Project 1 Report on

Contemporary Curriculum, Pedagogy, and Practice (C2P2)

S. Y. B. Tech Computer Engineering

Project 1 [BTECCE22408: Application Security]

By

NAME	ATHARV GURAV
YEAR	SECOND YEAR
SRN	202201652
DIVISION	D(D3)
ROLL NO	57

Department of Computer Engineering

Faculty of Science and Technology

Academic Year

2023-2024

Name of Guide

Prof :Sridevi Hiremath

Index

Project Statement:-

Global Bank is in the process of building a web application that includes a file upload system, which at present, is secured insufficiently. This flaw could potentially be abused by uploading files with malicious intent. Global Bank is required to evaluate and enact security enhancements for their file upload mechanism to prevent such exploits

Problem Description:-

- **In five lines describe in detail about the Problem statement**

1. **Current Insufficient Security**: Global Bank's file upload system lacks adequate security measures, making it vulnerable to exploitation by malicious actors.
2. **Risk of Malicious Uploads**: Without proper safeguards, attackers could upload files containing harmful code or malware, posing a significant threat to the integrity and confidentiality of the web application and its users' data.
3. **Urgent Need for Enhancements**: Immediate evaluation and implementation of robust security enhancements are essential to mitigate this vulnerability and prevent potential breaches.
4. **Required Security Measures**: Measures such as input validation, file type verification, and access controls must be implemented to fortify the file upload mechanism against exploitation.
5. **Potential Consequences**: Failure to address this security flaw could lead to severe consequences, including data breaches, financial losses, and damage to Global Bank's reputation.

Project stage- 1 details:

- **Write in detail the technology used along with the algorithm**

To strengthen the security of file uploads in the Global Bank web application and mitigate potential vulnerabilities, implementing a robust strategy involving both technology and algorithmic measures is essential. Here's a detailed plan:

File Type Verification: Implement a file type verification mechanism to ensure that only permitted file types are uploaded. This can be achieved by examining the file extension or using file signature analysis to detect the actual file type.

File Size Limit: Set appropriate limits on the size of uploaded files to prevent abuse of server resources and potential denial-of-service attacks. This can be configured at both the client-side and server-side.

Content Disposition: Ensure that uploaded files are served with the appropriate Content-Disposition header to prevent browsers from executing files that could potentially be harmful, such as executable files or scripts.

Antivirus Scanning: Integrate antivirus scanning functionality into the file upload process to detect and quarantine any files that may contain malware or other malicious content. This can be achieved by using third-party antivirus APIs or libraries.

Secure File Storage: Store uploaded files in a secure location with restricted access permissions to prevent unauthorized access or execution. Encrypt sensitive files at rest to protect against data breaches.

Content-Type Header Validation: Validate the Content-Type header of uploaded files to ensure that it matches the actual file content. This helps prevent attackers from disguising malicious files as harmless file types.

Implementing CSRF Protection: Implement Cross-Site Request Forgery (CSRF) protection to prevent unauthorized users from submitting malicious requests on behalf of authenticated users. This involves generating and validating CSRF tokens for each file upload request.

Input Validation: Validate all input fields associated with file uploads to prevent injection attacks such as SQL injection or command injection. Use secure coding practices and input validation libraries to sanitize user input effectively.

Security Headers: Utilize security headers such as Content-Security-Policy (CSP) and X-Content-Type-Options to enhance the security of the file upload feature and protect against various types of attacks, including cross-site scripting (XSS) and MIME sniffing.

Project stage- 1 details:

- **Write in detail the algorithm**

Step 1: File Type Verification: Check the file extension and verify it against a whitelist of allowed file types. Additionally, analyze the file signature to confirm its actual type.

Step 2: File Size Limit Check: Verify that the size of the uploaded file does not exceed the predefined maximum limit.

Step 3: Antivirus Scanning: Utilize an antivirus scanning algorithm to scan the uploaded file for known malware signatures or suspicious patterns.

