



INT6005CEM

BCSCUN

CS1

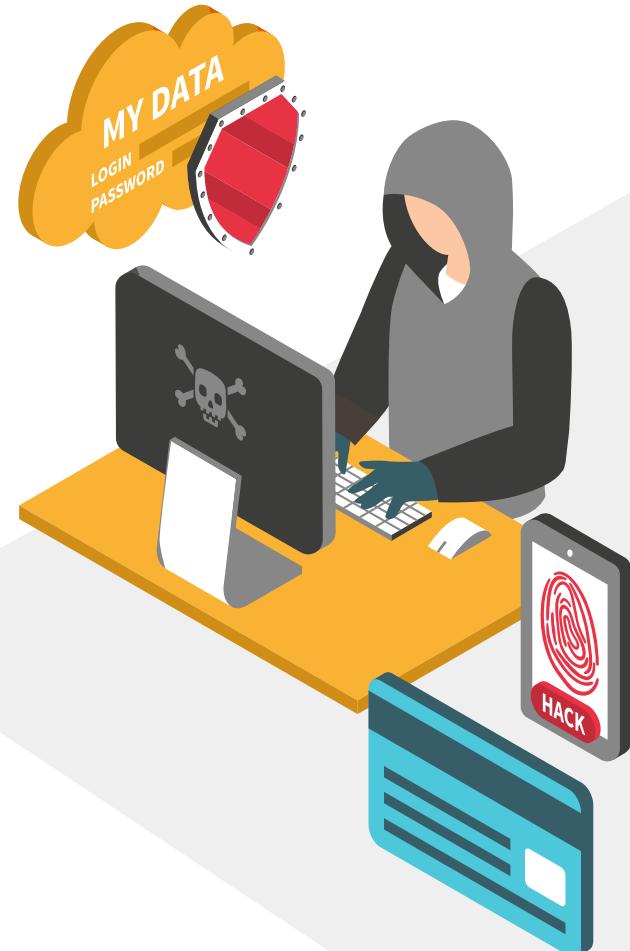
Lau En Sin (15731047)

Arief bin Abdul Latib (15730888)

Bryan Yeoh Seng Sheng (15730936)

Hsia Hao Ze (15730992)

Khor Cojean (15731014)



NECESSARY LINKS

GITHUB LINK

- Original System GitHub Link

<https://github.com/m-2199015/Online-Computer-Store.git>

- Enhanced System GitHub Link

https://github.com/Ensin2004/INT6005CEM_group_assignment_G23.git

USER MANUAL

- https://github.com/Ensin2004/INT6005CEM_group_assignment_G23/tree/main/User%20Manual

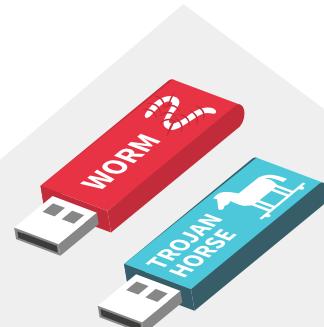


TABLE OF CONTENTS



01

SYSTEM OVERVIEW

02

SECURITY ANALYSIS

03

SECURITY IMPLEMENTATION

04

DISCUSSION

05

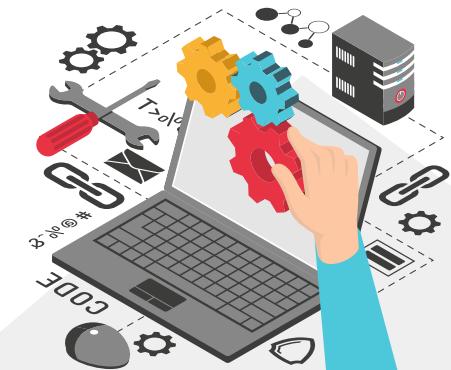
SUMMARY





01.

SYSTEM OVERVIEW



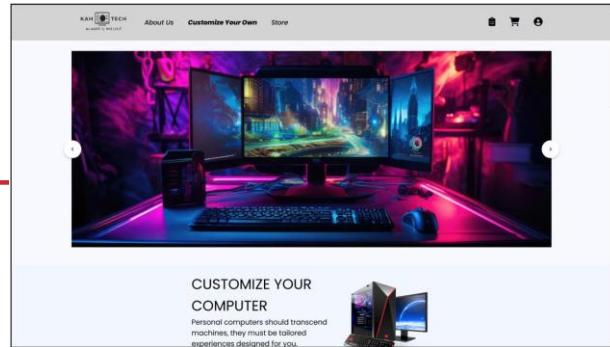
OUR SYSTEM

KAHTECH

Online computer store platform for customers in to browse PC components, and place order.

Features

Explore accessories, view product details and customize PC builds



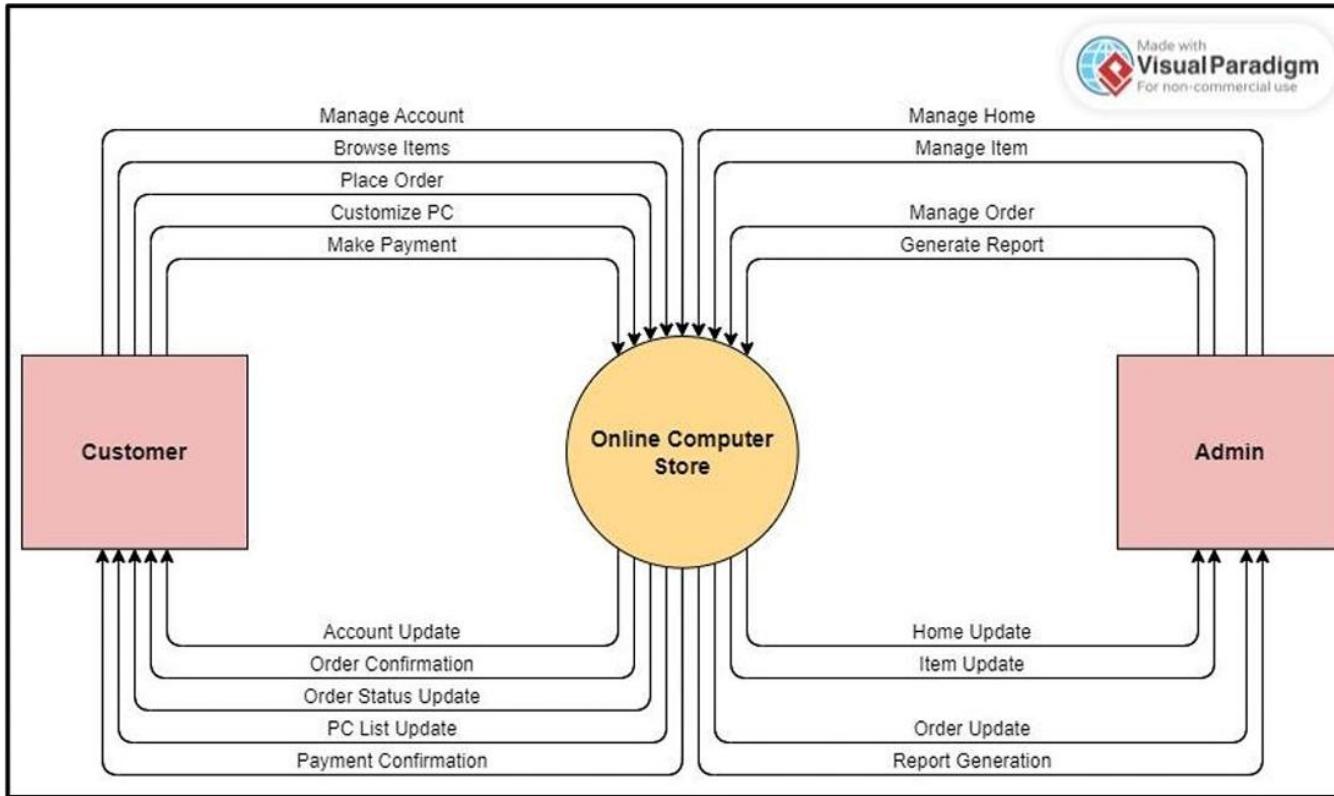
User roles

User and Admin

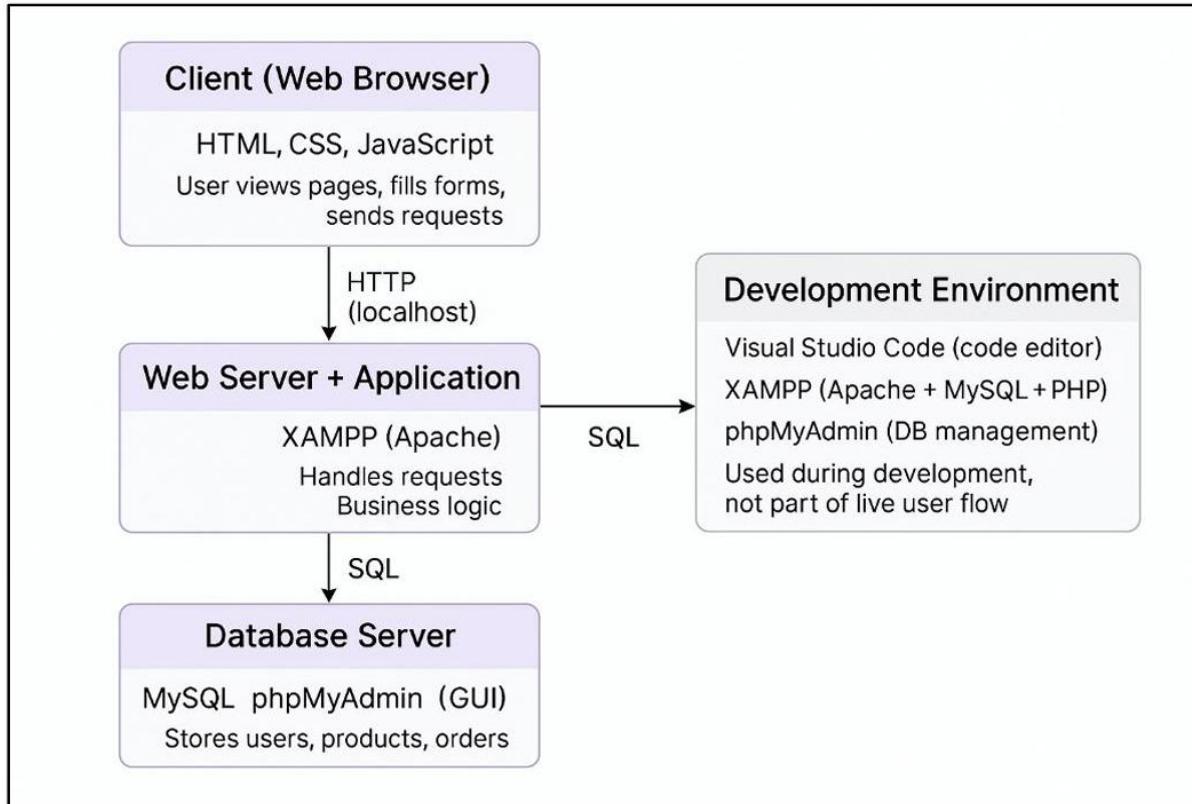
Ordering & Admin

Users can order with TNG e-Wallet or COD, Admins manage products, stock orders and reports

SYSTEM FUNCTIONALITIES



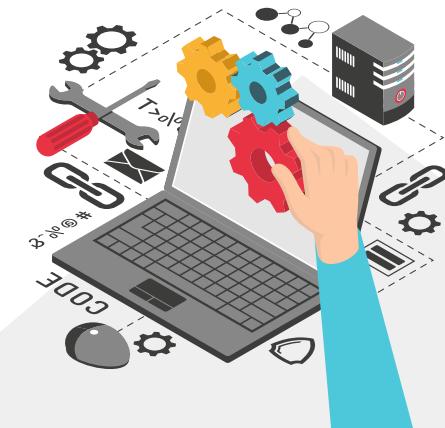
SYSTEM ARCHITECTURE





02.

