U-NET Jurnal Teknik Informatika
Vol. 04, No. 01, Februari 2020, pp. 08~13
e-ISSN: 2622-8238, p-ISSN: 2722-4287
DOI: 10.52332/u-net.v4i1.164

Implementasi Sistem Keamanan SQL Injection Dalam berbasis web

Zulkifli[1], Samsir[2],
[1]STIA Setih Setio, Muara Bungo, Indonesia
[2]Universitas Al Washliyah, Labuhanbatu, Indonesia

Info Artikel

Article history:

Received: 12 2019
Revised: 01 2020
Accepted: 02 2020

Kata Kunci:

Jaringan servel lokal
SQL Injeksi
website

Penulis Korespondensi:
Zulkifli
z.skom@yahoo.com

Abstract

The security of internet access network websites is something that needs to be taken very seriously. The attack caused by sql injection is able to break into the website defense system that we have if it is not equipped with strong security. Considering this website is widely accessible, it is considered necessary to pay attention to website security. There are several ways that can be used to test the security of a website, one of which is to do SQL Injection. SQL injection is a vulnerability that occurs when an attacker has the ability to influence Structured Query Language (SQL) queries that pass an application to a back-end database. By holding this research, it is expected that weaknesses can be obtained from the website. These weaknesses will be analyzed in order to obtain future solutions for the development of safer websites.

Abstrak

Kemanan website akses jaringan internet merupakan hal yang perlu diperhatikan sangat serius. Serangan yang diakibatkan oleh sql injection mampu membobol sistem pertahanan website yang kita miliki jika tidak dilengkapai dengan pengamanan yang kuat. Mengingat website ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan website. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap kemanan website, salah satunya adalah dengan melakukan SQL Injection. SQL injection adalah kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi Structured Query Language (SQL) query yang melewati suatu aplikasi ke database back-end. Dengan diadakannya penelitian ini, diharapkan dapat diperoleh kelemahan dari website. Kelemahan tersebut akan dianalisa sehingga memperoleh solusi kedepan guna pengembangan website yang lebih aman.

1. PENDAHULUAN

SQL injection adalah kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi Structured Query Language (SQL) query yang melewati suatu aplikasi ke database back-end. Dengan mampu mempengaruhi apa yang akan diteruskan ke database, penyerang dapat memanfaatkan sintaks dan kemampuan dari SQL, serta kekuatan dan fleksibilitas untuk mendukung fungsi operasi database dan fungsionalitas sistem yang tersedia ke database. Injeksi SQL bukan merupakan kerentanan yang eksklusif mempengaruhi aplikasi Web, kode yang menerima masukan dari sumber yang tidak dipercaya dan kemudian menggunakan input yang membentuk SQL dinamis bisa rentan (Clarke, 2009). Berdasarkan defenisi tersebut, dapat dikatakan bahwa serangan SQL Injection sangat berbahaya karena penyerang yang telah berhasil memasuki database sistem dapat melakukan manipulasi data yang ada pada database sistem. Proses manipulasi data yang tidak semestinya oleh penyerang dapat menimbulkan kerugian bagi pemilik website yang terinjeksi. Kebocoran data dan informasi merupakan hal yang fatal. Data-data tersebut dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Keamanan data dan informasi sangat penting dalam menjaga ketahanan sebuah website. Berdasarkan uraian-uraian tersebut, maka dinilai perlu untuk menguji kemanan website terhadap serangan SQL Injection, serta melakukan analisa terhadap kelemahan sistem yang ada, sehingga dapat diperoleh tindakan selanjutnya untuk perbaikan sistem. SQL (Structured Query Language) adalah sebuah bahasa yang dipergunakan untuk mengakses data dalam basis data relasional. Bahasa ini secara de facto merupakan bahasa standar yang digunakan dalam manajemen basis data

