ISSN: 2477-5126
e-ISSN:2548-9356

# Analisa Keamanan Data melalui *Website* Zahra *Software* Menggunakan Metode Keamanan Informasi *CIA Triad*

**Adi Hermawan[1]*, Tuti Hartati[2], Yudhistira Arie Wijaya[3]**
[1,2,3]Jurusan Teknik Informatika, STMIK Ikmi Cirebon, Cirebon
[1,2,3]Jln. Perjuangan No. 10B, Karyamulya, Kec. Kesambi, Kota Cirebon, Jawa Barat 45131
email: [1]adihermawan0720@gmail.com, [2]toohart2013@gmail.com, [3]yudhistira010471@gmail.com

***Abstract*** *– Today the development of technology is growing rapidly, including developments in the field of information technology, many companies are taking advantage of technological developments by using web apps as corporate data storage media so that serious action is needed in securing the web app. One company that takes advantage of the development of information technology by creating a web app called Zahra Software. Zahra Software is a web app that is used for corporate data storage. However, the company does not yet know the extent of the security of Zahra Software as a medium for storing company data so that analytical actions are needed to find out how far Zahra Software's security is according to the security indicators used by experts, namely the CIA Triad. The purpose of this study is to find out how far where is the security of the Zahra Software web app as a company data storage medium. This study uses the CIA Triad information security method consisting of confidentiality, integrity, and availability to measure the extent of security possessed by a web app. Based on the results of the study, it was found that the Zahra Software web app has met 3 main indicators of information security which consists of confidentiality including block direct, namely username and password verification, integrity includes data and user filtering, namely by distinguishing user access rights according to the selected level, and availability. includes authentication, namely the existence of a database consisting of a list of usernames and passwords that are allowed to access data.*

***Abstrak*** **–** Dewasa ini perkembangan teknologi semakin pesat tak terkecuali perkembangan pada bidang teknologi informasi, banyak perusahaan yang memanfaatkan perkembangan teknologi dengan menggunakan *web app* sebagai media penyimpanan data perusahaan sehingga perlu tindakan serius dalam mengamankan *web app* tersebut. Salah satu perusahaan yang memanfaatkan perkembangan teknologi informasi dengan membuat sebuah *web app* yang diberi nama Zahra *Software.* Zahra *Software* adalah sebuah *web app* yang dipergunakan untuk penyimpanan data perusahaan. Namun perusahaan belum mengetahui sejauh mana keamanan dari Zahra *Software* tersebut sebagai media penyimpanan data perusahaan sehingga perlu tindakan analisa untuk mengetahui sejauh mana keamanan yang dimiliki Zahra *Software* sesuai indikator keamanan yang digunakan oleh para ahli yaitu CIA Triad.. Tujuan dari penelitian ini adalah untuk mengetahui sejauh mana keamanan yang dimiliki oleh *web app* Zahra *Software* sebagai media penyimpanan data perusahaan. Penelitian ini menggunakan metode keamanan informasi CIA Triad yang terdiri dari *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) untuk mengukur sejauh mana keamanan yang dimiliki oleh suatu *web app*. Berdasarkan hasil penelitian didapatkan bahwa *web app* Zahra *Software* telah memenuhi 3 indikator utama keamanan informasi yang terdiri atas *confidentiality* meliputi *block direct* yaitu adanya verifikasi *username* dan *passwor*d, *integrity* meliputi filterisasi data dan *user* yaitu dengan membedakan hak akses pengguna sesuai level yang dipilih , serta *availability* yang meliputi *autentikasi* yaitu adanya *database* yang terdiri daftar *username* dan *pasword* yang diperbolehkan untuk mengakses data.

