 ISSN 2337-6805

RANCANG BANGUN PENGAMAN SISTEM LOGIN MENGGUNAKAN METODE CAPTCHA

DESIGN AND BUILD LOGIN SYSTEM SECURITY USING CAPTCHA METHOD

Dadang Rusmana
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
Jl.Moh.Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
Telp.(021) 7874647, Fax. (021) 7866955
dadangrusmana@istn.ac.id

ABTRAKSI
Pada umumnya CAPTCHA berupa *image* yang memuat huruf atau angka yang dirusak dengan berbagai jenis *noise*. Tes ini melibatkan *user* untuk mengetikkan hasil tebakan huruf atau angka yang ada pada *image*. Tetapi terkadang masih banyak *web* yang tidak mengetahui tingkat keamanan dari CAPTCHA yang ditampilkannya, sehingga *spam* masih bisa menyamar sebagai manusia untuk mengakses dan menyerang *web*. Pada tulisan ini, telah dibuat sebuah simulasi sistem pembaca otomatis untuk CAPTCHA *multiline background*, dimana memuat teks berupa angka yang panjang karakternya berjumlah 6. Untuk memecahkan teks yang ada pada CAPTCHA, dilakukan beberapa proses tahapan yaitu mengetikan urutan angka dan huruf yang tersusun pada gambar untuk di ketik pada sebuah kolom yang sudah tersedia tepat dibawahnya serta melakukan pengenalan terhadap karakter angka itu sendiri, serta membaca tulisan apa yang dimuat pada CAPTCHA tersebut. MD5 digunakan pada keperluan authentication, dimana dengan MD5 sebuah dokumen dapat dibuktikan integritas dan keasliannya. MD5 juga digunakan pada aplikasi digital signature (penandatangan sebuah dokumen digital) sebagai fingerprinting function.
Kata Kunci : CAPTCHA, MD5, Enkripsi

ABSTRACT
In general, image CAPTCHA form containing the letters or numbers tampered with various types of noise. This test involves the user to type in the result of guesses letters or numbers in the image. But sometimes there are still many who do not know the web of CAPTCHA security level of the display, so that spam can still be disguised as humans to access and attack web. In this thesis, we have created a simulation of automated reader system for multiline CAPTCHA background, which contains the text of a number that the character length totaling 6. To solve the existing text in the CAPTCHA, conducted several process steps, namely typing a sequence of numbers and letters that are arranged in the image to be typed on a column that is already available right below as well as doing an introduction to the numeric character itself, and read what was published in the CAPTCHA.. MD5 is used in authentication purposes, where the MD5 document integrity and authenticity can be proven. MD5 is also used in digital signature applications (signer of a digital document) as fingerprinting function.
Keywords: *CAPTCHA, MD5, Encryption*

1. PENDAHULUAN

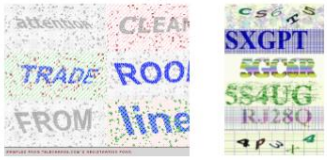
Sistem login adalah proses untuk mengakses komputer dengan memasukan identitas dari akun pengguna dan kata sandi untuk mendapatkan hak akses menggunakan sumber daya komputer tujuan. Pada saat melakukan login untuk masuk kedalam sistem, user akan diminta untuk masukkan identitas user seperti userid dan password sebagai antisipasi dalam hal pengamanan sistem. Password dapat di ubah sesuai dengan kebutuhan sedangkan userid tidak pernah di rubah karena berupa identitas unik yang merujuk ke user tertentu. Jika kedua pengamanan tersebut berhasil atau memenuhi maka user memiliki hak untuk mengakses sistem.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart) pada dasarnya adalah suatu progam yang sebagian besar manusia dapat melewatinya, akan tetapi komputer tidak dapat melewatinya (Ahn,2004). CAPTCHA digunakan untuk mencegah softwere otomatis (bot) untuk melakukan tindakan atas nama manusia yang sebenarnya. Tujuan utama CAPTCHAadalah memberikan uji tes yang mudah di jawab oleh manusia, tetapi tidak bisa di jawab oleh komputer. CAPTCHA terbagi dalam beberapa jenis, antara lain :

