Indian Institute of Technology, Gandhinagar

CS 432: DATABASES

Assignment 4: Deploying the DBMS

Institute Phone Directory

Group - 14

Aravind Krishna - 20110021
Arun Mani - 20110023
Hrishikesh CP -20110078
Mihika Jadhav - 20110113
Madhav Biswam -20110103
Rahul R Pai - 20120155
Shrija Agrawal - 20110197
Abhiram Geddam - 19110149
Kanishk Singh - 19110089
Ruthvik Mula - 19110124
Ninad Shah - 19110126
Prateek Kumar Jha - 19110159

under the guidance of Prof. Mayank Singh

3. Tasks

3.1 Responsibility of G1:   40 Pts.

1. The G1 takes two feedbacks from the stakeholders, one initial feedback (on or before 30th March 11:59 PM), and then makes relevant changes as suggested per the first feedback, then final feedback (on or before 10th April 11:59 PM) post changes. The write-up/documentation should have screenshots before the first feedback, after the first feedback, and after the second feedback. If a team discusses with multiple stakeholders, please fill out the forms again (Initial and final feedback forms). **(30 Points)**

The following are the implemented changes as per the two feedbacks taken from the stakeholders.

   a. Implementing Search bar:

Before feedback-1

Indian Institute of Technology Gandhinagar
Telephone Directory

Faculty At IITGN

faculty_id	first_name	last_name	dept_name	designation	block_no	room_no	office_phone_number	Contact Details
10861895	Lucy	Goodwin	Biological Engineering	Associate Professor	3	101	9206468795	Contact
11643101	Jarett	Hessel	Civil Engineering	Associate Professor	3	102	9885201804	Contact
12340912	Lauren	Blick	Chemical Engineering	Assistant Professor	3	103	9556788048	Contact
12340913	Nona	Wehner	Computer Science and Engineering	Department Head	3	104	7598279544	Contact
12340914	Kailyn	Kuhlman	Electrical Engineering	Department Head	3	303	7313061424	Contact
12340915	Brandt	Rohan	Mechanical Engineering	Assistant Professor	3	304	7613606677	Contact
12340916	Max	Lowe	Materials Engineering	Associate Professor	3	305	7249562277	Contact
12340918	Barry	Yost	Mathematics	Department Head	4	201	9866162808	Contact
12340919	Mikayla	Windler	Physics	Associate Professor	4	202	9063577650	Contact
12340920	Brandy	Nienow	Cognitive Science	Assistant Professor	4	203	8924582281	Contact
12340921	Vivien	Bashirian	Earth Sciences	Associate Professor	4	203	8924582281	Contact
12340922	Jaunita	Stracker	Humanities and Social Sciences	Department Head	5	301	8536023832	Contact

After feedback-1

Indian Institute of Technology Gandhinagar
Telephone Directory

Faculty

Search: [Lucy] [Search]

faculty_id	first_name	last_name	dept_name	designation	block_no	room_no	office_phone_number	Contact Details
10861895	Lucy	Goodwin	Biological Engineering	Associate Professor	3	101	9206468795	Contact
11643101	Jarett	Hessel	Civil Engineering	Associate Professor	3	102	9885201804	Contact
12340912	Lauren	Blick	Chemical Engineering	Assistant Professor	3	103	9556788048	Contact
12340913	Nona	Wehner	Computer Science and Engineering	Department Head	3	104	7598279544	Contact
12340914	Kailyn	Kuhlman	Electrical Engineering	Department Head	3	303	7313061424	Contact
12340915	Brandt	Rohan	Mechanical Engineering	Assistant Professor	3	304	7613606677	Contact
12340916	Max	Lowe	Materials Engineering	Associate Professor	3	305	7249562277	Contact
12340918	Barry	Yost	Mathematics	Department Head	4	201	9866162808	Contact
12340919	Mikayla	Windler	Physics	Associate Professor	4	202	9063577650	Contact

Indian Institute of Technology Gandhinagar
Telephone Directory

Faculty

Search: [____] [Search]

faculty_id	first_name	last_name	dept_name	designation	block_no	room_no	office_phone_number	Contact Details
10861895	Lucy	Goodwin	Biological Engineering	Associate Professor	3	101	9206468795	Contact

Home Page   Logout

Designed by Group "Ono"
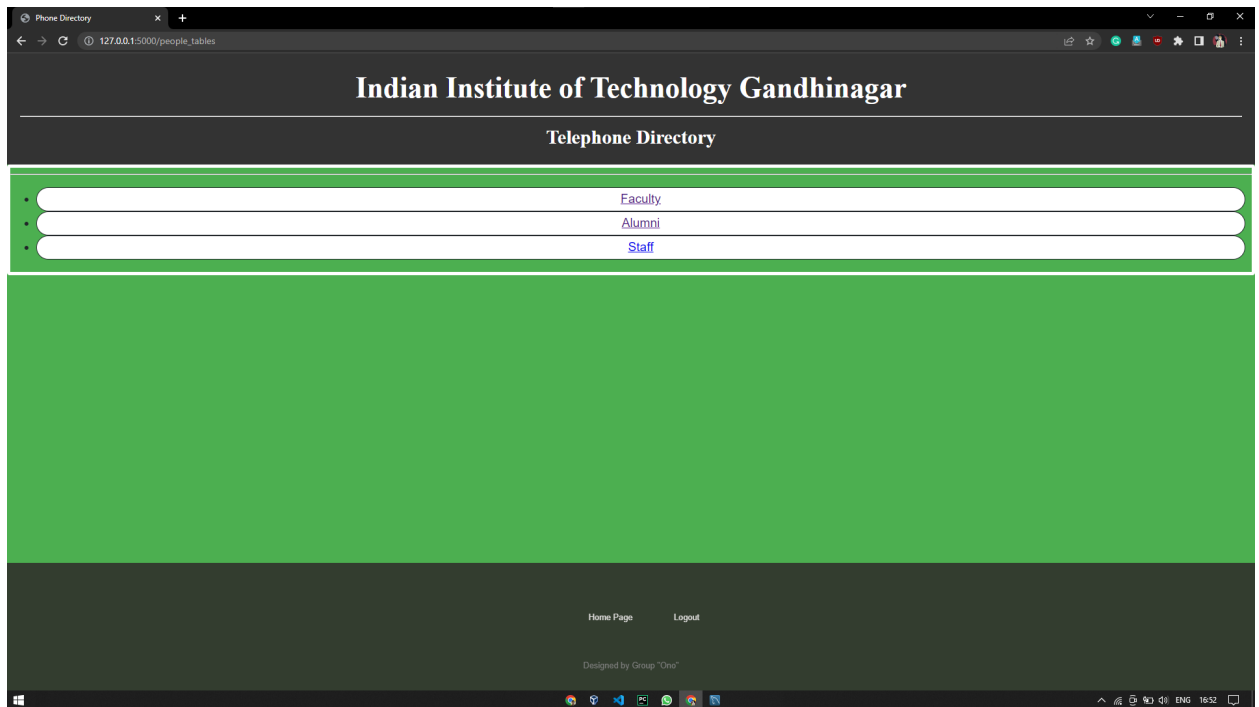
b. Restructuring the website