relasional. Saat ini hampir semua server basis data yang ada mendukung bahasa ini untuk melakukan manajemen datanya. Sejarah SQL dimulai dari artikel seorang peneliti dari IBM bernama EF Codd yang membahas tentang ide pembuatan basis data relasional pada bulan Juni 1970, Bahasa tersebut kemudian diberi nama SEQUEL (Structured English Query Language). Setelah terbitnya artikel tersebut, IBM mengadakan proyek pembuatan basis data relasional berbasis bahasa SEQUEL. Akan tetapi, karena permasalahan hukum mengenai penamaan SEQUEL, IBM pun mengubahnya menjadi SQL. Implementasi basis data relasional dikenal dengan System/R. Di akhir tahun 1970-an, muncul perusahaan bernama Oracle yang membuat server basis data populer yang bernama sama dengan nama perusahaannya. Dengan naiknya kepopuleran Oracle, maka SQL juga ikut populer sehingga saat ini menjadi standar de facto bahasa dalam manajemen basis data. Standarisasi Standarisasi SQL dimulai pada tahun 1986, ditandai dengan dikeluarkannya standar SQL oleh ANSI. Standar ini sering disebut dengan SQL86.Standar tersebut kemudian diperbaiki pada tahun 1989 kemudian diperbaiki lagi pada tahun 1992. Versi terakhir dikenal dengan SQL92. Pada tahun 1999 dikeluarkan standar baru yaitu SQL99 atau disebut juga SQL99, akan tetapi kebanyakan implementasi mereferensi pada SQL92. Saat ini sebenarnya tidak ada server basis data yang 100% mendukung SQL92. Hal ini disebabkan masing-masing server memiliki dialek masing-masing. Pemakaian dasar Secara umum, SQL terdiri dari dua bahasa, yaitu Data Definition Language (DDL) dan Data Manipulation Language (DML). Implementasi DDL dan DML berbeda untuk tiap sistem manajemen basis data (SMBD)[1], namun secara umum implementasi tiap bahasa ini memiliki bentuk standar yang ditetapkan ANSI. Artikel ini akan menggunakan bentuk paling umum yang dapat digunakan pada kebanyakan SMBD.

2. METODE PENELITIAN

Pada penelitian ini penulis menggunakan metode Waterfall. Waterfall atau Classic Life Cycle merupakan metode yang banyak digunakan pada Software Enginering, metode ini melakukan pendekatan secara sistematis dan terurut dari level kebutuhan sistem lalu menuju ke tahap analisis, desain, implementasi, dan pengujian sistem. Disebut Waterfall karena tahap demi tahap yang dilalui harus menunggu selesainya tahap sebelumnya dan berjalan berurutan.

3. DISKUSI DAN HASIL

3.1 Pengumpulan data

Pengguna SQL-Server Buat pengguna SQL-Server, khususnya admin/programer, cek file C:\Program Files\Microsoft SQL Server\MSSQL\Data\tempdb.mdf (atau folder default dimana data default SQL-Server diletakkan). File tempdb.mdf adalah file temporari dari sistem SQL-Server apabila server mendapat query yang melibatkan data yang kompleks. Yah semacam swap file gitu deh, untuk mengoptimalkan proses. Sayangnya, file ini bisa membengkak besar sekali. Di kantor saya pernah mencapai 32GB!. Kadang bingung juga, padahal sistem dalam kondisi idle (tidak ada koneksi ke server), kok ni file tidak dimampatkan lagi oleh SQL Server. Apabila hal ini terjadi cara mengatasinya cukup mudah, restart saja SQL- Servernya. Hopla! file pun kembali berukuran sekitar 8MB saja. Anda bisa melakukan cek secara berkala ke file ini, atau lebih gampangnya ya diberi scheduling untuk merestart server di jam-jam biasanya idle. SQL dapat digunakan dengan 2 cara : a. Interaktif SQL (SQL Interaksi), Memasukkan sebuah pernyataan SQL melalui terminal / microkomputer dan langsung diproses atau diinteprestasikan, hasilnya bisa dilihat secara langsung. b. Embedded SQL (SQL Sisipan), Dengan menyisipkan pernyataan SQL ke dalam sebuah program yang ditulis dengan bahasa pemrograman lain. Hasil pernyataan SQL tidak dapat dilihat langsung oleh pemakai, tapi diproses oleh program lain

Beberapa penelitian terkait yang membahas tentang SQL Injection adalah, Halfond dan Orso (2005) menyajikan dan mengevaluasi teknik baru untuk mendeteksi dan mencegah serangan SQL Injection. Teknik menggunakan pendekatan berbasis model untuk mendeteksi query illegal sebelum dieksekusi
pada basis data. Halfond dan Orso (2005) mengembangkan alat AMNESIA (Analysis and Monitoring for NEutralizing SQLInjection Attacks) yang menerapkan teknik secara statis dan dinamis untuk mengevaluasi teknik pada aplikasi web. Teknis statis menggunakan analisis program untuk membangun model query yang sah yang dapat dihasilkan aplikasi, sedangkan teknik dinamis menggunakan pemantauan runtime untuk memeriksa yang dihasilkan query dan memeriksa model statis yang dibangun. Halfond dan Orso (2005) mengusulkan model baru untuk melawan SQLIA yaitu kerentanan yang disebabkan oleh input pengguna yang tidak divalidasi dengan menggunakan kombinasi teknik analisis statis dan dinamis dan menerapkannya pada alat prototype AMNESIA.

