

# SISTEM PENGURUSAN REKOD PEKERJA BERASASKAN TEKNIK ENCRYPTION MENGGUNAKAN KAEDAH HASHING

AIDA RUZANA BINTI AHMAD YANI

DR. UMI ASMA' MOKHTAR

*Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia*

## ABSTRAK

Sistem Pengurusan Rekod Pekerja dibina untuk memudahkan pengurusan rekod pekerja dengan menyelenggara rekod dan menyimpan rekod secara efisien dan sistematik. Sistem pengurusan rekod memegang pangkalan data yang besar. Oleh itu sesebuah sistem itu cenderung terdedah kepada *human-error*. Rekod data mungkin tersilap diubah dan dibuang oleh pihak ketiga yang boleh menyebabkan rekod menjadi tidak sah, dimanipulasi dan rosak. Kajian ini bertujuan mengenal pasti teknik enkripsi dengan kaedah *hashing* dan membangun sistem rekod pekerja berasaskan teknik enkripsi dengan menggunakan kaedah *hashing* supaya keselamatan rekod terjamin. Kaedah yang digunakan dalam proses sistem ini adalah kaedah Pembangunan Aplikasi Pesat (Rapid Application Development, RAD). Pendekatan RAD meminimumkan peringkat perancangan dan memaksimumkan pembangunan prototaip, pengurusan projek dapat menghasilkan kecekapan yang lebih tinggi, pembangunan yang pantas dan komunikasi yang berkesan. Antara teknik yang digunakan adalah enkripsi dengan kaedah *hashing*. Hasilnya keselamatan laman web itu terjamin.

## 1 PENGENALAN

Rekod adalah satu bahan berbentuk bertulis ataupun bentuk lain yang menyimpan fakta atau peristiwa atau merakamkan maklumat termasuklah dokumen, kertas, bahan bercetak, buku, peta, plan, lukisan gambar foto, rakaman bunyi, rekod yang dihasilkan secara elektronik tanpa mengira bentuk mahupun ciri-ciri fizikal dan apa-apa salinannya. Pengurusan adalah penggunaan sumber yang paling minimum untuk

mendapatkan hasil yang optimum.

Pengurusan rekod pula adalah bidang pengurusan yang bertanggungjawab bagi mengadakan kawalan secara efisien dan sistematik ke atas pewujudan, penyelenggaraan dan pelupusan rekod. Kawalan ini termasuk proses penawanan bukti dan maklumat mengenai bukti dan maklumat mengenai aktiviti transaksi urusan organisasi dalam bentuk rekod. Secara amnya pangkalan data sering digunakan sebagai satu tempat menyimpan semua rekod yang boleh memberi risiko kepada keselamatan di organisasi tersebut seperti kecurian, penyalahgunaan dan pengubahan rekod tanpa izin. Oleh itu, sistem ini menggunakan teknik enkripsi dengan menggunakan kaedah *hashing* bagi memastikan sistem adalah selamat untuk digunakan.

Pengurusan maklumat dan rekod yang cekap dan teratur membolehkan sesebuah organisasi itu meningkatkan keupayaan dan keberkesanan penyampaian perkhidmatan yang berkualiti. Dengan menggunakan kombinasi enkripsi dan *hash*, keselamatan web dapat ditingkatkan. Setiap pengguna yang berdaftar memiliki User ID yang bertindak sebagai tandatangan digital dan hanya pengguna yang berdaftar boleh masuki sistem mengikut tahap penggunaan masing-masing.

Sebaliknya, sistem konvensional terdedah kepada kesilapan dan kecuaiannya manusia dan memakan masa untuk melakukannya. Dengan merapikan aliran dengan teknologi Sistem Pengurusan Rekod Pekerja ini sesuatu urusan itu dapat diselesaikan dengan lebih cepat dan cekap. Oleh itu, kajian ini akan membangun satu sistem rekod pekerja berasaskan teknologi ini supaya meningkatkan aspek keselamatan pangkalan data tersebut. Sistem ini juga akan lebih kemas dan lebih ringan akan mengelakkan kerosakan data dari terjadi atau mana-mana penggodam dari mencerooboh.