1) Hard Recognizing Text / Visual Based

Berdasarkan Visual (Visual Based) Virtual Based CAPTCHA memiliki beberapa variasi, yang paling umum digunakan saat ini adalah teks yang dimiringkan dan ditempelkan pada sebuah gambar dan pengenalan bentuk. CAPTCHA yang menggunakan teks dimiringkan yang ditempelkan pada gambar disebut Gimpy. Gimpy pertama kali dikembangkan oleh Luis yang mendesain versi

paling sederhana dari Gimpy, disebut EZ-Gimpy (Tsui,2004).
Perbedaan yang mendasar antara gimpy dan EZ-gimpy adalah Gimpy memiliki tiga atau lebih kata yang dimiringkan yang ditempelkan pada suatu gambar, sedangkan EZ-Gimpy hanya memiliki satu kata yang dimiringkan pada suatu gambar.



Gambar 1. Contoh *CAPTCHA* Type Visual Based
2) Sound Based

Berdasarkan suara (Sound Based) Sound based CAPTCHA kebanyakan digunakan untuk membantu mereka yang tuli atau mempunyai masalah dengan pendengaran. Suatu contoh sound based CAPTCHA adalah bunyi yang sesuai.Tes ini menjalankan klip audio yang berisi rekaman suatu urutan kata atau angka-angka yang dimiringkan dan jika kata atau angka- angka yang diduga tepat maka dapat melewati tes ini. (Tsui,2004).
3) Pattern Matching
CAPTCHA jenis ini benar-benar sangat unik, CAPTCHA ini berbentuk puzzle yang pecah-pecah dan memaksa pengguna harus menyusun puzzle atau CAPTCHA pattern matching tersebut.

Kriptografi
Kriptografi adalah suatu ilmu (yang mempelajari bagaimana (cara menjaga agar data atau pesan tetap aman saat dikirimkan, (dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied (Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga message-message agar tetap aman (secure).

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [bruce Schneier - Applied Cryptography]. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [A. Menezes, P. van Oorschot and S. Vanstone - Handbook of Applied Cryptography].
Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :
1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

Non-repudiasi., atau nirpenyangkalan adalah (usaha untuk mencegah terjadinya bpenyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

MD5 (Massage Digest 5)

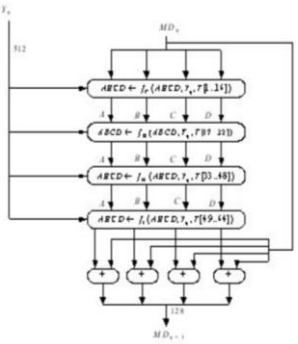
Algoritma scure hashing MD5 dirancang oleh Ron Rivest dan penggunaannya sangat populer dikalangan komunitas open source sebagai checksum untuk file yang dapat di download. MD5 juga kerap di gunakan untuk menyimpan password dan juga digunakan dalam digital signature dan certificate.

Spesifikasi lengkap untuk algoritma MD5 ada pada suatu RFC (request for comment). Besarnya blok untuk MD5 adalah 512 bit sedangkan digest size adalah 128 bit. Karena word size ditentukan sebesar 32 bit, satu blok terdiri dari 16 word sedangkan digest terdiri dari 4 word. Indeks untuk bit dimulai dari 0. Preprocessing dimulai dengan padding sebagai berikut:
Bit dengan nilai 1 ditambahkan setelah ahir naskah. Deretan bit dengan nilai 0 ditambah setelah itu sehingga besar dari naskah mencapai nilai 448 (mod 512) (setidaknya 0 dan sebanyaknya 511 bit dengan nilai 0 ditambahkan sehingga tersisa 64 bit untuk diisi agar besar naskah menjadi kelipatan 512).
64 bit yang tersisa diisi dengan besar naskah asli didalam bit. Jika besar naskah asli lebih dari 2^{64} bit maka hanya 64 bit lower order bit yang dimasukan sebelum high-order word.
MD5 adalah salah satu aplikasi yang digunakan untuk mengetahui bahwa pesan yang dikirim tidak ada perubahan sewaktu berada dijaringan. Algoritma MD5 secara garis besar adalah mengambil pesan yang mempunyai panjang variabel diubah menjadi “sidik jari” atau “intisari pesan” yang mempunyai panjang tetap yaitu 128 bit. Sidik jari ini tidapat di balik untuk medapatkan pesan, dengan kata lain tidak ada orang yang dapat melihat pesan dari sidik jari MD5.
Massage Digest 5 (MD5) adsalah salah sau penggunaan fungsi hash salah satu arah yang paling banyak digunakan. MD5 merupakan fungsi hash kelima yang dirancang oleh Ron Rivest dan didefinisikan pada RFC 321[10]. MD5 merupakan pengembang dari MD4 dimana terjadi penambahan satu ronde [1,3,10]. MD5 memproses teks memasukan kedalam blok-blok bit sebanyak 512 bit, kemudian dibagi kedalam 32 bit sub blok