Step 4: Content-Type Header Validation: Validate the Content-Type header of the uploaded file against its actual content to prevent content-type spoofing attacks.

Step 5: File Sanitization: Perform thorough sanitization of the file content to remove any potentially harmful elements or code snippets.

Step 6: Secure File Storage: Store the sanitized file in a secure location with restricted access permissions and apply encryption if necessary.
Content-Type Header Validation: Validate the Content-Type header of uploaded files to ensure that it matches the actual file content. This helps prevent attackers from disguising malicious files as harmless file types.

SOURCE CODE :

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Global Bank</title>
<style>
/* Global Styles */
* {
  margin: 0;
  padding: 0;
  box-sizing: border-box;
}

body {
  font-family: Arial, sans-serif;
}

/* Header Styles */
header {
  background-color: rgb(26, 26, 26);
  padding: 20px;
  color: darkteal;
  text-align: left;
  margin-bottom: 20px;
  border-bottom: 2px solid darkteal;
  display: flex;
  justify-content: space-between;
  align-items: center;
}

.logo-container {
  border: 2px solid rgb(198, 174, 42);
  padding: 10px;
  border-radius: 5px;
```

```
}

.logo {
  width: 100px;
}

.file-upload-container {
  display: flex;
  align-items: center;
  margin-right: 20px;
}

.file-upload-container input[type="file"] {
  display: none;
}

.file-upload-container button {
  background-color: rgb(198, 174, 42);
  color: darkteal;
  padding: 10px;
  font-size: 14px;
  border: 2px solid darkteal;
  cursor: pointer;
  margin-left: 10px;
}

.dropdown {
  position: relative;
  display: inline-block;
  margin: 0 10px;
}

.dropdown button {
  background-color: rgb(198, 174, 42);
  color: darkteal;
  padding: 12px;
  font-size: 16px;
  border: 2px solid darkteal;
  cursor: pointer;
}
```

```
.dropdown-content {
  display: none;
  position: absolute;
  background-color: beige;
  min-width: 160px;
  box-shadow: 0px 8px 16px 0px rgba(0, 0, 0, 0.2);
  z-index: 1;
  padding: 10px;
}

.dropdown-content a {
  color: black;
  padding: 10px 0;
  text-decoration: none;
  display: block;
}

.dropdown-content a:hover {
  background-color: rgb(198, 174, 42);
  color: darkteal;
}

.dropdown:hover .dropdown-content {
  display: block;
}

.dropdown:hover button {
  background-color: white;
}

.global-bank {
  font-weight: bold;
  font-size: 24px;
  color: rgb(198, 174, 42);
}

.language-section {
  margin-left: auto;
}
```

```
.login-search-container {
  display: flex;
  align-items: center;
  margin-right: 20px;
}

.login-btn {
  background-color: rgb(198, 174, 42);
  color: darkteal;
  padding: 12px;
  font-size: 16px;
  border: 2px solid darkteal;
  cursor: pointer;
  margin-right: 10px;
}

.search-input-container {
  position: relative;
}

.search-input {
  padding: 10px 45px 10px 10px; /* Adjusted padding for search input */
  border: 2px solid darkteal;
  border-radius: 5px;
  font-size: 16px;
  width: 200px; /* Adjusted width for search input */
}

.notification-icon {
  position: absolute;
  right: 10px;
  top: 50%;
  transform: translateY(-50%);
  color: darkteal;
}

.search-icon {
  position: absolute;
```

```
  right: 40px;
  top: 50%;
  transform: translateY(-50%);
}

/* Slider Styles */
.slider-container {
  position: relative;
  max-width: 100%;
  overflow: hidden;
  height: 450px; /* Increased height for slider */
  margin-bottom: 20px;
}

.slide {
  display: none;
}

.slide img {
  width: 100%; /* Set width to 100% */
  height: auto; /* Set height to auto to maintain aspect ratio */
}


