ARTIKEL ILMIAH TERPUBLIKASI

Analisis Keamanan Sistem Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Diponegoro

(Seminar Nasional Aplikasi Sains dan Teknologi Tgl. 13 Desember 2008 Yogyakarta
ISSN : 1979-911X, Hal : 175 – 186)

Oleh:

Ir. Kodrat Iman Satoto, MT

Program Studi Sistem Komputer
Fakultas Teknik
Universitas Diponegoro
2009

ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK BERBASIS WEB DI FAKULTAS TEKNIK UNIVERSITAS DIPONEGORO

Kodrat Iman Satoto, R. Rizal Isnanto, Ahmad Masykur

ABSTRACT

Web-based Academic Information System (web-based AIS) has been used by all students of Faculty of Engineering, Diponegoro University, Semarang. Therefore, all student academic records through the campus network needs to be done research on the security system is established so that safe.

The study was conducted by the steps of the analysis and testing of the system is installed, needs analysis, solution design problems, making improvements to the module, the module installation and repair module re-testing.

From the results of research conducted can be concluded that there are weaknesses in the login system. Weaknesses include the use of the Students number identification (NIM), as a default user name and password, the data the user name and password is not encrypted before sent to the server through the network, track a user name and password left behind in browser as a manager in the cache or password can be seen as a simple text (plaintext) is not encrypted. From the results of the analysis of the security, login system of AIS can be improved by implementation of HMAC MD5 encryption technology and Challenge Handshake Authentication Protocol (CHAP). Challenge raised by the server randomly and used as an encryption key in the process of HMAC MD5. With the use of the challenge your password sent a hash value will always be different at each session. Javascript in the client-side encryption used to do so before the data is sent to the server is encrypted.

Keywords: Academic Information System, login system, cryptography, security.

INTISARI

Sistem Informasi Akademik berbasis web (web-based SIA) telah digunakan oleh seluruh mahasiswa Fakultas Teknik Universitas Diponegoro Semarang. Oleh karena seluruh catatan akademik mahasiswa disimpan melalui jaringan kampus maka perlu dilakukan penelitian mengenai keamanan sehingga didapatkan sistem yang aman.

Penelitian ini dilakukan dengan langkah-langkah di antaranya analisis dan pengujian sistem terpasang, analisis kebutuhan, perancangan solusi permasalahan, pembuatan modul perbaikan, pemasangan modul dan pengujian ulang modul perbaikan.

Dari hasil penelitian yang dilakukan dapat disimpulkan bahwa terdapat kelemahan pada sistem login. Kelemahan tersebut meliputi penggunaan Nomor Induk Mahasiswa (NIM) sebagai nama pengguna dan kata sandi default, data nama pengguna dan kata sandi tidak dienkripsi sebelum dikirim ke server melalui jaringan, jejak nama pengguna dan kata sandi yang tertinggal di peramban sebagai cache atau dalam pengelola kata sandi dapat dilihat sebagai teks sederhana (plaintext) tidak terenkripsi. Dari hasil analisis keamanan tersebut, sistem login SIA dapat diperbaiki dengan penerapan teknologi enkripsi HMAC MD5 dan Challenge Handshake Authentication Protocol (CHAP). Challenge dibangkitkan oleh server secara acak dan digunakan sebagai kunci dalam proses enkripsi HMAC MD5. Dengan penggunaan challenge kata sandi yang dikirim berupa nilai hash akan selalu berbeda pada tiap sesi. Javascript di sisi klien digunakan untuk melakukan enkripsi sehingga data sebelum dikirim ke server sudah dalam keadaan terenkripsi.

Kata-kunci: Sistem Informasi Akademik, sistem login, kriptografi, keamanan.

PENDAHULUAN

LATAR BELAKANG MASALAH

Sistem Informasi Akademik (SIA) yang bersifat *online* memudahkan sivitas akademika untuk mengakses informasi berkaitan dengan kebutuhan akademis. Informasi dapat diakses dari komputer mana saja yang tersambung dengan jaringan kampus bila diketahui nama akun dan kata sandi yang dibutuhkan.

Salah satu celah kelemahan terdapat pada sistem login. Sistem login pada SIA versi 0.4 saat ini diduga sangat rentan terhadap pembobolan kata sandi oleh orang yang tidak berhak.

IDENTIFIKASI MASALAH

Secara normal sistem login sudah cukup aman. Sistem login yang saat ini digunakan berupa pasangan nama pengguna dan kata sandi. Nama pengguna dan kata sandi dikirimkan ke *server* berupa teks sederhana (*plaintext*) tanpa enkripsi.

Kemungkinan terjadinya penyusup atau pencurian data pengguna dan kata sandi dapat melalui dua cara. Pertama, dengan melakukan pengendusan (*sniffing*) lalulintas data antara terminal dengan *server*. Kedua, dengan melihat jejak yang ada di komputer terminal itu sendiri.

TUJUAN PENELITIAN

Tujuan dilakukannya penelitian ini adalah pencarian kelemahan aplikasi SIA versi 0.4 dari sisi keamanan dan pembuatan solusi atas permasalahan yang ditemukan sehingga didapat aplikasi yang lebih baik.

KAJIAN PUSTAKA

SISTEM INFORMASI AKADEMIK

Sistem Informasi Akademik (SIA) adalah perangkat lunak yang digunakan untuk menyajikan informasi dan menata administrasi yang berhubungan dengan kegiatan akademis. Dengan penggunaan perangkat lunak seperti ini diharapkan kegiatan administrasi akademis dapat dikelola dengan baik dan informasi yang diperlukan dapat diperoleh dengan mudah dan cepat.

Fitur yang tersedia pada aplikasi SIA Fakultas Teknik Undip versi 0.4 adalah kelompok pengguna, Internet *ready*, SMS-*based ready*, *online banking ready*, Dikti *Self-evaluation Ready,* fasilitas *guest*, fasilitas mahasiswa, fasilitas dosen, fasilitas BAA (Bagian Administrasi Akademik) dan fasilitas *supervisor* (Satoto, 2006).

