ANALISIS FORENSIK SERANGAN SQL INJECTION MENGGUNAKAN METODE STATIS FORENSIK

Imam Riadi, Rusydi Umar, Wasito Sukarno.
Jurusan Teknik Informatika, Program Pascasarjana,
Universitas Ahmad Dahlan (UAD)
Yogyakarta, Indonesia
Email: wasitoelektro@gmail.com

Abstrak-**Website Kemahasiswaan Universitas Ahmad Dahlan merupakan website yang digunakan sebagai media dan sarana informasi komunikasi Mahasiswa. Sehingga website ini dapat diakses secara luas dan memerlukan keamanan website. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap keamanan website tersebut. Salah satunya adalah dengan melakukan SQL (Structure Query Language) Injection. SQL Injection adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi[3]. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Dengan menggunakan SQL Injection ini maka akan dapat mengetahui apakah website tersebut pernah atau sedang ada penyerang yang memanipulasi data. Berdasarkan hasil penelitian terdapat beberapa ip address yang masuk melalui celah keamanan website kemahasiswaan. Penyerang menggunakan tool SQL Injection.[1]**

Kata kunci: SQL Injection, keamanan website

I. PENDAHULUAN

Penggunaan media informasi internet melalui Website memerlukan adanya keamanan yang dapat menutup celah keamanan dalam website tersebut. Dalam penelitian ini menganalisis celah keamanan terhadap serangan SQL Injection pada website kemahasiswaan Universitas Ahmad Dahlan yaitu *bimawa.uad.ac.id*. menurut pihak Administrator yang mengelola Website tersebut belum pernah ada penyusup yang mengubah atau memanipulasi data. Yang pernah ada adalah penyusup yang masuk tetapi tidak memanipulasi data dan hanya melihat isi dari website kemahasiswaan tersebut. SQL Injection adalah aksi hacking yang dilakukan di aplikasi client dengan memodifikasi perintah SQL yang ada di memori aplikasi client dan merupakan teknik mengeksploitasi web aplikasi yang didalamnya menggunakan database untuk penyimpanan data. Berdasarkan definisi tersebut maka serangan ini sangat berbahaya karena penyerang berhasil memasuki sistem database dan dapat memanipulasi data. Website kemahasiswaan di Universitas Ahmad Dahlan digunakan untuk memberikan pelayanan informasi kepada mahasiswa. Dalam hal ini website tersebut dapat diakses oleh banyak kalangan sehingga website tersebut rentan terhadap penyusup yang akan memanipulasi data kemahasiswaan.

Umumnya pengamanan data dikategorikan dua macam yaitu

Pencegahan (Presentif) dilakukan agar data tidak rusak atau hilang.

Pemulihan (Recovery) dilakuakn apabila data sudah terkena virus dan celah keamanan yang berlubang sudah dimasuki penyusup.[4]

II. METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah dengan menggunakan metode statis forensik. Sehingga dapat dilakukan pada saat komputer tidak terkoneksi dengan internet.

Digital Forensik adalah aplikasi dalam ilmu pengetahuan dan teknologi komputer untuk analisis dan pemeriksaan barang bukti digital dalam keterkaitannya dengan kejahatan. [5]

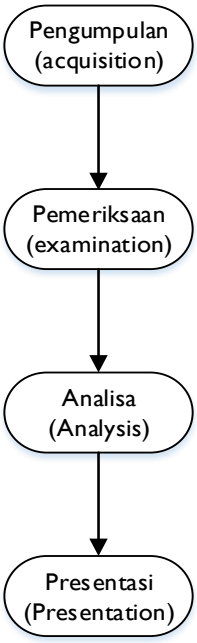
SQL Injection adalah teknik yang dilakukan oleh penyusup untuk masuk ke dalam database website tanpa menggunakan password terlebih dahulu. [6]

Dalam melakukan penelitian ini diperlukan 4 tahapan yaitu:

1. Pengumpulan (acquisition)
   Tahap ini dilakukan dengan meneliti untuk menemukan bukti-bukti yang mendukung penyelidikan. Media digital yang dapat dijadikan sebagai barang bukti adalah sistem komputer, media penyimpanan (misal Flash Disk, Hardisk, e mail, handphone, sms, log file, smart card.
2. Pemeriksaan (examination)
   Mencari data yang tersembunyi atau yang dihapus dan mendokumentasikannya media dalam mencari data adalah dengan menggunakan software (misal:OS Forensic, Helix3, Xways, Belkasoft).
3. Analisa (Analysis)
   Melakukan analisa terhadap bukti-bukti yang telah ditemukan. Analisis ini dapat dilakukan pada data sebagai berikut: alamat URL yang telah dikunjungi, pesan email, format ekstensi yang dipakai, dokumen spreedsheet yang dipakai, file yang dihapus atau diformat, password, registry windows, hidden file, log event viewers dan log aplikasi serta pengecekan metadata.