/* Moving red color line under the slider section */
.slider-line {
  height: 8px;
  background-color:rgb(198, 174, 42);
  position: absolute;
  bottom: 0;
  left: 0;
  animation: move 5s linear infinite; /* Animation for moving
line */
}

@keyframes move {
  0% {
    width: 0;
  }
  100% {
```

```
    width: 100%;
  }
}

/* Footer Styles */
footer {
  background-color: rgb(26, 26, 26);
  color: rgb(198, 174, 42);
  padding: 10px;
  position: relative;
}

.footer-menu {
  display: flex;
  flex-wrap: wrap;
  justify-content: space-between;
}

.footer-menu div {
  flex: 1;
  margin-right: 20px;
}

.footer-menu h3 {
  margin-bottom: 20px;
}

.footer-menu ul {
  list-style-type: none;
}

.footer-menu ul li {
  margin-bottom: 10px;
}

.footer-menu ul li a {
  color: white;
  text-decoration: none;
}
```

```
.footer-menu ul li a:hover {
  color: darkteal;
}
.file-upload-section {
  border: 2px solid rgb(198, 174, 42);
  border-radius: 5px;
  padding: 20px;
  margin: 20px auto;
  max-width: 400px; /* Adjust width as needed */
}

.file-upload-section input[type="file"] {
  background-color: rgb(198, 174, 42);
  display: block;
  margin-bottom: 10px;
}

.file-upload-section button {
  background-color: rgb(198, 174, 42);
  color: darkteal;
  padding: 10px 20px;
  font-size: 16px;
  border: 2px solid darkteal;
  cursor: pointer;
  margin-top: 10px;
}

#uploadMessage {
  color: red;
  margin-top: 10px;
}

</style>
</head>
<body>

<header>
  <div class="logo-container">
    <img src="https://encrypted-
tbn0.gstatic.com/images?q=tbn:ANd9GcQEBzXPUrAejB-
```

```
My89fHdIXrCBFZplATol6oiIufZs9Lg&s" alt="Global Bank
Logo" class="logo">
    <div class="global-bank">Global Bank</div>
  </div>

  <div class="file-upload-section">
    <input type="file" id="fileInput">
    <button onclick="uploadFile()">Upload File</button>
    <p id="uploadMessage"></p>
  </div>

  <div class="language-section">
    <div class="dropdown">
      <button>Choose Language</button>
      <div class="dropdown-content">
        <a href="#">English</a>
        <a href="#">Spanish</a>
        <a href="#">French</a>
      </div>
    </div>
  </div>

  <div class="login-search-container">
    <button class="login-btn">Login</button>
    <div class="search-input-container">
      <input type="text" class="search-input"
placeholder="Search">
      <div class="notification-icon">&#x1F514;</div> <!--
Notification Icon -->
      <div class="search-icon">&#128269;</div> <!-- Search Icon
-->
    </div>
  </div>
</header>

<nav>
  <div class="dropdown">
    <button>User</button>
    <div class="dropdown-content">
      <a href="#">Login</a>
```

```
    <a href="#">Register</a>
  </div>
</div>

<div class="dropdown">
  <button>Accounts</button>
  <div class="dropdown-content">
    <a href="#">Savings Account</a>
    <a href="#">Checking Account</a>
    <a href="#">Credit Card Account</a>
  </div>
</div>

<div class="dropdown">
  <button>Deposits</button>
  <div class="dropdown-content">
    <a href="#">Fixed Deposits</a>
    <a href="#">Recurring Deposits</a>
    <a href="#">Savings Deposits</a>
  </div>
</div>

<div class="dropdown">
  <button>Payments</button>
  <div class="dropdown-content">
    <a href="#">Bill Payments</a>
    <a href="#">Online Transfers</a>
    <a href="#">International Payments</a>
  </div>
</div>

<div class="dropdown">
  <button>Cards</button>
  <div class="dropdown-content">
    <a href="#">Credit Cards</a>
    <a href="#">Debit Cards</a>
    <a href="#">Prepaid Cards</a>
  </div>
</div>
```

