JIIFKOM (Jurnal Ilmiah Informatika & Komputer) STTR Cepu
E-Mail: jiifkom@sttrcepu.ac.id

Analisis Serangan dan Keamanan pada SQL Injection: Sebuah Review Sistematik

Tino Imam Maulana Pratama[1], Muhammad Danni Fawwas Songida[2], Indra Gunawan[3*]

Jurusan Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe [12]
Jurusan Informatika Sekolah Tinggi Teknologi Ronggolawe [3]

[*]Email: igunsttr@gmail.com

Tentang naskah:
-diterima, 14 Jun 2022
-direview, 27 Jun 2022
-diterbitkan, 1 Jul 2022

Kata kunci: SQL Injection; Analisis; Review Sistematik

Intisari

Situsweb merupakan salah satu layanan informasi yang banyak diakses oleh pengguna internet di dunia. Sebagai salah satu layanan informasi maka perlu dibangun situsweb yang mampu menangani permintaan (request) dari banyak pengguna dengan baik (reliable). 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. Metode SQL injection digunakan untuk memasukan perintah SQL sebagai input pada suatu website untuk mendapatkan akses ke dalam basis data. Jika basis data website dapat diakses, maka seorang hacker dapat dengan mudah mencuri berbagai data rahasia, bahkan dapat memanupulasi atau merusak data pada website tersebut

Keyword: *SQL Injection; Analysis; Systematic Review*

Abstract

The website is one of the most widely accessed information services by internet users in the world. As an information service, it is necessary to build a website that is able to handle requests from many users reliably. SQL Injection is a hacking action that is carried out in the client application by modifying the SQL commands that are in the client application memory and is a technique for exploiting web applications which use a database for data storage. SQL injection method is used to enter SQL commands as input on a website to gain access to the database. If the website database can be accessed, then a hacker can easily steal various confidential data, and can even manipulate or destroy data on the website

1. Pendahuluan

Pengembangan Situs web ini saat ini merupakan salah satu layanan informasi yang paling banyak digunakan oleh pengguna Internet di seluruh dunia. Sebagai sebuah layanan informasi, perlu dibangun sebuah website yang pasti dapat menjawab permintaan dari banyak pengguna. Pada dasarnya, sebuah situs web memiliki empat elemen dasar. Yaitu, browser, server, URL, halaman. Server web berisi halaman web yang berisi informasi dan dokumen yang ingin atau perlu didistribusikan oleh pengguna. (Azhar Andhika Putra, 2020)

Ancaman keamanan terhadap sistem Anda dan risiko serangan dapat berasal dari tiga aspek: integritas, kerahasiaan, dan ketersediaan. Oleh karena itu, penting untuk melindungi sistem berbasis digital Anda dari ketiga hal tersebut. (Gunawan, 2021).

Salah satu jenis risiko ini adalah injeksi SQL. Ini adalah tindakan peretasan yang dilakukan oleh aplikasi klien dengan memodifikasi perintah SQL di memori aplikasi klien yang merupakan eksploitasi aplikasi web yang membahayakan database yang digunakan untuk penyimpanan data. Dengan definisi ini, penyerang bisa membobol sistem database dan memanipulasi data, membuat serangan ini sangat berbahaya. (Wasito Sukarno, 2020)

Metode SQL injection digunakan untuk memasukkan perintah SQL sebagai input pada sebuah website untuk mengakses database. Dengan akses ke database sebuah situs web, peretas dapat dengan mudah mencuri berbagai data sensitif dan memanipulasi atau bahkan menghancurkan data di situs web tersebut. Salah satu cara untuk melindungi website Anda dari serangan SQL injection adalah melalui ilmu kriptografi. Ilmu kriptografi memungkinkan URL situs web dipalsukan sebagai kode atau kata sandi yang tidak dapat dibaca oleh siapa pun untuk mencegah serangan injeksi SQL pada situs web. (Azis Pratama Nugraha, 2017)

Kunjungan ke situs Cve Details melaporkan bahwa dalam waktu satu tahun pada tahun 2021, ditemukan bahwa jumlah total serangan injeksi SQL yang dilaporkan mencapai 738 hari.

