Penguatan Keamanan Sistem informasi Manajemen Tingkat Desa dengan Menerapkan One Time Password (OTP) dan AES-256

by Agus Hermanto, Isul Alifajri

Submission date: 06-Jul-2022 08:11AM (UTC+0700)
Submission ID: 1867089389
File name: Teknik_1461700113_Isul_Alifajri.pdf (809.47K)
Word count: 2890
Character count: 17190

Penguatan Keamanan Sistem informasi Manajemen Tingkat Desa dengan Menerapkan One Time Password (OTP) dan AES-256

Agus Hermanto[1], Isul Alifajri[2]

[1,2] Teknik Informatika, Universitas 17 Agustus 1945 Surabaya, Indonesia

[1]hermanto_if@untag-sby.ac.id

[2]isulalifajri@gmail.com

Abstrak*— Sistem informasi manajemen desa merupakan sebuah sistem informasi yang dapat membantu sebagian besar kegiatan administrasi di kantor desa. Dengan adanya sistem informasi manajemen tersebut akses data lebih fleksibel dan mudah di lakukan, akan tetapi adanya masalah keamanan untuk melindungi hak akses penggunanya dari pihak yang tidak memiliki otoritas menjadi salah satu masalah dalam sistem ini. Karena itu, untuk mengurangi terjadinya penggunaan sistem oleh pihak yang tidak memiliki izin, maka perlu di terapkan metode one time password dalam sistem ini, selain itu, untuk mengamankan data-data penting dalam database sistem ini di gunakan algoritma AES-256 untuk metode enkripsinya. Dalam sistem ini menggunakan bahasa pemrograman PHP dan MySQL sebagai penyimpanan databasenya. Dengan adanya metode one time password dan enkripsi AES-256 di harapkan dapat lebih meningkatkan keamanan pada system informasi manajemen ini.

***Kata kunci*: Sistem Informasi Manajemen, OTP, AES-256, PHP, MySQL.**

Abstract*— The village management information system is an information system that can assist most administrative activities in the village office. With this management information system, data access is more flexible and easier to do, but there are security issues to protect user access rights from unauthorized parties. Therefore, to reduce the use of the system by unauthorized parties, it is necessary to apply the one time password method in this system, in addition, to secure important data in the system database, the AES-256 algorithm is used for the encryption method. In this system using the programming language PHP and MySQL as database storage. With the one time password method and AES-256 encryption, it is expected to further improve the security of this management information system.

Keywords: Management Information System, OTP, AES-256, PHP, MySQL.

I. PENDAHULUAN

Sistem Informasi Manajemen merupakan suatu sistem yang di bangun untuk menyediakan informasi mendukung pengambilan keputusan pada kegiatan manajemen dalam suatu organisasi[1]. Sistem Informasi Manajemen Desa di butuhkan untuk mempermudah perangkat desa dalam proses pendataan dan pelayanan pada penduduk desa, Dengan adanya sistem informasi manajemen desa ini proses akses data lebih efisien dan fleksibel dan juga dapat mengurangi terjadinya kesalahan data.

Di satu sisi sistem informasi menguntungkan dan dapat meningkatkan kinerja dari semua komponen organisasi, tetapi dari sisi yang lain terutama dari sisi keamanan sistem informasi yang berbasis web sangat rentan untuk di sadap oleh pihak yang tidak memiliki otoritas. Banyak cara yang sering di gunakan oleh *cracker* untuk mengetahui username dan password dari sebuah akun. Akun yang di maksud di sini dapat berupa akun apa saja, seperti akun google, facebook dan lain sebagainya[2]. Salah satu cara yang di gunakan *cracker* untuk mengetahui informasi akun seseorang adalah *Spoofing*. *Spoofing* adalah suatu teknik pencurian data dengan cara memanipulasi informasi berupa organisasi, nama atau alamat hingga target yang di tuju percaya. *Spoofing* ini biasanya berisi link ataupun malware yang di kirimkan ke target. Media yang di gunakan untuk melakukan penipuan dengan metode *spoofing* biasanya berupa email palsu, website dan juga alamat IP[3]-[2].

