

Penambahan Keamanan dan Rancang Bangun Sistem Informasi Rekam Medis *Electronic* (RME)

Estu Sinduningrum¹⁾, Ikhwan Anjar Prabowo, Sriyono
Program Studi Teknik Informatika, Fakultas Teknik
Universitas Muhammadiyah Prof. DR. HAMKA.
Jl. Tanah Merdeka No.6, RT.10/RW.3, Rambutan, Kec. Ps. Rebo.
Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, 13830
¹⁾estu.ningrum@uhamka.ac.id

Diterima: 1 September 2019. Disetujui 20 September 2019. Dipublikasikan Nopember 2019

Abstrak – Perkembangan informasi yang terus meningkat, menyebabkan komputerisasi dalam berbagai macam bidang salah satunya adalah bidang kesehatan juga turut bertambah. Hal ini erat kaitannya dengan penggunaan *password* dalam area komputerisasi. Rawannya manipulasi *password* dinilai sebagai hal yang perlu dicegah menggunakan data *hiding*. Salah satu teknik dalam penyembunyian data yaitu kriptografi. Algoritma yang digunakan pada penelitian ini, yaitu algoritma genetika dan fungsi Hash SHA-1. Fungsi Hash SHA-1 adalah untuk mengenkrip *string password* yang di-input oleh *user* sehingga menghasilkan *chippertext* yang sulit ditebak. Perancangan untuk melindungi *database* pada satu rumah sakit di Jakarta menggunakan algoritma Hash SHA-1 yang ditanamkan di masukan (*login*) sistem informasi RME untuk melindungi dari akses yang tidak sah dari para peretas. Hasil percobaan dari 35 kali serangan *SQL Injection* selalu gagal *login*. Berdasarkan hasil *scan* menggunakan alat perangkat lunak Acunetix Web Vulnerability Scanner versi 6 maka diperoleh kesimpulan bahwa sistem dinyatakan kuat dan tidak terdeteksi adanya celah ataupun kelemahan.

Kata Kunci: kriptografi sha-1; rekam medis elektronik

I. PENDAHULUAN

Rekam medis adalah berkas yang berisi identitas, *anamnesa*, penentuan fisik, laboratorium, diagnosa dan tindakan medis terhadap seorang pasien yang dicatat baik secara tertulis maupun elektronik [1]. Sistem rekam medis dimulai dari pencatatan selama pasien mendapatkan pelayanan medik sampai dengan penyelenggaraan serta pengeluaran berkas rekam medis dan tempat

penyimpanan untuk melayani permintaan/peminjaman oleh pasien atau untuk keperluan lainnya [1]. Beberapa hal penting yang perlu diperhatikan terutama pada keamanan dari sebuah website dan yang menjadi titik kerentanan adalah *login* dan *database*.

Sistem *login* yang menggunakan *database* sebagai *authentication* dari *username* dan *password* sangat rentan untuk diretas. *SQL Injection* adalah salah satu teknik serangan yang umum diterapkan oleh para peretas untuk melakukan eksploitasi dari suatu *website*, dan akibatnya peretas bisa mendapatkan akses tidak sah kedalam sistem dan mengambil data langsung dari *database* [2].

Konsep RME mirip dengan rekam medis berbasis kertas, yaitu sebagai sarana mendokumentasikan data maupun informasi utama pada sarana pelayanan kesehatan. Kedua format seperti itu juga dapat diartikan sebagai alat komunikasi dan penyimpanan informasi kesehatan milik pasien pada sarana kesehatan. Dengan adanya rekam medis tersebut dapat diketahui mengenai siapa (*who*), apa (*what*), kapan (*when*), dimana (*where*), mengapa (*why*), dan bagaimana (*how*) pelayanan kesehatan diberikan kepada seorang pasien [3].

Kriptografi adalah teknik untuk mengubah suatu pesan masukan agar tidak dapat diketahui isinya, dan membentuk suatu bidang keilmuan yang disebut dengan sebutan ilmu kriptografi. Prinsip dasarnya dari kriptografi adalah menyembunyikan informasi dengan sedemikian rupa agar orang yang berhak menerima informasi tersebut saja yang dapat melihat isi dari informasi yang dikirim tersebut. Seiring dengan kemajuan teknologi, teknik yang dipergunakan untuk mengenkripsi data didalamnya mengandung unsur matematis yang membuat isi dari informasi tersebut semakin sukar untuk diketahui [4].

