IJAI (Indonesian Journal of Applied Informatics)
Vol. 5 No.1 Tahun 2020 pISSN: 2548-3846, eISSN: 2598-5981

Penetration Testing Database Menggunakan Metode *SQL Injection Via SQLMap* di *Termux*

Andria*, Ridho Pamungkas
Program Studi S1 Sistem Informasi, Fakultas Teknik, Universitas PGRI Madiun
Email : andria@unipma.ac.id*, ridho.pamungkas@unipma.ac.id

Info Artikel

Kata Kunci :
Basis Data, Pengujian Penetrasi, *SQL Injection*, *SQLMap*, *Termux*

Keywords :
Database, *Penetration testing*, *SQL Injection*, *SQLMap*, *Termux*

Tanggal Artikel
Dikirim : 21 Maret 2020
Direvisi : 07 September 2020
Diterima : 30 November 2020

Abstrak

Penetration testing (Pentesting) 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. Tujuan dari penelitian ini untuk pengujian keamanan database web server dan membantu pengelola atau admin situs web untuk dapat memeriksa adanya celah kerentanan database yang dapat dieskploitasi oleh peretas.

Abstract

Penetration testing (Pentesting) is a method of evaluating the security of a computer system and network by conducting a test, one of the testing methods that can be used is SQL Injection . SQL Injection is a hacking technique that focuses on testing the database as a data storage medium on the system. The tool used in this study is SQLMap which is an open source tool that can analyze, detect and exploit (a code that can specifically attack computer system security) on the SQL Injection bug. Testing was carried out using a Smartphone device with the Android operating system with the Termux application program as a linux-based terminal emulator. The purpose of this research is to test the security of the web server database and help the website manager or admin to be able to check for any database vulnerabilities that can be exploited by hackers.

1. PENDAHULUAN

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*, melainkan juga dapat diakses melalui jaringan komputer global yang saling terkoneksi dan dapat diakses dari jarak jauh dengan pemanfaaan layanan internet.

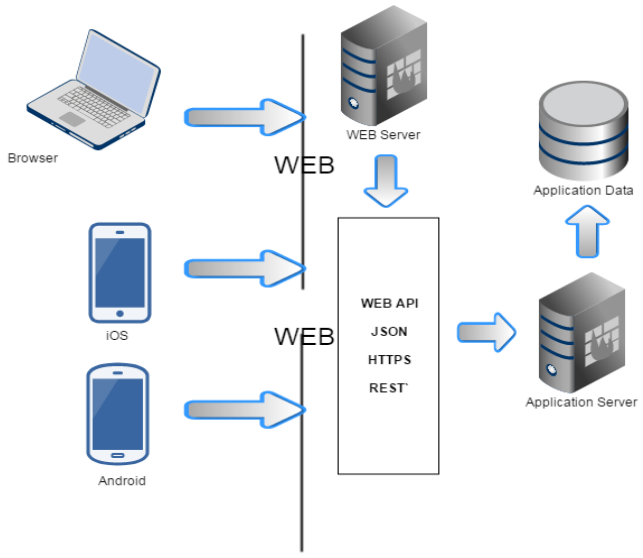
Dalam perkembangannya, keamanan data menjadi suatu bagian penting yang tidak dapat dipisahkan dalam implementasi suatu sistem infomasi. *Database* sebagai media penyimpanan data pada sistem informasi harus dapat dipastikan memiliki keamanan yang baik demi menjaga privasi data maupun kebergunaan dari 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.

