PENGEMBANGAN KEAMANAN SISTEM INFORMASI SST (*SELF SERVICE TERMINAL*) STMIK PRADNYA PARAMITA MALANG

Dinny Wahyu Widarti [1)], Samsul Arifin [2)]
[1] Manajemen Informatika, STMIK PPKIA Pradnya Paramita
email: dinnywidarti@gmail.com
[2] Teknik Informatika, STMIK PPKIA Pradnya Paramita
email: mas.arif73@gmail.com

Abstract

Information System Security is essential to ensure the proper functioning of the information system. Weak information system security may result that other people who do not have the right can be entered into the system information without passed the security and perform activities that can damage or destroy data on the information system, even can destroy that information system itself. On one side, security of the information system needs to be improved, like in login process to get into the information system. Login process becames a tool to pave the ways for someone to infiltrate into the information system. There are several ways to do so that login process to be secure, such as anti SQL Injection and Verification login with SMS Gateway. Expected by using the login process with anti SQL Injection and Verification login with SMS Gateway can reduce the occurrence of fraud against Information Systems in STMIK PPKIA Pradnya Paramita Malang.

Keywords: *Security, Information Systems, and SMS Gateway*

1. PENDAHULUAN

Setiap organisasi/lembaga manapun pasti mempunyai Sistem Informasi yang mengelola data secara internal. Begitu juga pada lembaga STMIK PPKIA Pradnya Paramita. Sistem Informasi yang ada di STMIK PPKIA Pradnya Paramita meliputi data Mahasiswa, Dosen, Perkuliahan, dan administrasi lainnya yang terkait dengan kampus. Pengguna sistem informasi di STMIK PPKIA Pradnya Paramita ini terdiri dari berbagai golongan, yaitu Pegawai, Dosen, dan Mahasiswa yang semuanya itu memiliki hak yang berbeda satu dengan lainnya. Diharapkan Sistem informasi dapat digunakan sebagaimana mestinya, namun bisa saja orang lain yang tidak mempunyai hak dapat masuk dengan sengaja ke dalam sistem informasi dan melakukan aktifitas yang merugikan bahkan merusak sistem informasi tersebut. Untuk menangani masalah tersebut perlu adanya sistem keamanan khusunya pada proses Login.

Proses login menjadi salah satu celah bagi seseorang yang tidak berhak dapat menyusup ke dalam sistem informasi, dan melakukan aktifitas yang merugikan atau merusak sistem informasi. Untuk itu keamanan proses login perlu ditingkatkan lagi, yaitu dengan anti SQL Injection dan Verifikasi login dengan SMS Gateway. Diharapkan dengan menggunakan proses login dengan anti SQL Injection dan Verifikasi login dengan SMS Gateway dapat mengurangi terjadinya kecurangan terhadap Sistem Informasi di STMIK PPKIA Pradnya Paramita Malang.

Rumusan Masalah yang akan dibahas pada penelitian ini adalah "Bagaimana mengembangkan keamanan sistem informasi pada proses login dengan SQL Injection dan Verifikasi login menggunakan SMS Gateway pada STMIK PPKIA Pradnya Paramita

Malang?"

Dalam penelitian ini, penulis membatasi permasalahan pada pengembangan keamanan sistem informasi pada proses login dengan SQL Injection dan Verifikasi login menggunakan SMS Gateway.

Tujuan dari penelitian ini diharapkan Sistem Informasi di STMIK PPKIA Pradnya Paramita Malang menggunakan proses login dengan anti SQL Injection dan Verifikasi login dengan SMS Gateway dapat mengurangi terjadinya kecurangan data.

Tujuan dari penelitian ini adalah terwujudnya pengembangan keamanansistem informasi di STMIK PPKIA Pradnya Paramita Malang menggunakan proses login dengan anti SQL Injection dan Verifikasi login melalui SMS Gateway dapat mengurangi terjadinya kecurangan data.

Adapun manfaat dari penelitian pengembangan keamanan sistem informasi di STMIK PPKIA Pradnya Paramita Malang yang dilaksanakan ini adalah:

1. Mengurangi terjadinya kecurangan data.
2. Menghindari penelusup.
3. Memberi kenyamanan pengguna akan keamanan datanya.