Fungsi *hash* (*hash function* atau *hash algorithm*) adalah suatu cara untuk menghasilkan sebuah *digital "fingerprint"* kecil dari sembarang data. Fungsi ini memecahkan dan mencampurkan data untuk menghasilkan *fingerprint* yang sering disebut sebagai nilai *hash* (*hash value*) [5]. Nilai *hash* ini sering direpresentasikan dengan sebuah *string* pendek dari huruf-huruf dan angka-angka yang kelihatan acak (berbentuk heksadesimal) [5]. Sebuah fungsi *hash* yang baik adalah suatu fungsi yang tidak (jarang) memiliki *output* nilai *hash* yang sama untuk *input* yang berbeda [5]. *Secure Hash Algorithm* (SHA) adalah fungsi *hash* satu arah yang diciptakan oleh institusi yang bernama NIST (*National Institute of Standard and Technology*). SHA dinyatakan sebagai standar fungsi *hash* satu arah. SHA dapat dianggap sebagai kelanjutan pendahulunya MD5 dan dapat dikatakan aman karena dibuat sedemikian sehingga secara komputasi tidak memungkinkan menemukan *string* yang berkaitan dengan *message digest* yang dihasilkan [5].

SHA1 dikatakan cukup aman karena proses SHA1 dihitung secara infisibel untuk mencari *string* yang sesuai untuk menghasilkan *message digest* atau dapat juga digunakan untuk mencari dua *string* berbeda yang akan menghasilkan *message digest* yang sama [6].

Berdasarkan data dan pemaparan di atas, maka dibuatlah perlindungan website sistem informasi rekam medis elektronik dengan memanfaatkan fitur *security* PHP dan *secure hash algorithm-1* sebagai algoritma kriptografi untuk mengenkripsi *string password*.

II. METODE PENELITIAN

Metode pengembangan pada penelitian menggunakan metode SDLC dengan model *Waterfall*. Model *Waterfall* sering disebut *classic life cycle* atau siklus hidup klasik yang menggambarkan penekanan sistematis dan juga berurutan pada pengembangan perangkat lunak yang dimulai dari spesifikasi kebutuhan pengguna kemudian berlanjut melalui tahapan perancangan, Pemodelan, Konstruksi, serta penyerahan sistem kepada para pelanggan dan berakhir dengan perawatan pada perangkat lunak yang telah dibuat [7]. Penjelasan untuk diagram alir penelitian, yaitu:

1. Identifikasi Masalah

Masalah yang terjadi adalah meningkatkan pengamanan *security* dari web rekam medis elektronik dari berbagai jenis serangan keamanan. Pada suatu rumah sakit di Jakarta, belum adanya sistem keamanan *database* untuk rekam medis elektronik. Bagaimana merancang sebuah sistem keamanan untuk rekam medis elektronik menggunakan *algoritma genetika* dan *fungsi Hash SHA-1*.

2. Pengumpulan Data

Metode yang digunakan dalam pengumpulan data adalah studi pustaka, wawancara, dan kuesioner.

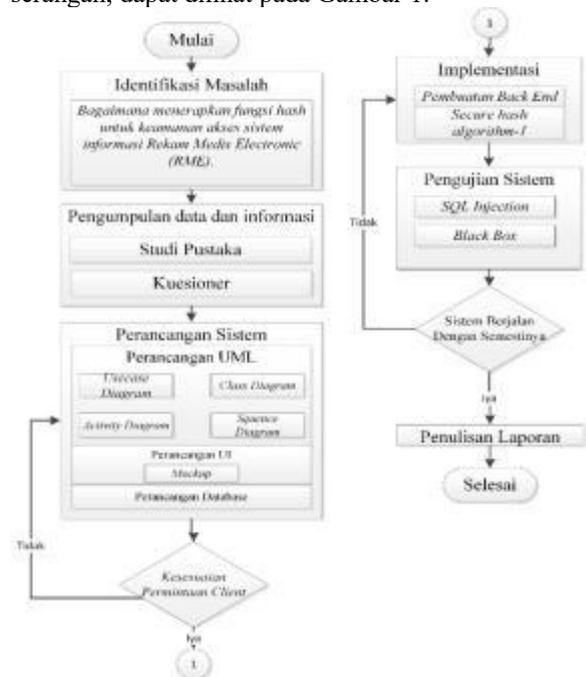
3. Perancangan Sistem

Langkah-langkah perancangan sistem diantaranya:

- 1) Perancangan *Database* menggunakan bahasa pemrograman MySQL.
- 2) Perancangan *Interface* menggunakan bahasa pemrograman PHP.
- 3) Perancangan Keamanan Sistem dengan penerapan fitur *Security* PHP.