Before feedback-1

Indian Institute of Technology Gandhinagar

Telephone Directory

- Faculty
- Student
- Student Council
- Alumni
- Labs
- Centres
- Services
- Student Group

Home Page   Logout

Designed by Group "Ono"
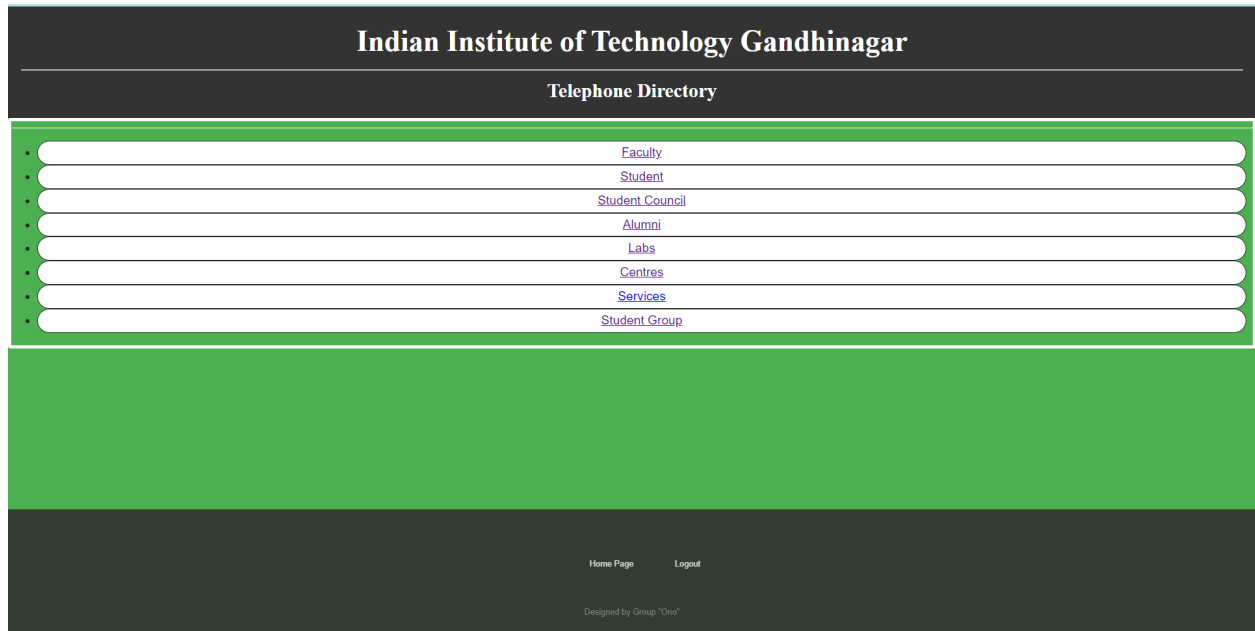
After feedback-1 (Grouping into categories to be structured)

Homepage

Indian Institute of Technology Gandhinagar

Telephone Directory

- People
- Facilities
- Students

Home Page   Logout

Designed by Group "Ono"
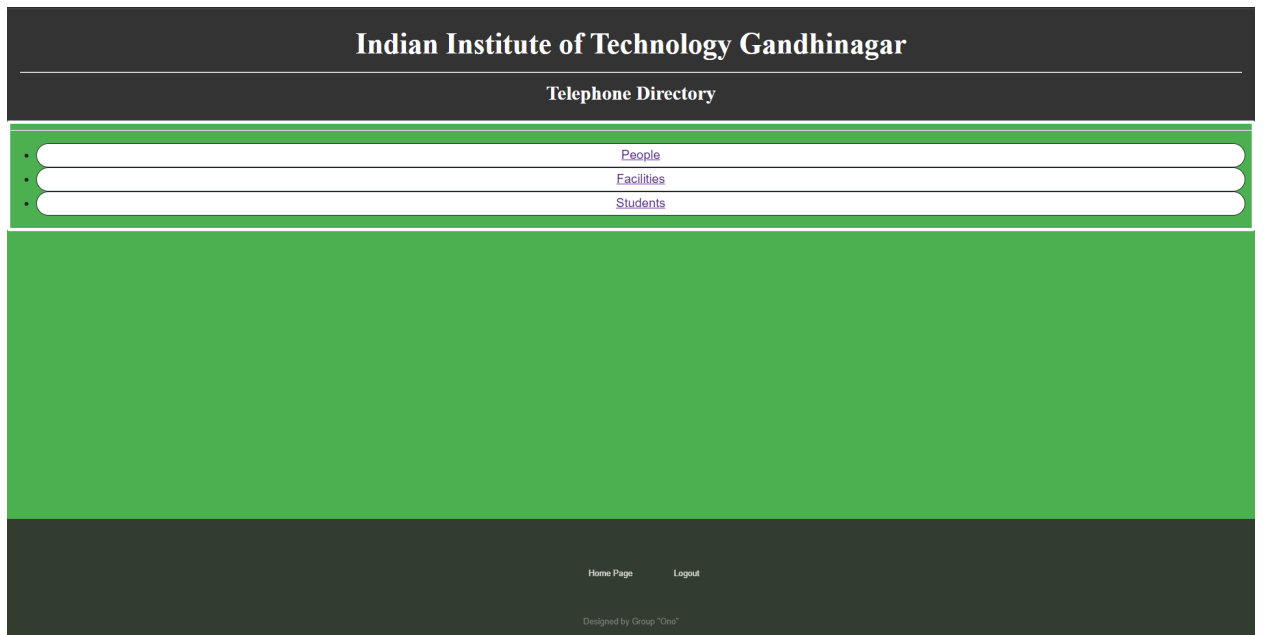
Homepage >> People