## 2 PENYATAAN MASALAH

Sistem pangkalan data merupakan satu medium yang penting bagi menyimpan semua rekod penting. Namun, tidak semua sistem mempunyai jaminan keselamatan. Setiap data yang terdapat dalam sistem cenderung terdedah kepada *human-error*. Rekod mungkin tersilap diubah dan dibuang oleh pihak ketiga justeru itu berlakunya kerosakan data. Apabila terdapat terlalu banyak kesalahan dalam sistem, kadar

integriti sistem tersebut akan menurun.

Penyelenggaraan data cenderung kepada pededahan data sulit dari sumber luaran. Ia merangkumi serangan ke atas data pengguna yang tidak dibenarkan. Kebocoran data pula dikelilingi oleh pendedahan kelemahan maklumat. Sesebuah maklumat data mungkin terdedah kerana pengguna yang diberi akses yang tidak wajar ke laman web.

Pencerobohan maklumat mungkin berlaku sekiranya keselamatan sistem tidak kukuh. Sistem keselamatan yang lemah mengakibatkan data-data yang terdapat dalam sistem terdedah kepada orang awam. Contohnya sistem pengurusan rekod pekerja yang menyimpan segala maklumat seseorang pekerja itu mungkin dicuri dan di ambil oleh seseorang penceroboh sistem. Sistem itu juga mungkin diubah oleh penggadam.

### 3 OBJEKTIF KAJIAN

Kajian ini bertujuan:

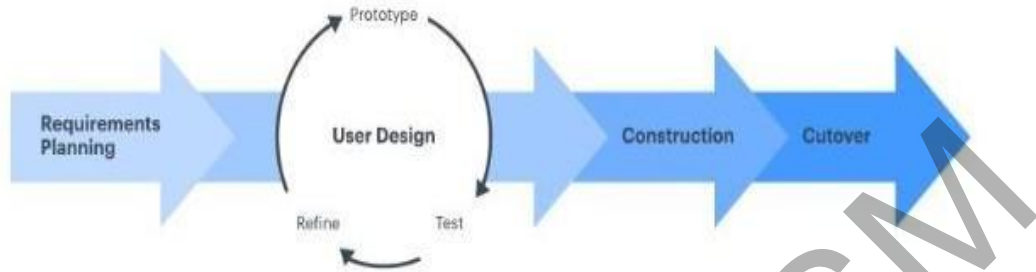
- I. Menenal pasti teknik *hashing* dan *encryption* dalam sistem rekod pekerja.
- II. Membangun sistem rekod pekerja berasaskan teknik *encryption* menggunakan kaedah *hashing*.

Sistem berasaskan *encryption* menggunakan kaedah *hashing* dibangun bagi memastikan tahap keselamatan dipertingkat kerana tidak melibatkan pihak ketiga untuk mengubah ataupun membuang rekod data.

### 4 METHOD KAJIAN

Kaedah yang digunakan dalam kajian ini adalah kaedah Pembangunan Aplikasi Pesat (Rapid Application Development, RAD). RAD adalah strategi pengurusan projek yang tangkas dalam pembangunan perisian. Pendekatan RAD adalah pemulihan projek yang cepat menjadikannya pilihan yang menarik. RAD meminimumkan peringkat perancangan dan memaksimumkan pembangunan prototaip. Dengan mengurangkan masa perancangan dan mamaksimumkan prototaip, pengurusan projek dapat

menghasilkan kecekapan yang lebih tinggi, pembangunan yang pantas dan komunikasi yang berkesan.



Rajah 1 Rapid Application Development (RAD)

#### 4.1 Fasa Perancangan

Fasa ini bersamaan dengan mensyuarat sampingan projek. Fasa perancangan dipendekkan berbanding metodologi pengurusan projek. Semasa peringkat ini, pengguna sistem dan pembangun sistem berkomunikasi untuk menentukan matlamat dan jangkaan untuk projek serta isu yang perlu ditangani semasa pembinaan. Semasa fasa ini, sesi penyelidikan masalah semasa, menetapkan keperluan projek dan memuktamadkan keperluan dengan setiap kelulusan pihak berkepentingan.

