INDIVIDUAL REPORT

COS10026 – Computing Inquiry Project

MINH HOANG DUONG

104487115

Assignment Part 2

I. Table of Contents:

II. Introduction

- We are making an all-encompassing report on a website created to aid in the recruitment of IT specialists for job vacancies within a company. This website illustrates a technical expansion of an initial project, serving as a demonstration of our team's prowess in enhancing website functionality by utilizing PHP and MySQL. Our main focus in this enhancement effort is on server-side processing, with the goal of reinforcing things like security, form handling, input validation, and data administration. The report has been made to provide the average person with an understanding of our joint effort, the work involved, and other innovative features. Finally, we also talked about a website's security measures in detail and how this could be improved.

III. Description of Website

A. Overview

- Our website is comprised of six pivotal pages, each dedicated to a distinct purpose:

1. **Home Page (index.php):** Functioning as the initial landing page, it encapsulates the essence of the company and provides an outline of visitors' expectations. There are included social media links on the page for easy contact. (See Image 2.1)

2. **Job Description (jobs.php)**: This page offers information about available job positions, encompassing role prerequisites, potential salary details, and required qualifications. You can search for details on different jobs using both search queries and filters. (Refer to Images 2.2.1 and 2.2.2)

3. **Group Detail (about.php):** Here, we share information about our team, showing each member's contributions and responsibilities in the assignment. There is a detailed schedule and relevant work included. (See Image 2.3)

4. **Group’s Enhancements (enhancement.php):** This page serves as a showcase for our ideas aimed at surpassing the course requirements, so enhancing accessibility and user-friendliness. We shared our best and realistic ideas here, and would implement them upon joint discussion. (Refer to Image 2.4)

5. **Applying Page (apply.php):** Prospective candidates can submit their applications via this page, which features a form that, upon submission, activates a PHP script for input processing and store data in a database. Information that users entered here are also editable afterwards ensuring you can correct potential errors. (See Image 2.5)

6. **Manager's Page (manage.php):** Pivotally introduced as part of our project enhancements, this page helps database management for the manager. They can do tasks such as data deletion, selection, and review. Secure access is ensured, and this also require manager authentication. (Refer to Images 2.6.1 and 2.6.2)

B. Technical Details and Innovations

- To enhance the website, we transitioned all files from HTML to PHP. This strategic move enabled code modularization and reusability, which is evident in our separation of header, footer, and background video into distinct files (header.inc, footer.inc, bgvideo.inc), subsequently included in the main site pages. We created a dedicated PHP file (processEOI.php) for the purpose of form input processing and validation. The resulting data is then stored in the MySQL database hosted on the Pheenix-Maria server. (See Images 2.7 and 2.8). Lastly, we introduced a manager's page to streamline database management through a user-friendly interface. (Refer to Image 2.9).

IV. Website’s Security

A. Implemented Features

- Security is a very important part in website development, has been thought about carefully during our project to keep data safe and make sure our web application stays strong. We've worked hard to protect our website, and here are some strong measures we put in place:

  1. **Input Sanitization**: We cleaned up the user input in all the forms on our website. This is a basic way to stop bad scripts from being put in and run, which could cause SQL attacks and other harmful code problems (owasp.org, 2023 (1)). By cleaning and filtering user input, we only use valid data. (Look at Image 2.10).
  2. **Server-side Validation**: This is an extra layer of safety to make sure all user input follows our rules and standards. By checking data on the server, we stop harmful code and SQL attacks. Even if wrong data gets past the first check, the server won't use it (owasp.org, 2023 (2)). (See Images 2.7 and 2.11).
  3. **Password Safety**: We added protection with passwords, especially for the manager's page. Only authorized people can use important parts like managing the database. We saved the passwords safely so no one else can get in (microsoft.com, 2023 (1)). (Refer to Image 2.6.1).
  4. **Error handling**: We made sure that errors don't show sensitive information. This helps keep our server and database hidden from people who want to attack (owasp.org, 2023 (3)). (Refer to Image 2.12).

B. Room for Improvements

- We were not able to implement all the features we wanted to because of constraints, these are the ideas we think that could improve the website's security:

1. **Checking Security and Updates**: We want to check our security often to find and fix any arising problems and keep our security up to date and strong. We also want to update our software like the server operating system, PHP, and MySQL from time to time.
2. **Two-Factor Safety (2FA):** Adding more safety would make it much harder for people to get in without permission. We will look at different 2FA methods to pick the best one for our website, thinking about how it affects users, the cost, and how safe it is (microsoft.com, 2023 (2)).

V. My Personal Contribution

- In the collaborative journey of developing this website, I played an instrumental role in crafting the 'About Us' page, transitioning it from about.html to about.php.
- Additionally, I took on the responsibility of processing application forms on the 'Apply Now' page, creating the processEOI.php file. This task entailed ensuring all security measures were meticulously implemented within the processing file, guaranteeing the safe and secure handling of user data.

VI. Reflection and Discussion

A. Reflection on personal journey

- Honestly, as a first-year CS student with relatively limited technical knowledge, the process for web development has been a challenging one. Most noticeable was that I had to adjust my workflow to accommodate a team environment, which was a first for me as a long-time sole developer and tech geek.
- Besides that, applying what I had learned in class took me some effort at first. Reasoning is that I am quite a "hands-on" person, and a lot of class material honestly flew over my head. Thanks to the assignment, I have had the opportunity to learn

things once again on the way and this has contributed significantly towards my understanding.

- Finally, I must mention how novel it is that I could access the required materials with ease thanks to the school's resources hub. Before, I have had to scour the web or forums for obscure issues. Now, with the knowledge database, I can approach problems from the foundation level, allowing for more concrete and efficient solutions.

B. Reflection on the result

- The journey of developing and improving the recruitment website has been a significant learning experience for our team. All in all, we were reasonably satisfied with the outcome. However, we acknowledge that there is room for improvement.
- For instance, when we think about how the website will be used in the real world, and the potential cyber threats, it becomes crucial to enhance our security measures. This involves implementing strong password policies, ensuring regular backups and updates, and using protective tools like Firewalls, Secure Hosting Services, and DDoS protection. One further issue is that we should consider the operational viability of our website, in case we would be the ones hosting. For example, things like hosting fees, income flow or PR effectiveness.