Homepage >> Facilities
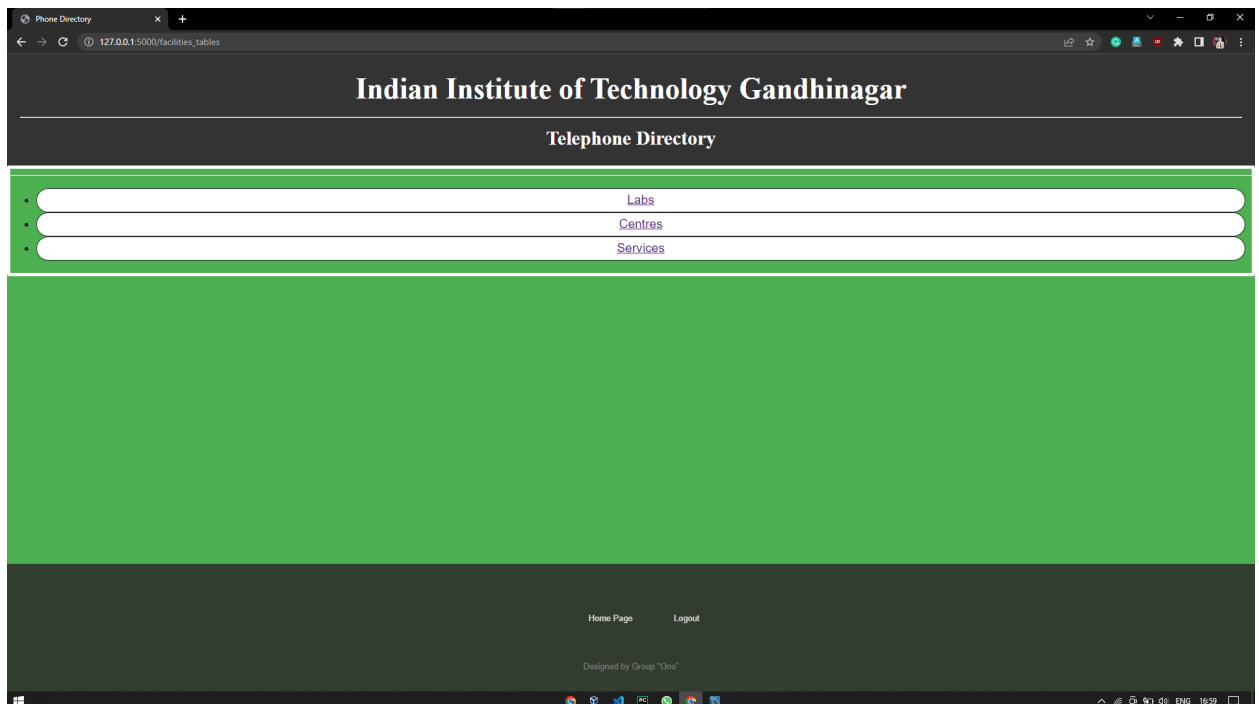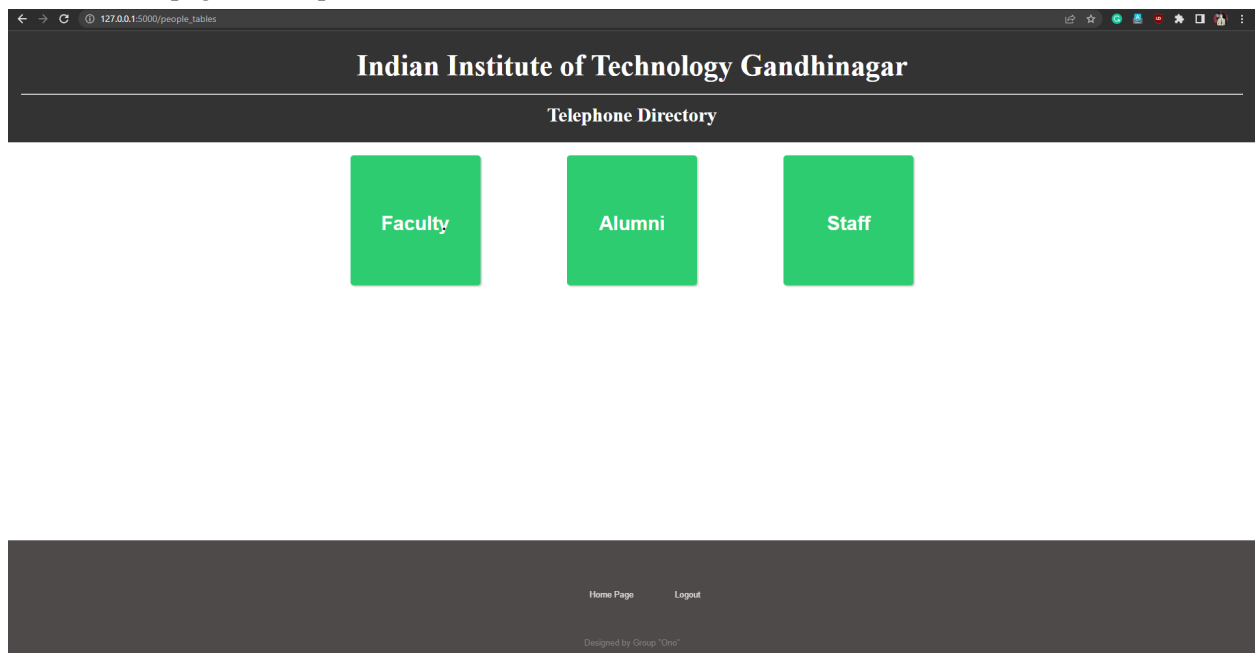
Homepage >> Students
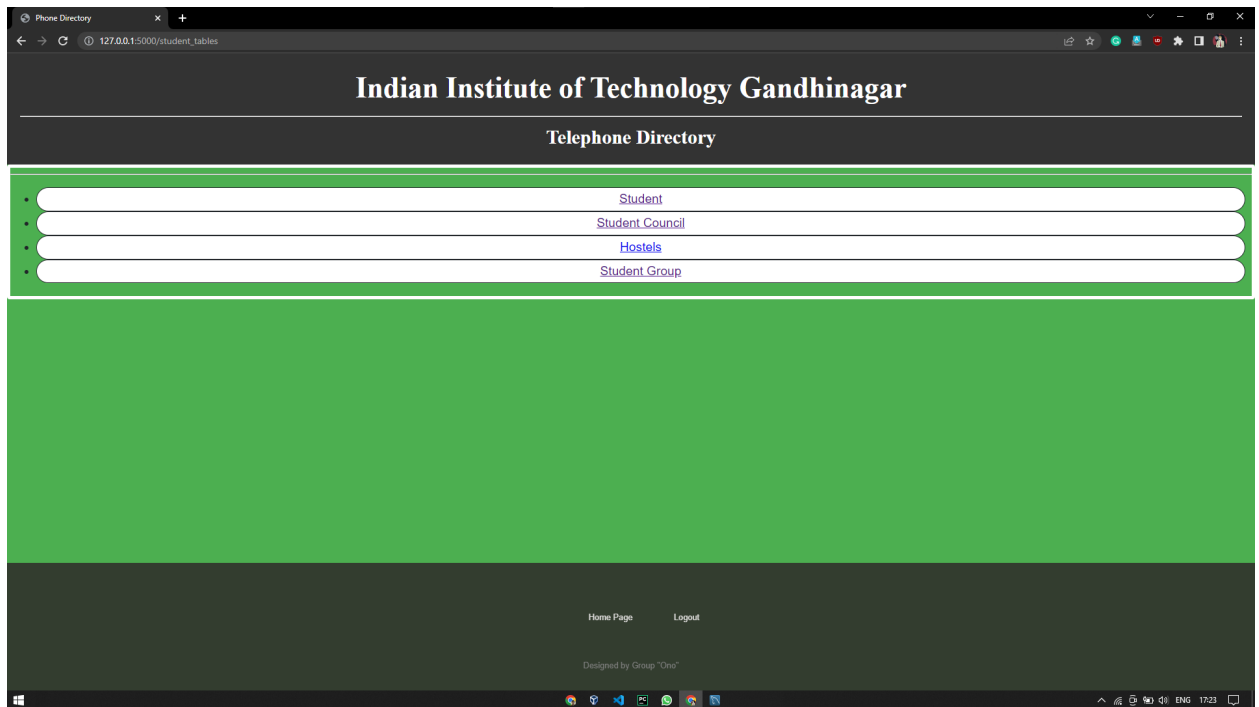
After feedback-2
   a.   Implemented cards for having a more friendly user interface
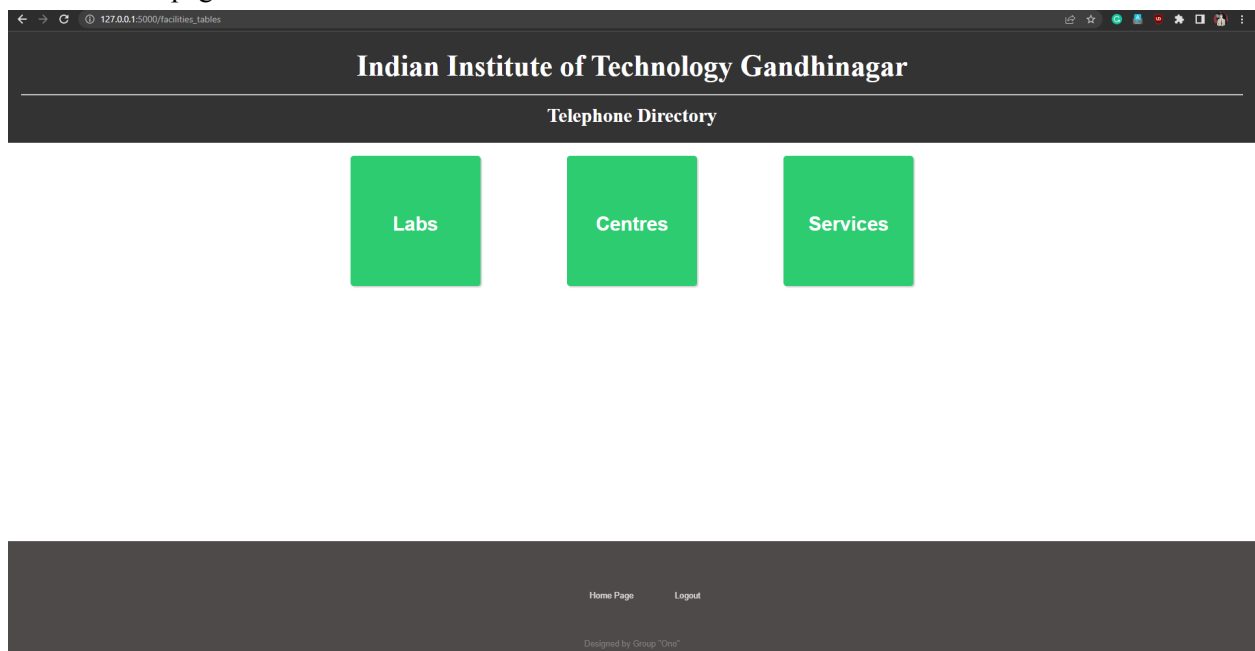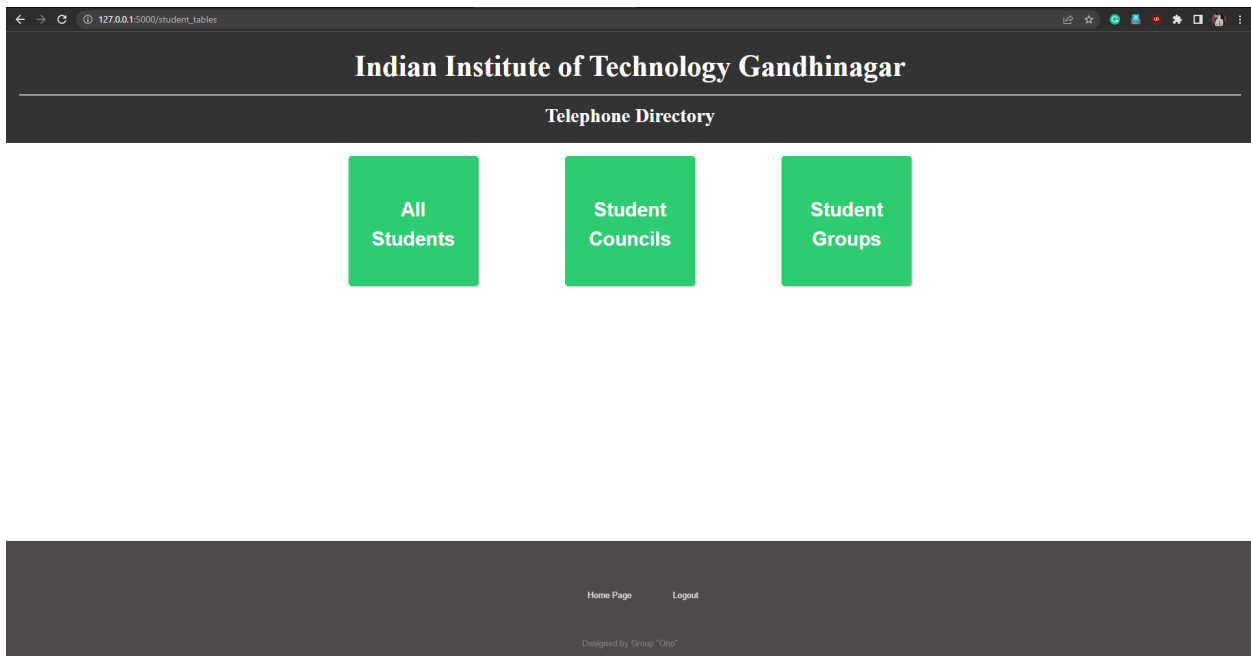   b.   Developed bigger buttons for a more comfortable interaction

