

## ANALISIS DAN PERBANDINGAN SQL INJECTION PADA .NET FRAMEWORK DENGAN MENGGUNAKAN SQL SERVER 2000 DAN SQL SERVER 2008

Erma Nindiaswari<sup>1</sup>, Kiki Maulana<sup>2</sup>, Yanuar Firdaus A.w.<sup>3</sup>

<sup>1</sup>Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

---

### Abstrak

Salah satu metode yang dipakai untuk melakukan penyerangan terhadap aplikasi website adalah SQL injection. SQL injection adalah teknik yang meng-eksploitasi celah keamanan yang muncul di sekitar lapisan basis data dan aplikasinya. Celah keamanan tersebut ditunjukkan pada saat user memasukkan nilai string dan karakter kontrol lain yang ada dalam instruksi SQL atau user memasukkan string dengan tipe data tidak sama yang seharusnya tidak diproses [3].

Dengan besarnya ancaman dari SQL injection maka mendorong para peneliti untuk melakukan evaluasi baik dari segi bahasa pemrograman maupun database seperti yang dilakukan oleh Chris Anley yang mencoba menerapkan SQL injection pada website berbasis bahasa pemrograman Active Server Pages dengan database SQL Server 2000 (SQL 1) [2]. Dari pengujian tersebut di dapatkan hasil bahwa masih banyak teknik SQL injection yang belum tertangani oleh sebuah website dengan konfigurasi tersebut. Oleh karena itu, perlu dilakukan penanganan dengan lebih memanfaatkan kemampuan, fungsi dan konfigurasi yang dimiliki oleh bahasa pemrograman dan database dalam sebuah aplikasi website.

Berdasarkan hasil pengujian dan melihat kemampuan .Net yang merupakan simbol berubahnya model pengembangan website yang menggunakan framework [11], serta melihat versi terbaru dari SQL Server adalah SQL Server 2008 (SQL 2) yang memiliki beberapa keunggulan dalam hal penanganan SQL injection dibandingkan dengan SQL 1 [12], maka dapat disimpulkan bahwa penggunaan .Net Framework dan SQL 2 lebih baik dibandingkan dengan penggunaan .Net Framework dan SQL 1 dari segi vulnerability terutama pada kasus SQL injection. Sehingga didapatkan hasil perbandingan antara kedua konfigurasi tersebut serta dapat diketahui bagaimana pengaruh bahasa pemrograman maupun database terhadap penanganan serangan SQL injection pada sebuah website.

**Kata Kunci :** SQL Injection, SQL Server 2000, SQL Server 2008, .Net Framework

---

### Abstract

One of method to attack a website application is SQL injection. SQL injection is a technique which explore interpose the security which appear on the database and it's application. Interpose the security shown when user enter the value of string and other character control in SQL instruction or user enter the string with the unequal data type which should not be processed [3].

With the threat of SQL injection, push all researcher to do the evaluation as have done Chris Anley who tried to apply the SQL injection at website base on Active Server Pages with SQL Server 2000 (SQL 1) [2]. The result shows that still a lot of technique of SQL injection which not yet been handled by a website with this configuration. Therefore, require a handling with exploit the ability, function and configuration owned by scripting language and database in a website application.

Pursuant to examination result and see the ability of .Net, that representing the symbol of model the website development using framework [11], and also see the newest version from SQL Server is SQL Server 2008 (SQL 2) that owning some excellence in the case of handling of SQL Injection compared to SQL 1 [12], inferential hence that using .Net Framework and SQL 2 are better than .Net Framework and SQL 1 from vulnerability especially in SQL injection. So we can get the result of comparison between that configuration and how influence of scripting language and database to handling attack of SQL Injection in a website.

**Keywords :** SQL Injection, SQL Server 2000, SQL Server 2008, .Net Framework

---

## 1. Pendahuluan

### 1.1 Latar Belakang Masalah

Salah satu metode yang biasa dipakai untuk melakukan penyerangan terhadap aplikasi *website* adalah *SQL injection*. Dengan mesin pencarian Google dapat dilihat hampir 1.45 juta *page website* yang sudah terinfeksi metode *SQL injection* ini [22]. Dengan besarnya ancaman dari *SQL injection* maka mendorong para peneliti untuk melakukan evaluasi baik dari segi bahasa pemrograman maupun *database* seperti yang dilakukan oleh Chris Anley dari Next Generation Security Software Ltd yang mencoba menerapkan *SQL injection* pada *website* berbasis bahasa pemrograman Active Server Pages dengan *database* SQL 1 [2]. Dari pengujian tersebut di dapatkan hasil bahwa masih banyak teknik *SQL injection* yang belum tertangani oleh sebuah *website* dengan konfigurasi tersebut. Namun hal tersebut belum diketahui apakah dari segi *database* atau bahasa pemrogramannya.