C. Discussion on privacy

- Apart from security, we should also be more aware of privacy concerns. Treating user data with the utmost care and confidentiality is of utmost importance. We understand the necessity of establishing robust privacy practices and policies to ensure that user information is safeguarded and used only for its intended purpose. As developers, we should protect user privacy and be able to handle data easily. These are the elements I think every web developer should uphold:

    1. **Accountability**: Developers should take responsibilities for their actions and ensure that privacy practices are adhered to, and any breaches are addressed promptly.
    2. **User empowerment**: Providing users with control over their data, including the ability to access, correct, and delete their information, would help them to protect their own privacy.

3. **Avoiding deceptive practices**: Ensuring that consent mechanisms and privacy policies are not designed to mislead or coerce users into agreeing to data collection is essential for ethical web practices.

VII. Conclusion

- To conclude, this report has aimed to cover various aspects of our website development project, including its structure, technical enhancements, and the rigorous security measures we've put in place. It has offered a window through which the reader can grasp our team's efforts in creating a secure and functional platform for recruiting IT specialists.
- As web developers, our responsibilities should go beyond just writing code and ensuring functionality. They also include a commitment to creating secure, efficient environments. This project has served as a step in that direction, helping us to understand the broader implications and ethical responsibilities inherent in the digital realm.

VIII. References

SQL injection prevention cheat sheet SQL Injection Prevention - OWASP Cheat Sheet Series. Available at: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html #primary-defenses(Accessed: 30 October 2023). (1)

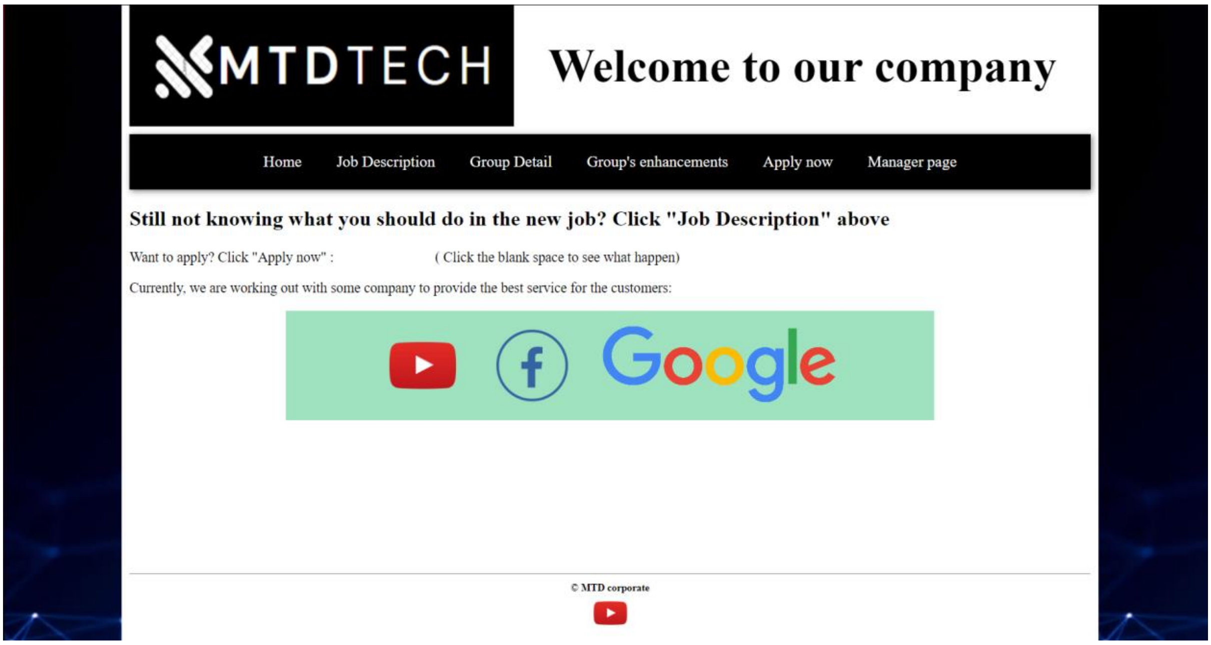
Zhong, W.Code injection, Code Injection | OWASP Foundation. Available at: https://owasp.org/www-community/attacks/Code_Injection(Accessed: 30 October 2023).(2)

Ferragamo, J. Improper error handling, Improper Error Handling | OWASP Foundation. Available at: https://owasp.org/www-community/Improper_Error_Handling(Accessed: 30 October 2023).(3)

What is password protection?: Microsoft security What Is Password Protection? | Microsoft Security. Available at: https://www.microsoft.com/en/security/business/security-101/what-is-password-protection (Accessed: 30 October 2023). (1)

What is Two-factor authentication (2FA)?: Microsoft security What is two-factor authentication (2FA)? | Microsoft Security. Available at: https://www.microsoft.com/en-au/security/business/security-101/what-is-two-factor-authentication-2fa (Accessed: 30 October 2023). (2)