SYSTEM ANALYSIS





SYSTEM ANALYSIS

01

Authentication

Lack of login rate limiting, super admin and forgot password features.

03

Email Account Handling

Lack of email verification and backup email implementation.



02

Password Security

Lack of strong password and password hashing implementation.

04

Data Privacy & User Education

Lack of data privacy policy and user education.



SYSTEM ANALYSIS

05

Session Management

Lack of session timeout, protection against session fixation and CSRF attacks.

07

Error Handling

Lack of page and system error handling.



06

Audit Logging

Lack of audit logging feature.

08

Input Validation & Cleaning

Lack of input validation, auto-trim, whitespace check and length input limit.



SYSTEM ANALYSIS

09

SQL Injection

Lack of protection against error-based, union-based and blind SQL injection.

11

Cryptography

Lack of protection against data-in-transit and data-at-rest.



10

Cross-Site Scripting (XSS)

Lack of protection against reflected, stored and DOM-based XSS.

12

Secure Cookies

Lack of secure cookies implementation.



SYSTEM ANALYSIS

13

Digital Certificate

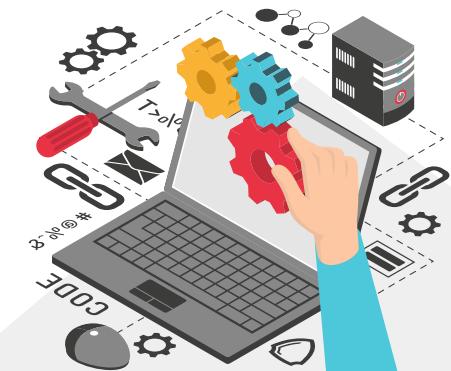
Lack of digital certificate deployment.





03.

SYSTEM IMPLEMENTATION





03.

SYSTEM IMPLEMENTATION (1. AUTHENTICATION)

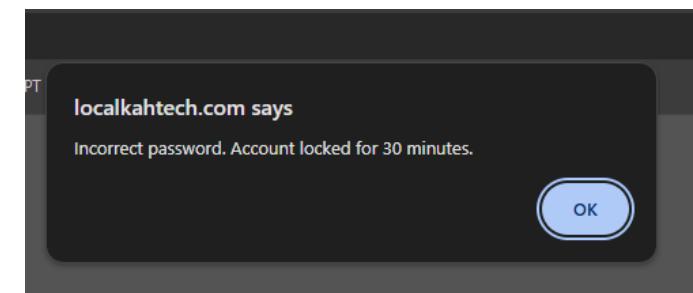
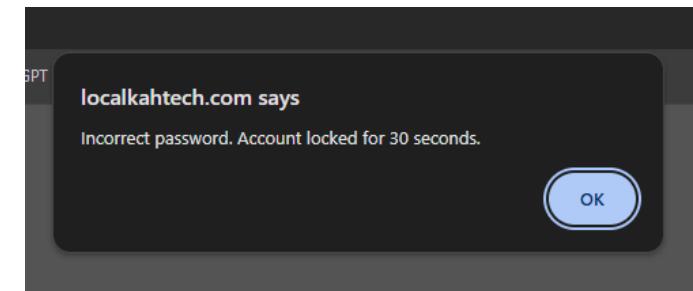




Login Rate Limiting

```
39
40     $current_time = date("Y-m-d H:i:s");
41
42     // Check whether account is locked or not
43     if (!is_null($row['lock_until']) && $row['lock_until'] > $current_time) {
44         $remaining = strtotime($row['lock_until']) - time();
45         echo "<script> alert('Account is locked. Please try again after (" . $remaining . " seconds.');" . window.location.href='..../login.php'; </script>";
46         exit();
47     }
48
49     // Check whether password is correct or not
50     if (!password_verify($password, $row['pwd'])) {
51         $wrong_pwd_count = $row['wrong_pwd_count'] + 1;
52         $lock_until = null;
53         $lock_message = '';
54
55         // Account lock time
56         if ($wrong_pwd_count < 6) {
57             $lock_until = null;
58             $lock_message = "Incorrect password.";
59         } elseif ($wrong_pwd_count == 6) {
60             $lock_until = date("Y-m-d H:i:s", strtotime("+30 seconds"));
61             $lock_message = "Incorrect password. Account Locked for 30 seconds.";
62         } elseif ($wrong_pwd_count == 7) {
63             $lock_until = date("Y-m-d H:i:s", strtotime("+1 minute"));
64             $lock_message = "Incorrect password. Account locked for 1 minute.";
65         } elseif ($wrong_pwd_count == 8) {
66             $lock_until = date("Y-m-d H:i:s", strtotime("+5 minutes"));
67             $lock_message = "Incorrect password. Account locked for 5 minutes.";
68         } elseif ($wrong_pwd_count == 9) {
69             $lock_until = date("Y-m-d H:i:s", strtotime("+10 minutes"));
70             $lock_message = "Incorrect password. Account locked for 10 minutes.";
71         } elseif ($wrong_pwd_count > 9) {
72             $lock_until = date("Y-m-d H:i:s", strtotime("+30 minutes"));
73             $lock_message = "Incorrect password. Account locked for 30 minutes.";
74         }
75
76         // Update database
77         mysql_query(
78             $conn,
79                 "UPDATE users SET wrong_pwd_count = '$wrong_pwd_count', lock_until = " . ($lock_until ? "'$lock_until'" : "NULL") . " WHERE id = '" . ($row['id']) . "'"
80         );
81
82         // Display messages
83         echo "<script> alert('$lock_message'); window.location.href='..../login.php'; </script>";
84     } else {
85

```



- Protect the system from brute-force and automated password-guessing attacks.





Super Admin Role Setup

```
$_SESSION['ID'] = $row['id'];
$_SESSION['AdminName'] = $row['admin_name'];
$_SESSION['role'] = $row['role'];
$_SESSION['status'] = $row['account_status'];
```

```
<?php if (isset($_SESSION['role']) && $_SESSION['role'] === 'super_admin') { ?>
    <a class="menu_button" href="managers.php">
        <i class="fa-solid fa-users-gear"></i>
        <p class="menu_text">MANAGERS</p>
    </a>
</?php } ?>
```

```
4 if (isset($_GET['id']) && isset($_GET['action'])) {
5     $adminId = $_GET['id'];
6     $action = $_GET['action'];
7
8     if ($action === 'ban') {
9         $sql = "UPDATE admins SET account_status = 'banned' WHERE id = ?";
10    } elseif ($action === 'unban') {
11        $sql = "UPDATE admins SET account_status = 'active' WHERE id = ?";
```

```
if (isset($row['account_status']) && strtolower(string: $row['account_status']) === 'banned') {
    echo "<script>alert('Your account has been banned. Please contact the system administrator.');" . window.history.go(-1);</script>";
    exit();
}
```

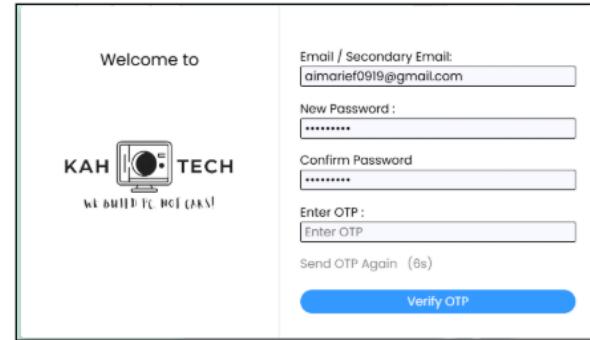


Role Based Access Control, managers do not have access to “managers” page, only admins are able to access it and manage managers.



Forgot Password Mechanism

```
$checkEmail = mysqli_num_rows(result: mysqli_query(mysql: $conn, query: "SELECT email FROM users WHERE LOWER(email) = LOWER('$email') OR LOWER(second_email) = LOWER('$email')"));  
  
if ($checkEmail == 0) {  
    echo "<script>alert('Email not exists'); window.history.go(-1);</script>";  
    exit;  
  
$otp = rand(min: 10000, max: 99999);  
$otpExpiresAt = time() + 60;  
// Send OTP via email  
$to = $email;  
$from = "kahtechpng@gmail.com";  
$fromName = "KAHTECH";  
$message = $otp . " is your OTP.";  
$subject = "Secondary Email Verification";  
$header = 'From: ' . $fromName . ' <' . $from . '>';  
  
mail(to: $to, subject: $subject, message: $message, additional_headers: $header)
```



- Avoid permanent lock out when user forget the password, also prevent social engineering risk especially for those who store their login information on another platform or physically.





03.

SYSTEM IMPLEMENTATION **(2. PASSWORD SECURITY)**





Strong Password Validation

```
script>
document.getElementById('newPassword').addEventListener('input', validatePassword);
document.getElementById('confirmPassword').addEventListener('input', validatePassword);

function validatePassword() {
    var password = document.getElementById('newPassword').value;
    var confirmPassword = document.getElementById('confirmPassword').value;
    var pwd_validation_container = document.getElementById('pwd_validation_container');
    var pwd_confirmation = document.getElementById('pwd_confirmation');
    var pwd_character = document.getElementById('pwd_character');
    var pwd_letter = document.getElementById('pwd_letter');
    var pwd_number = document.getElementById('pwd_number');
    var pwd_symbol = document.getElementById('pwd_symbol');
    var submit_btn = document.getElementById('submit_btn');

    const passwordRegex = /^(?=.*[a-zA-Z])(?=.*\d)(?=.*[$!@#%^&])[A-Za-z\d$!@#%^&]{8,20}$/;

    if (!passwordRegex.test(password) || confirmPassword != password) {
        submit_btn.disabled = true;
    }

    if (!passwordRegex.test(password)) {
        pwd_validation_container.style.display = "block";
        pwd_confirmation.style.display = "none";
    }

    if (password.length < 8 || password.length > 20) {
        pwd_character.style.display = "block";
    } else {
        pwd_character.style.display = "none";
    }

    if (!/[a-zA-Z]/.test(password)) {
        pwd_letter.style.display = "block";
    } else {
        pwd_letter.style.display = "none";
    }

    if (!/\d/.test(password)) {
        pwd_number.style.display = "block";
    } else {
        pwd_number.style.display = "none";
    }

    if (!/[!@#%^&]/.test(password)) {
        pwd_symbol.style.display = "block";
    } else {
        pwd_symbol.style.display = "none";
    }
}

else {
    pwd_validation_container.style.display = "none";
    pwd_confirmation.style.display = "block";
    submit_btn.disabled = false;
}
}


```



Name :

Email :

Phone Number :

Address :

New Password :

Password requirements:
* 8-20 characters
* at least one letter (A-Z)
* at least one number (0-9)
* at least one special characters (@\$!%*?&)
* no spaces allowed

Confirm Password

I confirm that I have read and agree to KAH TECH
 User Agreement and [Privacy & User Education Policy](#).

Sign up

Already have an account? [Log In](#).

Enforced strong password validation, requiring 8-20 characters, one letter, one number, one special character and no spaces allowed.