***Kata Kunci*** **–** teknologi informasi, *web app*, indikator keamanan informasi, metode CIA Triad.

## I. PENDAHULUAN

Pesatnya perkembangan teknologi informasi telah memberikan dampak positif di berbagai bidang, dan salah satu bidang yang mendapat manfaat dari perkembangan teknologi informasi adalah teknologi internet [1]. Situs web adalah salah satu hal utama yang digunakan banyak instansi pemerintah dan bisnis untuk melindungi data mereka dan mendorong aktivitas mereka [2]. Namun, banyak perusahaan yang membangun *website* sebagai penyimpanan data perusahaan tanpa memperhatikan apakah *website* yang mereka bangun memenuhi standar CIA Triad sebagai alat untuk mengukur keamanan *website* mereka [3]. Selain itu, Zahra *Software* adalah aplikasi web yang digunakan untuk penyimpanan data perusahaan pribadi, dan aplikasi web tersebut belum dianalisis lebih lanjut untuk keamanan informasi yang dimilikinya.

Menurut para ahli, ada tiga aspek penting dari indeks keamanan situs web, yang dikenal sebagai CIA Triad. CIA Triad itu sendiri terdiri dari kerahasiaan, integritas, dan ketersediaan [4]. Selain itu, berdasarkan observasi dan wawancara yang dilakukan, ditentukan bahwa Zahra *Software* belum melakukan analisis keamanan *website*, sehingga tidak diketahui sejauh mana keamanan *website* yang digunakan sebagai tempat penyimpanan data perusahaan tersebut agar keamanan data perusahaan dapat ditingkatkan lebih baik.

Penelitian sebelumnya yang berjudul "*Analyzing Data Center Information Security Using Cobit 5*" yang dilakukan oleh (Muhamad et al., 2017) berfokus pada analisis data *center* institusi yang pernah mengalami *shell injection*. Dari hasil pemeriksaan diketahui kadar APO13 dan DSS05 adalah

*) **penulis korespondensi**: Adi Hermawan
Email: adihermawan0720@gmail.com,

ISSN: 2477-5126
e-ISSN:2548-9356

1,54 dan 1,68 yang dapat dikatakan level 2. Artinya proses APO13 dan DSS05 berjalan dan terpelihara sesuai rencana [5]. Selain itu, penelitian sebelumnya yang berjudul "Analisis Sistem Informasi/Kinerja Teknologi Informasi di PT" oleh (Syarif et al., 2018). Bank Central Asia menggunakan framework IT *Balanced Scorecard*. Penelitian ini berfokus pada pengukuran kinerja aplikasi KlikBCA secara keseluruhan dari berbagai dimensi. Hasil penelitian menunjukkan bahwa Klik BCA berada pada level yang baik sebesar 71,71% [6]. Selain itu juga penelitian dengan judul "Analisis Kualitas *Website* Alumni Stikom Bali Menggunakan Metode Webqual" dilakukan oleh (Santiari & Rahayuda, 2018). Penelitian ini berfokus pada analisis kualitas *website* dan permasalahan yang dihadapi belum terupdate dengan dokumentasi dan informasi yang ada pada *website*. Akibatnya, ada tiga indikator penolakan di situs web yang memerlukan tindakan korektif, tiga di antaranya adalah kesulitan dalam memberikan informasi, reputasi yang baik, dan kesadaran masyarakat [7].

Berdasarkan tiga survei sebelumnya, analisis situs web sangat baik, tetapi hasil di lapangan menunjukkan bahwa serangan itu masih ada, analisisnya tidak komprehensif dan hanya fokus pada beberapa aspek, selanjutnya analisis webqual hanya berfokus pada kualitas interaksi, maka penelitian ini akan dilakukan analisa secara menyeluruh, tidak hanya berfokus pada aspek kualitas saja dan analisa yang dilakukan dengan menggunakan keseluruhan aspek sehingga sesuai dengan indikator keamanan CIA Triad.

Berdasarkan penjelasan di atas, penelitian ini menganalisis aplikasi web perangkat lunak zahra berdasarkan metode CIA Triad dan mengukur tingkat keamanan perangkat lunak zahra menurut indeks keamanan informasi yang biasa digunakan oleh para ahli yaitu triad Cia.