IX. Appendix



Welcome to our company

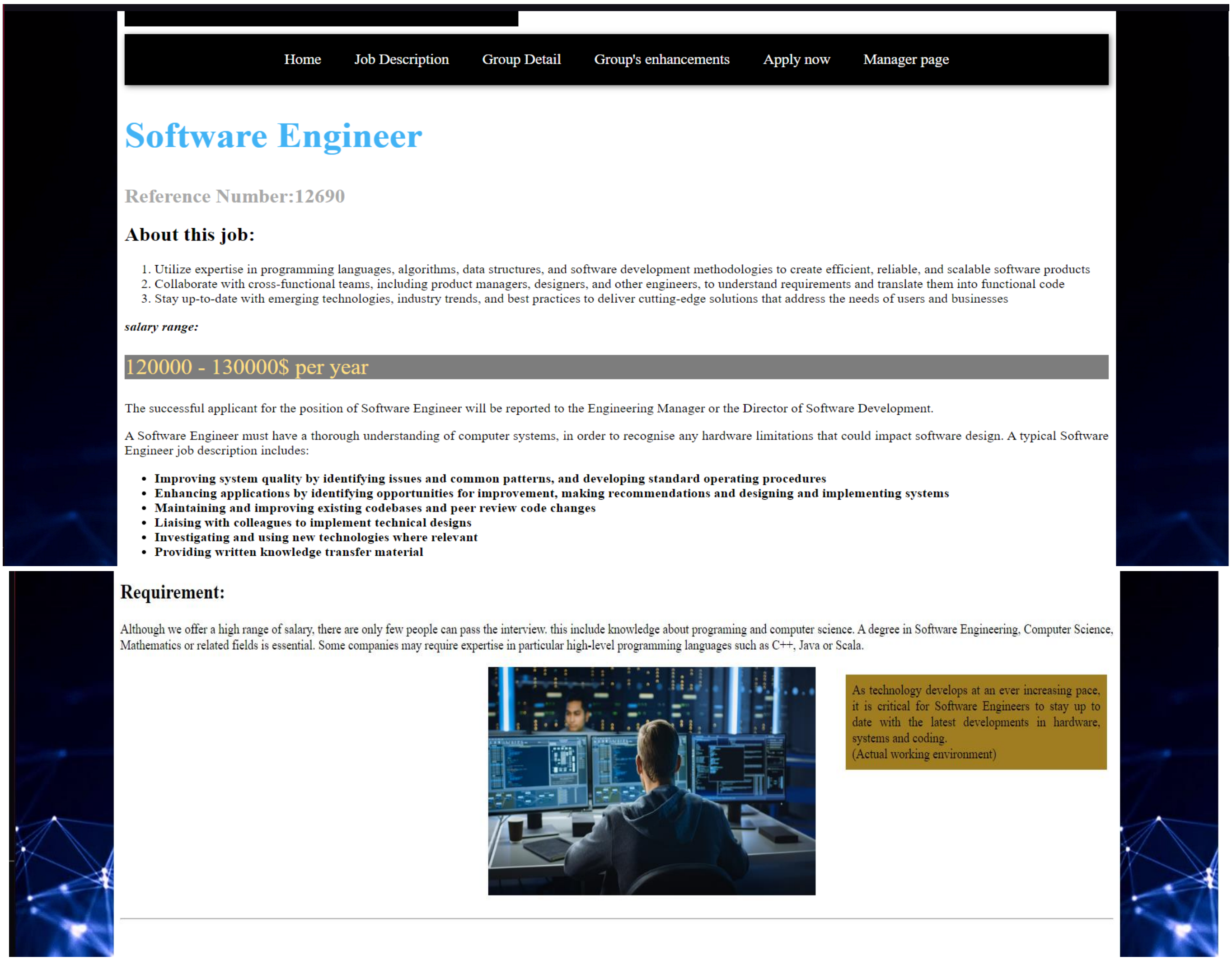
Still not knowing what you should do in the new job? Click "Job Description" above

Want to apply? Click "Apply now" : (Click the blank space to see what happen)

Currently, we are working out with some company to provide the best service for the customers:

© MTD corporate

Image 2.1: Home page (index.html).



Software Engineer

Reference Number:12690

About this job:

1. Utilize expertise in programming languages, algorithms, data structures, and software development methodologies to create efficient, reliable, and scalable software products
2. Collaborate with cross-functional teams, including product managers, designers, and other engineers, to understand requirements and translate them into functional code
3. Stay up-to-date with emerging technologies, industry trends, and best practices to deliver cutting-edge solutions that address the needs of users and businesses

salary range:

120000 - 130000$ per year

The successful applicant for the position of Software Engineer will be reported to the Engineering Manager or the Director of Software Development.

A Software Engineer must have a thorough understanding of computer systems, in order to recognise any hardware limitations that could impact software design. A typical Software Engineer job description includes:

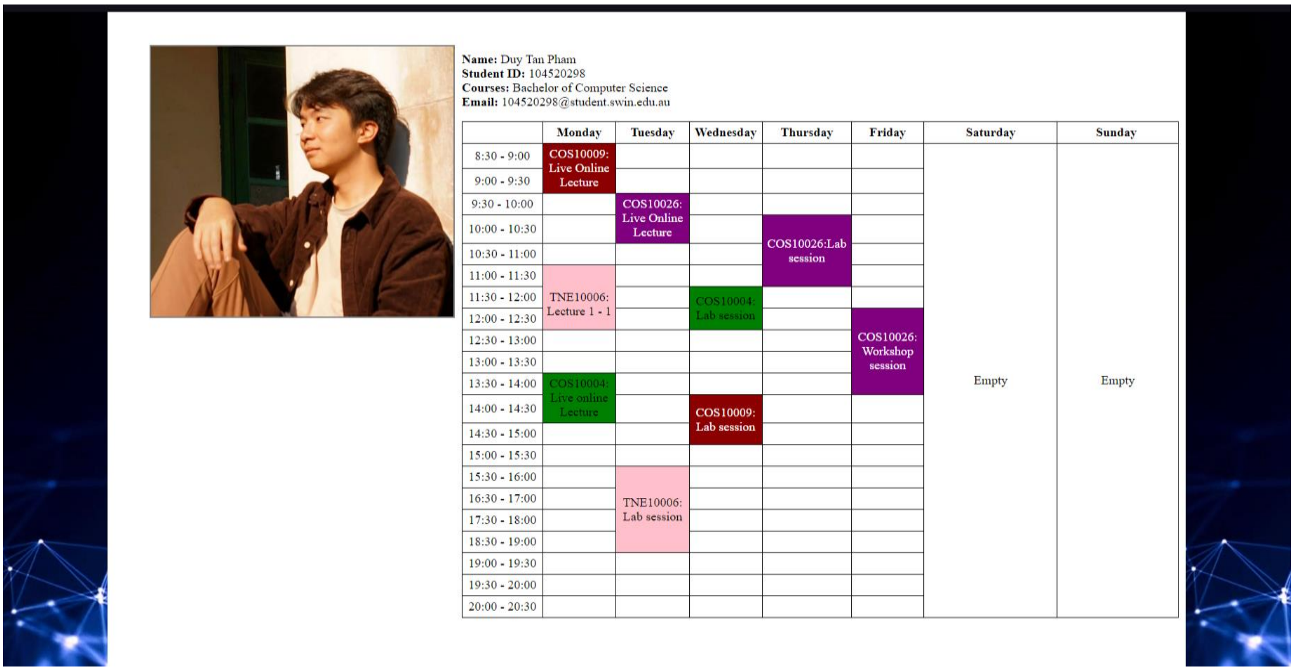
- **Improving system quality by identifying issues and common patterns, and developing standard operating procedures**
- **Enhancing applications by identifying opportunities for improvement, making recommendations and designing and implementing systems**
- **Maintaining and improving existing codebases and peer review code changes**
- **Liaising with colleagues to implement technical designs**
- **Investigating and using new technologies where relevant**
- **Providing written knowledge transfer material**

