INVESTIGASI FORENSIK SERANGAN WEBSITE SQL INJECTION MENGGUNAKAN METODE SCRIPTING PADA CRAWLTRACK

SKRIPSI

Oleh :

EXGO TRI ARIZKI
NPM. 1334010124

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2017

INVESTIGASI FORENSIK SERANGAN WEBSITE SQL INJECTION MENGGUNAKAN METODE SCRIPTING PADA CRAWLTRACK

SKRIPSI

Diajukan Untuk Memenuhi Sebagai Persyaratan
Dalam Memperoleh Gelar Sarjana Komputer
Program Studi Teknik Informatika

Oleh :

EXGO TRI ARIZKI
NPM. 1334010124

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2017

Judul	**: INVESTIGASI FORENSIK SERANGAN WEBSITE SQL INJECTION MENGGUNAKAN METODE SCRIPTING PADA CRAWLTRACK**
Penyusun	: Exgo Tri Arizki
Pembimbing I	: Eva Yulia P., S.Kom, M.Kom
Pembimbing II	: Kafi Ramadhan Borut, S.Kom, M.Kom

ABSTRAK

Keamanan website merupakan salah satu indikator penting dalam membangun sebuah website, berbicara tentang keamanan website tentu banyak sekali cara yang dilakukan *attacker* dalam menembus pertahanan sistem salah satunya dengan serangan *SQL Injection*. Dalam penelitian ini dilakukannya serangan terhadap website yang telah ditentukan untuk menguji kemanan website tersebut, selanjutnya dilakukan analisa dari pengujian terbsebut dan dari hasil analisa dapat diketahui metode serangan dan IP dari penyerang.

Dalam penelitian ini diimplementasikan pendeteksian serangan kepada sebuah website yang diserang melalui serangan *SQL Injection*. Serangan *SQL Injection* tersebut dilakukan sebagai uji coba serangan atas sistem keamanan Crawltrack. Menggunakan metode *scripting* pada Crawltrack merupakan cara terhubung antara halaman website dan *database* kepada sistem keamanan Crawltrack. Crawltrack yang bertindak sebagai keamanan dan pemblokiran serangan memberikan peran penting terhadap penelitian ini dengan cara memberikan informasi dari penyerangan sehingga dapat menutup kemungkinan serangan yang sama dikemudian hari.

Hasil dari penelitian ini berupa informasi penting mengenai detail serangan hingga identitas *attacker* melalui *IP address*, Informasi penting yang dihasilkan pada Crawltrack sendiri berupa laporan elektronik sehingga dapat disimpan dengan *file* atau dibuat dengan dokumen. Informasi tersebut dapat digunakan dalam bukti digital atas tindakan kriminal yang melanggar hukum melalui bukti digital forensik.

Keyword: Website, SQL Injection, Scripting, Crawltrack, Forensik

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah memberikan rahmat serta hidayah-Nya sehingga penyusunan laporan ini dapat diselesaikan.

Laporan ini disusun untuk tugas skripsi yang berjudul "**INVESTIGASI FORENSIK SERANGAN WEBSITE SQL INJECTION MENGGUNAKAN METODE SCRIPTING PADA CRAWLTRACK**".

Penulis menyadari bahwa laporan skripsi ini masih jauh dari kesempurnaan, atas segala kekurangan dan belum sempurnanya laporan skripsi ini, penulis sangat mengharapkan masukan, kritik, dan saran yang bersifat membangun kearah perbaikan dan penyempurnaan laporan ini.

Akhir kata penulis berharap semoga tugas skripsi ini dapat bermanfaat bagi semua pihak dan semoga amal baik yang telah diberikan kepada penulis mendapat balasan dari Tuhan Yang Maha Esa.