Tujuan utama dari penelitian ini adalah untuk menganalisis kualitas keamanan aplikasi web Zahra *Software* untuk melihat apakah aplikasi web yang digunakan sebagai penyimpanan data perusahaan tergolong aman dan bagi mahasiswa STMIK Ikmi Cirebon untuk memberikan referensi judul serta digunakan untuk penelitian selanjutnya.

*) **penulis korespondensi**: Tuti Hartati, MT
Email: toohart2013@gmail.com

## II. PENELITIAN YANG TERKAIT

Berikut ini daftar jurnal yang digunakan sebagai penelitian yang paling relevan :

1. Penelitian yang berjudul "Analisa Keamanan Web *Server Open Jurnal System* (OJS) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Osj Universitas Lancang Kuning)" penelitian ini mempunyai tujuan untuk melakukan pengujian keamanan terhadap web server yang dimiliki oleh univeritas lancang kuning, hasil dari penelitian menunjukan bahwa sistem keamanan yang sedang digunakan oleh univeritas tersebut tergolong aman [8].
2. Penelitian yang berjudul "Analisa Kualitas *Website* Tribunnews.com Menggunakan Metode Webqual dan *Importance Performance Analysis*" penelitian ini mempunyai tujuan untuk mengetahui kualitas layanan yang dimiliki oleh situs tribunnews.com apabila dilihat dari perspektif pengguna, hasil penelitian diharapkan mampu menjadi referensi bagi pengembangan situs tribunnew.com agar menjadi lebih baik [9].
3. Penelitian yang berjudul "Analisa Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking" Fokus penelitian ini adalah untuk mengetahui keamanan yang dimiliki oleh aplikasi internet banking BCA berdasarkan 3 aspek keamanan informasi, hasil penelitian menunjukan bahwa mayoritas dari keseluruhan karyawan tersebut menyatakan jika availability merupakan aspek paling penting yang mempengaruhi keamanan aplikasi [10].
4. Penelitian yang berjudul "Analisa Pengalaman Pengguna Pada *Website* Distro Management System (Dimans)" Penelitian ini berfokus pada analisa sistem manajemen yang digunakan oleh distro serta pengalaman pengguna dalam menggunakan media situs dimans, hasil penelitian menunjukan bahwa pada penelitian subjektif responden memberikan poin yang cenderung positif bahwa dapat dikatakan sangat baik [11].
5. Penelitian yang berjudul "Analisa Keamanan Kemudahan Dan Kepercayaan Terhadap Keputusan Pembelian Secara Online Di Lazada" Penelitian ini serius dalam mengetahui pengaruh keamanan, kemudahan serta kepercayaan dalam keputusan transaksi jual beli yang dilakukan media *e-commerce* lazada.co.id, hasil penelitian menunjukan bahwa pengaruh keamanan dan kemudahan berpengaruh positif namun pengaruh kepercayaan lebih mendominasi dari ketiga aspek tersebut [12].

## III. METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah metode CIA Triad. CIA Triad adalah indikator keamanan informasi yang digunakan oleh para ahli sebagai alat ukur keamanan sebuah *web app*, dimana CIA Triad terdiri atas *confidentiality* atau kerahasiaan, *integrity* atau integritas, serta *availability* atau ketersedian, dimana hal tersebut dapat dijelaskan melalui gambar dibawah ini :

ISSN: 2477-5126
e-ISSN:2548-9356

Gbr. 1 Tahapan Metode CIA Triad

a. *Confidentiality*
*Confidentiality* atau kerahasiaan adalah suatu langkah – langkah yang perlu dilakukan untuk memastikan kerahasiaan atau privasi suatu *web app* agar tidak di akses oleh orang yang tidak memiliki kewenangan, contoh penggunaan *confidentiality* adalah *block direct*.

b. *Integrity*
*Integrity* atau integritas adalah kepercayaan data atau keaslian data dimana data tidak boleh diubah oleh orang yang tidak memiliki kewenangan untuk mengakses data didalam nya sehingga perlu tindakan tidak hanya memfilter data namun juga memfilter penguna yang ada didalam *web app* tersebut agar orang yang tidak memiliki kewenangan tidak dapat mengakses data tersebut, contoh penggunaan *integrity* adalah filterisasi data dan *user*.