Password Hashing & Salting

```
$ARGON_OPTS = [  
    'memory_cost' => 131072, // 128 MB  
    'time_cost'     => 3,      // 3 iterations  
    'threads'       => 1  
];
```

```
'password = password_hash($_POST["newPassword"], PASSWORD_ARGON2ID, $ARGON_OPTS);
```

| | | | | | |
|----|-------------|---------------------------------|-------------|---------------------------|---|
| 16 | Kamen Rider | p22014743@student.newini.edu.my | 019-8284731 | Seri Melati, George Town | Kamen123@ |
| 17 | Tan Mei Mei | p22014743@student.newini.edu.my | 017-2374621 | Air Itam Dam | Tanmeime123@ |
| 19 | Junzo | junzobry28@gmail.com | 0123456789 | bryan 123, at jalan bryan | \$argon2id\$v=19\$m=131072,t=3,p=1\$8kxTbjjW7ktORjZEZE5kbw\$Hi/rZQBEULzlF+3Y8KpgczH5z0VVUMBRYvGEWM8dfEg |

| | | | |
|---|-----------|------|------|
| \$argon2id\$v=19\$m=131072,t=3,p=1\$8kxTbjjW7ktORjZEZE5kbw\$Hi/rZQBEULzlF+3Y8KpgczH5z0VVUMBRYvGEWM8dfEg | | | |
| | Meta Data | Salt | Hash |

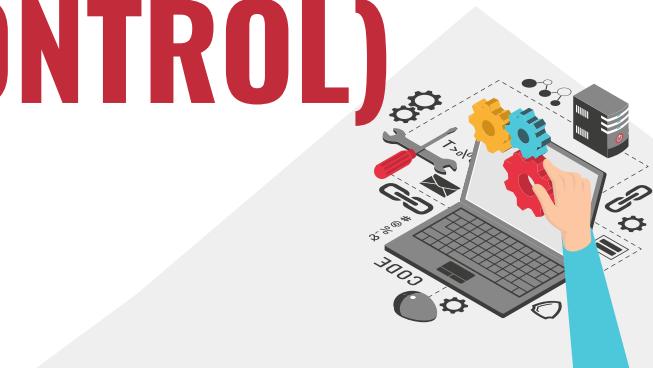


Converts passwords into irreversible hashes with unique salts instead of plaintext so stolen database data cannot reveal the original passwords



03.

SYSTEM IMPLEMENTATION **(3. MFA & EMAIL CONTROL)**





Email Verification

```
$checkResult = mysqli_num_rows(result: mysqli_query(mysql: $conn,
query: "SELECT user_name FROM users WHERE LOWER(user_name) = LOWER('$name');");
$checkEmail = mysqli_num_rows(result: mysqli_query(mysql: $conn,
query: "SELECT email FROM users WHERE LOWER(email) = LOWER('$email');");
$checkSecondaryEmail = mysqli_num_rows(result: mysqli_query(mysql: $conn,
query: "SELECT secondary_email FROM users WHERE LOWER(secondary_email) = LOWER('$email');"));

$otp = rand(min: 10000, max: 99999);
$otpExpiresAt = time() + 60;
// Send OTP via email
$to = $email;
$from = "kahtechpng@gmail.com";
$fromName = "KAHTECH";
$message = $otp . " is your OTP.";
$subject = "New Account Sign Up";
$header = 'From: ' . $fromName . ' <' . $from . '>';

mail(to: $to, subject: $subject, message: $message, additional_headers: $header)
```

The screenshot shows a registration form for a service named KAH TECH. The form fields include:

- Name: Arief Student
- Email: p22014743@student.newinti.edu.my
- Phone Number: 0123456789
- Address: Taman Seri Sarl
- New Password: (redacted)
- Confirm Password: (redacted)
- Enter OTP: (redacted)
- Send OTP Again (8s)
- Verify OTP (button)

Below the form, there is a note: "WE BUILT FC NOT CARST". At the bottom right, it says "Already have an account? Log in."

- Username and email addresses that are used cannot be used again and OTP will be sent for verification so one email can only sign up for one time to prevent any spamming of bot accounts which may lead to DDOS attack.





Backup Email / Recovery with MFA

```
$checkEmail = mysqli_num_rows(result: mysqli_query(mysql: $conn, query: "SELECT email FROM users WHERE LOWER(email) = LOWER('$email') OR LOWER(secondary_email) = LOWER('$email');");
$query = mysqli_query(mysql: $conn, query: "SELECT * FROM users WHERE email = '$firstEmail'");
$row = mysqli_fetch_assoc(result: $query);

if (mysqli_num_rows(result: $query) == 0 || $row['pwd'] != $confirmPassword) {
    echo "<script> alert('Wrong password'); window.history.go(-1); </script>";
    exit;
}

if ($checkEmail != 0) {
    echo "<script>alert('Email already exists'); window.history.go(-1);</script>";
    exit;
}

$noAutoSend = isset($_POST['no_autosend']) || isset($_GET['no_autosend']);
$otp = $_POST['otp'] ?? $_GET['otp'] ?? null;
$otpExpiresAt = $_POST['otp_expires_at'] ?? $_GET['otp_expires_at'] ?? null;

$firstEmail = htmlspecialchars(string: $_POST['primaryEmail'] ?? $_GET['primaryEmail'] ?? '');
$email = htmlspecialchars(string: $_POST['secondaryEmail'] ?? $_GET['secondaryEmail'] ?? '');
$confirmPassword = htmlspecialchars(string: $_POST['confirmPassword'] ?? $_GET['confirmPassword'] ?? '');

// Send OTP via email
$to = $email;
$from = "kahtech@gmail.com";
$fromName = "KAHTECH";
$subject = "Secondary Email Verification";
$header = 'From: ' . $fromName . '<' . $from . '>';

if (($otp === null) && !$noAutoSend) || isset($_POST['resend'])) {
    $otp = rand(min: 10000, max: 99999);
    $otpExpiresAt = time() + 60; // seconds
    $message = $otp . " is your OTP.";
    @mail(to: $to, subject: $subject, message: $message, additional_headers: $header);
}
```

Name :

Email :

Secondary Email (Optional) :

Phone Number :

Address :

New Password :

Confirm Password :

Email :

Enter OTP :

Send OTP Again

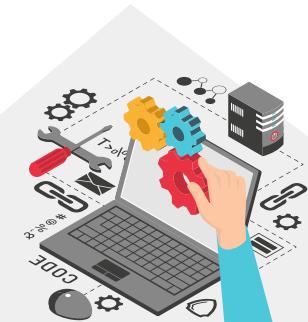
- If the main email has problems, the backup allows users to have a second way to prove ownership which prevent users from being permanently unavailable from the system.





03.

SYSTEM IMPLEMENTATION **(4. DATA PRIVACY & USER EDUCATION)**





Data Privacy & User Education

```
<!-- === consent checkbox === -->


<label style="display:flex; gap:8px; align-items:flex-start; line-height:1.4;">
    <input type="checkbox" id="agree_terms" style="margin-top:3px;">
    <span>
      I confirm that I have read, consent to, and agree to KAH TECH
      <a href="user-agreement.php" target="_blank" rel="noopener">User Agreement</a>
      and
      <a href="privacy-education.php" target="_blank" rel="noopener">Privacy & User Education Policy</a>
    </span>
  </label>
  <p id="agree_error" style="display:none; color:#c8392b; margin-top:6px;">
    Please tick the checkbox to agree before signing up.
  </p>


```

The screenshot shows a registration form with the following fields:

- Name: ensin
- Email: ensin2004@gmail.com
- Phone Number: 0191111111
- Address: inti college penang, bayan lepas
- New Password: [REDACTED]
- Confirm Password: [REDACTED]
- I confirm that I have read, consent to, and agree to KAH TECH User Agreement and Privacy & User Education Policy.
- Please tick the checkbox to agree to the User Agreement and Privacy Policy.

At the bottom is a large blue "Sign up" button.

User agreement

This screenshot shows the "User Agreement" page with the following content:

User Agreement

This Agreement governs your access and use of the KAH TECH websites, applications, and related services. By clicking on "I accept" or using our platforms, you agree to these terms.

Table of Contents

- 1 Acceptance of Terms
- 2 Eligibility & Account
- 3 Acceptable Use
- 4 Intellectual Property
- 5 Privacy & User Education Policy
- 6 Cookies & Analytics
- 7 Disclaimers & Limitation
- 8 Suspension/Termination
- 9 Arbitration
- 10 Governing Law

1 Acceptance of Terms

By agreeing for an account, accessing, or using our website you agree to be bound by this user agreement and our [Privacy & User Education Policy](#). If you do not agree, do not use the services.

2 Eligibility & Account

You must be at least 18 years old or have legal guardian consent to create an account.

- You are responsible for the confidentiality of your credentials and not disclose them under your account.
- Provide accurate information throughout when you change.

I agree to use a password manager and never reuse passwords across different sites.

3 Acceptable Use

You agree not to misuse the service. Prohibited behavior include (without limitation):

- attempting unauthorized access, probing, or security testing without explicit permission;
- transmitting malicious, harmful code or engaging in activities that disrupt or degrade service;
- spamming, flooding, or otherwise abusing the system;
- violating laws, regulations, or ethical standards, including those relating to privacy or rights.

We may investigate violations and comply with law enforcement or regulatory requests.

4 Intellectual Property

All trademarks, logos, marks, designs, and content are the property of KAH TECH or its licensors and are protected by applicable law. You may not copy, modify, or distribute materials without prior written consent.

Privacy & user education

This screenshot shows the "Privacy & User Education Policy" page with the following content:

Privacy & User Education Policy

KAH TECH is protecting your data and empowering you to stay safe online one step at a time. This page contains our privacy commitments with clear guidance for secure and responsible use.

Table of Contents

- 1 Privacy Overview
- 2 Data We Collect
- 3 How We Use Data
- 4 Security Measures
- 5 Cookies & Analytics

1 Privacy Overview

KAH TECH is committed to protect and respect our users, we do not sell or rent personal data. When we do it's for very specific purposes (sharing, analysis) they are stored by confidential and secure delegations.

2 Data We Collect

- Account data: name, email, phone number, address (provided during registration/appointment).
- Technical/device data: IP address, browser type, device identifiers, pages visited, interactions (or security, diagnostics, and performance).

3 How We Use Data

- It collects/changes your account, deliver core features, and provide support.
- To measure service reliability, prevent fraudulence, and improve user experience.
- To send promotional messages (policy updates, service alerts). Marketing messages are sent only with consent and can be opted out at any time.

4 Security Measures

We apply reasonable technical and organizational measures, including encryption in transit, password hashing of user accounts, audit logs, and vulnerability monitoring. No method of communication is 100% secure, but we continuously improve our mitigations.

I agree to keep my personal information up-to-date and enable two-factor authentication. Avoid sharing passwords across different sites.

5 Cookies & Analytics

We use cookies to keep you signed in, remember preferences, and understand usage. You can control cookies in your browser settings. Blocking cookies may impact some functionality.

These controls ensure every user clearly understands the terms, privacy practices and safety guidelines before creating an account





03.