Requirement:

Although we offer a high range of salary, there are only few people can pass the interview. this include knowledge about programing and computer science. A degree in Software Engineering, Computer Science, Mathematics or related fields is essential. Some companies may require expertise in particular high-level programming languages such as C++, Java or Scala.

As technology develops at an ever increasing pace, it is critical for Software Engineers to stay up to date with the latest developments in hardware, systems and coding.
(Actual working environment)

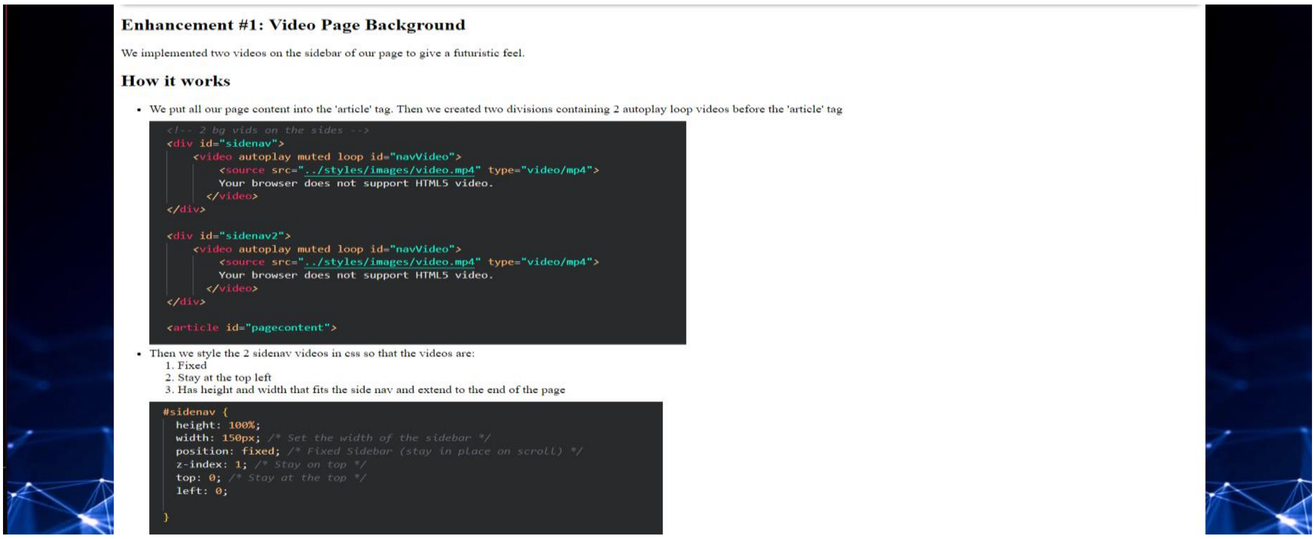
Image 2.2.1/2.2.2: Job Description (jobs.html).



Name: Duy Tan Pham
Student ID: 104520298
Courses: Bachelor of Computer Science
Email: 104520298@student.swin.edu.au

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
8:30 - 9:00	COS10009: Live Online Lecture					Empty	Empty
9:00 - 9:30							
9:30 - 10:00		COS10026: Live Online Lecture					
10:00 - 10:30				COS10026:Lab session			
10:30 - 11:00							
11:00 - 11:30	TNE10006: Lecture 1 - 1						
11:30 - 12:00			COS10004: Lab session				
12:00 - 12:30					COS10026: Workshop session		
12:30 - 13:00							
13:00 - 13:30							
13:30 - 14:00	COS10004: Live online Lecture						
14:00 - 14:30			COS10009: Lab session				
14:30 - 15:00							
15:00 - 15:30							
15:30 - 16:00		TNE10006: Lab session					
16:30 - 17:00							
17:30 - 18:00							
18:30 - 19:00							
19:00 - 19:30							
19:30 - 20:00							
20:00 - 20:30							

Image 2.3: The Group Detail (about.php).



Enhancement #1: Video Page Background

We implemented two videos on the sidebar of our page to give a futuristic feel.