sebanyak 16 buah. Keluaran dari MD5 berupa 4 buah blok yang masing-masing 32 bit yang mana akan terjadi 128 bit yang bisa disebut nilai hash[3,10]. Simpul utama MD5 mempunyai blok pesan dengan panjang 512 bit yang masuk kedalam 4 buah ronde. Hasil keluaran dari MD5 adalah berupa 28 bit dari byte terendah A dan tertinggi byte D.

Algoritma dan Cara Kerja :
Penjelasan Algoritma MD5
Setiap pesan yang akan dienkripsi, terlebih dahulu dicari beberapa banyak bit yang terdapat pada pesan. Kita anggap sebanyak b bit. Disini b adalah bit non negatif integer, b bisa saja nol dan tidak harus selalu kelipatan delapan.

Cara Kerja MD5
Langkah langkah pembuatan MD5 secara garis besar :
a. Penambahan bit-bit pengganjal (padding bits)
Pesan ditambah dengan sejumblah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512
Jika panjang pesan 448 bit, maka pesan tersebut di tambah dengan 512 bit menjadi 960 bit. Jadi, panjang bit-bit pengganjal adalah antara 1 sampai 512
Bit-bit pengganjal terdiri dari sebuah bit 1 diikuti dengan sisanya bit 0.
b. Penambahan nilai panjang pesan semula
Pesan yangbtelah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula.
Jika panjang pesan > 264 maka yang diambil adalah panjangnya dalam modulo 264. Dengan kata lain, jika panjang pesan semula adalah K bit, maka 64 bit yang di tambahkan dengan 64 bit yang di tambahkan menyatakan K modulo 264.
Setelah ditambahkan dengan 64 bit, panjang pesan sekarang mnjadi kelipatan 512 bit.
c. Inisialisasi penyangga (buffer) MD
MD5 membutuhkan 4 buah penyangga (buffer) yang masing masing panjangnya 32 bit. Total panjang penyangga adalah 4 X 32 = 128 bit. Keempat penyangga ini menampung hasil antra dan hasil akhir
Keempat penyangga ini di beri nama A, B, C, dan D. Setiap penyanga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut :
A = 01234567
B = 89ABCDEF
C = FEDCBA98
D = 76543210
d. Pengolahan pesan dalam blok berukuran 512 bit.
Pesan dibagi menjadi L buah blok yang masing-masing panjangnya 512 bit (Y0 sampai YL-1)
Setiap blok 512 bit diproses bersama dengan penyangga MD menjadi keluaran 128 bi, dan ini di sebut proses HMD5. Gambaran proses HMD5 Diperlihatkan pada gambar 2. berikut ini :



Gambar 2 . Proses HMD5

e. Inisialisai MD5
Ada MD5 terdapat empat buah word 32 bit register yang berguna untuk meninisialisasi massage digest pertama kali. Register register ini di inisialisasi dengan hexadesimal.
Word A : 01 23 45 67
Word B : 89 AB CD EF
Word C : FE DC BA 98
Word : 76 54 32 10
Register register ini bisa disebut dengan nama Chain variabel atau Variabel rantai