Oleh karena itu, penulisan penelitian ini dimaksudkan untuk melakukan studi tinjauan sistematis berdasarkan studi penelitian lain tentang injeksi SQL. Dalam menulis tinjauan sistematis ini, penulis lebih dari sekadar mengungkapkan pendapatnya tentang analitik dan data grup, menjelaskan cara menangani serangan injeksi SQL dan bagaimana serangan ini mengeksploitasi kerentanan situs web.

2. Kerangka Teori

Survei yang kami kumpulkan berasal dari Google Scholar, yang dapat diakses di web dan dapat diperoleh tanpa persyaratan. Selain itu, penulis mencari referensi penelitian.

2.1. Pemilihan Studi

1) Pencarian kata kunci, dipilih sesuai dengan minat penelitian penulis dalam meninjau serangan SQL Injection yang sesuai sebagai metode perlindungannya. Kata kunci yang digunakan dalam pencarian penelitian pada database yang disebutkan yaitu;" Teknik SQL Injection", "Ancaman SQL Injection", "Eksploitasi SQL Injection", "Keamaan Website".

2) Eksplorasi dan pemilihan judul, abstrak, dan kata kunci dari penelitian yang diidentifikasi dilakukan berdasarkan kriteria kelayakan.

3) Pembacaan lengkap atau sebagian penelitian yang memenuhi kriteria

kelayakan dilakukan untuk menentukan apakah penelitian tersebut layak masuk dalam tinjauan.

4) Daftar referensi penelitian ditelaah untuk menemukan studi yang relevan.

2.2. Pengumpulan Data

Pengumpulan data dilakukan secara manual dengan menggunakan alat bantu tabel ekstraksi data yang terdiri dari judul, penulis, tahun, nama jurnal/rapat, jenis penelitian, topik, metode penelitian, hasil pembahasan, dan kesimpulan. Studi yang relevan atau berpotensi terkait dievaluasi bersama. Peringkat terdiri dari membaca teks lengkap dan data yang diekstraksi. Perbedaan itu diselesaikan melalui diskusi antara penulis.

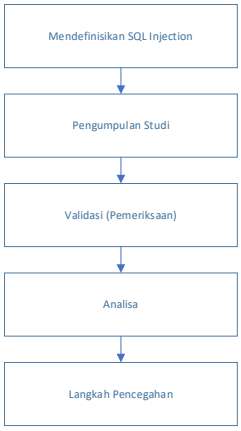
2.3. Pemilihan Item Data

Informasi yang diambil dari setiap penelitian terdiri dari:

1) Ancaman serangan SQL Injection; 2) Analisis serangan SQL Injection; 3) Teknik Eksploitasi SQL Injection; 4) Metode langkah penangan serangan SQL Injection

3. Metodologi

Terdapat beberapa langkah dalam penelitian ini yaitu dapat dilihat pada Gambar 1 dibawah ini:



Gambar 1 Metodologi Penelitian

4. Hasil dan Pembahasan

4.1 Seleksi Jurnal

Hasil pencarian database Google Shooter yang Anda pilih memberikan total 10 studi Indonesia dari tahun 2017 hingga 2021 yang cocok dengan kata kunci yang ingin Anda analisis. Akhirnya, enam studi dipilih yang memenuhi kriteria kelayakan dan menjadi sumber untuk tinjauan sistematis ini.

4.2 Karakteristik Jurnal

Informasi rinci dari enam studi / jurnal yang dipilih ada di Tabel 1 untuk ekstraksi data akhir. Ekstraksi data akhir ini merupakan tabel ekstraksi data yang hanya berisi penelitian-penelitian yang dipilih berdasarkan kriteria yang ada dalam proses pemilihan penelitian.