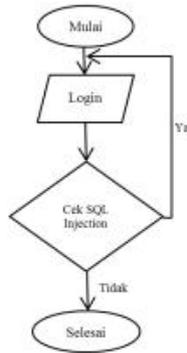
4. Pengujian

Pengujian keamanan dari penerapan *secure hash algorithm-1* adalah dengan menggunakan simulasi serangan *SQL Injection*. Yang diuji langsung kepada sistem melalui menu *login*. Tahapan simulasi serangan, dapat dilihat pada Gambar 1.



Gambar 1 Diagram Alir Penelitian

Pada Gambar 2 simulasi serangan menggunakan *SQL Injection* dilakukan dengan memasukkan kode serangan dalam *form login* untuk mengetahui apakah sistem pengamanan berhasil atau tidak. *SQL Injection* dicoba pada *form login* jika kondisinya 'ya' maka dilakukan *looping* ke *form login*. Jika tidak berhasil maka berhak masuk ke *input login* yang harus sesuai dengan data pada *database*, kemudian disesuaikan dengan data yang ada, jika sesuai maka masuk ke sistem dan sebagai bukti bahwa *SQL Injection* tidak dapat meretas sistem.



Gambar 2 Tahapan Simulasi Serangan SQL Injection

Pengujian perangkat lunak sistem ini bertujuan sebagai uji coba sebelum aplikasi dirilis kepada pengguna eksternal. Untuk menguji coba apakah aplikasi yang telah dibuat berjalan sesuai dengan *output* dari fungsi atau fitur yang digunakan oleh pengguna dan pengujian sistem juga bertujuan untuk mencari kesalahan atau *error* yang terdapat pada aplikasi yang telah dibuat.

Pengujian aplikasi dilakukan menggunakan teknik *black box* di mana teknik ini berguna untuk menguji coba secara keseluruhan fitur-fiturnya, apakah berfungsi semua atau masih terdapat *bug*, *error*, tanpa harus melihat *source code*-nya jika masih terdapat *error* maka ulangi ke proses pengkodean sistem, jika tidak ada *error* maka lanjut ke tahap selanjutnya. *Black-Box Testing* merupakan pengujian yang berfokus pada spesifikasi fungsional dari perangkat lunak, *tester* dapat mendefinisikan kumpulan kondisi *input* dan melakukan pengetesan pada spesifikasi fungsional program [8].

Pengujian hasil enkripsi pada *string password* yang telah di-*input* oleh *user*. Jika seorang *user* memasukkan kata “admin” pada kolom *username* dan *password*, maka kata “admin” pada *string password* dienkripsi sehingga menjadi sebuah *string* baru yang acak dan tidak mudah dikenali.

Dapat dilihat pada Tabel 1 bahwa sistem yang telah diterapkan diuji dengan skala likert, dengan data kuesioner yang diberikan kepada pengguna. Skala likert merupakan skala yang digunakan untuk pengukuran yang diperkenalkan oleh likert pada tahun (1932). Skala likert memiliki beberapa jenis pertanyaan yang dikombinasikan sehingga mampu membentuk suatu skor/nilai [9].

TABEL I. HASIL ENKRIPSI STRING PASSWORD DENGAN SHA-1

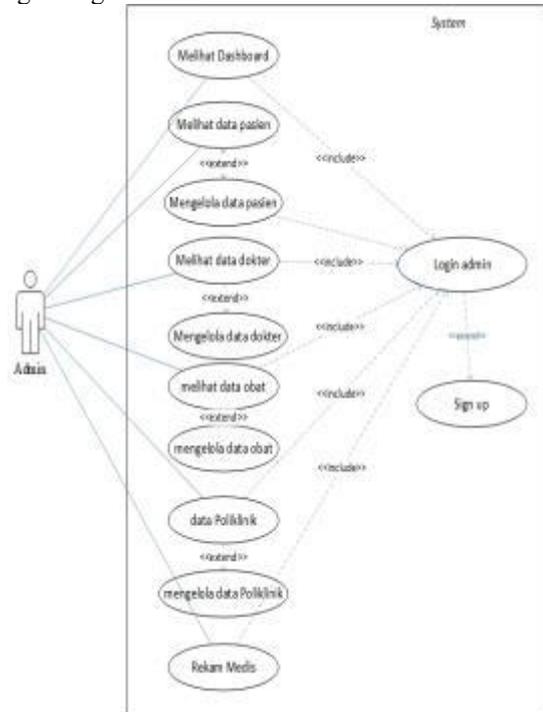
Username	Password
Admin	d033e22ae348aacc5660fc2140aec35850c4da997

5. Pembuatan Laporan

Pada tahap ini dijelaskan secara keseluruhan mengenai penelitian yang telah dirancang dan diuji.