Proses aktivasi merupakan bagian dari sintem ini untuk melakukan autentikasi terhadap pengguna. Proses aktivasi yang hanya menggunakan nik saat melakukan aktivasi ke dalam sebuah sistem. Hal tersebut masih kurang aman untuk melindungi pengguna dari pihak yang tidak bertanggung jawab. Oleh karena itu, untuk membatasi terjadinya penggunaan sistem oleh pihak yang tidak memiliki hak atau izin perlu di gunakan metode *one time password* pada saat aktivasi pengguna. *One time password* adalah sebuah password yang hanya berlaku untuk sesi login tunggal atau transaksi tunggal[4]. Sedangkan untuk pengamanan datanya dalam database akan di lakukan enkripsi dengan metode *AES-256*.

Dengan metode di atas, diharapkan dapat meningkatkan aspek keamanan pada system informasi manajemen desa dan tidak akan ada kerusakan data atau manipulasi data pada data yang ada dalam system tersebut, sehingga kemanan sistem informasi manajemen desa bisa lebih terjamin[5].

Berikut ini beberapa jurnal terdahulu terkait dengan penelitian yang di lakukan penulis:

Imam, dkk dalam dalam penelititannya tentang studi pengamanan login pada sistem informasi akademik menggunakan *one time password* dan algoritma *MD5*[2]. Menunjukkan bahwa bebrapa keuntungan yang du peroleh dengan metode yang di gunakan antara lain, OTP dengan

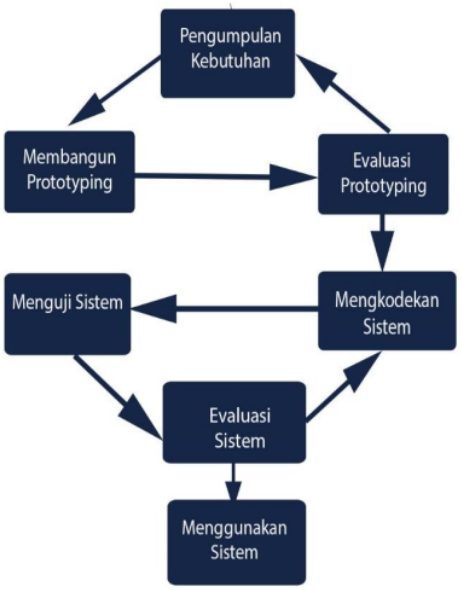
hash *MD5* memiliki hasil yang tidak mungkin sama sehingga sulit di tebak oleh *cracker*, apalagi yang menjadi masukan untuk menghasilkan OTP berasal dari nim, no telepon, dan waktu pada akses yang ketiganya adalah unik.

Agus, dkk melakukan penelitian tentang Pembuatan sistem informasi keuangan dengan model *asynchronous* untuk penguatan aspek keamanan informasi.[5] Hasil penelitian menunjukkan replikasi data asynchronous dalam sistem informasi dapat meningkatkan keamanan dan mengurangi kerentanan yang umumnya dimiliki oleh sistem informasi online. Enkripsi *AES 256* dapat digunakan sebagai keamanan tambahan untuk mencegah kebocoran informasi.

Penelitian ini bertujuan untuk merancang, membuat dan mengimplementasikan penguatan keamanan pada sistem informasi manajemen tingkat desa dengan menerapkan *One Time Password* (OTP) dan *AES-256*. Selain itu manfaat dari penelitian ini di harapkan dapat Mengurangi terjadinya penggunaan sistem oleh pihak yang tidak memiliki hak/izin, membantu mencegah terjadinya peretasan melalui data saat melakukan aktivasi oleh pihak yang tidak berkepentingan dan dapat membantu meningkatkan keamanan sistem.

II. METODOLOGI PENELITIAN

Dalam penelitian ini tahapan pembuatan sistem informasi manajemen desa menggunakan metode prototype. Ada beberapa tahapan yang di gunakan dalam metode prototype ini di antaranya: Pengumpulan Kebutuhan, Membangun Prototype, Evaluasi Prototype, Mengkodekan sistem, Menguji sistem, Evaluasi sistem dan Menggunakan sistem.



