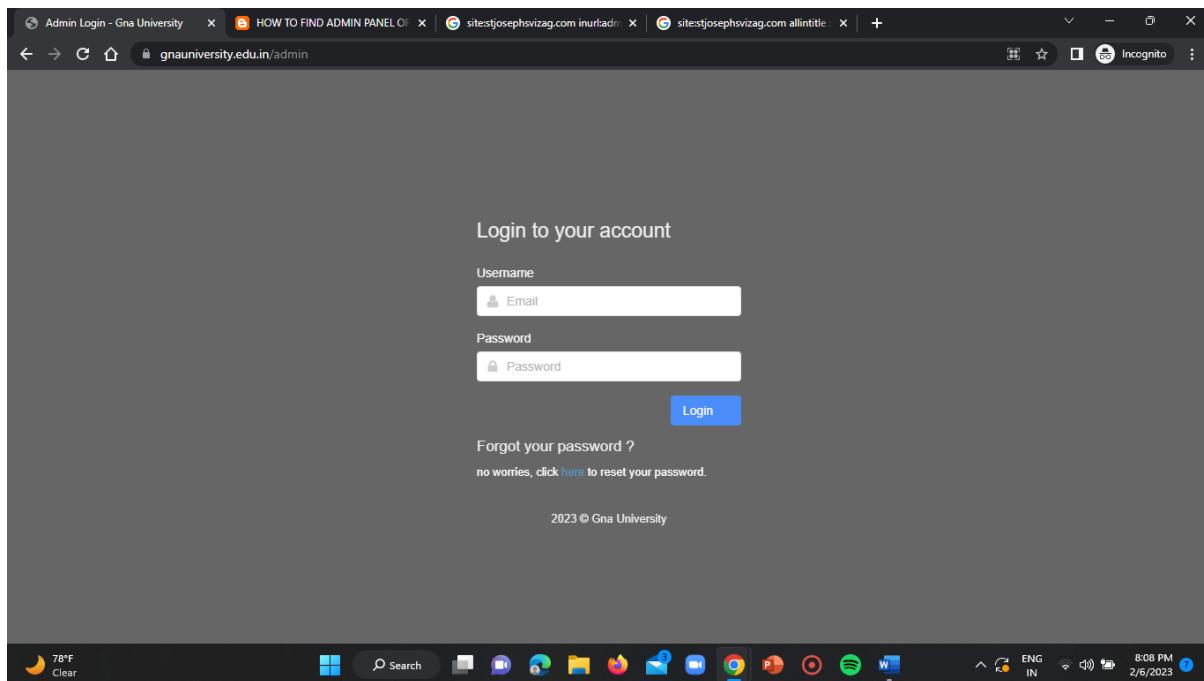
Step-11:

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>

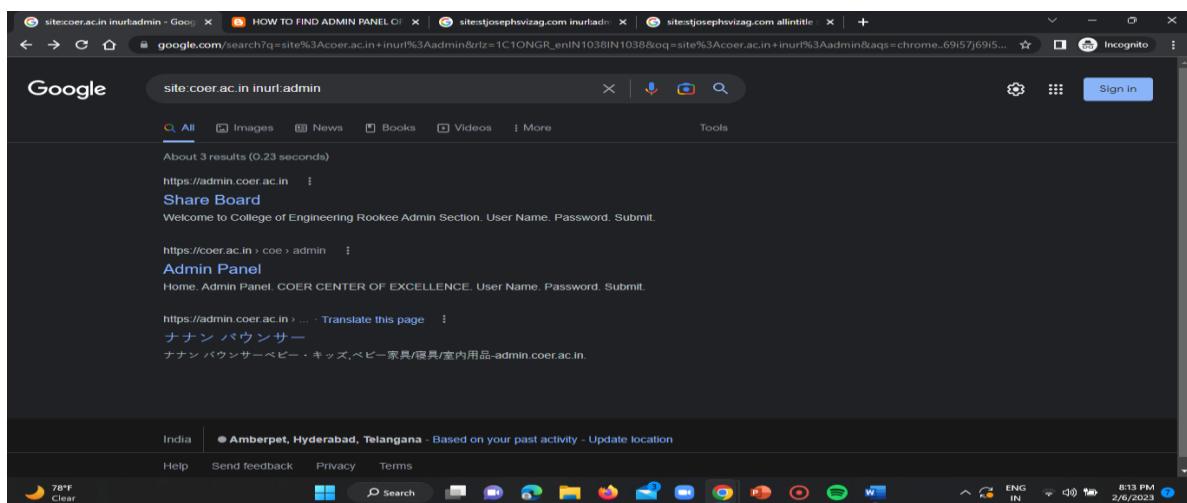


DOMAIN-5:

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”



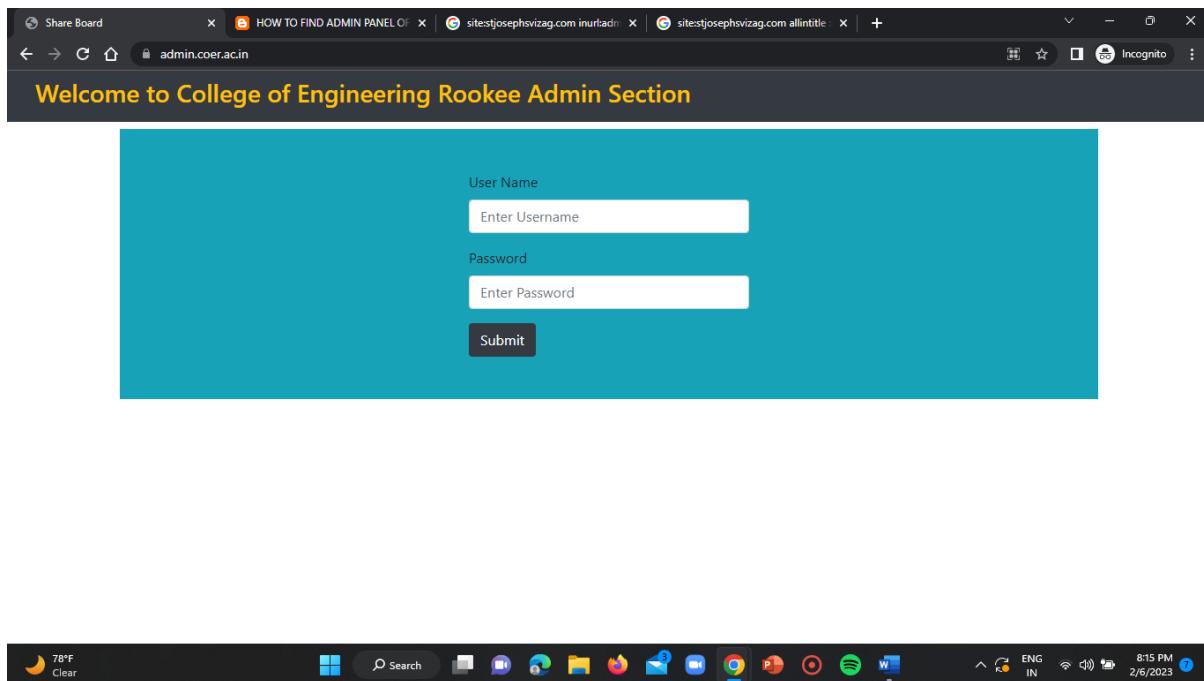
Step-13:

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

The screenshot shows a browser window with multiple tabs open. The active tab is the hunter.io homepage. The page features a search bar with the placeholder "company.com" and a red "Find email addresses" button. Below the search bar is a text input field with the placeholder "Enter a domain or company name to launch the search. For example, hunter.io.". A modal window titled "Domain Search" is overlaid on the page, containing a search bar with "buruniv.ac.in" and a "Search" button. The modal also includes a "Recent searches" section with "buruniv.ac.in". On the right side of the modal, there is a "Chrome extension" section with a "Close" button, a "Find email addresses from any website" checkbox, a "Save your leads in seconds" checkbox, and an "Add to Chrome" button. The browser's toolbar at the bottom shows various icons and the date/time "8:35 PM 2/6/2023".