Adapun penelitian sebelumnya yang berjudul "Analisis Celah Keamanan *Website* Menggunakan *Tools WEBPWN3R* di *Kali Linux*", menjelaskan bahwa adanya celah keamanan (*bug*) pada suatu website tentu memerlukan perhatian serius agar tidak dieksploitasi oleh pihak yang tidak bertanggung jawab. Berdasarkan hal tersebut, tentunya diperlukan adanya upaya preventif diantaranya dengan melakukan analisis terhadap kemungkinan adanya celah keamanan pada suatu website. Pada penelitian tersebut, *tools* yang digunakan adalah *WEBPWN3R* yang merupakan *Web Applications Security Scanner, tool open source* ini dapat menganalisa, mendeteksi adanya bug dari suatu website. Pengujian dilakukan menggunakan perangkat komputer bersistem operasi *Kali Linux*. Penelitian tersebut bertujuan untuk menganalisa adanya celah keamanan pada suatu *website* dan membantu *administrator* atau pengelola web untuk dapat mengetahui adanya kemungkinan celah keamanan pada suatu *website,* sehingga dapat segera dilakukan perbaikan dengan tepat berdasarkan temuan kerentanan atau celah keamanan yang terdapat pada website tersebut [1].

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 *Structured Query Language (SQL)* melalui *Uniform Resource Locator (URL) Address* untuk kemudian di eksekusi oleh basis data 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* .

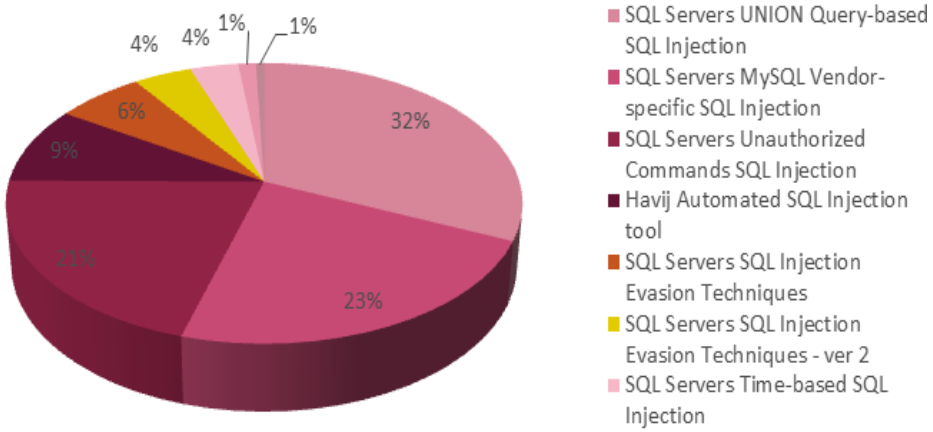
Uji keamanan dilakukan dengan menggunakan perangkat *Smartphone* yang memakai sistem operasi Android dengan program aplikasi *Termux* sebagai sebuah terminal berbasis linux. Tujuan penelitian ini adalah untuk menguji keamanan atau kerentanan *database* di *web server* dan membantu pengelola atau admin situs web untuk dapat memeriksa ada tidaknya celah keamanan atau kerentanan *database* yang dapat dieskploitasi oleh peretas sehingga dapat dilakukan upaya preventif dalam mengamankan *database* pada suatu *web server*.

Belakangan ini berkembang berbagai cara untuk meng*hack* 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 variabel yang kurang difilter, jadi hacker dapat dengan mudah mendapatkan data dari *web server* targetnya [2]