SISTEM LOGIN

Sistem login (*login*, juga biasa disebut sebagai *log in, log on, signon, sign on, signin, sign in*) adalah proses untuk mengakses komputer dengan memasukkan identitas dari akun pengguna dan kata sandi untuk mendapatkan hak akses menggunakan sumber daya komputer tujuan (Johnston, 2005).

Untuk melakukan login ke sistem biasanya membutuhkan pasangan akun pengguna dan kata sandi. Pasangan tersebut harus tepat dan keduanya adalah pasangan yang tidak bisa dipisahkan. Kata sandi dapat diubah sesuai dengan kebutuhan, sedangkan akun pengguna tidak pernah diubah karena berupa identitas unik yang merujuk ke pengguna tertentu.

KRIPTOGRAFI HMAC MD5

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data.

Proses yang digunakan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*). Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Fungsi *hash* merupakan fungsi yang secara efisien mengubah *string* masukan dengan panjang berhingga menjadi *string* keluaran dengan panjang tetap yang disebut nilai *hash*.

MD5 adalah salah satu dari serangkaian algortima *message-digest* yang dirancang oleh Profesor Ronald Rivest dari Massachusetts Institute of Technology (MIT). Ketika kerja analitis menunjukkan bahwa pendahulu MD5 — MD4 — mulai tidak aman, MD5 kemudian dirancang pada tahun 1991 sebagai pengganti dari MD4. *Hash* MD5 sepanjang 128-*bit* (16-*byte*), yang dikenal juga sebagai intisari pesan, *message digest* secara tipikal ditampilkan dalam bilangan heksadesimal 32-digit.

Keyed-Hash-Message-Authentication-Code atau disebut sebagai HMAC adalah salah satu metode kode autentikasi pesan (*message authentication code, MAC*) yang didasarkan pada fungsi kriptografi *hash* (Krawczyk, 1997). Pesan bersama dengan kunci dimasukkan dalam fungsi HMAC yang menghasilkan satu keluaran nilai *hash*.

COOKIE DAN STATUS SESI

Sifat *web* yang *stateless* – antara *server* dan klien segera memutus hubungan jika data telah selesai dikirim – sedangkan aplikasi membutuhkan status atau data yang akan terus dipakai saat aplikasi berjalan. Sifat *web* seperti itu dapat ditangani dengan menggunakan sesi (*session*). Status hubungan dan data pada aplikasi disimpan dalam sesi di *server* (Rickyanto, 2003).

Cookie digunakan untuk menyimpan identitas sesi yang berada di masing-masing peramban (*browser*). Identitas sesi adalah unik dan tidak mungkin terdapat duplikasi. Saat aplikasi *web* pertama kali diakses oleh peramban, sesi baru dibuat oleh *server* dengan identitas sesi yang unik. Identitas sesi digunakan untuk mengenali klien yang melakukan permintaan dan menjaga status hubungan antara klien dan *server*. Ketika pengguna melakukan navigasi di situs yang sama, identitas sesi tersebut akan dikirim beserta dengan data permintaan HTTP (HTTP *request*) dan *server* memberikan jawaban dengan menyertakan identitas sesi yang sama. Terdapat dua jenis *cookie*. *Cookie persistent* dan *non-persistent*. *Cookie persistent* disimpan pada komputer pengguna. *Cookie non-persistent* digunakan untuk mencatat aktivitas pengguna yang autentik pada waktu membuka situs *web*. Ketika sesi berakhir, *cookie non-persistent* akan dihapus (Burnett, 2005).

Identitas status sesi akan dicatat sebagai pengguna yang autentik ketika pengguna telah login dengan benar. Saat keluar dari sistem (logout) identitas sesi dicatat di *server* sebagai pengunjung yang tidak autentik.

JAVASCRIPT

Javascript adalah bahasa lintas-*platform* yang diperkenalkan pertama kali oleh Netscape. Javascript merupakan salah satu bahasa naskah (*scripting*) berorientasi-objek. Javascript memberikan sarana untuk menjalankan aplikasi melalui Internet. Aplikasi klien berjalan di peramban seperti Netscape Navigator dan aplikasi *server* berjalan di *server* seperti Netscape Enterprise Server. Javascript dapat digunakan untuk membuat HTML dinamis yang mengolah masukan pengguna dan memelihara data menggunakan objek khusus (Holzner, 2002).

SISTEM LOGIN CHAP

Sistem login CHAP (*Challenge Handshake Authentication Protocol*) merupakan tipe protokol autentikasi dengan sebuah kunci – berupa data acak – dikirim kepada agen autentikasi klien yang digunakan untuk mengenkripsi kata sandi sebelum dikirim ke *server*.

CONTENT MANAGEMENT SYSTEM

Content Management System (CMS) adalah sistem yang digunakan untuk mengatur situs *web*. Biasanya, CMS mengandung dua elemen: *Content Management Application* (CMA) dan *Content Delivery Application* (CDA). CMA merupakan elemen yang memudahkan seorang manajer isi (*content manager*) atau penulis – tanpa harus mengetahui *Hypertext Markup Language* (HTML) – untuk membuat, mengatur, mengubah dan menghapus isi dari situs *web*. Elemen CDA digunakan untuk menyusun informasi untuk memperbarui isi situs *web*.

METODOLOGI

Dalam melakukan analisis, digunakan beberapa metode yaitu studi literatur, pengujian sistem yang sudah ada, perumusan solusi permasalahan dan penerapan solusi permasalahan. Masing-masing metode memiliki keterkaitan satu dengan lainnya.

STUDI LITERATUR

Tahap ini dilakukan dengan mengumpulkan bahan-bahan pustaka (literatur) sesuai dengan masalah yang dihadapi. Literatur sebagian besar didapat dari Internet karena sebagian besar referensi buku cetak tidak ditemukan.