   Homepage

Homepage >> People

Indian Institute of Technology Gandhinagar

Telephone Directory

Faculty   Alumni   Staff

Home Page   Logout

Designed by Group "Ono"

Homepage >> Facilities

Indian Institute of Technology Gandhinagar

Telephone Directory

Labs   Centres   Services

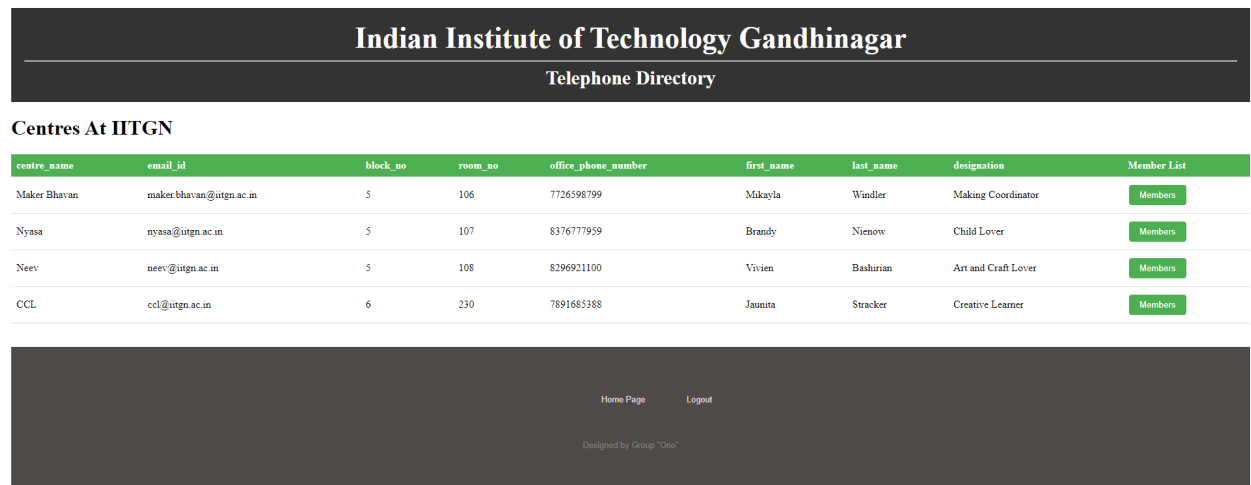Home Page   Logout

Designed by Group "Ono"