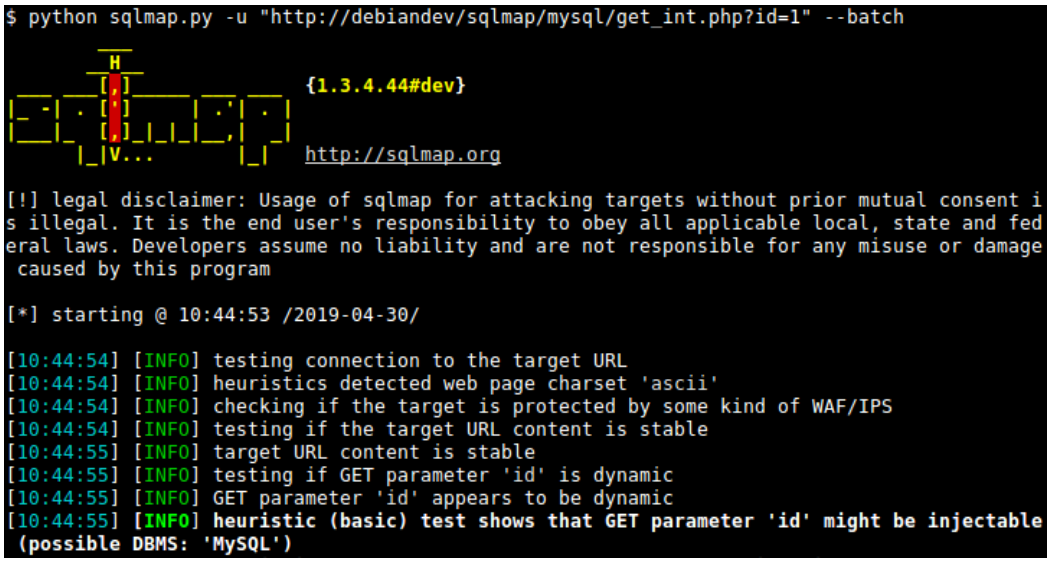
Gambar 1. Alur dan Perangkat *Application Server* (*www.starrybyte.com*)

Pada gambar 1 dapat dijelaskan bahwa pada penerapan sisi *Application Server* terdapat alur dan perangkat yang digunakan. Dimulai dengan perangkat laptop maupun ponsel yang terkoneksi dengan *web server* kemudian diteruskan ke *application server* dan dilanjutkan ke *application data* yang menampung informasi penting dari suatu sistem informasi. 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 factor kualitas, kualitas informasi dapat mendiskripsikan mengenai kualitas konten dari suatu *website* [4].



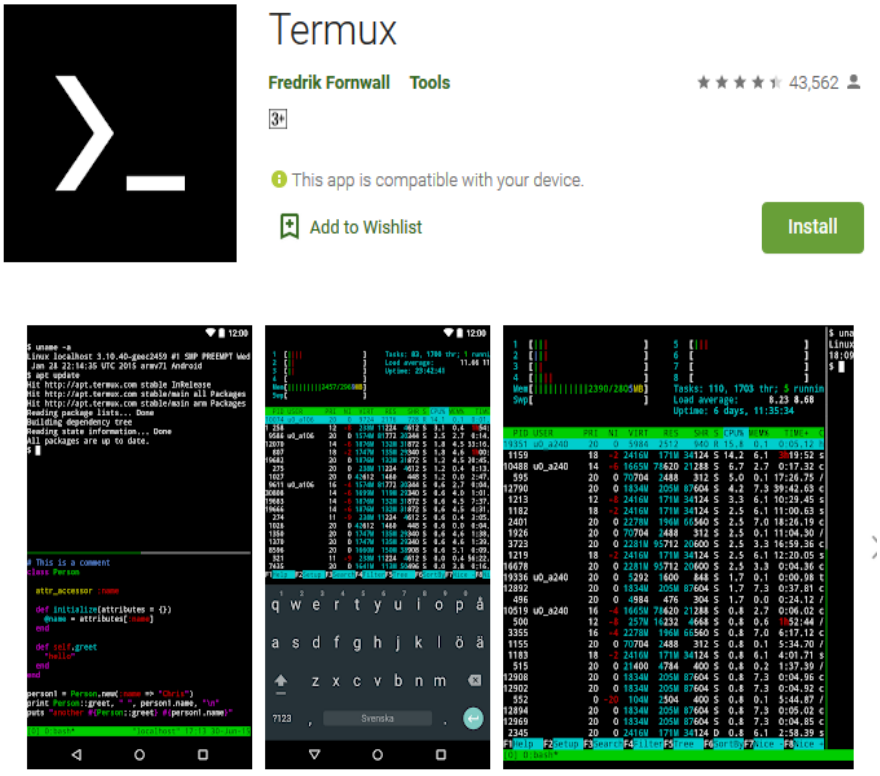
Gambar 2. *SQL Injection Trends* (*blog.checkpoint.com*)

Pada gambar 2 menunjukkan bahwa tren *SQL Injection* yang merupakan jenis celah keamanan yang paling sering ditemukan pada suatu situs web. 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*. Adapun tampilan *tool SQLMap* di aplikasi *Termux* ditunjukkan pada gambar 3 sebagai berikut.