ALAT DAN BAHAN

1. SIA Fakultas Teknik UNDIP Versi 0.4
   SIA pada versi ini adalah yang digunakan di Teknik Elektro program Ekstensi Fakultas Teknik Undip dan dapat diakses melalui Internet dengan alamat http://sia-ft.undip.ac.id/elektroext/.
2. CMS Drupal
   CMS Drupal merupakan salah satu E-CMS yang sangat populer saat ini. CMS ini dipilih karena kemampuannya untuk membuat modul sendiri termasuk modul sistem login. CMS Drupal dapat dilihat di situs resminya http://www.drupal.org/.
3. Peramban Firefox dan Internet Explorer
   Kedua peramban ini dipilih karena peramban terbanyak yang digunakan pada terminal di lingkungan kampus FT Undip. Digunakan dua versi peramban Firefox yaitu versi 1.0 dan versi 1.5. Internet Explorer 6.0 digunakan untuk pengujian pada terminal yang berbasis Microsoft Windows.
4. Fiddler v1.1
   Fiddler merupakan salah satu program pemantau sesi (*session inspector*) dengan target peramban Microsoft Internet Explorer. Dengan perangkat lunak ini lalulintas data dari/ke Internet Explorer dapat dipantau.
5. Ethereal 0.99
   Ethereal adalah salah satu program pengendus (*sniffer*) aliran data yang melewati jaringan. Ethereal ditempatkan antara *server* dan peramban. Semua paket data yang melewati perangkat keras (seperti *ethernet card* dan *router*) dapat dipantau.

PENGUMPULAN DATA

Data pengguna dapat diambil dari daftar NIM yang terdaftar karena NIM dijadikan sebagai nama pengguna pada SIA versi 0.4. Cara pengumpulan data NIM termudah adalah dari daftar mahasiswa yang terdapat pada SIA. Ada dua jalan untuk mendapatkan data mahasiswa menggunakan SIA. Pertama pada menu *Mencari data mahasiswa* dan kedua pada menu *Daftar peserta matakuliah*.

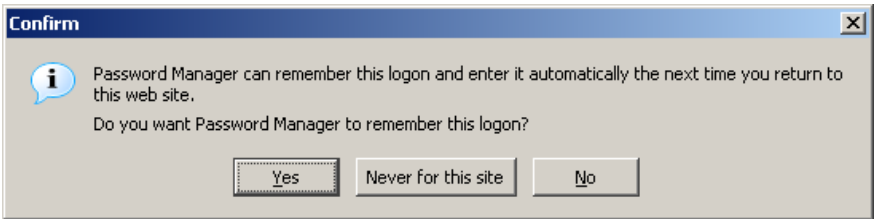
Data kata sandi dapat diambil dengan dua cara. Pertama menggunakan kata sandi *default*. Kata sandi *default* untuk SIA versi 0.4 adalah sama dengan NIM pengguna. Kedua dengan metode *social engineering* yaitu metode pendekatan dengan pengguna. Metode ini membutuhkan keahlian khusus tidak hanya dalam hal teknis tetapi juga segi psikologi. Cara mudah untuk melakukan *social engineering* pada kasus ini adalah dengan

menjebak nama pengguna dan kata sandi untuk disimpan pada Firefox.

ANALISIS DAN PENGUJIAN SISTEM

Pengujian pertama adalah masalah sistem login. Pencurian data kata sandi dapat dilakukan dengan cara pengendusan data yang melewati jaringan antara klien dengan *server*.

Pengujian berikutnya adalah dengan melihat jejak data yang tertinggal di komputer terminal (klien). Komputer terminal yang disediakan sebagian besar menggunakan peramban Firefox sehingga target penelitian adalah peramban Firefox. Pada peramban Firefox terdapat fasilitas untuk menyimpan kata sandi.



Gambar 1. Konfirmasi penyimpanan kata sandi pada Firefox 1.0

Seperti terlihat pada Gambar 1, pada Firefox 1.0 tombol *default* dialog penyimpanan kata sandi adalah *Yes* yang berarti akan menyimpan kata sandi dalam pengelola kata sandi (*password manager*). Hal ini mungkin tidak terlalu rentan pada Firefox 1.5 karena tombol *default* dialog untuk menyimpan kata sandi bukan *Yes* melainkan *Not Now* seperti ditunjukkan pada Gambar 2.

Gambar 2. Jendela option → privacy → password Firefox 1.5

Penekanan tombol *Yes* pada Firefox 1.0 (tombol *Remember* pada Firefox 1.5) akan mengakibatkan kata sandi tersimpan dalam pengelola kata sandi. Tombol *Never for this site* digunakan untuk mencatat kata sandi untuk situs yang dikunjungi (dalam kasus ini adalah SIA) tidak akan pernah disimpan ke dalam pengelola kata sandi. Tombol *No* pada Firefox 1.0 (tombol *Not Now* pada Firefox 1.5) berfungsi untuk tidak menyimpan kata sandi ke dalam pengelola kata sandi hanya pada saat tombol *No* ditekan.

Kata sandi yang tersimpan dapat dilihat hanya dengan penekanan tombol *View Saved Passwords* pada jendela *Option → Privacy → Passwords* seperti terlihat pada Gambar 3. Dengan cara ini, data nama pengguna kata sandi semua pengguna yang telah menggunakan komputer terminal baik untuk tujuan akses SIA maupun layanan Internet lainnya dapat dilihat dengan mudah.

PERUMUSAN SOLUSI PERMASALAHAN

Dalam merumuskan solusi permasalahan, tiap masalah didokumentasikan. Dari dokumentasi permasalahan dicarikan solusi untuk memperbaiki sistem.

Gambar 3. Jendela option → privacy → password Firefox 1.5

PENERAPAN SOLUSI PERMASALAHAN

Berdasarkan hasil analisis pengujian, studi literatur dan perumusan solusi masalah dibuat model untuk solusi yang akan digunakan. Dari model tersebut kemudian dibuat kode program sederhana untuk diujicobakan. Bila hasil uji coba tersebut berhasil, bagian kode program tersebut kemudian ditempelkan pada bagian proyek yang memiliki kelemahan.