Salah satu bahasa pemrograman yang dipakai untuk membangun sebuah situs *website* adalah .Net Framework. .Net merupakan *framework* produk dari Microsoft yang mendukung banyak bahasa pemrograman seperti VB, C#, J#, C++ dll, yang menjadi simbol berubahnya model pengembangan *web* yang menggunakan *framework* untuk mengembangkan situs secara efisien [11]. Selain itu, banyak sekali jenis *database* yang dipakai untuk membangun sebuah situs *website* misalnya SQL Server. SQL Server juga merupakan produk dari Microsoft, yang menggunakan Transact-SQL, yaitu jenis bahasa untuk basis data SQL yang dikeluarkan oleh perusahaan Microsoft dan Sybase. Versi terbaru dari SQL Server adalah SQL Server 2008 (SQL 2). Versi terbaru inilah yang didesain khusus dan sesuai dengan lingkungan .Net Framework 3.5, dimana terdapat *object-object* pada .Net Framework 3.5 yang menyatu dengan SQL 2 dan SQL 2 ini memiliki beberapa keunggulan dalam hal penanganan *SQL injection* dibandingkan dengan SQL 1 [10].

Dengan melihat kemampuan .Net Framework dan SQL 2, maka melalui tugas akhir ini akan dilakukan analisis dan perbandingan *SQL injection* pada .Net Framework dengan menggunakan SQL 1 dan SQL 2. Sehingga dapat diketahui bagaimana ketahanan dan teknik penanganan yang tepat pada kedua konfigurasi *website* tersebut dan didapatkan hasil perbandingan serta bagaimana pengaruh bahasa pemrograman maupun *database* terhadap penanganan serangan *SQL injection*.

### 1.2 Perumusan Masalah

Rumusan masalah yang ada pada Tugas Akhir ini yaitu sebagai berikut :

1. Bagaimana ketahanan dan teknik penanganan yang tepat terhadap *SQL injection* pada .Net Framework dan SQL Server 2000 (SQL 1).
2. Bagaimana ketahanan dan teknik penanganan yang tepat terhadap *SQL injection* pada .Net Framework dan SQL Server 2008 (SQL 2).
3. Bagaimana hasil perbandingan penanganan *SQL injection* pada .Net Framework dengan menggunakan SQL Server 2000 (SQL 1) dan SQL Server 2008 (SQL 2).

4. Bagaimana pengaruh bahasa pemrograman maupun *database* terhadap penanganan serangan *SQL injection* dalam hal ini adalah SQL Server 2000 (SQL 1) dan SQL Server 2008 (SQL 2) dengan menggunakan .Net Framework.

Adapun batasan masalah dari Tugas Akhir ini adalah :

1. Analisis dan perbandingan *SQL injection* dilakukan pada .Net Framework 3.5, SQL Server 2000 *Personal Edition* dan SQL Server 2008 *Web Edition*.
2. Analisis dan perbandingan *SQL injection* dilakukan dengan tidak melihat pengaruh aplikasi *server* yang digunakan.

### 1.3 Tujuan

Adapun tujuan yang ada pada Tugas Akhir ini adalah sebagai berikut :

1. Mengetahui bagaimana ketahanan dan teknik penanganan yang tepat terhadap *SQL injection* pada .Net Framework dan SQL Server 2000 (SQL 1) dengan membuat simulasi uji berupa *website* yang dibangun dengan konfigurasi tersebut.
2. Mengetahui bagaimana ketahanan dan teknik penanganan yang tepat terhadap *SQL injection* pada .Net Framework dan SQL Server 2008 (SQL 2) dengan membuat simulasi uji berupa *website* yang dibangun dengan konfigurasi tersebut.
3. Menganalisis perbandingan penanganan *SQL injection* pada .Net Framework dengan menggunakan SQL Server 2000 (SQL 1) dan SQL Server 2008 (SQL 2).
4. Menganalisis bagaimana pengaruh bahasa pemrograman maupun *database* terhadap penanganan serangan *SQL injection* dalam hal ini adalah SQL Server 2000 (SQL 1) dan SQL Server 2008 (SQL 2) dengan menggunakan .Net Framework.