III. HASIL DAN PEMBAHASAN

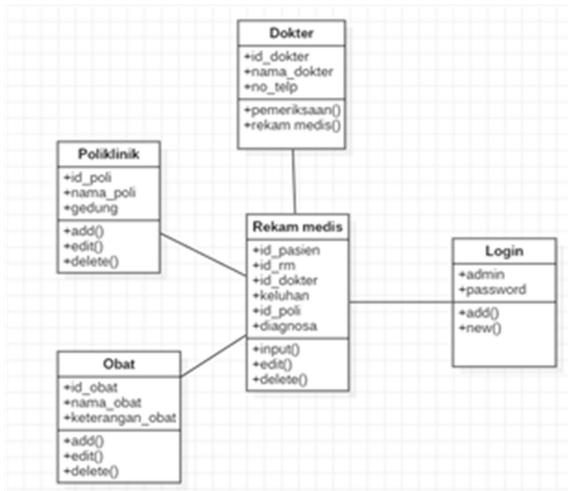
Perancangan *use case diagram* ditunjukkan pada Gambar 3. Keamanan ini diletakkan pada bagian login admin.



Gambar 3 Rancangan Usecase Diagram Sistem

Perancangan *class diagram*, *class diagram* menggambarkan struktur status *class* dalam sistem. *Class diagram* termasuk ke dalam bagian UML *view* yaitu *logical view* dimana *class diagram* ini menjelaskan bagaimana fungsional dari sistem, struktur statis (*class*, *object*, *relationship*) dan kombinasi yang terjadi saat *object* mengirimkan pesan ke *object* lain di dalam satu fungsi tertentu. Berikut ini adalah gambaran *class diagram* pada penelitian ini seperti yang bisa dilihat pada Gambar 4.

Hasil dari rancangan *interface* dapat dilihat pada Gambar 5 yang merupakan tampilan halaman *login* dimana terdapat dua jenis pengguna yaitu admin dan perawat. Pada halaman ini *user* bisa melakukan *sign up* dengan mengisi data pada masing masing kolom yang telah disediakan. Gambar 6 merupakan tampilan halaman kelola data pasien yang dapat diakses oleh admin. Admin dapat menambah, menghapus serta meng-*edit* data pasien pada halaman ini.



Gambar 4 Perancangan Class Diagram



Gambar 5 Tampilan Interface Login



Gambar 6 Tampilan Interface Kelola Data Pasien

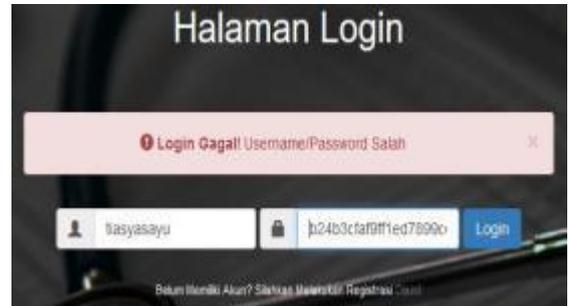
Gambar 7, merupakan tampilan halaman kelola data Obat yang hanya dapat diakses oleh admin. Admin dapat menambah, menghapus, serta mengedit data rekam medis pada halaman ini.



Gambar 7 Tampilan Interface Kelola Data Rekam Medis

IV. PENGUJIAN KEAMANAN SISTEM

Pengujian yang dilakukan pada penelitian ini dengan cara memasukkan *string password* pada halaman login seperti pada Tabel II. Hasil pengujian dapat dilihat pada Gambar 8.



Gambar 8 Hasil pengujian kewan system

Pengujian *SQL Injection*, *SQL Injection* adalah sebuah teknik yang digunakan untuk menyalahgunakan sebuah celah keamanan yang terdapat pada lapisan basis data sebuah aplikasi [2]. Pada penelitian ini telah dilakukan serangan menggunakan *SQL Injection* namun pada kesempatan ini dilakukan kepada website yang memiliki tingkat keamanan yang baik. Berikut skenario pengujiannya dapat dilihat pada Tabel II.