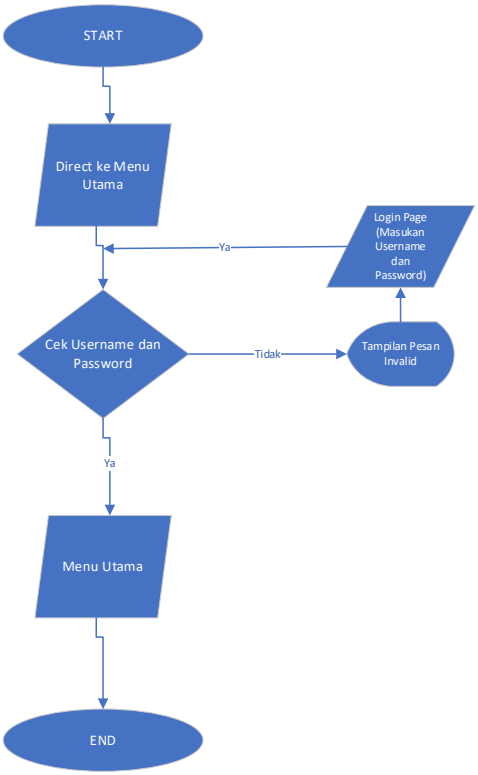
c. *Availability*
*Availability* atau ketersediaan data ialah serangkaian langkah – langkah yang digunakan untuk memberikan jaminan autentikasi kepada pengguna bahwa data didalam nya tidak dapat diakses oleh orang yang tidak memiliki kewenangan, contoh penggunaan *availability* adalah dengan menggunakan *username* dan *password* sebelum mengakses data yang ada didalam *web app*.

## IV. HASIL DAN PEMBAHASAN

### A. *Confidentiality*

#### *1. Block Direct*

*a. Flowchart*




Gbr. 2 *Flowchart Block Direct*

Berdasarkan *Flowchart* di atas, pengguna yang mencoba mengakses menu utama (home.php) secara langsung harus melewati verifikasi *username* dan *password*. Jika nama pengguna dan kata sandi nol, jendela peringatan akan ditampilkan dan pengguna akan diarahkan ke halaman *login*, memberikan nama pengguna dan kata sandi yang terdaftar di server. Jika nama pengguna dan kata sandi divalidasi dan terdaftar, pengguna dapat mengakses menu utama melalui aplikasi web.

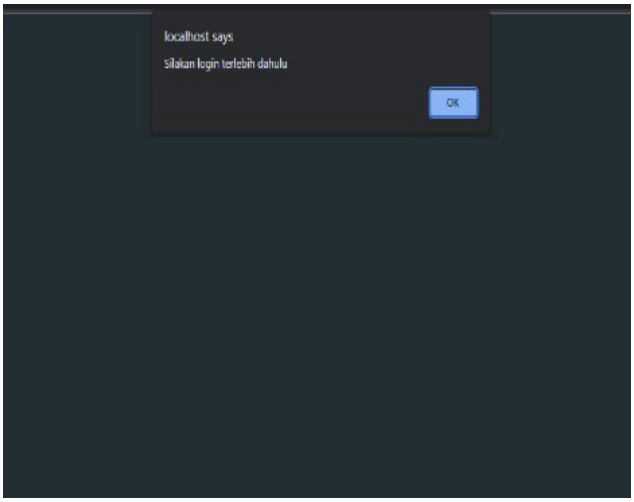
*b. Coding*

```
<?php
<- - Block Direct - ->
session_start();
if (empty($_SESSION['username']) or empty($_SESSION['level']))
{
    echo "<script>alert('Silakan login terlebih
dahulu');document.location='index.php'</script>";
}
```

Gbr. 3 *Coding Block Direct*

*Coding* yang digunakan adalah dengan menggunakan percabangan ***if*** dimana jika *session username* dan level tersebut *empty* (kosong) maka muncul pesan "Silakan login terlebih dahulu" kemudian pengguna akan diarahkan ke *login page* (index.php) untuk memasukan *username*, *password* dan level yang terdaftar.

