Beta Testing Document

for

ConnVerse

Version 1.0

Prepared by

Group 03: Group Name: MahaDevS

Aaditi Anil Agrawal	220006	aaditiaa22@iitk.ac.in
Arshit	220209	arshitsk22@iitk.ac.in
Chayan Kumawat	220309	chayank22@iitk.ac.in
Dobariya Jenil Bharatbhai	220385	dobariyajb22@iitk.ac.in
Harsh Agrawal	220425	harshag22@iitk.ac.in
Harshit	220436	harshit22@iitk.ac.in
Harshit Srivastava	220444	harshitsr22@iitk.ac.in
Naman Kumar Jaiswal	220687	namankj22@iitk.ac.in
Prem Kansagra	220816	premk22@iitk.ac.in
Priyanshu Singh	220830	spriyanshu22@iitk.ac.in

Course: CS253

Mentor TA: *Abhilash*

Date: 13th Apr 2024

Revisions

Version	Primary Author(s)	Description of Version	Date Completed
1.0	MahaDevs	Initialized the document and added the necessary details.	12/04/2024

1 Introduction

The specified software is a comprehensive project management website designed to streamline the project allocation process for students under professors at IIT Kanpur. The primary objective is to simplify and enhance the experience for students by providing a centralized platform where they can effortlessly explore a diverse range of projects offered by different professors. This platform enables students to master relevant skill sets within specific domains, gaining valuable exposure in the process.

The website facilitates a seamless interaction between students and professors, allowing students to send project requests with all the necessary credentials specified by the professors. Students can search for projects based on domains, specific professors, or branch-wise preferences On the professor's end, the software provides a unified platform for managing student requests, eliminating the need to sift through numerous emails. Professors can easily view a list of student requests, including relevant credentials such as CPI, resumes, and experience details.

Additionally, professors can communicate with all students simultaneously, keeping them informed about specific activities and posting materials to help them prepare for tests or interviews. Overall, the software aims to optimize project management workflows for both students and professors, saving time and enhancing collaboration within the academic community at IIT Kanpur.

2 List of Reported Bugs

BUG 1: Overflowing "Show More" Button for projects info block

Tested Feature: Projects section "Show More" Button

Description:

The "Show More" button in the user interface is overflowing its container, causing it to display incorrectly or in a non-functional manner. This issue affects the usability and aesthetics of the interface.

Tester Name: PREM

Testing Date: 03/04/2024

Bug Details:

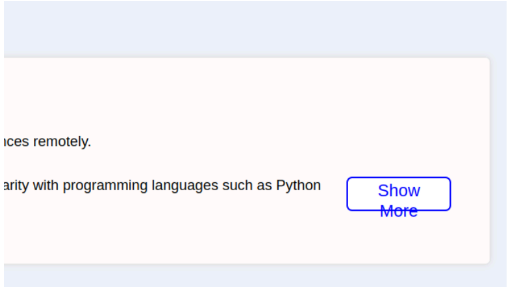
- Login to the application with your login details.
- Navigate to the Projects section of the interface and go to any project.
- Observe that the "Show More" button is overflowing its container or displaying improperly.

Bug Report Date: 06/04/2024

Has the bug been fixed? Yes

Date of Bug fixing: 12/04/2024

Any other comment : The issue is impacting the user experience significantly, as it affects both functionality and aesthetics. It is essential to address this promptly to enhance user satisfaction.



ıces remotely.

arity with programming languages such as Python

BUG 2: Inability to Request Multiple Projects in a Single Login Session

Tested Feature: Multiple Projects Request

Description: Currently, users are unable to request multiple projects in a single login session, which is causing inconvenience and inefficiency. Users expect to be able to request access to multiple projects without having to log in separately for each project.

Tester Name: Chayan

Testing Date: 04/04/2024

Bug Details:

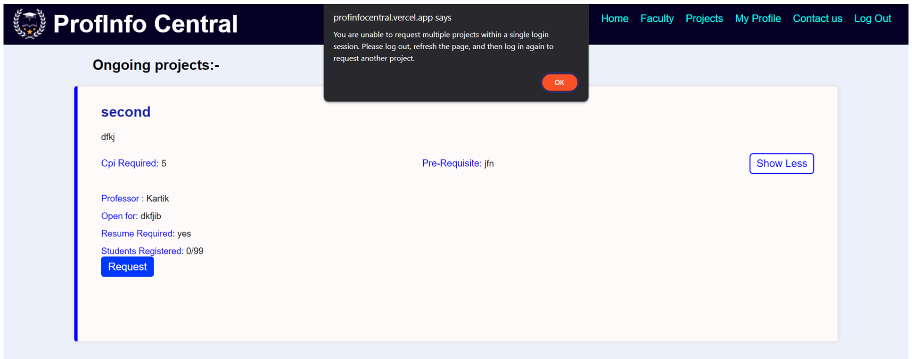
- Log in to the system.
- Attempt to request access to multiple projects within the same login session.
- Notice that the system does not provide an option or functionality to request multiple projects simultaneously.

Bug Report Date: 06/04/2024

Has the bug been fixed? Tried but not fixed

Date of Bug fixing: 12/04/2024

Any other comment : This bug significantly hampers user productivity and creates frustration by requiring users to perform repetitive actions for each project request. Implementing the ability to request multiple projects in a single login session is crucial for enhancing user experience and system efficiency.



profinfocentral.vercel.app says

You are unable to request multiple projects within a single login session. Please log out, refresh the page, and then log in again to request another project.

Ongoing projects:-

second

dfkj

Cpi Required: 5

Pre-Requisite: jfn

Professor : Kartik

Open for: dkfjib

Resume Required: yes

Students Registered: 0/99

BUG 3: Unauthorized Project Approval or Rejection

Tested Feature: Project Approval/Rejection

Description: Currently, a vulnerability exists in the backend system that allows any student to approve or reject project applications without proper authentication. This poses a significant security risk as unauthorized users can manipulate project approvals, potentially leading to unauthorized access or misuse of resources.

Tester Name: Arshit

Testing Date: 04/04/2024

Steps to Reproduce:

- Access the backend URL: https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/user/professor/approveproject/6608238793c73fbf7e42f788/220385
- Replace <6608238793c73fbf7e42f788> with the ID of the MERN stack project.
- Replace <220385> with the roll number of the student whose project application you want to approve.
- Notice that the project application is approved without proper professor authentication.
- Replace <approveproject> with <rejectproject> to reject the project**.**

Bug Details:

- **Expected Behavior:** Project approvals should only be allowed by professors with appropriate authentication credentials. Unauthorized users, including students, should not be able to approve or reject project applications.

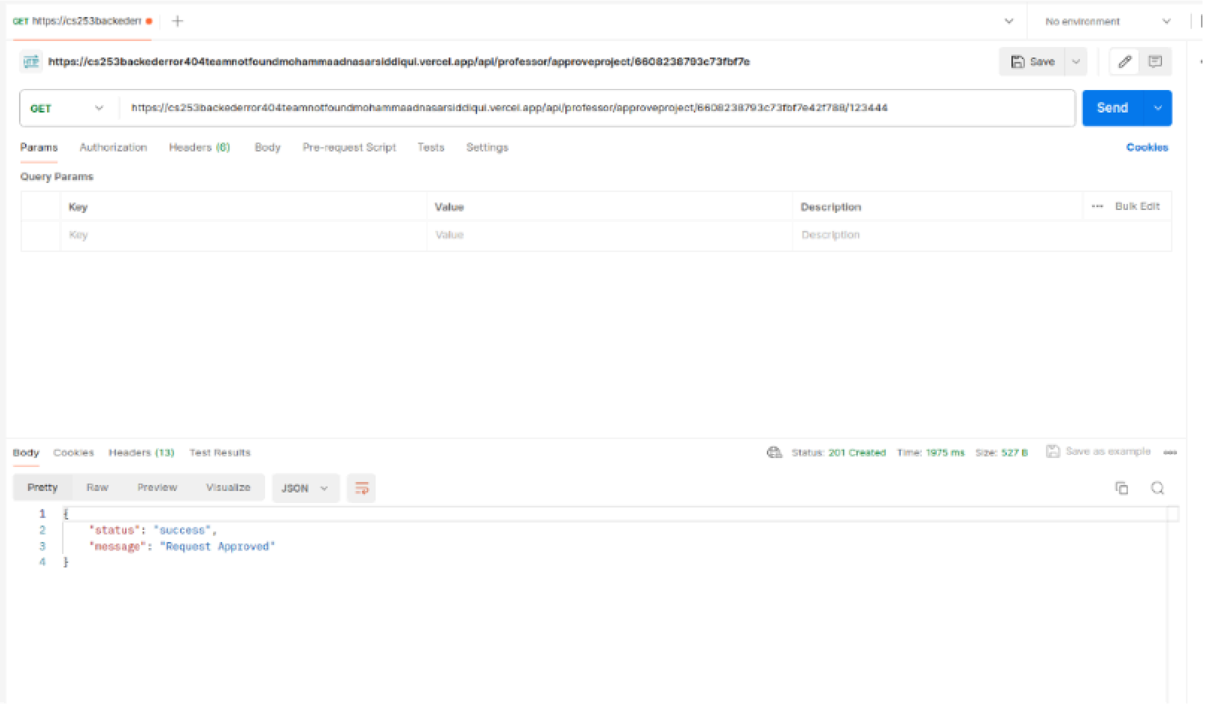
- **Actual Behavior:** Any student can manipulate project approvals or rejections by accessing the specific URL without proper authentication, compromising the security and integrity of the system.

Recommended Fix: Implement proper Middleware authentication and authorization checks to ensure that only authorized users, such as professors, can approve or reject project applications.

Bug Report Date: 06/04/2024

Has the bug been fixed? : Not Really

Date of Bug fixing: 10 Apr 2024



https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/professor/approveproject/6608238793c73fbf7e

GET https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/professor/approveproject/6608238793c73fbf7e42f788/123444

Status: 201 Created Time: 1975 ms Size: 527 B

```
{
    "status": "success",
    "message": "Request Approved"
}
```

BUG 4: Retain Student Request Status on Screen After Action

Tested Feature: Student project request management

Description:Currently, when a faculty member accepts or rejects a student's project request, the request is not immediately removed from the screen and just stays there, leading to confusion and clutter. This behavior does not provide a clear indication that the action has been taken and may cause misunderstanding.

Tester Name: **Chayan**

Testing Date: **03/04/2024**

Steps to Reproduce:

- Log in as a faculty member.
- Navigate to the section for managing projects. Open requests for the project.
- Accept or reject a student's project request.
- Observe that the request is still visible on the screen after the action is taken.