TABEL II. SKENARIO SERANGAN *SQL INJECTION*

No	Variable SQL	Dampak Serangan
1	'or 1=1#	Gagal login
2	"or 1=1-	Gagal login
3	'or 1=1-	Gagal login
4	'or'a'='a'#	Gagal login
5	'or"a"="a"#	Gagal login
6	Admin'#	Gagal login
7	'or 'x'='x'#	Gagal login
8	Admin' or 1=1#	Gagal login
9	hi' or 'a'='a'#	Gagal login
10	hi") or ("a"="a	Gagal login
11	Admin' or 0=0#	Gagal login
12	"or"a"="a	Gagal login
13	"or 0=0#	Gagal login
14	admin ' or 'x'='x	Gagal login
15	"or "x"="x	Gagal login
16) or ('x'='x	Gagal login
17	' or 1=1--	Gagal login
18	" or 1=1--	Gagal login
19	Or 1=1--	Gagal login
20	' or a=a--	Gagal login
21	" or "a"="a	Gagal login
22	hi" or 1=1 --	Gagal login
23	admin'--	Gagal login
24	'having 1=1--	Gagal login
25	hi' or 'a'='a	Gagal login
26	hi" or 1=1--	Gagal login
27	admin'--	Gagal login
28	"or 0=0--	Gagal login

29	admin 'or''a''='a'#	Gagal login
30	admin hi' or a'='a'#	Gagal login
31	admin'or l=1#	Gagal login
32	admin hi' or a'='a'#	Gagal login
33	hi' or 'a'='a#	Gagal login
34	hi') or ('a'='a	Gagal login
35	hi') or ("a"='a#	Gagal login

Gambar 9 merupakan hasil pengujian *Threat* Sistem dengan bantuan perangkat lunak Acunetix Web Vulnerability Scanner versi 6. Pengujian ini dilakukan dengan menggunakan parameter pengujian *Default* untuk mengetahui adanya celah dan kelemahan dari Sistem Informasi Rekam Medis Elektronik yang sudah dibangun. Dari Gambar 9 dapat diambil kesimpulan bahwa sistem rekam medis elektronik yang telah dibangun tidak terdapat adanya celah dan kelemahan.



Gambar 9 Hasil Pengujian Pencarian Celah dan Kelemahan Sistem

Selanjutnya dilakukan pengujian deskripsi *string password* melalui *website generator*. Gambar 10 merupakan hasil pengujian dekripsi pada *string password* yang sudah ada dalam *database* dan dijadikan akses untuk login ke dalam *website*.



Gambar 10 Hasil Pengujian Dekripsi String Password

Pada Gambar 10 dijelaskan bahwa *string* enkripsi SHA-1 terhadap kata "admin" masih bisa di dekripsi menggunakan *web generator*. Hasil yang didapat dari pengujian sistem yang dibangun menggunakan metode *black box* untuk sistem *admin*, dapat dilihat pada Tabel III.

TABEL III. HASIL UJI SISTEM ADMIN DENGAN MENGGUNAKAN METODE *BLACK BOX*

No.	Pengujian	Hasil	Keterangan
1	Mengisi form <i>login</i> dengan mengisi <i>username</i> dan <i>password</i> lalu menekan tombol <i>login</i>	<i>Admin</i> masuk kehalaman utama (<i>dashboard</i>).	Sukses
2	Memilih menu Pasien, Dokter, Obat, Poliklinik, Rekam medis.	Pasien : menampilkan data pasien. Dokter : menampilkan data dokter Obat : menampilkan data obat. Poliklinik : menampilkan halaman data poiklinik. Rekam medis : menampilkan halaman data rekam medis.	Sukses
3	Memilih menu Pasien, menambah data, mengubah data, menghapus data, klik tombol kembali, dan tombol simpan data.	Memilih menu pasien : menampilkan halaman pasien, Menambah data : menampilkan halaman tambah data pasien. Ubah data : mengubah data pasien berdasarkan id yang dipilih Hapus data : menghapus data pasien berdasarkan id yang dipilih Kembali : kembali ke halaman data pasien. Simpan : menyimpan data	Sukses
4	Menekan tombol PDF,CSV,EXEL,PRINT,COPY	PDF: <i>mendownload</i> data yang terdapat pada tabel daftar pasien dalam format PDF. CSV : <i>mendownload</i> data yang terdapat pada tabel daftar pasien dalam format Exel Comma Separated Values. Exel : <i>mendownload</i> data yang terdapat pada tabel pasien dalam format Exel Print : mencetak data yang terdapat pada tabel daftar pasien. Copy : mensalin data pada daftar pasien ke <i>Clipboard</i>	Sukses
5	Memilih menu Dokter, menambah data, mengubah data, menghapus data, klik tombol kembali, dan tombol simpan data	Memilih menu dokter : menampilkan halaman dokter, Menambah data : menampilkan halaman tambah data dokter. Ubah data : mengubah data dokter berdasarkan id yang dipilih Hapus data : menghapus data dokter berdasarkan id yang dipilih.	Sukses