Surabaya, Mei 2017

Peneliti

UCAPAN TERIMA KASIH

Puji syukur atas ke hadirat Tuhan Yang Maha Esa yang telah memberikan bimbingan dan karunia-Nya, sehingga dapat terselesaikannya skripsi ini. Dengan terselesaikannya skripsi ini tidak terlepas pula bantuan dari banyak pihak yang telah memberi saran dan masukan dalam penyusunan. Dalam hal ini Peneliti mengucapkan terima kasih sebagai perwujudan rasa dan puji syukur atas terselesaikannya skripsi ini yang ditujukan kepada:

1. Kedua orang tua yang telah memberikan doa, kasih sayang, dana, serta semangat saat proses penelitian ini berlangsung.
2. Kepada kakak dan adik yang telah memberikan doa dan dukungan selama perkuliahan berlangsung hingga saat ini.
3. Kepada orang yang tersayang Fariza H.F.R. yang telah memberikan semangat dan dukungan selama perkuliahan hingga saat ini.
4. Prof. Dr. Ir Teguh Soedarto, MP selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Ibu Dr. Ir. Ni Ketut Sari, MT. Selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
6. Bapak Budi Nugroho, S.Kom, Msc. Selaku Ketua Program Studi Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
7. Ibu Eva Yulia P., S.Kom, M.Kom. selaku dosen pembimbing I pada skripsi ini, yang banyak memberikan masukan, dorongan dan saran pengembangan dalam proses skripsi ini.

8. Bapak Kafi Ramadhan Borut, S.Kom, M.Kom. selaku dosen pembimbing II pada skripsi ini, yang telah banyak memberikan saran, dorongan dan pembenahan dalam penyusunan laporan hingga terselesaikannya skripsi ini.
9. Kepada sahabat-sahabat saya Fajri M, Putu Bayu, Yohanes Agaphea, Fadhil Fermadhan, Tito dan teman-teman lainnya yang tidak bisa saya sebut satu-satu yang telah mendukung selama proses pembelajaran di Universitas Pembangunan Nasional "Veteran" Jawa Timur.
10. Kepada Zahran Rahardian yang selalu memberi saya kabar tentang berkas skripsi (*server* berkas skripsi).

Surabaya, Juni 2017

Peneliti

DAFTAR ISI

ABSTRAK i

KATA PENGANTAR ii

UCAPAN TERIMA KASIH iii

DAFTAR ISI v

DAFTAR GAMBAR viii

DAFTAR TABEL xi

BAB 1 PENDAHULUAN 1

1.1. Latar Belakang 1
1.2. Rumusan Masalah 4
1.3. Batasan Masalah 4
1.4. Tujuan Penelitian 5
1.5. Manfaat Penelitian 6
1.6. Metodologi 6
1.7. Sistematika Penulisan 8

BAB II TINJAUAN PUSTAKA 10

2.1. Penelitian Terdahulu 10
2.2. Website 10
2.3. Jaringan Komputer 12
2.4. *SQL Injection* 14
2.5. Keamanan Jaringan 15
2.6. SQLMAP 17
2.7. XAMPP 17
2.8. *Scripting* 19
2.9. CrawlTrack 19
2.10. Model Sistematis Investigasi Digital Forensik 20

BAB III ANALISIS DAN PERANCANGAN 23

3.1. Rancangan Skenario 23
3.1.1. Skenario Uji Coba Program *SQL Injection* 23

3.1.2. Skenario Uji Coba Manual Code *SQL Injection* 24
3.2. Spesifikasi Kebutuhan Sistem 26
3.3. Perancangan 29
3.3.1. *Flowchart* Alur mekanisme 29
3.3.2. *Flowchart* Alur Sistem 31
3.4. Rancangan Uji Coba Serangan 34
3.5. Analisa Rancangan Uji Coba Serangan *SQL Injection* 35
3.6. Rancangan Proses Investigasi Forensik 36
BAB IV IMPLEMENTASI DAN HASIL 39
4.1. Infrastruktur Crawltrack Menggunakan *Scripting Code* 39
4.2. Implementasi Sistem 40
4.3. Konfigurasi Interface pada *PC* utama 42
4.4. Konfigurasi VirtualBox 43
4.4.1. Konfigurasi *Interface* pada Virtualbox 43
4.4.2. Konfigurasi *Interface* pada Sistem Virtual 45
4.5. Konfigurasi *Web Server* 46
4.6. Konfigurasi Database di Web Server 47
4.7. Konfigurasi Database di Web Hosting 48
4.8. Konfigurasi Crawltrack 49
4.8.1. Instalasi Program Crawltrack 49
4.8.2. Konfigurasi *Scripting* Program Crawltrack 53
4.8.3. Konfigurasi Pendeteksian Serangan 54
4.9. Uji Coba Serangan *SQL Injection* 55
4.9.1. Uji Coba Serangan *SQL Injection* Tanpa Keamanan 55
4.9.2. Uji Coba Serangan *SQL Injection* Keamanan Opsi 1 71
4.9.3. Uji Coba Serangan *SQL Injection* Keamanan Opsi 2 78
4.10. Analisa Hasil Uji Coba Serangan *SQL Injection* 81
4.11. Proses Investigasi Forensik 82
BAB V KESIMPULAN DAN SARAN 86