Bug Details:

- **Expected Behavior**: After accepting or rejecting a student's project request, the request should be immediately removed from the screen to maintain a clean and organized interface. However, a notification or visual indicator should confirm that the action has been processed successfully.
- **Actual Behavior**: Currently, after accepting or rejecting a student's project request, the request remains on the screen, leading to clutter and confusion. There is no clear indication that the action has been taken, which may cause misunderstanding among users.
- **Recommended Fix**:
  - Modify the system to immediately remove student project requests from the screen after accepting or rejecting them to maintain a clean interface.
  - Implement a notification or visual indicator to confirm to users that the action has been successfully processed.

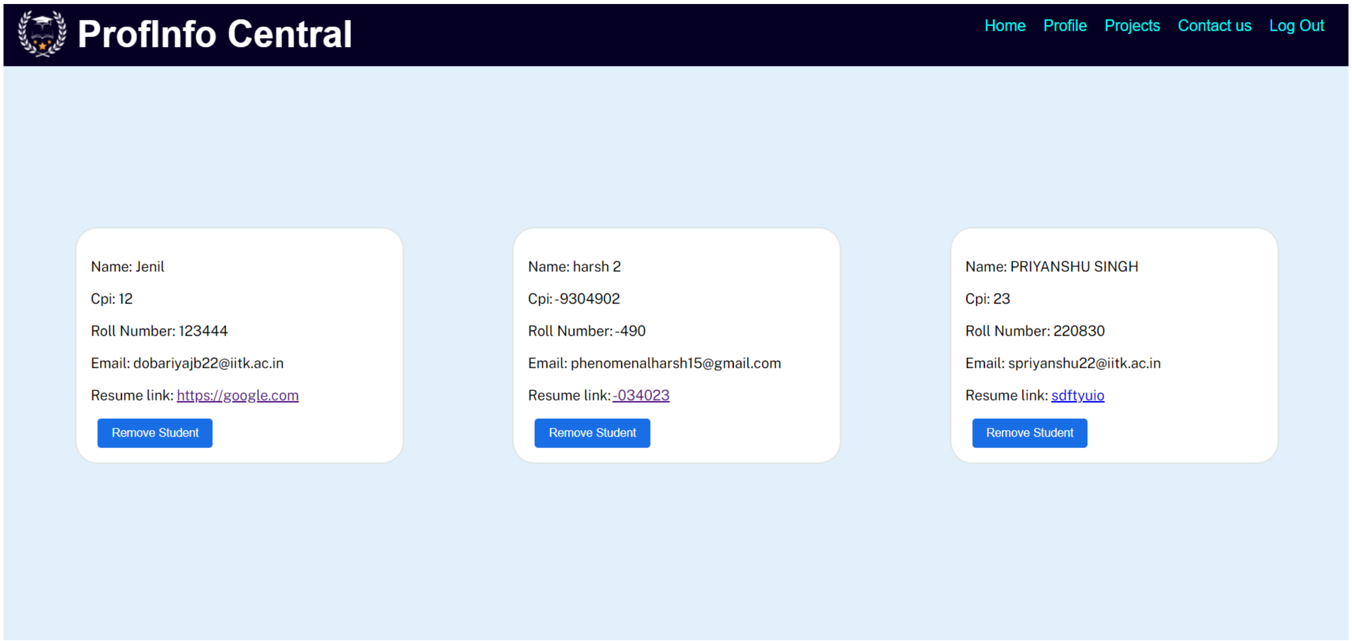
Bug Report Date: 06/04/2024

Has the bug been fixed? : Tried but not fixed

Date of Bug fixing : 11/04/2024

Additional Information:

Furthermore if we reject a student and then accept and then reject he stays accepted which is questionable.



Name: Jenil
Cpi: 12
Roll Number: 123444
Email: dobariyajb22@iitk.ac.in
Resume link: https://google.com

Name: harsh 2
Cpi: -9304902
Roll Number: -490
Email: phenomenalharsh15@gmail.com
Resume link: -034023

Name: PRIYANSHU SINGH
Cpi: 23
Roll Number: 220830
Email: spriyanshu22@iitk.ac.in
Resume link: sdftyuio

BUG 5: Duplicate Projects Shown and Saved

Tested Feature: **Duplicate Projects**

Description : When adding a new project, if the "Save" button is clicked multiple times due to high loading times, the project is saved multiple times, resulting in duplicate entries. The same project is shown multiple times in the interface, causing confusion and clutter.

Tester Name: **Jenil**

Testing Date: **03/04/2024**

Steps to Reproduce:

- Navigate to the section displaying projects.
- Attempt to add a new project.
- Click on the "Save" button multiple times due to high loading times.
- Notice that multiple instances of the same project are saved.

Bug Details:

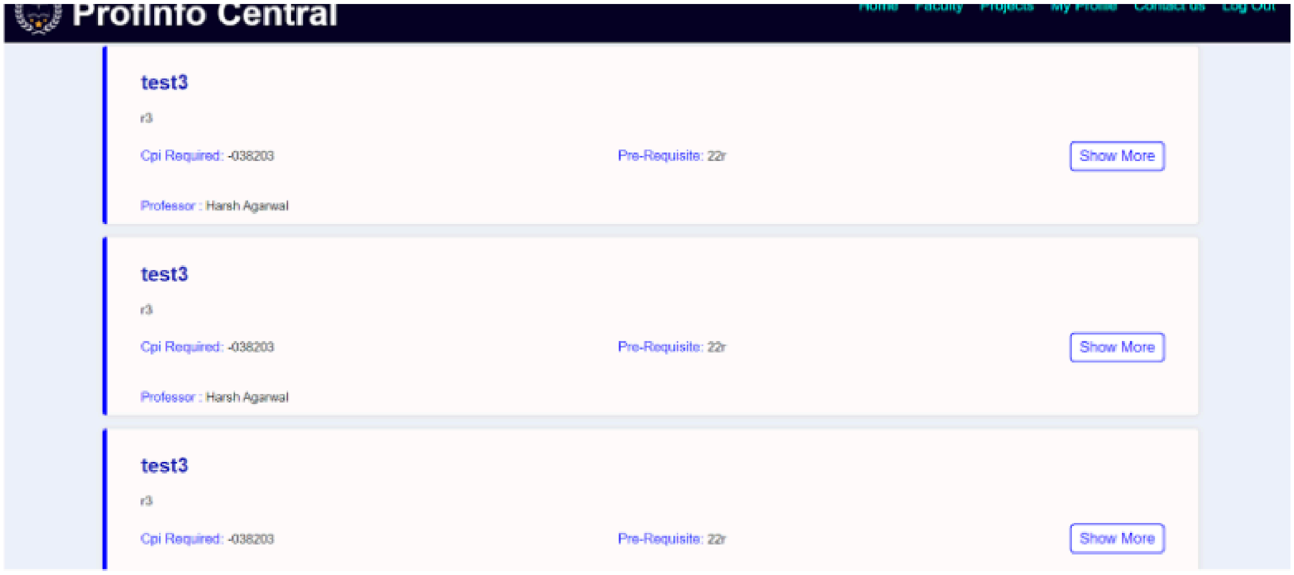
- **Expected Behavior:** Projects should be displayed only once in the interface, avoiding duplication and clutter. When adding a new project, clicking the "Save" button multiple times should not result in duplicate entries being saved.
- **Actual Behavior:** The same project is displayed multiple times in the interface, leading to confusion and clutter. Additionally, clicking the "Save" button multiple times during project addition results in duplicate entries being saved, which is undesirable.
- **Recommended Fix:**
  - Implement logic to prevent the display of duplicate projects in the interface.
  - Enhance the project addition process to handle multiple clicks on the "Save" button gracefully, ensuring that only one instance of the project is saved.

Bug Report Date: 06/04/2024

Has the bug been fixed?: **No**

Date of Bug fixing: 10/04/2024

Additional Information: This issue affects the usability and integrity of the system by cluttering the interface and creating duplicate entries in the database. Resolving this bug is crucial for providing a smooth and efficient user experience.



test3

r3

Cpi Required: -038203 Pre-Requisite: 22r

Professor : Harsh Agarwal

test3

r3

Cpi Required: -038203 Pre-Requisite: 22r

Professor : Harsh Agarwal

test3

r3

Cpi Required: -038203 Pre-Requisite: 22r

BUG 6: Infinite Loop When No Project Requests Exist

Tested Feature: **No Project Requests Exist**

Description : When a faculty member navigates to the "requests" section, an infinite loop occurs if there are no project requests present. This behavior disrupts the user experience and prevents faculty members from accessing other sections of the system.

Tester Name: **Harshit Srivastava**

Testing Date: **03/04/2024**

Steps to Reproduce:

- Log in as a faculty member.
- Navigate to the "requests" section.
- Observe that an infinite loop occurs if there are no project requests present.

Bug Details:

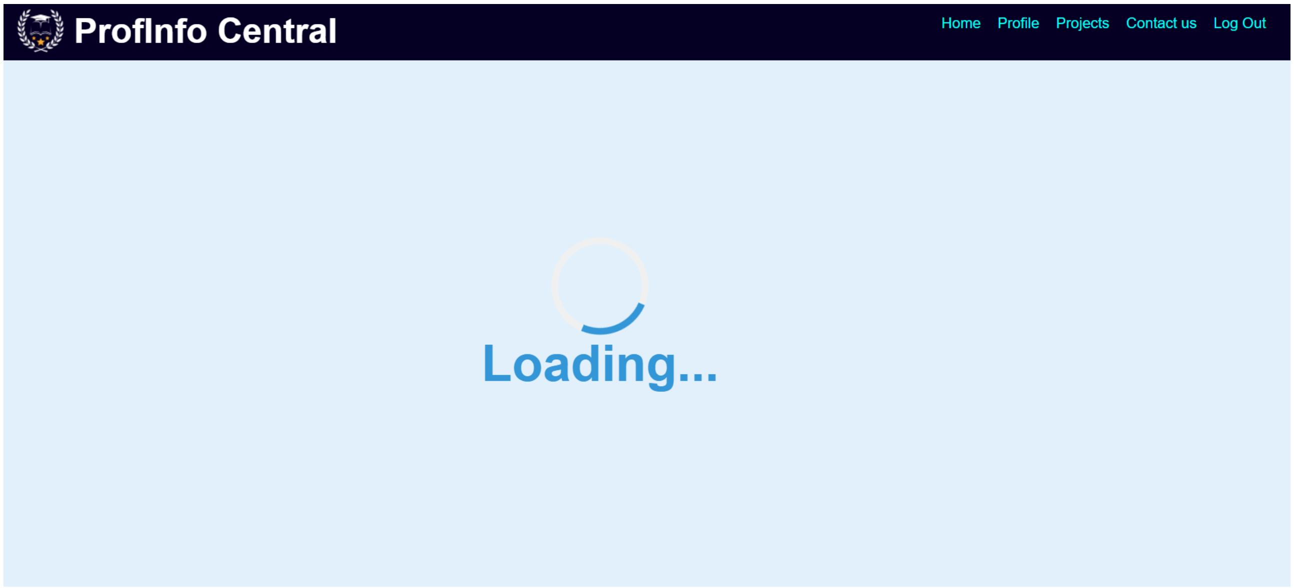
- **Expected Behavior:** When there are no project requests present, navigating to the "requests" section should display a message indicating the absence of requests, without causing an infinite loop.
- **Actual Behavior:** Navigating to the "requests" section when no project requests exist triggers an infinite loop, preventing faculty members from accessing other sections of the system and causing frustration.
- **Recommended Fix:**
    - Modify the system to handle the absence of project requests gracefully, displaying a message to the user instead of triggering an infinite loop.
    - Implement error handling mechanisms to prevent infinite loops and ensure a smooth user experience.