2. METODOLOGI PENELITIAN

Metode Pembuatan Sistem Keamanan
Metode perancangan sistem keamanan menggunakan model paradigma model air terjun (waterfall), karena menghasilkan sistem yang terstruktur dengan baik ditiap prosesnya. Dengan metode waterfall, tahap-tahap dalam perancangan aplikasi pada model waterfall diantaranya:

Gambar 3. Alur Diagram Pembuatan Sistem Keamanan

Tahap awal yang dilakukan sebelum membuat aplikasi adalah dengan mengumpulkan informasi yang berhubungan dengan aplikasi yang akan dibangun sebanyak-banyaknya melalui metode literatur, observasi, dan wawancara, serta mencari informasi melalui internet.

DesainCAPTCHA
Setelah mengumpulkan informasi, langkah selanjutnya adalah membuat desain dari aplikasi yang akan dibangun. Proses desain ini akan menerjemahkan kebutuhan-kebutuhan dari analisis yang sudah dilakukan sebelumnya, sebelum memulai pengkodean.

ISSN 2337-6805

Pengkodean
Pada tahap selanjutnya yaitu melakukan pengkodean. Pengkodean dilakukan menggunakan Notepad ++. Agar desain yang telah dibuat dapat berjalan sesuai dengan perancangan sistem, maka harus dilakukan sebuah pengkodean.

Pengujian
Ketika kode dibuat, pengujian program dimulai. Proses pengujian dilakukan untuk memastikan bahwa semua pernyataan telah diuji untuk menemukan kesalahan-kesalahan yang ada. Memastikan bahwa sistem berjalan sesuai dengan kebutuhan dan desain yang telah dibuat. metode yang dilakukan untuk menguji aplikasi yaitu, metode black box.

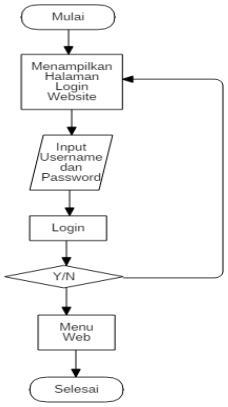
Pembuatan Laporan
Pengumpulan data dilakukan dengan cara mempelajari, meneliti, dan menelaah berbagai literatur yang bersumber dari buku-buku, jurnal ilmiah, situs internet, dan bacaan lainnya yang berkaitan dengan penelitian yang dilakukan.

Proses Sistem Keamanan
Secara umum sistem keamanan yang dirancang dan diimplementasikan pada websitePetani Buah Belimbing yaitu :

Proses login
User akan diminta untuk mengisi form :

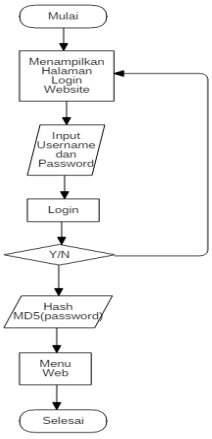
Gambar 4. Proses Login Website
Setelah user menginputdan menekan tombol login sistem akan melakukan validasi terhadap username, password dan CAPTCHA yang user masukan. Pada proses login kebanyakan sistem hanya menggunakan username dan password untuk proses otontefikasi. Adanya penambahan sistem keamanan pada halaman login menggunakan sistem CAPTCHA ini bertujuan untuk meningkatkan sistem keamanan pada halaman login dari serangan bot yang dapat mengancam kestabilan website petani buah belimbing dimana bot tersebut dapat mencoba masuk atau penetrasi terhadap sistem website, karena bot tersebut dapat melakukan penetrasi terhadap halaman login secara abnormal.
Selain penambahan sistem keamanan CAPTCHA terdapat juga keamanan pada hasil input dari user yaitu password yang dienkripsi menggunakan metode MD5 (massage digest 5) tujuan diterapkannya MD5 terhadapa passworduser untuk menjaga privasi data user dari serangan penyadapan dan pencurian data oleh para pelaku cyber crime.