Gambar 1. Model Prototype

Berikut ini adalah deskripsi dari tahapan model prototyping:

1. *Pengumpulan Kebutuhan*

Pada tahap ini, penulis mengumpulkan data yang di butuhkan dari elemen sistem yang akan di terapkan ke dalam bentuk web. Dimana penulis mengumpulkan data mengenai sistem informasi manajemen, *one time password* dan algoritma *AES-256*.

2. *Membangun Prototyping*

Pada tahap ini, penulis membuat perancangan sementara yang nantinya akan di sajikan. Misalnya dengan membuat perancangan form login, form pendaftaran, form otp dan yang lainnya.

3. *Evaluasi Prototyping*

Evaluasi ini di lakukan oleh penulis apakah prototyping yang sudah di bangun sudah sesuai dengan yang di harapkan. Jika sudah sesuai maka langkah 4 yang akan di ambil. Jika tidak, maka prototyping di revisi dengan mengulang langkah 1 dan 2.

4. *Mengkodekan Sistem*

Dalam tahap ini, prototyping yang sudah di sepakati, akan di terjemahkan ke dalam bahasa pemrograman yang di gunakan. Dimana bahasa pemrograman yang di gunakan penulis dalam penelitian ini, yaitu bahasa pemrograman PHP, CSS dan Javascript.

5. *Menguji sistem*

Setelah sistem sudah siap di jalankan, kemudian di lakukan proses pengujian. Pengujian ini di lakukan dalam hal fungsionalitas dan keamanan sistem informasi.

6. *Evaluasi sistem*

Pada tahap ini, penulis mengevaluasi apakah sistem yang sudah selesai sudah sesuai dengan yang di inginkan. Jika sudah sesuai, maka proses di lanjutkan ke tahap selanjutnya. Jika tidak, maka tahap sebelumnya di ulang kembali.

7. *Menggunakan sistem*

Sistem yang telah di uji dan di terima siap untuk gunakan.

III. HASIL DAN PEMBAHASAN

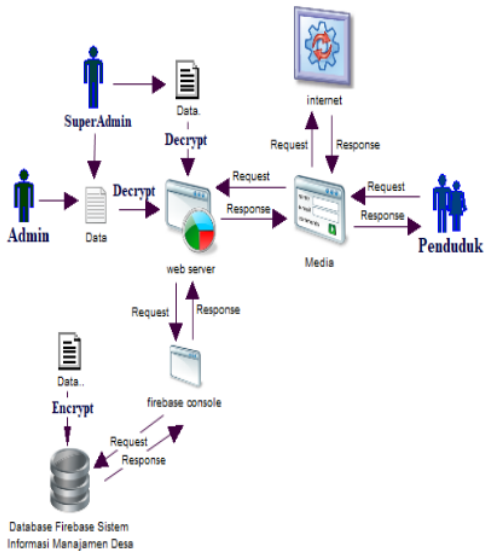
Berikut ini merupakan hasil dan pembahasan dari penelitian ini :

1. *Arsitektur Aplikasi*

Rancangan Arstektur aplikasi yang telah di buat dalam penelitan ini adalah sebagai berikut:

- Penduduk yang menggunakan sistem informasi ini dengan media yang ada seperti handphone, laptop, komputer harus terhubung ke internet untuk mengakses sistem informasi.

- Data-data penting yang ada di sistem nanti akan tersimpan di dalam database dalam bentuk enkripsi, kemudian akan di tampilkan kembali ke dalam sistem dalam bentuk dekripsi.
- Data-data yang ada di dalam sistem nantinya akan di kelola oleh admin dan superadmin.



Gambar 2. Arsitektur Aplikasi

2. *Tampilan Sistem*

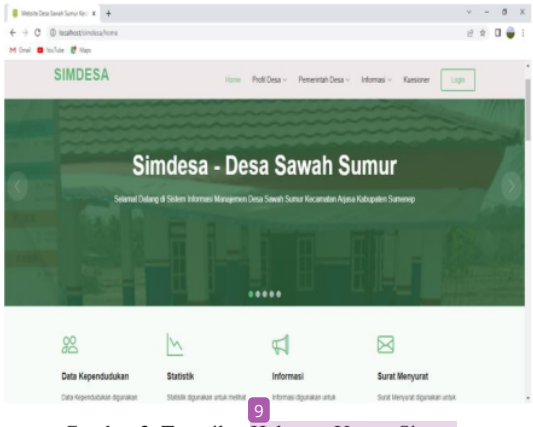
Disini akan di jelaskan beberapa tampilan dari berbagai proses yang terjadi di dalam sistem informasi manajemen desa, terutama proses *one time password* dan enkripsi AES-256 yang di terapkan dalam sistem ini. Berikut merupakan tampilan-tampilan yang telah di buat dalam sistem ini:

