Penetration Testing Database Menggunakan Metode SQL Injection Via SQLMap di Termux

by Ridho Pamungkas

Submission date: 03-Nov-2022 03:33PM (UTC+0700)
Submission ID: 1943266179
File name: PAPER_ANDRIA_UNIPMA-IJIE_1.docx (1.14M)
Word count: 1486
Character count: 9834

Penetration Testing Database Menggunakan Metode SQL Injection Via SQLMap di Termux

Andria[1], Ridho Pamungkas[2]
[1,2]Universitas PGRI Madiun; Jl Setia Budi No. 85, Madiun
[1,2]Jurusan Sistem Informasi, Fakultas Teknik, UNIPMA, Madiun
e-mail: [1]andria@unipma.ac.id, [2]ridho.pamungkas@unipma.ac.id

Abstrak— *Penetration Testing (Pentest) merupakan sebuah metode evaluasi terhadap keamanan pada suatu sistem dan jaringan komputer dengan melakukan suatu pengujian, salah satu metode pengujian yang dapat digunakan adalah SQL Injection. SQL Injection merupakan suatu teknik hacking dengan fokus pengujian pada database sebagai media penyimpanan data pada sistem. Tool yang digunakan pada penelitian ini ialah SQLMap yang merupakan tool open source yang dapat menganalisa, mendeteksi dan melakukan exploit (sebuah kode yang dapat menyerang keamanan sistem komputer secara spesifik) pada bug SQL Injection. Pengujian dilakukan menggunakan perangkat Smartphone bersistem operasi Android dengan program aplikasi Termux sebagai emulator terminal berbasis linux. Penelitian ini bertujuan untuk menguji keamanan database pada suatu web server dan membantu administrator atau pengelola web untuk dapat memeriksa adanya celah keamanan database yang dapat dieskploitasi oleh peretas.*

Kata kunci : *Penetration Testing, Database, SQL Injection, SQLMap, Termux*

I. PENDAHULUAN

Perkembangan Teknologi Informasi dan Sistem Informasi yang semakin pesat membawa perubahan besar dalam dunia usaha atau organisasi. Pemanfaatan Teknologi Informasi dan Sistem Informasi (TI/SI) dapat menjadi bagian yang sangat penting bagi keberlangsungan suatu organisasi dalam menjalankan kegiatan operasionalnya. Pemanfaatan TI/SI yang baik dan tepat sasaran perlu direncanakan dengan baik dalam bentuk suatu rancangan yang akan menjadi dasar panduan dalam melakukan pengembangan Sistem Informasi [1].

Database sebagai media penyimpanan data pada suatu sistem informasi tentunya memiliki peranan yang sangat penting dilihat dari aspek privasi data dan kebergunaan dalam kelengkapan fitur suatu sistem informasi. Seiring perkembangan teknologi yang begitu pesat, suatu database tidak lagi hanya dapat diakses melalui server lokal / localhost (offline), melainkan juga dapat diakses melalui jaringan komputer global yang saling terkoneksi dan dapat diakses dari jarak jauh dengan pemanfaaan layanan internet.

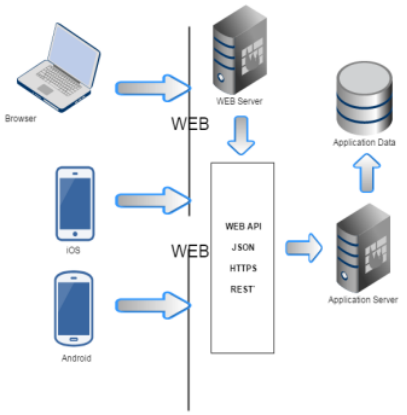
Dalam perkembangannya, keamanan data menjadi suatu bagian penting yang tidak dapat dipisahkan dalam implementasi suatu sistem infomasi. Database sebagai media penyimpanan data pada sistem informasi harus dapat dipastikan memiliki keamanan yang baik demi menjaga privasi data maupun kebergunaan dari sistem informasi tersebut. Data harus dilindungi dari segala bentuk kemungkinan ancaman para peretas yang tidak memiliki akses secara sah dengan cara melakukan upaya preventif, seperti penetration testing yang secara sederhana dapat diartikan sebagai suatu metode evaluasi dan pengujian keamanan suatu sistem dan jaringan komputer termasuk didalamnya berkaitan dengan keamanan data.