Bug Report Date : 06/04/2024

Has the bug been fixed? : Tried but not fixed

Date of Bug fixing : 11/04/2024

Additional Information: This issue severely impacts the usability of the system by rendering the "requests" section inaccessible when no project requests exist. Resolving this bug is essential for ensuring a seamless user experience for faculty members.



BUG 7: Overflowing Text in Project Description Causes UI Issues

Tested Feature: **UI Issues**

Description:When a large amount of text is added to the project description, it overflows from the project section, causing UI issues. Additionally, buttons for viewing enrolled students, project requests, and showing more information are missing, making it difficult to interact with the project.

Tester Name: **Priyanshu Singh**

Testing Date : 03/04/2024

Steps to Reproduce:

- Log in to the system as a faculty or a student.
- Navigate to the project section.
- Add a large amount of text to the project description.
- Observe that the text overflows from the project section.
- Notice that buttons for viewing enrolled students, project requests, and showing more information are missing.

Bug Details:

- **Expected Behavior:** The project description should be displayed within the project section without overflowing, even with a large amount of text. Additionally, buttons for interacting with the project, such as viewing enrolled students, project requests, and showing more information, should be accessible and visible.
- **Actual Behavior:** Adding a large amount of text to the project description causes it to overflow from the project section, leading to UI issues. Furthermore, important buttons for interacting with the project are missing, making it challenging to access relevant information and perform necessary actions.
- **Recommended Fix:**
    - Implement proper text wrapping or truncation to prevent overflowing of text in the project description.

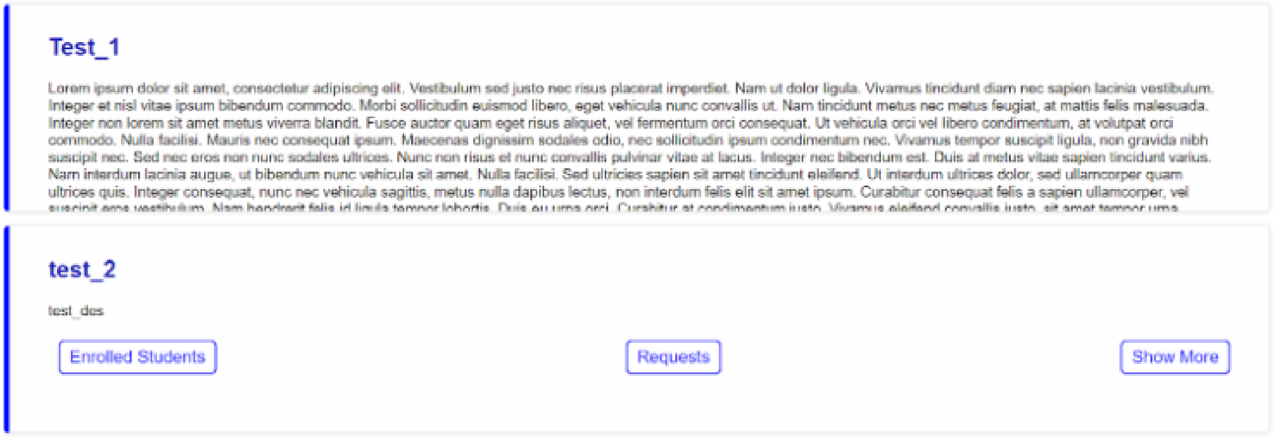
- Ensure that buttons for viewing enrolled students, project requests, and showing more information are visible and accessible, even with large amounts of text in the project description.

Bug Report Date : 06/04/2024

Has the bug been fixed? : Tried but not fixed

Date of Bug fixing : 10/04/2024

Additional Information: This issue negatively impacts the usability and accessibility of the system by making it difficult for users to interact with project information. Resolving this bug is crucial for ensuring a seamless user experience.



Test_1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum sed justo nec risus placerat imperdiet. Nam ut dolor ligula. Vivamus tincidunt diam nec sapien lacinia vestibulum. Integer et nisl vitae ipsum bibendum commodo. Morbi sollicitudin euismod libero, eget vehicula nunc convallis ut. Nam tincidunt metus nec metus feugiat, at mattis felis malesuada. Integer non lorem sit amet metus viverra blandit. Fusce auctor quam eget risus aliquet, vel fermentum orci consequat. Ut vehicula orci vel libero condimentum, at volutpat orci commodo. Nulla facilisi. Mauris nec consequat ipsum. Maecenas dignissim sodales odio, nec sollicitudin ipsum condimentum nec. Vivamus tempor suscipit ligula, non gravida nibh suscipit nec. Sed nec eros non nunc sodales ultrices. Nunc non risus et nunc convallis pulvinar vitae at lacus. Integer nec bibendum est. Duis at metus vitae sapien tincidunt varius. Nam interdum lacinia augue, ut bibendum nunc vehicula sit amet. Nulla facilisi. Sed ultricies sapien sit amet tincidunt eleifend. Ut interdum ultrices dolor, sed ullamcorper quam ultrices quis. Integer consequat, nunc nec vehicula sagittis, metus nulla dapibus lectus, non interdum felis elit sit amet ipsum. Curabitur consequat felis a sapien ullamcorper, vel suscipit eros vestibulum. Nam hendrerit felis id ligula tempor lobortis. Duis eu urna orci. Curabitur at condimentum justo. Vivamus eleifend convallis justo, sit amet tempor urna

test_2

test_des

BUG 8: Request Button Not Functional on Faculty Page

Tested Feature : **Request Button Not Functional**

Description : Clicking the request button through the faculty page does not trigger any response, rendering the button non-functional. This issue undermines the purpose of providing the button and hinders the ability of users to request projects.

Tester Name : Aaditi Agrawal

Testing Date : 03/04/2024

Steps to Reproduce:

- Log in to the system.
- Navigate to the faculty tab.
- Select a faculty - Harsh Agrawal (Test Faculty).
- Select a project associated with the faculty.
- Attempt to click the request button.
- Observe that the button does not trigger any response.

Bug Details:

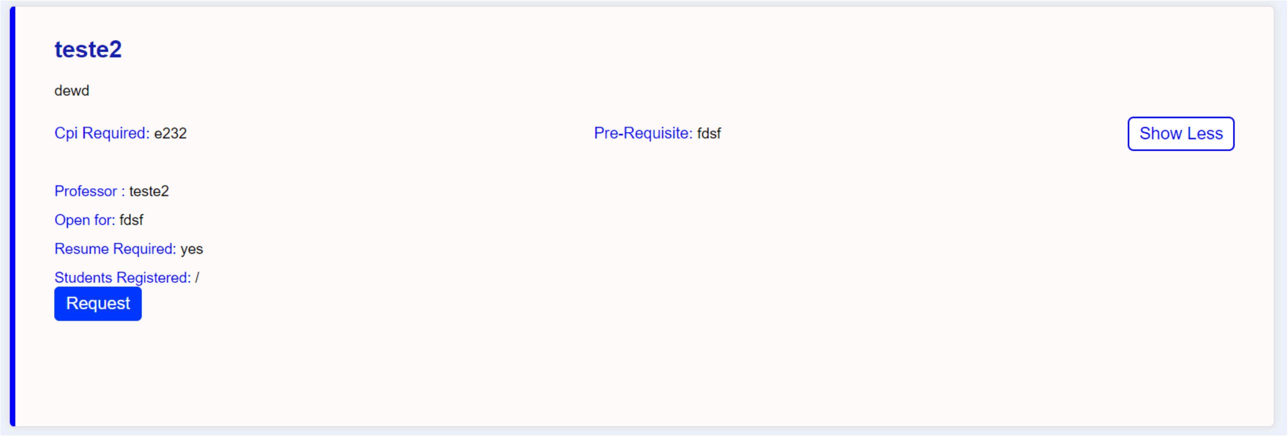
- **Expected Behavior:**Clicking the request button on the faculty page should initiate the process of requesting the selected project. Users should be able to interact with the button and request projects seamlessly..
- **Actual Behavior**: The request button on the faculty page does not respond to user clicks, making it impossible for users to request projects through this interface. This renders the button ineffective and frustrates users attempting to request projects.
- **Recommended Fix:**
  - Identify and resolve the underlying issue causing the request button to be non-functional on the faculty page.
  - Ensure that clicking the request button initiates the process of requesting the selected project as expected

Bug Report Date : 06/04/2024

Has the bug been fixed? : Tried but not fixed

Date of Bug fixing : 11/04/2024

Additional Information: This issue significantly impacts the usability and functionality of the system by preventing users from requesting projects through the faculty page. Resolving this bug is essential for providing a seamless and efficient user experience.



teste2

dewd

Cpi Required: e232

Pre-Requisite: fdsf

Professor : teste2

Open for: fdsf

Resume Required: yes

Students Registered: /

BUG 9: Unauthorized Project Request by Student

Tested Feature : Security Vulnerability

Description : There is a vulnerability in the backend system that allows a student to request a project on behalf of another student without proper authentication. This security flaw poses a significant risk as it allows unauthorized users to manipulate project requests, potentially leading to unauthorized access or misuse of resources.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name : Harsh Agrawal

Testing Date : 03/04/2024

Steps to Reproduce:

- Access the backend URL: https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/user/123444/requestproject/6608238793c73fbf7e42f788
- Replace <12344> with the roll number of the student making the request.
- Replace <6608238793c73fbf7e42f788> with the ID of the project.
- Notice that the project request is made without requiring proper authentication.