A. Tampilan Halaman Utama Sistem

Pada halaman utama ini sistem akan menampilkan beberapa tampilan menu dan informasi-informasi mengenai desa. Menu-menu yang di tampilkan pada halaman ini yaitu:

- Menu Profil Desa yang terdiri dari submenu profil wilayah desa dan sejarah desa. Pada submenu profil wilayah menjelaskan tentang letak wilayah, kondisi geografis, kondisi demografi dan ekonomi dan kondisi sarana dan prasarana desa.
- Menu Pemerintah desa yang terdiri dari submenu visi dan misi, pemerintah desa, dan badan permusyawaratan desa.
- Menu Informasi yang terdiri dari submenu agenda, pengumuman, dan berita desa.
- Menu Kuesioner di gunakan untuk mengumpulkan informasi dari user yang menggunakan sistem ini mengenai sistem yang telah di jalankan.
- Menu Login di gunakan untuk masuk ke dalam sistem informasi.

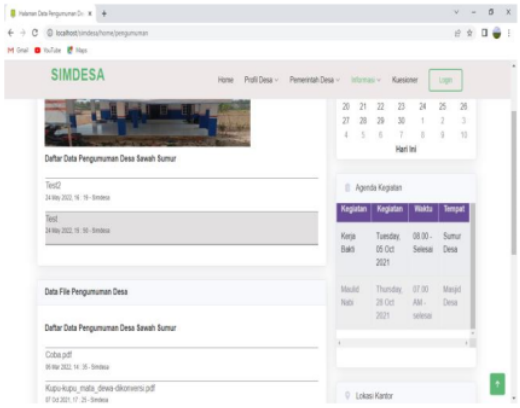
Selain itu pada halaman utama ini juga menjelaskan fitur-fitur apa saja yang di sediakan dalam sistem informasi manajemen ini.



Gambar 3. Tampilan Halaman Utama Sistem

B. Tampilan Halaman Pengumuman

Pada halaman ini, sistem akan menampilkan beberapa data pengumuman mengenai desa. Data pengumuman yang di tampilkan pada halaman ini berupa teks dan file pdf. Selain itu, pada halaman ini juga menampilkan informasi tambahan lainnya, seperti menampilkan kalender, agenda kegiatan dan lokasi peta kantor desa.

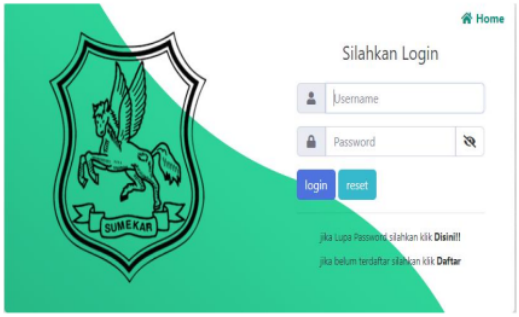


Gambar 4. Tampilan Halaman Pengumuman

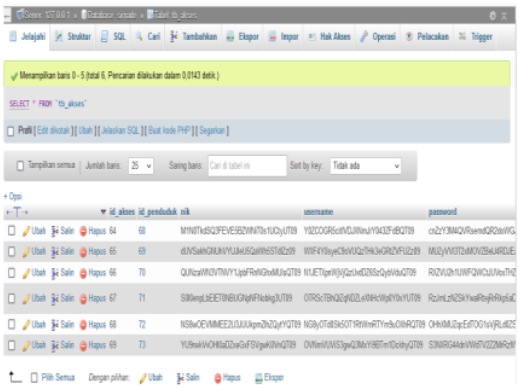
C. Tampilan Halaman Login

Pada halaman ini terdapat dua form inputan dan button untuk login. Inputan tersebut terdiri dari username dan password. Sedangkan button nya terdiri dari login dan reset. Pada halaman ini user yang ingin masuk ke dalam sistem di minta untuk memasukkan username dan