Penelitian ini membahas mengenai teknik pengujian keamanan dengan metode SQL Injection yang merupakan suatu teknik hacking dengan fokus pengujian pada database sebagai media penyimpanan data pada sistem dengan cara memasukkan suatu perintah-perintah SQL melalui URL Address untuk kemudian dieksekusi oleh database yang terdapat pada web server. Tool yang digunakan pada penelitian ini ialah SQLMap yang merupakan tool open source yang dapat menganalisa, mendeteksi dan melakukan exploit (sebuah kode yang dapat menyerang keamanan sistem komputer secara spesifik) pada bug SQL Injection. Pengujian dilakukan menggunakan perangkat Smartphone bersistem operasi Android dengan program aplikasi Termux sebagai sebuah terminal berbasis linux.

Penelitian ini bertujuan untuk menguji keamanan database pada suatu web server dan membantu administrator atau pengelola web untuk dapat memeriksa adanya celah keamanan database yang dapat dieskploitasi oleh peretas sehingga dapat dilakukan upaya preventif dalam mengamankan database pada suatu web server.

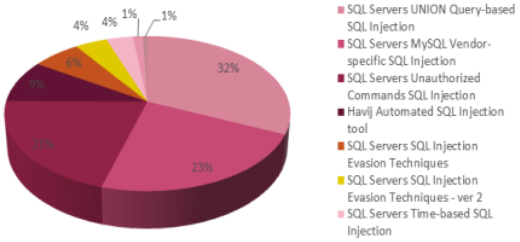
II. LANDASAN TEORI

Belakangan ini berkembang berbagai cara untuk menghack suatu web server tergantung dengan kelemahan dari web server tersebut. Salah satu dengan cara hacking web server dengan SQL Injection. SQL Injection merupakan sebuah teknik hacking dimana seorang penyerang dapat memasukkan perintah-perintah SQL melalui URL untuk dieksekusi oleh database. Penyebab utama dari celah ini adalah variable yang kurang di filter, jadi hacker dapat dengan mudah mendapatkan data dari web server targetnya [2]



Gambar 1. Application Server
(*http://www.starrybyte.com*)

Keamanan data pada suatu web server dapat dijadikan salah satu indikator kualitas website. Menurut Endang Supriyati, kualitas *website* dipengaruhi tiga hal yaitu kulitas system (*system quality*),kualitas layanan(*service quality*) dan kualitas informasi (*information quality*) [3]. Kualitas *website* dipengaruhi oleh beberapa faktor kualitas, kualitas informasi dapat mendiskripsikan mengenai kualitas konten dari suatu *website* [4].

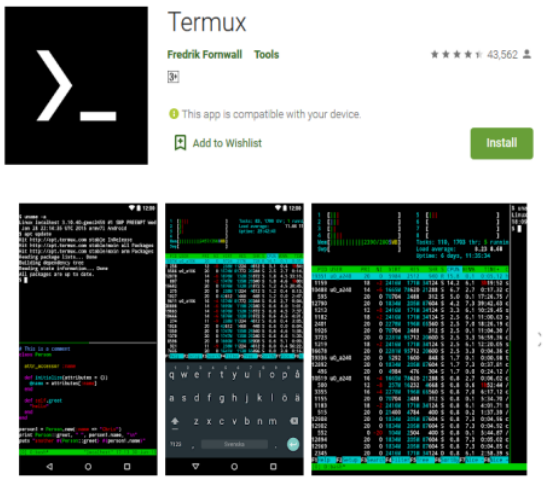


Gambar 2. SQL Injection Trends
(*https://blog.checkpoint.com*)

Salah satu contoh aplikasi SQL injeksi adalah SQLMAP, yang memeriksa situs web untuk kerentanannya [5]. SQLMap merupakan sebuah tool dengan sumber terbuka (open source) untuk mengeksekusi bug SQL dengan memasukkan perintah-perintah query tertentu melalui URL situs. SQLMap terdapat pada *operating system* Kali Linux, namun seiring perkembangannya SQLMap juga dapat dijalankan di Smartphone dengan sistem operasi Android melalui aplikasi Termux.

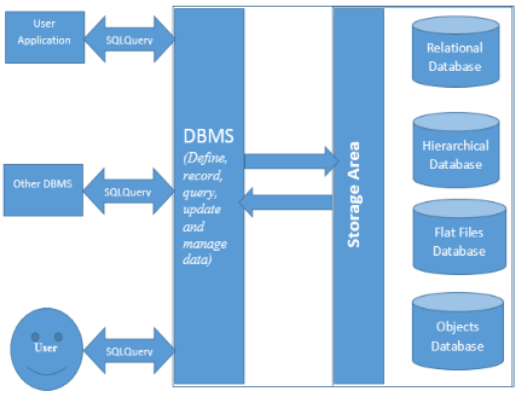
Gambar 3. SQLMap Tool
(*http://sqlmap.org/*)

Termux adalah aplikasi gratis yang dapat diunduh melalui PlayStore, termux merupakan emulator terminal Android yang juga merupakan environtment Linux. Aplikasi ini dapat dijalankan secara langsung tanpa harus dilakukan rooting sehingga dapat langsung di install dan digunakan. Kegunaan aplikasi ini diantaranya dapat dijadikan media untuk melakukan pengujian keamanan terhadap suatu kerentanan pada database.