PENGUJIAN ULANG SISTEM

Tahap akhir adalah pengujian untuk mendapatkan hasil yang maksimal. Pengujian akhir dimaksudkan untuk mencari kelemahan yang masih ditemui pada solusi yang diberikan. Dari hasil pengujian bila ditemukan kesalahan, maka solusi dievaluasi kembali dan diperbaiki untuk mendapatkan hasil yang terbaik.

HASIL PENELITIAN DAN PEMBAHASAN

PENGUJIAN SISTEM AUTENTIKASI

Pengujian sistem autentikasi dilakukan dengan berbagai cara yaitu dengan kata sandi *default*, pencurian kata sandi yang melintas pada jaringan, teknik SQL *injection* dan pencarian jejak kata sandi yang berada di komputer terminal. Masing-masing teknik memiliki tingkat kesulitan masing-masing.

PENCARIAN DAFTAR PENGGUNA

Untuk mendapatkan daftar pengguna tidak sulit. Pada sistem *log* SIA versi 0.4, Nomor Induk Mahasiswa (NIM) digunakan sebagai nama pengguna. Salah satu cara adalah dengan melihat daftar mahasiswa pada lembar presensi atau daftar mahasiswa dari sumber lain yang dipublikasi. Cara lainnya adalah dengan melihat daftar mahasiswa dari aplikasi SIA.

PENGUJIAN SISTEM LOGIN DENGAN KATA SANDI DEFAULT

Salah satu kelemahan SIA versi 0.4 adalah penggunaan kata sandi *default*. Kata sandi *default* SIA versi 0.4 adalah sama dengan nama pengguna.

Dari hasil uji menggunakan objek daftar mahasiswa yang mengikuti mata kuliah Basis Data, didapatkan tiga belas dari empat puluh empat (29,5%) mahasiswa masih menggunakan kata sandi *default*. Daftar mahasiswa objek uji yang masih menggunakan kata sandi *default* dapat dilihat pada Tabel 4.1.

Tabel 1. Daftar mahasiswa peserta mata kuliah Sistem Basis Data yang belum mengubah kata sandi *default*

No	NIM	Nama	Kata Sandi
1	L2F304222	CANDRA HERU P	L2F304222
2	L2F304224	DENDY ACHMAD A.	L2F304224
3	L2F304237	HELMY YANUAR P	L2F304237
4	L2F304244	IRAWAN SUPRIYATMO	L2F304244
5	L2F304271	RIZKA PRATHESA	L2F304271
6	L2F305173	ADI PAMUNGKAS	L2F305173
7	L2F305188	ANI HIDAYATI	L2F305188
8	L2F305191	ARI PURTANTO SN	L2F305191
9	L2F305209	FAJAR SARI K.	L2F305209
10	L2F305215	HENGKY IRAWAN	L2F305215
11	L2F305223	LINDA LAURAWATI	L2F305223
12	L2F305240	SUBIONO AHMAD	L2F305240
13	L2F305245	TOMMY ADHI K. M.	L2F305245

Keterangan: data diambil dari http://sia-ft.undip.ac.id/elektroext/

Teknik pengujian kata sandi *default* yang lain adalah dengan mempergunakan alat bantu. Alat bantu ini pada prinsipnya hanya berupa program komputer yang dapat melakukan percobaan sistem login secara otomatis berdasarkan nilai yang ditetapkan dan menghasilkan laporan keberhasilan. Alat bantu ini dibuat untuk mempercepat analisis pengguna yang masih menggunakan kata sandi *default* SIA.

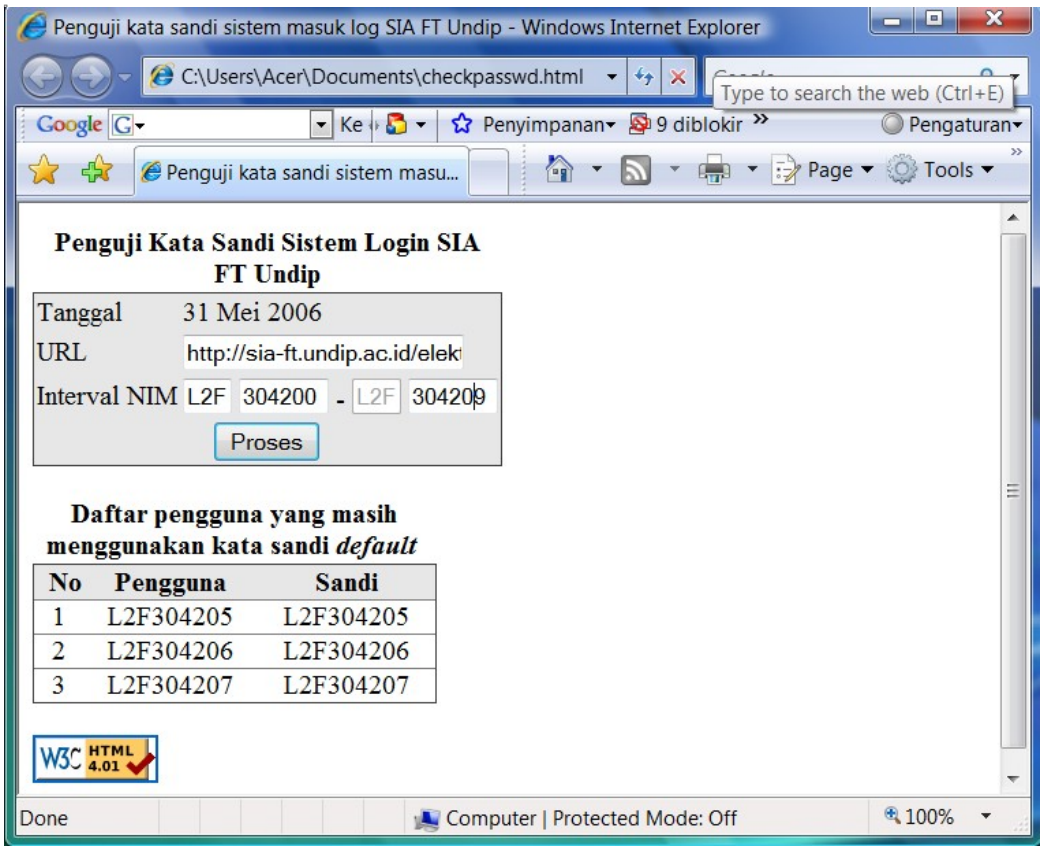
Pada Gambar 4 diperlihatkan tampilan program penguji kata sandi *default* SIA FT Undip. Pada pengujian ini, diberi parameter *Interval NIM* diisi dengan nilai L2F304200 – L2F30409. Dari hasil pengujian tersebut didapat tiga mahasiswa masih menggunakan kata sandi *default*. Dengan memasukkan *Interval NIM* L2F304200 – L2F304299 didapatkan bahwa terdapat tiga puluh lima mahasiswa masih menggunakan kata sandi *default*.