#### 4.2 Fasa Reka Bentuk Pengguna

Semasa fasa ini, pengguna dan pembangun bekerjasama untuk memastikan keperluan dipenuhi pada setiap proses reka bentuk. Pembangun sistem menyesuaikan di mana pengguna menguji setiap prototaip pada setiap peringkat untuk memastikan ia memenuhi jangkaan mereka. Kaedah ini memberi peluang kepada pembangun untuk membetulkan sistem sehingga mencapai reka bentuk yang memuaskan.

#### 4.3 Fasa Pembinaan

Fasa ini mengambil prototaip dan sistem beta dari fasa reka bentuk dan menukarkannya ke model kerja. Fasa ini melibatkan persediaan untuk pembinaan pesat, memprogram dan pembangunan aplikasi dan pengkodan unit, integrasi dan ujian sistem. Fasa ketiga ini penting kerana pengguna masih memberi input sepanjang proses, mereka boleh mencadangkan perubahan atau idea baru sekiranya masalah

timbul.

Copyright@FTSM

#### 4.4 Fasa Pelaksanaan

Fasa ini dimana produk selesai dilancarkan. Ia termasuk penukaran data, ujian dan perubahan kepada sistem baru serta latihan pengguna. Semua perubahan terakhir dibuat semasa pengkod dan pengguna terus mencari bug dalam sistem.

Perkakasan yang digunakan haruslah dapat menyokong semua proses pembangunan sistem rekod pelajar ini. Perkakasan yang akan digunakan adalah seperti berikut:

- 1) Komputer riba 15'' (intel core i5)
- 2) 8GB Random Access Memory (RAM)

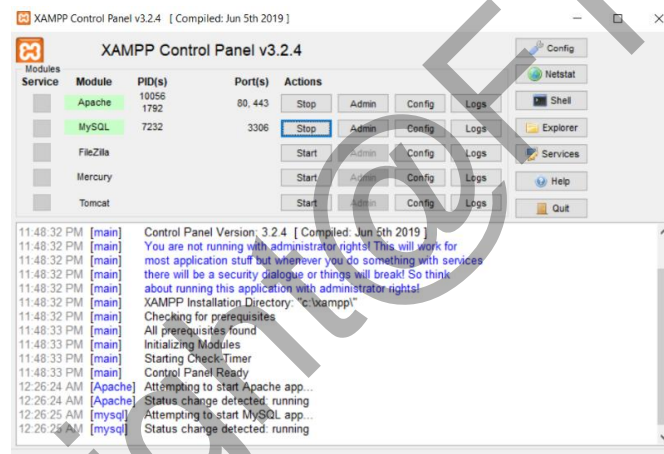
Untuk pembangunan sistem ini, perisian yang akan digunakan adalah:

|                 |   |
|-----------------|---|
| Sublime text    | Sesebuah teks editor untuk menulis sumber kod.  |
| My SQL Database | Sebuah sistem pengurusan pangkalan data sumber terbuka.   |
| Xampp           | XAMPP adalah pakej stack penyelesaian pelayan web serampang dan sumber terbuka yang dibangunkan oleh Apache Friends, yang terdiri terutamanya daripada Apache HTTP Server, pangkalan data MariaDB, dan penterjemah untuk skrip yang ditulis dalam PHP dan bahasa pengaturcaraan Perl. |