Step-2:

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

ST#IS#4899

The screenshot shows the hunter.io search interface. The search bar at the top contains the URL <http://buruniv.ac.in/>. Below the search bar, there is a list of results for the domain buruniv.ac.in, with 46 results found. A modal window titled "Chrome extension" is open, showing that the hunter.io extension can find email addresses from any website and save leads in seconds. The extension icon is available for download.

Step-3:

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

The screenshot shows the detailed search results for buruniv.ac.in. The search bar indicates 46 results found. The results list includes two email addresses: pio@buruniv.ac.in and webmaster@buruniv.ac.in. Both emails have a confidence score of 94% and are categorized under IT / Engineering. To the right of the results, there are filters for Company (buruniv.ac.in) and Technologies. The hunter.io extension icon is visible in the browser toolbar.

E-MAIL ADDRESSES OF THE TARGET DOMAIN-1:

- 1) pio@buruniv.ac.in
- 2) webmaster@buruniv.ac.in
- 3) [dean arts@buruniv.ac.in](mailto: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.

The screenshot shows the hunter.io search interface. The search bar at the top contains the URL "http://hindusthan.net/". Below the search bar, there is a list of search results for the domain "hindusthan.net":

- Hindusthan College Of Arts And Science (hindusthan.net) - 20 results
- Hindusthan (hindusthan.org) - 1 result
- Hindusthan Speciality Chemicals Ltd (hindusthan.co.in) - 4 results
- Hindusthan Animal Care (hindusthananimalcare.com) - no results
- Hindusthan Bank (hindusthanbank.com) - 2 results

On the right side of the results, there is a sidebar with the following features:

- Find email addresses from any website
- Save your leads in seconds
- Add to Chrome (button)

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

The screenshot shows the hunter.io search interface. In the search bar, the query "gnauniversity.edu.in" is entered. Below the search bar, there's a list of results from "Gna University". A modal window titled "Chrome extension" is open, showing that 13 results were found for "hunter.io" and providing options to "Add to Chrome". The browser's taskbar at the bottom shows various open tabs and system icons.

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

The screenshot shows the detailed search results for "gnauniversity.edu.in". The results table lists 13 entries, including "admissions@gnauniversity.edu.in" and "cadcam@gnauniversity.edu.in". On the right side of the interface, there are filters for "Company" (set to "Gna University"), "Email pattern" (set to "(first).(last)@gnauniversity.edu.in"), "Accept all: NO", and "Industry: Technology". The browser's taskbar at the bottom shows various open tabs and system icons.

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

ST#IS#4899

- 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

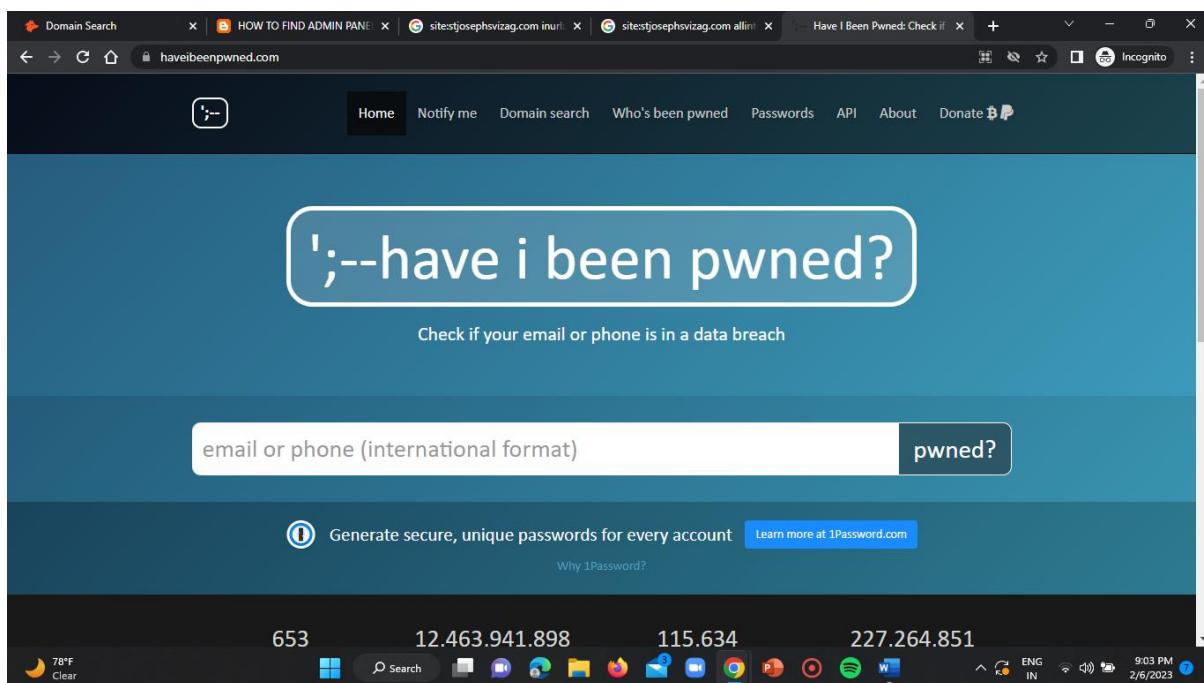
B – BIT:

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

The screenshot shows the Have I Been Pwned? website. The search bar contains "pio@buruniv.ac.in". A large red banner at the top says "Oh no — pwned!" and indicates "Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)". Below the banner, there are three steps to better security: 1. Protect yourself using 1Password to generate and save strong passwords for each website. 2. Enable 2 factor authentication and store the codes inside your 1Password account. 3. Subscribe to notifications for any other breaches. Then just change that unique password. The bottom of the page features social media links and a "Donate" button.

The screenshot shows the "Breaches you were pwned in" section of the Have I Been Pwned? website. It lists two breaches: "Onliner Spambot (spam list)" and "Verifications.io". The "Onliner Spambot" entry includes a link to a blog post titled "Inside the Massive 711 Million Record Onliner Spambot Dump". The "Verifications.io" entry includes a link to a blog post titled "800 million emails leaked online by email verification service". Both entries mention compromised data such as email addresses and passwords.

ST#IS#4899

2) webmaster@buruniv.ac.in

The screenshot shows a web browser window with multiple tabs open at the top. The active tab is for the website haveibeenpwned.com. The main content area features a large blue header with the text '';--have i been pwned?' in white. Below the header is a sub-header 'Check if your email or phone is in a data breach'. A search bar contains the email address 'webmaster@buruniv.ac.in'. To the right of the search bar is a dark blue button labeled 'pwned?'. The main body of the page is green and displays the message 'Good news — no pwnage found!' in white. Below this message, it says 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. At the bottom of the page, there is a '3 Steps to better security' section with three small illustrations and a 'Start using 1Password.com' button. The browser's taskbar at the bottom shows various pinned icons and the system tray on the right.

3) dean_arts@buruniv.ac.in

This screenshot is identical to the one above, showing the Have I Been Pwned? website for the email 'dean_arts@buruniv.ac.in'. The layout, search bar, results message ('Good news — no pwnage found!'), and bottom security steps section are all the same. The browser interface and taskbar at the bottom are also identical.

4) registrar@buruniv.ac.in

The screenshot shows a web browser window with the URL haveibeenpwned.com in the address bar. The main heading is '**';--have i been pwned?**' with a subtitle 'Check if your email or phone is in a data breach'. A search bar contains the email address `registrar@buruniv.ac.in`. To the right of the search bar is a button labeled 'pwned?'. Below the search area, a large red banner displays the message 'Oh no — pwned!' and indicates that the email was found in 7 data breaches. A link to 'subscribe to search sensitive breaches' is also present. At the bottom of the banner, there is a section titled '3 Steps to better security' with three small icons and a 'Start using 1Password.com' button. The Windows taskbar at the bottom of the screen shows various application icons and the date/time as 2/6/2023.