Sistem Berjalan
Sistem Berjalan Login Admin



Gambar 5. Flowchart Sistem BerjalanLogin Admin
Gambar diatas menunjukan proses sistem berjalan. Dimana pada sistem berjalan belum terdapat sistem keamanan pada halaman login, dimana user hanya menginput username dan password untuk masuk kehalaman login.
a. Mulai
Dimana proses user membuka website petani buah belimbing
b. Menampilkan Halaman LoginWebsite
User membuka halaman loginwebsite petani buah belimbing
c. Input Username dan Password
Setelah membuka halaman loginwebsite petani buah belimbing user diwajibkan agar mengisi usernamedan passwordyang sudah dia miliki
d. Login
Setelah user menginput usernamedan passworduser memilih tombol login. Setelah user memilih tombol loginmaka sistem akan memprose jika benar maka akan masuk ke menu admin tersebut, dan jika user salah memasukan username dan password maka user akan kembali ketampilan halaman login dan user harus menginput username dan password yang benar.

Sistem Usulan



Gambar 6. Flowchart Sistem Usulan*Login* Admin

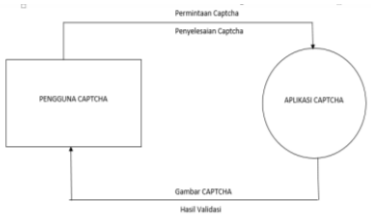
ISSN 2337-6805

Gambar diatas menunjukan proses sistem usulan. Dimana pada sistem usulan sudah terdapat sistem keamanan menggunakan CAPTCHA dan MD5.
Setelah user menginput username password dan CAPTCHA apabila benar maka sistem akan lansung mengenkripsi password yang ada. Tetapi apabila hasil input username pasword dan CAPTCHA salah maka sistem akan menampilkan kembali alamat login.
a. Mulai
Dimana proses user membuka website
b. Menampilkan Halaman LoginWebsite
User membuka halaman login website
c. Input Username, Password dan CAPTCHA
Setelah membuka halaman login website user diwajibkan agar mengisi username,password dan CAPTCHA
d. Login
Setelah user menginput username, password dan CAPTCHAuser memilih tombol login. Setelah user memilih tombol login maka sistem akan memproses. Jika benar maka akan lanjut ke proses selanjutnya, dan jika user salah memasukan username, password dan CAPTCHA maka user akan kembali ketampilan halaman login dan user harus menginput username, password dan CAPTCHA yang benar.
e. HashMD5
Setelah user memilih tombol login maka sistem akan memproses jika benar maka password akan terHash menggnakan MD5 secara otomatis dan user akan masuk ke akun user tersebut/selesai, dan jika user salah maka passwordtidak akan terHash dan user akan kembali ketampilan halaman login dan user harus menginput usernamepassword dan CAPTCHA yang benar.

3. HASIL DAN PEMBAHASAN

Diagram Konteks Model CAPTCHA

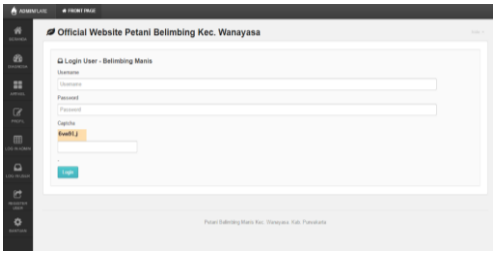
Diagram konteks dan diagram alir data digunakan untuk mendeskripsikan secara fungsional aliran informasi yang ditransformasikan pada saat data bergerak dari input menjadi output. Diagram konteks selalu mengandung satu proses yang mewakili sistem secara keseluruhan. Pada diagramkonteks untuk CAPTCHA, entitas adalah pengunjung situs web. Pengunjung mengakses halaman web tertentu untuk meminta ditampilkan persoalan CAPTCHA. Berdasarkan teks persoalan yang ditampilkan, pengunjung memasukkan jawaban persoalan. Hasil pemeriksaan dengan membandingkan teks persoalan dengan jawaban persoalan disampaikan kepada pengunjung. Diagram Konteks pada pengembangan CAPTCHA ini dijelaskan pada gambar 7.