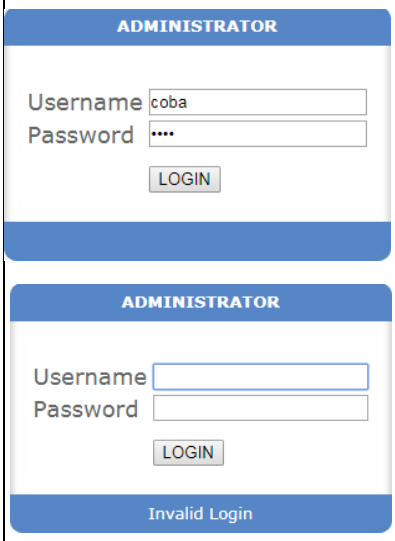
3.2 Analisis dan Desain Sistem
Pada bagian ini akan dijelaksan bagaimana bentuk serangan Sql injection pengujian dalam jaringan local server pada sebuah website.

3.3 Implementasi
Pada bagian ini akan dijelasakan tentang implementasi sebuah Tampilan dan source code tanpa anti sql injection dan tampilan dan source code menggunakan anti sql injection

3.3.1 Implementasi SQL Injeksi
Pada bagian ini akan dijelaskan proses pembobolan website dari login admin dengan cara SQL Injeksi dengan dua model yaitu SQL Injeksi pada website tanpa menggunakan teknik penggunaan maxlength dan inut type number dan website yang menggunakan teknik penggunaan masxlength dan inut type number. Untuk detail penjelasan dapat dilihat pada pembahasan berikuti ini.

A. System tampilan dan source code tanpa anti sql injection
Pada bagian ini akan ditampilkan source code login tanpa anti sql injection dengan pembahasan sebagai berikut :

Tabel 1. Tampilan dan source code tanpa anti sql injection

Gambar form login	Source code form login
Hasil dapat login ke admin 	1. $userid = $_POST['userid']; 2. $password = $_POST['password'];

Keterangan Tabel
1. pada baris pertama merupakan variable username yang terdapat dalam table database. Kelemahan terdapat karena semua karakter yang sifantnya peretasan akan mudah tembus kedalaam sistem karena tidak ada proses pemfilteran.
2. pada baris kedua merupakan variable password yang terdapat dalam table database. Kelemahan terdapat karena semua karakter yang sifantnya peretasan akan mudah tembus kedalaam sistem karena tidak ada proses pemfilteran.

B. System tampilan dan source code menggunakan anti sql injection
Pada bagian ini akan ditampilkan source code login menggunakan anti sql injection dengan pembahasan sebagai berikut :

Tabel 2. Tampilan dan source code menggunakan anti sql injection

Gambar form login	Source code form login

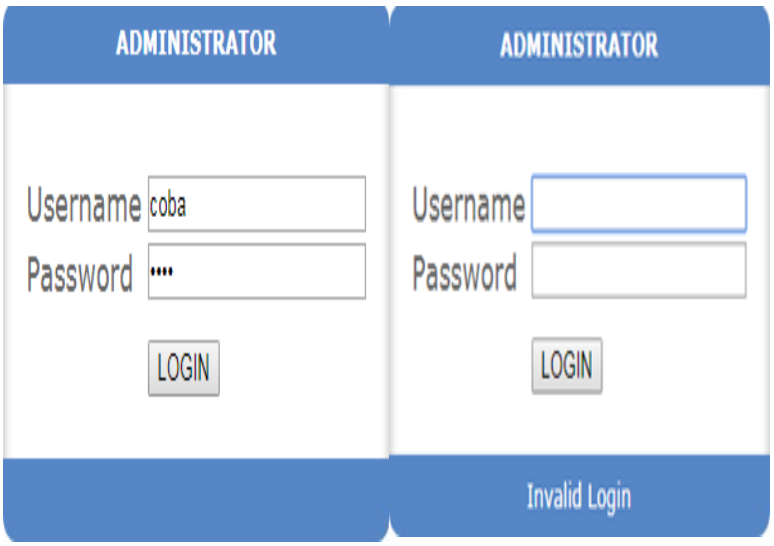
	function antiinjek($data){
	$filter=mysql_real_escape_string(htmlspecialchars(stripslashes(strip_tags($dat a,ENT_QUOTES))));
	return $filter;
	}
	$username = antiinjek($_POST['knk']);
	$password = antiinjek(md5($_POST['kunci']));