### 1.4 Metodologi Penyelesaian Masalah

Metodologi yang akan digunakan dalam menyelesaikan Tugas Akhir ini adalah sebagai berikut :

1. Studi Literatur  
Mempelajari literatur-literatur yang berkaitan dengan konsep *SQL injection*, SQL Server dan .Net Framework.
2. Analisis dan Perancangan  
Menganalisis struktur fungsionalitas .Net Framework, SQL 1 dan SQL 2 terutama dari sisi *vulnerability*nya dan membuat rancangan perangkat lunak.
3. Implementasi  
Pembangunan *website* yang berbasis .Net Framework dengan menggunakan SQL 1 dan SQL 2.

4. Testing  
Menerapkan teknik penyerangan *SQL injection* pada *website* yang telah dibangun. Apakah *website* tersebut telah aman dari *SQL injection* serta menerapkan teknik penanganan yang tepat terhadap *SQL injection*.
5. Analisis Hasil *Testing*  
Menganalisis teknik penanganan dan ketahanan terhadap *SQL injection* pada .Net Framework dengan menggunakan SQL 1 dan SQL 2 sehingga didapatkan hasil perbandingan antara kedua konfigurasi tersebut serta kesimpulan tentang bagaimana pengaruh bahasa pemrograman dan *database* terhadap penanganan *SQL injection* pada sebuah *website*.
6. Pembuatan Laporan  
Mendokumentasikan tahap-tahap yang telah dilakukan mulai dari studi literatur sampai analisis hasil *testing*.



## 5. Penutup

### 5.1 Kesimpulan

Berdasarkan hasil pengujian SQL *injection* pada aplikasi berbasis .Net Framework dan SQL 1 serta .Net Framework dan SQL 2 disertai dengan penanganan yang dilakukan serta analisis sebelum dilakukan penanganan dan setelah dilakukan penanganan, maka dapat diambil kesimpulan yaitu :

1. .Net Framework dan SQL 1 memiliki kemampuan/*feature* dengan keunggulan dan kelemahan masing-masing. Agar hasil penanganan injeksi lebih baik maka dapat dilakukan penggabungan *feature* keduanya atau dapat juga menggunakan *feature* yang hanya dari .Net Framework tanpa melibatkan penanganan dari SQL 1.
2. .Net Framework dan SQL 2 memiliki kemampuan/*feature* dengan keunggulan dan kelemahan masing-masing. Agar hasil penanganan injeksi lebih baik maka dapat dilakukan penggabungan *feature* keduanya atau dapat juga menggunakan *feature* yang hanya dari .Net Framework tanpa melibatkan penanganan dari SQL 2.
3. Jika melihat dari pemrosesan *error* hasil injeksi dan *feature* penanganan SQL *injection* maka SQL 2 lebih unggul dibandingkan SQL 1 karena SQL 2 kurang detail dalam menampilkan *error* informasi *database* dan mempunyai *feature* Policy Based Management yang dapat dimanfaatkan untuk penanganan SQL *injection*.
4. Dalam penanganan SQL *injection*, pengaruh *database* dalam hal ini SQL 1 dan SQL 2 tidak memberikan pengaruh berarti/signifikan. Karena penggunaan kemampuan/*feature* yang hanya dari .Net Framework pun dapat dijadikan pilihan tanpa melibatkan penanganan dari *database* sehingga semua *preprocessing* dilakukan oleh *frontend*/bahasa pemrograman dan *backend/database* hanya menerima apapun nilai yang dilewatkan kepadanya

### 5.2 Saran

Analisis dan perbandingan SQL *injection* dapat juga dilakukan pada *framework* dari bahasa pemrograman lain misalnya Kohana pada PHP, dll. Selain itu, jika Policy Based Management pada SQL 2 dapat dikembangkan lebih jauh lagi misalnya dengan penambahan *policy*, *facet*, *target*, *condition* dalam hal keamanan oleh pihak produsen, maka keamanan aplikasi dan *database* akan menjadi lebih baik mengingat sampai saat ini belum ada injeksi yang dapat menyerang sebuah *policy*.

