U-NET Jurnal Teknik Informatika
Vol. 04, No. 01, Februari 2020, pp. 01~06
e-ISSN: 2622-8238, p-ISSN: 2722-4287
DOI: https://doi.org/xxxxxxxxxxxxxxxxxx

Implementasi Max Length dan Input Type Number Pada Form Login Website Untuk Mencegah Penetrasi SQL Injeksi Secara Paksa

Zulkifli[1], Samsir[2], Azrai Sirait[3]
[1]STIA Setih Setio, Muara Bungo, Indonesia
[2]Universitas Al Washliyah, Labuhanbatu, Indonesia
[3]Universitas Asahan, Kisaran, Indonesia

Info Artikel

Article history:

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

Kata Kunci:

maxlength
SQL Injeksi
website
HTML
PHP

Penulis Korespondensi:
Zulkifli
z.skom@yahoo.com

Abstract

In the world of IT, websites are very vulnerable to hacker attacks in various types of ways so that they can break into the security of the target website. SQL injection attacks are often carried out on breaching websites from the login form by entering a special injection username and password so that the website can be hacked easily. In securing a website from injection attacks, there are various ways, one of which is by using the max length technique and input type number. The maxlength technique and input type number are made in the form of php or html source code which is inserted into the login form source code in the username and password input section. One of the advantages of this maxlengnth and input type technique is that it limits the input of the username and changes the format of the password input to only numbers, which means it will prevent hackers from forcibly penetrating the SQL injection attack on the website.

Abstrak

Dalam dunia IT pada website sangat rentan akan serangan hacker dengan berbagai jenis cara agar mereka dapat membobol kemanan website target. Serangan SQL Injeksi sering dilakukan pada pembobolan website dari form login dengan menginputkan username dan password khusus injeksi sehingga website dapat dibobol dengan mudah. Dalam mengamankan sebuah website dari serangan injeksi beragam caranya salah satunya dengan menggunakan teknik maxlength dan input type number. Teknik maxlengntht dan input type number ini dibuat dalam bentuk source code php atau html yang disisipkan kedlalam source code form login pada bagian input username dan password. Salah satu keunggulan teknik maxlengnth dan input type ini akan membuat batasan inputan username dan mengubah format inputan password hanya bertipekan angka saja yang artinya akan mencegah hacker dalam melakukan penetrasi secara paksa dalam serangan SQL Injeksi pada website

1. PENDAHULUAN

Teknologi dibidang IT yaitu pada website saat ini sangat berkembang pesat tidak dapat dibendung seiring perkembangan zaman. Website sudah banyak yang berkembang dari mulai plat form php native, cms bahkan platform frame work yang saat ini sudah tersebar dan banyak digunakan oleh hamper seluruh lini aktivitas kegiatan. Dalam pembuatan website hal yang paling rentan menjadi masalah adalah sisi kemanan system website tersebut. Saat ini banyak terjadi pembobolan situs website dari mulai situs webisite perusahaan sampai dengan situs website pemerintahan. Beragam macam jenis-jenis serangan terhadap kemanan website yakni dengan membobol login admin dengan menggunakan banyak teknik yakni ada menggunakan serangan brute force dan yang paling familiar menggunakan serangan sql injeksi.

Mengamankan website dengan menggunakan teknik maxlength dan input type number ini akan mengubah inputan formlogin pada username terbatas hanya 4-8 karakter saja dan mengubah inputan password yang seharusnya type text atau type password diubah menjadi type number. Mengubah kedua parameter ini dengan batasan input karakter dan type inputan number membuat kinerja serangan SQL. Injeksi tidak akan

berpengaruh dan tidak dapat berjalan sehingga website akan aman dari bentuk serangan SQL Injeksi Secara Penetrasi atau secara paksa.

Metode untuk menghindari SQL Injection dapat dilakukan kedalam dua cara yaitu secara client-side dan server-side. Pada metode Client-Side yaitu menerima 'Shadow SQL Query' dari server-side dan melakukan pengecekan terhadap deviasi yang terjadi antara shadow query dengan query dinamis yang dibentuk oleh masukan dari pengguna. Jika ditemukan adanya deviasi maka dapat dipastikan bahwa masukannya tidak benar (Malicious) [1]. Dengan demikian diperlukan sebuah metode yang mampu memberikan solusi tepat. Untuk dapat menentukan metode yang tepat maka dianggap perlu mengenal karakter dan cara kerja dari kegiatan penyerangan tersebut. Dalam penelitian ini diperkenalkan jenis penyerangan dengan cara sql injection secara server side scripting untuk kemudian diberikan solusi menghindarinya. Dalam penelitian ini diangap perlu mengangkat jenis serangan SQL Injection dikarenakan bahwa total serangan terhadap situs-situs yang ada di Indonesia adalah 28.430.843 dan jenis serangan paling besar adalah melalui SQL [2].