This screenshot shows the same browser window after clicking on one of the breach links from the previous screenshot. It displays a section titled 'Breaches you were pwned in'. It starts with a general note about what a breach is and how using a password manager like 1Password can help. Below this, two specific breach details are listed: 'Onliner Spambot' and 'Anti Public Combo List'. Each entry includes a small icon, a brief description, and a 'Compromised data' section. The 'Onliner Spambot' entry notes that it involved 711 million unique email addresses. The 'Anti Public Combo List' entry notes that it involved 458 million unique email addresses. Both entries mention that the data was used for credential stuffing. The Windows taskbar at the bottom remains visible.

ST#IS#4899

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 check 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

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: 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	12,463,941,898	115,634	227,264,851
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

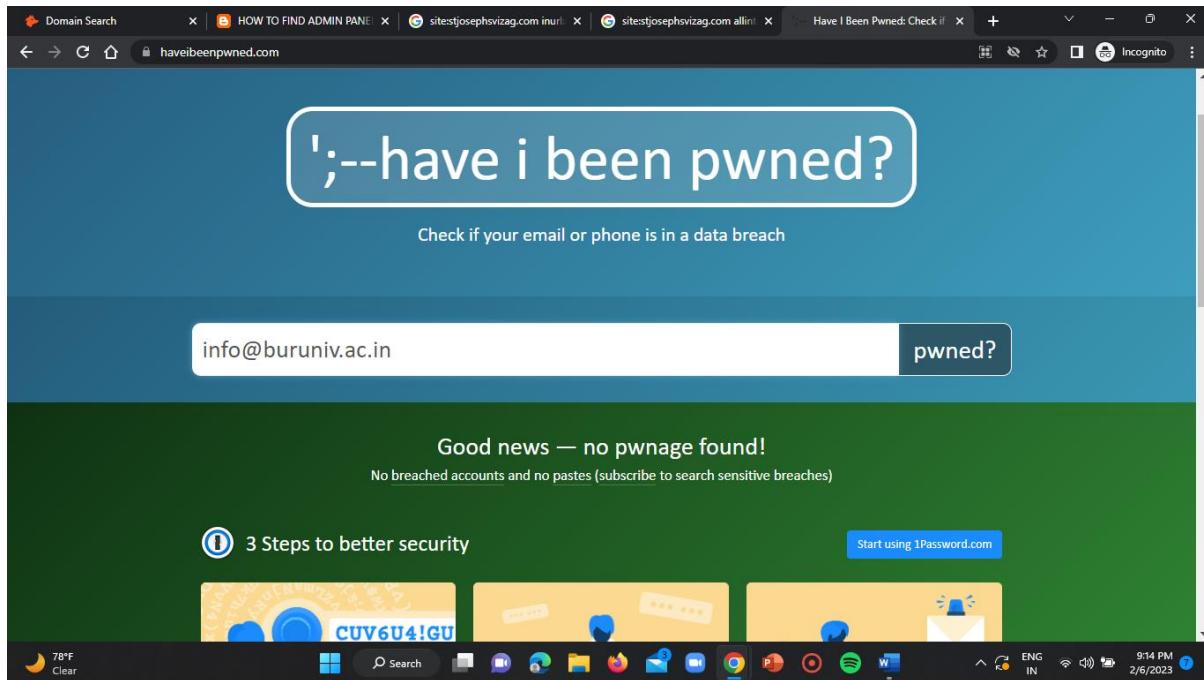
	772,904,991 Collection #1 accounts
	763,117,241 Verifications.io accounts
	711,477,622 Onliner Spambot accounts

Recently added breaches

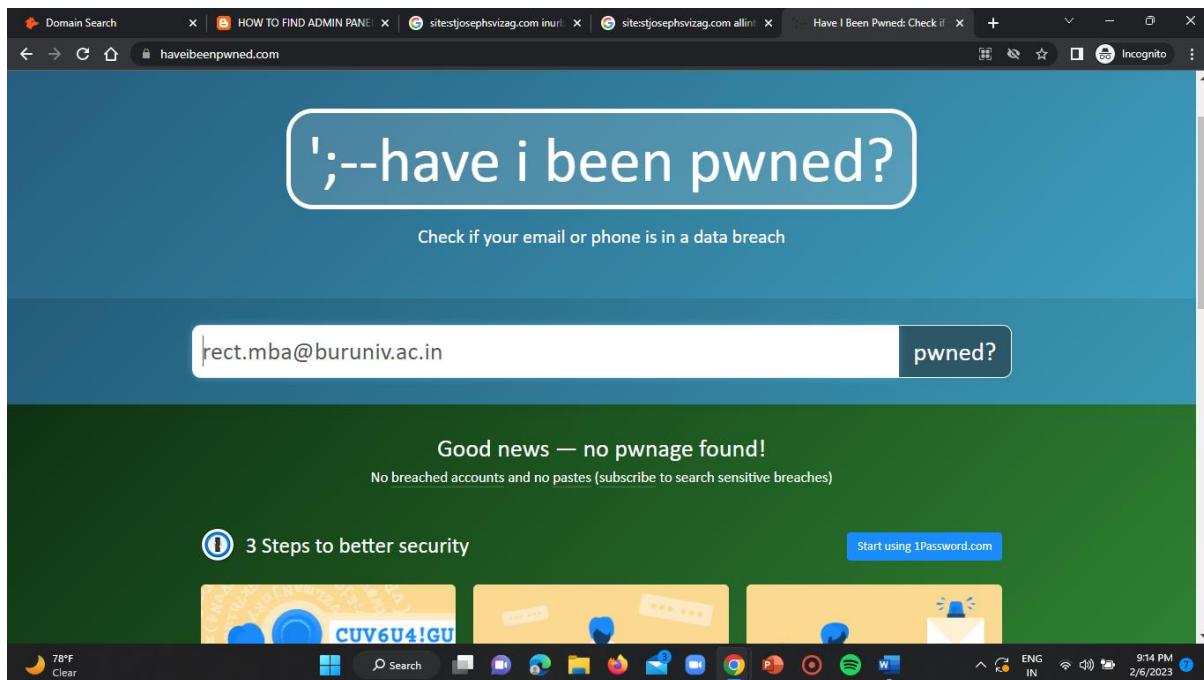
	8,159,573 Truth Finder accounts
	11,943,887 Instant Checkmate accounts
	18,850 School District 42 accounts

ST#IS#4899

5) info@buruniv.ac.in



6) rect.mba@buruniv.ac.in



ST#IS#4899

7) [rect.chemistry@buruniv.ac.in](https://haveibeenpwned.com/Check?Email=rect.chemistry@buruniv.ac.in)

The screenshot shows a web browser window with the URL haveibeenpwned.com in the address bar. The main content area features a large button with the text "';--have i been pwned?'". Below it is a sub-header "Check if your email or phone is in a data breach". A search bar contains the email address "rect.chemistry@buruniv.ac.in" and a "pwned?" button. The result section below says "Good news — no pwnage found!" and "No breached accounts and no pastes (subscribe to search sensitive breaches)". There is also a "3 Steps to better security" section and a "Start using 1Password.com" button. The browser's taskbar at the bottom shows various open tabs and system icons.

8) [rect.sanskrit@buruniv.ac.in](https://haveibeenpwned.com/Check?Email=rect.sanskrit@buruniv.ac.in)

This screenshot is identical to the one above, showing the same search results for the email address "rect.sanskrit@buruniv.ac.in". It displays the same "Good news — no pwnage found!" message and the same user interface elements, including the "3 Steps to better security" section and the "Start using 1Password.com" button. The browser's taskbar at the bottom is also visible.

ST#IS#4899

9) [rect.hindi@buruniv.ac.in](https://haveibeenpwned.com/CheckIfEmailOrPhoneIsInDataBreaches?Email=rect.hindi@buruniv.ac.in)

A screenshot of a web browser window. The address bar shows 'haveibeenpwned.com'. The main content area has a large white box with rounded corners containing the text ':--have i been pwned?'. Below this, smaller text reads 'Check if your email or phone is in a data breach'. A search bar contains the email address 'rect.hindi@buruniv.ac.in'. To the right of the search bar is a dark blue button with the word 'pwned?'. Below the search bar, a green banner displays the message 'Good news — no pwnage found!'. Underneath the banner, smaller text says 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. At the bottom of the page, there's a '3 Steps to better security' section with three small images and a 'Start using 1Password.com' button. The browser's taskbar at the bottom shows various open tabs and system icons.