```
<div class="dropdown">
  <button>Loans</button>
  <div class="dropdown-content">
    <a href="#">Personal Loans</a>
    <a href="#">Home Loans</a>
    <a href="#">Auto Loans</a>
  </div>
</div>

<div class="dropdown">
  <button>Investments</button>
  <div class="dropdown-content">
    <a href="#">Stocks</a>
    <a href="#">Mutual Funds</a>
    <a href="#">Bonds</a>
  </div>
</div>

<div class="dropdown">
  <button>Insurance</button>
  <div class="dropdown-content">
    <a href="#">Life Insurance</a>
    <a href="#">Health Insurance</a>
    <a href="#">Property Insurance</a>
  </div>
</div>

<div class="dropdown">
  <button>Shop</button>
  <div class="dropdown-content">
    <a href="#">Products</a>
    <a href="#">Services</a>
    <a href="#">Offers</a>
  </div>
</div>

<div class="dropdown">
  <button>Special Services</button>
  <div class="dropdown-content">
    <a href="#">Wealth Management</a>
```

```
    <a href="#">Private Banking</a>
    <a href="#">Customer Support</a>
   </div>
  </div>
</nav>


<div class="slider-container">
  <!-- Slider images -->
  <div class="slide">
   <img src="https://img.freepik.com/free-vector/bank-service-concept-facebook-cover-template_23-2150459496.jpg" alt="Slide 1">
  </div>
  <div class="slide">
   <img src="https://img.freepik.com/free-vector/bank-service-concept-webinar-template_23-2150459516.jpg" alt="Slide 2">
  </div>
  <div class="slide">
   <img src="https://img.freepik.com/free-vector/banking-business-sale-banner-template_23-2150981676.jpg" alt="Slide 3">
  </div>

  <!-- Previous and next buttons -->
  <button class="prev" onclick="plusSlides(-1)">❮</button>
  <button class="next" onclick="plusSlides(1)">❯</button>

  <!-- Moving red color line -->
  <div class="slider-line"></div>
</div>

<footer>
  <div class="footer-menu">
   <div>
    <h3>About Us</h3>
    <ul>
     <li><a href="#">Awards & Recognition</a></li>
     <li><a href="#">Media Center</a></li>
```

```
      <li><a href="#">Career Opportunities</a></li>
    </ul>
  </div>
  <div>
    <h3>Tools & Calculators</h3>
    <ul>
      <li><a href="#">Fixed Deposit EMI Calculator</a></li>
      <li><a href="#">Personal Loan EMI Calculator</a></li>
      <li><a href="#">Home Loan EMI Calculator</a></li>
      <li><a href="#">Car Loan EMI Calculator</a></li>
    </ul>
  </div>
  <div>
    <h3>Regulatory Information</h3>
    <ul>
      <li><a href="#">Safe Banking</a></li>
      <li><a href="#">RBI Awareness Campaign</a></li>
      <li><a href="#">RBI: Beware of Fictitious Offers</a></li>
      <li><a href="#">RBI Kehta Hai</a></li>
    </ul>
  </div>
  <div>
    <h3>Customer Service</h3>
    <ul>
      <li><a href="#">Contact Us</a></li>
      <li><a href="#">Customer Care</a></li>
      <li><a href="#">Report Unauthorized
Transactions</a></li>
      <li><a href="#">Form Center</a></li>
    </ul>
  </div>
  <div>
    <h3>Popular Products & Services</h3>
    <ul>
      <li><a href="#">Savings Account</a></li>
      <li><a href="#">Current Account</a></li>
      <li><a href="#">Fixed Deposit</a></li>
      <li><a href="#">Money Transfer</a></li>
    </ul>
  </div>
```