		Kembali : kembali ke halaman data dokter. Simpan : menyimpan data	
6	Memilih menu Obat, menambah, mengubah, menghapus data, dan klik tombol kembali, dan tombol simpan data.	Memilih menu obat: menampilkan halaman obat, Menambah data : menampilkan halaman tambah data obat. Ubah data : mengubah data obat berdasarkan id yang dipilih Hapus data : menghapus data obat berdasarkan id yang dipilih. Kembali : kembali ke halaman data obat. Simpan : menyimpan data	Sukses
7	Memilih menu Poliklinik, menambah data, mengubah data, klik tombol kembali, dan tombol simpan data.	Memilih menu poliklinik: menampilkan halaman poliklinik, Menambah data : menampilkan halaman tambah data poliklinik. Ubah data : mengubah data poliklinik berdasarkan id yang dipilih Hapus data: menghapus data poliklinik berdasarkan id yang dipilih. Kembali : kembali ke halaman data poliklinik. Simpan : menyimpan perubahan	Sukses
8	Memilih menu Rekam medis, menambah data, mengubah data, klik tombol kembali, dan tombol simpan data.	Memilih menu Rekam medis: tampil halaman Rekam medis, Menambah data : menampilkan halaman tambah data Rekam medis. Ubah data : mengubah data rekam medis berdasarkan id pasien, id dokter, id obat yang dipilih Hapus data : menghapus data Rekam medis berdasarkan id pasien, id dokter, id obat yang dipilih. Kembali : kembali ke halaman data Rekam medis. Simpan : menyimpan data	Sukses

Pengujian sistem untuk pengguna dilakukan oleh para relawan. Peneliti telah membagikan kuesioner kepada 25 orang responden, untuk melakukan uji coba terhadap kinerja sistem dan fungsi dari fitur-fitur yang disediakan dalam Sistem Informasi Rekam Medis Elektronik ini. Dengan harapan untuk mengetahui apakah sistem sudah berjalan dengan semestinya. Tabel IV berisi pertanyaan yang diajukan.

TABEL IV. DAFTAR PERTANYAAN KUESIONER

No	Kuesioner
1	Keamanan data Anda adalah hal yang sangat penting.
2	Kriptografi sangat berguna untuk pengamanan data dalam suatu sistem terkomputerisasi.
3	Sudah mengetahui sistem informasi rekam medis elektronik.
4	Sudah mengetahui bahwa sistem yang telah Anda uji saat ini adalah salah satu model dari sistem informasi rekam medis.
5	Anda tidak menemukan kesulitan dalam mengoperasikan sistem informasi rekam medis elektronik tersebut.
6	Tombol-tombol menu yang tersedia berfungsi dengan baik.

Skala likert digunakan untuk menghitung hasil ataupun tanggapan dan penilaian yang didapat dari tahap pengujian sistem. Tabel V berisi hasil perhitungan kuesioner.

TABEL V. HASIL PERHITUNGAN KUESIONER

No	Skor					Nilai Maximum (N-Max)	Jumlah Skor					Persentase (%)	
	1	2	3	4	5		1	2	3	4	5		Jumlah
1	0	0	0	7	18	125	0	0	0	28	90	118	94.4
2	0	0	6	7	12		0	0	18	28	60	106	84.8
3	0	3	6	7	9		0	6	18	28	45	97	77.6
4	0	0	7	8	10		0	0	21	32	50	103	82.4
5	0	0	5	7	13		0	0	15	28	65	108	86.4
6	0	0	4	6	15		0	0	12	24	75	111	88.8
Jml	0	3	28	42	77		0	6	84	168	385	643	514.4
Rata-rata												85.73333333	

$$\begin{aligned} \text{Nilai Maximal (N-Max)} &= \text{Jumlah responden} \times \text{Skor} \\ &= 25 \times 5 \\ &= 125 \end{aligned}$$

$$\begin{aligned} \text{Jumlah Persentase} &= \text{Total jumlah skor} / \text{N-Max} \times 100 \\ \text{Rata-rata} &= \text{Jumlah persentase} / \text{total skor} \\ &= 514 / 6 \\ &= 86 \% \end{aligned}$$

Pengujian sistem bagi pengguna oleh para relawan dengan membagikan kuesioner berupa sekumpulan pertanyaan mengenai pengujian sistem ini dengan harapan mendapatkan nilai persentase kepuasan dari pengguna mengenai sistem yang telah dibangun. Adapun rincian dari pada masing masing pertanyaan terbilang adalah sebagai berikut:

1. Pentingnya keamanan data

Berdasarkan pertanyaan pertama yang diajukan kepada para responden, "Setujukah anda bahwa keamanan data milik pribadi anda adalah hal yang sangat penting?" Sebanyak 18 responden

menjawab sangat setuju, dan 7 responden menyatakan setuju. Nilai persentase kesuksesan hasil dari pertanyaan pertama adalah 94% dengan penjelasan sebagai berikut:

- a. Sangat setuju memiliki nilai 5, setuju memiliki nilai 4.
- b. Skor tertinggi dalam penelitian ini adalah 125 dari 25 responden, angka 125 merupakan nilai batas tertinggi yang didapat jika seluruh responden memilih sangat setuju seluruhnya $25 \times 5 = 125$.