PEMANTAUAN SESI

Pemantauan sesi bertujuan untuk mendapatkan data pengujian pada komputer setempat (*local computer*). Pemantauan sesi pada peramban Internet Explorer dapat dilakukan menggunakan Fiddler dengan membuka alamat SIA di alamat situs http://sia-ft.undip.ac.id/elektroext/.

Pada penelitian ini, didapatkan *string* sesi yang dapat dianalisis sebagai berikut: PHPSESSID=31b957b8657927e3163dc6a23201c39e&uname=L2F304219&pass=p455w0rd&op=login

Masing-masing data pada *string* sesi dipisahkan dengan karakter *ampersand* (&). *String* yang didapat menunjukkan bahwa pengguna melakukan operasi sistem login (*string* op=login) dengan nama pengguna L2F309219 (*string* uname=L2F304219) dan kata sandi p455w0rd (*string* pass=p455w0rd). Dari hasil pemantauan ini dapat disimpulkan bahwa data nama pengguna dan kata sandi tidak terenkripsi sebelum dikirimkan melalui jalur transmisi data.



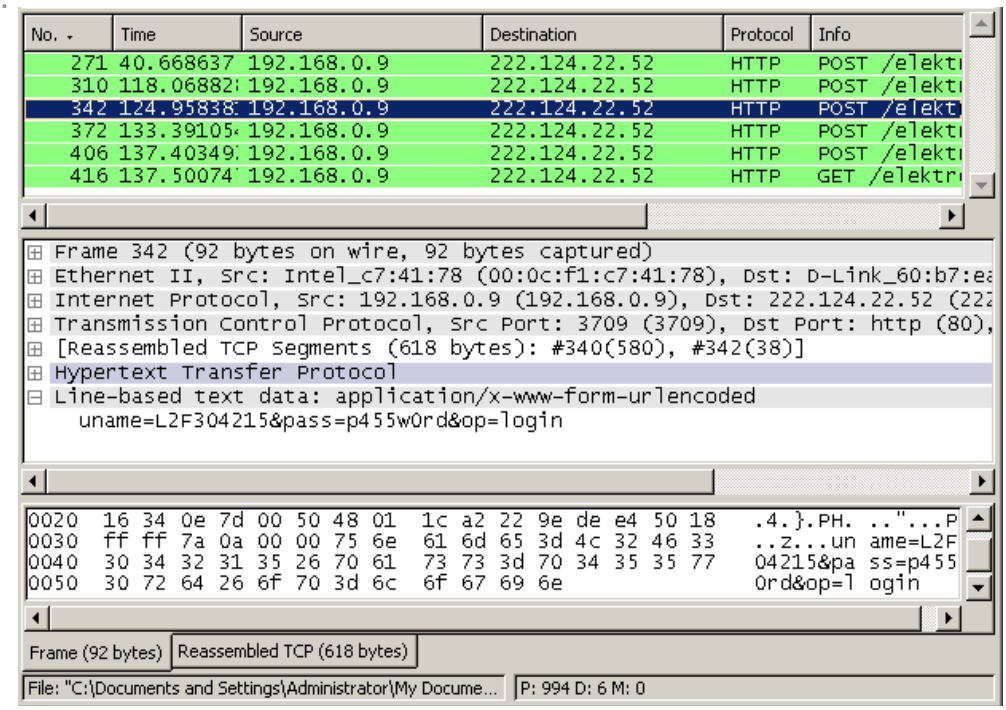
Gambar 4. Tampilan program penguji kata sandi *default*

PENGENDUSAN MENGGUNAKAN ETHEREAL

Hasil pengendusan seperti ditunjukkan pada Gambar 5 didapat beberapa *frame* data. Daftar *frame* data yang berhasil ditangkap ditunjukkan pada kotak sebelah atas, terjemahan *frame* data ditampilkan di kotak tengah, sedangkan kotak bawah digunakan untuk menampilkan *frame* dalam format heksadesimal. Dari data yang didapat terdapat beberapa nama pengguna dan kata sandi yang ditangkap sebagaimana ditunjukkan pada Tabel 2.

