PENCEGAHAN SERANGAN SQL *INJECTION* DENGAN MELAKUKAN ENKRIPSI PARAMETER *UNIFORM RESOURCES LOCATOR* (URL) MENGGUNAKAN ALGORITMA KRIPTOGRAFI HASH DAN *FILTER ESCAPE STRING*

SKRIPSI

Ghozi Ihza Humamda

1710511010

PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2021

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Ghozi Ihza Humamda

NIM : 1710511010

Tanggal : 30 juni 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 30 Juni 2021

Yang Menyatakan,

(Ghozi Ihza Humamda)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Ghozi Ihza Humamda

NIM : 1710511010

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti NonEkslusif (Non-Exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul:

PENCEGAHAN SERANGAN SQL *INJECTION* DENGAN MELAKUKAN ENKRIPSI PARAMETER *UNIFORM RESOURCES LOCATOR* (URL) MENGGUNAKAN ALGORITMA KRIPTOGRAFI HASH DAN *FILTER ESCAPE STRING*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 30 Juni 2021

Yang Menyatakan,

(Ghozi Ihza Humamda)

LEMBAR PERSETUJUAN

Dengan ini menyatakan bahwa proposal berikut:

Nama : Ghozi Ihza Humamda

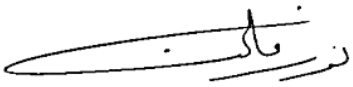
NIM : 1710511010

Program Studi : Informatika

Judul : Pencegahan Serangan SQL *Injection* Dengan Melakukan Enkripsi Parameter Uniform Resources Locator (URL) Menggunakan Algoritma Kriptografi HASH dan *Filter Escape String*

Sebagai bagian persyaratan yang diperlukan untuk mengikuti ujian Sidang Tugas Akhir/Skripsi pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Menyetujui,

Dosen Pembimbing 1	Dosen Pembimbing 2
	
(Henki Bayu Seta, S.Kom., MTI)	(Noor Falih, S.Kom., M.T)

Mengetahui,

Ketua Program Studi

(Yuni Widiastiwi, S.Kom., Msi.)

Ditetapkan : Jakarta

Tanggal Persetujuan : 30 Juni 2021

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut :

Nama : Ghozi Ihza Humamda

NIM : 1710511010

Program Studi : Informatika

Judul Skripsi : Pencegahan Serangan SQL *Injection* Dengan Melakukan Enkripsi Parameter Uniform Resources Locator (URL) Menggunakan Algoritma Kriptografi HASH dan *Filter Escape String.*

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Yuni Widiastiwi, S.Kom., Msi.	**Bayu Hananto, S.Kom, M.Kom.**
Penguji I	Penguji II
Henki Bayu Seta, S.Kom., MTI.	**Noor Falih, S.Kom., M.T.**
Pembimbing I	Pembimbing II
Dr. Ermatita, M.Kom.	**Yuni Widiastiwi, S.Kom., Msi.**
Dekan	Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Pengesahan : 22 Juli 2021

PENCEGAHAN SERANGAN SQL *INJECTION* DENGAN MELAKUKAN ENKRIPSI PARAMETER *UNIFORM RESOURCES LOCATOR* (URL) MENGGUNAKAN ALGORITMA KRIPTOGRAFI HASH DAN *FILTER* ESCAPE STRING

Ghozi Ihza Humamda

ABSTRAK

SQL *Injection* merupakan salah satu jenis atau teknik serangan *website* yang paling sering dijumpai bahkan menurut *website* owasp.org teknik atau serangan berjenis *Injection* ini masih menempati posisi teratas, cara kerja dari serangan ini yaitu dengan memanfaatkan celah keamanan yang terjadi pada layer basis data dari sebuah aplikasi. Hal tersebut dapat terjadi karena data yang diinputkan oleh pengguna akan divalidasi dan dimuat dalam baris perintah *query* SQL. Dengan demikian data tersebut akan menjadi bagian dari query SQL. Serangan ini memberikan dampak yang cukup serius ini dikarenakan pada serangan berjenis injeksi ini langsung menargetkan sebuah *database* dari suatu *website*. Terdapat banyak cara untuk mencegah serangan berjenis injeksi ini, salah satunya dengan menggunakan Enkripsi pada parameter *Uniform Resource Locator* (URL) dan menerapkan *filter Escape String*, selain mudah diterapkan sebuah salah satu kelebihan dari enkripsi juga dapat dimanfaatkan untuk menyembunyikan parameter asli dari URL, sehingga penyerang kesulitan untuk memodifikasi URL tersebut. Hasil yang didapat dari pengujian dengan menerapkan metode Enkripsi parameter URL dan *filter Escape String* serangan SQL *Injection* tidak berhasil menembus *database website*.