How it works

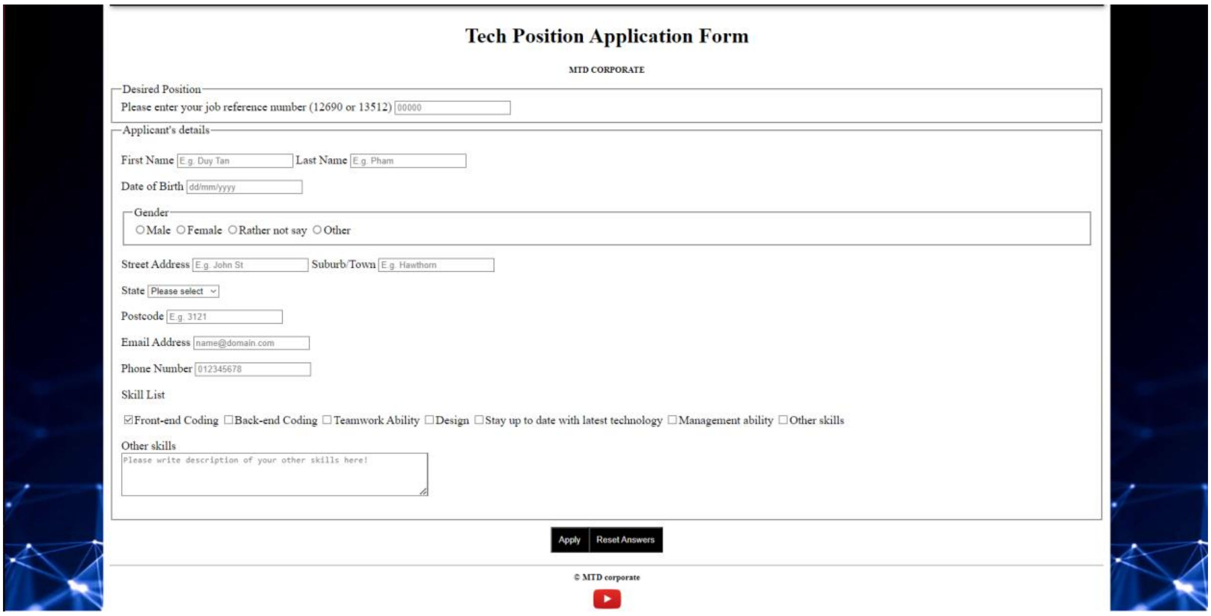
- We put all our page content into the 'article' tag. Then we created two divisions containing 2 autoplay loop videos before the 'article' tag

```
<!-- 2 bg vids on the sides -->
<div id="sidenav">
    <video autoplay muted loop id="navVideo">
        <source src="../styles/images/video.mp4" type="video/mp4">
        Your browser does not support HTML5 video.
      </video>
</div>

<div id="sidenav2">
    <video autoplay muted loop id="navVideo">
        <source src="../styles/images/video.mp4" type="video/mp4">
        Your browser does not support HTML5 video.
      </video>
</div>

<article id="pagecontent">
```

- Then we style the 2 sidenav videos in css so that the videos are:
  1. Fixed
  2. Stay at the top left
  3. Has height and width that fits the side nav and extend to the end of the page

```
#sidenav {
  height: 100%;
  width: 150px; /* Set the width of the sidebar */
  position: fixed; /* Fixed Sidebar (stay in place on scroll) */
  z-index: 1; /* Stay on top */
  top: 0; /* Stay at the top */
  left: 0;

}
```

Image 2.4: Group’s enhancement page.



Tech Position Application Form

MTD CORPORATE

Desired Position

Please enter your job reference number (12690 or 13512) 00000

Applicant's details

First Name E.g. Duy Tan Last Name E.g. Pham

Date of Birth dd/mm/yyyy

Gender

○Male ○Female ○Rather not say ○Other

Street Address E.g. John St Suburb/Town E.g. Hawthorn

State Please select

Postcode E.g. 3121

Email Address name@domain.com

Phone Number 012345678

Skill List

☑Front-end Coding □Back-end Coding □Teamwork Ability □Design □Stay up to date with latest technology □Management ability □Other skills

Other skills

Please write description of your other skills here!

Image 2.5: The application form on the applying page.

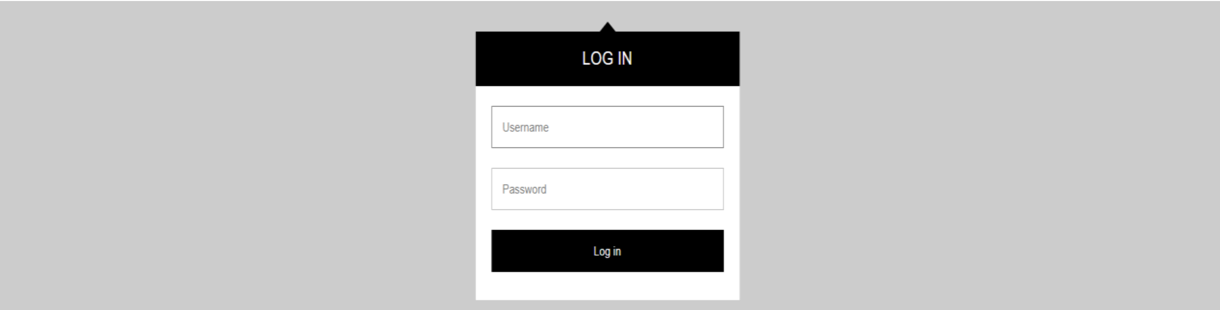
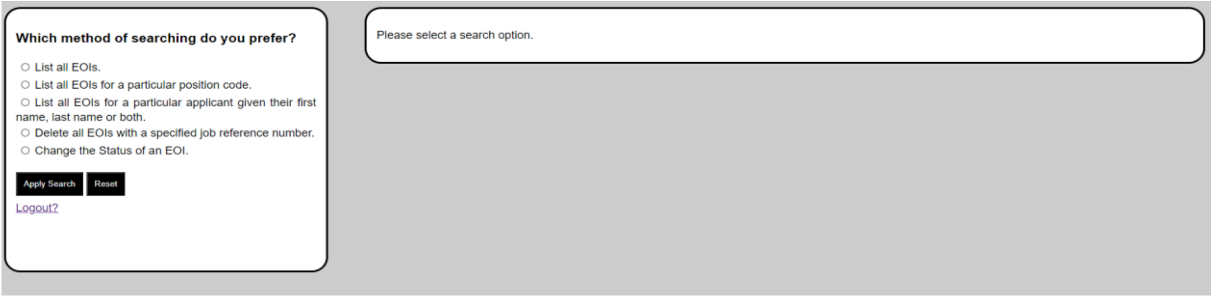


Image 2.6.1: The login form of the manager's page.



Which method of searching do you prefer?

○ List all EOIs.

○ List all EOIs for a particular position code.