SYSTEM IMPLEMENTATION

(5. SESSION MANAGEMENT & CSRF PROTECTION)

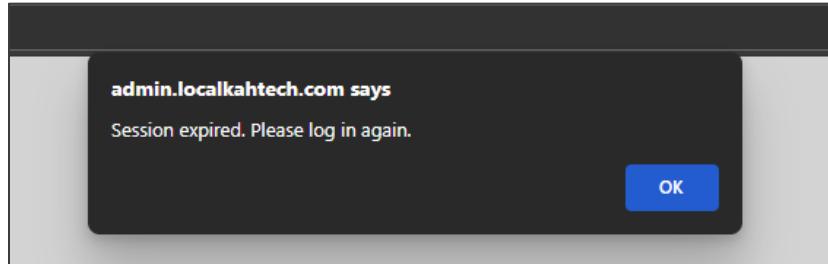




Session Timeout

```
JS sessionTimeout.js ✘ security.php
js > JS sessionTimeout.js > ...
js > 1 // Timeout minutes
2 const timeoutMinutes = 5;
3
4 // Timeout seconds
5 const timeoutSeconds = timeoutMinutes * 60;
6
7 // Idle time counter in seconds
8 let idleTime = 0;
9
10 // Session flag
11 let sessionExpired = false;
12
13 // Reset idle time counter
14 function resetIdleTime() {
15   |   idleTime = 0;
16 }
17
18 // Increment idle time every 10 seconds
19 const idleInterval = setInterval(() => {
20   if (sessionExpired) return;
21
22   idleTime += 10;
23
24   // Log out if idle time = timeout time
25   if (idleTime >= timeoutSeconds) {
26     sessionExpired = true;
27     window.location.href = "includes/logoutAccount.php?timeout=1";
28   }
29 }, 10000);
30
31 // Detect user activity and reset idle time counter
32 document.addEventListener("mousemove", resetIdleTime);
33 document.addEventListener("click", resetIdleTime);
34 document.addEventListener("scroll", resetIdleTime);
35 document.addEventListener("keydown", resetIdleTime);
```

```
16
17 // Session Timeout Check
18 $timeoutSeconds = 300;
19
20 if (isset($_SESSION['LastActivity']) && (time() - $_SESSION['LastActivity']) >= $timeoutSeconds) {
21   |   echo "<script> window.location.href='includes/logoutAccount.php?timeout=1'; </script>";
22   |   exit;
23 }
24
25 $_SESSION['LastActivity'] = time();
26
```



- Protect the system from risks associated with unattended devices, shared computers and session misuse.





Session Regeneration

```
loginuser.php X logoutAccount.php  
includes > loginuser.php > ...  
88     mysqli_query(  
89         $conn,  
90         "UPDATE users SET wrong_pwd_count = 0, lock_until = NULL WHERE id = '{$row['id']}'"  
91     );  
  
    // Regenerate session ID (prevent session fixation)  
    session_regenerate_id(true);  
  
    // Update session  
    $_SESSION['ID'] = $row['id'];  
    $_SESSION['UserName'] = $row['user_name'];  
  
    // Display messages  
    echo "<script> alert('Log in successfully'); window.location.href='../../index.php'; </script>";  
100  
101
```

```
loginuser.php X logoutAccount.php X  
includes > logoutAccount.php > ...  
25     $params['httponly']  
26     );  
27 }  
  
// 3. Destroy the session on the server  
30 session_unset();  
31 session_destroy();  
  
// 4. Start new empty session with new session id  
34 session_start();  
35 session_regenerate_id(true);  
  
// 5. Redirect with alert  
38 echo "<script>alert('Log out successfully'); window.location.href='../../index.php';</script>";  
39 exit;
```

| EXCLUSIONS | | IndexedDB | cookies | localStorage | sessionStorage | File API | Web Workers | IndexedDB | Cookies | localStorage | sessionStorage | File API | Web Workers |
|---------------|------------------------|------------------|---------|---------------------------|----------------|----------|-------------|-----------|---------|--------------|----------------|----------|-------------|
| cfz_google... | %7B%22nzc_ga... | .cl... | / | 2... | 130 | ✓ | ✓ | Lax | | | | | |
| cfz_reddit | %7B%22fZaD_re... | .cl... | / | 2... | 139 | ✓ | ✓ | Lax | | | | | |
| kndctr_8A... | GY1NzQwOTcx... | .cl... | / | 2... | 137 | ✓ | ✓ | Lax | | | | | |
| OptanonC... | isGpcEnabled=0... | .cl... | / | 2... | 391 | | | Lax | | | | | |
| PHPSESSID | 1lrqjke0cgpij4cs0ns... | localStorage | / | S... | 35 | ✓ | ✓ | St... | | | | | |
| zaraz-cons... | {"Tuku":true,"aM... | .cl... | / | 2... | 38 | | | St... | | | | | |
| Cookie Value | | Show URL-decoded | | 1lrqjke0cgpij4cs0nsd5afa5 | | | | | | | | | |

Before login

| EXCLUSIONS | | IndexedDB | cookies | localStorage | sessionStorage | File API | Web Workers | IndexedDB | cookies | localStorage | sessionStorage | File API | Web Workers |
|---------------|---------------------|------------------|---------|---------------------------|----------------|----------|-------------|-----------|---------|--------------|----------------|----------|-------------|
| cfz_google... | %7B%22nzc_ga... | .cl... | / | 2... | 130 | ✓ | ✓ | Lax | | | | | |
| cfz_reddit | %7B%22fZaD_re... | .cl... | / | 2... | 139 | ✓ | ✓ | Lax | | | | | |
| kndctr_8A... | GY1NzQwOTcx... | .cl... | / | 2... | 137 | ✓ | ✓ | Lax | | | | | |
| OptanonC... | isGpcEnabled=0... | .cl... | / | 2... | 391 | | | Lax | | | | | |
| PHPSESSID | 24chhpdm456atkr... | localStorage | / | S... | 35 | ✓ | ✓ | St... | | | | | |
| zaraz-cons... | {"Tuku":true,"aM... | .cl... | / | 2... | 38 | | | St... | | | | | |
| Cookie Value | | Show URL-decoded | | 24chhpdm456atkrupi4ea4g98 | | | | | | | | | |

After login

- Attackers can no longer reuse or fix the session ID on the victim's device, mitigate the risk of session fixation attacks.





CSRF Token Implementation

The figure displays several screenshots illustrating a CSRF implementation and an attack. On the left, the code for `updateUserAccount.php` shows session handling and CSRF token creation. In the middle, a browser window shows an attempt to attack `editAccountForm.php`. The rightmost screenshot shows a ChatGPT interface where an error message from `localkahtech.com` is displayed.

Code Snippet (`updateUserAccount.php`):

```
3 // Start session if not started
4 if (session_status() === PHP_SESSION_NONE) {
5     session_start();
6 }
7
8 // Create new CSRF token if not set or expired
9 function createCSRFToken() {
10
11    if (!isset($_SESSION['CSRFToken']) || !isset($_SESSION['CSRFTokenExpiry']) || time() > $_SESSION['CSRFTokenExpiry']) {
12        $_SESSION['CSRFToken'] = bin2hex(random_bytes(32));
13        $_SESSION['CSRFTokenExpiry'] = time() + 1800;
14    }
15
16    return $_SESSION['CSRFToken'];
17 }
18
19 // Check CSRF token
20 function checkCSRFToken($token) {
21
22    // Ensure all variables are set
23    if (!isset($_SESSION['CSRFToken']) || !isset($_SESSION['CSRFTokenExpiry']) || !isset($token)) {
24        return false;
25    }
26
27    // Check CSRF token expiry
28    if (time() > $_SESSION['CSRFTokenExpiry']) {
29        unset($_SESSION['CSRFToken']);
30        unset($_SESSION['CSRFTokenExpiry']);
31        return false;
32    }
33
34    // Check CSRF token validity
35    if (hash_equals($_SESSION['CSRFToken'], $token)) {
36        unset($_SESSION['CSRFToken']);
37        unset($_SESSION['CSRFTokenExpiry']);
38        return true;
39    } else {
40        return false;
41    }
42 }
43
44 // Create hidden input for CSRF token
45 function createCSRFInput() {
46     $token = createCSRFToken();
47     echo "<input type='hidden' name='csrfToken' value='" . htmlspecialchars($token) . "'>";
48 }
```

Browser Screenshot:

`editAccountForm.php` code snippet:

```
36     <!-- Biggest box in body to set background -->
37     <div class="accDisplay">
38         <!-- Set up sign in content -->
39         <form class="signUp" action="includes/updateUserAccount.php" method="post" enctype="multipart/form-data">
40             <input type="text" name="username" value="" />
41             <div class="signUpPw" >
42                 <div class="img_container">
```

`updateUserAccount.php` code snippet:

```
10 session_start();
11 require_once "dbh.inc.php";
12 require_once "csrf.php";
13
14 > $ARGON_OPTS = [
15 ];
16
17 if ($_SERVER["REQUEST_METHOD"] == "POST") {
18
19     // Check CSRF token
20     if (!isset($_POST['csrfToken']) || !checkCSRFToken($_POST['csrfToken'])) {
21         die('<script> alert("Invalid or expired CSRF token. Please refresh the page and try again."); window.history.go(-1); </script>');
22     }
23
24     // Collect Form data
25     $name = htmlspecialchars(trim($_POST["newUsername"]));
26     $email = htmlspecialchars(trim($_POST["newEmail"]));
27     $phone = htmlspecialchars(trim($_POST["newPhone"]));
28 }
```

ChatGPT Screenshot:

localkahtech.com says
Invalid or expired CSRF token. Please refresh the page and try again.

- CSRF token prevents request from unauthorized websites to be executed.



03.

SYSTEM IMPLEMENTATION **(6. LOGGING & MONITORING)**





Logging & Monitoring

Admin

Account

Audit Logs

Actor (Name ID) Action Outcome Entity Type Entity ID Export CSV

e.g. #1 e.g. admin_update All e.g. items e.g. 55 Reset Apply

From (date) To (date) Search summary Per Page mm/dd/yyyy mm/dd/yyyy contains... 20

| Time | Actor | Action | Entity | Summary | Outcome | IP | View |
|---------------------|----------------|------------------|-----------|---|---------|---------|----------------------|
| 2025-11-14 19:25:49 | #1 super_admin | login_success | - | Admin logged in | success | 1.1.1.1 | View |
| 2025-11-14 19:25:26 | #1 | login_failure | - | Admin login failed: name=admin, email=envin2004@gmail.com | failure | 1.1.1.1 | View |
| 2025-11-14 19:25:08 | #1 super_admin | logout | admins #2 | Admin logged out | success | 1.1.1.1 | View |
| 2025-11-14 18:44:53 | #1 super_admin | login_success | - | Admin logged in | success | 1.1.1.1 | View |
| 2025-11-14 18:44:34 | #1 super_admin | login_failure | - | Wrong password for admin #1 | failure | 1.1.1.1 | View |
| 2025-11-14 18:43:55 | #1 super_admin | logout | admins #2 | Admin logged out | success | 1.1.1.1 | View |
| 2025-11-14 18:24:15 | #1 super_admin | item_soft_delete | items #3 | Soft-deleted item #3 | success | 1.1.1.1 | View |

| # | Name | Type | Collation | Attributes | Null | Default | Comments | Extra | Action |
|----|----------------|-------------------------------|--------------------|------------|---------------------|---------|----------------|-------|--|
| 1 | id | bigint(20) | | No | None | | AUTO_INCREMENT | | Change Drop More |
| 2 | actor_admin_id | int(11) | | Yes | NULL | | | | Change Drop More |
| 3 | actor_role | enum('manager','super_admin') | utf8mb4_general_ci | Yes | NULL | | | | Change Drop More |
| 4 | action | varchar(64) | utf8mb4_general_ci | No | None | | | | Change Drop More |
| 5 | entity_type | varchar(64) | utf8mb4_general_ci | Yes | NULL | | | | Change Drop More |
| 6 | entity_id | int(11) | | Yes | NULL | | | | Change Drop More |
| 7 | summary | varchar(255) | utf8mb4_general_ci | No | None | | | | Change Drop More |
| 8 | before_json | longtext | utf8mb4_bin | Yes | NULL | | | | Change Drop More |
| 9 | after_json | longtext | utf8mb4_bin | Yes | NULL | | | | Change Drop More |
| 10 | outcome | enum('success','failure') | utf8mb4_general_ci | No | success | | | | Change Drop More |
| 11 | ip_address | varchar(45) | utf8mb4_general_ci | Yes | NULL | | | | Change Drop More |
| 12 | user_agent | varchar(255) | utf8mb4_general_ci | Yes | NULL | | | | Change Drop More |
| 13 | created_at | datetime | | No | current_timestamp() | | | | Change Drop More |

Audit Entry

Time: 2025-11-14 18:24:13
Actor: #1 (super_admin)
Action: item_soft_delete | Entity: items #3
Outcome: success | IP: 1.1.1.1
UA: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Summary: Soft-deleted item #3

Before

```
{
  "id": "3",
  "item_name": "Razer Basilisk V3 Customizable Wired Chroma RGB Gaming Mouse",
  "item_status": "Active"
}
```

After

```
{
  "id": "3",
  "item_name": "Razer Basilisk V3 Customizable Wired Chroma RGB Gaming Mouse",
  "item_status": "Deleted"
}
```



Strengthens accountability, supports incident investigation and ensures all critical actions are fully traceable.