2. Fungsi Kriptografi

Berdasarkan pertanyaan yang diajukan kepada para responden, "Setujukah anda bahwa penerapan algoritma kriptografi dapat memudahkan anda untuk mengamankan data data pribadi milik anda?" Sebanyak 12 responden menjawab sangat setuju sekali, 7 responden menilai setuju, dan 6 responden menyatakan biasa. Nilai persentase kesuksesan hasil dari pertanyaan kedua adalah 84% dengan penjelasan sebagai berikut:

- a. Sangat setuju memiliki nilai 5, setuju memiliki nilai 4.
- b. Skor tertinggi dalam penelitian ini adalah 125 dari 25 responden, angka 125 merupakan nilai batas tertinggi yang didapat jika seluruh responden memilih sangat setuju seluruhnya $25 \times 5 = 125$.

3. Rekam Medis Elektronik

Berdasarkan pertanyaan yang diajukan kepada para responden mengenai pengetahuan mengenai Sistem Informasi Rekam Medis Elektronik. Sebanyak 9 orang responden menjawab sangat mengetahui, 7 orang responden menjawab mengetahui, 6 orang responden menjawab hanya pernah mendengar, 3 orang responden menjawab tidak mengetahui. Nilai kesuksesan dari persentase pertanyaan ketiga adalah 77% dan penjelasannya sebagai berikut:

- a. Sangat mengetahui memiliki nilai 5, mengetahui nilai 4, pernah mendengar memiliki nilai 3, dan tidak mengetahui memiliki nilai 2.
- b. Skor tertinggi dalam penelitian ini adalah 125 dari 25 responden, angka 125 merupakan nilai batas tertinggi yang didapat jika seluruh responden memilih sangat setuju seluruhnya $25 \times 5 = 125$.

4. User Experience

Berdasarkan pertanyaan keempat yang diajukan kepada para responden mengenai bagaimana tanggapan para responden ketika pertama kali menggunakan sistem yang dibangun. Sebanyak 10 orang responden menjawab bahwa sistem sangat nyaman digunakan, 8 orang responden menjawab bahwa sistem nyaman digunakan, dan 7 orang responden menjawab bahwa sistem biasa saja. Nilai persentase kesuksesan hasil dari pertanyaan ke

empat ini adalah 82% dengan penjelasan sebagai berikut:

- a. Sangat setuju memiliki nilai 5, setuju memiliki nilai 4, dan biasa memiliki nilai 3
- b. Skor tertinggi dalam penelitian ini adalah 125 dari 25 responden, angka 125 merupakan nilai batas tertinggi yang didapat jika seluruh responden memilih sangat setuju seluruhnya $25 \times 5 = 125$.

5. User Friendly

Berdasarkan pertanyaan yang diajukan kepada para responden, "Apakah anda masih menemukan kesulitan dalam pengoperasian sistem ini?" Sebanyak 13 responden menjawab sangat mudah digunakan, 7 responden menjawab mudah digunakan, dan 5 responden menyatakan biasa. Nilai persentase kesuksesan hasil dari pertanyaan kelima adalah 86 % dengan penjelasan sebagai berikut:

- a. Sangat setuju memiliki nilai 5, setuju memiliki nilai 4, dan biasa memiliki nilai 3.
- b. Skor tertinggi dalam penelitian ini adalah 125 dari 25 responden, angka 125 merupakan nilai batas tertinggi yang didapat jika seluruh responden memilih sangat setuju seluruhnya $25 \times 5 = 125$.