Gambar 7. Diagram Konteks *CAPTCHA*

Perancangan*Interface*

Pada tahap perancangan *interface* ini dihasilkan desain antarmuka *CAPTCHA* seperti gambar dibawah ini. Gambar tersebut menunjukkan *CAPTCHA* dalam keadaan baru terbuka.



Gambar 8. Keadaan awal antar muka *CAPTCHA*

Pada CAPTCHA tersebut terdapat beberapa bagian, yaitu:
a. Bagian teks judul: Berisi nama dari CAPTCHA itu sendiri, teks tersebut tidak mengandung tautan.
b. Bagian utama: Bagian ini adalah yang paling utama dari CAPTCHA. Bagian ini mengandung potongan-potongan angka yang telah diacak- acak, pengguna diminta untuk menyusun potongan angka tersebut dengan cara mengetikan kembali susunan angka yang benar.
c. Bagian Preview: Bagian ini menampilkan gambar utuh dari angka yang ada pada bagian utama sehingga memudahkan pengguna dalam penyusunan angka.

Pembangkit Angka dan Session

Pada bagian ini pembuatan script untuk membangkitkan gambar CAPTCHAdimulai. Secara garis besar script ini terbagi menjadi beberapa bagian utama,yaitu:
a. Bagian yang membuat gambar baru berdasarkan sumber gambar lain. Pada bagian ini sebuah baris script PHP akan membuat sebuah gambar baru dari sebuah script sumber yang diberikan dari script lain, gambar baru yang terbuat nantinya akan identik dengan gambar sumber.
b. Bagian yang menyimpan kembali susunan angka kedalam sebuah session. Bagian ini bertugas untuk menyimpan kembali susunan angka yang telah dihasilkan kedalam sebuah session yang telah disiapkan.

Hasil Implementasi CAPTCHA

CAPTCHA yang dihasilkan adalah dalam berbentuk plugin php, dimana CAPTCHA bisa dipasangkan pada aplikasi web lain yang berbasis

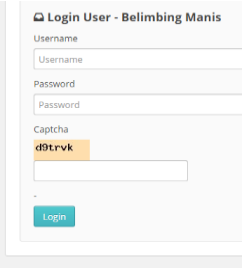
php selain dari aplikasi yang digunakan pada penelitian ini. Beberapa parameter harus disesuaikan ketika melakukan integrasi dengan sebuah aplikasi web diantaranya seperti perameter lokasi folder tempat penyimpanan file gambar sumber,lokasi folder tempat penyimpanan dan lainnya.

ImplementasiCAPTCHA sebagai berikut:

a. Filelogin.php. Fileini menampilkan textbox dan CAPTCHA.

b. FileCAPTCHA.php.File inti yang berisikan langkah kerja pembentukan angka, sistem kerja CAPTCHA, validasiCAPTCHA.

Hasil implementasi tampilanCAPTCHA sebagai berikut:



Gambar 9 . Form LoginCAPTCHA

Pengujian

Pengujian dilakukan untuk mengetahui apakah CAPTCHA dapat mencapai tujuan yang diinginkan dan menemukan kesalahan-kesalahan yang mungkin terjadi pada bagian implementasi.

Pengujian Blackbox

CAPTCHA yang telah dikembangkan selanjutnya akan diuji dengan menggunakan metode blackbox. Tahap pengujian dilakukan dengan tujuan untuk menjamin sistem yang dibuat sesuai dengan hasil analisis dan perancangan serta menghasilkan kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan. Pengujian dibagi dua yaitu pengujian menampilkan CAPTCHA dan pengujian sistem CAPTCHA.

Berikut hasil pengujian menampilkan CAPTCHA pada tabel1.

Tabel 1. Pengujian Menampilkan CAPTCHA

Deskripsi	Prosedur Pengujian	Input	Keluaran yang diharapkan	Kriteria evaluasi hasil	Hasil yang didapatkan
Pengujian menampilkan CAPTCHA	1. Masuk kan alamat index.php pada browser 2. Apabila alamat benar,maka tampil form dan CAPTCHA	-	Tampilnya form dan CAPTCHA	Tampilnya form dan CAPTCHA	Tampilnya form dan CAPTCHA

Selanjutnya Pengujian sistem dilakukan setelah CAPTCHA berhasil diintegrasikan pada form login. Terdapat dua skenario pada pengujian ini,yaitu:

a. SkenarioNormal Login

Skenario ini digunakan untuk menguji CAPTCHA dengan memasukkan data login yang valid dan menyusun CAPTCHA dengan benar. Hasil yang diharapkan dari pengujian ini adalah data-data login dibandingkan dengan data yang ada di database dan user bisa login dengan sukses jika hasil perbandingan itu valid.