03.

SYSTEM IMPLEMENTATION (7. ERROR HANDLING)





Unified Error Page

```
<VirtualHost *:443>
    ServerName www.localkahtech.com
    ServerAlias localkahtech.com
    DocumentRoot "C:/xampp/htdocs/INT6005CEM_group_assignment_G23/Online Computer Store"

    ServerSignature Off
    ErrorDocument 404 /errors/404.php
    ErrorDocument 500 /errors/500.php

    Alias /Image "C:/xampp/htdocs/INT6005CEM_group_assignment_G23/Image"

    <Directory "C:/xampp/htdocs/INT6005CEM_group_assignment_G23/Image">
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    SSLEngine on
    SSLCertificateFile "conf/ssl.crt/server.crt"
    SSLCertificateKeyFile "conf/ssl.key/server.key"

    Header always set Strict-Transport-Security "max-age=31536000"
</VirtualHost>
```

```
function handleErrorAndExit($message = 'Unexpected error during sign up.') {
    error_log('[SIGNUP ERROR] ' . $message);
    http_response_code(500);
    header("Location: ../errors/500.php");
    exit;
}
```

KAH TECH
WE BUILD FOR THE FUTURE!

404

Page not found

The page you're looking for doesn't exist, has been moved, or the link is incorrect.

[Back to Home](#)

KAH TECH
WE BUILD FOR THE FUTURE!

500

Something went wrong

An unexpected error occurred on our side. Please try again in a moment.

[Back to Home](#)



Provides a single safe fallback screen so unexpected failures show controlled messages without exposing system details.



Suppress Sensitive Details

```
display_errors=Off  
  
; The display of errors which occur during PHP's startup sequence are handled  
; separately from display_errors. We strongly recommend you set this to 'off'  
; for production servers to avoid leaking configuration details.  
; Default Value: On  
; Development Value: On  
; Production Value: Off  
; https://php.net/display-startup-errors  
display_startup_errors=Off  
  
; Besides displaying errors, PHP can also log errors to locations such as a  
; server-specific Log, STDERR, or a location specified by the error_log  
; directive found below. While errors should not be displayed on productions  
; servers they should still be monitored and Logging is a great way to do that.  
; Default Value: Off  
; Development Value: On  
; Production Value: On  
; https://php.net/Log-errors  
log_errors=On
```

```
24999 59 2025] [php:warn] [pid 51472:tid 1936] [client ::1:2988] PHP Warning: Undefined variable $img3_file_name in C:\\xampp\\htdocs\\Online-Computer-Store-main\\Admin Online Compu  
25000 59 2025] [php:warn] [pid 51472:tid 1936] [client ::1:2988] PHP Warning: Undefined variable $img4_file_name in C:\\xampp\\htdocs\\Online-Computer-Store-main\\Admin Online Compu  
25001 59 2025] [php:warn] [pid 51472:tid 1936] [client ::1:2988] PHP Warning: Undefined variable $img5_file_name in C:\\xampp\\htdocs\\Online-Computer-Store-main\\Admin Online Compu  
25002 59 2025] [php:error] [pid 51472:tid 1936] [client ::1:2988] PHP Fatal error: Uncaught mysqli_sql_exception: Unknown column 'abc' in 'field list' in C:\\xampp\\htdocs\\Online-Computer-Store-main\\Admin Online Compu  
25003 22 2025] [php:error] [pid 51472:tid 1944] [client 127.0.0.1:54030] script 'C:/xampp/htdocs/INT6005CEM_group_assignment_G23/Online Computer Store/hello.php' not found or unable  
25004 38 2025] [php:error] [pid 51472:tid 1944] [client 127.0.0.1:54030] script 'C:/xampp/htdocs/INT6005CEM_group_assignment_G23/Online Computer Store/hello.php' not found or unable  
25005 21 2025] [php:notice] [pid 51472:tid 1920] [client 127.0.0.1:31054] [LOGIN ERROR] Table 'computer_store.bryan' doesn't exist, referer: https://localkahtech.com/login.php  
25006
```



Hides internal system information so errors reveal only safe messages, preventing attackers from learning anything useful for exploitation



03.

SYSTEM IMPLEMENTATION

(8. INPUT VALIDATION & CLEANING)





Input Validation

```
// ----- Name validation -----
function validateName() {
  const name = nameInput.value.trim();
  const error = document.getElementById('nameError');

  // Letters, spaces, apostrophes, dots, hyphens; length 2-50
  const nameRegex = /^[A-Za-z\s'.-]{2,50}$/;

  if (name.length === 0) {
    error.style.display = "none";
    isNameValid = false;
  } else if (nameRegex.test(name)) {
    error.style.display = "none";
    isNameValid = true;
  } else {
    error.style.display = "block";
    isNameValid = false;
  }

  updateSubmitButton();
}

// ----- Email validation -----
function validateEmail() {
  const error = document.getElementById('emailError');
  const email = emailInput.value.trim();

  if (email.length === 0) {
    error.style.display = "none";
    isEmailValid = false;
  } else if (emailInput.validity.valid) {
    error.style.display = "none";
    isEmailValid = true;
  } else {
    error.style.display = "block";
    isEmailValid = false;
  }

  updateSubmitButton();
}
```

```
// ----- Malaysian phone validation -----
function validatePhone() {
  const phone = phoneInput.value.trim();
  const error = document.getElementById('phoneError');

  // Simple Malaysian format:
  // - starts with 0
  // - total 10 or 11 digits
  const phoneRegex = /^0\d{8,9}$/;

  if (phone.length === 0) {
    error.style.display = "none";
    isPhoneValid = false;
  } else if (phoneRegex.test(phone)) {
    error.style.display = "none";
    isPhoneValid = true;
  } else {
    error.style.display = "block";
    isPhoneValid = false;
  }

  updateSubmitButton();
}
```



Please enter a valid name (letters only).

Name : Bryan12

Please enter a valid email address.

Email : bryanyeoh68@gmail.com

Please enter a valid Malaysian phone number (starting with 0).

Phone Number : 010550473a

New Password :

Confirm Password :

I confirm that I have read and agree to KAH TECH User Agreement and Privacy & User Education Policy.

User Agreement and Privacy & User Education Policy.

[Sign up](#)

Already have an account? [Log in](#).



Input validation checks whether submitted data follows the required rules so only safe, expected values enter the system, blocking harmful or invalid inputs.



Trim & Whitespace Checks

```
$name = htmlspecialchars(trim($_POST["newUsername"]));  
$email = htmlspecialchars(trim($_POST["newEmail"]));  
$phone = htmlspecialchars(trim($_POST["newPhone"]));  
$address = htmlspecialchars(trim($_POST["newAddress"]));  
$password = password_hash($_POST["newPassword"], PASSWORD_ARGON2ID, $ARGON_OPTS);
```

A screenshot of a web form titled "KAH TECH". The form fields include:

- Name: Bryan
- Email: bryanyeh681@gmail.com
- Phone Number: 0105504731
- Address: haha hahahaha
- New Password: (redacted)
- Confirm Password: (redacted)

Below the form is a checkbox labeled "I confirm that I have read and agree to KAH TECH User Agreement and Privacy & User Education Policy." followed by a "Sign up" button and a "Log in" link.

| | | | | |
|----------|-----------------------|------------|---------------------------|---|
| 19 Junzo | junzobryn28@gmail.com | 0123456789 | bryan 123, at jalan bryan | \$argon2id\$v=19\$m=131072,t=3,p=1\$NkxTbjJWtktORjZEZE... |
| 20 Bryan | bryanyeh681@gmail.com | 0105504731 | haha hahahaha | \$argon2id\$v=19\$m=131072,t=3,p=1\$ZEV1T1ZCuktVQ1Q4aD... |

Trim and whitespace checks remove extra spaces and hidden characters so the system processes clean, accurate input and blocks sneaky manipulation.