password pada form yang telah di sediakan. Setelah itu sistem akan memverifikasi apakah username dan password yang di masukkan sesuai dengan yang ada di dalam tabel login pada database sistem. Jika tidak sesuai, maka sistem akan menampilkan pesan kesalahan. Jika sesuai, maka sistem akan mengarahkan pengguna ke dalama halaman sistem informasi manajemen desa berdasarkan level masing-masing pengguna. Data-data untuk login sudah dalam bentuk enkripsi dalam database, seperti yang di tunjukkan pada Gambar 6. Tampilan untuk halaman login dapat di lihat pada Gambar 5.



Gambar 5. Tampilan Halaman Login

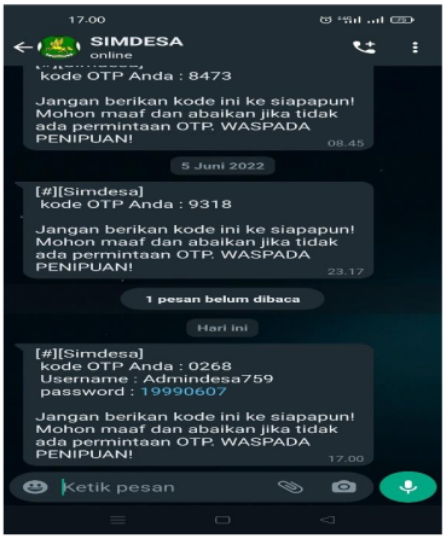


Gambar 6. Tampilan Data Login dalam Bentuk Enkripsi dalam Database

D. Tampilan Halaman Pendaftaran

Halaman ini di gunakan untuk tahap aktivasi pengguna yang sebelumnya sudah di masukkan oleh superadmin ke dalam database sistem tapi statusnya masih belum aktif. Pada halaman ini terdapat satu form inputan dan button untuk aktivasi pengguna. Pengguna di minta untuk memasukkan nik untuk proses aktivasinya. Setelah memasukkan nik, sistem akan memverifikasi apakah nik yang di masukkan sesuai dan ada dalam database. Jika tidak sesuai maka sistem akan menampilkan pesan kesalahan. Jika sesuai maka sistem akan mengarahkan ke halaman verifikasi otp untuk verifikasi kode otp yang telah di kirimkan secara otomatis oleh sistem melalui pesan WhatsApp ke nomor telepon yang sesuai dengan nik yang telah di masukkan. Selain kode otp sistem juga mengirimkan username dan password untuk di gunakan pengguna saat ingin masuk ke dalam sistem. Pesan yang di kirimkan pada pengguna dapat di lihat pada Gambar 8. Tampilan pada halaman pendaftaran di tunjukkan pada Gambar 7.

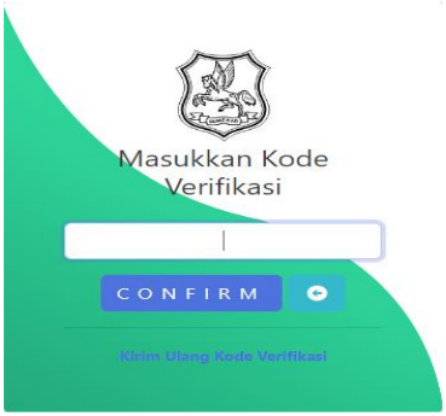
Gambar 7. Tampilan Halaman Pendaftaran



Gambar 8. Tampilan Pesan WhatsApp Kode OTP

E. Tampilan Halaman Verifikasi Kode OTP

Pada halaman ini user diminta untuk memasukkan kode otp yang telah di kirimkan melalui pesan whatsapp seperti pada Gambar 8. Setelah itu, sistem akan memverifikasi apakah kode otp yang di masukkan sesuai dengan yang ada di dalam database. Jika tidak sesuai, sistem akan menampilkan pesan kesalahan. Jika sesuai maka sistem akan menampilkan pesan bahwa proses aktivasi telah sukses di lakukan dan akan mengarahkan ke halaman login. Selain itu, jika user tidak mendapatkan pesan kode otp, user bisa mengklik menu untuk kirim ulang kode verifikasi yang ada pada halaman kode otp. Tampilan Halaman Verifikasi kode OTP dapat di lihat pada Gambar 9.