*c. Testing*




Gbr. 4 *Testing Block Direct*

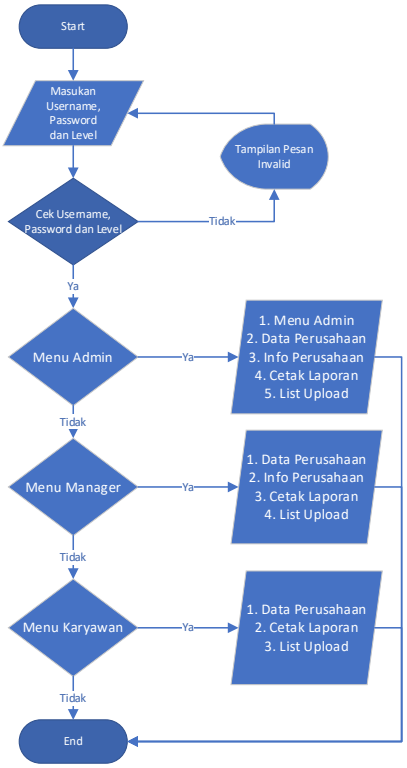
Gambar diatas adalah hasil pengetesan mengenai *block direct* dimana pengguna yang tidak memiliki akses memaksa masuk tanpa melewati proses autentikasi terlebih dahulu maka pengguna tersebut akan ter-block kemudian pengguna tersebut akan diarahkan ke login page untuk memasukan *username* dan *password*.

ISSN: 2477-5126
e-ISSN:2548-9356

**B. *Integrity***

**1.** Filterisasi Pengguna dan Data

*a. Flowchart*




Gbr. 5 *Flowchart* Filterisasi Pengguna dan Data

*Flowchart* diatas menjelaskan bahwa pengguna diharuskan memasukan *username*, *password* serta memilih level pengguna dimana hal tersebut bertujuan untuk membedakan akses pengguna sesuai level yang dipilih, setelah itu pengguna akan diarahkan ke *homepage* sesuai dengan level yang sudah di tentukan serta data yang di filterisasi untuk mencegah terekspos nya data secara menyeluruh kepada pihak yang tidak memiliki wewenang, sehingga data menjadi lebih terlindungi dan kebocoran data pun dapat di minimalisir.

b. *Coding*

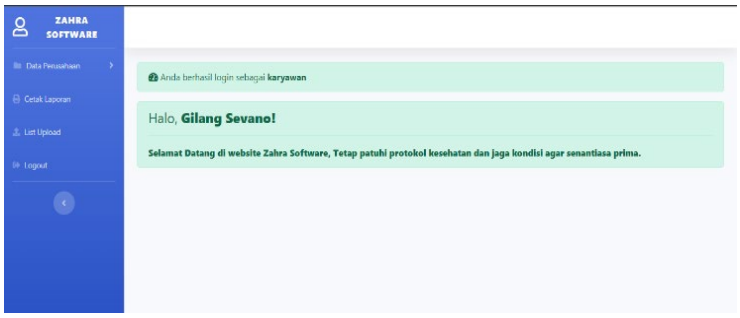
```
<-- Filterisasi -->
$cek_user =mysqli_query($koneksi, "SELECT * FROM user WHERE username
= '$username' and level = '$level' ");
$user_valid = mysqli_fetch_array($cek_user);
if($user_valid){
if($password == $user_valid['password']){
session_start();
$_SESSION['username'] = $user_valid['username'];
$_SESSION['nama_lengkap'] = $user_valid['nama_lengkap'];
$_SESSION['level'] = $user_valid['level'];
  if($level == "karyawan"){          header('location:home_karyawan.php');
} elseif ($level == "hrd") {
          header('location:home_manager.php');
} elseif ($level == "admin") {
header('location:home_adm.php');
}
} else{
    echo "<script>alert('Maaf Login Gagal, password salah'); document.location =
'index.php'</script>";
}
} else{
echo "<script>alert('Maaf Login Gagal, username tidak terdaftar');
document.location = 'index.php'</script>";
}
```