Input Limiting

```
<div class="signUpInfo">
  <label for="Username">Name :</label>
  <input required type="text" id="Username" name="newUsername" maxlength="50" placeholder="Enter Username">
  <p class="limit-warning" id="nameLimit">Character limit reached (50)</p>
  <p class="validation-error" id="nameError">Please enter a valid name (letters only).</p>

  <label for="Email">Email :</label>
  <input required type="email" id="Email" name="newEmail" maxlength="100" placeholder="Enter Email">
  <p class="limit-warning" id="emailLimit">Character limit reached (100)</p>
  <p class="validation-error" id="emailError">Please enter a valid email @address.</p>

  <label for="Phone">Phone Number :</label>
  <input required type="text" id="Phone" name="newPhone" maxlength="11" placeholder="Enter Phone Number">
  <p class="limit-warning" id="phoneLimit">Character limit reached (11)</p>
  <p class="validation-error" id="phoneError">Please enter a valid Malaysian phone number (starting with 01).</p>

  <label for="Address">Address :</label>
  <input required type="text" id="Address" name="newAddress" maxlength="200" placeholder="Enter Address">
  <p class="limit-warning" id="addressLimit">Character limit reached (200)</p>

  <label for="newPassword">New Password :</label>
  <div class="pwd-wrapper">
    <input required type="password" id="newPassword" name="newPassword" maxlength="20" placeholder="Enter New Password">
    <i class="fa-solid fa-eye-slash toggle-eye" onclick="togglePassword('newPassword', this)"></i>
  </div>
  <p class="limit-warning" id="newPwdLimit">Character limit reached (20)</p>
  <div class="pwd_validation_container" id="pwd_validation_container">
    <p>Password requirements:</p>
    <p class="pwd_validation" id="pwd_character">* at least 8-20 characters</p>
    <p class="pwd_validation" id="pwd_letter">* at least one character (A-Z)</p>
    <p class="pwd_validation" id="pwd_number">* at least one number (0-9)</p>
    <p class="pwd_validation" id="pwd_symbol">* at least one special characters ($@!%?&)</p>
  </div>
  <p class="pwd_validation" id="pwd_space">* no spaces allowed</p>
  </div>

  <label for="confirmPassword">Confirm Password:</label>
  <div class="pwd-wrapper">
    <input required type="password" id="confirmPassword" name="confirmPassword" maxlength="20" placeholder="Confirm Password">
    <i class="fa-solid fa-eye-slash toggle-eye" onclick="togglePassword('confirmPassword', this)"></i>
  </div>
  <p class="limit-warning" id="confirmPwdLimit">Character limit reached (20)</p>
  <p class="pwd_confirmation" id="pwd_confirmation">Password not match</p>
</div>
```

```
// Field Limit Warning
function setupLimitWarning(inputId, warningId, max) {
  const input = document.getElementById(inputId);
  const warning = document.getElementById(warningId);

  input.addEventListener('input', () => {
    if (input.value.length === max) {
      warning.style.display = "block";
    } else {
      warning.style.display = "none";
    }
  });
}

// Initialize limit warnings for all fields
setupLimitWarning('Username', 'nameLimit', 50);
setupLimitWarning('Email', 'emailLimit', 100);
setupLimitWarning('Phone', 'phoneLimit', 11);
setupLimitWarning('Address', 'addressLimit', 200);
setupLimitWarning('newPassword', 'newPwdLimit', 20);
setupLimitWarning('confirmPassword', 'confirmPwdLimit', 20);

// ----- Attach validation listeners -----
nameInput.addEventListener('input', validateName);
emailInput.addEventListener('input', validateEmail);
phoneInput.addEventListener('input', validatePhone);
```

```
function validatePrice(input) {
  const warning = document.getElementById("priceWarning");
  if (parseFloat(input.value) > parseFloat(input.max)) {
    input.value = input.max;
    warning.style.display = "block";
  } else {
    warning.style.display = "none";
  }
}

function validateStock(input) {
  const warning = document.getElementById("stockWarning");
  if (parseInt(input.value) > parseInt(input.max)) {
    input.value = input.max;
    warning.style.display = "block";
  } else {
    warning.style.display = "none";
  }
}

// Field Limit Warning
function setupLimitWarning(inputId, warningId, max) {
  const input = document.getElementById(inputId);
  const warning = document.getElementById(warningId);

  input.addEventListener('input', () => {
    if (input.value.length === max) {
      warning.style.display = "block";
    } else {
      warning.style.display = "none";
    }
  });
}

// Initialize limit warnings for all fields
setupLimitWarning('name', 'nameLimit', 255);
setupLimitWarning('description', 'descriptionLimit', 999);
```

Input limiting restricts data size and format so only safe, valid inputs are accepted, blocking malicious or oversized submissions.





Input Limiting

User Sign Up Form Limit

Name :

Character limit reached (50)

Email :

Character limit reached (100)

Phone Number :

Character limit reached (11)

Address :

Character limit reached (200)

New Password :

Character limit reached (20)

Confirm Password

Character limit reached (20)

Sign up

Already have an account? [Log in.](#)

Admin Add Item Form Limit

Admin

Account

Item Name : INTEL CORE i7 12700hahosahdjsahdjhahshdashdjhshjoahdjjshaldhashdjhshdhsahdjhshdo|hjdshajdhsoahdjsa

Character limit reached (295)

Description : 12700hahosahdjsahdjhahshdashdjhshjoahdjjshaldhashdjhshdhsahdjhshdo|hjdshajdhsoahdjsa

Character limit reached (999)

Category : --- Select Category ---

Price (RM) : 999999999
Maximum value is 999999999

Stock : 9999
Maximum value is 9999

ADD ITEM





03.

SYSTEM IMPLEMENTATION (9. SQL INJECTION PREVENTION)





SQL Prevention

Input Sanitization

```
/**  
 * Basic sanitization only (no validation here):  
 * - trim  
 * - strip HTML tags  
 * - remove special symbols (keeps letters/numbers/space/-/_/.,)  
 */  
3 references  
function sanitize_basic(?string $s): string {  
    if ($s === null) return '';  
    $s = trim(string: strip_tags(string: $s));  
    // allow: a-z, A-Z, 0-9, space, dash, underscore, dot, comma  
    $s = preg_replace(pattern: '/[^a-zA-Z0-9 \-\_\.\,]/u', replacement: ' ', subject: $s);  
    // collapse multiple spaces  
    $s = preg_replace(pattern: '/\s+/u', replacement: ' ', subject: $s);  
    return $s;  
}  
  
// Sanitize inputs  
$category_raw = $_GET['category'] ?? null;  
$search_raw   = $_GET['search'] ?? null;
```

```
$category = $category_raw !== null ? sanitize_basic(s: $category_raw) : null;  
$search   = $search_raw  !== null ? sanitize_basic(s: $search_raw)  : null;
```

Together, these layered controls ensure all user inputs are safely handled and malicious SQL commands are fully prevented from reaching or manipulating the database



Escaping Special Characters

```
// utf8mb4 for safety  
$conn->set_charset(charset: 'utf8mb4');  
  
$like_esc = $conn->real_escape_string(string: "%{$search}%");  
$sql_legacy = "  
SELECT items.id, items.item_name, items.price, items.stock_qty, items.description,  
    items.image1, items.image2, items.image3, items.image4, items.images,  
    categories.category_name  
FROM items  
LEFT JOIN categories ON items.category_id = categories.id  
WHERE item_status = 'Active'  
AND (  
    LOWER(items.item_name)          LIKE LOWER('{$like_esc}')  
    OR LOWER(items.description)     LIKE LOWER('{$like_esc}')  
    OR LOWER(categories.category_name) LIKE LOWER('{$like_esc}')
```

Parameterized Queries

```
$like = "%{$search}%";  
$sql = "  
SELECT items.id, items.item_name, items.price, items.stock_qty, items.description,  
    items.image1, items.image2, items.image3, items.image4, items.images,  
    categories.category_name  
FROM items  
LEFT JOIN categories ON items.category_id = categories.id  
WHERE item_status = 'Active'  
AND (  
    LOWER(items.item_name)          LIKE LOWER(?)  
    OR LOWER(items.description)     LIKE LOWER(?)  
    OR LOWER(categories.category_name) LIKE LOWER(?)  
);  
$stmt = $conn->prepare(query: $sql);  
if ($stmt) {  
    $stmt->bind_param(types: "sss", var: $like, vars: $like, $like); // escaping not needed for prepared statements  
    $stmt->execute();  
    $itemResult = $stmt->get_result();  
    $stmt->close();
```



SQL Prevention

Error based SQL Injection

Admin

KAH TECH
WE BUILD IT, WE TEST IT

🔍

ALL
MOUSE
KEYBOARD
MONITOR
GRAPHIC CARD
CPU
MEMORY
STORAGE
MOTHERBOARD

Results for ` AND EXTRACTVALUE(1, CONCAT(0x7e,(SELECT DATABASE()),0x7e)) --` — 0 items

No results for ` AND EXTRACTVALUE(1, CONCAT(0x7e,(SELECT DATABASE()),0x7e)) --`

Union based SQL Injection

Admin

KAH TECH
WE BUILD IT, WE TEST IT

🔍

ALL
MOUSE
KEYBOARD
MONITOR
GRAPHIC CARD
CPU
MEMORY
STORAGE
MOTHERBOARD

Results for ` UNION SELECT NULL,NULL,'testing!23',NULL, NULL, NULL --` — 0 items

No results for ` UNION SELECT NULL,NULL,'testing!23',NULL, NULL, NULL --`

Blind SQLi Injection (Boolean)

Admin

KAH TECH
WE BUILD IT, WE TEST IT

🔍

ALL
MOUSE
KEYBOARD
MONITOR
GRAPHIC CARD
CPU
MEMORY
STORAGE
MOTHERBOARD

Results for ` OR '1'='1` --` — 0 items

No results for ` OR '1'='1` --`

Blind SQLi Injection (Time)

Admin

KAH TECH
WE BUILD IT, WE TEST IT

🔍

ALL
MOUSE
KEYBOARD
MONITOR
GRAPHIC CARD
CPU
MEMORY
STORAGE
MOTHERBOARD

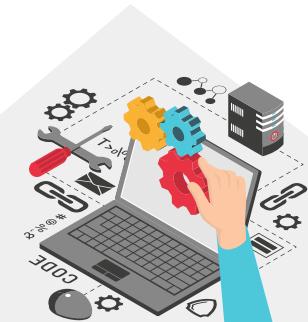
Results for ` OR IF(!=1,SLEEP(2),0) AND '1'='1` --` — 0 items

No results for ` OR IF(!=1,SLEEP(2),0) AND '1'='1` --`



03.

SYSTEM IMPLEMENTATION (10. XSS MITIGATION)





XSS Mitigation

```
/**  
 * Output-encoding helpers (XSS mitigation by context)  
 */  
  
10 references  
function e(string $s): string {           // HTML text/attribute  
    return htmlspecialchars(string: $s ?? '', flags: ENT_QUOTES, encoding: 'UTF-8');  
}  
  
2 references  
function q(string $s): string {           // URL query parameter  
    return urlencode(string: $s);  
}  
  
1 reference  
function qp(string $s): string {          // URL path segment  
    return rawurlencode(string: $s);  
}  
  
$catHref = "store.php?category=" . q(s: $catName);  
$cls = $isSelected ? 'category_button selected' : 'category_button';  
echo '<a class="'. $cls .'" href="'.$catHref.'>' .  
    strtoupper(string: e(s: $catName)) . '</a>';
```

```
<!-- search bar -->  
<form class="search_bar" action="store.php" method="get">  
    <div class="search_box">  
        <input  
            type="text"  
            name="search"  
            placeholder="Search"  
            value="<?php echo isset($_GET['search']) ? e(s: $_GET['search']) : ''; ?>"  
        >  
        <button type="submit"><i class="fa-solid fa-magnifying-glass"></i></button>  
    </div>  
</form>  
  
$id      = (int)$row['id']; // numeric only  
$name   = e(s: $row['item_name']);  
$desc   = e(s: $row['description']);  
$price  = e(s: $row['price']);  
// guard filename, then URL-encode for path usage  
$img1f  = basename(path: $row['image1'] ?? '');  
$imgSrc = "../Image/" . qp(s: $img1f);  
$stock  = (int)$row['stock_qty'];  
$detailsHref = "itemDetails.php?item={$id}";
```



Ensure that any malicious input is safely neutralised and displayed as harmless text, preventing scripts from ever running in the browser



XSS Mitigation

Script Tag

The screenshot shows a browser developer tools Network tab with a search bar containing '<script>alert(1)</script>'. The results table shows one item: 'store.php?search=%22%3C%21%22...'. The response payload column displays the script tag: '<script>alert(1)</script>'.

Attribute Injection

The screenshot shows a browser developer tools Network tab with a search bar containing 'autofocus onfocus='alert()''. The results table shows one item: 'store.php?search=%22%20autofocus%20onfocu...'. The response payload column displays the attribute: 'autofocus onfocus='alert()''.

Image Error Handler

The screenshot shows a browser developer tools Network tab with a search bar containing 'img src=x onerror=alert()>'. The results table shows one item: 'store.php?search=%22%3E%21%22...'. The response payload column displays the image error handler: 'img src=x onerror=alert()>'.

JavaScript URL

The screenshot shows a browser developer tools Network tab with a search bar containing 'img src=x onerror=alert()>'. The results table shows one item: 'store.php?search=%22%3E%21%22...'. The response payload column displays the JavaScript URL: 'img src=x onerror=alert()>'.



