TASK 2

**INTERNSHIP TASK-2**:

TARGET DOMAINS:

1.buruniv.ac.in

2.stjosephsvizag.com

3.hindusthan.net

4.gnauniversity.edu.in

5.coer.ac.in

Question 1:

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

Question 2a:

Gather 10 email addresses from any 3 given domains.

Note: domain/sub-domain registered emails only.

Question 2b:

Find whether the mails have been breached and if breached provide the resource (download link) where can you 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 1 country only.

**Summary of Steps**:

Step 1: To find the admin login pages from the given target domains using footprinting.

Step 2: To gather email addresses from the given target domains and to check whether the email IDs have been breached or not.

Step 3: To find the publicly available Camera that are available in shodan.io/OSINT framework.

**STEPS/PROCEDURE**:

STEP 1: To find the admin pages of the given target domains.

We can find an admin login page using google dorks which are available in Google Hacking Database.

For buruniv.ac.in: <https://www.buruniv.ac.in/mbahr/adminlogin.html>

Google dork:

Graphical user interface, text

Description automatically generated

Admin login page:

Graphical user interface

Description automatically generated

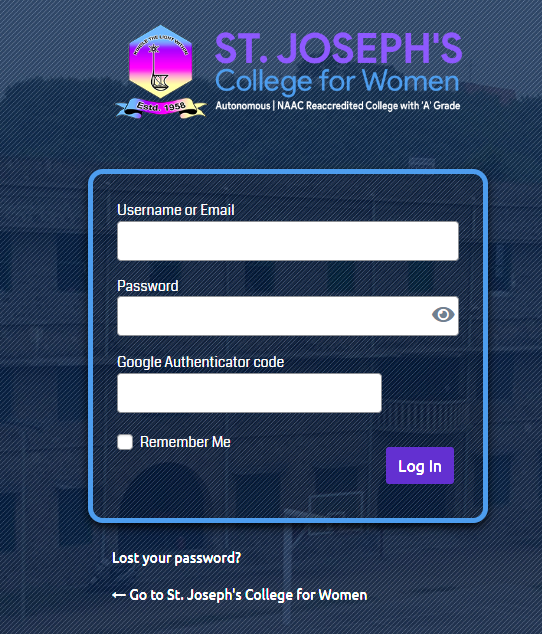
For stjosephvizag.com:

Google dork: <https://stjosephsvizag.com/admin>

Graphical user interface

Description automatically generated

Admin login page:



For Hindustan.net: <https://hicas.ac.in/admin/>

Google dork:

Graphical user interface, text

Description automatically generated

Here we get the admin page in a Sub domain named hicas.ac.in

Admin login page:

Graphical user interface, application, website

Description automatically generated

For gnauniversity.edu.in: <https://www.gnauniversity.edu.in/admin>

Google dork:

Graphical user interface, text, logo

Description automatically generated

Admin login page:

Graphical user interface, application

Description automatically generated

For coer.ac.in:

Google dork:

Graphical user interface, text, application

Description automatically generated

Admin login page:

Graphical user interface, application

Description automatically generated

STEP 2:

Gather 10 email addresses from any 3 given domains and to check whether the emails have been breached or not.

We can gather emails from a website called findmassleads : <https://www.findmassleads.com/email-finder>

For hindustan.net:

[info@hindusthan.net](mailto:info@hindusthan.net)

[hicas@hindusthan.net](mailto:hicas@hindusthan.net)

[hitech@hindusthan.net](mailto:hitech@hindusthan.net)

[hitprincipal@hindusthan.net](mailto:hitprincipal@hindusthan.net)

[admission@hindusthan.net](mailto:admission@hindusthan.net)

[bed@hindusthan.net](mailto:bed@hindusthan.net)

[barch@hindusthan.net](mailto:barch@hindusthan.net)

[drplacement@hindusthan.net](mailto:drplacement@hindusthan.net)

[hitinfo@hindusthan.net](mailto:hitinfo@hindusthan.net)

[hit.office@hindusthan.net](mailto:hit.office@hindusthan.net)

For buruniv.ac.in:

[dean\_arts@buruniv.ac.in](mailto:dean_arts@buruniv.ac.in)

[rect.germanlanguage@buruniv.ac.in](mailto:rect.germanlanguage@buruniv.ac.in)

[webmaster@buruniv.ac.in](mailto:webmaster@buruniv.ac.in)

[pio@buruniv.ac.in](mailto:pio@buruniv.ac.in)

[registrar@buruniv.ac.in](mailto:registrar@buruniv.ac.in)

[rect.mbahr@buruniv.ac.in](mailto:rect.mbahr@buruniv.ac.in)

[rect.tourism@buruniv.ac.in](mailto:rect.tourism@buruniv.ac.in)

[rect.hist@buruniv.ac.in](mailto:rect.hist@buruniv.ac.in)

[rect.education@buruniv.ac.in](mailto:rect.education@buruniv.ac.in)

[info@buruniv.ac.in](mailto:info@buruniv.ac.in)

For coer.ac.in:

[deansw@coer.ac.in](mailto:deansw@coer.ac.in)

[anuradha@coer.ac.in](mailto:anuradha@coer.ac.in)

[dyregistrar@coer.ac.in](mailto:dyregistrar@coer.ac.in)

[academic@coer.ac.in](mailto:academic@coer.ac.in)

[scholarship@coer.ac.in](mailto:scholarship@coer.ac.in)

[placement@coer.ac.in](mailto:placement@coer.ac.in)

[himanshuchauhan@coer.ac.in](mailto:himanshuchauhan@coer.ac.in)

[brijmohansingh@coer.ac.in](mailto:brijmohansingh@coer.ac.in)

[bdpatel@coer.ac.in](mailto:bdpatel@coer.ac.in)

[asyadav@coer.ac.in](mailto:asyadav@coer.ac.in)

-To find whether the above emails are breached or not

We can check that using a website called as HAVEIBEENPAWNED.com(https://haveibeenpwned.com) and another online platform called \_IntelligenceX(https://intelx.io).