Keterangan Tabel 2

1. Pada baris pertama merupakan variable fungsi anti injeksi sql
2. Melakukan proses pemfilteran terhadap jenis serangan injeksi
3. Memjalankan fungsi injeksi
4. Variable login dengan username telah dilakukan pemfilteran anti injeksi
5. Variable login dengan password telah dilakukan pemfilteran anti injeksi

3.4. Pengujian Sistem

Pada pengujian kali ini adalah sisem website yang yang tidak dilengkapai dengan sistemkemanan sql injeksi sehingga akan terlihat proses pembobol sistem website dari dalam jaringan computer. Untuk detail berikut perhatikan gambar 1 dibawah ini

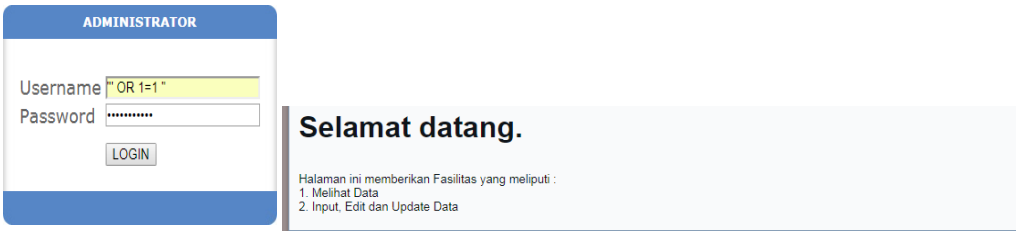


Gambar 1. Login gagal dengan data yang salah

Pada gambar 1 diatas merupakan form login website yang dilakukan pengujian dengan memasukkan username dan password yang tida terdapat dalam database dan hasilnya invalid login yang berarti login gagal. Berikut perhatikan ketika kita coba masukan data yang benar yang dapat dilihat pada gambar 2 dibawah ini

Gambar 2. Login berhasil dengan data yang benar

Pada gambar 2 diatas menunjukkan proses login dengan data user dan password yang benar dan hasilnya sistem akan membaca data dnegan status valid sehingga menampilkan halaman admin sebuah website. Nah bagaiaman untuk seraangan SQL injeksi mari perhatikan gambar 3 berikut ini



Gambar 3. Login berhasil dengan penetrasi sql injection

pada gambar 3 menjukkan karakter ("' OR 1=1 ") yang di inputkan pada kolom username dan password maka akan mampu melakukan penetrasi kedalam sistem hingga dapat login bebas masuk kedalam sistem admin tanpa harus memasukkan data yang benar.

4. KESIMPULAN

Adapun kesimpulan yang terdapat dalam penelitian ini adalah sebagai berikut :

Dalam sistem website yang terkoneksi oleh jaringan internet maupun local server akan pasti akan rentan terhadap serangan hacker baik secara sengaja maupun sebaliknya. Ketahanan sistem dipengaruhi dari infrastruktur jaringan yang benar dan desain sistem kemananan website yang baik. Teknik sql injeksi ini dapat digunakan pada website manapun selagi tidak ada sistem kemanan didalamnya maka dari itu harus dilakukan evaluasi agardapat menanggulangi serangan jenis sql injekksi tersebut.

REFERENSI

[1] F. Edi, P. T. Informatika, and F. U. A. Labuhanbatu, "UNET | Jurnal Ilmiah Teknik Informatika LPPM Universitas Al Washliyah Labuhanbatu UNET | Jurnal Ilmiah Teknik Informatika ISSN . 2460-3694 , Vol . 2 No . 1 Februari 2018," vol. 2, no. 1, pp. 2–5, 2018.