Bug Details:

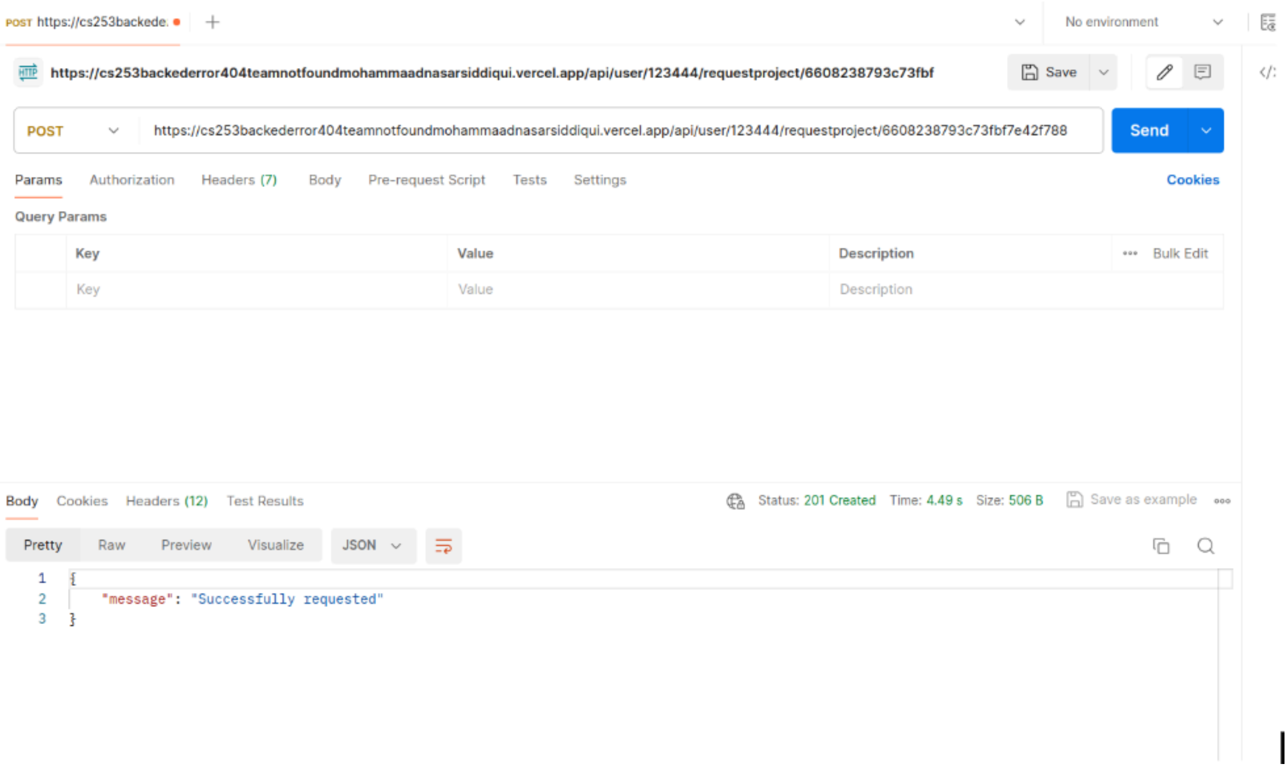
- **Expected Behavior:** Project requests should only be allowed by students after proper authentication. A student should not be able to request a project on behalf of another student without appropriate authorization.
- **Actual Behavior**: Any student can manipulate project requests by accessing the specific URL without proper authentication, compromising the security and integrity of the system.
- **Recommended Fix:**
    - Implement proper authentication and authorization checks to ensure that only authorized users can request projects.
    - Restrict access to the project request endpoint to authenticated students only.

Bug Report Date : 06/04/2024

Has the bug been fixed? : No

Date of Bug fixing : 10/04/2024

Additional Information : This can easily go into the direction of impersonation and spoiling the academic lineage of IIT Kanpur.



https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/user/123444/requestproject/6608238793c73fbf

POST https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/user/123444/requestproject/6608238793c73fbf7e42f788

Query Params

Key	Value	Description
Key	Value	Description

Status: 201 Created Time: 4.49 s Size: 506 B

```
{
    "message": "Successfully requested"
}
```

BUG 10 : Unauthenticated Project Deletion

Tested Feature : Security Vulnerability

Description : A project can be deleted by hitting the route https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/ap/professor/deleteproject/<project_id> without requiring any authentication. This vulnerability poses a significant security risk as it allows unauthorized users to delete projects without proper authorization.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name : Harshit Chikara

Testing Date : 03/04/2024

Steps to Reproduce:

- Access the specified route: https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/ap/professor/deleteproject/<project_id>.
- Replace <project_id> with the _id of any project.
- Notice that the project is deleted without requiring any authentication.

Bug Details:

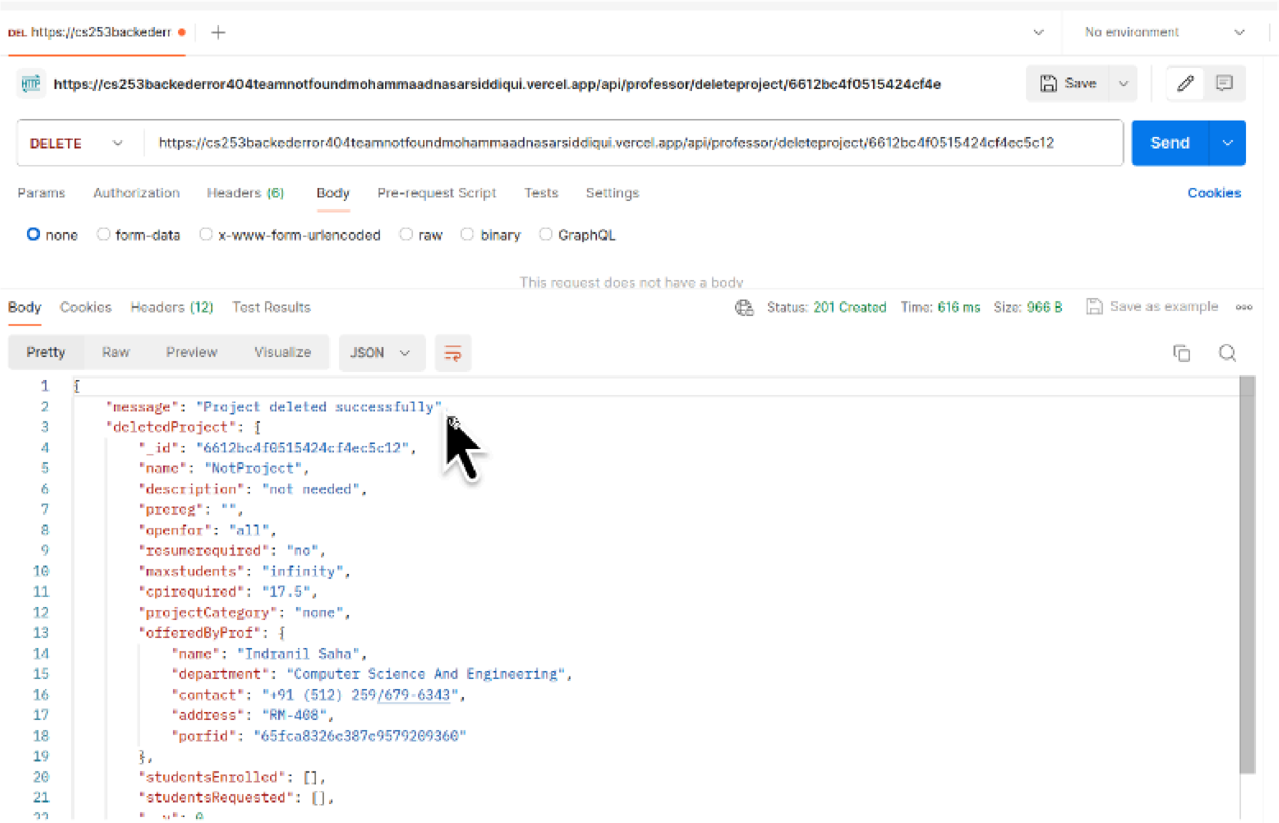
- **Expected Behavior:** Project deletion should only be allowed for authenticated users with the necessary permissions. Unauthorized users should not be able to delete projects.
- **Actual Behavior**: Unauthorized users can delete projects by simply accessing the specified route without any authentication, compromising the security of the system.
- **Recommended Fix:**
  - Implement proper authentication and authorization checks to ensure that only authorized users can delete projects.
  - Restrict access to the project deletion route to authenticated users with appropriate permissions.

Bug Report Date : 06/04/2024

Has the bug been fixed? : No

Date of Bug fixing : 11/04/2024

Additional Information: This security vulnerability poses a significant risk to the integrity and security of the system by allowing unauthorized users to delete projects. Resolving this issue is crucial for ensuring the confidentiality and integrity of project data.



https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/professor/deleteproject/6612bc4f0515424cf4e

DELETE https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/professor/deleteproject/6612bc4f0515424cf4ec5c12

Body: ● none

This request does not have a body

Status: 201 Created Time: 616 ms Size: 966 B

```
{
    "message": "Project deleted successfully",
    "deletedProject": {
        "_id": "6612bc4f0515424cf4ec5c12",
        "name": "NotProject",
        "description": "not needed",
        "prereg": "",
        "openfor": "all",
        "resumerequired": "no",
        "maxstudents": "infinity",
        "cpirequired": "17.5",
        "projectCategory": "none",
        "offeredByProf": {
            "name": "Indranil Saha",
            "department": "Computer Science And Engineering",
            "contact": "+91 (512) 259/679-6343",
            "address": "RM-408",
            "porfid": "65fca8326c387c9579209360"
        },
        "studentsEnrolled": [],
        "studentsRequested": [],
        "__v": 0
```

BUG 11 : Unauthenticated Project Creation

Tested Feature : Security Vulnerability

Description:

Students can create projects by hitting the route https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/professor/isaha/createproject without any verification. Additionally, professors can create projects on behalf of other professors by hitting the same route with the mentor's ID. This vulnerability allows unauthorized users to create projects without proper authentication or verification.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name : Naman Jaiswal

Testing Date : 03/04/2024

Steps to Reproduce :

- Notice that the project is deleted without requiring any authentication.
- Access the specified route: https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/professor/isaha/createproject.
- Replace isaha with the ID (username from email) of the mentor for the project.
- Notice that the project is created without requiring any authentication or verification.

Bug Details:

- **Expected Behavior:** Project creation should only be allowed for authenticated users with the necessary permissions. Additionally, professors should not be able to create projects on behalf of other professors without proper authorization.
- **Actual Behavior**: Unauthorized users, including students and professors, can create projects by accessing the specified route without any authentication or verification, compromising the security and integrity of the system.
- **Recommended Fix:**

- ○ Implement proper authentication and authorization checks to ensure that only authorized users can delete projects.