6. Fungsional

Berdasarkan pertanyaan yang diajukan kepada para responden, "Apakah ketika saat pengujian, seluruh tombol berfungsi sebagaimana seharusnya?" Sebanyak 15 responden menjawab berfungsi sangat baik, 6 responden menilai berfungsi baik dan 4 menjawab biasa. Nilai persentase kesuksesan hasil dari pertanyaan kelima adalah 88% dengan penjelasan sebagai berikut:

Berdasarkan pertanyaan yang diajukan kepada para responden, Apakah ketika saat pengujian, seluruh tombol berfungsi sebagaimana seharusnya? Sebanyak 15 responden menjawab berfungsi sangat baik, 6 responden menilai berfungsi baik dan 4 menjawab biasa. Nilai persentase kesuksesan hasil dari pertanyaan kelima adalah 88% dengan penjelasan sebagai berikut:

- a. Sangat setuju memiliki nilai 5, setuju memiliki nilai 4, dan biasa memiliki nilai 3.
- b. Skor tertinggi dalam penelitian ini adalah 125 dari 25 responden, angka 125 merupakan nilai batas tertinggi yang didapat jika seluruh responden memilih sangat setuju seluruhnya $25 \times 5 = 125$.

V. KESIMPULAN DAN SARAN

Berdasarkan hasil dari percobaan yang dilakukan maka dapat disimpulkan bahwa sistem aman dan mampu mencegah serangan SQL Injection dapat dilihat pada Tabel 1. Hasil percobaan dari 35 kali serangan selalu gagal login. Berdasarkan hasil scan pada Gambar 9 menggunakan alat bantuan

perangkat lunak *Acunetix Web Vulnerability Scanner versi 6* mengenai celah dan kelemahan dari sistem. Sistem dinyatakan kuat dan tidak terdeteksi adanya celah ataupun kelemahan. Telah dibuat Sistem Informasi Rekam Medis Elektronik yang telah menerapkan fungsi enkripsi pada string *password* menggunakan *Security Hash Algorithm-1*. Hasil pengujian didapatkan rata-rata 86%, yang berarti pemanfaatan *security* dengan *Security Hash Algorithm-1*.

Saran untuk perbaikan dan pengembangan penelitian selanjutnya adalah antara lain: melakukan penambahan kombinasi algoritma lain agar proses dekripsi melalui *website generator* dapat diminimalisir. Menambahkan fitur keamanan penunjang untuk membangkitkan kode OTP. Menerapkan Sistem Informasi Rekam Medis Elektronik pada sistem operasi lain seperti *iOS*, *Windows Phone*, *Android (Mobile)*.

REFERENSI

- [1] R. Silalahi and E. J. Sinaga, "Perencanaan Implementasi Rekam Medis Elektronik Dalam Pengelolaan Unit Rekam Medis Klinik Pratama Romana," *J. Manaj. Inf. Kesehat. Indones.*, vol. 7, no. 1, p. 22, 2019.
- [2] S. Lika, R. Dwi, P. Halim, and I. Verdian, "ANALISA SERANGAN SQL INJEKSI MENGGUNAKAN SQLMAP Implementation," *J. Sist. dan Teknol. Inf.*, vol. 4, no. 2, pp. 88–94, 2018.
- [3] R. Dwi., "Identifikasi ketidaklengkapan rekam medis pasien rawat inap Rumah Sakit Muhammadiyah Lamongan.," *J. Adm. Kesehat. Indones.*, vol. 1:2, pp. 192–199, 2013.
- [4] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016.
- [5] K. Aryasa and Y. T. Paulus, "Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Dalam Library Pada Pemrograman Java," *Creat. Inf. Technol. J.*, vol. 1, no. 1, p. 57, 2015.
- [6] M. S. Ramadhan, P. F. Ariyani, T. Informatika, F. T. Informasi, and U. B. Luhur, "PENINGKATAN KEAMANAN LOGIN WEBSITE DENGAN IMPLEMENTASI ONE TIME PASSWORD MENGGUNAKAN ALGORITMA SHA1 DAN MD5 BERBASIS MOBILE," vol. 1, no. 2, pp. 689–696.
- [7] S. Maesaroh, D. R. Ramlan, and Arsul, "Rancang Bangun Sistem Informasi Kepegawaian (Simpeg) Dengan Sdlc Metode Waterfall Studi Kasus Di Kantor Bkpld Kabupaten Tasikmalaya," *Tedc*, vol. 11, no. 2, pp. 197–202, 2017.
- [8] M. S. Mustaqbal, R. F. Firdaus, and H. Rahmadi, "PENGUJIAN APLIKASI MENGGUNAKAN BLACK BOX TESTING BOUNDARY VALUE ANALYSIS (Studi Kasus : Aplikasi Prediksi Kelulusan SNMPTN)," vol. I, no. 3, pp. 31–36, 2015.
- [9] S. Syofian, T. Setyaningsih, and N. Syamsiah, "Otomatisasi metode penelitian skala likert berbasis web," *Tinf-023*, no. November, pp. 1–8, 2015.