Gambar 3. Tampilan *Tool SQL Map* (*SQLMap.org*)

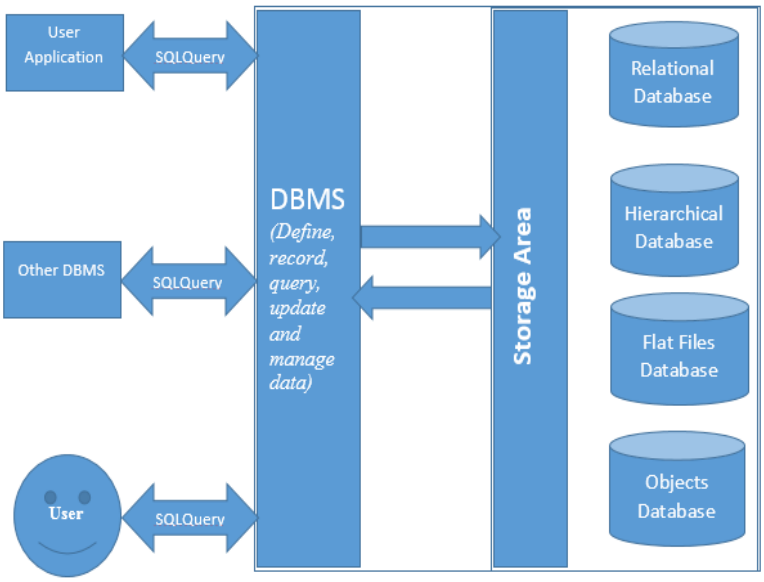
Termux adalah aplikasi gratis yang dapat diunduh melalui PlayStore, *Termux* merupakan *emulator terminal Android* yang juga merupakan *environtment Linux*. Aplikasi ini dapat dijalankan secara langsung tanpa harus dilakukan *rooting* sehingga dapat langsung di *install* dan digunakan. Kegunaan aplikasi ini diantaranya dapat dijadikan media untuk melakukan uji keamanan / kerentanan terhadap suatu *database*. Aplikasi *Termux* dapat di *install* melalui *Google Play Store* seperti terlihat pada gambar 4 sebagai berikut.



Gambar 4. Halaman *Termux* di *Google Play Store* *(play.google.com)*

Database merupakan suatu kumpulan data terhubung (*integrated*) yang disimpan secara bersama

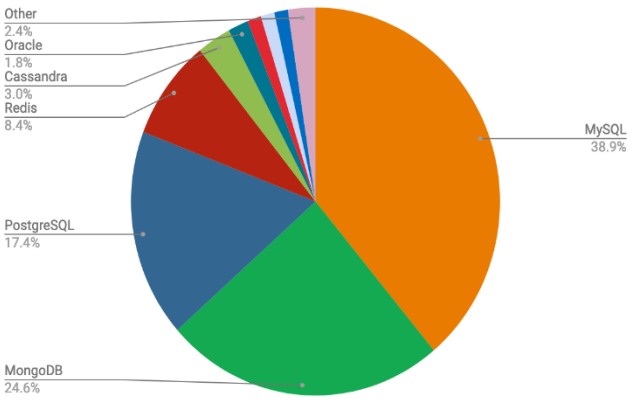
pada suatu media, data disimpan dengan cara tertentu sehingga mudah untuk digunakan sehingga proses modifikasi data dapat dilakukan dengan mudah dan terkontrol [6]. Perancangan *database* difungsikan untuk menentukan struktur tabel dan relasi tabel yang akan diimplementasi ke dalam basis data *MySQL*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



Gambar 5. *Database Management System (DBMS)* (*sqlrelease.com*)

Gambar 5 dapat dijelaskan bahwa *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.