For Hindustan.net:

1.info@hindusthan.net

This email has been breached.

#### Database link: <https://intelx.io/?did=2008f493-d7bc-42f6-80d0-fb3bb2ed80c>

**2.** hicas@hindusthan.net

This email has been breached.

#### Database link: <https://intelx.io/?did=b99e2dba-4db7-4c0c-889a-871e06156226>

**3.** hitech@hindusthan.net

This email has been breached.

#### Database link: <https://intelx.io/?did=86f5cf1f-c0af-4411-b20d-2bf839893b80>

**4.** hitprincipal@hindusthan.net

This email has been breached.

#### Database link: <https://intelx.io/?did=79cbe28f-0d53-4a65-ae8a-bd334577f55d>

#### 5. admission@hindusthan.net

This email has been breached.

Database link: <https://intelx.io/?did=138bdd9a-3265-4264-99798ad97869fb83>

6. [hit.office@hindusthan.net](mailto:hit.office@hindusthan.net)

The email has been breached.

Database link: <https://intelx.io/?did=887785a7-bf5d-4905-9241-7abf95fccdb1>

For buruniv.ac.in:

1. pio@buruniv.ac.in

This email has been breached.

Database link: <https://intelx.io/?did=8b892c52-6f21-4159-a7b1-e336684228c8>

2. registrar@buruniv.ac.in

This email has been breached.

Database link: <https://intelx.io/?did=30a60521-6c68-4491-868e-38fb3ae39a7a>

For coer.ac.in:

1. anuradha@coer.ac.in

This email has been breached.

Database link: <https://intelx.io/?did=061185ed-8741-45b0-9a44-d147278f0905>

2. [academic@coer.ac.in](mailto:academic@coer.ac.in)

This email has been breached.

Database link: <https://intelx.io/?did=19ba985f-ce73-42f1-9250-3acf4abd50bf>

3. [himanshuchauhan@coer.ac.in](mailto:himanshuchauhan@coer.ac.in)

This email has been breached.

Database link: <https://intelx.io/?s=himanshuchauhan%40coer.ac.in>

4. [brijmohansingh@coer.ac.in](mailto:brijmohansingh@coer.ac.in)

This email has been breached.

Database link: <https://intelx.io/?did=546aab2f-d710-49a1-9975-48287e8944dd>

5. [bdpatel@coer.ac.in](mailto:bdpatel@coer.ac.in)

This email has been breached.

Database link: <https://intelx.io/?did=c1a7d9f3-df98-4f39-b803-ddb9b39a7fd6>

STEP 3: To find the publicly available webcams in a specific country.

To find Live publicly accessible cameras I have used an Online platform named Earthcam.com(https://www.earthcam.com) that I have found in OSINT framework.

These are the following cams that I have found in JAPAN:

1.ODAIBA LIVE CAM**:** <https://www.youtube.com/watch?v=Z3IiNYJI4nc>

2.Live camera / Tokyo Shibuya: <https://www.youtube.com/watch?v=y65ueOclDaE>

3.Today 4K Panorama: <https://www.youtube.com/watch?v=8i9ltzhq80s>

4.Meteor shower & starry sky 24/7 Live from Kiso, JAPAN:

<https://www.youtube.com/watch?v=SDRS6JQulmI>

5.Kanazawa station Live Webcam Ishikawa, Japan :

<https://www.youtube.com/watch?v=i5ZEjaFK-II>

6.Ishikawa Prefectural Office Live camera:

<https://www.youtube.com/watch?v=Vsw4mZn--fE>

7.Live Scenery overlooking land, sea and sky, Tokyo JAPAN /TOKYO bay Live cam:

<https://www.youtube.com/watch?v=_ByNEL0Ton4>

**Conclusion**:

In this Document we have found out

1. How to find admin login pages from a given target domain.
2. How to check whether the emails that have been found from the target domain have been breached or not.
3. How to find the publicly available cameras/webcams in a specific country.

Tools used:

Google Dorks: These are used to find specific inputs which are required for the attacker.

Google dorks can be found in Google hacking database.

Findmassleads.com: It is an online platform which retrieves all the email addresses present in a domain in bulk.

Haveibeenpwned.com: This website is used to check whether the given email address has ever been a part of a data breach or not.

\_IntelligenceX.com: It is another Online platform that is used to check whether the given email address has been breached or not and provides the database link if the corresponding email has been breached.

Shodan.io: An online platform which gives access to all the publicly available Webcams/cameras around the world.

Earthcam.com: Another online platform which gives access about all the Live cameras/ webcams that are publicly available.

Foot printing is an important step in Ethical hacking which involves gaining information from publicly available sources and getting to know more about the target domain like to know the vulnerabilities of the target domain etc...