5.1. Kesimpulan 86
5.2. Saran 86
DAFTAR PUSTAKA 88

DAFTAR GAMBAR

Gambar 2.1 Security Methodology 15
Gambar 2.2 *Systematic Digital Forensic Investigation Model (SRDFIM)* 20
Gambar 3.1 Rancangan uji coba program 23
Gambar 3.2 Rancangan Uji Coba Manual..... 25
Gambar 3.3 Flowchart sistem kerja Attacker 29
Gambar 3.4 Flowchart website yang tidak dilindungi SQL Inejction..... 31
Gambar 3.5 Flowchart website anti SQL Injection hanya merekam serangan ... 32
Gambar 3.6 Flowchart anti SQL Inejction merekam & memblokir serangan..... 33
Gambar 3.7 tampilan dari adds on hackbar dalam browser Google Chrome..... 34
Gambar 3.8 Tampilan dari program SQLMAP 34
Gambar 3.9 Tampilan dari Program Havij 35
Gambar 4.1 Infrastruktur Crawltrack menggunakan *scripting code* 39
Gambar 4.2 Tampilan login pada Crawltrack 40
Gambar 4.3 Tampilan menu utama pada Crawltrack..... 41
Gambar 4.4 Tampilan dari menu pendeteksian serangan..... 41
Gambar 4.5 Tampilan konfigurasi pada perangkat inti atau PC utama..... 42
Gambar 4.6 Konfigurasi interface OS kali linux pada virtualbox..... 44
Gambar 4.7 Konfigurasi interface OS windows 7 pada Virtualbox..... 44
Gambar 4.8 Konfigurasi interface pada sistem operasi virtual OS windows 7... 45
Gambar 4.9 Konfigurasi interface pada sistem operasi virtual OS Kali linux 46
Gambar 4.10 Konfigurasi interface pada web server XAMPP 46
Gambar 4.11 Konfigurasi database pada web server 47
Gambar 4.12 Konfigurasi database pada web hosting 48
Gambar 4.13 Konfigurasi penggubungan pengguna dan database..... 49
Gambar 4.14 konfigurasi instalasi pemilihan bahasa 49
Gambar 4.15 Konfigurasi petunjuk instalasi program..... 50
Gambar 4.16 Konfigurasi instalasi penghubung ke database..... 50
Gambar 4.17 Konfigurasi instalasi penghubung database selesai..... 51
Gambar 4.18 Konfigurasi instalasi pengaturan website 51
Gambar 4.19 Konfigurasi instalasi pengaturan website selesai 51
Gambar 4.20 Konfigurasi instalasi pembuatan akun administrator 52
Gambar 4.21 Konfigurasi instalasi pembuatan akun administrator selesai..... 52
Gambar 4.22 Konfigurasi scripting pada Crawltrack..... 53
Gambar 4.23 Konfigurasi scripting pada halaman website..... 54
Gambar 4.24 Konfigurasi pendeteksian serangan pada crawltrack..... 54
Gambar 4.25 code injection ke dalam URL pada parameter web server 56
Gambar 4.26 Memasukkan target serangan web server pada Havij..... 57