SQL Injeksi Merupakan sebuah kerentanan yang menyebabkan seorang penyerang memiliki kemampuan untuk mempengaruhi query SQL yang dikirimkan melalui aplikasi ke database. Dengan kemampuan tersebut seorang penyerang dapat mempengaruhi syntax SQL, kekuatan, fleksibilitas dari database pendukung fungsional dan mempengaruhi fungsi sistem operasi yang dialokasikan untuk database. SQL Injection tidak hanya mempengaruhi aplikasi web tapi juga semua program lain yang menggunakan kalimat SQL. Semua program yang menggunakan input dinamis dari luar (untrusted) dapat terserang oleh SQL. [3]

Dalam mengantispasi serangan SQL Injeksi ini bergam pula dari mulai memberikan filter dari source code untuk query sampai dengan menggunakan verifikasi robot. Dalam pengamanan website dari serangan SQL Injeksi sebenarnya ada yang sederhana yang jarang diketahui oleh banyak programmer dan develover website yaitu dengan cara menggunakan teknik maxlength dan input type number yang artinya adalah pertama membatasi jumlah karkater inputan username dan mengubah type inputan text atau password menjadi jenis number. Pada prinsipnya serangan SQL Injeksi ini melalui form login admin dengan melakukan injeksi menggunakan software khusus sampai denegan menggunakan cara paksa atau disebut penetrasi yang mana hacker menerobos masuk dengan menginputkan username dan password khusus injeksi dengan kolaborasi angak dan huruf dengan parameter karakter yang ditentukan panjangnya.

Beberapa hal yang membuka kesempatan bagi penyerang untuk melakukan SQL Injection yaitu Memanfaatkan keuntungan dari sebuah sebuah aplikasi yang tidak terlindungi pada fungsi autentikasi pengguna karena tidak adanya validasi. Umumnya seorang penyerang membajak login field yang tidak terlindungi untuk memperoleh akses database. SQL Interpreter tidak dapat membedakan antara perintah yang dimaksud dengan kode yag di-inject oleh penyerang yang kemudian dieksekusi dan mengakibatkan terekspos nya database. Peyerang kemudian dapat mengakali aplikasi untuk mengekstrak semua data, menanamkan malicious script.

2. METODE PENELITIAN

Pada penelitian ini penulis menggunakan metode SDLC 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. Adapun tahapan-tahapan pada penelitian ini adalah:

a. Pengumpulan Data

Tahapan ini dilakukan untuk memperoleh data yang diperlukan dalam pembuatan dan pengembangan system website dari mulai pengumpulan gambar, isi konten yang dimuat, source code dan pendukung data lainnya.

b. Analisis

Tahapan analisis dilakukan untuk menganalisis permasalahan dan menentukan kebutuhan yang diperlukan dalam pembuatan sistem. Hasil analisis tersebut kemudian dijadikan dasar dalam membuat perancangan desain sistem.

c. Desain

Tahapan desain dilakukan untuk mengetahui alur data dan proses yang terjadi sistem. Perancangan desain sistem dilakukan menggunakan Unified Modeling Language (UML).

d. Implementasi Sistem

Tahapan implementasi dilakukan untuk menerjemahkan desain yang telah dibuat menggunakan bahasa pemrograman agar dapat dikembangkan menjadi sebuah sistem atau perangkat lunak. Sistem akan dibuat dan dikembangkan berbasis web menggunakan framework php native untuk mencoba melihat dua perbandingan system kemanan yang digunakan pada salah satu website yang dibuat sebagai bahan uji coba.

e. Pengujian Sistem

Tahapan pengujian sistem dilakukan untuk mengetahui apakah sistem yang dibuat telah sesuai dengan tujuan yang direncanakan. Pengujian sistem dilakukan menggunakan metode black-box testing.