Tabel 2. Data hasil pengendusan menggunakan Ethereal

No	Data Tangkapan
1	uname=L2F304248&pass=jangantanya&op=login
2	uname=L2F304248&pass=jangantanya&op=login
3	uname=L2F304215&pass=p455w0rd&op=login
4	uname=L2F305211&pass=L2F305211&op=login
5	uname=L2F305188&pass=L2F305188&op=login



Gambar 5. Hasil pengendusan menggunakan Ethereal

TEKNIK SQL INJECTION

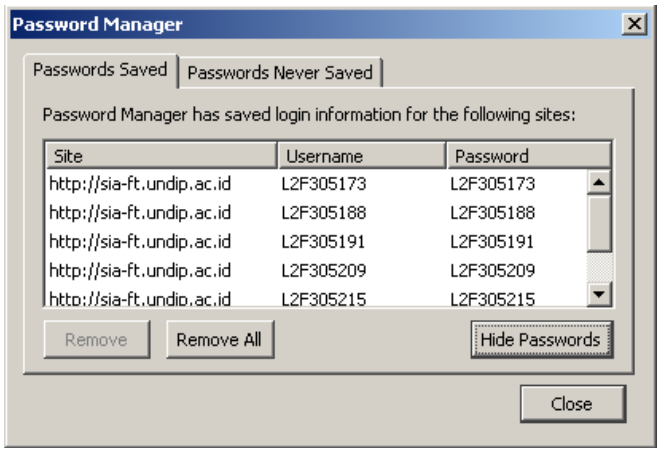
Pengujian pertama dilakukan dengan menambahkan *query* di belakang nama pengguna yaitu “L2F304209' OR 1=1 --” (tanpa tanda kutip ganda). Jika aplikasi yang dibuat belum menangani kelemahan akibat penyerangan dengan teknik SQL *injection*, maka pengunjung dapat masuk dengan nama pengguna L2F304209 tanpa harus mengetahui kata sandi akun tersebut. Pada pengujian ini sistem tidak dapat ditembus dengan teknik SQL *injection* di atas. Pengujian selanjutnya dengan memanfaatkan *query string* pada baris alamat peramban.

Setelah melakukan sistem login dengan pengguna terautorisasi, baris alamat situs akan berisi URL alamat situs ditambah dengan *query string* yaitu http://sia-ft.undip.ac.id/ elektroext/user.php?op=userinfo&bypass=1&uname=L2F305188.

Pengujian dilakukan dengan merubah nilai *query string* uname dari nilai asli menjadi nama pengguna lain sebagai contoh L2F304205. Dari hasil pengujian didapat bahwa aplikasi tidak mengalami kesalahan sehingga dapat disimpulkan bahwa keamanan aplikasi tidak dapat ditembus dengan teknik SQL *injection*.

PENCARIAN JEJAK KATA SANDI PADA TERMINAL

Pengujian pada peramban Firefox dilakukan dengan melakukan sistem login. Setelah penekanan tombol *Masuk*, peramban menanyakan apakah kata sandi tersebut akan diingat oleh pengelola kata sandi seperti ditunjukkan pada Gambar 1. Dalam pengujian ditekan tombol *Yes* untuk menyimpan kata sandi tersebut ke dalam pengelola kata sandi. Pengujian dilakukan pada tujuh nama pengguna yang berbeda. Setelah dilihat pada pengelola kata sandi ternyata kata sandi tersimpan dan dapat dilihat dengan mudah seperti terlihat pada Gambar 6.



Gambar 6.
Daftar nama pengguna dan kata sandi pada jendela Password Manager Firefox

PERBAIKAN SISTEM AUTENTIKASI

SIA yang terpasang pada saat ini dibuat menggunakan bahasa PHP dan basis data MySQL. Pembuatan modul perbaikan juga digunakan bahasa dan basis data yang sama. Untuk dapat membuat sistem autentikasi harus ada sebuah sistem yang berjalan sebagai bahan uji. *Content Management System* (CMS) Drupal digunakan sebagai sistem yang akan diuji dan sekaligus sebagai kerangka kerja (*framework*) dalam membangun sistem yang utuh.

PERANCANGAN

Pada tahap ini digunakan bagan alir untuk membantu menggambarkan proses yang terjadi. Terdapat dua bagan alir yaitu bagan alir di sisi klien dan bagan alir sisi *server*. Keduanya memiliki hubungan timbal balik antara *server* dan klien. Pada waktu peramban pertama kali melakukan permintaan terhadap *server*, sesi baru dibuat oleh *server* dan mengirimkan formulir sistem login beserta data acak *challenge* digunakan untuk proses autentikasi seperti terlihat pada Gambar 7.

Bagan alir dapat dilihat pada Gambar 7. Pada bagan alir bagian klien dibutuhkan beberapa fungsi diantaranya pengambilan data nama pengguna, kata sandi, *challenge*, enkripsi HMAC MD5 dan pengiriman data ke *server*.