Penelitian pengembangan keamanan proses login anti SQL Injection dan Verifikasi login dengan SMS Gateway dengan yang akan dilaksanakan ini diharapkan dapat membantu meningkatkan sistem keamanan pada Sistem Informasi di STMIK PPKIA Pradnya Paramita Malang dan memberikan luaran berupa publikasi ilmiah padaJurnal Nasional.

2. KAJIAN LITERATUR

A. Sistem Informasi

Sistem Informasi berasal dari kata Sistem dan Informasi. Menurut Mc Leod dalam buku Yakub (2012) sistem adalah sekelompok elemen-elemen yang terintegrasi dengan tujuan yang sama untuk mencapai tujuan. Sedangkan Informasi adalah data yang diolah menjadi bentuk lebih berguna dan lebih berarti bagi yang menerimanya.

Menurut Abdul Kadir (2014) Sesungguhnya yang dimaksud dengan sistem informasi tidak harus melibatkan computer. Sistem informasi yang menggunakan computer biasa disebut sistem informasi berbasis computer (*Computer-Based Information System* atau CBIS).

Menurut O'Brian dalam buku Yakub (2012) sistem informasi merupakan kombinasi teratur dari orang-orang, perangkat keras, perangkat lunak, jaringan komunikasi, dan sumber daya data yang mengumpulkan, mengubah, dan menyebarkan informasi dalam sebuah organisasi.

Menurut Rudy Tantra (2012) sistem adalah entitas atau satuan yang terdiri dari dua atau lebih komponen atau subsistem (sistem yang lebih kecil) yang saling berhubungan dan terkait untuk mencapai suatu tujuan. Sedang informasi dapat dipahami sebagai pemrosesan input yang terorganisir, memiliki arti, dan berguna bagi orang yang menerimanya. Jadi sistem informasi adalah cara yang terorganisir untuk mengumpulkan, memasukkan, dan memproses data dan menyimpannya, mengelola, mengontrol dan melaporkannya sehingga dapat mendukung perusahaan atau organisasi untuk mencapai tujuan.

Sehingga dapat disimpulkan bahwa sistem adalah kumpulan elemen-elemen yang saling terkait untuk mencapai suatu tujuan, dan informasi adalah data yang sudah diolah sehingga berarti bagi penerimanya. Sedangkan sistem informasi merupakan kumpulan elemen-elemen yang saling terkait dan bertujuan untuk mengolah data menjadi informasi.

B. Keamanan

Keamanan merupakan faktor

yang perlu diperhatikan dalam membangun sistem informasi, agar sistem informasi dapat terhindar dari ancaman akibat kerusakan sistem.

Menurut Abdul Kadir (2014), ancaman terhadap sistem informasi dapat dibagi menjadi dua macam, yaitu ancaman aktif dan ancaman pasif. Ancaman aktif mencakup kecurangan dan kejahatan terhadap komputer, sedangkan ancaman pasif mencakup kegagalan sistem, kesalahan manusia, dan bencana alam.

Keamanan yang dimaksud disini termasuk keamanan yang bertujuan untuk mencegah ancaman aktif, yaitu keamanan data dalam suatu sistem informasi tertentu dari orang lain yang hendak merusak data dan sistem didalamnya.

Menurut Dony Arius (2006) aspek-aspek ancaman keamanan antara lain:

1. *Interruption*
   Merupakan suatu ancaman terhadap *availability*. Informasi dan data yang ada dalam sistem computer dirusak dan dihapus sehingga jika dibutuhkan, data atau informasi tersebut tidak ada lagi.
2. *Interception*
   Merupakan ancaman terhadap kerahasiaan (*secrecy*). Informasi yang ada disadap atau orang yang tidak berhak mendapatkan akses ke komputer dimana informasi tersebut disimpan.
3. Modifikasi
   Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan diubah sesuai keinginan orang tersebut.
4. *Fabrication*
   Merupakan ancaman terhadap integritas.Orang yang tidak berhak berhasil meniru (memalsukan) sistem informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.

Menurut IBISA (2013) setiap komponen di dalam sistem informasi berbasis komputer memiliki keamanan sendiri-sendiri. Dalam sistem komputer memiliki empat parameter keamanan yang sangat penting:

1. *Physical Security* (yang merupakan lapisan luar).
2. *System Security.*
3. *Application Security.*
4. *Data Security* (yang merupakan lapisan dalam dan terpenting)

Fungsi keamanan pada suatu sistem informasi sangatlah penting agar sistem informasi dapat digunakan sebagaimana mestinya.