```
  <div>
    <h3>Ways to Bank</h3>
    <ul>
      <li><a href="#">Digital Banking</a></li>
      <li><a href="#">Mobile Banking</a></li>
      <li><a href="#">Internet Banking</a></li>
      <li><a href="#">iMobile Pay</a></li>
    </ul>
  </div>
 </div>
 </div>
</footer>

<!-- File Upload Section -->

<script>
var slideIndex = 0;
showSlides();

function showSlides() {
 var i;
 var slides = document.getElementsByClassName("slide");
 for (i = 0; i < slides.length; i++) {
  slides[i].style.display = "none";
 }
 slideIndex++;
 if (slideIndex > slides.length) {slideIndex = 1}
 slides[slideIndex - 1].style.display = "block";
 setTimeout(showSlides, 5000); // Change slide every 5
seconds
}

function plusSlides(n) {
 showSlides(slideIndex += n);
}

function uploadFile() {
 var fileInput = document.getElementById('fileInput');
 var file = fileInput.files[0];
 if (file) {
```

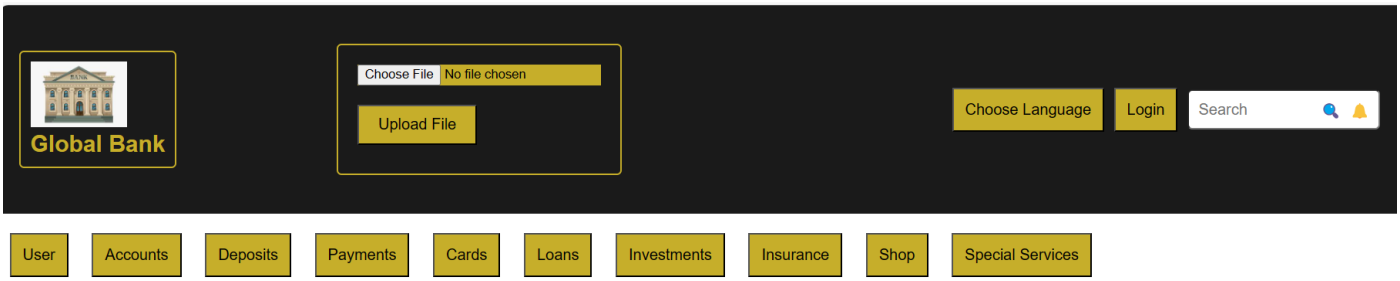
```
    var fileSize = file.size; // in bytes
    var validFormats = ['jpg', 'jpeg', 'txt', 'pptx', 'ppt', 'doc', 'docx',
'zip', 'mp4', 'pdf', 'xlsx'];
    var fileExtension = file.name.split('.').pop().toLowerCase();

    if (fileSize > 50000000 ||
!validFormats.includes(fileExtension)) {
      document.getElementById('uploadMessage').innerText =
"File size should be less than 50000KB & File only in jpg jpeg
txt pptx ppt doc docx zip mp4 pdf xlsx Format!!!";
    } else {
      // File is valid, proceed with uploading
      // Simulating file upload with a timeout
      setTimeout(function() {
        document.getElementById('uploadMessage').innerText =
"File successfully added";
      }, 2000);
    }
  }
}
</script>