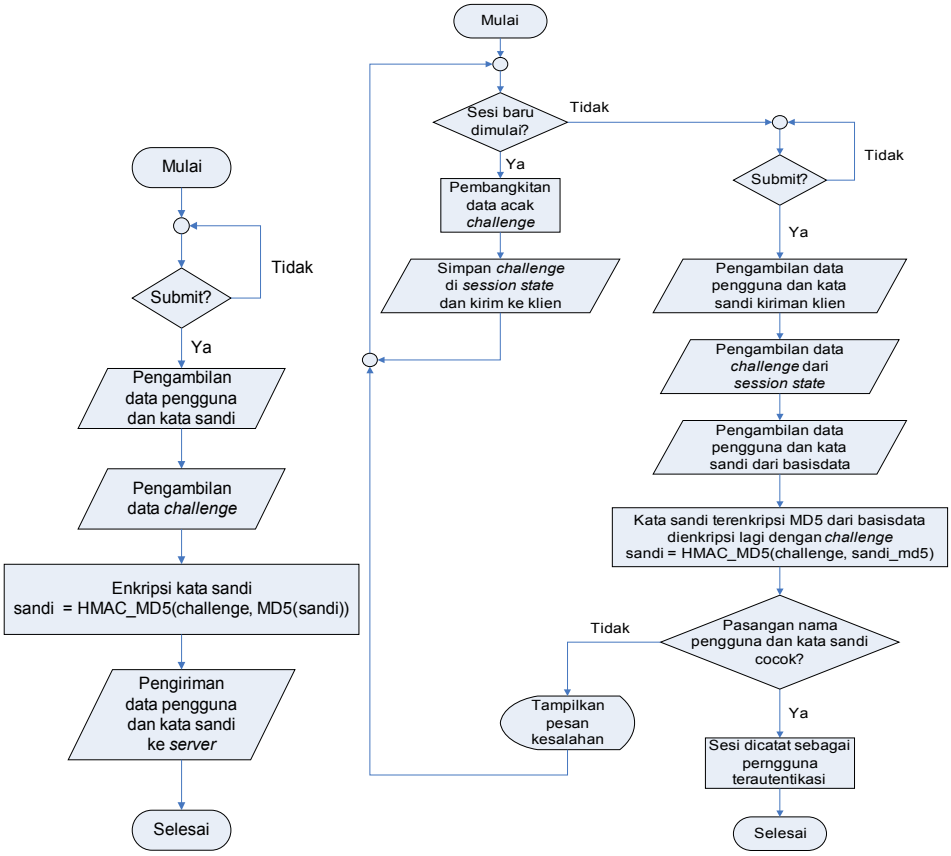
PEMBUATAN MODUL

Modul dibuat berupa modul blok sebagai pengganti modul *userlogin* asli Drupal. Modul diberi nama *chaplogin* dan disimpan dalam berkas *chaplogin.module.* Modul *chaplogin* dibuat dengan algoritmanya enkripsi HMAC MD5. Terdapat dua bekas pendukung yang digunakan untuk enkripsi di sisi klien yaitu *chaplogin.js* dan *md5.js*.

PEMASANGAN, AKTIVASI DAN KONFIGURASI MODUL

Modul dipasang sebagai pengganti modul asli dengan cara melepas modul asli dan kemudian memasang modul *chaplogin* serta mengaktifkannya. Langkah-langkah pemasangan modul dapat dilihat pada dokumentasi Drupal di http://www.drupal.org/.

Pada penelitian ini Drupal dipasang di direktori akar *web* yaitu /www/ pada *server* sia.phpnet.us sehingga dapat diakses secara langsung menggunakan alamat http://sia.phpnet.us/. Pemasangan modul *chaplogin* dilakukan dengan unggah (*upload*) berkas-berkas modul (chaplogin.js, chaplogin.module dan md5.js) menggunakan FTP ke direktori /www/modules/chaplogin/.



Gambar 7.
Bagan alir login di sisi klien (kiri) dan *server* (kanan) dengan enkripsi HMAC MD5

PENGUJIAN MODUL CHAPLOGIN

Pengujian modul autentikasi dilakukan dengan berbagai cara, sama seperti pengujian sistem sebelumnya yaitu dengan kata sandi *default*, pencurian kata sandi yang melintas pada jaringan, teknik SQL *injection* dan pencarian jejak kata sandi yang berada di komputer terminal.

PENGUJIAN KATA SANDI DEFAULT

Pada pengujian kata sandi dengan *default*, modul *chaplogin* dinyatakan lulus uji karena setiap pengguna mendaftarkan diri sendiri dengan nama akun pengguna dan kata sandi sendiri. Dalam sistem tidak terdapat kata sandi *default* sehingga tidak dimungkinkan adanya penyusupan dengan menggunakan kata sandi *default*.

PEMANTAUAN SESI

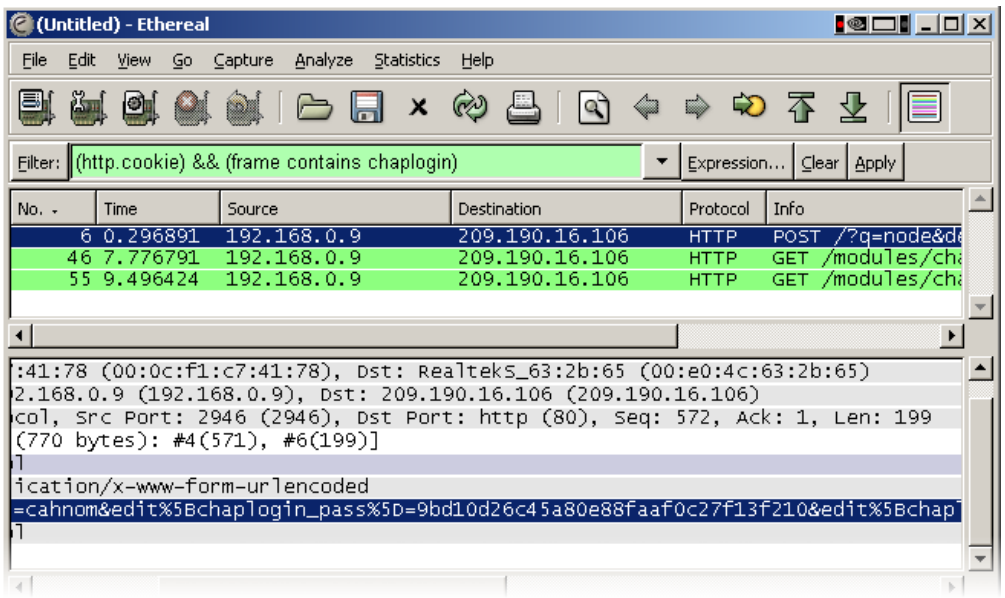
Dengan bantuan Fiddler, sesi dapat dipantau untuk mendapatkan data pengguna dan kata sandi. Pengujian dilakukan dengan pemantauan sesi HTTP POST yang kemungkinan berisi nama pengguna dan kata sandi.

Dari data sesi HTTP POST yang didapat dari pemantauan sesi terlihat bahwa data sesi berisi edit%5Bchaplogin_name%5D=cahnom&edit%5Bchaplogin_pass%5D= 9bd10d26c45a80e88faaf0c27f13f210&edit%5Bchaplogin_challenge%5D=405f5f5a&op= Login&edit%5Bchaplogin_mode%5D=1&edit%5Bform_id%5D=chaplogin-form.