Salah satu bentuk keamanan sistem adalah dengan memberikan login dan password sesuai dengan hak masing-masing user.

C. SST (*Self Service Terminal*)

SST (*Self Service Terminal*) adalah suatu sistem informasi berbasis web yang digunakan di lingkungan STMIK PPKIA Pradnya Paramita Malang.

Semua aktifitas didalam SST tersebut dapat dilakukan sendiri secara mandiri oleh mahasiswa aktif maupun dosen (khususnya Dosen Pembina Akademik) STMIK PPKIA Pradnya Paramita Malang.

Tujuan SST digunakan untuk melakukan berbagai aktifitas seperti mengisi dan menyetujui KRS (Kartu Rencana Studi), melihat KHS (Kartu Hasil Studi), memperbarui biodata mahasiswa, melihat jadwal kuliah,dan lain-lain.

SST dapat digunakansecara online, yaitu digunakandimanapun beradadan kapanpun.

D. Proses Login

Proses login merupakan salah

satu usaha untuk memberikan keamanan pada data dalam suatu sistem. Bentuk proses login adalah sebuah halaman web yang berisi dua masukan yaitu user dan pasword, serta satu tombol proses.

Proses login pada SST di STMIK PPKIA Pradnya Paramita terbagi menjadi dua login, yaitu login untuk mahasiswa dan dosen. Untuk login mahasiswa menggunakan user NIM (Nomor Induk Mahasiswa) dan pasword berupa pin yang disediakan sistem secara acak.

Sedangkan untuk Dosen menggunakan user NIK (Nomor Induk Karyawan) dan password berupa NIDN (Nomor Induk Dosen Nasional). Dua masukan tersebut akan diproses dengan membandingkan data di database, bila nim/nik dan password cocok, maka akan dapat masuk ke sistem SST, bila tidak cocok maka akan tertolak.

E. SMS Gateway

SMS Gateway merupakan pintu gerbang bagi penyebaran informasi yang menggunakan sms (Tarigan:2013). Penyebaran yang dimaksud disini adalah penyebaran pesan ke banyak nomor secara otomatis dan cepat yang langsung terhubung dengan database tanpa harus mengetik nomor dan isi pesan berulang kali.

F. SQL Injection

SQL Injection adalah sebuah metode untuk memasukkan perintah SQL sebagai input melalui sebuah web untuk mendapatkan akses database (Efvy Zam:2015).

Proses login saat ini, mudah disusupi dengan metode SQL Injection. Sehingga orang lain dapat login dan masuk ke sistem SST di STMIK PPKIA Pradnya Paramita.

Untuk mengatasi SQL Injection ini, maka kode pemrograman harus diubah agar bisa mecegah aksi SQL Injection.

3. METODE PENELITIAN

Pada sistem informasi SST yang sedang digunakan di STMIK PPKIA saat ini menggunakan proses login untuk dapat masuk dan mengolah sistem informasinya. Proses login yang berjalan saat ini, masih menggunakan kode pemrograman sederhana, sehingga mudah disusupi dengan metode SQL Injection. Selain itu, nim/nik dan password dapat dengan mudah diterka oleh orang lain, sehingga orang lain dapat login dan masuk ke sistem SST.

Penyebab terjadinya serangan SQL Injection adalah tidak adanya penanganan terhadap karakter-karakter tertentu. Terutama pada petik satu (‘) dan juga karakter double minus (--) yang menyebabkan suatu aplikasi dapat disisipi dengan perintah SQL.

Untuk mengatasi SQL Injection, maka kode pemrograman harus diubah agar bisa mecegah aksi SQL Injection. Sedangkan untuk menambah keamanan dalam proses login ditambah dengan sebuah kode verifikasi. Kode verifikasi ini akan dikirim oleh sms gateway ke nomor telepon seluler milik mahasiswa sesuai nim. Sehingga apabila ada orang lain yang mengetahui nim dan pin seorang mahasiswa, maka orang lain itu tidak bisa masuk ke system SST, karena tidak bisa mengetahui kode verifikasi yang terkirim ke nomor telepon mahasiswa melalui sms.