## 5 HASIL KAJIAN

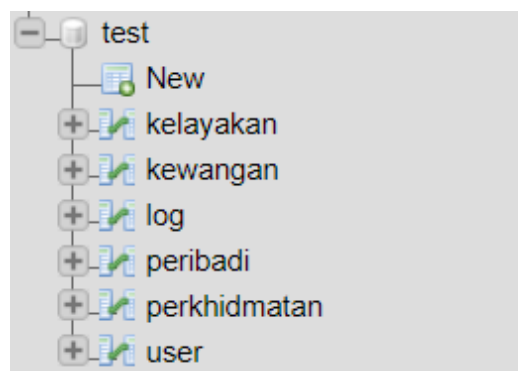
Bahagian ini membincangkan tentang hasil implementasi Sistem Pengurusan Rekod Pekerja. Antara beberapa perkara yang diambil kira semasa proses implementasi adalah, konsep reka bentuk sistem iaitu apakah yang harus dilakukan oleh sistem. Selain itu reka bentuk logik, bagaimana sistem ini harus dilihat oleh pengguna dan akhir sekali adalah reka bentuk fizikal sistem, bagaimana sistem harus dibina.

Sublime Text telah digunakan bagi implementasi algoritma. Sublime Text adalah penyunting kod sumber *shareware* lintas *platform* dengan antara muka pengaturcaraan aplikasi Phyton. Sistem ini dibangunkan dengan menggunakan beberapa bahasa pengaturcaraan seperti HTML, PHP, MySql, CSS, JavaScript dan Bootstrap. PHPMyAdmin digunakan bagi menguruskan pangkalan data secara *web based* dengan menggunakan *localhost*. Sistem Pengurusan Rekod Pekerja ini serta perisian XAMPP berfungsi sebagai pelayan web lintas *platform*. Rajah 5.1 menunjukkan XAMPP *Control Panel* untuk menentukan sama ada Apache dan MySQL sedang berjalan dan untuk memulakan atau menghentikannya.



Rajah 5.1: Perisian XAMPP

Rajah 5.2 menunjukkan pangkalan data bagi Sistem Pengurusan Rekod Pekerja. PHPMyAdmin membolehkan pengguna mengubah, menghapus dan mencipta jadual pangkalan data MySQL.



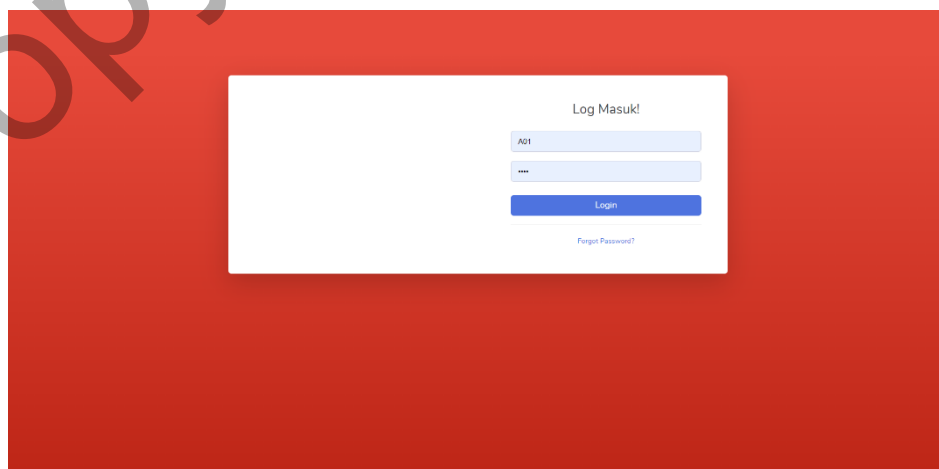
Rajah 5.2: Pangkalan data PHPMyAdmin

Rajah 5.3 menunjukkan pengaturcaraan untuk menyambungkan sistem ke pangkalan data bagi memudahkan kerja pengambilan data.

```
dbh.inc.php
1 <?php
2 $dbServername = "lrgs.ftsm.ukm.my";
3 $dbUsername = "a166067";
4 $dbPassword = "*****";
5 $dbName = "a166067";
6
7 // Create connection
8 $conn = mysqli_connect($dbServername, $dbUsername, $dbPassword, $dbName);
9
10 // Check connection
11 if (!$conn) {
12     die("Connection failed: " . mysqli_connect_error());
13 }
14
```

Rajah 5.3: Pengaturcaraan bagi menyambung ke pangkalan data.