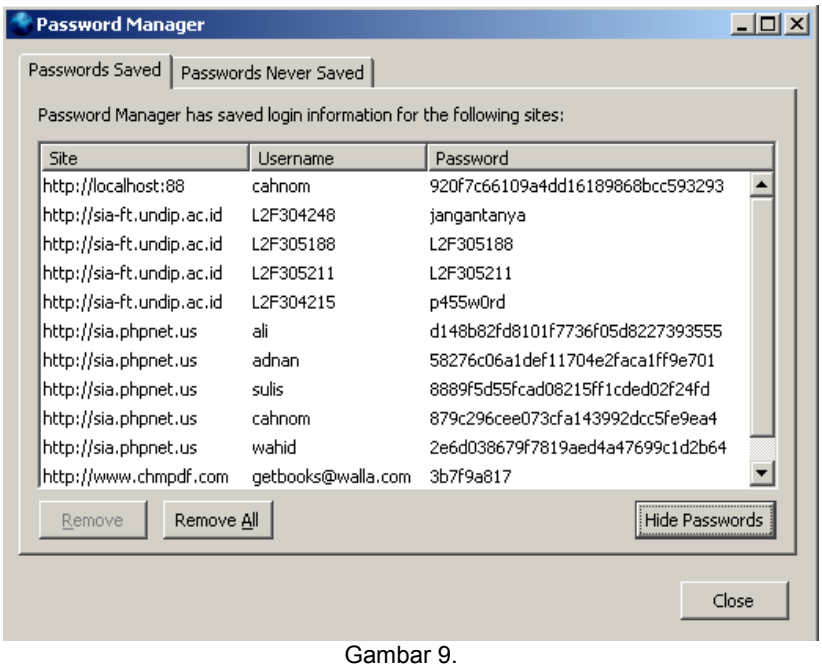
Dapat dilihat bahwa pengguna sistem login sebagai cahnom dan kata sandi telah terenkripsi. Pengujian kali ini dinyatakan lulus uji karena kata sandi tidak dapat dilihat secara langsung melalui data sesi yang dipantau.

PENGENDUSAN DATA

Dari hasil pengendusan dapat disimpulkan bahwa data telah lebih aman pada waktu melintasi jalur transmisi. Data dienkripsi di peramban dengan Javascript sebelum dikirimkan ke *server.* Seperti terlihat pada gambar 8 bahwa data kata sandi yang berhasil diendus merupakan kata sandi yang telah dienkripsi.



Gambar 8. Hasil pengendusan modul *chaplogin* menggunakan Ethereal



Gambar 9.
Daftar nama pengguna dan kata sandi terenkripsi pada jendela Password Manager Firefox

TEKNIK SQL *INJECTION*

Pengujian dengan teknik ini dilakukan dengan memasukkan nama pengguna sebagai “cahnom' OR 1=1 --” (tanpa tanda kutip ganda) tanpa kata sandi. Dari hasil pengujian didapat bahwa teknik ini tidak dapat digunakan untuk menembus sistem login yang dibuat.

PENCARIAN JEJAK KATA SANDI PADA TERMINAL

Digunakan lima contoh pengguna dengan nama pengguna berbeda dan kata sandi yang sama yaitu “rahasia” (tanpa tanda kutip ganda). Pada gambar 9 terlihat bahwa kata sandi telah terenkripsi pada semua pengguna yang mencoba sistem login ke sistem dengan alamat URL http://sia.phpnet.us/

PENUTUP

KESIMPULAN

Telah dilakukan Analisis Keamanan Sistem Informasi Akademik Fakultas Teknik Undip Versi 0.4 dengan hasil yang menyatakan bahwa;

1. Data kata sandi pada sistem login tidak dienkripsi sebelum dikirim ke *server,*
2. Penggunaan kata sandi *default* sama dengan nama pengguna menjadikan sistem rawan penyusup,
3. Data sesi yang dikirim dari peramban ke *server* tidak terenkripsi,
4. Penyerangan dengan teknik SQL *injection* tidak dapat dilakukan pada sistem login maupun *query string* pada baris alamat,
5. Jejak nama pengguna dan kata sandi dapat dilihat pada pengelola kata sandi peramban Firefox sebagai teks tidak terenkripsi.

Perbaikan atas kelemahan sistem yang telah dilakukan meliputi;

1. Data kata sandi pada sistem login telah dienkripsi sebelum dikirim ke *server,*
2. Tidak digunakan sandi *default* melainkan kata sandi dibuat oleh pengguna sendiri,
3. Data kata sandi dalam sesi yang dikirim ke *server* telah terenkripsi dengan metode CHAP dan algoritma enkripsi HMAC MD5,
4. Jejak nama pengguna dan kata sandi pada pengelola kata sandi sebagai nilai *hash*.

SARAN

Dari penelitian yang telah dilakukan, perlu dilakukan beberapa penelitian lebih lanjut;

1. Perlu dilakukan analisis metode pendaftaran pengguna baru sehingga kata sandi yang dimasukkan tidak dapat dicuri dengan mudah,
2. Perlu dilakukan penelitian penggunaan *salt* sebagai kunci unik untuk masing-masing pengguna yang tersimpan dalam basis data. Penelitian ini kemudian dibandingkan dengan sistem enkripsi yang dilakukan pada penelitian yang telah dilakukan sehingga diketahui sistem enkripsi mana yang lebih sesuai,
3. Perlu dilakukan penelitian perbandingan penggunaan metode CHAP dengan algoritma enkripsi HMAC MD5 dibandingkan dengan metode HTTPS sehingga diketahui kelebihan dan kekurangan masing-masing metode.

DAFTAR PUSTAKA

1. Burnett, M., *Hacking the Code: ASP.NET Web Application Security*, California, 2005
2. Holzner, S., *Inside JavaScript*, Indianapolis, 2002
3. Johnston, P. A., *Login System*, http://pajhome.org.uk, Oktober 2005
4. Krawczyk, H., *Keyed-Hashing for Message Authentication*, http://www.ietf.org/rfc/rfc2104.txt, Februari 1997
5. Rickyanto, I., *Membuat Aplikasi Web dengan ASP.NET*, Jakarta, 2003
6. Satoto, K. I., *Tentang Sistem Informasi Akademik Fakultas Teknik Undip*, http://sia-ft.undip.ac.id/, Maret 2006