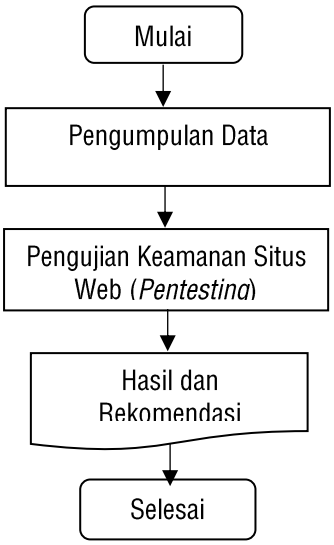
Gambar 6. *DBMS Trends* (*http://highscalability.com*)

2. METODE PENELITIAN

Pada penelitian ini, adapun metode yang digunakan adalah metode *Systematic Literature Review (SLR)* yang merupakan metode *literature review* yang mengidentifikasi, menilai, dan menginterpretasi seluruh

temuan-temuan pada suatu topik penelitian. Adapun temuan celah kerentanan pada situs web didapat dengan melakukan eksperimen atau uji coba secara langsung ke *web server* target dengan menggunakan inputan atau masukan perintah *SQL* tertentu melalui *URL Address* suatu situs web.

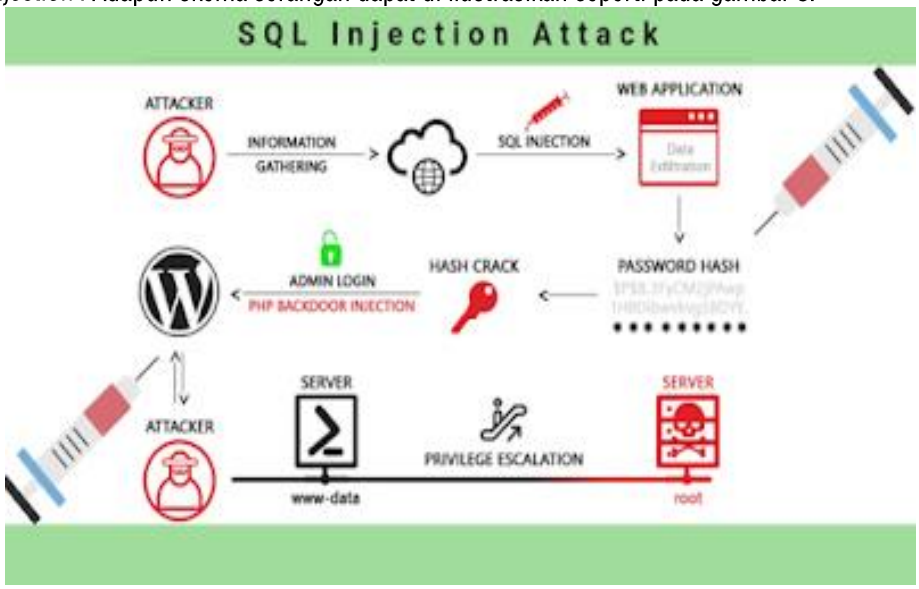
Pada penelitian ini, pengumpulan data berupa data utama yang didapat dari studi lapangan yang terdiri dari hasil observasi terhadap situs web target. Selain itu pengumpulan data yang diperoleh dari penelitian sebelumya berupa jurnal dan sumber referensi lain seperti buku.