10) [rect.education@buruniv.ac.in](https://haveibeenpwned.com/CheckIfEmailOrPhoneIsInDataBreaches?Email=rect.education@buruniv.ac.in)

A screenshot of a web browser window, identical to the previous one but with a different email address. The address bar shows 'haveibeenpwned.com'. The main content area has a large white box with rounded corners containing the text ':--have i been pwned?'. Below this, smaller text reads 'Check if your email or phone is in a data breach'. A search bar contains the email address 'rect.education@buruniv.ac.in'. To the right of the search bar is a dark blue button with the word 'pwned?'. Below the banner, a green banner displays the message 'Good news — no pwnage found!'. Underneath the banner, smaller text says 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. At the bottom of the page, there's a '3 Steps to better security' section with three small images and a 'Start using 1Password.com' button. The browser's taskbar at the bottom shows various open tabs and system icons.

11) info@hindusthan.net

The screenshot shows a search result for the email address info@hindusthan.net. The main message is '';--have i been pwned?' with a subtitle 'Check if your email or phone is in a data breach'. Below this, the email address is entered into a search bar, and a button labeled 'pwned?' is shown. The result section starts with 'Oh no — pwned!' and states 'Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)'. It includes a '3 Steps to better security' section with icons for a password manager and a lock, and a 'Start using 1Password.com' button. The bottom part of the page lists three data breaches: 'Onliner Spambot (spam list)', 'Cit0day (unverified)', and 'IndiaMART'. Each entry includes a small icon, a brief description, and a 'Compromised data' section. The browser taskbar at the bottom shows various open tabs and system status.

'';--have i been pwned?

Check if your email or phone is in a data breach

info@hindusthan.net

pwned?

Oh no — pwned!

Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

Onliner Spambot (spam list): In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moxuEiq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled [Inside the Massive 711 Million Record Onliner Spambot Dump](#).

Compromised data: Email addresses, Passwords

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

IndiaMART: In August 2021, 38 million records from Indian e-commerce company IndiaMART were found being traded on a popular hacking forum. Dated several months earlier, the data included over 20 million unique email addresses alongside names, phone numbers and physical addresses. It's unclear whether IndiaMART intentionally exposed the data attributes as part of the intended design of the platform or whether the data was obtained by exploiting a vulnerability in the service.

Compromised data: Email addresses, Names, Phone numbers, Physical addresses

78°F Clear

12) hicet@hindusthan.net

The screenshot shows a browser window with the URL haveibeenpwned.com. In the search bar, the email address `hicet@hindusthan.net` is entered. A button labeled "pwned?" is visible. Below the search bar, the text "Oh no — pwned!" is displayed in large white letters on a red background. A subtext below it says "Pwned in 3 data breaches and found no pastes (subscribe to search sensitive breaches)". There are three illustrated steps: Step 1 shows two people looking at a password; Step 2 shows a person enabling 2-factor authentication; Step 3 shows a person subscribing to notifications. A blue button "Start using 1Password.com" is located in the top right corner of the main content area. The bottom of the screen shows a Windows taskbar with various icons and system status.

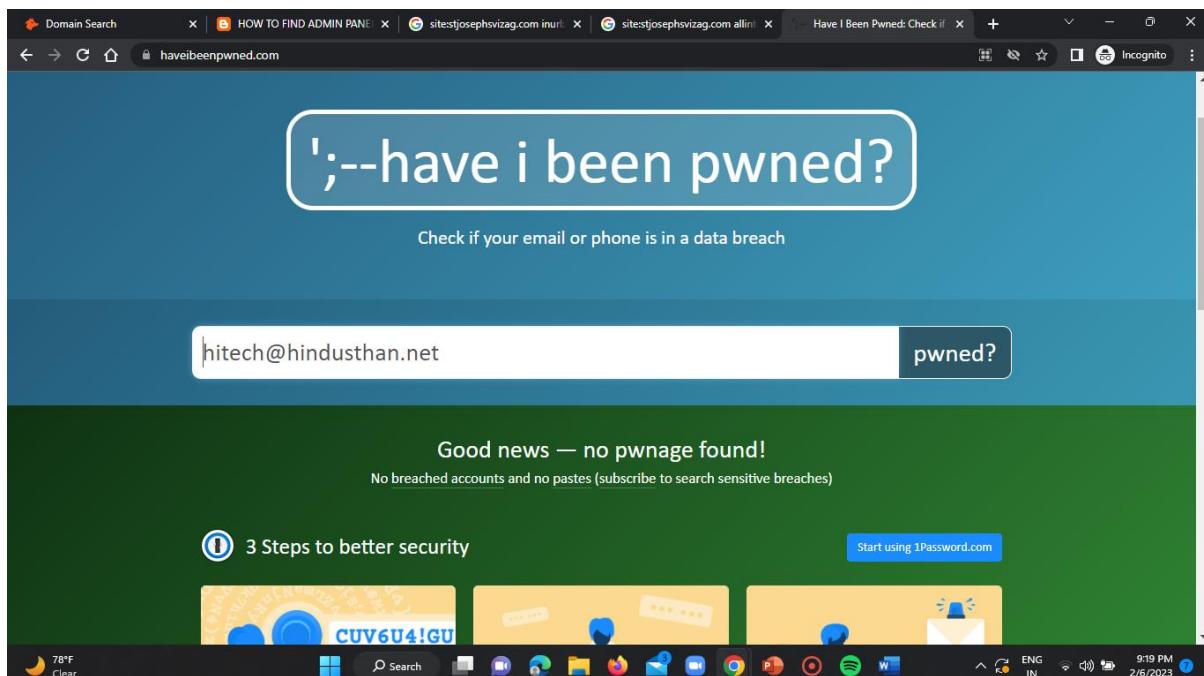
The screenshot shows the same browser window with the URL haveibeenpwned.com. The page displays a message: "ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk." Below this, there are three sections of breached data:

- Collection #1 (unverified):** This section discusses the "773 Million Record Collection #1" Data Breach, mentioning credential stuffing lists from January 2019. It includes a small icon of a document with horizontal lines. The compromised data listed is "Email addresses, Passwords".
- Exploit.In (unverified):** This section discusses the "Exploit.In" breach from late 2016, which contained 593 million unique email addresses. It includes a small icon of a document with horizontal lines. The compromised data listed is "Email addresses, Passwords".
- IIMJobs:** This section discusses a data breach at the Indian job portal IIMJobs in December 2018, which exposed 4.1 million unique email addresses. It includes a small icon of a person running. The compromised data listed is "Dates of birth, Email addresses, Geographic locations, IP addresses, Job applications, Job cover letters, Names, Phone numbers".

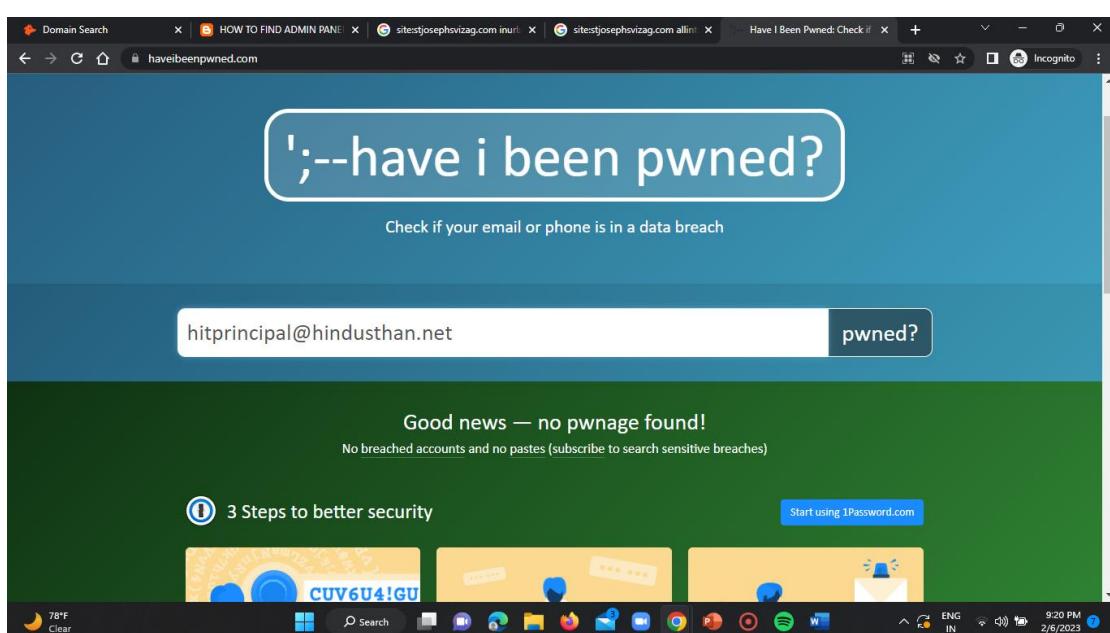
The bottom of the screen shows a Windows taskbar with various icons and system status.