- ○ Restrict access to the project deletion route to authenticated users with appropriate permissions.

Bug Report Date : 06/04/2024

Has the bug been fixed? : No

Date of Bug fixing : 10/04/2024

Additional Information: This security vulnerability poses a significant risk to the integrity and security of the system by allowing unauthorized users to delete projects. Resolving this issue is crucial for ensuring the confidentiality and integrity of project data.

BUG 12 : Infinite Requests on Faculty Projects Page

Tested Feature: Security Vulnerability

Description:

When navigating to the faculty projects page, an infinite number of requests are made to the route https://cs253backederror404teamnotfoundmohammaadnasarsiddiqui.vercel.app/api/user/faculty/wiley01516, where wiley01516 is the faculty's username. This behavior results in excessive network traffic and impacts the performance of the application.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name : Priyanshu

Testing Date: 03/04/2024

Steps to Reproduce:

- Log in to the system.
- Navigate to the faculty projects page.
- Open the browser's network tab or inspect the page's requests.
- Observe continuous requests being made to the specified route.

Bug Details:

- **Expected Behavior:** Navigating to the faculty projects page should result in a single request being made to fetch the necessary data for displaying the projects. Subsequent requests should not occur unless explicitly triggered by user actions.
- **Actual Behavior**: Continuous requests are made to the specified route when navigating to the faculty projects page, resulting in an infinite loop of requests and impacting the performance of the application.
- **Recommended Fix:**
    - Implement proper authentication and authorization checks to ensure that only authorized users can delete projects.
    - Restrict access to the project deletion route to authenticated users with appropriate permissions.

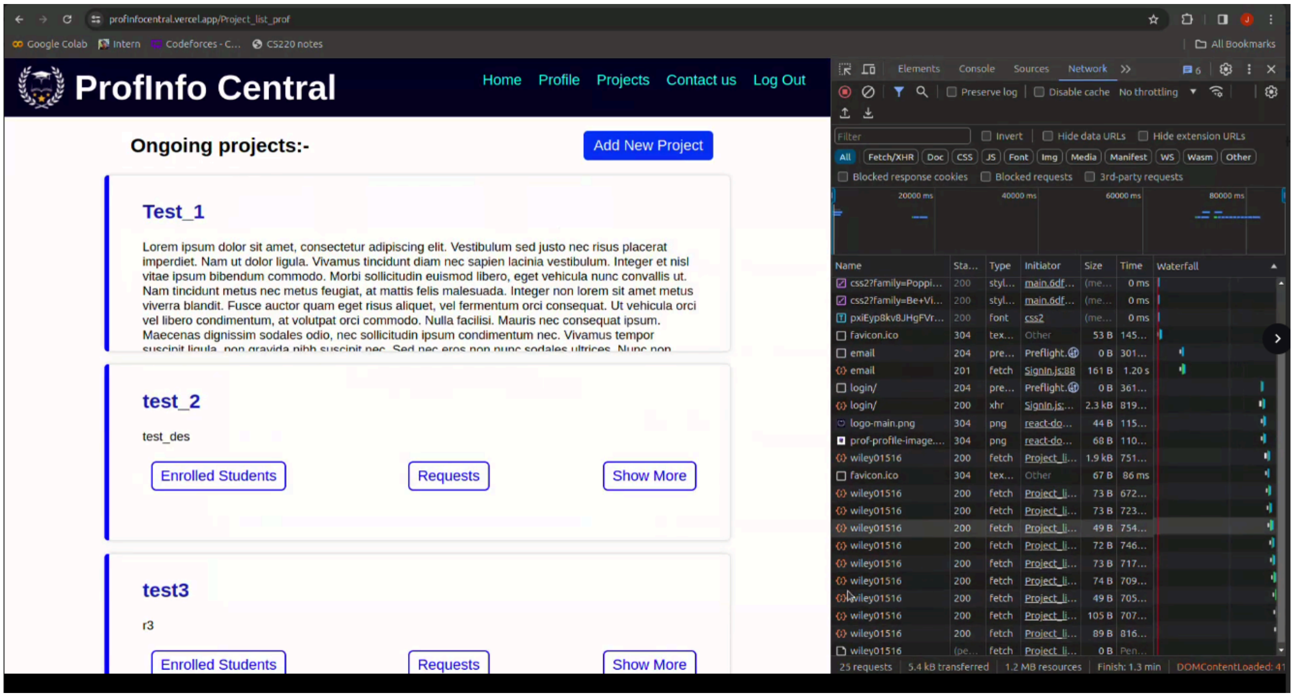
Bug Report Date : 06/04/2024

Has the bug been fixed? : No

Date of Bug fixing : 11/04/2024

Additional Information: This frontend bug negatively impacts the performance and user experience of the application by causing excessive network traffic and potential slowdowns. Resolving this issue is essential for ensuring optimal performance and usability.

BUG Demo Video: video



Ongoing projects:-

Test_1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum sed justo nec risus placerat imperdiet. Nam ut dolor ligula. Vivamus tincidunt diam nec sapien lacinia vestibulum. Integer et nisl vitae ipsum bibendum commodo. Morbi sollicitudin euismod libero, eget vehicula nunc convallis ut. Nam tincidunt metus nec metus feugiat, at mattis felis malesuada. Integer non lorem sit amet metus viverra blandit. Fusce auctor quam eget risus aliquet, vel fermentum orci consequat. Ut vehicula orci vel libero condimentum, at volutpat orci commodo. Nulla facilisi. Mauris nec consequat ipsum. Maecenas dignissim sodales odio, nec sollicitudin ipsum condimentum nec. Vivamus tempor suscipit ligula, non gravida nibh suscipit nec. Sed nec eros non nunc sodales ultrices. Nunc non

test_2

test_des

test3

r3

Name	Sta...	Type	Initiator	Size	Time
css2?family=Poppi...	200	styl...	main.6df...	(me...	0 ms
css2?family=Be+Vi...	200	styl...	main.6df...	(me...	0 ms
pxiEyp8kv8JHgFVr...	200	font	css2	(me...	0 ms
favicon.ico	304	tex...	Other	53 B	145...
email	204	pre...	Preflight.	0 B	301...
email	201	fetch	SignIn.js:88	161 B	1.20 s
login/	204	pre...	Preflight.	0 B	361...
login/	200	xhr	SignIn.js:...	2.3 kB	819...
logo-main.png	304	png	react-do...	44 B	115...
prof-profile-image....	304	png	react-do...	68 B	110...
wiley01516	200	fetch	Project_li...	1.9 kB	751...
favicon.ico	304	tex...	Other	67 B	86 ms
wiley01516	200	fetch	Project_li...	73 B	672...
wiley01516	200	fetch	Project_li...	73 B	723...
wiley01516	200	fetch	Project_li...	49 B	754...
wiley01516	200	fetch	Project_li...	72 B	746...
wiley01516	200	fetch	Project_li...	73 B	717...
wiley01516	200	fetch	Project_li...	74 B	709...
wiley01516	200	fetch	Project_li...	49 B	705...
wiley01516	200	fetch	Project_li...	105 B	707...
wiley01516	200	fetch	Project_li...	89 B	816...
wiley01516	(pe...	fetch	Project_li...	0 B	Pen...

25 requests | 5.4 kB transferred | 1.2 MB resources | Finish: 1.3 min | DOMContentLoaded: 41

BUG 13 : Unable to Delete Student After Approval

Tested Feature: Security Vulnerability

Description :

After a faculty member approves a student for a project, they are unable to delete the student despite the presence of a delete option. Clicking the delete button does not trigger any action, rendering it non-functional and preventing faculty members from managing project enrollments effectively.

Vulnerability Type :

- Lack of access controls
- Authentication bypass

Tester Name : Chayan

Testing Date : 03/04/2024

Steps to Reproduce :

- Log in as a faculty member.
- Approve a student for a project.
- Attempt to delete the approved student.
- Click the delete button.
- Observe that the button does not trigger any action.

Bug Details:

- **Expected Behavior:** Faculty members should be able to delete students from a project after approving them, using the delete option provided. Clicking the delete button should initiate the process of removing the student from the project.
- **Actual Behavior**:Despite the presence of a delete option, clicking the delete button after approving a student does not trigger any action. Faculty members are unable to delete students from projects, hindering their ability to manage project enrollments effectively.
- **Recommended Fix:**
  - Identify and resolve the underlying issue causing the delete button to be non-functional after approving a student for a project.
  - Ensure that clicking the delete button initiates the process of removing the student from the project as expected.

Bug Report Date: 06/04/2024

Has the bug been fixed? : No

Date of Bug fixing : 10/04/2024

Additional Information: This issue significantly impacts the usability and functionality of the system by preventing faculty members from managing project enrollments effectively. Resolving this bug is essential for ensuring a seamless user experience.

BUG 14 : No Method to Register as Faculty and Lack of Contact Information for Developers

Tested Feature: Security Vulnerability

Description:

There is currently no method provided for registering as a faculty member, and attempting to contact the developers for assistance yields no results as there is no contact information available before the login. This lack of registration method and absence of contact information make it virtually impossible for faculty members to join the application, hindering its usability and adoption.

Vulnerability Type :

- Lack of access controls
- Authentication bypass

Tester Name : Aaditi Agrawal

Testing Date : 03/04/2024

Steps to Reproduce:

- Attempt to register as a faculty member.
- Notice that there is no method available for faculty registration.
- Attempt to contact the developers for assistance.
- Observe that there is no contact information provided

Bug Details:

- **Expected Behavior**: Faculty members should be provided with a method for registering on the application, allowing them to join and utilize its features effectively. Additionally, contact information for reaching out to the developers should be available for users requiring assistance.
- **Actual Behavior**:There is no method provided for faculty registration, and attempting to contact the developers yields no results as there is no contact information available. This lack of registration method and absence of contact information make it impossible for faculty members to join and use the application.
- **Recommended Fix:**
    - Implement a dedicated registration method or form for faculty members to register on the application.

  - Provide clear and accessible contact information for users to reach out to the developers for assistance or inquiries.

Bug Report Date : 06/04/2024

Has the bug been fixed? : Tried but not fixed

Date of Bug fixing : 11/04/2024

Additional Information: The absence of a registration method for faculty members and lack of contact information for developers severely hinder the usability and adoption of the application. Resolving this issue is crucial for ensuring that the software can be effectively utilized by faculty members.