Gambar 7. Alur Penelitian

3. HASIL DAN PEMBAHASAN

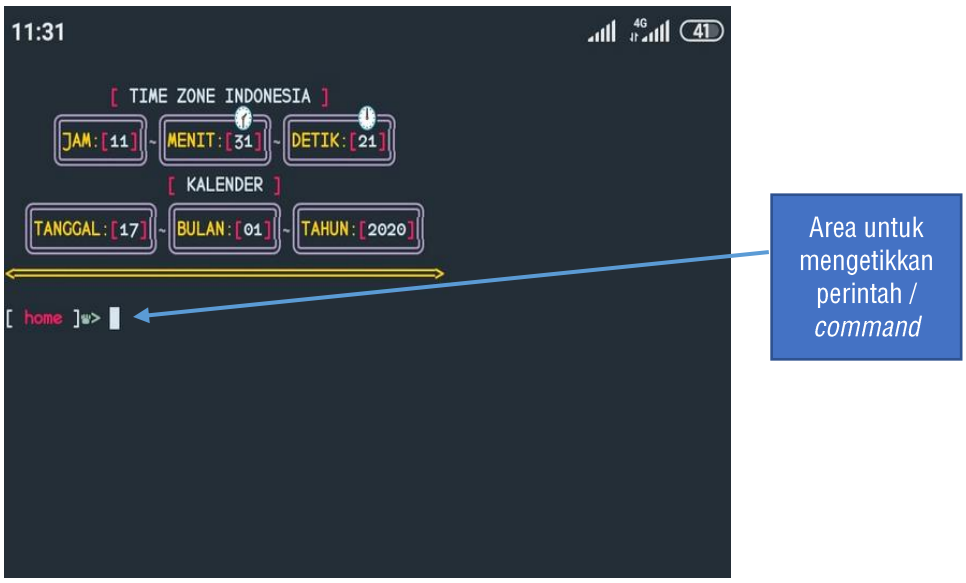
Pada peneltian ini, adapun perangkat atau alat-alat yang digunakan seperti *Smartphone* bersistem operasi *Android, Termux* sebagai *emulator terminal Android* dan *SQLMap* untuk menganalisa dan mengeksekusi *bug SQL Injection* . Adapun skema serangan dapat di ilustrasikan seperti pada gambar 8.



Gambar 8. *SQL Injection Attack (Iamhek1337.me)*

Pada gambar 8 dapat dijelaskan bahwa *SQL Injection* merupakan suatu teknik penyerangan web dengan menggunakan kode *SQL (Structured Query Language)* yang berbahaya untuk memanipulasi *database.* Seorang *attacker* atau penyerang terlebih dahulu mengumpulkan informasi dari situs web target, kemudian mencari adanya celah *SQL Injection* pada *web application* yang kemudian dilanjutkan dengan pengujian celah keamanan secara lebih spesifik dengan *tool* seperti *SQLMap* yang apabila *bug* tersebut valid maka *attacker* dapat masuk pada *server database* yang menyimpan informasi sensitif dari situs web tersebut.

Adapaun langkah pertama kali yang perlu dilakukan sebelum melakukan pengujian celah keamanan sistem adalah menginstall terlebih dahulu aplikasi *Termux* yang dapat diunduh melalui *PlayStore*. Buka aplikasi *Termux* dan ketikkan beberapa perintah berikut untuk melakukan *update* maupun *install package* yang diperlukan. Tampilan awal aplikasi *Termux* seperti ditunjukkan pada gambar 9.



