

Vol. 5 No. 1
NOVEMBER
TAHUN 2020

ISSN : 2598-5981



INDONESIAN JOURNAL OF APPLIED INFORMATICS



D3 TEKNIK INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS SEBELAS MARET
Jl. Ir. Sutami No. 36A Kentingan Surakarta 57126
Telp./Fax 0271-663450



Anda Dapat Mengunjungi Website melalui alamat
<https://jurnal.uns.ac.id/ijai/>



IJAI (Indonesian Journal of Applied Informatics) Vol. 5, No. 1 (2020)

SUSUNAN REDAKSI
INDONESIAN JOURNAL OF APPLIED INFORMATICS
PROGRAM STUDI DIPLOMA III TEKNIK INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS SEBELAS MARET SURAKARTA

Penasehat

Drs. SANTOSO TRI HANANTO, M.Acc., Ak.
(Dekan Sekolah Vokasi, Universitas Sebelas Maret Surakarta)

Penanggung Jawab

Hartatik, M.Si.
(Kepala Program Studi DIII Teknik Informatika SV Universitas Sebelas Maret Surakarta)

Ketua Editor

Fendi Aji Purnomo, S.Si.,M.Eng. (Scopus ID: 57193325119)
Universitas Sebelas Maret

Anggota Editor

Hartatik, M.Si. (Scopus ID : 57031919500)
Universitas Sebelas Maret
Sahirul Alim Tri B, S.Kom, M.Eng.
Universitas Sebelas Maret

Reviewer

Eko Harry P,S.T.,M.Info.Tech (Scopus ID : 56611900000)
Universitas Sebelas Maret
Nanang Maulana, S.Si, M.Eng. (Scopus ID : 57193325345)
Universitas Sebelas Maret
Liliek Triyono, ST.M.Eng. (SINTA ID : 5980680)
Politeknik Negeri Semarang
Dian Prajarini, ST. M.Eng. (SINTA ID : 5982955)
Sekolah Tinggi Seni Rupa Dan Desain Visi Indonesia
Dwi Hanto M.Si. (SINTA ID : 6694817)
Lembaga Ilmu Pengetahuan Indonesia

Alamat Redaksi:

Gd. A Lt. 1 Prodi Diploma III Teknik Informatika
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Sebelas Maret
Jl. Ir. Sutami 36A Kentingan Jebres 57126
Telp./Fax 0271-663450
Email : ijai@mipa.uns.ac.id
Website : <https://jurnal.uns.ac.id/ijai>

FOCUS AND SCOPE

Indonesian Journal of Applied Informatics menerbitkan artikel-artikel yang memiliki arti penting di bidangnya masing-masing sekaligus memberikan kontribusi terhadap disiplin ilmu informatika secara keseluruhan dan penerapannya.

Scope jurnal meliputi beberapa topik, tetapi tidak menutup kemungkinan berkisar mengenai technopreneur, cloud computing, E-Commerce, mobile Application, Information Systems, Geographic Informaton System, Database Management, Web Application, E-Learning, Game Development, Multimedia Application, Software Engineering, Computer Network, Human Computer Interaction, Decision Support System, Animation, Instrumentation, IoT.

PUBLICATION INFORMATION

Indonesian Journal of Applied Informatics (e-ISSN: 2598-5981)

Indonesian Journal of Applied Informatics akan ditertibkan satu tahun sebanyak 2 kali frekuensi terbitan yaitu di bulan Mei dan November. Di tahun 2020 di bulan Mei telah terbit issue yang kelima yaitu IJAI volume 5 Nomor 1 semenjak terbit pertama kali di bulan November 2016.

Indonesia Journal of Applied Informatics yang disebut IJAI telah menerbitkan artikel full teks dalam bentuk PDF melalui media online dengan alamat <https://jurnal.uns.ac.id/ijai>. Indonesian Journal of Applied Informatics diterbitkan oleh Program Studi Teknik Informatika Sekolah Vokasi Universitas Sebelas Maret.