Implementasi antara muka Sistem Pengurusan Rekod Pekerja ini mementingkan beberapa elemen. Sistem ini dibina secara jelas bagi elemen *button*, *alert*, *label* dan pesanan bagi memudahkan pengguna memahami sistem. Warna dan tekstur antara muka juga diambil kira supaya dapat pengguna dapat memberi perhatian mereka kepada perkara penting dalam sistem. Konsistensi bagi setiap antara muka juga amat penting supaya pengguna merasa lebih selesa dengan susun atur dan reka bentuk di seluruh web pengguna dapat menyelesaikan sesuatu dengan mudah dan cekap. Rajah 5.4 menunjukkan antara muka log masuk pengguna. Halaman ini membolehkan pengguna log masuk ke dalam sistem.

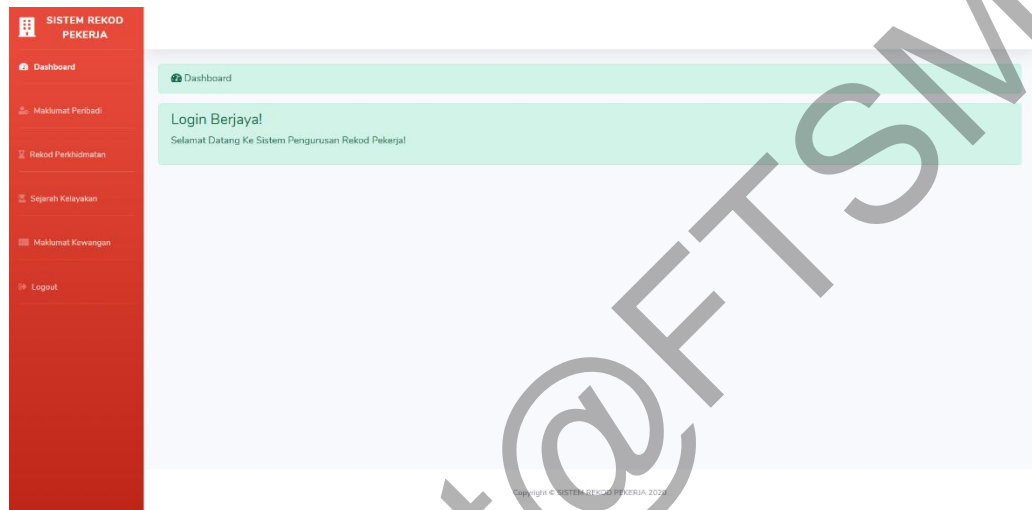


The image shows a user login interface. It features a white rectangular form centered on a solid red background. The form is titled "Log Masuk!". Below the title, there are two input fields: the first is for the username, containing the text "A01"; the second is for the password, with the characters masked by dots. Below these fields is a blue button labeled "Login". At the bottom of the form, there is a link that says "Forgot Password?".