Untuk mengembangkan keamanan sistem informasi SST di STMIK PPKIA Pradnya Paramita diperlukan tahapan-tahapan penelitian. Tahapan-tahapan yang digunakan mengacu pada S*ystem Development Life Cycle* (SDLC). Langkah-langkah penelitian yang dilakukan meliputi :

Analisis masalah dan pengumpulan data, terdiri dari :

1. Menganalisis masalah yang terjadi pada sistem informasi SST di STMIK PPKIA Pradnya Paramita.
2. Menyusun daftar permasalahan yang dihadapi oleh Mahasiswa,

Dosen dan Karyawan yang berhubungan langsung dengan data di SST.
3. Mengumpulkan data yang terkait.
4. Menganalisis data yang diperlukan.
5. Mendesain alur sistem informasi SST di STMIK PPKIA Pradnya Paramita.
6. Menentukan dan merancang Pemodelan Sistem
7. Merancang antar muka aplikasi.
8. Pengkodingan program.
9. Pengimplementasian program.
10. Pengujian program dan perbaikan.

A. Analisis Masalah dan Pengumpulan Data

Analisis dilakukan dengan melakukan survey langsung ke bagian yang terkait di STMIK PPKIA Pradnya Paramita yaitu Mahasiswa, Dosen, dan Karyawan terkait sistem tersebut. Berdasarkan hasil survei disusun daftar permasalahan yang dihadapi sebagai berikut:

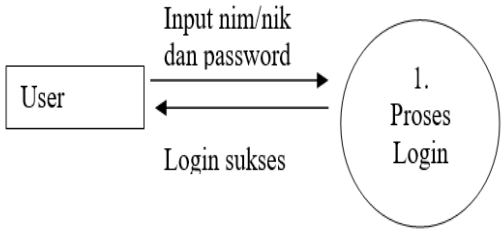
1. Ketika proses login dapat ditembus oleh orang lain yang tidak memiliki login dan password.
2. Orang lain yang telah masuk ke dalam sistem dapat merusak data di dalam sistem. Data yang dirusak antara lain adalah:
   a) KRS (Kartu Rencana Studi)
   b) Biodata Mahasiswa

B. Desain Sistem

Langkah-langkah dalam desain pengembangan pengamanan sistem informasi SST adalah sebagai berikut:

DESAIN SISTEM LOGIN YANG SEDANG BERJALAN

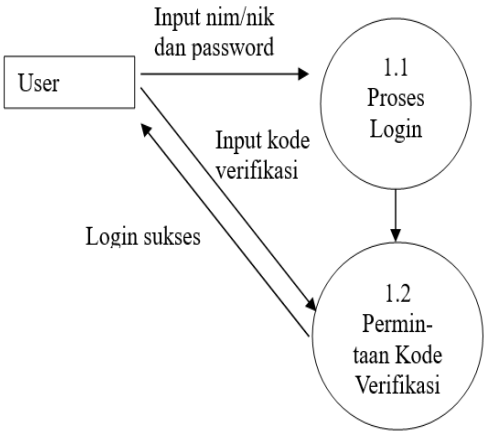
Sistem login yang sedang berjalan pada sistem informasi SST di STMIK PPKIA Pradnya Paramita adalah seperti pada gambar 1. User berasal dari mahasiswa atau dosen memasukkan id berupa nim/nik serta password untuk dapat masuk ke sistem informasi SST.