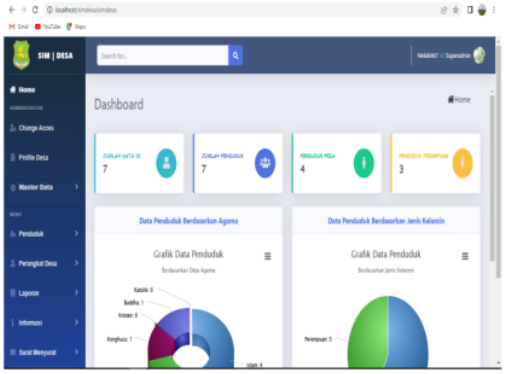


Gambar 9. Tampilan Halaman Verifikasi Kode OTP

F. Tampilan Halaman Dashboard Superadmin

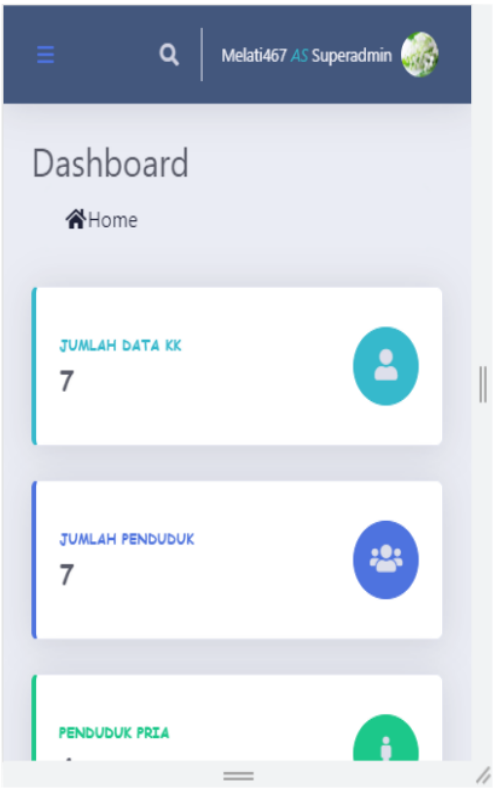
Pada halaman ini menampilkan beberapa tampilan menu dan informasi-informasi mengenai penduduk desa dalam bentuk grafik, menu-menu yang di tampilkan antara lain:

- Menu Master Data di gunakan untuk mengelola data master dalam sistem informasi ini.
- Menu Profil Desa di gunakan untuk mengisi data profile desa untuk di tampilkan pada halaman utama sistem informasi.
- Menu Penduduk di gunakan untuk mengelola data penduduk desa.
- Menu Perangkat Desa, untuk mengisi data perangkat desa.
- Menu Laporan, untuk membuat laporan mengenai desa, baik itu mengenai laporan penduduk atau pembangunan desa.
- Menu Informasi, di gunakan untuk mengisi informasi-informasi yang akan di tampilkan pada menu utama sistem, seperti informasi pengumuman dan berita desa.
- Menu Surat Menyurat, di gunakan untuk membuat dan mencetak surat.
- Menu Manajemen Akses di gunakan untuk mengelola data akses user.
- Menu Manajemen Desa di gunakan untuk mengelola data manajemen desa.



Gambar 10. Tampilan Halaman Dashboard Superadmin

Tampilan sistem informasi manajemen desa ini juga sudah responsive dan mendukung tampilan mobile. Sehingga dapat memudahkan pengguna dalam menggunakan sistem ini.



Gambar 11. Tampilan Responsive Simdesa

3. Pengujian

Pengujian yang di gunakan dalam penelitian ini meliputi pengujian pada aspek kualitas apakah sistem berjalan sesuai dengan yang di harapkan. Pengujian pada aspek keamanan untuk memastikan bahwa sistem yang di jalankan aman untuk di gunakan.