Homepage >> Students

c. Updated the database and table column titles to ensure effective communication
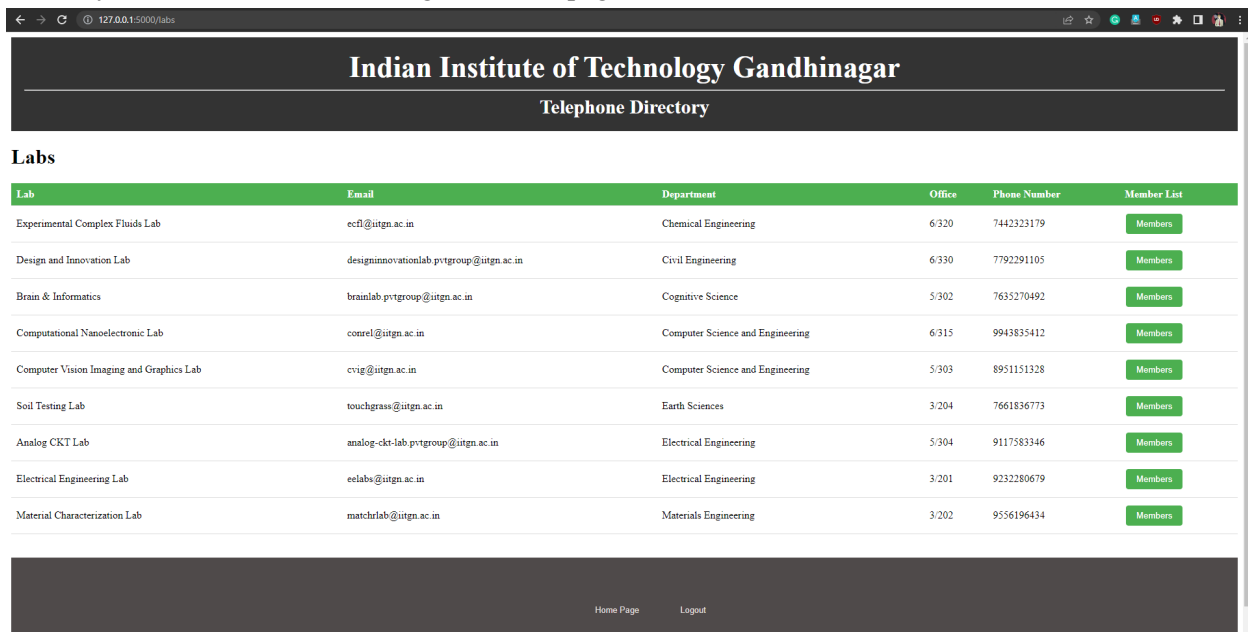
Before and after feedback-1

After feedback-2

Centres

Centre	Email	Office	Phone Number	Faculty Coordinator	Designation	Member List
Maker Bhavan	maker.bhavan@iitgn.ac.in	5/106	7726598799	Mikayla Windler	Making Coordinator	Members
Nyasa	nyasa@iitgn.ac.in	5/107	8376777959	Brandy Nienow	Child Lover	Members
Neev	neev@iitgn.ac.in	5/108	8296921100	Vivien Bashirian	Art and Craft Lover	Members
CCL	ccl@iitgn.ac.in	6/230	7891685388	Jaunita Stracker	Creative Learner	Members

Home Page   Logout

Designed by Group "One"

Similarly, column names were changed in other pages as:

Labs

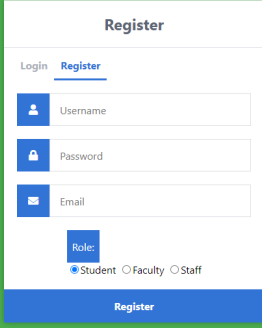| Lab	Email	Department	Office	Phone Number	Member List
Experimental Complex Fluids Lab	ecfl@iitgn.ac.in	Chemical Engineering	6/320	7442323179	Members
Design and Innovation Lab	designinnovationlab.pvtgroup@iitgn.ac.in	Civil Engineering	6/330	7792291105	Members
Brain & Informatics	brainlab.pvtgroup@iitgn.ac.in	Cognitive Science	5/302	7635270492	Members
Computational Nanoelectronic Lab	conrel@iitgn.ac.in	Computer Science and Engineering	6/315	9943835412	Members
Computer Vision Imaging and Graphics Lab	cvig@iitgn.ac.in	Computer Science and Engineering	5/303	8951151328	Members
Soil Testing Lab	touchgrass@iitgn.ac.in	Earth Sciences	3/204	7661836773	Members
Analog CKT Lab	analog-ckt-lab.pvtgroup@iitgn.ac.in	Electrical Engineering	5/304	9117583346	Members
Electrical Engineering Lab	eelabs@iitgn.ac.in	Electrical Engineering	3/201	9232280679	Members
Material Characterization Lab	matchrlab@iitgn.ac.in	Materials Engineering	3/202	9556196434	Members

Home Page   Logout

Here, the office room number columns were merged to a more common format used by community members.

2. Attach screenshots of different views [along with a write-up on their privileges] of the database as seen by different classes of users. **(10 Points)**

There are three classes of the database users for this phone directory database. They are Student, Faculty, and Staff. Implementing authentication enables access and edit privileges in the database through the website. For example, students are not able to access the contact details of the faculty while a faculty can look up the contract details of their fellow faculty.