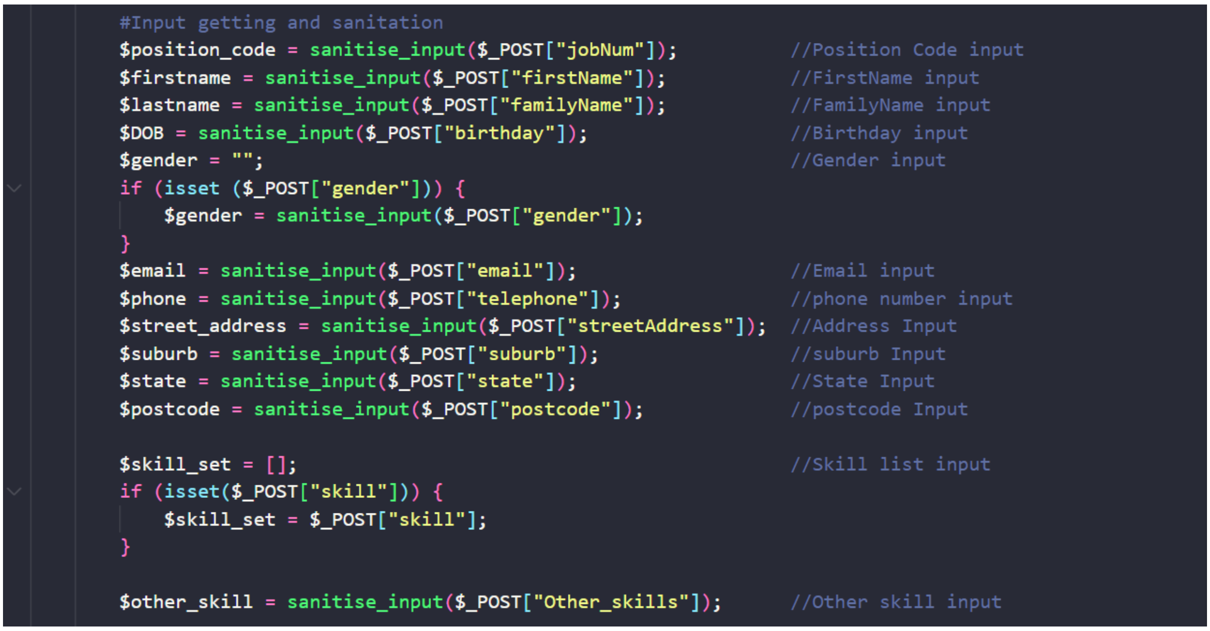
○ List all EOIs for a particular applicant given their first name, last name or both.

○ Delete all EOIs with a specified job reference number.

○ Change the Status of an EOI.

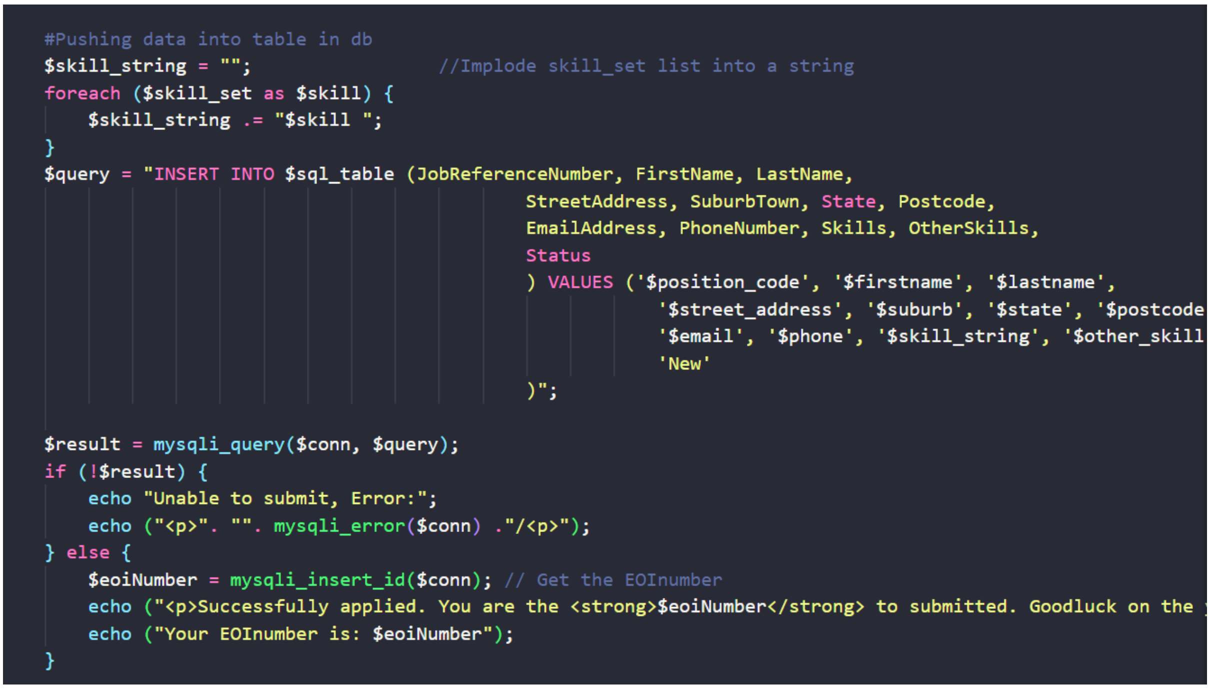
Please select a search option.

Image 2.6.2: The manager's page managing form.