Gambar 4. Termux on Google Play
(*https://play.google.com*)

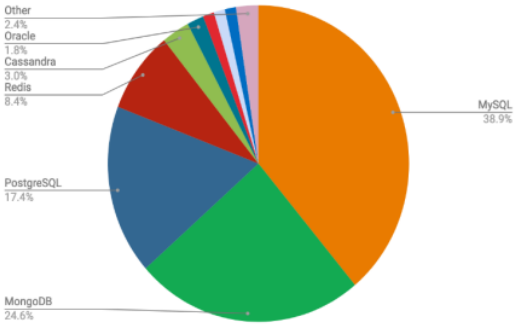
Database merupakan suatu kumpulan data terhubung (*integrated*) yang disimpan secara bersama pada suatu media, data disimpan dengan cara tertentu sehingga mudah untuk digunakan sehingga proses modifikasi data dapat dilakukan dengan mudah dan terkontrol [6]. Perancangan *database* difungsikan untuk menentukan struktur tabel dan relasi tabel yang akan diimplementasi ke dalam basis data MySQL [7].



Gambar 5. Database Management System (*https://www.sqlrelease.com*)

Database Management System (DBMS) merupakan perangkat lunak untuk mengendalikan pembuatan, pemeliharaan, pengolahan, dan penggunaan data yang berskala besar. Penggunaan DBMS saat ini merupakan hal yang sangat penting dalam segala aspek, baik itu dalam skala yang besar atau kecil. Sebagai contoh media social Facebook menggunakan DBMS untuk menyimpan data-data pengguna facebook yang sangat banyak kedalam DBMS MySQL [8].

Secara sederhana, *Database Management System* (DBMS) merupakan tools yang dapat digunakan untuk mengelola basis data. DBMS yang populer digunakan yaitu MySQL. Seperti ditunjukkan pada gambar 6 sebagai berikut.



Gambar 6. DBMS Trends (*http://highscalability.com*)

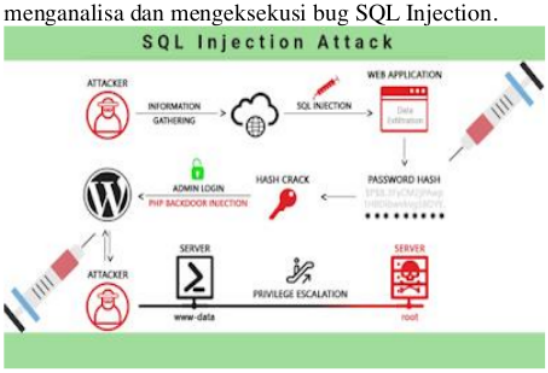
III. METODE

Metode penelitian ini menggunakan metode penelitian kuantitatif dengan melakukan uji coba atau eksperimen langsung ke web server target dengan memasukkan perintah-perintah SQL tertentu melalui URL Address suatu situs. Adapun pengumpulan data dengan dua cara yaitu:

1) Studi pustaka, mempelajari jurnal-jurnal ilmiah dan laporan penelitian
2) Studi lapangan, melakukan penetration testing atau pengujian secara langsung ke web target

IV. HASIL

Perangkat yang digunakan pada penelitian ini meliputi: Smartphone bersistem operasi Android, Termux sebagai emulator terminal Android dan SQLMap untuk menganalisa dan mengeksekusi bug SQL Injection.



Gambar 7. Ilustrasi Serangan SQL Injection (*https://www.lamhek1337.me*)

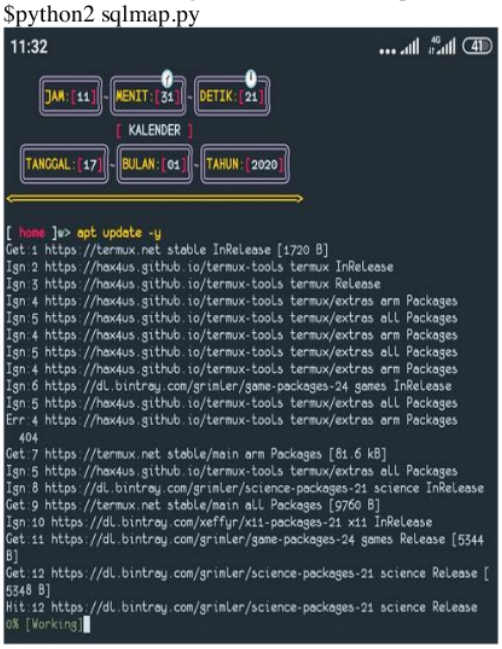
Pertama kali yang perlu dilakukan adalah menginstall terlebih dahulu aplikasi Termux yang dapat diunduh melalui PlayStore. Buka aplikasi Termux dan ketikkan beberapa perintah berikut untuk mengupdate maupun menginstall package yang diperlukan.