ST#IS#4899

13) hitech@hindusthan.net



14) hitprincipal@hindusthan.net



ST#IS#4899

15) hicas@hindusthan.net

The screenshot shows the Have I Been Pwned? website. At the top, there is a large button with the text "';--have i been pwned?'". Below it, a sub-header says "Check if your email or phone is in a data breach". A search bar contains the email address "hicas@hindusthan.net" and a "pwned?" button. The main content area has a red background and displays the message "Oh no — pwned!" followed by "Pwned in 4 data breaches and found no pastes (subscribe to search sensitive breaches)". Below this, there is a section titled "3 Steps to better security" with three small icons. The Windows taskbar at the bottom shows various pinned icons and the date/time as 9:20 PM 2/6/2023.

The screenshot shows the "Breaches you were pwned in" section of the Have I Been Pwned? website. It lists three specific breaches with icons and details:

- 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](#).
- 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.
- 2,844 Separate Data Breaches (unverified):** In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single "unverified" data breach.

The Windows taskbar at the bottom shows various pinned icons and the date/time as 9:21 PM 2/6/2023.

ST#IS#4899

The screenshot shows a data breach entry for Lumin PDF. It includes a red header with the Lumin PDF logo and a brief description of the breach. Below this, there are four large numbers representing the count of breached data: 653 pwned websites, 12,463,941,898 pwned accounts, 115,634 pastes, and 227,264,851 paste accounts. Further down, sections for 'Largest breaches' and 'Recently added breaches' are visible, each listing several breached datasets with their respective counts.

16) barch@hindusthan.net

The screenshot shows the main search interface of the Have I Been Pwned? website. A prominent search bar at the top contains the email address 'barch@hindusthan.net'. To the right of the search bar is a large button labeled 'pwned?'. Below the search bar, a message states 'Good news — no pwnage found!' followed by the subtext 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. At the bottom of the page, there is a section titled '3 Steps to better security' with a call-to-action button 'Start using 1Password.com'.

ST#IS#4899

17) school@hindusthan.net

'';--have i been pwned?

Check if your email or phone is in a data breach

pwned?

Oh no — pwned!

Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Why 1Password?

[f](#) [t](#) [b](#) [p](#) [Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

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

IndiaMART: In August 2021, 38 million records from Indian e-commerce company IndiaMART were found being traded on a popular hacking forum. Dated several months earlier, the data included over 20 million unique email addresses alongside names, phone numbers and physical addresses. It's unclear whether IndiaMART intentionally exposed the data attributes as part of the intended design of the platform or whether the data was obtained by exploiting a vulnerability in the service.

Compromised data: Email addresses, Names, Phone numbers, Physical addresses

18) admission@hindusthan.net

The screenshot shows a web browser with multiple tabs open. The active tab is 'haveibeenpwned.com'. The page displays a large button with the text '';--have i been pwned?'. Below it, a sub-header reads 'Check if your email or phone is in a data breach'. A search bar contains the email address 'admission@hindusthan.net' and a blue button labeled 'pwned?'. The main content area shows a red banner with the text 'Oh no — pwned!' and 'Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)'. Below the banner, there's a section titled '3 Steps to better security' with three numbered steps: 1. Protect yourself using 1Password to generate and save strong passwords for each website; 2. Enable 2 factor authentication and store the codes inside your 1Password account; 3. Subscribe to notifications for any other breaches. Then just change that unique password. There are also links to 'Start using 1Password.com' and 'Why 1Password?'. At the bottom, there's a 'Donate' button with social media sharing icons. The browser's taskbar at the bottom shows various pinned icons.

This screenshot shows the same '3 Steps to better security' section from the previous page. It includes the same three steps: 1. Protect yourself using 1Password to generate and save strong passwords for each website; 2. Enable 2 factor authentication and store the codes inside your 1Password account; 3. Subscribe to notifications for any other breaches. Then just change that unique password. Below this, there's a section titled 'Breaches you were pwned in' with a note about what a breach is and how 1Password helps. It features a logo for IndiaMART and a link to its compromised data. At the bottom, there are statistics: 653 pwned websites, 12,463,941,898 pwned accounts, 115,634 pastes, and 227,264,851 paste accounts. The browser's taskbar at the bottom shows various pinned icons.

ST#IS#4899

19) ecampus@hindusthan.net

The screenshot shows the Have I Been Pwned? website interface. At the top, there is a navigation bar with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below the navigation bar, a large button contains the text ':--have i been pwned?'. Underneath it, a subtext reads 'Check if your email or phone is in a data breach'. A search input field contains the email address 'ecampus@hindusthan.net', and a button next to it says 'pwned?'. The main content area has a dark red background. It displays the message 'Oh no — pwned!' in white text, followed by 'Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)'. Below this, there is a section titled 'Breaches you were pwned in' with a sub-section about Nitro. At the bottom, there are statistics: '653 pwned websites', '12,463,941,898 pwned accounts', '115,634 pastes', and '227,264,851 paste accounts'. The bottom of the page features a 'Largest breaches' section with a table and a 'Recently added breaches' section with a table.

Domain Search | HOW TO FIND ADMIN PANE | sitestjosephsvizag.com inurl | sitestjosephsvizag.com allint | Have I Been Pwned: Check if | Incognito

Home Notify me Domain search Who's been pwned Passwords API About Donate

:--have i been pwned?

Check if your email or phone is in a data breach

ecampus@hindusthan.net pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security Start using 1Password.com

78°F Clear

each website. account. unique password.

Why 1Password?

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

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

653	12,463,941,898	115,634	227,264,851
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
762,117,241	Verifications in accounts

Recently added breaches

8,159,573	Truth Finder accounts
11,042,007	Instant Checkmate accounts

78°F Clear

20) bed@hindusthan.net

The screenshot shows a web browser window with multiple tabs open. The active tab is 'haveibeenpwned.com'. The page displays a large button with the text ':--have i been pwned?'. Below it, a sub-header reads 'Check if your email or phone is in a data breach'. A search bar contains the email address 'bed@hindusthan.net' and a 'pwned?' button. The main content area shows a red banner with the text 'Oh no — pwned!' and 'Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)'. Below the banner, there's a section titled '3 Steps to better security' with three numbered steps: 1. Protect yourself using 1Password to generate and save strong passwords for each website; 2. Enable 2 factor authentication and store the codes inside your 1Password account; 3. Subscribe to notifications for any other breaches. Then just change that unique password. At the bottom, there's a 'Why 1Password?' link, social media sharing icons, and a 'Donate' button. The status bar at the bottom of the screen shows weather information (78°F Clear), system icons, and the date/time (9:24 PM 2/6/2023).

ST#IS#4899

21) admissions@gnauniversity.edu.in

The screenshot shows a web browser window with the URL haveibeenpwned.com in the address bar. The page title is '';--have i been pwned?'. A search bar contains the email address admissions@gnauniversity.edu.in. Below the search bar is a large button labeled 'pwned?'. The main content area displays the message 'Oh no — pwned!' in white text on a dark red background. It states: 'Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)'. There is a '3 Steps to better security' section with a link to 'Start using 1Password.com'. The bottom of the screen shows a Windows taskbar with various icons and system status.