Gbr. 6 *Coding* Filterisasi Data dan Pengguna

*Coding* yang digunakan adalah dengan menggunakan cabang ***if***. Di sini, jika kata sandi yang dimasukkan cocok dengan kata sandi yang terdaftar di database, variabel $user_valid dijalankan. Jika benar, program berikut akan dijalankan. Di mana nama pengguna = nama pengguna, kata sandi = kata sandi, dan level = level, berdasarkan input pengguna, mengidentifikasi apakah program mengidentifikasi pengguna sebagai karyawan dan menjalankan program untuk mengambil pengguna. Masuk ke halaman *home* karyawan yaitu home_karawan.php, namun jika *user* yang teridentifikasi bukan karyawan maka akan dialihkan ke halaman *home* lain sesuai dengan inputan *user*, namun apabila ID lengkap dari *user* yang terdaftar tidak dapat ditemukan, program untuk menampilkan pesan "Maaf, login gagal. Nama pengguna tidak terdaftar."

c. *Testing*


Gbr. 7 *Testing* Filtersasi Data Dan Pengguna (Admin)




Gbr. 8 *Testing* Filterisasi Data dan Pengguna (Manager)

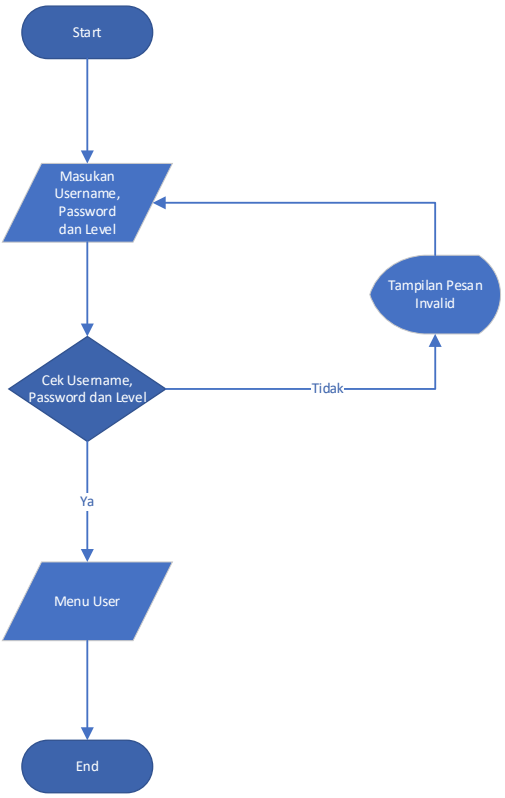
ISSN: 2477-5126
e-ISSN:2548-9356

Gbr. 9 *Testing* Filterisasi Data dan Pengguna (Karyawan)

**C. *Integrity***

***1.*** Autentikasi

*a. Flowchart*




Gbr. 10 *Flowchart* Autentikasi

*Flowchart* diatas menjelaskan bahwa pengguna diharuskan memasukan *username* dan *password* sebelum mengakses informasi yang ingin didapatkan, apabila *username* dan *password* tersebut terdaftar maka pengguna akan diarahkan menu *user* dan diperbolehkan mengakses informasi yang mereka butuhkan namun apabila *username* dan *password* yang pengguna inputkan tidak terdaftar maka pesan *invalid* akan muncul dan pengguna akan kembali diarahkan memasukan *username* dan *password* yang terdaftar di *database*.