BUG 15 : Lack of Protection Against Script-Based Attacks

Tested Feature: Security Vulnerability

Description:

The application currently lacks protection mechanisms such as reCAPTCHA or Cloudflare to mitigate script-based attacks. This vulnerability exposes the server to potential denial-of-service (DoS) attacks, where malicious actors can overload the server with excessive requests, leading to downtime and service disruption.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name: Arshit

Testing Date: 03/04/2024

Steps to Reproduce:

- Access the application without any protection mechanisms in place.
- Initiate script-based attacks, such as sending a high volume of requests within a short period.
- Observe the server's response to the excessive load.

Bug Details:

- **Expected Behavior**: The application should be equipped with protection mechanisms, such as reCAPTCHA or Cloudflare, to mitigate script-based attacks and prevent server overload. These mechanisms should enforce rate limiting and request validation to ensure the server's stability and availability.
- **Actual Behavior**: Due to the absence of protection mechanisms, the application is vulnerable to script-based attacks, allowing malicious actors to overload the server with excessive requests and potentially disrupt its operation.
- **Recommended Fix:**
    - Implement reCAPTCHA or Cloudflare to provide protection against script-based attacks.
    - Configure rate limiting and request validation to mitigate the impact of malicious traffic on the server.

- Monitor server logs for suspicious activity and implement proactive measures to mitigate attacks.

Bug Report Date: 06/04/2024

Has the bug been fixed?: **No**

Date of Bug fixing: 11/04/2024

Additional Information: This security vulnerability poses a significant risk to the availability and stability of the application by exposing it to potential denial-of-service attacks. Resolving this issue is crucial for ensuring the continued operation and reliability of the server.

BUG 16 : Profile Not Updating After Requesting a Project

Tested Feature: Security Vulnerability

Description:

After requesting a project, the user's profile does not update to reflect the change. This issue prevents users from accurately tracking their project requests and may lead to confusion regarding the status of their requests.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name: Prem

Testing Date: 03/04/2024

Steps to Reproduce:

- Go to the projects tab.
- Select a project.
- Click the request button to request the project.
- Navigate to the profile tab.
- Observe that the profile does not show the updated project request.

Bug Details:

- **Expected Behavior**: After requesting a project, the user's profile should update to reflect the change, displaying the requested project and its status. This allows users to track their project requests accurately.
- **Actual Behavior**: The profile does not update after requesting a project, failing to reflect the user's recent activity and project requests. This inconsistency may lead to confusion and difficulty in tracking project requests.
- **Recommended Fix:**
    - Implement logic to update the user's profile after requesting a project, ensuring that the requested project is accurately displayed.
    - Verify that the necessary data is being correctly updated in the backend database upon project request.

Bug Report Date: 06/04/2024

Has the bug been fixed?: **Not Really**

Date of Bug fixing:

Additional Information: This bug affects the user experience by preventing users from accurately tracking their project requests through their profile. Resolving this issue is essential for providing a seamless and intuitive user experience.

BUG 17: Remove Redundant "Register New Student" Option Below Faculty Login and add "Register New Faculty"

Tested Feature: UI Improvement

Description:

When logging in as a faculty member, the option for registering a new student is displayed below the faculty login, similar to the option below the student login. However, clicking this option still registers another student, which is redundant and serves no purpose for faculty members. This UI element takes up unnecessary space and should be removed to streamline the login interface for faculty members.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name: **Priyanshu**

Testing Date: 03/04/2024

Steps to Reproduce:

- Visit the login page.
- Select the option to log in as a faculty member.
- Observe the presence of the "Register New Student" option below the faculty login.

Bug Details:

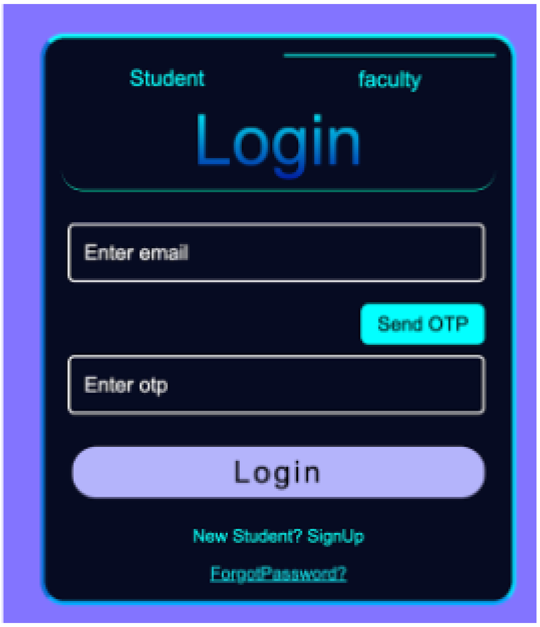
- **Expected Behavior**: The UI should be Relevant Minimalistic and never feel over the top or bare minimum. The UI can surely be improved for the best by first of all using the same styling for Register Option in Student and Faculty. Furthermore, adding "Register new Faculty" option should be added in its correct place.
- **Recommended Fix:**
  - Remove the "Register New Student" option from the interface below the faculty login to avoid confusion and streamline the login process for faculty members.
  - Ensure that the interface only displays relevant options and actions based on the user's role and context.

Bug Report Date: 06/04/2024

Has the bug been fixed?: Tried but not fixed

Date of Bug fixing:

Additional Information: Removing the redundant "Register New Student" option from the faculty login interface will improve usability and clarity for faculty members. This UI improvement enhances the overall user experience and reduces unnecessary clutter in the interface.



BUG 18 : Lack of Error Message for Faculty with No Ongoing Projects

Tested Feature: UI Error

Description:

When selecting a faculty member from the faculty tab who has no ongoing projects, the user is presented with a blank screen. There is no error message indicating that the faculty member does not have any ongoing projects, leading to confusion for the user. This lack of feedback makes it difficult for users to understand why no projects are displayed and may leave in frustration.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name: Harshit Chikara

Testing Date: 03/04/2024

Steps to Reproduce:

- Go to the faculty tab.
- Select a faculty member who has no ongoing projects.
- Observe the blank screen displayed without any error message.

Bug Details:

- **Expected Behavior**: When selecting a faculty member with no ongoing projects, the interface should display an error message indicating that the faculty member does not have any ongoing projects. This provides clear feedback to the user and helps prevent confusion.
- **Actual Behavior**: Upon selecting a faculty member with no ongoing projects, the interface displays a blank screen without any error message. This lack of feedback makes it difficult for users to understand why no projects are displayed and may lead to confusion.
- **Recommended Fix:**
    - Implement logic to display an error message when selecting a faculty member with no ongoing projects, indicating that the faculty member does not have any ongoing projects as of now.

  - Ensure that the error message is prominently displayed to the user to prevent confusion and frustration.

Bug Report Date: 06/04/2024

Has the bug been fixed?: **Tried but not fixed**

Date of Bug fixing: 10/04/2024

Additional Information: Providing clear and informative error messages enhances the user experience by guiding users through the interface and helping them understand the system's behavior. Resolving this UI error will improve usability and prevent user confusion.

BUG 19 : Lack of Definite Ordering and Search Option in Faculty Tab

Tested Feature: UI Error

Description:

The faculty tab lacks a definite ordering of faculty members, and there is no search option available to easily find specific faculty members. This oversight makes it challenging for users to navigate through the list of faculty members efficiently and locate the desired faculty member. Providing a definite ordering and implementing a search option would greatly enhance the usability and user experience of the faculty tab.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name: Aaditi Agrawal

Testing Date: 03/04/2024

Steps to Reproduce:

- Navigate to the faculty tab.
- Observe the absence of a definite ordering of faculty members.
- Attempt to search for a specific faculty member using a search option.
- Notice that there is no search option available.

Bug Details:

- **Expected Behavior**: The faculty tab should display faculty members in a definite ordering, such as alphabetical order or based on relevance. Additionally, a search option should be available to allow users to quickly find specific faculty members by name or other relevant criteria.
- **Actual Behavior**: The faculty tab lacks a definite ordering of faculty members, making it challenging for users to navigate through the list. Furthermore, there is no search option available to facilitate the quick identification of specific faculty members.
- **Recommended Fix:**
  - Implement logic to order faculty members in a definite manner, such as alphabetical order or based on relevance.

- Introduce a search option that allows users to search for specific faculty members by name or other relevant criteria.

Bug Report Date: 06/04/2024

Has the bug been fixed?: Tried but not fixed

Date of Bug fixing: 11/04/2024

Additional Information: Providing a definite ordering and search option in the faculty tab improves the usability and user experience by enabling users to navigate through the list of faculty members more efficiently. This UI enhancement enhances the overall usability of the application.

BUG 20 : Lack of Error Handling for Invalid Inputs in Login and Signup

Tested Feature: UI Error

Description:

The login and signup forms lack proper error handling for invalid inputs. When users provide invalid or incorrect input data, such as an invalid email format or a password that does not meet the requirements, the system fails to provide appropriate error messages to guide users on the correct input format. This lack of error handling makes it difficult for users to identify and correct input errors, leading to frustration and usability issues.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name: **Chayan**

Testing Date: **03/04/2024**

Steps to Reproduce:

- Attempt to log in or sign up with invalid input data, such as an invalid email format or a password that does not meet the requirements.
- Submit the form with the invalid input data.
- Observe the absence of error messages indicating the invalid input fields and guiding users on the correct input format.

Bug Details:

- **Expected Behavior**: When users provide invalid input data in the login or signup forms, the system should display clear and informative error messages indicating the invalid input fields and providing guidance on the correct input format. This helps users identify and correct input errors, improving the overall user experience..
- **Actual Behavior**: The login and signup forms lack proper error handling for invalid inputs, failing to provide error messages when users submit invalid input data. This lack of feedback makes it challenging for users to identify and correct input errors, leading to frustration and usability issues
- **Recommended Fix:**

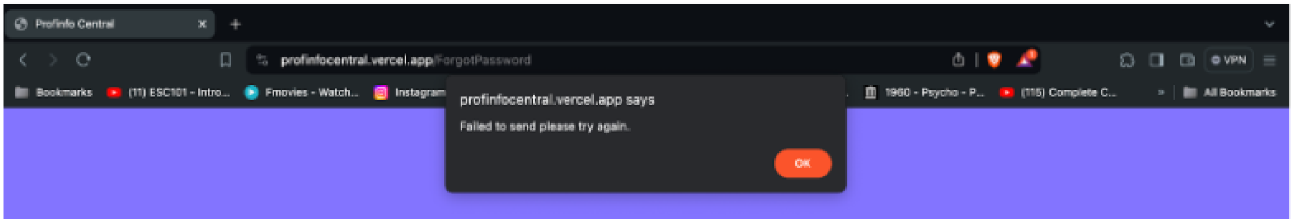
- ○ Implement validation logic in the login and signup forms to detect invalid input data, such as invalid email formats or passwords that do not meet the requirements.
- ○ Display clear and informative error messages when users submit invalid input data, indicating the invalid input fields and providing guidance on the correct input format.