## Daftar Pustaka

- [1] Amri, M. Choirul. 2003. *Cepat Mahir Visual Basic .NET*. IlmuKomputer : Jakarta.
- [2] Anley, Chris. 2002. *Advanced SQL Injection In SQL Server Applications*. NGSSoftware Ltd.
- [3] Ciebal. 2009. *SQL Injection*. <http://www.ciebal.web.id/sql-injection/comment-page-1/>. Didownload tanggal 2 Juli 2009.
- [4] Darmarisa, Febrina. 2009. *Tugas Akhir Analisis dan Perbandingan SQL injection pada PHP dan Ruby on Rails*. IT Telkom : Bandung.
- [5] FunctionX, Inc. 2009. *Microsoft SQL Server*. <http://functionx.com/>. Didownload tanggal 2 Januari 2010.
- [6] Heriyanto, Trisno. 2009. *SQL Injection Masih Jadi Favorit Dedemit Maya*. <http://www.detikinet.com/read/2009/05/12/173851/1130320/323/sql-injection-masih-jadi-favorit-dedemit-maya>. Didownload tanggal 12 Agustus 2009.
- [7] Kikuta, Aji. 2008. *.Net Framework*. <http://ajidotnet.wordpress.com/category/net-framework/page/2/>. Didownload tanggal 6 Agustus 2009.
- [8] Komputer, Wahana. 2008. *Cepat Menguasai Visual Studio .NET 2008 Express*. Penerbit Andi : Yogyakarta.
- [9] Kusumo, Ario Suryo. 2007. *ASP.Net 2.0 Dengan VB 2005*. Elex Media Komputindo : Jakarta.
- [10] Lobel, Leonard dkk. 2008. *Programming Microsoft SQL Server 2008*. <http://my.safaribooksonline.com/9780735625990/ch04lev1sec1>. Didownload tanggal 29 Oktober 2009.
- [11] Masyarakat Digital Gotong Royong (MDGR). 2008. *Pengantar Sistem Operasi Komputer Jilid Pertama*. <http://bebas.vlsm.org/v06/Kuliah/SistemOperasi/BUKU/SistemOperasi-4.X-1/ch08s08.html>. Didownload tanggal 2 Juni 2009.
- [12] Microsoft. 2009. *SQL Server Security*. <http://microsoft.com/>. Didownload tanggal 2 Juni 2009.
- [13] Microsoft. 2010. *.NET Framework*. <http://msdn.microsoft.com/en-us/netframework/default.aspx>. Didownload tanggal 2 Januari 2010.

- [14] Microsoft. 2010. *SQL Server*. <http://msdn.microsoft.com/en-us/sqlserver/default.aspx>. Didownload tanggal 2 Januari 2010.
- [15] Nugroho, Aryo. 2009. *Menguasai T-SQL Query dan Programming SQL Server 2008*. Penerbit Andi : Yogyakarta.
- [16] Pratama, Mochamad Rizki. 2009. *Mengenal UML*. <http://iqnov.com/2009/05/mengenal-uml/>. Didownload tanggal 27 Mei 2009.
- [17] Rachmans. 2008. *Mengenal .NET Framework (Bagian 2)*. <http://rachmans.com/index.php?pilih=news&mod=yes&aksi=lihat&id=8>. Didownload tanggal 28 April 2009.
- [18] Raharjo, Budi. 2002. *Keamanan Sistem Informasi Berbasis Internet*. PT Insan Indonesia & PT INDOCISC : Jakarta.
- [19] Robi'in, Bambang. 2005. *Manajemen dan Administrasi Database dengan SQL Server 2000*. Penerbit Andi : Yogyakarta.
- [20] Siregar, Edison. 2006. *Membangun Aplikasi Berbasis Web Dengan ASP.NET 2.0*. Penerbit Andi : Yogyakarta.
- [21] Trikarsono, Aryo. 2008. *SQL Server : Sekilas Policy-Based Management di SQL Server 2008*. <http://miimlc.metrodata.co.id/forum/blogs/aryo/archive/2008/12/30/sql-server-sekilas-policy-based-management-di-sql-server-2008.aspx>. Didownload tanggal 30 Desember 2009.
- [22] Ulysses, Jonh Fredrik. 2008. *Beberapa Situs Pemerintah Amerika dan Inggris Menjadi Target Serangan SQL Injection*. <http://www.beritanet.com/Technology/Security/Situs-Pemerintah-Amerika-Inggris-Menjadi-Target-Serangan-SQL-Inj.html>. Didownload tanggal 9 Agustus 2009.
- [23] WoNX. 2007. *MELINDUNGI APLIKASI DARI SQL INJECTION*. [http://www.jogjahacking.org/artikel\\_lengkap.php?aid=53](http://www.jogjahacking.org/artikel_lengkap.php?aid=53). Didownload tanggal 14 Januari 2010.
- [24] Zierafiezta. 2009. *Algoritma dan teknik menangkal SQL injection*. <http://kabarit.com/2009/06/algoritma-dan-teknik-menangkal-sql-injection/>. Didownload tanggal 11 Agustus 2009.