Gambar 1 Desain proses login ke SST yang sedang berjalan

DESAIN SISTEM LOGIN YANG DIUSULKAN

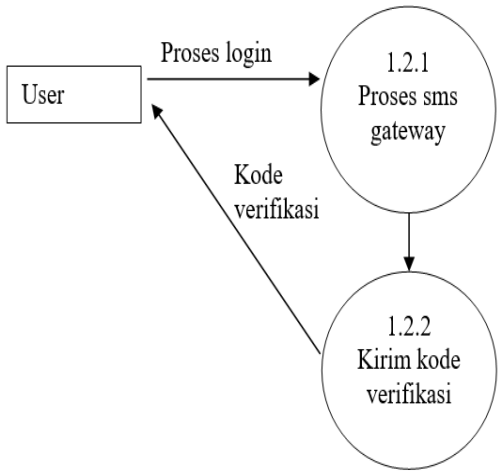
Sistem login yang diusulkan pada sistem informasi SST di STMIK PPKIA Pradnya Paramita adalah seperti pada gambar 2. User berasal dari mahasiswa atau dosen yang memasukkan id berupa nim/nik serta password kemudian saat pilih tombol "Login" sistem akan mengirimkan kode verifikasi melalui sms (sort message servis) ke nomor telepon seluler pemilik user. Kode verifikasi yang telah terkirim dapat dimasukkan ke inputan yang muncul setelah klik tombol "login". Kemudian klik "Submit" untuk masuk ke dalam sistem informasi SST STMIK PPKIA Pradnya Paramita.



Gambar 2Desain proses login ke SST yang disusulkan

DESAIN SISTEM PENGIRIMAN KODE VERIFIKASI

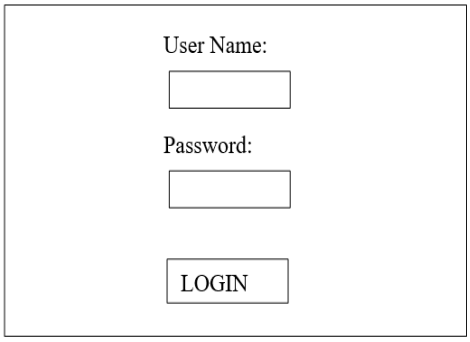
Kode verifikasi yang harus dimasukkan oleh user di proses login didapatkan dari sms yang telah terkirim ke nomor telepon selular, hal ini dapat dilihat pada gambar 3.



Gambar 3 Desain pengiriman kode verifikasi

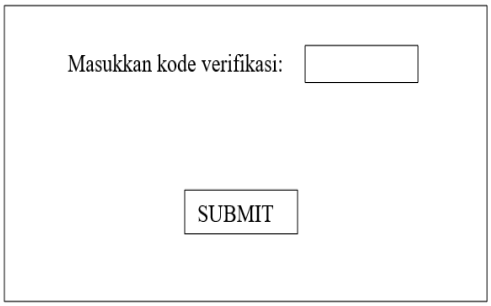
DESAIN ANTAR MUKA

Desain Antar Muka adalah rancangan antar muka untuk aplikasi proses login. Gambar 4 merupakan tampilan awal login pada sistem SST. Masukkan Username dan Password, lalu pilih tombol Login.



Gambar 4 Desain interface proses login

Setelah proses Login, selanjutnya user akan mendapatkan nomor verifikasi yang dikirim ke nomor telepon selular sesuai pemilik user yang baru saja diinputkan. Kode verifikasi tersebut dapat langsung diinputkan ke dalam halaman selanjutnya seperti pada Gambar 5. Setelah klik "Submit" selanjutnya user sudah dapat masuk ke dalam sistem SST.



Gambar 5 Desain input kode verifikasi

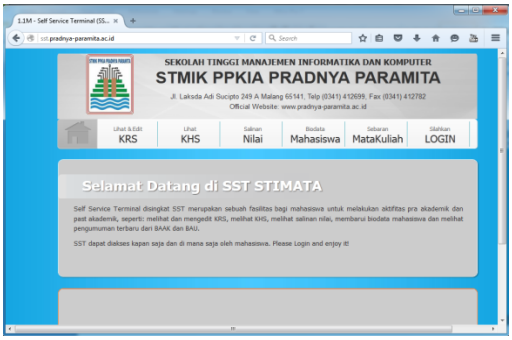
4. HASIL DAN PEMBAHASAN

Berdasarkan rancangan dan desain sistem yang telah disusun, maka diperoleh hasil antara lain hasil antar muka dan hasil pengujian program.

A. Hasil Antar Muka

Berdasarkan desain sistem yang telah dirancang pada bab sebelumnya, maka Penelitian ini telah diimplementasikan pada sistem informasi SST STMIK PPKIA Pradnya Paramita.