22) cadcams@gnauniversity.edu.in

The screenshot shows a web browser window with the URL haveibeenpwned.com in the address bar. The page title is '';--have i been pwned?'. A search bar contains the email address cadcams@gnauniversity.edu.in. Below the search bar is a large button labeled 'pwned?'. The main content area displays the message 'Good news — no pwnage found!' in white text on a dark green background. It states: 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. There is a '3 Steps to better security' section with a link to 'Start using 1Password.com'. The bottom of the screen shows a Windows taskbar with various icons and system status.

ST#IS#4899

23) sushant.anand@gnauniversity.edu.in

The screenshot shows a web browser window with the URL haveibeenpwned.com in the address bar. The main content area features a large button with the text "';--have i been pwned?'". Below it is a subtext "Check if your email or phone is in a data breach". A search bar contains the email address sushant.anand@gnauniversity.edu.in. To the right of the search bar is a blue button labeled "pwned?". The result section below says "Good news — no pwnage found!" and "No breached accounts and no pastes (subscribe to search sensitive breaches)". There is also a "3 Steps to better security" section and a "Start using 1Password.com" button. The bottom of the screen shows a Windows taskbar with various icons and a weather widget indicating 78°F Clear.

24) parveen.singh@gnauniversity.edu.in

The screenshot shows a web browser window with the URL haveibeenpwned.com in the address bar. The main content area features a large button with the text "';--have i been pwned?'". Below it is a subtext "Check if your email or phone is in a data breach". A search bar contains the email address parveen.singh@gnauniversity.edu.in. To the right of the search bar is a blue button labeled "pwned?". The result section below says "Good news — no pwnage found!" and "No breached accounts and no pastes (subscribe to search sensitive breaches)". There is also a "3 Steps to better security" section and a "Start using 1Password.com" button. The bottom of the screen shows a Windows taskbar with various icons and a weather widget indicating 78°F Clear.

ST#IS#4899

25) info@gnauniversity.edu.in

The screenshot shows the Have I Been Pwned? website interface. At the top, there's a search bar with the email address "info@gnauniversity.edu.in" and a button labeled "pwned?". Below the search bar, a large blue header features the text "';--have i been pwned?'". Underneath, a sub-header reads "Check if your email or phone is in a data breach". The main content area has a dark red background. It displays the message "Oh no — pwned!" in white. Below this, it says "Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)". There's a section titled "3 Steps to better security" with three icons: a lock, a key, and a shield. To the right of this is a "Start using 1Password.com" button. The bottom of the page shows a Windows taskbar with various application icons.

This screenshot shows the same Have I Been Pwned? website as above, but with a different URL in the address bar: "haveibeenpwned.com/account". The main content area now displays a section titled "Breaches you were pwned in". It includes a paragraph about what a breach is and how using a password manager like 1Password helps. Below this, there's a section titled "Data Enrichment Exposure From PDL Customer" with a small icon of a document. It describes a specific breach where researchers found 1.2 billion records. Further down, there's a section titled "Compromised data" listing various types of information exposed. At the bottom, there are four large numerical statistics: "653 pwned websites", "12,463,941,898 pwned accounts", "115,634 pastes", and "227,264,851 paste accounts". The bottom of the page shows a Windows taskbar.

ST#IS#4899

26) icohost@gnauniversity.edu.in

A screenshot of a web browser window showing the 'Have I Been Pwned?' website. The URL in the address bar is 'haveibeenpwned.com'. The main heading is '';--have i been pwned?'. Below it is a sub-heading 'Check if your email or phone is in a data breach'. A search bar contains the email address 'icohost@gnauniversity.edu.in' and a button labeled 'pwned?'. The result section says 'Good news — no pwnage found!' and 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. There is a '3 Steps to better security' section with a link to 'Start using 1Password.com'. The browser's taskbar at the bottom shows various open tabs and system icons.

27) iso@gnauniversity.edu.in

A screenshot of a web browser window showing the 'Have I Been Pwned?' website. The URL in the address bar is 'haveibeenpwned.com'. The main heading is '';--have i been pwned?'. Below it is a sub-heading 'Check if your email or phone is in a data breach'. A search bar contains the email address 'iso@gnauniversity.edu.in' and a button labeled 'pwned?'. The result section says 'Good news — no pwnage found!' and 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. There is a '3 Steps to better security' section with a link to 'Start using 1Password.com'. The browser's taskbar at the bottom shows various open tabs and system icons.

ST#IS#4899

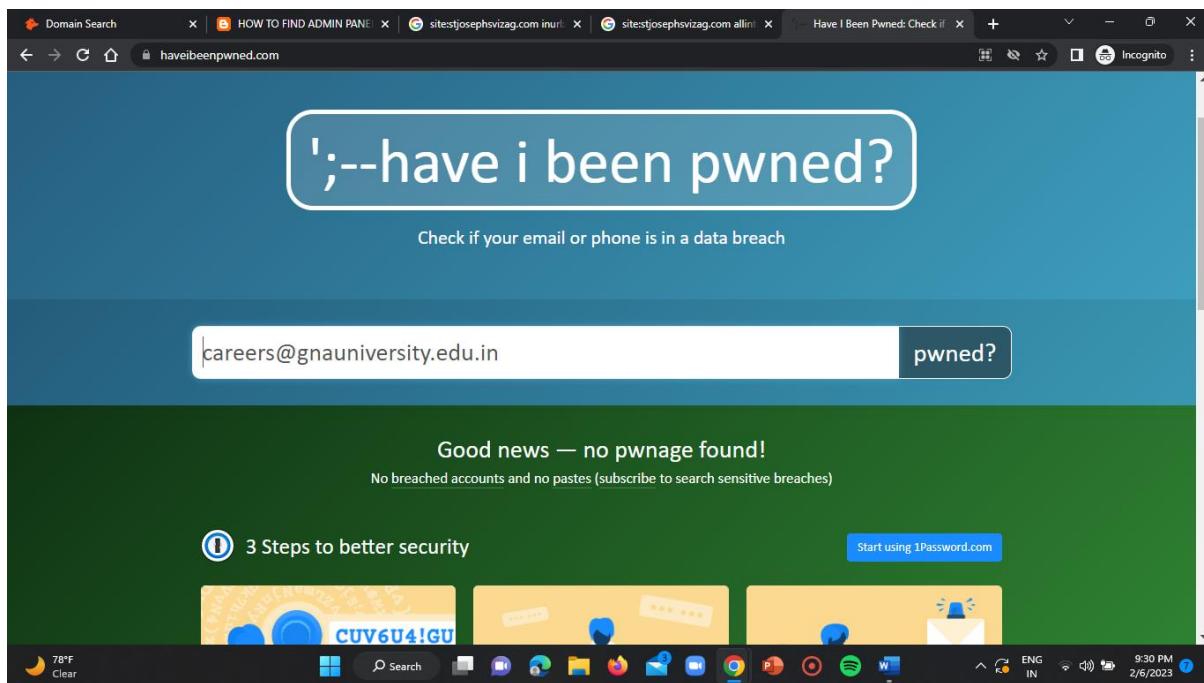
28) research@gnauniversity.edu.in

A screenshot of a Google Chrome browser window. The address bar shows 'haveibeenpwned.com'. The main content area features a large white button with the text '';--have i been pwned?'. Below it is a subtext 'Check if your email or phone is in a data breach'. A search bar contains the email 'research@gnauniversity.edu.in' and a 'pwned?' button. The background is dark blue. At the bottom, there's a green section with the text 'Good news — no pwnage found!', followed by 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. A '3 Steps to better security' section is shown with three icons: a lock, a key, and a shield. A 'Start using 1Password.com' button is also present. The taskbar at the bottom shows various application icons and the date/time '9:29 PM 2/6/2023'.