03.

SYSTEM IMPLEMENTATION **(11. DIGITAL CERTIFICATE DEPLOYMENT)**





Digital Certificate Deployment

The image displays three screenshots of browser developer tools, specifically focusing on the Network tab and Certificate Viewer.

- Left Screenshot:** Shows the "Privacy and security" section of the developer tools. It indicates that the page is secure (valid HTTPS). It shows the certificate is valid and trusted, issued by Internet Widgets Pty Ltd for localkahtech.com. It also shows connection settings and resources are served securely.
- Middle Screenshot:** A "Certificate Viewer" window for localkahtech.com. It shows the "General" tab with details:
 - Issued To:** Common Name (CN) - localkahtech.com, Organization (O) - Internet Widgets Pty Ltd, Organizational Unit (OU) - <Not Part Of Certificate>
 - Issued By:** Common Name (CN) - localkahtech.com, Organization (O) - Internet Widgets Pty Ltd, Organizational Unit (OU) - <Not Part Of Certificate>
 - Validity Period:** Issued On: Sunday, November 9, 2025 at 1:06:51 PM, Expires On: Monday, November 9, 2026 at 1:06:51 PM
 - SHA-256 Fingerprints:** Certificate: 0ace45cc86a3bed3ddaeef67fa8bde586032d186aa513c5402b23529034a520a, Public Key: 5895e47730aa68ced760dc196bb0ef1bd611dc3483e42623e39e17d120bbc035
- Right Screenshot:** The Network tab of the developer tools showing a timeline of requests. One request for "index.php" is selected, showing detailed headers and response data. The response body includes the PHP code for the index page.

- Provides authenticated and encrypted communication, significantly improving overall data confidentiality and integrity.





03.

SYSTEM IMPLEMENTATION **(12. CRYPTOGRAPHY IMPLEMENTATION)**





Data-in-Transit (HTTPS/ TLS1.3)

Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by localkahtech.com.

[View certificate](#)

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES_256_GCM.

Resources - all served securely

All resources on this page are served securely.

```
C:\Users\User>ping localkahtech.com
```

```
Pinging localkahtech.com [127.0.0.1] with 32 bytes of data:  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 127.0.0.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Capturing from Adapter for loopback traffic capture
```

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
```

```
ipaddr == 127.0.0.1 & & top.port == 443
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------|-------------|----------|--------|--|
| 5 | 1.067254 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 52384 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=256 SACK_PERM |
| 6 | 1.067354 | 127.0.0.1 | 127.0.0.1 | TCP | 60 | 52384 + 52384 [SYN, ACK] Seq=0 Win=65535 Len=0 MSS=256 SACK_PERM |
| 7 | 1.067393 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 52384 + 443 [ACK] Seq=1 Win=65288 Len=0 |
| 8 | 1.068401 | 127.0.0.1 | 127.0.0.1 | TLSv1.3 | 1770 | Client Hello [SNI=localkahtech.com] |
| 9 | 1.068452 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 443 + 52384 [ACK] Seq=1 Ack=1727 Win=63744 Len=0 |
| 10 | 1.129993 | 127.0.0.1 | 127.0.0.1 | TLSv1.3 | 1866 | Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data |
| 11 | 1.139866 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 52384 + 443 [ACK] Seq=1823 Ack=1823 Win=63488 Len=0 |
| 12 | 1.134731 | 127.0.0.1 | 127.0.0.1 | TLSv1.3 | 124 | Change Cipher Spec, Application Data |
| 13 | 1.134807 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 443 + 52384 [ACK] Seq=1823 Ack=1807 Win=63488 Len=0 |
| 14 | 1.136404 | 127.0.0.1 | 127.0.0.1 | TLSv1.3 | 363 | Application Data |
| 15 | 1.136431 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 52384 + 443 [ACK] Seq=1807 Ack=2142 Win=63232 Len=0 |
| 16 | 1.136966 | 127.0.0.1 | 127.0.0.1 | TLSv1.3 | 363 | Application Data |
| 17 | 1.137003 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 52384 + 443 [ACK] Seq=1807 Ack=2461 Win=62976 Len=0 |
| 18 | 1.240497 | 127.0.0.1 | 127.0.0.1 | TLSv1.3 | 866 | Application Data |
| 19 | 1.240586 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 443 + 52384 [ACK] Seq=2461 Ack=2629 Win=62720 Len=0 |
| 20 | 1.241173 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 58842 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM |
| 21 | 1.241274 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 443 + 58842 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM |
| 22 | 1.241310 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 58842 + 443 [ACK] Seq=1 Ack=1 Win=65288 Len=0 |
| 23 | 1.242281 | 127.0.0.1 | 127.0.0.1 | TLSv1.3 | 2169 | Client Hello [SNI=localkahtech.com] |
| 24 | 1.242315 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 443 + 58842 [ACK] Seq=1 Ack=2126 Win=63232 Len=0 |

```
> Frame 8: Packet, 1770 bytes on wire (14160 bits), 1770 bytes captured (14160 bits) on interface [Dev1 Null/Loopback]
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 52384, Dst Port: 443, Seq: 1, Ack: 1, Len: 1726
> Transport Layer Security
  > Stream index: 0
    > TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      > Version: TLS 1.3 (0x0303)
      > Length: 1726
        > Handshake Protocol: Client Hello
          Handshake Type: Client Hello (1)
          Length: 1717
        > Version: TLS 1.2 (0x0303)
        Random: 40e85293d5259df5f092594c46ed2026737aa49464cb16c959f6ea511b78e3
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-------------------------|-------------------------|-------------------------|-------------|---|---|
| 0020 | 09:01:00:05:03:03:40 | b8 77 1a d7 50 18 00 ff | ab 3f 00 00 | 16:03:01:06 | 0020 | b8 77 1a d7 50 18 00 ff ab 3f 00 00 16:03:01:06 |
| 0030 | 09:01:00:06:05:03:03:40 | e8 52 93 d5 25 9d f5 7f | 00 20 7a 13 01 13 01 | 0030 | e8 52 93 d5 25 9d f5 7f 00 20 7a 13 01 13 01 | |
| 0050 | 09:01:00:06:05:03:03:40 | d5 9e c1 51 1b 78 c3 20 | 65 0f 81 37 f3 f4 ac c4 | 0050 | d5 9e c1 51 1b 78 c3 20 65 0f 81 37 f3 f4 ac c4 | |
| 0060 | 09:01:00:06:05:03:03:40 | c3 d8 08 11 09 6f cf | d9 d1 2b c2 69 24 ea 7b | 0060 | c3 d8 08 11 09 6f cf d9 d1 2b c2 69 24 ea 7b | |
| 0070 | 09:01:00:06:05:03:03:40 | 7e 00 20 7a 13 01 13 01 | 00 20 7a 13 01 13 01 | 0070 | 7e 00 20 7a 13 01 13 01 | |
| 0080 | 09:01:00:06:05:03:03:40 | 00 20 7a 13 01 13 01 | 00 35 01 00 00 00 00 | 0080 | 00 20 7a 13 01 13 01 00 35 01 00 00 00 | |
| 0090 | 09:01:00:06:05:03:03:40 | 00 44 0d 00 00 00 00 | 02 68 32 20 2b 00 07 07 | 0090 | 00 44 0d 00 00 00 00 02 68 32 20 2b 00 07 07 | |
| 0098 | 09:01:03:04:03:03:00:00 | 00 12 00 10 04 03 08 04 | 00 12 00 10 04 03 08 04 | 0098 | 00 12 00 10 04 03 08 04 | |
| 0100 | 09:01:03:04:03:03:00:00 | 00 12 00 10 04 03 08 04 | 00 12 00 10 04 03 08 04 | 0100 | 00 12 00 10 04 03 08 04 | |
| 0108 | 09:01:03:04:03:03:00:00 | 00 04 cd aa 09 01 00 00 | 00 04 c9 96 00 00 00 00 | 0108 | 00 04 cd aa 09 01 00 00 00 04 c9 96 00 00 00 | |
| 0120 | 09:01:03:04:03:03:00:00 | 00 04 c9 96 00 00 00 00 | 00 04 c9 96 00 00 00 00 | 0120 | 00 04 c9 96 00 00 00 00 00 04 c9 96 00 00 00 | |
| 0130 | 09:01:03:04:03:03:00:00 | 57 f5 41 2b e9 f9 fb | b1 10 50 84 07 79 7d 20 | 0130 | 57 f5 41 2b e9 f9 fb b1 10 50 84 07 79 7d 20 | |

TLS 1.3 setup ensures all traffic fully encrypted and protected in transit, keeping sensitive data secure without needing extra application-level encryption.





Data-at-Rest (AES-256-GCM)

Before & After:

| # | Name | Type | Collation | Attributes | Null | Default |
|----|-----------------|--------------|--------------------|------------|--------------------|---------|
| 1 | id | int(11) | | | No | None |
| 2 | user_name | varchar(255) | utf8mb4_general_ci | | No | None |
| 3 | email | varchar(255) | utf8mb4_general_ci | | No | None |
| 4 | secondary_email | varchar(255) | utf8mb4_general_ci | Yes | NULL | |
| 5 | phone | varchar(15) | utf8mb4_general_ci | | No | None |
| 6 | user_address | varchar(255) | utf8mb4_general_ci | | No | None |
| 7 | pwd | varchar(255) | utf8mb4_general_ci | | No | None |
| 8 | user_image | varchar(255) | utf8mb4_general_ci | Yes | no_profile_pic.png | |
| 9 | wrong_pwd_count | int(11) | | | Yes | 0 |
| 10 | lock_until | datetime | | | Yes | NULL |

Key:

```
<?php
echo bin2hex(string: random_bytes(length: 32));
?>
```

localhost/INT6005CEM_security_group_assignment_G23/Online-0
60d4d9476c34544beecd52ff72cdfaec819202e5d715b97648f723c69cdeb32ec

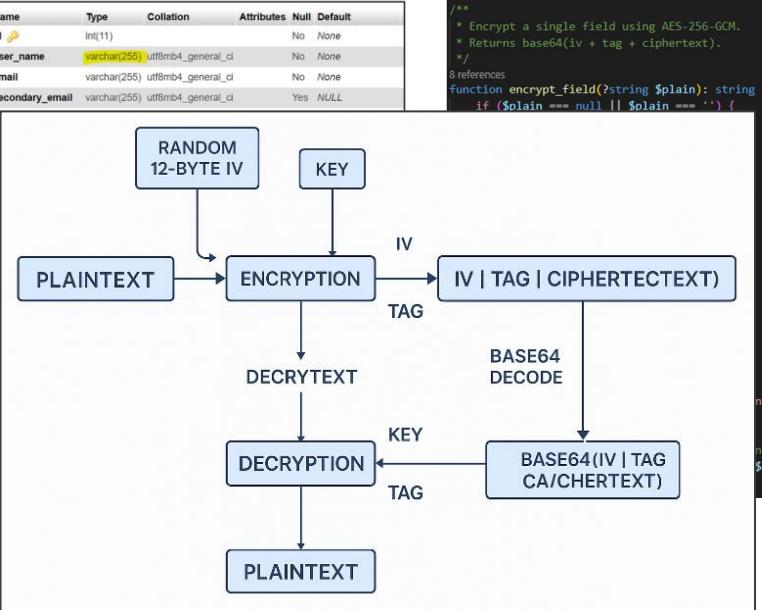
```
// 32-byte encryption key
// Generate in keygen.php
const ENC_KEY_HEX = '60d4d9476c34544beecd52ff72cdfaec819202e5d715b97648f723c69cdeb32ec';