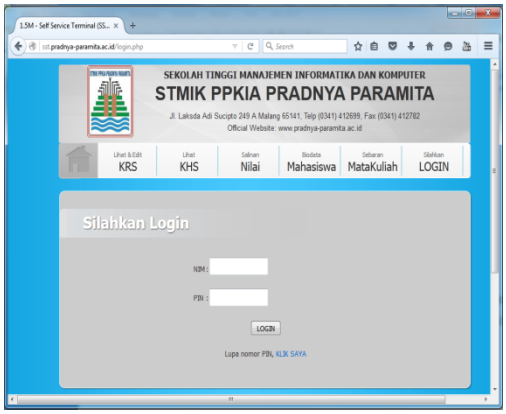
Gambar 6 merupakan halaman awal (pada halaman web sst.pradnya-paramita.ac.id) sebelum masuk ke sistem informasi SST STMIK PPKIA Pradnya Paramita.



Gambar 6 Halaman awal sst.pradnya-paramita.ac.id

Dari gambar 6 klik tombol "Silahkan Login" untuk masuk ke proses

login sistem informasi SST STMIK PPKIA Pradnya Paramita. Setelah itu akan muncul halaman proses login seperti pada gambar 7.



Gambar 7 Halaman proses login

B. Pengujian Program

Pengembangan keamanan sistem informasi SST STMIK PPKIA Pradnya Paramita dengan anti SQL Injection dan Verifikasi login melalui SMS Gateway pada proses login telah siap digunakan pada situs web sst.pradnya-paramita.ac.id.

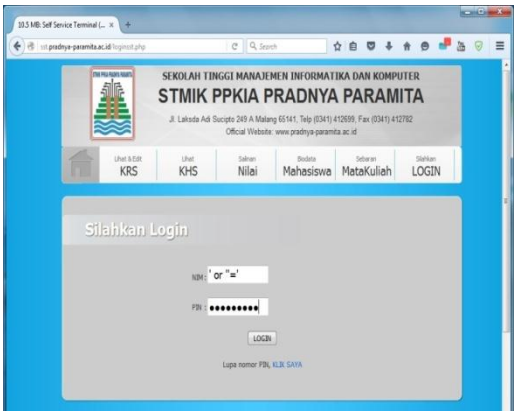
B.1. Pengujian Anti SQL Injection

Serangan SQL Injection adalah tidak adanya penanganan terhadap karakter-karakter tertentu. Namun setelah kode pemrograman diubah agar bisa mecegah aksi SQL Injection, maka Serangan SQL Injection dapat teratasi. Gambar 8 merupakan kode yang dimasukan ke dalam program untuk mencegah Serangan SQL Injection.

```
$user_name=mysql_real_escape_string(htmlentities(trim($_POST['user']
$password=mysql_real_escape_string(htmlentities(trim($_POST['passw']
```

Gambar 8 Kode Program untuk mengatasi serangan SQL Injection

Kemudian sistem informasi SST STMIK PPKIA Pradnya Paramita dicoba dimasukkan SQL Injection seperti pada gambar 9. Setelah klik tombol login maka gagal masuk login yang ditandai dengan munculnya pesan dialog seperti gambar 10.