A. Pengujian Pada Aspek Kualitas

Pengujian pada aspek kualitas di lakukan dengan menguji fungsionalitas sistem. Pada pengujian fungsionalitas di gunakan metode *black box*. Hasil pengujian *black box* dapat di lihat pada Tabel 1.

Tabel 1. Pengujian Fungsionalitas dengan *black box*

Fitur	Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Data Berita	Mengklik salah satu berita yang di tampilkan pada halaman utama desa	Menampilkan data berita sesuai dengan yang pilih.	Data Berita berhasil di tampilkan sesuai dengan yang di pilih	[v] berhasil [] gagal
Profile Desa	Mengklik menu profile desa	Menampilkan halaman Profile desa	Data Profile desa berhasil di tampilkan	[v] berhasil [] gagal
Dashboard	Mengklik Grafik Data Penduduk	Menampilkan Data Penduduk Pada Grafik dengan Valid	Data tampil dengan benar pada grafik	[v] berhasil [] gagal
Data KK	Menginputkan Data KK	Data KK tersimpan dalam basis data	Data Kartu Keluarga berhasil tersimpan dalam basis data	[v] berhasil [] gagal
Data Penduduk	Menginputkan Data Penduduk	Data Penduduk tersimpan dalam basis data	Data Penduduk yang di inputkan berhasil tersimpan dalam basis data	[v] berhasil [] gagal
Data Informasi	Menginputkan Data Informasi	Data Informasi tersimpan dalam basis data	Data Informasi yang di inputkan tersimpan dalam basis data	[v] berhasil [] gagal
Data Gambar	Mengubah gambar dalam sistem	Menyimpan perubahan Data Gambar	Data Gambar berhasil di simpan	v] berhasil [] gagal
Data Perangkat	Menginputkan Data Perangkat	Data Perangkat tersimpan dalam basis data	Data Perangkat yang di inputkan tersimpan dalam basis data	[v] berhasil [] gagal
Data Surat	Menginputkan Data Surat	Data surat yang di inputkan tersimpan dalam basis data	Data surat yang di inputkan berhasil tersimpan dalam basis data	[v] berhasil [] gagal
User Profile	Mengubah data profile	Menyimpan perubahan data profile	Data Profile berhasil di simpan	[v] berhasil [] gagal
Manajemen Akses	Mengubah data manajemen akses	Menyimpan perubahan data manajemen akses	Data Manajemen Akses Berhasil di simpan	[v] berhasil [] gagal
Manajemen Desa	Mengklik Menu manajemen desa	Menampilkan data manajemen desa	Berhasil menampilkan data manajemen desa	[v] berhasil [] gagal
Log Aktivitas	Mengklik menu log aktivitas	Menampilkan data aktivitas user	Berhasil menampilkan data aktivitas yang di lakukan user	[v] berhasil [] gagal

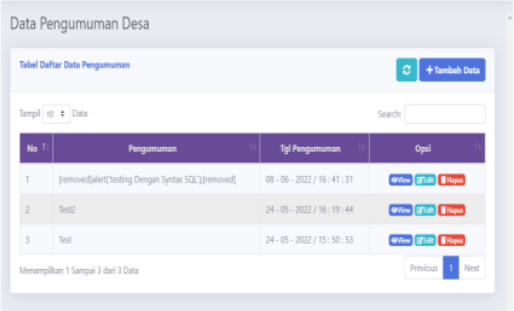
B. Pengujian Pada Aspek Keamanan

Pengujian pada aspek keamanan menggunakan metode SQL Injection dan Cross Site Scripting.

Pengujian SQL Injection di lakukan dengan memasukkan syntaq sql dalam form input pada halaman tambah pengumuman dalam sistem informasi manajemen desa. Pengujian ini menunjukkan hasil yang baik. Syntax

sql yang di inputkan langsung di hapus otomatis oleh sistem. Hasil Pengujian dapat di lihat pada Gambar 12, 13.