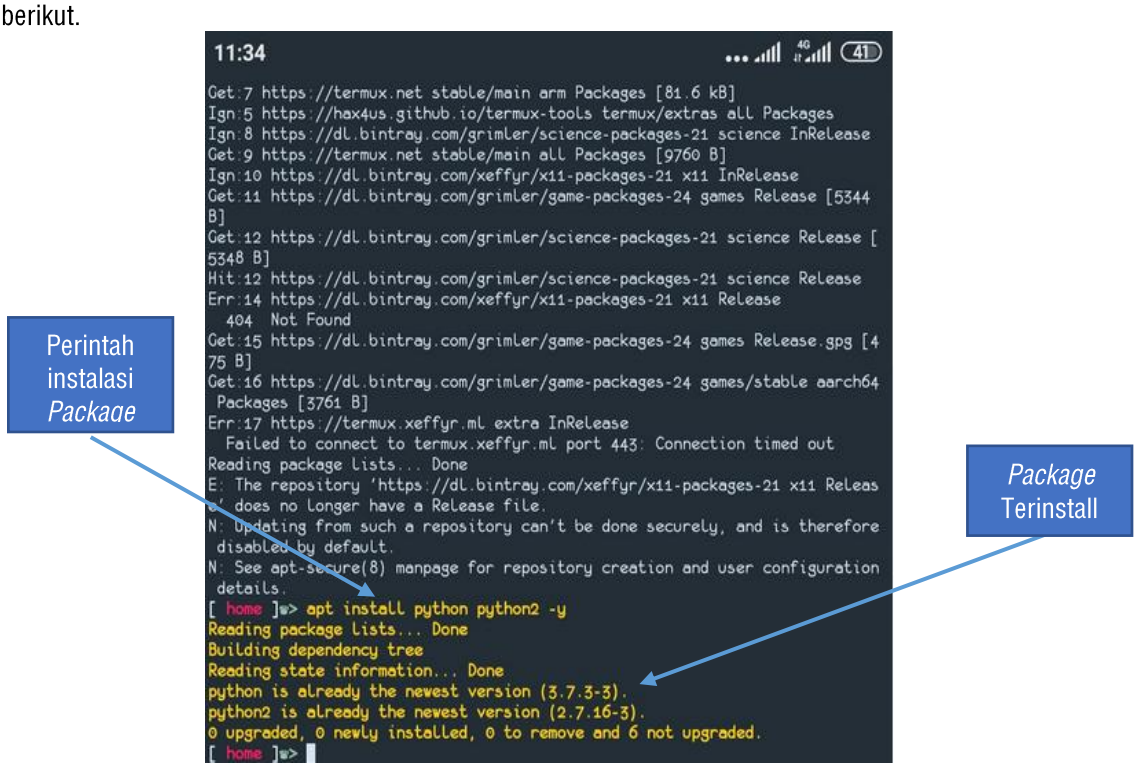
Gambar 9. Tampilan Awal Aplikasi *Termux*

Setelah aplikasi *Termux* terbuka, maka perlu dilakukan langkah-langkah konfigurasi sebagai berikut

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 7ias *cloning*
   $apt install git
4. Perintah / *command* untuk *clone SQLMap Tool*
   $git clone https://github.com/*SQLMap*project/*SQLMap*
5. Perintah atau *command* untuk masuk ke direktori *SQLMap*
   $cd *SQLMap*
6. *Command* atau perintah untuk dapat menjalankan *SQLMap Tool*
   $python2 *SQLMap*.py