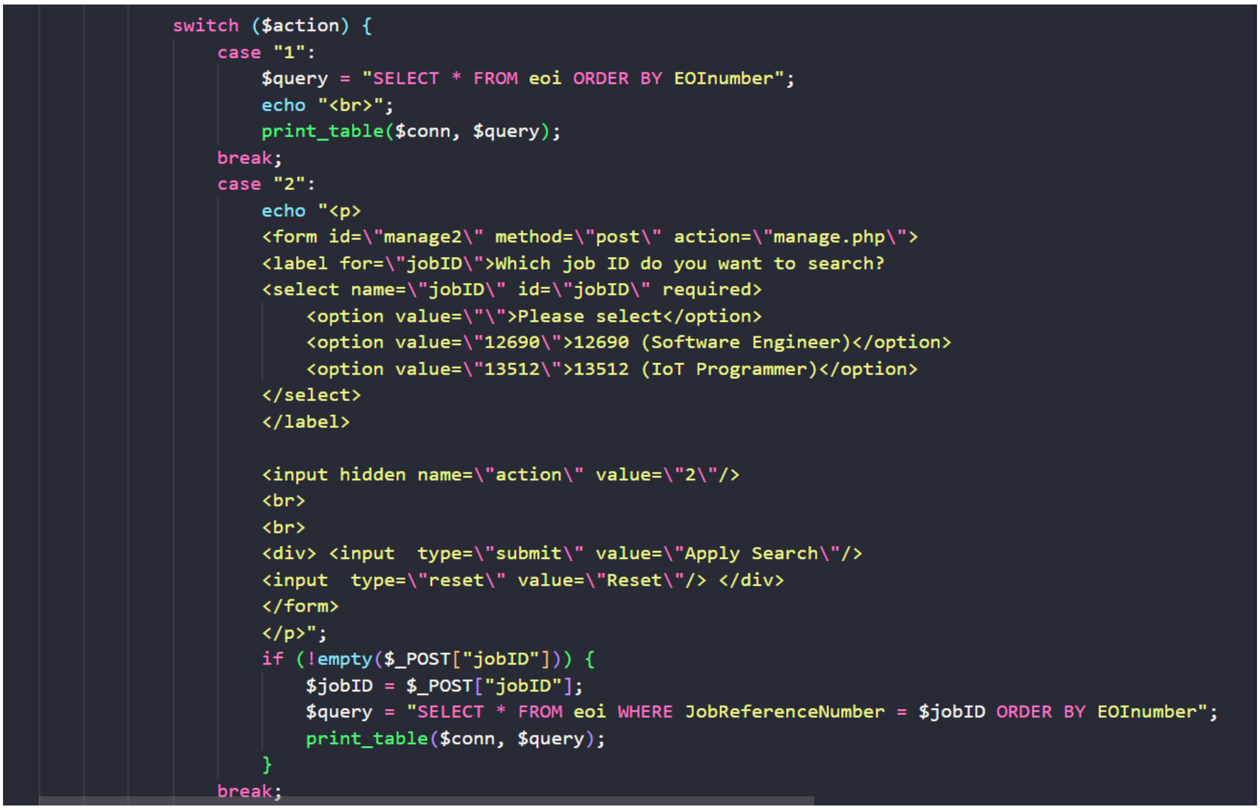
```
#Input getting and sanitation
$position_code = sanitise_input($_POST["jobNum"]);          //Position Code input
$firstname = sanitise_input($_POST["firstName"]);           //FirstName input
$lastname = sanitise_input($_POST["familyName"]);           //FamilyName input
$DOB = sanitise_input($_POST["birthday"]);                  //Birthday input
$gender = "";                                               //Gender input
if (isset ($_POST["gender"])) {
    $gender = sanitise_input($_POST["gender"]);
}
$email = sanitise_input($_POST["email"]);                   //Email input
$phone = sanitise_input($_POST["telephone"]);               //phone number input
$street_address = sanitise_input($_POST["streetAddress"]);  //Address Input
$suburb = sanitise_input($_POST["suburb"]);                 //suburb Input
$state = sanitise_input($_POST["state"]);                   //State Input
$postcode = sanitise_input($_POST["postcode"]);             //postcode Input

$skill_set = [];                                            //Skill list input
if (isset($_POST["skill"])) {
    $skill_set = $_POST["skill"];
}

$other_skill = sanitise_input($_POST["Other_skills"]);      //Other skill input
```

Image 2.7: Input getting and processing from the applying form in the processEOI.php



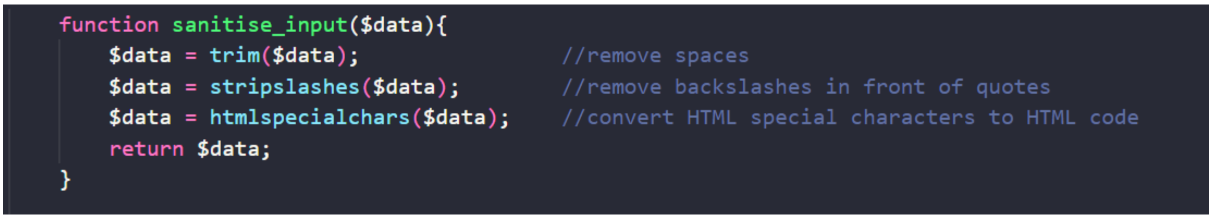
```
#Pushing data into table in db
$skill_string = "";             //Implode skill_set list into a string
foreach ($skill_set as $skill) {
    $skill_string .= "$skill ";
}
$query = "INSERT INTO $sql_table (JobReferenceNumber, FirstName, LastName,
                                            StreetAddress, SuburbTown, State, Postcode,
                                            EmailAddress, PhoneNumber, Skills, OtherSkills,
                                            Status
                                            ) VALUES ('$position_code', '$firstname', '$lastname',
                                                        '$street_address', '$suburb', '$state', '$postcode
                                                        '$email', '$phone', '$skill_string', '$other_skill
                                                        'New'
                                            )";

$result = mysqli_query($conn, $query);
if (!$result) {
    echo "Unable to submit, Error:";
    echo ("<p>". "". mysqli_error($conn) ."/<p>");
} else {
    $eoiNumber = mysqli_insert_id($conn); // Get the EOInumber
    echo ("<p>Successfully applied. You are the <strong>$eoiNumber</strong> to submitted. Goodluck on the
    echo ("Your EOInumber is: $eoiNumber");
}
```

Image 2.8: Saving input onto MySQL database by executing query.