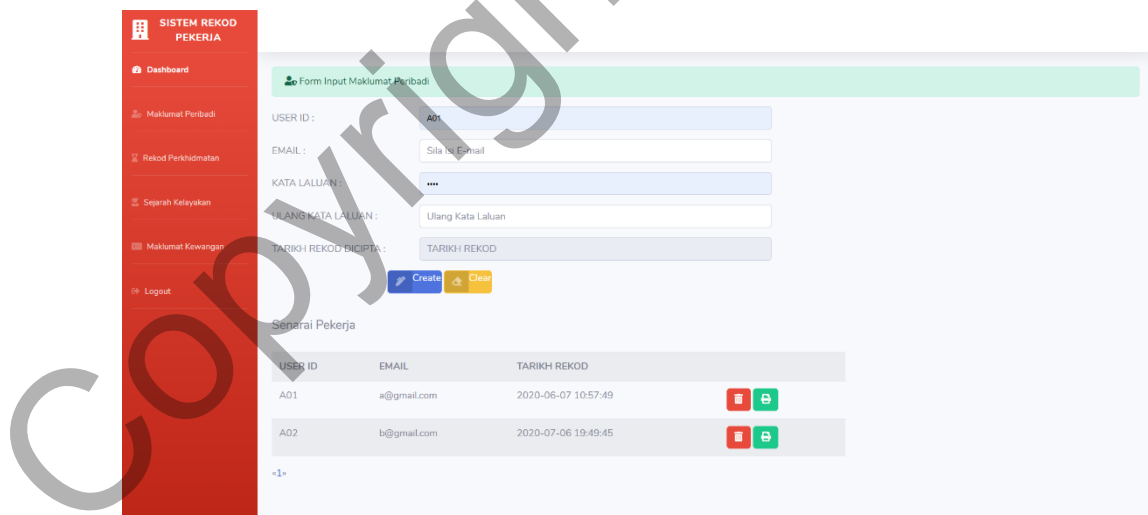
Rajah 5.4: Antara Muka Log Masuk Pengguna



Rajah 5.5 menunjukkan antara muka *dashboard*. Setelah pengguna log masuk kedalam sistem terdapat *flashdata* akan menyatakan pengguna berjaya log masuk. Laman ini menyediakan kemudahan kepada *admin* mengemaskini data pekerja, di sebelah kiri laman, terdapat menu untuk *admin* menambah dan mengemaskini rekod. Terdapat butang berlabel seperti *Dashboard*, *Maklumat Peribadi*, *Rekod Perkhidmatan*, *Sejarah Kelayakan*, *Maklumat Kewangan* dan *Logout*.



Rajah 5.5: Antara Muka Dashboard



Rajah 5.6: Antara Muka Halaman Maklumat Peribadi

Rajah 5.6 menunjukkan antara muka senarai rekod sedia ada di fungsian *Maklumat Peribadi*. Laman ini membolehkan *admin* mencipta User ID dan maklumat peribadi pekerja ke dalam sistem dengan menggunakan butang *create* setelah admin mengisi

ruangan yang disediakan. Laman ini juga membolehkan admin untuk melihat butiran rekod pekerja dengan butang *print* serta menghapus rekod dengan butang *delete*.

Laman ini juga mengkaitkan teknik *hashing* sebaik sahaja *admin* mencipta User ID dan kata laluan bagi pengguna yang lain seperti di rajah 5.7. Sistem ini menggunakan algoritma *password\_hash* bagi menukarkan kata laluan kepada nilai hash dan disimpan ke dalam pangkalan data seperti rajah 5.8.



```
112
113     $sql = "INSERT INTO users (uidUsers, emailUsers, pwdUsers) VALUES (?, ?, ?)";
114
115     $stmt = mysqli_stmt_init($conn);
116
117     if (!mysqli_stmt_prepare($stmt, $sql)) {
118         header("Location: ../signup.php?error=sqlerror");
119         exit();
120     }
121     else {
122
123
124
125
126
127         $hashedPwd = password_hash($password, PASSWORD_DEFAULT);
128
129
130         mysqli_stmt_bind_param($stmt, "sss", $username, $email, $hashedPwd);
131
132         mysqli_stmt_execute($stmt);
133
134         header("Location: ../signup.php?signup=success");
135         exit();
136     }
137 }
138 }
139 }
140 }
141
142 mysqli_stmt_close($stmt);
143 mysqli_close($conn);
144 }
```