Berikut merupakan gambar ilustrasi dari metode penelitian yang dilakukan:

Gambar 1. Metode Penelitian

3. DISKUSI DAN HASIL

3.1 Pengumpulan data

Pada bagian ini penulis hanya mengumpulkan data berupa dua rancangan website yang rentan akan seragangan SQL Injeksi tanpa menggunakan teknik maxlength dan input type number. Kemdian rancnagan weibsite yang kedua merupakan pengembangan dengan menggnakan teknik maxlength dan input type number untuk mencegah penetrasi paksa dalam SQL Injeksi dengan pengujian dari server penyedia layanan hosting serta pengumpulan data sintax SQL Injeksi yang biasa digunakan hacker untuk meretas website dapat dilihat pada table berikut.

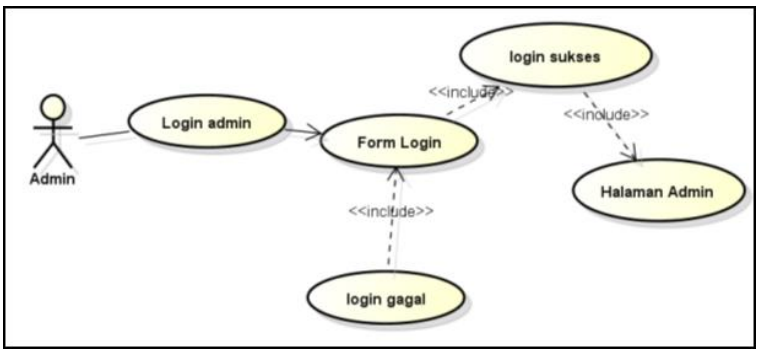
Tabel 1. Data sintax SQL Injeksi yang umum digunakan hacker

No	Sintax SQL Injeksi pada username	Sintax SQL Injeksi pada password
1	' or 1=10 limit 10’	' or 100=15 limit 10’
2	'" OR 1=1	or ‘1’=’1
3	admin	' or '1'='1
4	'" OR 1=1	' or 'x'='x
5	'" OR 1=1	' or 0=0 --
6	'" OR 1=1	" or 0=0 --
7	'" OR 1=1	or 0=0 --
8	'" OR 1=1	' or 0=0 #
9	'" OR 1=1	" or 0=0 #
10	'" OR 1=1	or 0=0 #
11	'" OR 1=1	' or 'x'='x
12	'" OR 1=1	" or "x"="x
13	'" OR 1=1	') or ('x'='x
14	'" OR 1=1	' or 1=1--
15	admin	1') and '1'='1--

Pada table 1 diatas merupakan sintax yang biasanya digunakan oleh para hacker untuk melakukan peretasan website dengan metode SQL Injeksi menarget form login.

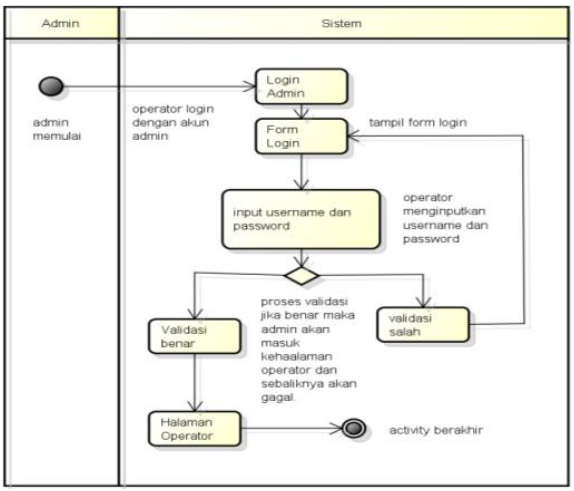
3.2 Analisis dan Desain Sistem

Untuk menjelaskan alur dan konsep dari penelitian, penulisan menggunakan Unified Modeling Language (UML) untuk memodelkan alur penelitian yang dilakukan. UML digambarkan mulai dari use case dan activity diagram. UML dari system website dapat dilihat pada gambar.



Gambar 2. Use Case Login Admin

Pada gambar 2 use case terdapat scenario admin yang melakukan aktivitas login admin dengan menginputkan username serta password. Jika validasi benar maka admin akan dapat login dan masuk kehalaman operator dan sebaliknya tidak dapat login. Pada activity diagram merupakan aktivitas admin untuk masuk kedalam halaman operator dengan menginputkan akun admin yang resmi secara normal. Jika akun admin benar maka system akan melakukan validasi untuk memproses masuk kedalam halaman admin jika akun admin tidak resmi maka akan gagal login kecuali melakukan prosedur diluar validasi seperti aktivitas hacking dengan cara illegal.