The updated register page looks like following (Different users in the user class)

For instance, consider the example used above.
Logged in as Faculty: (Presenting Faculty privileges)

Indian Institute of Technology Gandhinagar

Telephone Directory

Faculty

Search: [_____] [Search]

faculty_id	first_name	last_name	dept_name	designation	block_no	room_no	office_phone_number	Contact Details
10861895	Lucy	Goodwin	Biological Engineering	Associate Professor	3	101	9206468795	Contact
11643101	Jarett	Hessel	Civil Engineering	Associate Professor	3	102	9885201804	Contact
12340912	Lauren	Blick	Chemical Engineering	Assistant Professor	3	103	9556788048	Contact
12340913	Nona	Wehner	Computer Science and Engineering	Department Head	3	104	7598279544	Contact
12340914	Kailyn	Kuhlman	Electrical Engineering	Department Head	3	303	7313061424	Contact
12340915	Brandt	Rohan	Mechanical Engineering	Assistant Professor	3	304	7613606677	Contact
12340916	Max	Lowe	Materials Engineering	Associate Professor	3	305	7249562277	Contact
12340918	Barry	Yost	Mathematics	Department Head	4	201	9866162808	Contact
12340919	Mikayla	Windler	Physics	Associate Professor	4	202	9063577650	Contact
12340920	Brandy	Nienow	Cognitive Science	Assistant Professor	4	203	8924582281	Contact
12340921	Vivien	Bashirian	Earth Sciences	Associate Professor	4	203	8924582281	Contact
12340922	Jaunita	Stracker	Humanities and Social Sciences	Department Head	5	301	8536023832	Contact

Logged in as Student: (Cannot access faculty contact information)

Faculty

Search: [   ] [Search]

faculty_id	first_name	last_name	dept_name	designation	block_no	room_no	office_phone_number
10861895	Lucy	Goodwin	Biological Engineering	Associate Professor	3	101	9206468795
11643101	Jarett	Hessel	Civil Engineering	Associate Professor	3	102	9885201804
12340912	Lauren	Blick	Chemical Engineering	Assistant Professor	3	103	9556788048
12340913	Nona	Wehner	Computer Science and Engineering	Department Head	3	104	7598279544
12340914	Kailyn	Kuhlman	Electrical Engineering	Department Head	3	303	7313061424
12340915	Brandt	Rohan	Mechanical Engineering	Assistant Professor	3	304	7613606677
12340916	Max	Lowe	Materials Engineering	Associate Professor	3	305	7249562277
12340918	Barry	Yost	Mathematics	Department Head	4	201	9866162808
12340919	Mikayla	Windler	Physics	Associate Professor	4	202	9063577650
12340920	Brandy	Nienow	Cognitive Science	Assistant Professor	4	203	8924582281
12340921	Vivien	Bashirian	Earth Sciences	Associate Professor	4	203	8924582281
12340922	Jaunita	Stracker	Humanities and Social Sciences	Department Head	5	301	8536023832

3.2 Responsibility of G2:   40 Pts.

1. Concurrent multi-user access: Multiple users with different roles can access and update the database concurrently. In such a scenario, the same item can not be updated by two different users. For example, locks can be applied to tables in MySQL. **(10 Points)**

Let us consider the situation where two admins are simultaneously trying to edit the alumni entry in the database. Let them be admin 1 and admin 2.

In the following, they are opened in side by side windows. The left is admin 1 and right is admin 2. Admin 1 is editing the alumni entry of Van Cum to change the name to Van Conn.

While admin1 is editing the entry, if admin 2 tries to edit any entry in the alumni table, admin 2 will see the following message on the top of the website saying that it is currently being edited by another user and to return to this a bit later. After a couple of seconds, admin 2 is navigated outside the alumni page to the select table page.

Once admin 1 finishes editing the entry, admin 2 can now be able to edit entries in the alumni table. The updated alumni entry here is Van Conn. If the admin 2 wants, they can edit any entry in the alumni table now.

This holds true for any number of users ensuring consistent concurrent multi-user access.

Whenever the "Edit" button is clicked, the table's name, user's email and the selected row's primary key get appended to the "locks_" table in our database.

Before redirecting to the edit page, the row selected is checked against the "locks_" table and if there's an entry corresponding to that particular row, then the user is prompted that the row is under modification, and they get redirected to the table selection page.

Once the modification is complete, i.e., "Update" button is clicked, the entry corresponding to that row is deleted from the "locks_" table.

This way the locks on tables have been implemented.

2. Implement the changes in the database as per the feedback received from stakeholders. **(30 Points)**

These changes based on the stakeholders' feedback are reflected in the live website and the data presented in it based on their respective permissions. The implementations are represented through the screenshots presented in this document. The Github repository of the same is submitted.

3.3 Responsibility of G1 & G2:   20 Pts

1. Documentation and screenshots of a total of 2 attacks [SQL Injection and XSS] performed and the defenses against those attacks. **(15 points)**
   a. Additional attack and defense will lead to 10 **bonus** points for the team. *(Maximum 20 bonus points)*

SQL INJECTION

SQL injection is when the user inputs an SQL statement instead of the required data in a search box. When the input values are concatenated with the queries, say query = "SELECT * FROM phone_directory_user WHERE username = '" + username+str('), the database can be manipulated maliciously. Instead of concatenation we can parameterize the inputs and thereby avoid SQL injection.
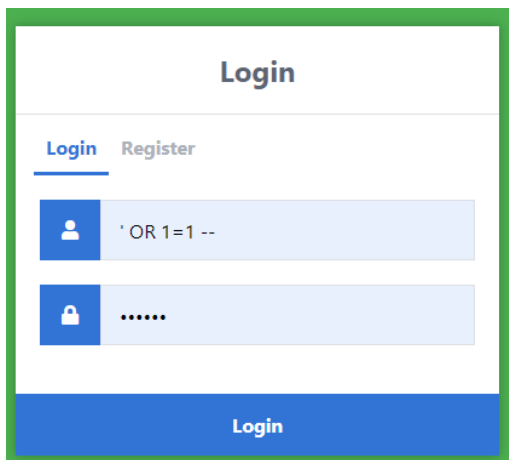
```
# Check if "username" and "password" POST requests exist (user submitted form)
if request.method == 'POST' and 'username' in request.form and 'password' in request.form:
    # Create variables for easy access
    username = request.form['username']
    password = request.form['password']
    # Check if account exists using MySQL
    cursor = db.cursor()
    cursor.execute('SELECT * FROM phone_directory_user WHERE username = %s', (username,))
    # Fetch one record and return result
    account = cursor.fetchone()
    user = User.get_by_username(username)
    # If account exists in accounts table in out database
    if user:
        if check_password_hash(user.password, password):
            login_user(user, remember=False)
            return redirect(url_for('home'))
        else:
            # Account doesnt exist or username/password incorrect
            msg = 'Incorrect password!'
    else:
        msg = 'User not found'
else:
    # If the user is already logged in, redirect to the home page
```

Attack 1:

(SQL Injection)

On providing username as 'OR 1=1 –, the query becomes SELECT * FROM phone_directory_user WHERE username = '' OR 1=1 –. This is always True. Hence the user can login without valid credentials. Since we have parameterized queries, it will show the message user not found.

Fig: SQL injection Attack 1

Fig: Screen after attempted login

Attack 2:
(XSS Attack)

Non-Persistent XSS using the input <script>alert('ATTACK')</script>

The search fields are used to search for tuples using the first name. Hence, we are only allowing alphabetic characters in our search field.

An attempt to execute the above statement will redirect the user to the "LOGIN" page after 3 seconds.