Gambar 8. Tampilan Aplikasi Termux

1. Perintah untuk mengupdate package
   $apt update –y
2. Perintah untuk menginstall bahasa python
   $apt install python python2 –y
3. Perintah untuk menginstall git agar bisa cloning
   $apt install git
4. Perintah untuk mengeksekusi tool SQLMap
   $git clone https://github.com/sqlmapproject/sqlmap
5. Perintah untuk masuk ke directory tool

$cd sqlmap

6. Perintah untuk menjalankan tool SQLMap
   $python2 sqlmap.py



Gambar 9. Proses Instalasi Package

Gambar 10. Package Terinstall

Selanjutnya, tahap penetration testing dengan metode SQL Injection menggunakan SQLMap melalui aplikasi Termux. Pada penelitian ini dicontohkan sebuah situs yang memiliki celah keamanan. Pengujian dilakukan dengan memasukkan perintah-perintah SQL melalui URL. Kemudian, SQLMap akan melakukan analisa dan mengeksekusi dari perintah-perintah tersebut seperti yang ditampilkan pada gambar 5.

Gambar 11. SQLMap Mengeksekusi Perintah SQL Injection

Berdasarkan hasil penetration testing yang ditampilkan pada gambar 5 tersebut dapat dijelaskan bahwa terdapat celah keamanan yang dapat dieksploitasi oleh peretas sehingga dapat menampilkan database yang ada pada suatu web server. Hal ini tentu sangat berbahaya mengingat peran database sebagai media penyimpanan data yang menyimpan informasi penting. Sehingga perlu dilakukan upaya preventif agar akses yang tidah sah (illegal) dapat diantisipasi agar tidak mengakibatkan dampak serius seperti penyalahgunaan data oleh pihak yang tidak bertanggung jawab.

V. KESIMPULAN

Penetration testing sangat diperlukan untuk pengujian dan evaluasi terhadap adanya kemungkinan celah keamanan. Hasil dari penetration testing dapat dijadikan dasar untuk perbaikan agar sistem informasi yang dibangun lebih aman dan terhindar dari serangan para peretas jahat *(blackhat)* yang dapat merugikan.

DAFTAR PUSTAKA

[1] Andria dan Hani Atun Mumtahana, "Perancangan Sistem Informasi Prakerin Universitas PGRI Madiun Berbasis Web", *Generation Journal, Vol. 3 No.1, Januari 2019*.

[2] Halib, Bin Badaruddin. Edy Budiman dan Hario Jati Setyadi, "Teknik Hacking Web Server Dengan SQLMap di Kali Linux", *JURTI, Vol 1 No. 1, Juni 2017, ISSN: 2579-8790*

[3] Supriyati, Endang, "Studi Empirik Social Commerce (S-Commerce) Dari Sudut Pandang Kualitas Website", *Jurnal SIMETRIS, 2015*.

[4] Andria, "Evaluasi Kualitas Web Portal Fakultas Teknik UNIPMA Dengan Metode McCall", *Jurnal Sistem Informasi Indonesia (JSII) Volume 3 Nomor 2 (2018)*.

[5] Lika, Sudiharyanto, Roy Dwi Putra Halim, Ihsan Verdian, "Analisa Serangan SQL Injeksi Menggunakan SQLMAP, *Positif: Jurnal Sistem dan Teknologi Informasi*, *Volume 4, No. 2,2018, pp. 88-94*.

[6] Worang and E. Sutanta, "Sistem Basis Data",*Yogyakarta: Graha Ilmu, 2004*.

[7] Andria, "Perancangan Sistem Informasi Administrasi Surat Desa Menggunakan Basis Data MySQL", *Research: Journal of Computer, Information System & Technology Management, Vol.1 No.2, April 2018, Pages 12 – 16*.

[8] Warman, Indra dan Rizki Ramdaniansyah, "Analisis Perbandingan Kinerja Query Database Management System (DBMS) Antara MySQL 6.7.16 dan MariaDB 10.1", *Jurnal TEKNOIF Vol 6 No 1 April 2018*.

Penetration Testing Database Menggunakan Metode SQL Injection Via SQLMap di Termux

ORIGINALITY REPORT

17%	14%	6%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

1%

★ worldwidescience.org

Internet Source

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		