Gambar 3. Use Case Login Admin

3.3 Implementasi

Pada bagian ini akan dijelasakan tentang implemntasi sebuah website publikasi RPS atau disebut Website menampilkan informasi Rencana pembelajaran semester yang terdapat menu home untuk menampilkan informasi beranda, menu daftar matakuliah untuk melihat daftar semua mata kuliah yang ada dan menu login untuk admin melakuka nlogin ke halaman operator.

Gambar 4. Tampilan website

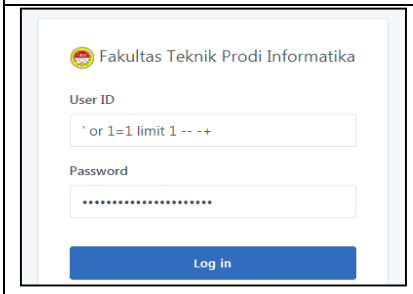
3.3.1 Implementasi SQL Injeksi

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 website tanpa penggunaan teknik maxlength dan input type number

Pada bagian ini akan ditampilkan source code login.php dan tampilan form login dengan pembahasan sebagai berikut :

Tabel 2. Tampilan dan source code login php tanpa teknik maxlengtht dan input type number

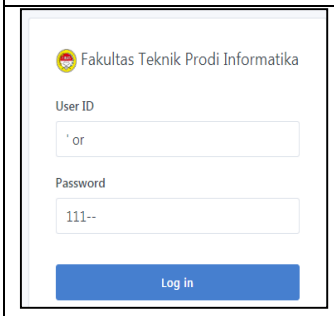
Gambar form login	Source code form login
 Hasil dapat login ke admin	 <label class="form-label">User ID</label> <input type="text" class="form-control" name="userid" placeholder="Enter UserID" required> <label class="form-label"> Password </label>

	<input type="password" class="form-control" name="password" placeholder="Password" required>

Pada table 2 form login contoh A dapat kita lihat pada bagian source code bewarna merah tidak terdapat maxlength untuk pembatasan inputan username atau userid sehingga hacker dapat menginputkan sintax SQL Injeksi di inputan username tersebut secara bebas. Kemudian lihat source code yang bewarna hijau juga tidak menggunakan input type number tetapi memakai type password yang artinya pada inputan password dengan type password ini tidak efektif mencegah serangan SQL Injeksi karena hacker bisa bebas memasukan sintax Injeksi dengan secara paksa apalagi inputan tidak dibatasi dengan maxlength. Untuk melihat perbandingan lainnya dapat dilihat pada bagian B berikut.

B. System website penggunaan teknik maxlength dan input type number
Pada bagian ini akan ditampilkan source code login.php dan tampilan form login dengan pembahasan sebagai berikut:

Tabel 3. Tampilan dan source code login php menggunakan teknik maxlengtht dan input type number

Gambar form login	**Source code form login**
 Login tidak berhasil 	 <label class="form-label">User ID</label> <input type="text" class="form-control" name="userid" maxlength="5" placeholder="Enter UserID" required> <label class="form-label"> Password </label> <input type="number" class="form-control" name="password" maxlength="10" placeholder="Password" required>

Pada table 3 diatas merupakan tampilan form login dan source code merupakan penggunaan teknik maxlength dan input type number. Dapat dilihat perbedaanya diamana saat hacker menngunakan sintax SQL Injeksi pakai username menggunaan (' or 1=1 limit 1 -- -+) dengan karakter text 21 maka tidak berhasil karena tidak lengkap diakibatkan kareba sudah dibatasi maxlength menjadi 5 karakter saja sehingga tampilan pada form login inputan username hanya dapat menampung teks (‘or) saja. Kemudian lihat pada bagian inputan password sebab sudah di ubah input type menjadi angka atau number maka sintax SQL Injeksi yang seharusnya (' or 1=1 limit 1 -- -+) berubah menjadi (111--) yang artinya sintax itu berubah mengikuti format angka dan panjang arakter inputan hanya menjadi 5 karakter saja hal ini membuat tidak befungsinya proses pembobolan website dengan teknik penetrasi Paksa SQL Injeksi.

3.4. Pengujian Sistem
Pada penelitian ini digunakan metode pengujian black box testing. Pengujian dilakukan dengan menguji bagian antarmuka dari sistem informasi, setiap bagian dari antarmuka tersebut diuji agar dapat ditentukan apakah

sistem sudah berjalan sesuai dengan fungsi yang diharapkan [8]. Tujuan dari pengujian ini adalah untuk mengetahui kesalahan pada sistem yang dibuat. Berikut adalah hasil pengujian menggunakan metode black box testing yang ditampilkan dalam bentuk tabel:

Tabel 4. Hasil pengujian sistem.