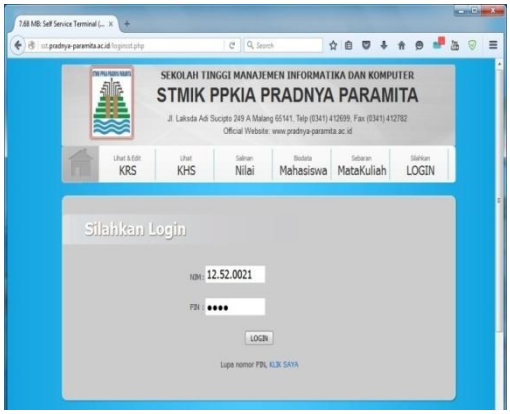


Gambar 9 Percobaan memasukkan SQL Injection

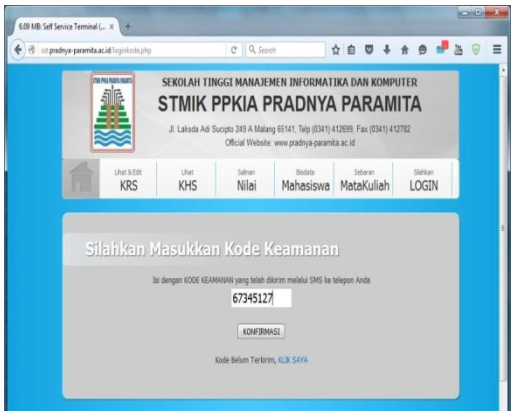
Gambar 10 Konfirmasi Login Gagal

B.2. Pengujian Verifikasi Login

Selanjutnya dilakukan pengujian Verifikasi login melalui SMS Gateway. Masukkan nim serta pin pada halaman proses login pada gambar 7. Sebagai contoh dimasukkan nim "12.52.0021" serta pin "xxxx" kemudian klik tombol "LOGIN" seperti pada gambar11. Jika pin yang dimasukkan salah, maka akan muncul pesan dialog gagal login seperti gambar 10. Jika pin yang dimasukkan benar, maka selanjutnya akan muncul form masukkan kode keamanan seperti gambar 12 dan akan terkirim sms dari sms gateway seperti pada gambar 13.

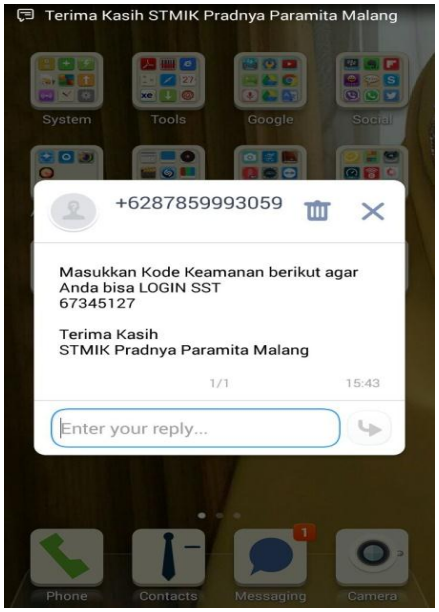


Gambar 11 Masukkan NIM dan PIN

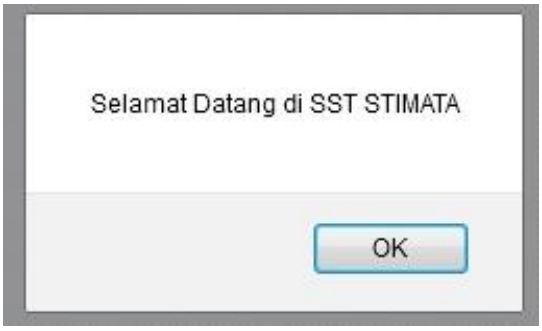


Gambar 12 Masukkan Kode Keamanan

Kode keamanan yang harus dimasukkan dapat diperoleh melalui sms yang telah dikirim dari sistem ke nomer handphone pemilik user masing-masing seperti pada gambar 13. Setelah kode tersebut dimasukkan kemudian klik tombol "KONFIRMASI", jika kode yang dikirimkan benar makan proses login berhasil dan muncul dialog login berhasil seperti gambar 14.



Gambar 13 SMS Gateway



Gambar 14 Konfirmasi Login Berhasil

5. KESIMPULAN

Dengan adanya pengembangan keamanan sistem informasi pada Self Service Terminal (SST) STMIK PPKIA Pradnya Paramita ini, diharapkan dapat membantu segi keamanan dan kenyamanan bagi pengguna (khususnya mahasiswa STMIK PPKIA Prdanya Paramita Malang) saat melakukan login. Serta diharapkan dapat mengamankan data yang tersimpan pada SST STMIK PPKIA Pradnya Paramita.

6. REFERENSI

Ariyus, Dony. 2006. *Computer Security*. Penerbit ANDI.

Kadir, Abdul. 2014 . *Pengenalan SIstem Informasi Edisi Revisi*. Penerbit Andi.

Tantra, Rudi. 2012. *Manajemen Proyek Sistem Informasi*. Penerbit Andi. Yogyakarta.

Tarigan, D.E., 2013. *Membangun SMS Getaway Berbasis Web dengan Codeigniter*. Lokomedia. Yogyakarta.

Yakub. 2012. *Pengantar Sistem Informasi*. Graha Ilmu. Yogyakarta.

Zam, Efvy. 2015. *Teknik Hacking dengan SQL Injection.* Elex Media Komputindo. Jakarta.