Rajah 5.7: Pengkodan Hashing kata laluan

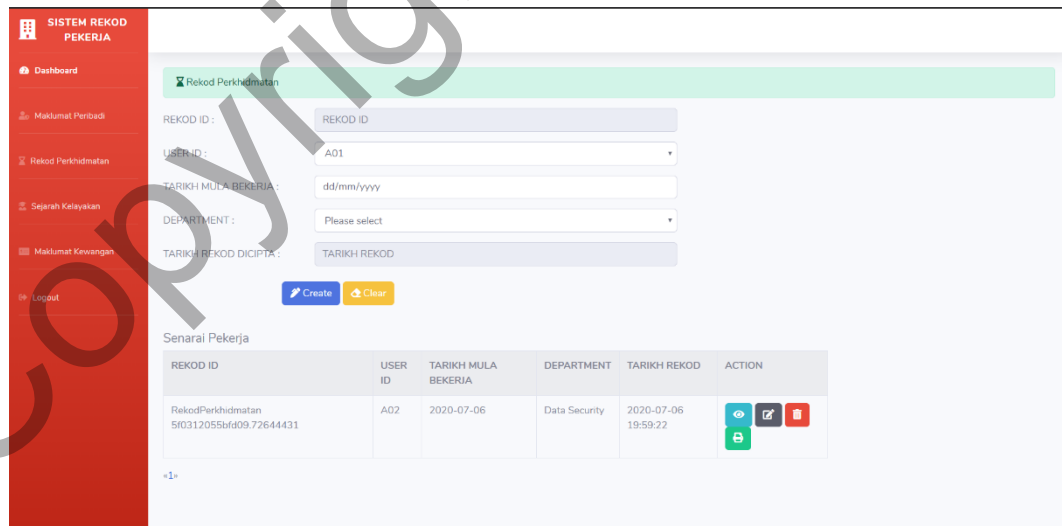
| uidUsers | emailUsers  | pwdUsers   |
|----------|-------------|--|
| A01      | a@gmail.com | \$2y\$10\$0o1QoYPL.4I9yYI3r0IrPeJkuMRsSHTYR080qhL9aVG... |
| A02      | b@gmail.com | \$2y\$10\$yG83lt/O/v7hZ3EsKYCG..uwddeCwYzF9CL80bEI3o1... |
| A03      | c@gmail.com | \$2y\$10\$bdtvkFB/eHJsVH0wJAyIEe8RWjjlVWA.aVs.nUSEET5... |

Rajah 5.8: Nilai hash yang disimpan ke dalam pangkalan data

Rajah 5.9 menunjukkan sekiranya pengguna hendak log masuk ke dalam sistem pengkodan *password\_verify* digunakan untuk mencari semula kata laluan yang dimasukkan dalam pangkalan data, *dehash* kata laluan tersebut dan *verify* sekiranya kata laluan itu adalah benar.

Rajah 5.9: Pengkodan Verify Kata laluan

```
logininc.php
30 $sql = "SELECT * FROM users WHERE uidUsers=? OR emailUsers=?";
31
32 $stmt = mysqli_stmt_init($conn);
33
34 if (!mysqli_stmt_prepare($stmt, $sql)) {
35     header("Location: ../index.php?error=sqlerror");
36     exit();
37 }
38 else {
39     mysqli_stmt_bind_param($stmt, "ss", $mailuid, $mailuid);
40
41     mysqli_stmt_execute($stmt);
42
43     $result = mysqli_stmt_get_result($stmt);
44
45     if ($row = mysqli_fetch_assoc($result)) {
46         $pwdCheck = password_verify($password, $row['pwdUsers']);
47     }
48     if ($pwdCheck == false) {
49         header("Location: ../index.php?error=wrongpwd");
50         exit();
51     }
52     else if ($pwdCheck == true) {
53         session_start();
54     }
55 }
```



Rajah 5.10: Antara Muka Halaman Rekod Perkhidmatan

Rajah 5.10 ialah antara muka rekod perkhidmatan. Laman ini membolehkan *admin* manambah rekod perkhidmatan pekerja ke dalam sistem. Rekod boleh ditambah melalui User ID yang telah wujud. Halaman ini juga membolehkan melihat *detail* rekod, *update* rekod, print rekod dan *delete* rekod pekerja.