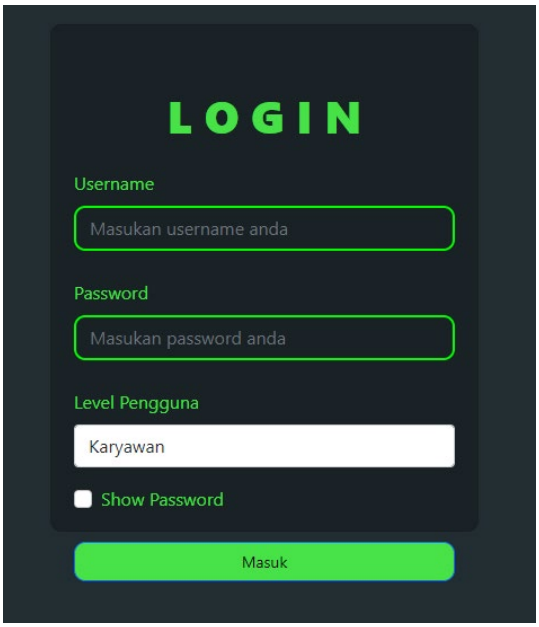
b. *Coding*

```
<-- Autentikasi -->
$username = mysqli_real_escape_string($koneksi,
$_POST['username']);
$password = mysqli_real_escape_string($koneksi,
$_POST['password']);
$level = mysqli_real_escape_string($koneksi, $_POST['level']);
$cek_user =mysqli_query($koneksi, "SELECT * FROM user WHERE
username = '$username' and level = '$level' ");
```

Gbr. 11 *Coding* Autentikasi

*Coding* diatas menjelaskan bahwa variabel $*username*, $*password* dan $level adalah variabel yang diambil dari "*username*, *passwword* dan level" yang ada di *database*, dimana fungsi *mysqli_real_escape_string* berfungsi untuk menghambat terjadi serangan *sql injection* sehingga data yang sudah di inputkan akan di kirim ke *database* dan dalam proses pengiriman itu kemungkinan terjadi nya penyusup yang masuk akan di hambat oleh fungsi *mysqli_real_escape_string* selanjutnya variabel yang sudah dipanggil tersebut berasal dari $cek_user yang memanggil keseluruhan data yang tertampung di tabel *user*.

c. *Testing*




Gbr. 11 *Testing* Autentikasi

Gambar diatas menjelaskan bahwa pengguna diharuskan memasukan *username*, *password* dan memilih level yang sesuai, kemudian apabila pengguna seudah memasukan *username*, *password* dan sudah menentukan level pengguna selanjutnya pengguna akan diarahkan ke *homepage* sesuai level yang dipilih tersebut, namun apabila pengguna yang dimasukan tidak terdaftar maka pesan *invalid* akan muncul dan pengguna akan kembali diarahkan ke tampilan awal login untuk memasukan kembali *username* dan *password* yang sebenarnya.

Menurut buku berjudul "Pemrograman Web Edisi Revisi" [13] dan buku berjudul "Panduan Cepat Belajar HTML, PHP & MySql" [14] mengatakan bahwa standar *coding* yang baik adalah :

- *Coding* yang dibuat harus simpel agar dapat menekan proses *compiling* lebih cepat
- Penulisan *coding* harus efisien dan tidak berulang, hal tersebut agar mempermudah *programer* dalam menjelaskan *coding* yang mereka buat.
- Penulisan *coding* harus konsisten dalam penamaan variabel, *namespace* dan ukuran huruf sehingga mudah untuk dipahami.
- Memberikan komentar agar mempermudah identifikasi *coding* yang digunakan.

Dan berdasarkan *coding* yang digunakan diatas dimana penggunaan *coding* lebih sederhana, tidak berulang, dan pemberian komentar untuk mengidentifikasi maksud dan

tujuan *coding* itu dibuat maka dapat dikatakan *coding* yang digunakan sudah sesuai standar

## V. KESIMPULAN

Dari hasil pembahasan dan penelitian yang sudah dibahas sebelum nya dapat disimpulkan bahwa :

1. Analisis keamanan data dengan metode keamanan informasi CIA Triad menunjukkan bahwa Zahra *Software* memenuhi standar indeks keamanan informasi.
2. Analisis didasarkan pada beberapa aspek dari masing-masing indikator *confidentiality* berfokus pada aspek *block direct*, *integrity* berfokus pada aspek filter data dan pengguna, serta *availability* berfokus pada aspek autentikasi dengan analisis yang dilakukan mengenai alur diagram, *coding* yang digunakan serta hasil akhir yang menunjukan bahwa program berjalan sesuai rencana yang sudah ditetapkan.