Fig: An attempt at creating a dialogue box by the user.
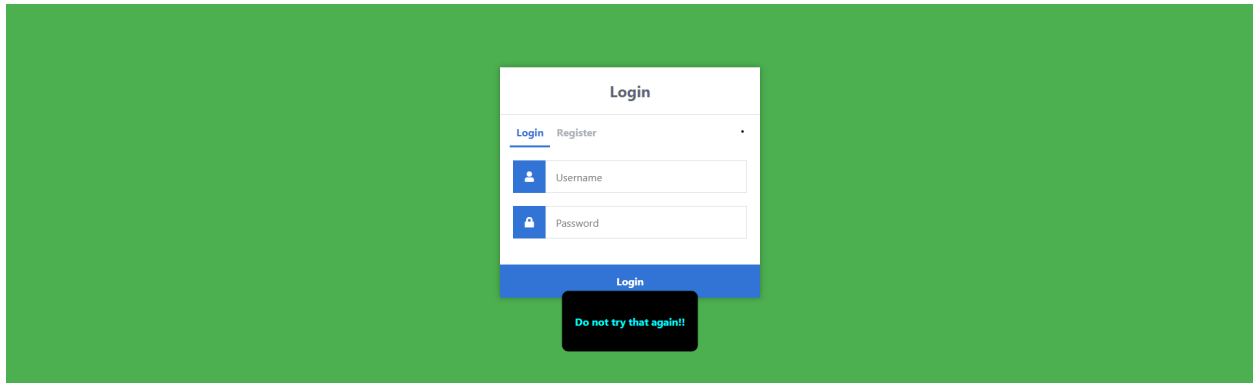
Fig: Screen after the attempted attack

```python
@app.route('/search', methods=['POST'])
@login_required
def search():
    table_name = request.form['table'].lower()
    # print(table_name)
    if not re.match(r'^[a-zA-Z]',request.form['search_input']):
        error = 'Do not try that again!!'
        flash(error)
        return render_template('login.html', error=error)
```

Attack 3: (Bonus Attack)

(SQL Injection)

SQL Injection using Batched SQL Statements:

A batch of statements are two or more SQL statements separated by a semicolon.

Faculty

Search: [Lucy; DROP TABLE faculty;] [Search]

ID	Name	Department
10861895	Lucy Goodwin	Biological Engineering
11643101	Jarett Hessel	Civil Engineering
12340912	Lauren Blick	Chemical Engineering
12340913	Nona Wehner	Computer Science and Engineering
12340914	Kailyn Kuhlman	Electrical Engineering

Fig: An attempt at using Batched statements to manipulate data with no edit access.

Faculty

Search: [_____] [Search]

ID	Name	Department
10861895	Lucy Goodwin	Biological Engineering
11643101	Jarett Hessel	Civil Engineering
12340912	Lauren Blick	Chemical Engineering
12340913	Nona Wehner	Computer Science and Engineering
12340914	Kailyn Kuhlman	Electrical Engineering

Fig: Unaltered database even after executing the query

2. Show that all the relations and their constraints, finalized after the second feedback, are present and valid as per the ER diagram constructed in Assignment 1. **(5 points)**

The relations and constraints this phone directory database follows are mentioned in the ER diagram during assignment 1. The ER diagram is attached at the end of section 3.3 for reference.
None of these constraints have been violated and neither of them needed any update while populating the database with data. The essence of primary key, foreign key, participation, and mapping cardinalities have been maintained.

For instance, let us consider the following relations and their corresponding constraints.
The relevance of the primary and foreign keys are still maintained.

    a. *council_advisor*

```
198   CREATE TABLE `council_advisor` (
199       `faculty_id` int DEFAULT NULL,
200       `council_name` varchar(30) NOT NULL,
201       PRIMARY KEY (`council_name`),
202       KEY `fk_council_faculty_ID` (`faculty_id`),
203       CONSTRAINT `fk_council_faculty_ID` FOREIGN KEY (`faculty_id`) REFERENCES `faculty` (`faculty_id`) on delete cascade,
204       CONSTRAINT `fk_council_faculty_name` FOREIGN KEY (`council_name`) REFERENCES `student_council` (`council_name`) on delete cascade
205   ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
```

The current database still ensures
I. One-to-One cardinality between *council* and *faculty*
II. Total Participation from *student_council* and Partial Participation from *faculty*

b. *student_council_member:*

```
878  CREATE TABLE `student_council_member` (
879      `student_id` int NOT NULL,
880      `council_name` varchar(30) DEFAULT NULL,
881      `position` varchar(30) DEFAULT NULL,
882      PRIMARY KEY (`student_id`,`council_name`),
883      KEY `fk_council_name` (`council_name`),
884      CONSTRAINT `fk_council_name` FOREIGN KEY (`council_name`) REFERENCES `student_council` (`council_name`) on delete cascade,
885      CONSTRAINT `fk_student_ID` FOREIGN KEY (`student_id`) REFERENCES `student` (`student_id`) on delete cascade
886  ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
```

The current database still ensures
I. Many-to-Many cardinality between *student* and *student_council*.
II. Total Participation from *student_council* and Partial Participation from *student*

c. *student_enrolled*

```
906  CREATE TABLE `student_enrolled` (
907      `student_id` int NOT NULL,
908      `program_name` varchar(30) DEFAULT NULL,
909      `start_year` int DEFAULT NULL,
910      `end_year` int DEFAULT NULL,
911      `dept_name` varchar(100) DEFAULT NULL,
912      PRIMARY KEY (`student_id`),
913      KEY `fk_dept_student_enrolled` (`dept_name`),
914      KEY `fk_program_enrolled` (`program_name`),
915      KEY `fk_prog_start_enrolled` (`start_year`),
916      KEY `fk_prog_end_enrolled` (`end_year`),
917      CONSTRAINT `fk_dept_student_enrolled` FOREIGN KEY (`dept_name`) REFERENCES `departments` (`dept_name`) on delete cascade,
918      CONSTRAINT `fk_prog_end_enrolled` FOREIGN KEY (`end_year`) REFERENCES `program` (`end_year`) on delete cascade,
919      CONSTRAINT `fk_prog_start_enrolled` FOREIGN KEY (`start_year`) REFERENCES `program` (`start_year`) on delete cascade,
920      CONSTRAINT `fk_program_enrolled` FOREIGN KEY (`program_name`) REFERENCES `program` (`program_name`) on delete cascade,
921      CONSTRAINT `fk_student_enrollemt` FOREIGN KEY (`student_id`) REFERENCES `student` (`student_id`) on delete cascade
922  ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
```

The current database still ensures
I. Many-to-One cardinality between *student* and *program*
II. Total Participation from both *student* and *program*

Entity-Relationship Diagram

The Github repository can be accessed from here: GitHub

Additional Feedback suggestions and justification for not implementing them:

a. Built-in back button on web page to move up one folder (i.e category) in the database. This is not needed at this stage as its relevance lies in the future when the database and website are scaled up.

b. Including photographs of people like faculty and staff in the database. This is relevant only at the time of deploying the database for the IITGN community as extensive data collection is needed.

c. Including LinkedIn and other relevant Social Media platform handles of faculty, clubs, and other services. Not implemented as data collection and verification needs lots of time and resources.

d. Developing the option of 'Forgot Password' on the login page. We did not implement it as the use case of this website does not need this at this point.