Kata Kunci : SQL *Injection*, Enkripsi, *Uniform Resources Locator* (URL), *Escape String*

SQL INJECTION ATTACK PREVENTION BY ENCRYPTING UNIFORM RESOURCES LOCATOR (URL) PARAMETER USING CRYPTOGRAPHIC HASH ALGORITHM AND FILTER ESCAPE STRING

Ghozi Ihza Humamda

ABSTRACT

SQL Injection is one of the most common types or techniques of website attacks even according to the website owasp.org techniques or attacks of this type of Injection still occupy the top position, the way this attack works is by utilizing security gaps that occur in the database layer of an application. This can happen because the data inputted by the user will be validated and loaded in the SQL query command line. Thus the data will be part of the SQL query. This attack has a serious impact because this type of Injection attack directly targets a database of a website. There are many ways to prevent attacks of this type of Injection, one of which is by using Encryption in uniform resource locator (URL) parameters and applying the Escape String filter, in addition to being easy to implement one of the advantages of encryption can also be used to hide the original parameters of the URL, making it difficult for attackers to modify the URL. Results obtained from testing by applying url parameter encryption method and Escape String filter SQL Injection attack did not successfully penetrate the website database.

Keywords : SQL Injection, Encryption, Uniform Resources Locator (URL), Escape String

KATA PENGANTAR

Penulis ucapkan rasa puji dan syukur kehadirat Allah S.W.T karena atas berkat rahmat dan hidayah-Nya, penulis dapat menyelesaikan skripsi di pertengahan masa pandemi COVID-19 ini. Adapun judul untuk skripsi ini adalah:

PENCEGAHAN SERANGAN SQL *INJECTION* DENGAN MELAKUKAN ENKRIPSI PARAMETER *UNIFORM RESOURCES LOCATOR* (URL) MENGGUNAKAN ALGORITMA KRIPTOGRAFI HASH DAN *FILTER* ESCAPE STRING

Selanjutnya penulis ingin mengucapkan banyak – banyak terima kasih yang kepada pihak-pihak yang selalu sabar untuk menemani, membimbing, serta memberi saran terbaik yang mana tanpa kehadiran mereka, mungkin penulisan ini tidak akan pernah selesai seperti sekarang ini. Adapun pihak terkait antara lain:

1. Kedua orang tua yang telah memberi dukungan dan semangat serta mendoakan penulis agar dapat menyelesaikan naskah skripsi ini tanpa kendala.
2. Bapak Henki Bayu Seta, S.Kom., MTI selaku dosen pembimbing satu yang membimbing penulis dalam menyusun naskah skripsi ini.
3. Bapak Noor Falih, S.Kom., M.T. selaku dosen pembimbing dua yang juga telah membimbing dalam penulisan naskah skripsi ini.
4. Ibu Yuni Widiastiwi., S.Kom., M.Si selaku dosen penguji yang telah memberi arahan dan saran komprehensif.
5. Bapak Bayu Hananto, S.Kom., M.Kom. selaku dosen penguji yang telah memberi arahan dan saran komprehensif.
6. Bapak/Ibu dosen Informatika Universitas Pembangunan Nasional Veteran Jakarta yang telah memberi ilmu yang banyak dan bermanfaat.
7. Teman-teman semua di Tim NaQoS yang telah sabar dan selalu memberikan dukungan moral serta menyediakan waktu untuk melakukan diskusi tentang tugas akhir ini.

Kemudian penulis juga menyadari bahwa penyusunan skripsi ini masih jauh dari kata sempurna, namun penulis berharap agar pihak yang membaca naskah ini mendapatkan ilmu yang dapat digunakan kelak. Dan penulis juga berharap atas kritik dan saran yang konstruktif dari pembaca.

Akhir kata, semoga Allah S.W.T memberi balasan yang berlipat ganda atas kebaikan dan jasa kepada semua pihak yang turut membantu penyelesaian naskah skripsi ini. Semoga tujuan daripada penulisan skripsi ini dapat tercapai sesuai dengan harapan.