Gambar 12. Pengujian SQL Injection 1

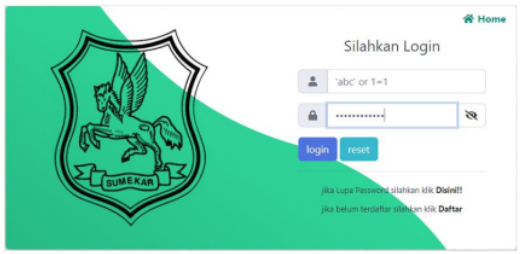


Gambar 13. Pengujian SQL Injection 2

Pengujian SQL Injection juga di lakukan dengan tools untuk melakukan pengujian. Pengujian di lakukan dengan cara menambahkan sintaks sql melalui url sistem informasi. Hasil dari pengujian ini menunjukkan tidak ada sintaks sql yang berhasil di jalankan. Pengujian dengan SQL Injection di tunjukkan pada Gambar 14.

Gambar 14. Pengujian SQL Injection dengan Tools

Pada pengujian Cross Siste Scripting menunjukkan keamanan pada sistem informasi tidak bisa di bobol. Script yang di masukkan di anggap salah dan proses berhasil di hentikan oleh sistem. Pengujian dengan Cross Site Scripting di tunjukkan pada Gambar 15, 16.



Gambar 15. Cross Site Scripting 1

Gambar 16. Cross Site Scripting 2

IV. KESIMPULAN

Berdasarkan penelitian yang telah di lakukan pada sistem informasi manajemen desa ini, di dapatkan beberapa kesimpulan sebagai berikut:

1. Keberadaan sistem informasi manajemen desa memudahkan masyarakat untuk mengetahui informasi-informasi mengenai desa.
2. Penerapan One Time Password dan Algoritma AES-256 dapat menambah keamanan proses aktivasi pada sistem informasi manajemen desa ini.
3. Algoritma AES-256 dapat mengamankan kode OTP yang telah di dapatkan untuk di kirim ke nomor telepon pengguna.
4. Hasil dari kode OTP hanya di kirim ke nomor telepon pengguna yang sesuai dengan nik yang di daftarkan melalui WhatsApp Gateway.
5. Penggunaan Algoritam AES-256 dapat membantu mengamankan data-data penting dalam database.

REFERENSI

[1] M. Dwiajie, "Pengertian Sistem Informasi Manajemen," 1996. http://file.upi.edu/browse.php?dir=Direktori/FIP/PRODI._PERPUSTAKAAN_DAN_INFORMASI/MIYARSO_DWI_AJIE/Makalah_a.n_Miyarso_Dwiajie/ (accessed Jan. 07, 2022).

[2] K. I. Santoso, E. Sediyono, and Suhartono, "Studi Pengamanan Login Pada Sistem Informasi Akademik Menggunakan Otentifikasi One Time Password Berbasisis SMS dengan Hash MD5," *J. Sist. Inf. Bisnis*, vol. 01(2013), 2013.

[3] J. Wang, *Computer Network Security*. Beijing, 2009.

[4] A. Prayogo and M. A. Rony, "Implementasi One Time Password pada Sistem Login dengan Algoritma SHA-256 dan DES pada Aplikasi EO Blucampus Berbasis Client Server," *SKANIKA*, vol. VOLUME 1 N, 2018.

[5] A. Hermanto, S. Hadijono, and N. Fadilah, "Pembuatan Sistem Informasi Keuangan Dengan Model Arsitektur Asynchronous Untuk Penguatan Aspek Keamanan Informasi," *Konf. Nas. Ilmu Komput.*, no. ISSN : 2338-2899, 2020.

Penguatan Keamanan Sistem informasi Manajemen Tingkat Desa dengan Menerapkan One Time Password (OTP) dan AES-256

ORIGINALITY REPORT

9%	9%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	stmikbinapatria.academia.edu Internet Source	3%
2	jom.fti.budiluhur.ac.id Internet Source	2%
3	www.semanticscholar.org Internet Source	1%
4	abhymujahidmuda.blogspot.com Internet Source	1%
5	anzdoc.com Internet Source	1%
6	docplayer.info Internet Source	1%
7	Submitted to UIN Sunan Ampel Surabaya Student Paper	<1%
8	repository.uinsu.ac.id Internet Source	<1%
	adoc.pub	

9	Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		