ISBN: 978-602-19568-2-3

4. Presentasi (Presentation)
   Menguraikan secara detail laporan hasil penyelidikan dengan bukti-bukti yang sudah diproses secara mendalam dan dapat dipertanggungjawabkan secara ilmiah di hadapan pihak yang berwenang. Beberapa hal penting yang dicantumkan dalam presentasi adalah sebagai berikut:
   a) Tanggal dan waktu terjadinya pelanggaran
   b) Tanggal dan waktu saat investigasi
   c) Permasalahan yang terjadi
   d) Waktu analisa laporan
   e) Ditemukannya bukti
   f) Teknik yang digunakan
   g) Bantuan orang lain[1]

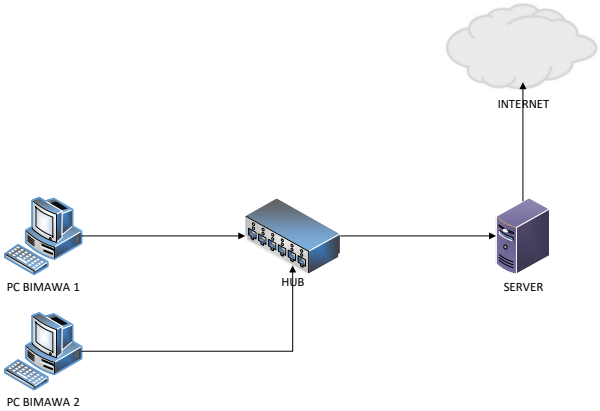


Gambar 1. Proses Analisis forensic[1]

III. HASIL DAN PEMBAHASAN

Analisis penanganan SQL Injection dilakukan dengan cara:

a) Saat menginisialisasi sebuah variable di kode pemrograman atau kode program dari database query dilakukan validasi terhadap karakter berbahaya Membatasi input yang panjang sehingga penyerang tidak dapat menginjeksi ke dalam form login
b) Mengatasi error yang keluar dari database dengan cara menghilangkan atau menyembunyikan kode program.[2]



Gambar 2 Konfigurasi jaringan Komputer di computer kemahasiswaan

IV. KESIMPULAN

Setelah dilakukan penelitian ini maka dapat disimpulkan sebagai berikut:

1. Analisis menggunakan website bimawa.uad.ac.id dengan metode statis forensik.
2. Hasil analisis penyerang menggunakan SQL Injection untuk masuk ke celah keamanan.
3. Dari hasil pengamatan yang dilakukan dengan metode statis forensic Penyerang hanya melihat isi data belum mengubah database yang ada di website.

V. DAFTAR PUSTAKA

[1] Resi Utami Putri dan Jazi Eko Istiyanto Program Studi S2 Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Gadjah Mada, "Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada server Universitas Gadjah Mada" jurnal IJCCS Vol. 6 No. 2 July 2012 pp. 101-112.
[2] Rudi Samuel Pardosi Cyber Security Research Center. " Kali Linux Top Hacking"
[3] Rahajeng Ellysa, Muhammad Husni dan Baskoro Adi Pratomo Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh November (ITS). "Pendeteksi Serangan SQL Injection Menggunakan Algoritma SQL Injection Free Secure pada Aplikasi Web". JurnalTeknikPOMITS Vol. 2 No. 1 Tahun 2013.
[4] Paryati jurusan Teknik Informatika UPN Veteran Yogyakarta "Keamanan Sistem Informasi" Seminar Nasional Informatika 2008.
[5] Yeni Dwi Rahayu, Yudi Prayudi Magister Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia. "Membangun Integrated Digital Forensics Investigation Framework (IDFIF) Menggunakan Metode Sequential logic" Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA) 15 Maret 2014.
[6] Moh. Dahlan, Ananstasya Latubessy, Mukhamad Nurkamid Program Studi Teknik Elektro Fakultas Teknik Universitsa Muria Kudus. "Analisa Keamanan Web Server terhadap Serangan Possibility SQL Injection". Prosiding SNATIF ke-2 Tahun 2015.

ISBN: 978-602-19568-2-3