Table 1.1 Ekstrasi Data Final

No	Penulis	Nama Jurnal/Konferensi	Tipe Penelitian	Topik	Metode	Hasil Pembahasan	Kesimpulan
1.	Riadi, Rusydi & Wasito, 2020	Analisa Serangan SQL Injection Menggunakan Metode Statis Forensik	Review Penelitian	Digital Forensik dapat diterapkan untuk tindak analisis kejahatan SQL Injection	Statis Forensik	Variabel dalam kode program kueri basis data, validasi karakter jahat dilakukan. Membatasi panjang input sehingga penyerang tidak dapat memasukkannya ke dalam formulir login. Teknologi : • Digital Forensik	Pencegahan SQL Injection dapat dilakukan dengan menerapkan form validasi pada input login.
2.	Azhar, 2020	Analisis Kerentanan Pada Situs www.unisti.ac.id	Review Jurnal	Scanning Kerentanan Website Menggunakan Tools	Action Research	Scanning tool digunakan untuk menemukan kerentanan SQL Injection maupun Cross Site Scripting(XSS) pada situsweb. Teknologi : Webcruiser	Aplikasi scanner dapat digunakan untuk analisis kerentanan yang ada pada suatu website untuk dilakukan tindakan pencegahan dan perbaikan.
3	Nugraha & Gunandhi, 2016	Penerapan Kriptografi Base64 Untuk Keamanan URL Website Dari SQL Injection	Review Jurnal	Peran kriptografi Base 64 untuk keamanan data.	Kualitatif	Algoritma Base64 dapat diterapkan untuk mengatasi kebocoran database.	Algoritma Base64 dapat mengidentifikasi kerentanan Web dari SQLi.
4.	Muslih, Fitri & Radiah, 2019	Pentration Testing Tool Untuk Menguji Kerentanan SQL Injection Secara Otomastis Berbasis Web	Review Jurnal	Tools Penguji kerentanan website	Studi Literatur	Pengujian celah keamanan ini berupa analisis terhadap website yang akan diuji dengan tools scaning.	Celah SQL Injection dapat ditemukan beserta celah keamanan website lainya.

5.	Putri & Istiyanto	Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada	Review Jurnal	Studi Digital Forensik Jaringan UGM pada kasus serangan SQL Injection		Proses Forensik	Pada penelitian forensik jaringan di UGM dilakukan dengan mengambil data pada IDS Snort yang merupakan sistem pendeteksi penyusup pada jaringan
6.	Wiguna Prabowo Ananda, 2020	Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website	Review Jurnal	Metode web application firewall dengan memblokir serangan sql injection yang masuk berdasarkan konfigurasi rules.		Action Research	Pencegahan terhadap serangan SQL injection yang dapat dicegah dengan Firewall.

5. Simpulan

Setelah melakukan penelitian dan perbandingan serta studi literature terhadap pola serangan dan pertahanan SQL Injection dalam berbagai jurnal maupun penelitian, hasil yang didapatkan adalah ;

1. Penerapan Form Validation dapat diterapkan pada inputan login untuk mencegah bypass sql i.

2. Integritas dari URL yang telah dienkripsi akan lebih terjaga, karena metode SQL injection tidak dapat diterapkan pada URL yang telah dienkripsi.

3. Analisis kerentan suatu website dapat dilakukan secara manual maupun dengan tools vulnerabilities assement.

4. Dari hasil pengamatan metode forensic juga terdapat temuan bahwa penyerang dengan teknik serangan sql injection dapat masuk melalui local server

5. Penyerang SQL Injection dapat masuk kedalam website dengan celah tersebut dan mampu melakukan tidakan level user admistrator.

Daftar Pustaka

Gunawan, I. (2021). *Keamanan Data: Teori dan Implementasi*. Sukabumi: Jejak Publisher.

Gunadhi, E. And Nugraha, A.P., 2016. Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection. *Jurnal Algoritma*, *13*(2), pp.391-398.

Mushlih, M., Fitri, R. And Wardiah, I., 2019, December. Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web. In *Seminar Nasional Riset Terapan* (Vol. 4, pp. A41-A47). P3M Politeknik Negeri Banjarmasin.

Putra, A.A., 2020. Analisa kerentanan pada situsweb www. Unisti. Ac. Id. *Informanika*, *6*(2).

Riadi, I., Umar, R. And Sukarno, W., 2016. Analisis Forensik Serangan Sql Injection Menggunakan Metode Statis Forensik. In *Pros. Interdiscip. Postgrad. Student Conf. 1st* (Vol. 1, pp. 102-103).

Wiguna, B., Prabowo, W.A. and Ananda, R., 2020. Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, *11*(2), pp.245-256.