Hasil pengujian dengan menggunakan skenario normal ini ditampilkan seperti pada gambar 9, Pada gambar diatas sedang dilakukan tahap ujicoba proses login pada halaman login admin yang telah diimplementasikan sebelumnya dengan algoritma MD5. Dengan menginputkan :

Username : Keanu
Password : 123456
CAPTCHA : 3bgldx

Langkah selanjutnya adalah melakukan proses login. Namun sebelum itu pada gambar dibawah ini ditampilkan username dan password yang sudah terdaftar di dalam database.

Dalam proses login diatas antara data yang diinput akan dibandingkan dengan data yang sudah ada dalam database. Jika sesuai maka proses login berhasil.

Gambar 10. Hasil Deskrip MD5

Dapat kita lihat pada gambar diatas merupakan hasil deskripsi dari hasil Hash MD5 yang tersimpan dalam database menghasilkan angka 123456.

Gambar 11. Verifikasi Hasil CAPTCHA

Setelah melakukan loginuser akan menerima informasi mengenai hasil verifikasi kode CAPTCHA yang sebelumnya sudah diinputkan dalam form login. Gambar diatas merupakan informasi yang disampaikan apabila user berhasil memasukan kode CAPTCHA yang valid.

4. SIMPULAN

Setelah melakukan analisis, desain serta implementasi terhadap website untuk penggunaan CAPTCHA dan MD5, maka dapat disimpulkan sebagai berikut :

a. Dari hasil pengujian yang dilakukan dari halaman register MD5 dapat berfungsi dan berjalan

ISSN 2337-6805

dengan baik pada halaman tersebut. Password berhasil di Hash menjadi MD5 sehingga dapat meningkatkan keamanan dari website tersebut.
b. Sistem saat ini memiliki tiga parameter terhadap proses login yaitu username dan password yang dimiliki oleh user dan juga kode CAPTCHA yang ditampilkan.

5. DAFTAR PUSTAKA

[1] Akil, Ibnu, 2016, ***Rekayasa Perangkat Lunak Dengan Model Unified Proses StudiKasus****: Sistem* Informasi Journal, Jurnal Pilar Nusa Mandiri,12(1). Astria, Firman dan

[2] D. M. Khairina, "Analisis Keamanan Sistem Login," *J. Inform. Mulawarman*, vol. 6, no. 2, pp. 64–67, 2011.

[3] Rusdianto. and A. Qashlim, "Implementasi Algoritma Md5 Untuk Keamanan Dokumen," *J. Ilm. Ilmu Komput.*, vol. 2, no. 2, pp. 2442–4512, 2016.

[4] S. T. Suci Oktaviana[1],, Satria Perdana Arifin, S.T, M.T.I[2], Ibnu Surya, "Sistem Pakar Diagnosa Penyakit Ginjal Menggunakan Metode Hill Climbing," *Sist. Pakar Diagnosa Penyakit Ginjal Menggunakan Metod. Hill Climbing*, vol. 1, pp. 1–10, 2012.

[5] A. Sulistyohati and T. Hidayat, "Aplikasi Sistem Pakar Diagnosa Penyakit Ginjal Dengan Metode Dempster-Shafer," *Semin. Nas. Apl. Teknol. Inf.*, vol. 2008, no. Snati, pp. 1907–5022, 2008.

[6] Inayatullah, "Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password," *J. Algoritm.*, vol. 3, no. 3, pp. 1–5, 2007.

[7] R. Munir, "Fungsi Hash Satu-Arah dan Algoritma MD5," *Dep. Tek. Inform. Inst. Teknol. Bandung*, pp. 0–17, 2004.