29) dean.foh@gnauniversity.edu.in

A screenshot of a Google Chrome browser window, identical to the previous one but with a different email address. The address bar shows 'haveibeenpwned.com'. The main content area features a large white button with the text '';--have i been pwned?'. Below it is a subtext 'Check if your email or phone is in a data breach'. A search bar contains the email 'dean.foh@gnauniversity.edu.in' and a 'pwned?' button. The background is dark blue. At the bottom, there's a green section with the text 'Good news — no pwnage found!', followed by 'No breached accounts and no pastes (subscribe to search sensitive breaches)'. A '3 Steps to better security' section is shown with three icons: a lock, a key, and a shield. A 'Start using 1Password.com' button is also present. The taskbar at the bottom shows various application icons and the date/time '9:29 PM 2/6/2023'.

30) careers@gnauniversity.edu.in

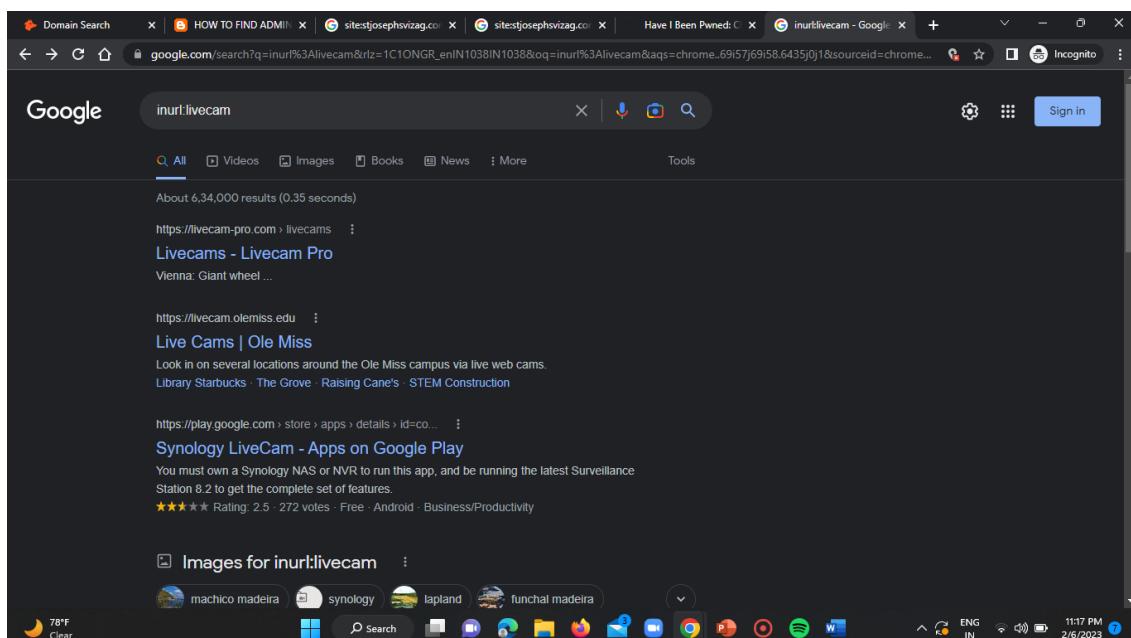


SOLUTION-3 :-

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.



ST#IS#4899

Step-2:

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

The screenshot shows the official website of the University of Mississippi. At the top, there's a navigation bar with links for Prospective Students, Current Students, Faculty & Staff, Parents & Families, Alumni & Friends, Visitors, Apply to Ole Miss, Give to Ole Miss, and Regional Campuses. Below the navigation bar is the university's logo and a search bar. The main content area features a section titled "Live Webcams" with several thumbnail images of different campus locations: STEM Construction, Guyton Hall Courtyard, Grove Stage, and others. To the right, a sidebar lists various live cam categories like STEM CONSTRUCTION, GUYTON HALL COURTYARD, GROVE, UNION PLAZA, QUADRANGLE, LIBRARY STARBUCKS, UNION CAFÉ, and COULTER STARBUCKS. A cookie consent banner at the bottom asks for permission to use cookies, with options to accept or decline.

CAM-1:

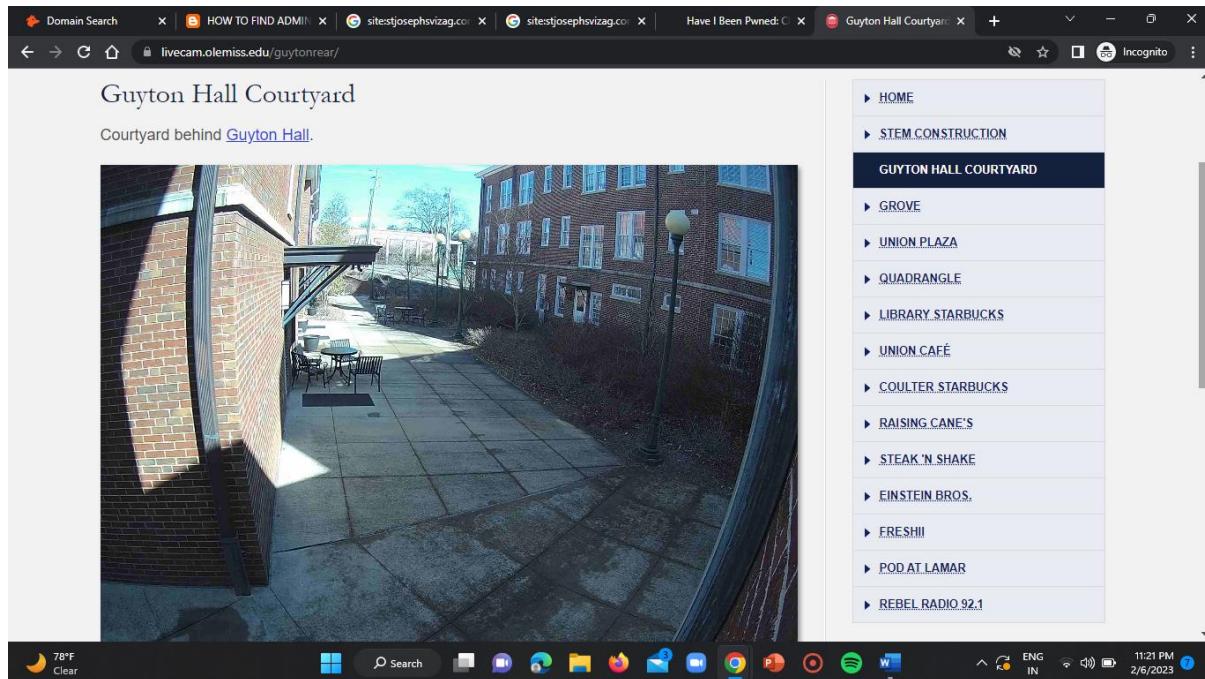
LINK = <https://livecam.olemiss.edu/stemeast/>

This screenshot shows a specific live cam from the University of Mississippi website, focusing on the STEM building construction site. The page title is "Construction of Jim & Thomas Duff Center for Science and Technology Innovation". It includes a photograph of the large, modern building under construction, surrounded by construction equipment and materials. The sidebar on the right remains the same, listing various live cam locations. The Windows taskbar at the bottom shows the date as 2/6/2023 and the time as 11:19 PM.