No	Kelas Uji	Skenario Pengujian	Hasil Pengujian
1	Halaman *Home*	admin dan user dapat mengakses menu home sehingga menampilkan informasi halaman home pada beranda	Sesuai
2	Menu Daftar Matakuliah	Halaman yang tampil adalah informasi daftar matakuliah yang sudah ada dalam database.	Sesuai
3	Menu *Login*	Halaman ini menampilkan form login untk admin masuk ke halaman operator.	Sesuai

4. KESIMPULAN

Adapun kesimpulan yang terdapat dalam penelitian ini adalah sebagai berikut :

a. SQL Injeksi merupakan salah satu teknik dari sekian bnayaknya cara untk membobol website yang digunakan oleh hacker
b. SQL Injeksi akan mudah dioperasikan pada website yang tidak menggunakan proteksi atau kemanan website
c. SQL Injeksi dapat juga dicegah dengan cara menerapkan kemanan website melalui penggunaan captcha, OTP,anti injeksi dibagian sintax query database pada source code dan menerapkan validasi tertentu seperti membatasi jumlah inptan karakter serta mengubah jenis inputan pada form login

REFERENSI

[1] Indonesia Cyber Security Report 2015, Id-SIRTII/CC, 2015
[2] Justin Clarke, (2009), SQL Injection Attacks and Defense, Syngress Publisher
[3] N. L. P. S. Aditya Herdinata Putra, Dian Pramana, "Sistem Manajemen Arsip Menggunakan Framework Laravel dan Vue.Js (Studi Kasus : BPKAD Provinsi Bali)," J. Sist. dan Inform., vol. 13, no. 2, 2019.
[4] SQL Injection Fact Sheet, Veracode, 2012
[5] Z. Zulkifli and S. Samsir, "Implementasi Sistem Keamanan SQL Injection Dalam berbasis web," U-NET Tek. Inform., vol. 04, no. 01, pp. 13–17, 2020.
[6] S. Samsir and S. Z. 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.
[7] W. Fahrozi and S. Samsir, "PENERAPAN ANALYTICAL NETWORK PROCESS (SAW) DALAM MENENTUKAN RAS AYAM SERAMA SIMPLE ADDECTIV WEIGHTING," U-NETJurnalTeknik Inform., vol. 3, no. 5, pp. 23–27, 2019.
[8] W. Fahrozi, S. Samsir, and D. I. G. Hts, "Penerapan E-Commerce Pada Toko Bunga Underwear," U-NET J. Tek. Inform., vol. 04, no. 01, pp. 4–9, 2020.
[9] S. 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," Riau J. Comput. Sci., vol. 05, no. 01, pp. 38–47, 2019.
[10] S. Samsir and M. Siddik, "RANCANG BANGUN SISTEM INFORMASI POS (POINT OF SALE) UNTUK KASIR MENGGUNAKAN KONSEP BAHASA," JOISIE J. Inf. Syst. Informatics Eng., vol. 4, no. 1, pp. 43–48, 2020.
[11] Samsir, S., Ambiyar, A., Verawardina, U., Edi, F., & Watrianthos, R. (2021). Analisis Sentimen Pembelajaran Daring Pada Twitter di Masa Pandemi COVID-19 Menggunakan Metode Naïve Bayes. JURNAL MEDIA INFORMATIKA BUDIDARMA, 5(1), 157-163.
[12] Syawaluddin, F. A., Yana, R. F., Siagian, T. N., & Watrianthos, R. (2020). Efektifitas Media ICT dalam Meningkatkan Motivasi Belajar dan Hasil Belajar Pendidikan Agama Islam Kelas X SMK Swasta Siti Banun Rantauprapat Kabupaten Labuhan Batu. Pena Cendikia, 2(1), 18-26.
[13] S. Samsir and F. Edi, "UNET | Jurnal Ilmiah Teknik Informatika LPPM Universitas Al Washliyah Labuhanbatu UNET | Jurnal Ilmiah Teknik Informatika ISSN . 2460-3694 , Vol . 2 No . 1 Februari 2018," U-NET J. Tek. Inform., vol. 2, no. 1, pp. 2–5, 2018.