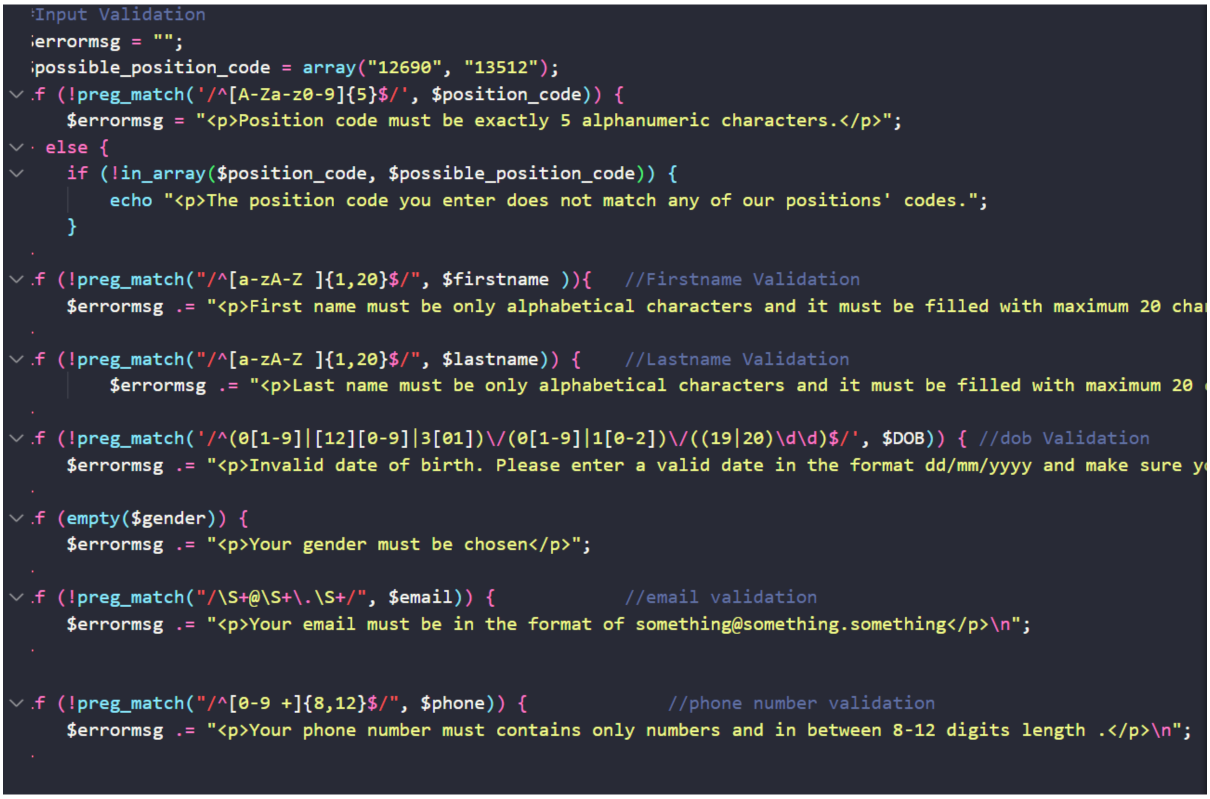
```
            switch ($action) {
                case "1":
                    $query = "SELECT * FROM eoi ORDER BY EOInumber";
                    echo "<br>";
                    print_table($conn, $query);
                break;
                case "2":
                    echo "<p>
                    <form id=\"manage2\" method=\"post\" action=\"manage.php\">
                    <label for=\"jobID\">Which job ID do you want to search?
                    <select name=\"jobID\" id=\"jobID\" required>
                        <option value=\"\">Please select</option>
                        <option value=\"12690\">12690 (Software Engineer)</option>
                        <option value=\"13512\">13512 (IoT Programmer)</option>
                    </select>
                    </label>

                    <input hidden name=\"action\" value=\"2\"/>
                    <br>
                    <br>
                    <div> <input  type=\"submit\" value=\"Apply Search\"/>
                    <input  type=\"reset\" value=\"Reset\"/> </div>
                    </form>
                    </p>";
                    if (!empty($_POST["jobID"])) {
                        $jobID = $_POST["jobID"];
                        $query = "SELECT * FROM eoi WHERE JobReferenceNumber = $jobID ORDER BY EOInumber";
                        print_table($conn, $query);
                    }
                break;
```

Image 2.9: Query executed based on selection of the manager through UI.



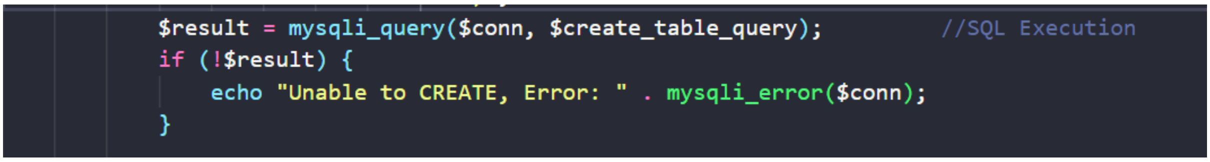
```
function sanitise_input($data){
    $data = trim($data);            //remove spaces
    $data = stripslashes($data);    //remove backslashes in front of quotes
    $data = htmlspecialchars($data);    //convert HTML special characters to HTML code
    return $data;
}
```

Image 2.10: Sanitise input function implementation on login form, application form and management form.



```
Input Validation
errormsg = "";
possible_position_code = array("12690", "13512");
.f (!preg_match('/^[A-Za-z0-9]{5}$/', $position_code)) {
    $errormsg = "<p>Position code must be exactly 5 alphanumeric characters.</p>";
  else {
    if (!in_array($position_code, $possible_position_code)) {
        echo "<p>The position code you enter does not match any of our positions' codes.";
    }

.f (!preg_match("/^[a-zA-Z ]{1,20}$/", $firstname )){   //Firstname Validation
    $errormsg .= "<p>First name must be only alphabetical characters and it must be filled with maximum 20 cha

.f (!preg_match("/^[a-zA-Z ]{1,20}$/", $lastname)) {    //Lastname Validation
        $errormsg .= "<p>Last name must be only alphabetical characters and it must be filled with maximum 20

.f (!preg_match('/^(0[1-9]|[12][0-9]|3[01])\/(0[1-9]|1[0-2])\/((19|20)\d\d)$/', $DOB)) { //dob Validation
    $errormsg .= "<p>Invalid date of birth. Please enter a valid date in the format dd/mm/yyyy and make sure y

.f (empty($gender)) {
    $errormsg .= "<p>Your gender must be chosen</p>";

.f (!preg_match("/\S+@\S+\.\S+/", $email)) {            //email validation
    $errormsg .= "<p>Your email must be in the format of something@something.something</p>\n";


.f (!preg_match("/^[0-9 +]{8,12}$/", $phone)) {             //phone number validation
    $errormsg .= "<p>Your phone number must contains only numbers and in between 8-12 digits length .</p>\n";
```

Image 2.11: Server-side validation being implemented into application form.



```
$result = mysqli_query($conn, $create_table_query);         //SQL Execution
if (!$result) {
    echo "Unable to CREATE, Error: " . mysqli_error($conn);
}
```

Image 2.12: Error handling in Querry execution (proccessEOI.php)