Bug Report Date: 06/04/2024

Has the bug been fixed? : **No**

Date of Bug fixing: 11/04/2024

Additional Information: Proper error handling for invalid inputs is essential for guiding users through the login and signup process and ensuring a smooth and frustration-free user experience. Resolving this issue will improve the usability and effectiveness of the login and signup forms.



profinfocentral.vercel.app says

Failed to send please try again.

This message is blank and unhelpful giving us no insight over what to do to fix the error on the user side.

BUG 21 : Profile Creation Page Collapses on Invalid Input, Requiring User to Refill Form

Tested Feature: Bug on 2.0 version

Description:

When a user provides invalid input on the create profile page, the page collapses entirely, and the user is required to refill the form from scratch. This behavior is frustrating for users, as it forces them to re-enter all the information, even if only a single field is invalid. The create profile page should handle invalid input gracefully, displaying error messages for individual fields without collapsing the entire page

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name : Harsh Agrawal

Testing Date : 03/04/2024

Steps to Reproduce:

- Navigate to the create profile page.
- Enter invalid input in one or more fields (e.g., incorrect format for email, missing required fields).
- Submit the form.
- Observe that the page collapses entirely, and the user is prompted to refill the form from scratch.

Bug Details:

- **Expected Behavior**: When a user provides invalid input on the create profile page, the page should display error messages for individual fields with invalid input, allowing the user to correct them without losing the entered data. The page should not collapse entirely, preserving the user's progress in the form.
- **Actual Behavior**: Upon providing invalid input on the create profile page, the page collapses entirely, requiring the user to refill the form from scratch. This behavior is frustrating for users and can lead to a poor user experience.
- **Recommended Fix:**
    - Implement client-side validation on the create profile form to detect invalid input before submission.

  - Display error messages next to individual fields with invalid input, allowing users to correct them without losing their entered data.
  - Ensure that the page does not collapse entirely when invalid input is detected, preserving the user's progress in the form.
  - Try to solve the checks on the input boxes on the Frontend Side itself.

Bug Report Date: 06/04/2024

Has the bug been fixed?: Tried but not fixed

Date of Bug fixing: 09/04/2024

Additional Information: Improving the error handling on the create profile page will enhance the user experience by providing more informative feedback and preventing unnecessary frustration for users. Resolving this issue is essential for creating a smoother and more user-friendly profile creation process.

BUG 22 : Project Status Not Updated to "Requested" After Requesting a Project

Tested Feature: Bug on 2.0 version

Description:

After a user requests a project, the project status is not updated to "Requested" when the project is opened again. Instead, it continues to show the option to request the project, indicating that the request status was not properly updated. This inconsistency in project status display can lead to confusion for users regarding the status of their project requests.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name : **Arshit Narang**

Testing Date : **03/04/2024**

Steps to Reproduce:

- Navigate to the projects page.
- Select a project.
- Click the request button to request the project.
- Navigate to any other tab or log out and log in again.
- Return to the projects page and open the previously requested project.

Bug Details:

- **Expected Behavior**: After requesting a project, the project status should be updated to "Requested" and should reflect this status consistently, even after navigating to other tabs or logging out and logging back in. This ensures that users can easily track the status of their project requests.
- **Actual Behavior**: Upon opening the project again after requesting it, the project status does not update to "Requested" and continues to show the option to request the project. This inconsistency in project status display can confuse users about the status of their project requests.
- **Recommended Fix:**
  - Implement logic to properly update the project status to "Requested" after a user requests the project.

- Ensure that the project status is consistently displayed as "Requested" even after navigating to other tabs or logging out and logging back in.

Bug Report Date: 06/04/2024

Has the bug been fixed? : Tried but not fixed

Date of Bug fixing: 11/04/2024

Additional Information: Correcting the inconsistency in project status display after requesting a project will improve user confidence in the system and prevent confusion regarding the status of project requests. Resolving this issue is essential for providing a seamless user experience.

BUG 23 : No Error Handling for Invalid Link to Resume

Tested Feature: Bug on 2.0 version

Description:

The system lacks error handling for invalid links provided in the resume field during profile creation. When users enter a random or invalid link, the system fails to detect and handle this error, potentially leading to broken links or incorrect resume information. Proper error handling is necessary to ensure data integrity and provide users with feedback on their input errors.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name: **Naman Jaiswal**

Testing Date: **03/04/2024**

Steps to Reproduce:

- Navigate to the projects page.
- Select a project.
- Click the request button to request the project.
- Navigate to any other tab or log out and log in again.
- Return to the projects page and open the previously requested project.

Bug Details:

- **Expected Behavior**: When users provide an invalid or random link in the resume field, the system should detect this error and display an appropriate error message, indicating that the provided link is invalid. This helps users correct their input errors and ensures the accuracy of resume information.
- **Actual Behavior**: The system fails to handle invalid links provided in the resume field, allowing users to submit the form without any feedback on the invalid input. This lack of error handling can result in broken links or incorrect resume information, impacting user experience and data integrity.
- **Recommended Fix:**
    - Implement validation logic to detect invalid links provided in the resume field during profile creation.

  - ○ Display an error message when users provide an invalid link, indicating that the provided link is invalid and prompting users to enter a valid link.

Bug Report Date: 06/04/2024

Has the bug been fixed?: **Tried but not fixed**

Date of Bug fixing: 10/04/2024

Additional Information: Implementing error handling for invalid links in the resume field is essential for maintaining data integrity and providing users with feedback on their input errors. Resolving this issue will improve the accuracy and reliability of resume information in user profiles.

BUG 24 : Method to Update Resume

Tested Feature: Feature Request

Description:

Currently, there is no method provided for users to update their resume after profile creation. This limitation prevents users from keeping their resume information up to date and may result in outdated or incorrect resume information displayed on their profiles. Providing a method to update the resume is essential for maintaining the accuracy and relevance of user profiles.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name: **Jenil**

Testing Date: **3/04/2024**

Steps to Reproduce:

- Implement a user interface component for updating the resume.
- Allow users to upload a new resume file or enter a new resume link.
- Update the backend logic to handle resume updates and store the new resume information.

Bug Details:

- **Expected Behavior**: Users should be able to access a dedicated section or page in their profile settings to update their resume information. This section should provide options for uploading a new resume file or entering a new resume link. Upon submission, the system should update the user's resume information accordingly.

Bug Report Date: 06/04/2024

Has the bug been fixed?: **Tried but not fixed**

Date of Bug fixing: 12/04/2024

Additional Information: Providing users with the ability to update their resume information is crucial for ensuring the accuracy and relevance of their profiles. This feature enhances user control and customization options, contributing to a better overall user experience.

BUG 25 : No Error Handling for Invalid Link to Resume

Tested Feature: Invalid Input

Description:

The system accepts invalid input for creating a new project, allowing users to input nonsensical or incorrect values such as "ojfa" for the minimum CPI requirement. This behavior compromises the integrity of project data and may lead to confusion or incorrect data processing. Proper validation of input fields is necessary to ensure that only valid and meaningful values are accepted when creating a new project.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name : **Harshit Srivastava**

Testing Date : **03/04/2024**

Steps to Reproduce:

- Login as a faculty and Navigate to the page for creating a new project.
- Input invalid or nonsensical values, such as "ojfa" for the minimum CPI requirement.
- Submit the form to create the new project.
- Observe that the system accepts the invalid input without displaying any error messages or rejecting the input.

Bug Details:

- **Expected Behavior**: When creating a new project, the system should validate input fields and reject any invalid or nonsensical values provided by the user. This includes enforcing constraints such as minimum and maximum values for numeric fields and ensuring that text inputs are within reasonable limits and formats.
- **Actual Behavior**: The system accepts invalid input for creating a new project, allowing users to input nonsensical values such as "ojfa" for the minimum CPI requirement. This lack of input validation compromises the integrity of project data and may lead to confusion or incorrect data processing.
- **Recommended Fix:**
  - Implement comprehensive input validation for all input fields when creating a new project.

- Enforce constraints such as minimum and maximum values for numerical fields and validate text inputs against expected formats and limits.
- Display informative error messages when users provide invalid input, guiding them to correct their input errors before submitting the form.

Bug Report Date: 06/04/2024

Has the bug been fixed?:**Tried but not fixed**

Date of Bug fixing: 11/04/2024

Additional Information: Proper input validation is essential for maintaining data integrity and ensuring that only valid and meaningful data is accepted by the system. Resolving this issue will improve the accuracy and reliability of project data and enhance the overall user experience.

BUG 26 : Automatic Logout When Reloading Page

Tested Feature: Invalid Input

Description:

- After the user signs in, whenever users reload the page, they are automatically logged out, which disrupts their workflow and experience.

Vulnerability Type

- Lack of access controls
- Authentication bypass

Tester Name : **Arshit Narang**

Testing Date : **04/04/2024**

Steps to Reproduce:

- Log in to the system.
- Navigate to another page within the application and Reload the page.
- Notice that the user is logged out automatically.