[2] D. I. G. H. Wirhan Fahrozi, Samsir, "Penerapan E-Commerce Pada Toko Bunga Underwear," *J. Tek. Inform.*, vol. 04, no. 01, pp. 1–6, 2020.

[3] S. Samsir, S. Suparno, and M. Giatman, "Predicting the loan risk towards new customer applying data mining using nearest neighbor algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 830, no. 3, 2020, doi: 10.1088/1757-899X/830/3/032004.

[4] R. A. Purba, S. Samsir, M. Siddik, S. Sondang, and M. F. Nasir, "The optimalization of backpropagation neural networks to simplify decision making," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 830, no. 2, 2020, doi: 10.1088/1757-899X/830/2/022091.

[5] Samsir, "Klasifikasi Penyakit Tenggorokan Hidung Telinga (THT) Menggunakan Jaringan Syaraf Tiruan Dengan Metode Learning Vektor Quantization (THT) Di RSUD Rantauprapat Labuhanbatu Klasifikasi penyakit Tenggorokan Hidung Telinga (THT) Menggunakan," vol. 05, no. 01, pp. 38–47, 2019.

[6] P. T. Informatika and F. U. A. Labuhanbatu, "U-NET : Jurnal Teknik Informatika LPPM – Universitas Al Washliyah Labuhanbatu 18 | P a g e U-NET : Jurnal Teknik Informatika Sebagai langkah awal yang dilakukan supaya dapat mengetahui gambaran permasalahan yang dihadapi oleh bagian kesiswaan adalah denga," vol. 3, no. 4, pp. 18–22, 2019.

[7] M. Siddik and S. Samsir, "Rancang Bangun Sistem Informasi Pos (Point of Sale) Untuk Kasir Menggunakan Konsep Bahasa Pemrograman Orientasi Objek," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 4, no. 1, p. 43, 2020, doi: 10.35145/joisie.v4i1.607.

[8] Samsir and Syaiful Zuhri Harahap, "Application Design Resume Medical By Using Microsoft Visual Basic. Net 2010 At the Health Center Appointments," *Int. J. Sci. Technol. Manag.*, vol. 1, no. 1, pp. 14–20, 2020, doi: 10.46729/ijstm.v1i1.5.

[9] W. Fahrozi, P. T. Informatika, T. Informatika, F. U. A. Labuhanbatu, T. Mulia, and K. Medan, "U-NET : Jurnal Teknik Informatika LPPM – Universitas Al Washliyah Labuhanbatu 23 | P a g e U-NET : Jurnal Teknik Informatika Sebagai langkah awal yang dilakukan supaya dapat mengetahui gambaran permasalahan yang dihadapi dalam menentukan rasa yam serama a," vol. 3, no. 5, pp. 23–27, 2019.

[10] M. V. B. Net, "PADA TOKO URIP MOTOR," no. September, pp. 1–6, 2020.

[11] Samsir, D. I. G. Hts, and S. Z. Harahap, "SPK Untuk Pemilihan Kepala Sekolah Menggunakan Metode Saw dan Profile Matching," *U-NET J. Tek. Inform.*, 2020.

[12] J. H. P. Sitorus *et al.*, "Perancangan pengontrol lampu rumah miniatur dengan menggunakan micro controler arduino berbasis android 1," vol. 4, no. 1, pp. 1–11, 2020.

[13] U. Verawardina, F. Edi, and R. Watrianthos, "Analisis Sentimen Pembelajaran Daring Pada Twitter di Masa Pandemi COVID-19 Menggunakan Metode Naïve Bayes," vol. 5, pp. 157–163, 2021, doi: 10.30865/mib.v5i1.2604.

[14] S. Zulkifli, "Implementasi Sistem Keamanan SQL Injection Dalam berbasis web," *Ejurnal.Univalabuhanbatu.Ac.Id*, vol. 04, no. 01, pp. 13–17, 2020, [Online]. Available: https://ejurnal.univalabuhanbatu.ac.id/index.php/u-net/article/download/164/130.

[15] Syaiful Zuhri Harahap and Samsir, "Application Design The Data Collection Features of The Hotel Shades of Rantauprapat Using VBNET," *Int. J. Sci. Technol. Manag.*, 2020, doi: 10.46729/ijstm.v1i1.4.