Gambar 4.27 Mendapatkan Informasi database web server 57
Gambar 4.28 Mencari tabel yang dianggap penting di database web server 58
Gambar 4.29 Mencari isi kolom dari database web server..... 58
Gambar 4.30 Membuka isi dari kolom pada database web server 59
Gambar 4.31 Tahap masuk kedalam database melalui parameter web server 59
Gambar 4.32 Proses scanning URL untuk mencari celah web server..... 59
Gambar 4.33 Proses scanning menentukan versi MYSQL web server..... 60
Gambar 4.34 Ditemukan kelemahan dengan parameter artikel web server 60
Gambar 4.35 Log dari proses scanning database web server..... 61
Gambar 4.36 Tampilan dari kolom database yang ada pada web server 61
Gambar 4.37 Tahap masuk kedalam database melalui tabel web server 61
Gambar 4.38 Tampilan dari isi tabel pada database web server 62
Gambar 4.39 Tahap masuk kedalam database melalui kolom web server..... 62
Gambar 4.40 Tampilan dari isi kolom pada database web server..... 62
Gambar 4.41 Tahap membuka isi dari kolom pada web server 63
Gambar 4.42 Petunjuk untuk memilih melakukan crack katasandi atau tidak.... 63
Gambar 4.43 Tampilan akhir dari serangan SQL Injection pada SQLMAP..... 63
Gambar 4.44 code injection ke dalam URL pada parameter web hosting 64
Gambar 4.45 Memasukkan target serangan pada Havij 64
Gambar 4.46 Mendapatkan Informasi database web hosting..... 65
Gambar 4.47 Mencari tabel yang dianggap penting di database web hosting 65
Gambar 4.48 Mencari isi kolom dari database web hosting 66
Gambar 4.49 Membuka isi dari kolom pada database web hosting..... 66
Gambar 4.50 Parameter URL yang diduga kelemahan pada web hosting..... 67
Gambar 4.51 Tahap masuk kedalam database melalui parameter web hosting .. 67
Gambar 4.52 Proses scanning URL untuk mencari celah web hosting..... 67
Gambar 4.53 Proses scanning penggunaan versi MYSQL web server..... 68
Gambar 4.54 Ditemukan kelemahan dengan parameter artikel web hosting..... 68
Gambar 4.55 Log dari proses scanning database web hosting..... 68
Gambar 4.56 Tampilan dari kolom database yang ada pada web hosting 69
Gambar 4.57 Tahap masuk kedalam database melalui tabel web hosting 69
Gambar 4.58 Tampilan dari isi tabel pada database web hosting 69
Gambar 4.59 Tahap masuk kedalam database melalui kolom web hosting..... 70
Gambar 4.60 Tampilan dari isi kolom pada database web hosting..... 70
Gambar 4.61 Tahap membuka isi dari kolom pada web hosting 70
Gambar 4.62 Petunjuk untuk memilih melakukan crack katasandi atau tidak.... 70
Gambar 4.63 Tampilan akhir dari serangan SQL Injection pada SQLMAP..... 71
Gambar 4.64 Keamanan opsi 1 hanya merekam serangan pada web server..... 72
Gambar 4.65 Hasil rekaman dari manual code pada web server..... 72
Gambar 4.66 keamanan hanya merekam serangan pada uji coba Havij 73
Gambar 4.67 IP address dari windows 7 serangan web server opsi 1..... 73
Gambar 4.68 Identitas Attacker havij berhasil direkam program Crawltrack..... 74

Gambar 4.69 keamanan hanya merekam serangan pada uji coba SQLMAP 75
Gambar 4.70 IP address dari kali linux serangan web server opsi 1 75
Gambar 4.71 Identitas Attacker SQLMAP berhasil direkam Crawltrack 76
Gambar 4.72 merekam dan memblokir serangan pada uji coba manual code 79
Gambar 4.73 Hasil blokir serangan dari manual code web server 79
Gambar 4.74 Hasil rekaman serangan dari manual code web server 79
Gambar 4.75 Bukti transaksi Hosting 83

DAFTAR TABEL

Tabel 3.1 Daftar kebutuhan penelitian 26
Tabel 4. 1 Perbandingan Tanpa Keamanan dan Keamanan Opsi 1 77
Tabel 4. 2 Perbandingan Keamanan Opsi 1 dan Keamanan Opsi 2 80