Bug Details:

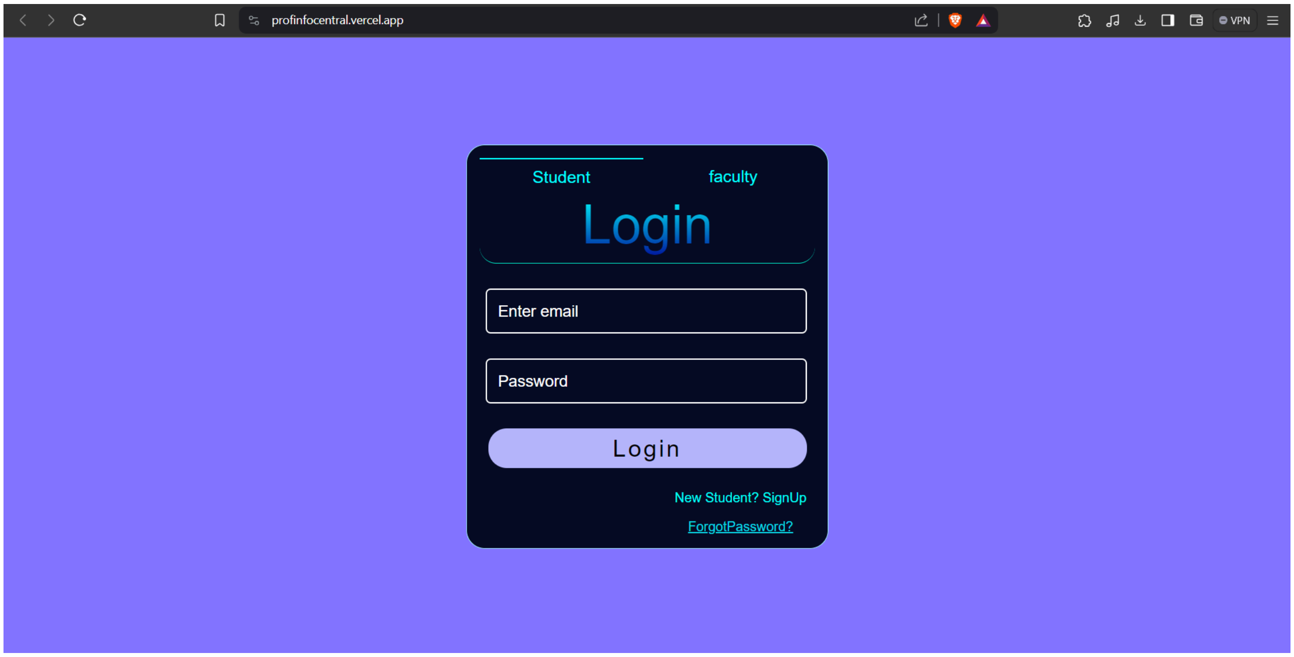
- **Expected Behavior**: Users should remain logged in even after reloading the page or navigating to different sections of the application. There should be a session data for the sign in.
- **Actual Behavior**: TUsers are logged out automatically upon reloading the page and directed to the sign - in page, leading to inconvenience and potential data loss.

Bug Report Date : 06/04/2024

Has the bug been fixed? : Tried but not fixed

Date of Bug fixing : 10/04/2024

Additional Information: This issue significantly affects user experience and may lead to frustration and loss of productivity. The loss of user data and progress is also hazardous.



BUG 27 : Unauthorized Access/Register to any Non IITK User

Tested Feature: Invalid Input

Description:

Currently, the website does not enforce restrictions on user authentication, allowing anyone to log in and access sensitive information and functionalities. Email authentication being not limited to IITK students and professors poses a huge security risk.

Vulnerability Type

- Authentication bypass

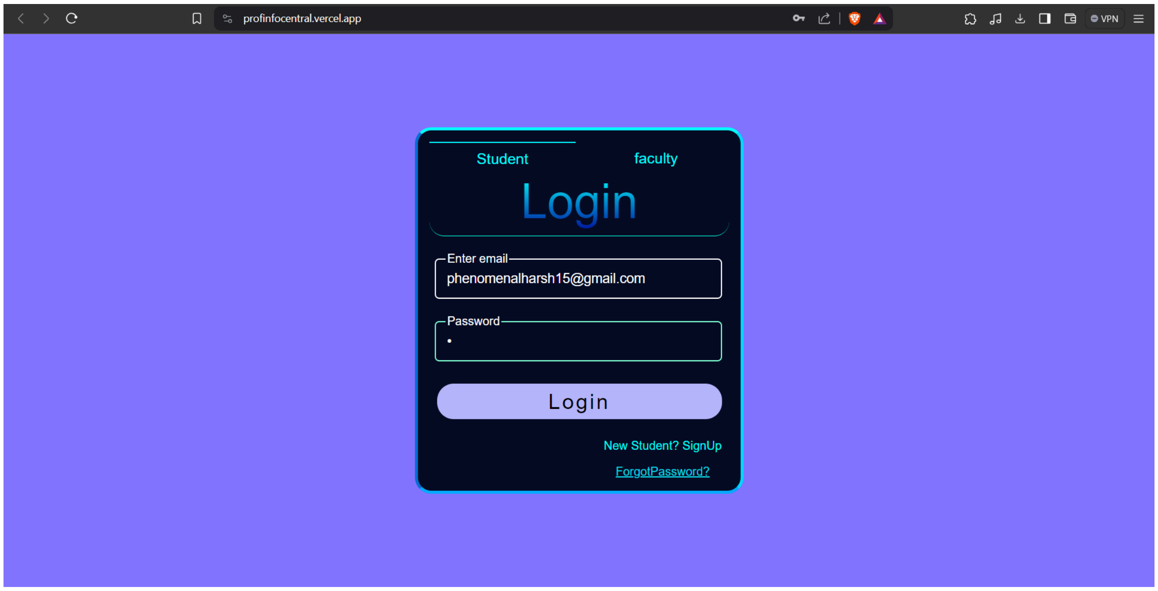
Tester Name: **Prem**

Testing Date: **03/04/2024**

Steps to Reproduce:

- Visit the website.
- Attempt to register with any non IITK / unauthorized email id.
- Notice that unauthorized users can access these routes and view sensitive information.

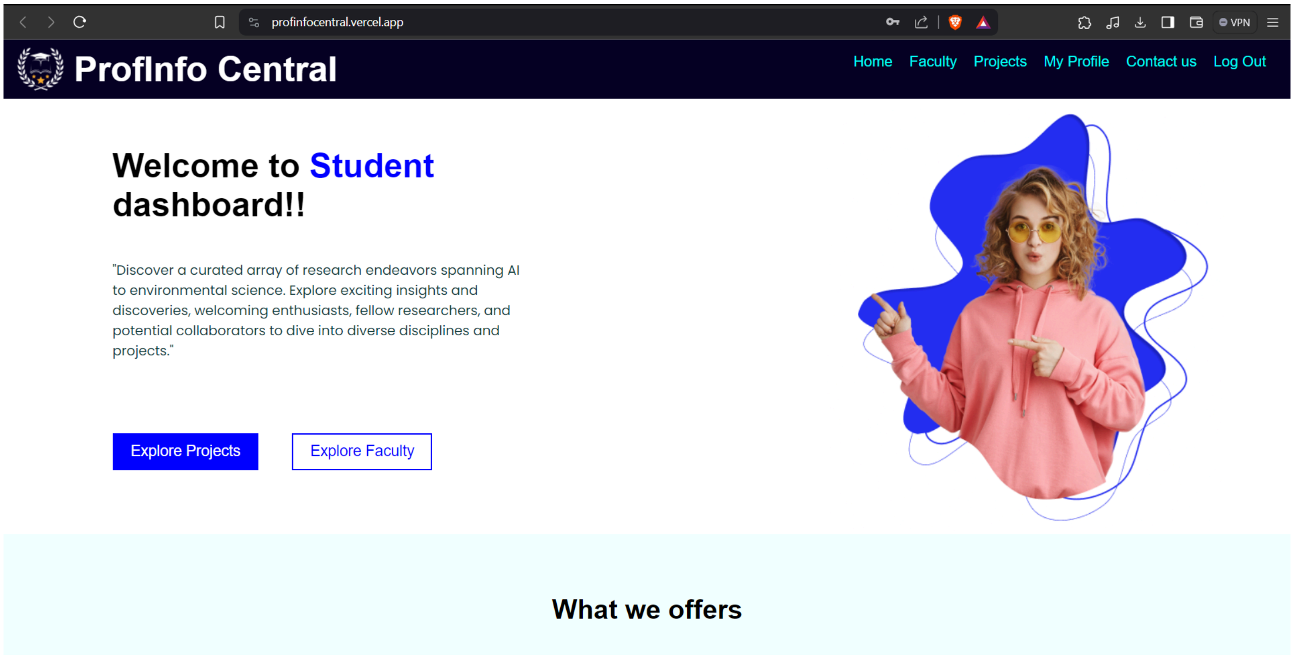
Logging in using another non IITK email (unauthorized):


profinfocentral.vercel.app

Enter email: phenomenalharsh15@gmail.com

Password: •

Login Successful:



Welcome to Student dashboard!!

"Discover a curated array of research endeavors spanning AI to environmental science. Explore exciting insights and discoveries, welcoming enthusiasts, fellow researchers, and potential collaborators to dive into diverse disciplines and projects."

What we offers

Bug Details:

- **Expected Behavior**: Only Authenticated users of IITK should be able to register themselves and then login for accessing further functionalities.
- **Actual Behavior**: Any unauthenticated third party can register themselves on the platform and login to access the data and project routes.
- **Recommended Fix:**
    - Restrict email authentication to IITK students and professors only, using domain-based filtering or verification.

Bug Report Date: 06/04/2024

Has the bug been fixed? : Tried but not fixed

Date of Bug fixing : 11/04/2024

Additional Information: This security vulnerability poses a significant risk to user data and privacy. Implementing proper access controls and restricting email authentication to authorized domains are essential steps in mitigating this risk and ensuring the security of the website.

3 Overall Quality of the Software

The user Manual guide is rudimentary and lacks readability, leaving users to grapple with understanding the functionalities assigned to every position. While purportedly containing screenshots, these visual aids fail to correctly guide customers thru the software, ensuing in a convoluted navigation experience. Overall, the person manual falls short of expectations.

Furthermore, the set up script furnished with the software program is insufficient, because it fails to seamlessly set up important dependencies and modules, leading to capability issues throughout setup. The accompanying release script, at the same time as a gift, gives little assistance in jogging the software easily. In assessing the codebase, it will become obvious that whilst the software program is modular, it lacks comprehensive documentation, making it challenging for developers to recognize and adjust. Although organized into wonderful folders, the absence of meaningful feedback exacerbates the problems in know-how the code's functionality.

Despite ostensibly meeting the minimal useful requirements mentioned in the Software Requirement Specification, the software's feature set stays lackluster. It fails to offer progressive solutions or cope with key person desires successfully. Moreover, the software program neglects vital non-useful necessities, thereby compromising its overall performance, protection, and scalability.

Overall, the software's inadequacies render it unsatisfactory for end-consumer attractiveness. A pertinent recommendation from the testing crew is for the builders to prioritize improving the user interface and design of the internet site. This could entail streamlining navigation and improving the classy enchantment to improve user revel in and satisfaction.

Appendix A - Group Log

Sr. No.	Date	Activity	Members
1	03-04-2024	During this meeting, we crafted a timeline for future meetings and beta testing phases. Over the course of four hours, we delved into the intricacies of the software, comprehensively digesting the User Manual, Implementation Documentation, and Software Requirement Document.	All
2	06-04-2024	We added the bugs to the issues section of GitHub. These issues were collated by nearly all members of the group during the previous meeting. This session spanned five hours, during which we formally reported 27 issues on GitHub	All
3	07-04-2024	We assigned some members to take charge of writing the beta testing document and some to make the presentation ppt, and some to fix the bugs in our github repo.	All
4	12-04-2024	We reviewed the software beta testing document and then made the suitable changes in the doc.	All