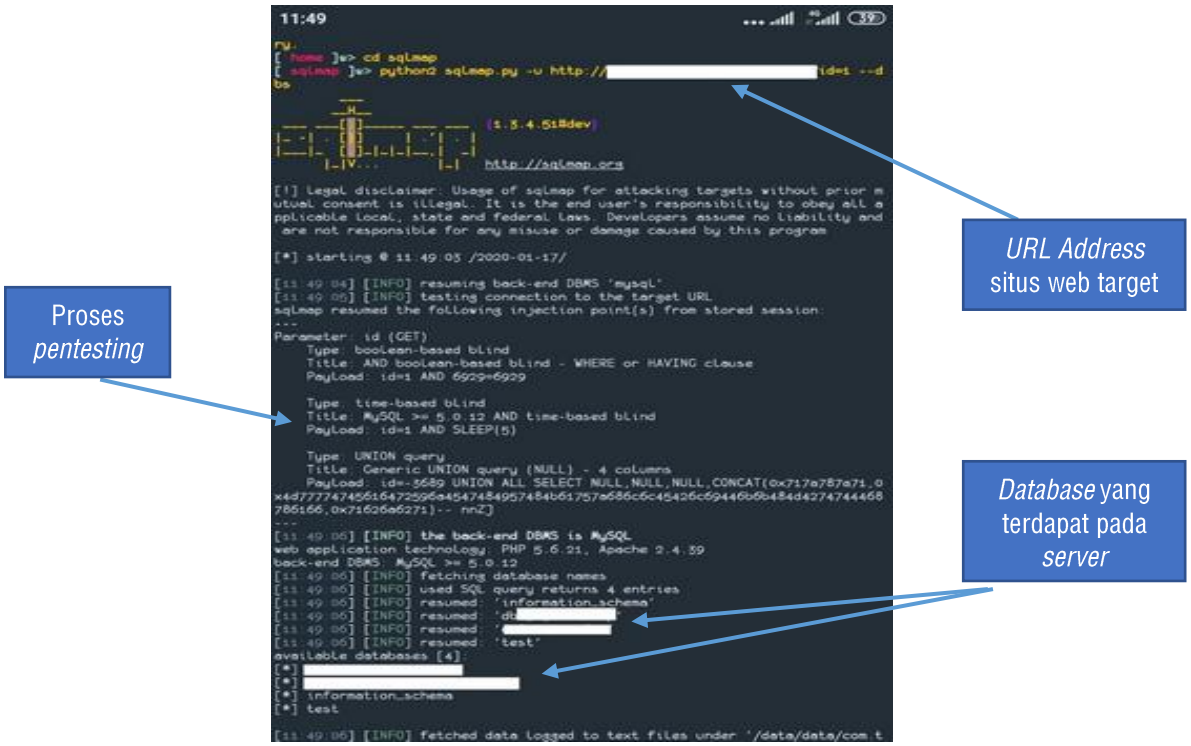
Gambar 10. Proses *Install Package*

Pada gambar 10 tersebut menunjukkan proses instalasi paket-paket yang dibutuhkan sebelum dapat melakukan *penetration testing database* menggunakan *tool SQLMap* pada aplikasi *Termux*. Setelah proses instalasi *package* atau paket selesai dan berhasil maka akan ditunjukkan seperti pada gambar 11 sebagai berikut.



Gambar 11. *Package* Berhasil Terinstall

Selanjutnya, tahap *penetration testing* dengan metode *SQL Injection* menggunakan *SQLMap* melalui aplikasi *Termux*. Pada penelitian ini dicontohkan sebuah situs web yang memiliki celah keamanan pada lapisan basis data. 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 12. Beberapa bagian pada gambar 12 sengaja disensor karena mengandung informasi sensitif dan melindungi privasi web target.



Gambar 12. *SQLMap* Mengeksekusi Perintah *SQL Injection* dan Menampilkan Hasil

Berdasarkan hasil *penetration testing* yang ditampilkan pada gambar 12 tersebut dapat diuraikan bahwa terdapat adanya celah keamanan atau kerentanan yang memungkinkan untuk dilakukan eksploitasi oleh *hacker* / peretas sehingga dapat menampilkan dan mengakses struktur *database* yang terdapat di *web server*. Hal tersebut tentu sangat riskan dan berbahaya mengingat peran *database* sebagai media penyimpanan data yang menyimpan informasi penting. Sehingga, berdasarkan temuan tersebut perlu dilakukan upaya pencegahan / preventif agar akses yang tidah semestinya, akses tidak sah (*illegal access*) dapat diantisipasi dan diminimalisir agar tidak mengakibatkan dampak kerugian yang serius seperti penyalahgunaan data oleh pihak-pihak yang tidak bertanggung jawab.

4. 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 terjamin keamanannya serta dapat terhindar dari serangan *hacker* atau peretas yang berniat jahat *(blackhat)* yang sangat merugikan. Pada penelitian ini didapatkan temuan celah keamanan yang disebut dengan *SQL Injection* yaitu sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi.

Adapun solusi yang dapat dilakukan oleh pengelola web atau *web administrator* untuk mencegah atau menutupi celah kerentanan tersebut yaitu diantaranya dengan menggunakan *parameterized query* atau *prepared statement*, memberikan batasan hak akses, melakukan validasi input pengguna, memberikan enkripsi basis data dan menyembunyikan pesan *error.*

.

DAFTAR PUSTAKA

[1] Andria, "Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux, "*Generation Journal / Vol.4 No.2 / e-ISSN:2549-2233 / p-ISSN:2580-4952, Juli 2020.*

[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 S QL 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.*