// Convert hex to binary key
const ENC_METHOD = 'aes-256-gcm';
```

2 references

```
function get_enc_key(): string {
    return hex2bin(string: ENC_KEY_HEX);
}
```

Encryption:



```
/*
 * Encrypt a single field using AES-256-GCM.
 * Returns base64(iv + tag + ciphertext).
 */
8 references
27 references
function encrypt_field(?string $plain): string {
    if ($plain === null || $plain === '') {
        return '';
    }

    $blob = base64_decode(string: $encoded, strict: true);
    if ($blob === false || strlen(string: $blob) < 12 + 16) {
        return '';
    }

    $iv = substr(string: $blob, offset: 0, length: 12);
    $tag = substr(string: $blob, offset: 12, length: 16);
    $cipher = substr(string: $blob, offset: 28);

    if ($cipher === false) {
        return 'Encryption failed';
    }

    $plain = openssl_decrypt(
        data: $cipher,
        cipher algo: ENC_METHOD,
        passphrase: get_enc_key(),
        options: OPENSSL_RAW_DATA,
        iv: $iv,
        tag: $tag
    );
}

return $plain === false ? '' : $plain;
}
```



Data-at-Rest (AES-256-GCM)

Code-Based Verification Against Database Value

Test: AES-256-GCM decryption

User #28 – Ensin

Compares the encrypted values in the database with the decrypted output and the expected real values (username, email, phone, address).

| Field | Database value (encrypted) | After decrypt_field() | Expected real value | Result |
|-----------------|---|-----------------------|---------------------|------------|
| username | Nwksly+F+HZG1TUS14a1A+p0suRf9RDcCwztNUJ6n1CnAs | Ensin | Ensin | MATCH |
| email | K5EWocjzEmCdybz6R21IVD0QZ4N51WLHRjXz6NTH8UH2bfU6rExN29FBtbH2Dw= | ensin2004@gmail.com | ensin2004@gmail.com | MATCH |
| secondary_email | | - | | Not tested |
| phone | Goh5s1e/YLvvLqI17sBbKqjVGwdLcnusabG9stPDMd8QaDzR1E= | 0193818893 | 0193818893 | MATCH |
| user_address | Ksy1nTg6peXQphszZ+z890sD0PnY8rY8wEvhOwAbNRSF6fRM1vp1vM9w== | ensin is kawaii | ensin is kawaii | MATCH |

● MATCH – decrypted value is exactly the same as the expected real value.
● NOT MATCH – decrypted value is different from the expected value.
● Not tested – no expected value provided (e.g. secondary email not set).

UI-Level Check

Name : **Ensin**

Email : **ensin2004@gmail.com**

Phone Number : **0193818893**

Address : **ensin is kawaii**

New Password : *********

Confirm Password : *********

I confirm that I have read and agree to KAH TECH
 [User Agreement](#) and [Privacy & User Education Policy](#).

Sign up

Already have an account? [Log In](#).

EDIT **LOG OUT**

AES-256-GCM setup ensures sensitive database fields remain unreadable if leaked while still decrypting safely and accurately when the system needs them.





03.

SYSTEM IMPLEMENTATION **(13. BROWSER COOKIE)**





Browser Cookie Security

```
session_set_cookie_params([
    'lifetime' => 0,           // expires when browser closes
    'path' => '/',
    'secure' => true,          // only over HTTPS
    'httponly' => true,        // JS cannot access it
    'samesite' => 'Strict' // strong CSRF protection
]);
```

Browser cookies are configured with strict security settings to protect from theft, sniffing and CSRF attacks

The screenshot shows a browser window with developer tools open, specifically the Application tab. The page content displays a dark-themed website with sections for 'About Us' and 'Customize Your Own'. In the developer tools, the Application tab lists various storage components like Manifest, Service workers, Storage, and Cookies. The Cookies section shows a table with one row for the PHPSESSID cookie. The table columns include Name, Value, Domain, Path, Expires, Size, HttpOnly, Secure, SameSite, Partition, Cross-Site, and Priority. The 'Value' column for the cookie contains the value '2glikoja311324h5oi8qehai54e'. A red box highlights this row.

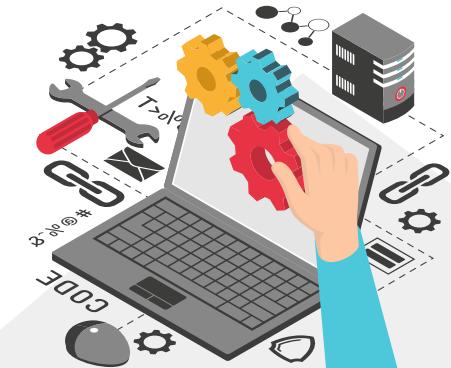
| Name | Value | Dom... | Path | Expires | Size | Http... | Secure | Same... | Partit... | Cross... | Priority |
|-----------|-----------------------------|----------|------|----------|------|---------|--------|---------|-----------|----------|----------|
| PHPSESSID | 2glikoja311324h5oi8qehai54e | local... | / | Sessi... | 35 | ✓ | ✓ | Strict | | | Med... |





04.

DISCUSSION





OWASP TOP 10 COVERAGE

| ACHIEVED | PARTIALLY ACHIEVED | NOT APPLICABLE |
|---|--|---|
| <p>A01 – Broken Access Control</p> <p>A02 – Cryptographic Failures</p> <p>A03 – Injection (SQLi)</p> <p>A05 – Security Misconfiguration</p> <p>A07 – Identification & Authentication Failures</p> <p>A09 – Security Logging & Monitoring Failures</p> | <p>A04 – Insecure Design</p> <p>A06 – Vulnerable & Outdated Components</p> <p>A08 – Software & Data Integrity Failures</p> | <p>A10 – Server-Side Request Forgery (SSRF)</p> |



REMAINING VULNERABILITIES AFTER CONTROL

A01

Broken Access Control

- New pages/APIs may skip role checks
- Risk of exposing sensitive IDs in URLs
- **Fix:** Follow consistent access control rules

A03

Injection

- Legacy code may use unsafe SQL
- **Fix:** Enforce prepared statements in code reviews



A02

Cryptographic Failures

- AES/TLS depends on proper key storage
- Require encryption and strict access to backups
- **Fix:** Improve key handling & backup encryption

A04

Insecure Design

- Controls exist but no formal threat modelling
- **Fix:** Use simple design/threat checklist



REMAINING VULNERABILITIES AFTER CONTROL

A05

Security Misconfiguration

- Configurations may drift during deployment
- New servers may miss error pages or HSTS
- **Fix:** Use deployment checklists to prevent drift

A07

Identification & Authentication Failures

- Strong passwords + rate limiting exist
- Still vulnerable to credential stuffing and no MFA for admins
- **Fix:** Enforce MFA for admins; offer MFA for users



A06

Vulnerable & Outdated Components

- Libraries may become outdated silently
- No automated dependency monitoring
- **Fix:** Add automated scanning and patch cycles

A08

Software & Data Integrity Failures

- No code-signing or pipeline integrity checks
- **Fix:** Harden DevOps pipeline and use signed releases



REMAINING VULNERABILITIES AFTER CONTROL

A09

Security Logging & Monitoring Failures

- Logs not analysed centrally
- Suspicious activity may be detected late
- **Fix:** Centralize logs / SIEM

A10

SSRF

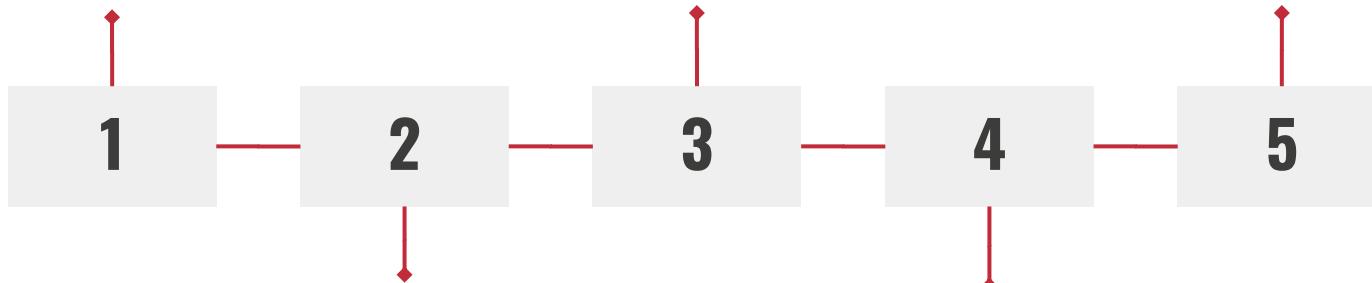
- Not currently applicable
- Future features (webhooks, URL fetchers) could introduce SSRF
- **Fix:** Apply SSRF-safe design for URL-fetching features



FUTURE ENHANCEMENT

Full MFA for Admins

- Enable MFA for all admin login
- Use TOTP + controlled recovery
- Reduces password compromise



Automated Dependency Scanning

- Track all libraries/component
- Use Composer/NPM/Git scans
- Catch CVEs before deployment

Secure SDLC & Checklists

- Use security checklists in reviews
- Quick threat-modelling for major changes
- Prevents new vulnerabilities



CSP & Browser Hardening

- Add CSP to block untrusted scripts
- Set security headers (nosniff, DENY, referrer policy)
- Mitigates XSS + clickjacking

Centralized Logging & Alerts

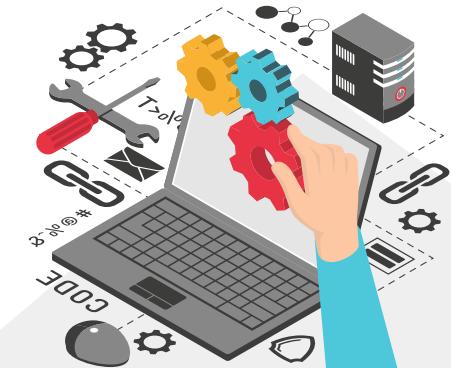
- Send app + server logs to SIEM/ELK
- Dashboards + alerts for anomalies
- Faster threat detection





05.

SUMMARY



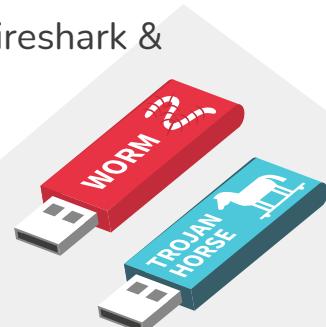
SUMMARY

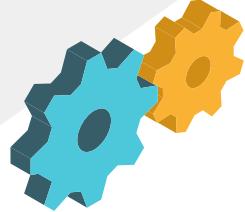
CONCLUSION

- System now addresses most OWASP Top 10 risks
- Major OWASP risks addressed (SQLi, XSS, weak sessions, no TLS, plaintext passwords)
- Implemented Argon2id, TLS 1.3, CSRF, secure cookies, logging & safer queries
- Overall system now far more secure and closer to production-ready

LEARNING OUTCOME ACHIEVED

- Hands-on experience with SQLi, XSS, session abuse & crypto issues
- Implemented real defenses: Argon2id, AES-GCM, TLS, CSRF, secure sessions
- Improved risk prioritization (Likelihood × Severity)
- Gained skills with Burp, Wireshark & dev tools





THANK YOU