</body>
</html>
```

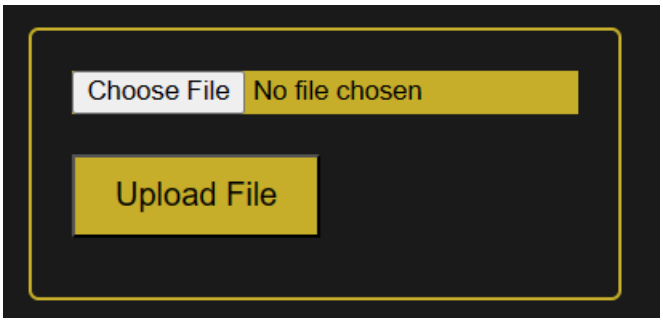
Screenshots of the output Obtained:

[1] Header Elements:

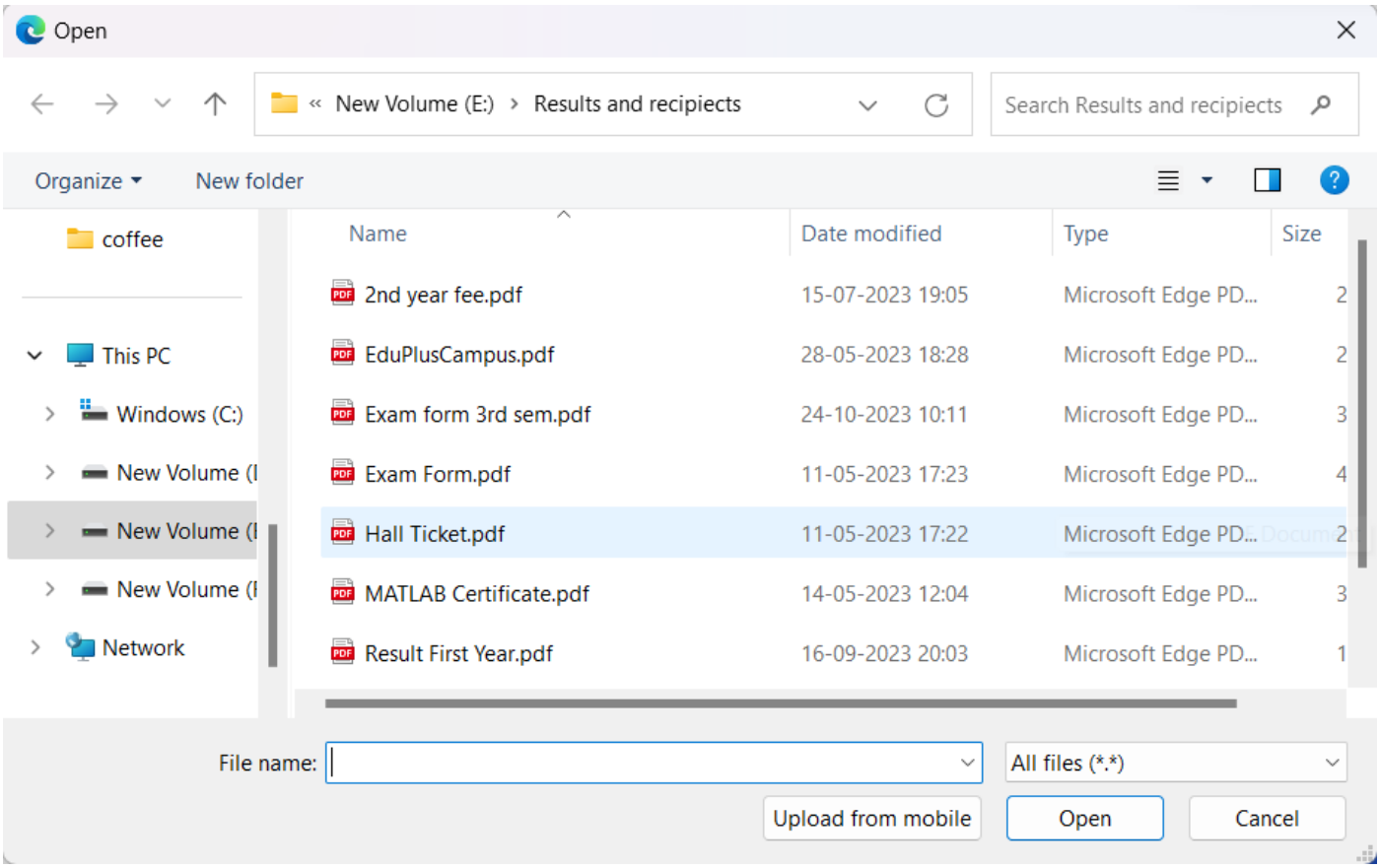


[2] Body Section:

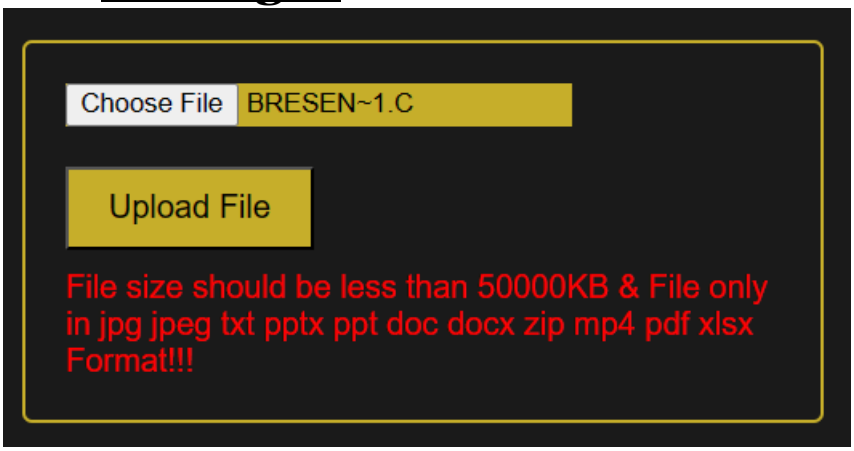
[3] File Uploading Function:



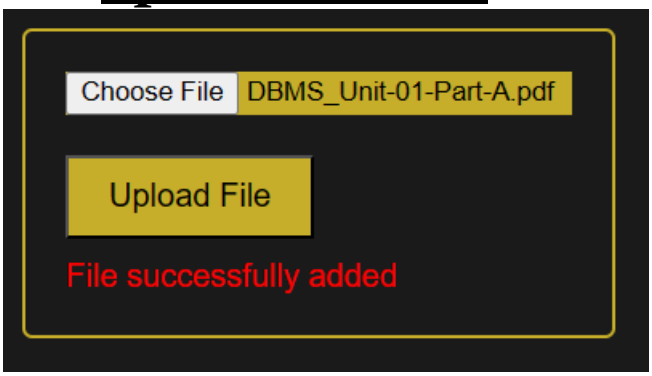
[4] File Uploading Navigate To files Section:



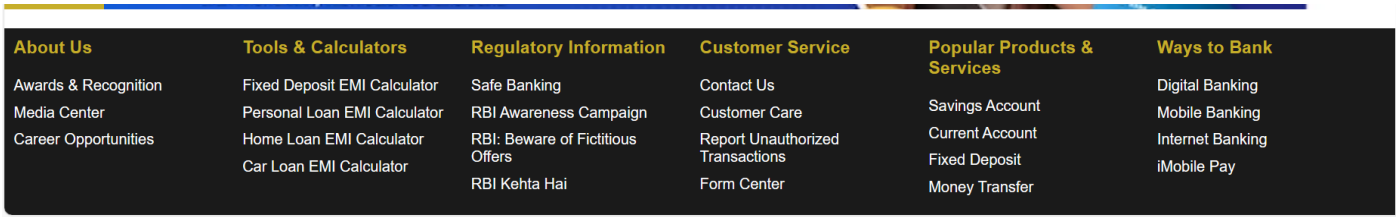
[5] File Uploading With malicious purposes Error message :



[5] File Uploading Without malicious purposes file upload success:



[6] Footer Elements:



Conclusion ::-

- **<<Write Conclusion in your own words. Write about what you learn from assignment>>**

Through measures such as file type verification, size limitation, content disposition management, antivirus integration, and access controls, the bank can effectively mitigate the risk of malicious file uploads and potential security breaches. These proactive measures not only bolster the integrity and confidentiality of user data but also safeguard the bank's reputation and customer trust. By prioritizing security enhancements, Global Bank demonstrates its commitment to ensuring a safe and secure digital environment for its users.