DAFTAR ISI

PERNYATAAN ORISINALITAS ii

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS iii

LEMBAR PERSETUJUAN iv

LEMBAR PENGESAHAN v

ABSTRAK vi

ABSTRACT vii

KATA PENGANTAR viii

DAFTAR ISI x

DAFTAR GAMBAR xiii

DAFTAR TABEL xiv

BAB 1 PENDAHULUAN 1

1.1. Latar Belakang 1

1.2. Rumusan Masalah 3

1.3. Tujuan Penelitian 3

1.4. Manfaat Penelitian 4

1.5. Batasan Masalah 4

1.6. Luaran Yang Diharapkan 4

1.7. Sistematika Penulisan 4

BAB 2 LANDASAN TEORI 6

2.1. *Website* 6

2.1.1. Protokol HTTP 6

2.1.2. URL 7

2.2. *Database* & *My*SQL 7
2.3. Keamanan 8
2.4. Kriptografi 8
2.4.1. Enkripsi & Fungsi Hash 9
2.4.2. MD5 & Cara Kerja MD5 9
2.5. Serangan Siber & Macam – Macam Serangan Siber 11
2.6. SQL *Injection* & Cara Kerja SQL *Injection* 11
2.7. SQLMap 13
2.8. *Filter* Escape String 13
2.9. Penelitian Terkait 14
BAB 3 METODOLOGI PENELITIAN 19
3.1. Kerangka Pikir 19
3.1.1. Identifikasi Masalah 20
3.1.2. Studi Literatur 20
3.1.3. Perancangan Perangkat Lunak 21
3.1.4. Flowchart Algoritma Enkripsi MD5 22
3.1.5. Pengujian Sistem 23
3.1.6. Dokumentasi 24
3.2. Alat Bantu Penelitian 24
3.2.1 Perangkat Keras 24
3.2.2 Perangkat Lunak 25
3.3. Jadwal Penelitian 25
BAB 4 PEMBAHASAN 26
4.1. Analisa Kerentanan 26

4.1.1. Pengujian Pertama 27
4.1.2. Analisa *Source code* 38
4.1.3. Pengujian Kedua 39
4.1.4. Analisa *Source code* 46
4.2. Pencegahan Serangan SQL *Injection* 47
4.2.1. Menerapkan *Filter Escape String* 47
4.2.2. Menambahkan Teknik Scripting 48
4.2.3. Menerapkan *Filter* Regular Expression 48
4.3. Penerapan Metode Untuk Pencegahan SQL *Injection* 48
4.3.1. Enkripsi Parameter Url Dengan Menggunakan MD5. 49
4.3.2. Penerapan *Filter* Escape String 52
4.4. Pengujian Ketiga 53
4.4.1. Bagian Pertama 54
4.4.2. Bagian Kedua 57
4.5. Hasil Keseluruhan Pengujian 61
BAB 5 PENUTUP 65
5.1. Kesimpulan 65
5.2. Saran 66
DAFTAR PUSTAKA 67
RIWAYAT HIDUP 70
LAMPIRAN 72

DAFTAR GAMBAR

Gambar 1 Ilustrasi Serangan SQL *Injection* 12
Gambar 2 Cara Kerja *Filter* Escape String..... 14
Gambar 3 Diagram Alir Kerangka Pikir Penelitian 19
Gambar 4 Diagram Alir Perangkat Lunak 21
Gambar 5 Flowchart Enkripsi MD5 22
Gambar 6 Skema Pengujian Sistem 23
Gambar 7 Halaman Utama *Website* 28
Gambar 8 Halaman Show URL Tidak Terenkripsi 29
Gambar 9 Pengujian Apakah *Website* Vulnerable Serangan SQL*Injection* 29
Gambar 10 Melakukan Enumerasi 29
Gambar 11 Dump Data Dari *Database* 30
Gambar 12 Halaman Show URL Tidak Terenkripsi 32
Gambar 13 Halaman Show URL Terenkripsi 39
Gambar 14 Diagram Alir Penerapan Metode Untuk Mencegah SQL*Injection*.. 48
Gambar 15 *Database Website* Dengan URL Terenkripsi 51

DAFTAR TABEL

Tabel 1 Penelitian Terkait 16
Tabel 2 Jadwal Penelitian 25
Tabel 3 *Payload* Yang Di Ujicoba 27
Tabel 4 Hasil Dari Setiap Pengujian *Payload* 31
Tabel 5 Hasil Serangan SQLMap *Website* Polos 37
Tabel 6 Hasil Serangan SQLMap *Website* Parameter URL Ter-enkripsi 45
Tabel 7 Hasil Serangan SQLMap *Website* Parameter URL Ter-enkripsi dan Memiliki *Filter* Escape String Dengan Performance Default 57
Tabel 8 Hasil Serangan SQLMap *Website* Parameter URL Ter-enkripsi dan Memiliki *Filter* Escape String Dengan Performance Maksimal 61
Tabel 9 Hasil Keseluruhan Pengujian 61