ST#IS#4899

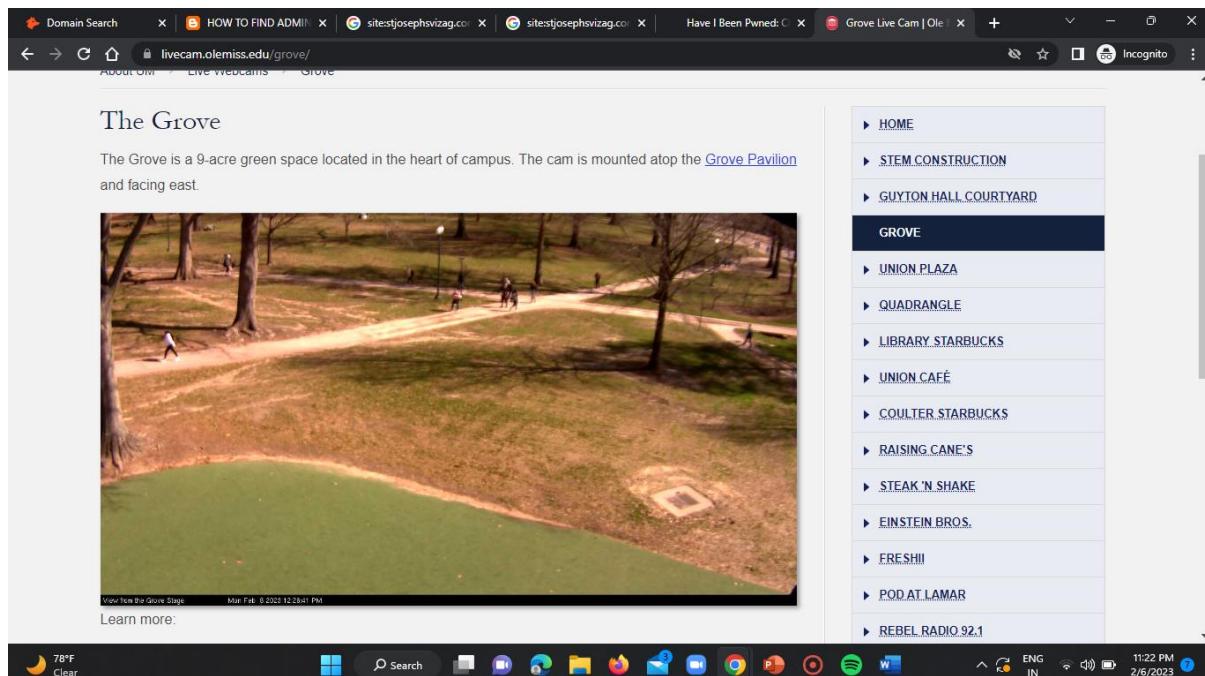
CAM-2:

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



CAM-3:

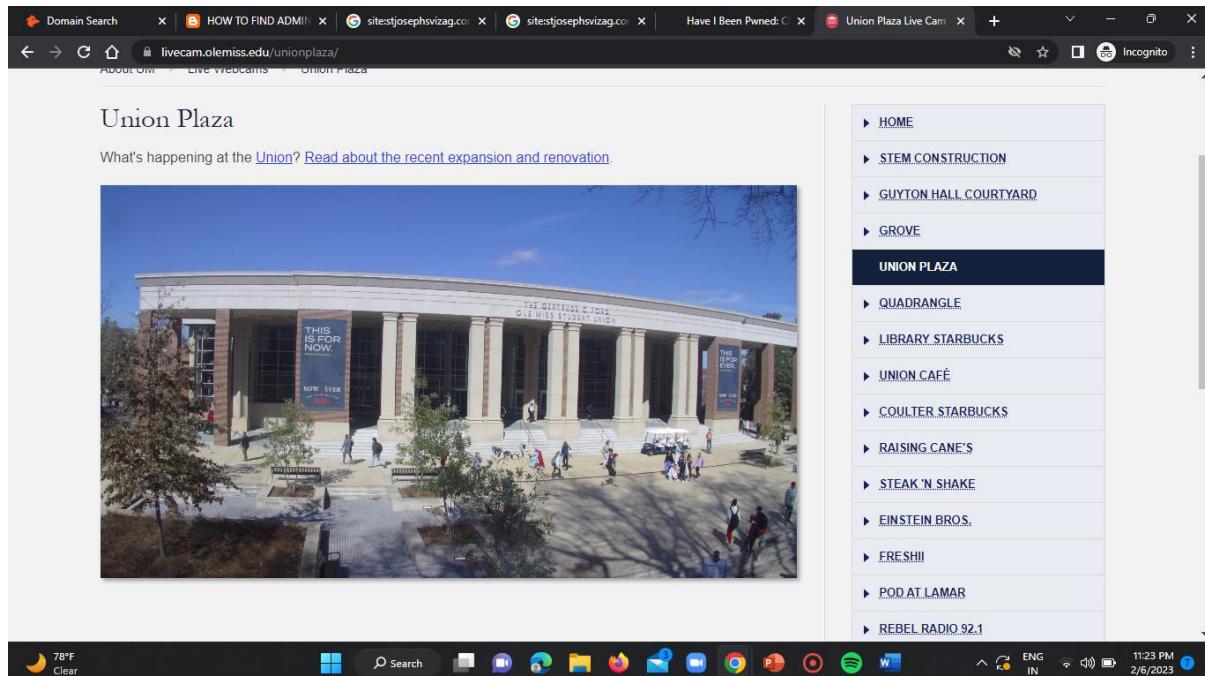
LINK = <https://livecam.olemiss.edu/grove/>



ST#IS#4899

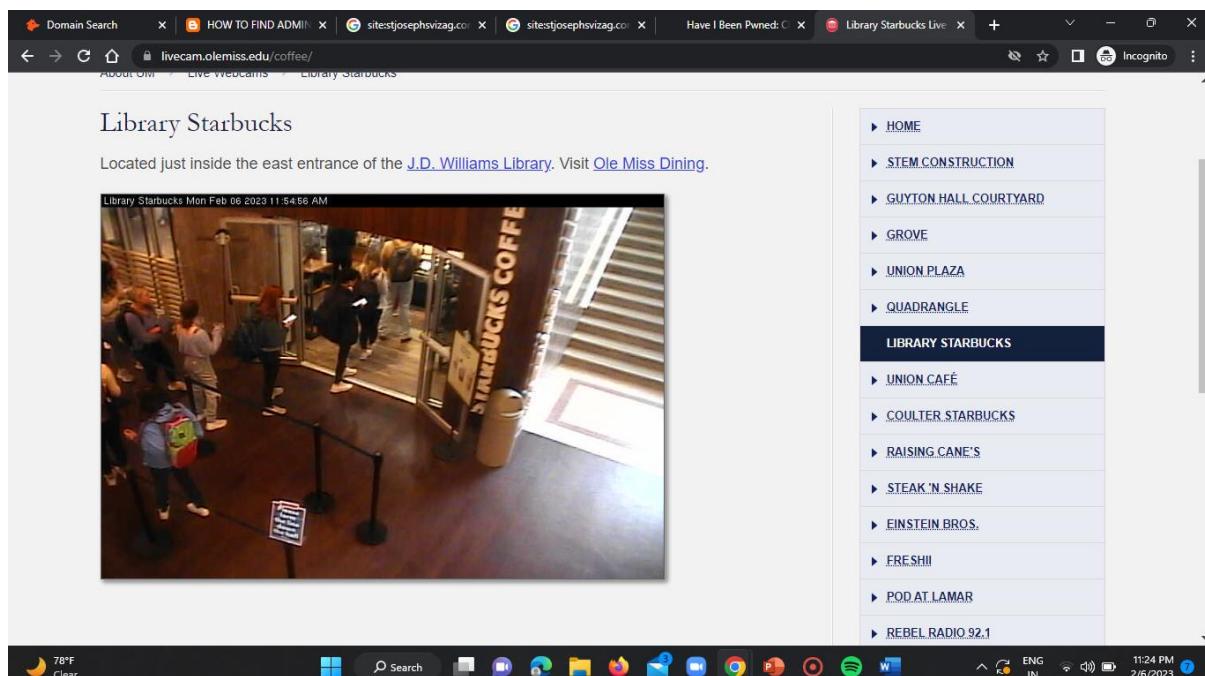
CAM-4:

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/>



A screenshot of a web browser displaying a live cam feed of the Union Café. The page title is "Union Café". Below the title, a caption reads "Just how busy is the [Union Café](#)?". The main content is a live video feed showing the interior of the cafeteria, which includes several round tables with wooden tops and metal frames, and matching wooden stools. In the background, there are shelves stocked with various items and a few people walking through the space.

CAM-7:

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



A screenshot of a web browser displaying a live cam feed of Einstein Bros. Bagels. The page title is "Einstein Bros. Bagels". The main content is a live video feed showing the interior of the shop. A woman in a pink shirt is seated at a red booth in the foreground, while another person is standing near the counter. The shop has a colorful checkered floor and wooden counters.

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 them using the footprinting technique.