Contributions

Name	Group	Contributions
Aravind Krishna - 20110021	G1	8.33%
Arun Mani - 20110023	G1	8.33%
Hrishikesh CP -20110078	G1	8.33%
Mihika Jadhav - 20110113	G1	8.33%
Madhav Biswam -20110103	G1	8.33%
Rahul R Pai - 20120155	G1	8.33%
Shrija Agrawal - 20110197	G1	8.33%
Abhiram Geddam - 19110149	G2	8.33%
Kanishk Singh - 19110089	G2	8.33%
Ruthvik Mula - 19110124	G2	8.33%
Ninad Shah - 19110126	G2	8.33%
Prateek Kumar Jha - 19110159	G2	8.33%

Appendix

A1. The responses for feedback 1 by the stakeholders are as follows

Do you think the website is easy to use?

19 responses

- Yes
- No
- Maybe

94.7%
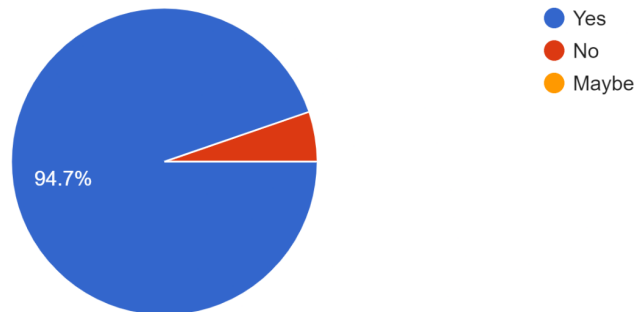
Do you think the website is useful?

19 responses

- Yes
- No
- Maybe

10.5%

84.2%
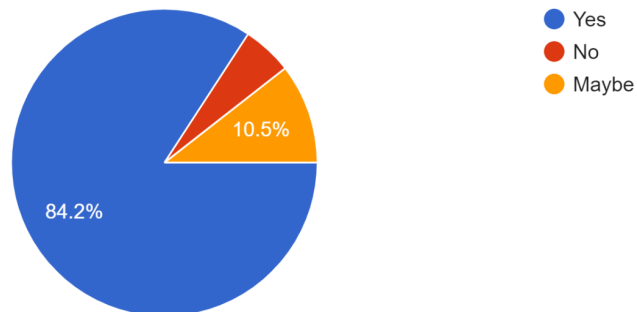
Any feature that is missing?

There should be a search option to access the names There should be a in built back button I don't think there is a need for home page if the only function of the pge is to access the phone directory.
Relocating to the webpage, if the logo is clicked.
Images should have included

Search for the required field
Maybe photograph of the person might help.
Options in case i forget the password
Search feature for easy use.
Search panel
Could may be include LinkedIn profile of profs and students. Rest almost all infos are available on the website.
back button, admin page who can insert delete,;... search , filter, sub section by year in alumni
Emails can be hyperlinked to mail
search function
A search feature for admins to find necessary rows.

What other features would you like to include in it? Please answer in detail

The search option- to access the names
A searching feature
Other social media handles could also help the user
There should be a search option and a back button.
Add forgot password
Search feature
Search panel can be included
Privacy Features
Maybe only show relevant info, not everything
There is enough information as of now.
Anyone with the site can create an account. There should a mechanism to stop that.
use boostrap... make website responsive
Could add pictures of designated person
search function has got to be a non negotiable component to save time and effort
1. authentication and separate views for faculty and students for privacy issues. 2. admin page to delete registered users or change authentication and access.

Suggest any changes in the UI or functions to make it user friendly.

Could make the options in tile format.(square)
Could incorporate more animations
Make the font easier to read and softwr
More graphics might make the website attractive
Colour combination could be better. The home page could have options in the center rather than the top since there is currently nothing in the center.
Better website navigation
Could be visually pleasing.
Design can be be improved
Search button
Could be more colourful and more interactive themes
There could be a background photo and maybe lighter colours.
maybe add icons to make look more attractive
The link to the telephone directory could be put below the welcome back message on the homepage
change the color maybe, increase font size on footer band
1. home page could be better designed with a path to follow rather than just links. 2. back buttons in every page. 3. directory display page could be made with cards instead of just columns.

Please mention any other comments or suggestions.

The website is good, but the looks can be better. I also hope that it can handle large numbers of users logging onto it.

Will the current version of our webapp, replace the deployed version we follow?
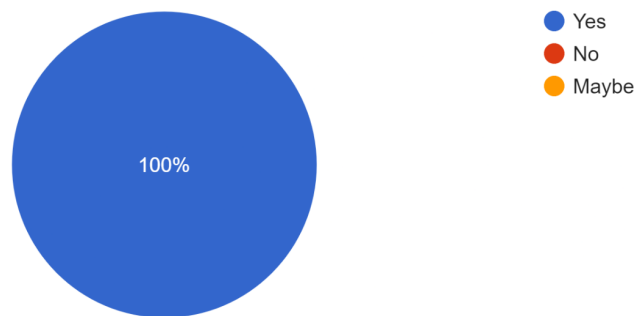19 responses
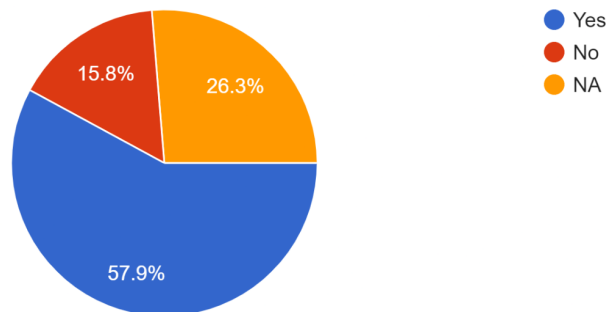
A2. The responses for feedback 2 by the stakeholders are as follows

Do you feel the web app is more user friendly than the previous version?
6 responses

Any feature that is still missing?

| Back Button, Home Page Cards |
| Back button |
| Forgot password option |
| Privacy features are still missing |

Please explain your previous answer briefly. It would be really helpful to us.

Back button to take us to previous page, there are only three options on home page it could be made into a card for better UI
Back buttons still not implemented
If the stakeholders misplaced their login credentials, they need to be able to retrieve it
The search bar is included and is helpful to fetch data
Everyone still has access to all phone numbers, there should be some limited accesses
Everything is included

Do you feel the changes you suggested were incorporated in the new design?

6 responses

- Yes
- No
- Maybe

33.3%

66.7%
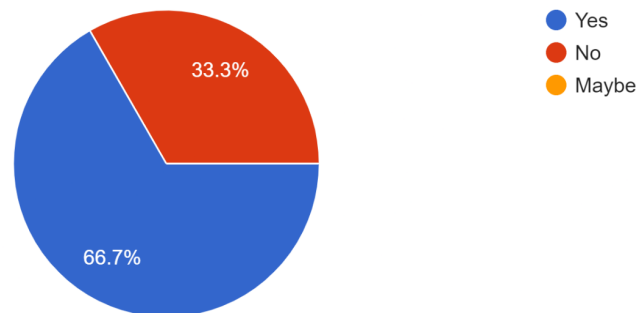
Please mention any other comments concerning the application.

overall better navigation with search button
Trying to include search based on department name in faculty would be helpful
A seperate link is created to navigate to home page, at the bottom of the page. It would be more comfortable if we would be able to navigate to home page through clicking the icon in the title as well

Will the current version of our webapp, replace the deployed version we follow?

6 responses

- Yes
- No
- NA

16.7%

83.3%