**SISTEM REKOD PEKERJA**

Dashboard

Maklumat Pribadi

Rekod Perkhidmatan

Sejarah Kelayakan

Maklumat Kewangan

Logout

**Sejarah Kelayakan**

REKOD ID:

USER ID:

PENCAPAIAN AKADEMIK TERTINGGI:

TARIKH REKOD DICIPTA:

Senarai Pekerja

| REKOD ID                                    | USER ID | PENCAPAIAN TERTINGGI | TARIKH REKOD           | ACTION  |
|---|---------|----------------------|------------------------|---|
| SejarahKelayakan<br>5f03124a39ba34.63602777 | A02     | SARJANAMUDA          | 2020-07-06<br>20:00:41 | <input type="button" value="Detail"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> |

+1-

Rajah 5.11: Antara Muka Halaman Sejarah Kelayakan

Rajah 5.11 menunjukkan antara muka sejarah kelayakan. Laman ini membolehkan *admin* manambah sejarah kelayakan pekerja ke dalam sistem. Rekod boleh ditambah melalui id yang telah wujud. Halaman ini juga membolehkan melihat *detail* rekod, *update* rekod, print rekod dan *delete* rekod pekerja.

**SISTEM REKOD PEKERJA**

Dashboard

Maklumat Pribadi

Rekod Perkhidmatan

Sejarah Kelayakan

Maklumat Kewangan

Logout

**Maklumat Kewangan**

REKOD ID:

USER ID:

PENDAPATAN - RM:

TANGGUNGAN:

TARIKH REKOD DICIPTA:

Senarai Pekerja

| REKOD ID                                    | USER ID | PENDAPATAN (RM) | JUMLAH TANGGUNGAN | TARIKH REKOD           | ACTION  |
|---|---------|-----------------|-------------------|------------------------|---|
| MaklumatKewangan<br>5f03124a39ba34.63602777 | A02     | 3500            | 3                 | 2020-07-06<br>20:02:40 | <input type="button" value="Detail"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> |

+1-

Rajah 5.12: Antara Muka Halaman Maklumat Kewangan

Rajah 5.12 menunjukkan antara muka maklumat kewangan sedia ada. Laman ini membolehkan *admin* manambah maklumat kewangan pekerja ke dalam sistem. Rekod boleh ditambah melalui id yang telah wujud. Halaman ini juga membolehkan melihat *detail* rekod, *update* rekod, print rekod dan *delete* rekod pekerja.

## 6 KESIMPULAN

Sistem Pengurusan Rekod Pekerja ini adalah sebuah sistem yang berasaskan web. Dalam era kini yang mempunyai teknologi yang canggih dan berkembang, sistem ini dibina bagi mejamin keselamatan rekod dan memudahkan pengguna untuk menyimpan dan menyelenggara maklumat.

Teknologi Sistem Pengurusan Rekod Pekerja ini bergantung pada teknik *hashing*, kaedah matematik, dan kriptografi, justeru menawarkan kadar keselamatan yang lebih besar. Metodyang diguna pakai ialah metod *Rapid Application Development* (RAD) Beberapa fungsian juga telah ditetapkan. Setiap sistem yang dibangunkan mempunyai kelebihan tersendiri.

## 7 RUJUKAN

Anon. 2016. What Is TheDifference Between Hashing And Encrypting. <https://www.securityinnovationeurope.com/blog/page/whats-the-difference-between-hashing-and-encrypting> [30 September 2019]

Curtis Dicken. 2019. So, You Want Your Pages to be Encrypted , Huh? <https://www.htmlgoodies.com/beyond/reference/article.php/3472781/So-You-Want-Your-Pages-to-be-Encrypted-Huh.htm> / [29 September 2019]

Jonathan Suth. 2014. Securely Hash Password With PHP. <https://jonsuh.com/blog/securely-hash-passwords-with-php/> [30 Januari 2020]

Lucidchart Content Team. 2018. 4 Phases Of Rapid Application Development Methodology. <https://www.lucidchart.com/blog/rapid-application-development-methodology> [2 Oktober 2019]

Miker Irick. 2017. Data Hashing And Encryption And How They Enhance Security. <https://sandstormit.com/data-hashing-and-encryption-and-how-they-enhance-security/> [29 September 2019]

Copyright@FTSM