## UCAPAN TERIMA KASIH

Terima Kasih kepada pihak perusahan PT. Siraj Badawi Cukup Rupiah (SBCR) atas izin observasi, wawancara dan penelitian yang dilakukan terkait Zahra *Software* serta pihak STMIK Ikmi Cirebon atas arahan dan bimbingan dalam penulisan jurnal ini.

## DAFTAR PUSTAKA

[1] Huda, N. (2019). Analisis Kinerja *Website* Pt Pln (Persero) Menggunakan Metode Pieces. *Sistemasi*, *8*(1), 78–89.

[2] Bekti. (2018). Konsep Dasar Web Server. *Website Adalah Media Presentasi Online Untuk Sebuah Perusahaan Atau Lembaga Maupun Perorangan. Website Dapat Digunakan Sebagi Media Penyampaian Informasi Secara Online. Website Juga Merupakan Suatu Sistem Yang Berkaitan Dengan Dokumen Yang Digunakan Sebag*, *35*, 35.

[3] Wijaya, Y. D. (2021). *EVALUASI KEAMANAN SISTEM INFORMASI PASDEAL BERDASARKAN INDEKS KEAMANAN INFORMASI ( KAMI ) ISO / IEC 27001 : 2013*. *4*(2), 115–130.

[4] Yusnita Sari, I., Muttaqin, Jamaludin, Simarmata, J., Rahman, M. A., Iskandar, A., Fernando, A., Sugianto, Giap, Y. C., & Hazriani. (2020). *Keamanan Data Dan Informasi*.

[5] Muhamad, I., Matin, M., & Wardhani, L. K. (2017). *ANALISIS KEAMANAN INFORMASI DATA CENTER MENGGUNAKAN COBIT 5*. *10*(2). https://doi.org/10.15408/jti.v10i2.7026

[6] Syarif, A. F., Basuki, P. N., & Wijaya, A. F. (2018). *Analisa Kinerja Sistem Informasi / Teknologi Informasi pada PT. Bank Central Asia Menggunakan Kerangka IT Balanced Scorecard*. *10*(1), 1491–1502.

[7] Santiari, P. L., & Rahayuda, I. G. S. (2018). Analisis Kualitas *Website* Alumni Stikom Bali Menggunakan Metode Webqual. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *5*(2), 231. https://doi.org/10.25126/jtiik.201852576

[8] Guntoro, Costaner, L., & Musfawati. (2020). *Analisis keamanan web server open journal system (ojs) menggunakan metode issaf dan owasp (studi kasus ojs universitas lancang kuning)*. *05*, 45–55.

[9] Barus, E. E., Suprapto, & Herlambang, D. A. (2021). Analisis Kualitas *Website* Tokome Menggunakan Metode Webqual 4.0 dan Importance Performance Analysis. *Jurnal Informatika Universitas Pamulang*, *6*(1), 57. https://doi.org/10.32493/informatika.v6i1.8130

[10] Dianta, I. A., & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan Pada Nasabah Pengguna Internet Banking. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *3*(1), 1. https://doi.org/10.29407/intensif.v3i1.12125

[11] Suastini, N. K., Raditya Putra, I. G. L. A., & Satwika, I. P. (2018). Analisis Pengalaman Pengguna Pada *Website* Distro Management System (Dimans). *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *10*(3), 135–144.

[12] Rafidah, I. (2017). Analisis Keamanan, Kemudahan, dan Kepercayaan Terhadap Keputusan Pembelian Secara Online di Lazada. *Jurnal Ilmu Dan Riset Manajemen*, *6*(2), 1–17.

[13] Hidayatullah, P., & Kawistara, K. J. (2017). *Pemrograman Web Edisi Revisi*. Informatika Bandung.

[14] Prasetyo Adi, A. (2020). *Panduan Cepat Belajar HTML, PHP, & MySql*. PT. Elex Media Komputindo.