Indonesian Journal of Applied Informatics telah diindeks oleh Google Scholar, Mendelay, Crossref, Garuda dan terakreditasi Sinta4



Berdasarkan KEPUTUSAN DIREKTUR JENDERAL PENGUATAN RISET DAN PENGEMBANGAN KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI REPUBLIK INDONESIA Nomor 30/E/KPT/2019 Tentang Peringkat Akreditasi Jurnal Ilmiah Periode VI Tahun 2019, **IJAI (Indonesian Journal Of Applied Informatics) Mendapat Peringkat IV Sinta mulai terbitan Volume 2 Nomor 1.**

PENGINDEKS DAN ABSTRAKSI

(IJAI) Indonesian Journal of Applied Informatics telah diindeks dan diabstraksi oleh:

- 1 Google scholar (<https://scholar.google.co.id/citations?user=kHqfkQAAAAJ&hl=id>)
- 2 Mendeley (<https://www.mendeley.com/profiles/indonesian-journal-of-ijai/>)
- 3 Crossref
(<https://search.crossref.org/?q=indonesian+journal+of+applied+informatics&type=Journal+Article&publication=Indonesian+Journal+of+Applied+Informatics&publisher=Universitas+Sebelas+Maret&source=Crossref>)
- 4 Garuda (<http://garuda.ristekdikti.go.id/journal/view/13990>)
- 5 SINTA (<http://sinta2.ristekdikti.go.id/journals/detail?page=3&id=5390>)

DAFTAR ISI

Tim Editorialii
Ruang Lingkupiii
Jurnal Pengindeks dan Abstraksiiii
Daftar Isiiv
 Penetration Testing Database Menggunakan Metode <i>SQL Injection</i> Via <i>SQLMap</i> di Termux	
Andria1-10
 Pengolahan Citra untuk Membedakan Ikan Segar dan Tidak Segar Menggunakan <i>Convolutional Neural Network</i>	
Arif Agustyawan11-19
 Rancang Bangun Dan Evaluasi Media Pengenalan Hewan Serangga Dengan Teknologi <i>Augmented Reality</i>	
Fendi Aji Purnomo*, Taufiqurrahman, Nanang Maulana Y, Hartatik, Berliana Kusuma Riasti, Kristian Hendro Subroto20-31
 Optimasi Model Prediksi Kelulusan Mahasiswa Menggunakan <i>Algoritma Naive Bayes</i>	
Hartatik32-38
 Analisis Efektifitas Penggunaan <i>Auto Scaler Barcode</i> pada <i>Inner Box</i> Menggunakan Metode Pengujian Validitas dan Reliabilitas (Studi Kasus: PT. Duta Nichirindo Pratama)	
Ade Sumaedi*, Makhsun, Achmad Hindasyah39-49
 Analisis <i>POM QM V5.2 For Windows</i> pada Penerapan Metode <i>ABC</i> dan <i>EOQ</i> Dalam Pengendalian Persediaan Bahan Baku <i>PVC Compound</i> (Studi Kasus PT.SMI)	
Amin Widodo*, Achmad Hindasyah, Makhsun Makhsun50-59
 <i>Internet of Things</i> pada Dashboard Informasi Kandang Jangkrik	
Qurnia Dwi Yoga Putra, Puji Winar Cahyo*60-66
 Implementasi <i>Naïve Bayes</i> untuk Klasifikasi Tunggakan Iuran Sekolah	
Rizal Nur Alfi*, Jajam Haerul Jaman, Riza Ibnu Adam67-75
 Editorial	
RETRACTION NOTICE TO : Komparasi Algoritma <i>Machine Learning</i> dan <i>Deep Learning</i> untuk <i>Named Entity Recognition</i> : Studi Kasus Data Kebencanaan	
Nuli Giarsyani	

Halaman Belakang

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 diesklopatasi 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 pemanfaatan layanan internet.

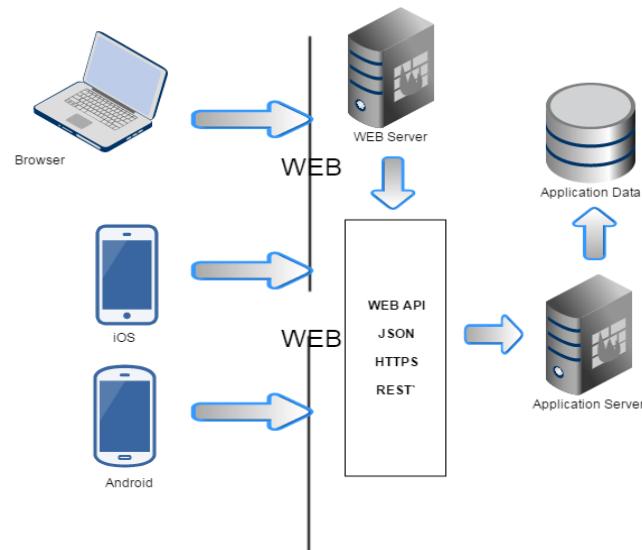
Dalam perkembangannya, keamanan data menjadi suatu bagian penting yang tidak dapat dipisahkan dalam implementasi suatu sistem informasi. *Database* sebagai media penyimpanan data pada sistem informasi harus dapat dipastikan memiliki keamanan yang baik demi menjaga privasi data maupun kebergunaan dari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

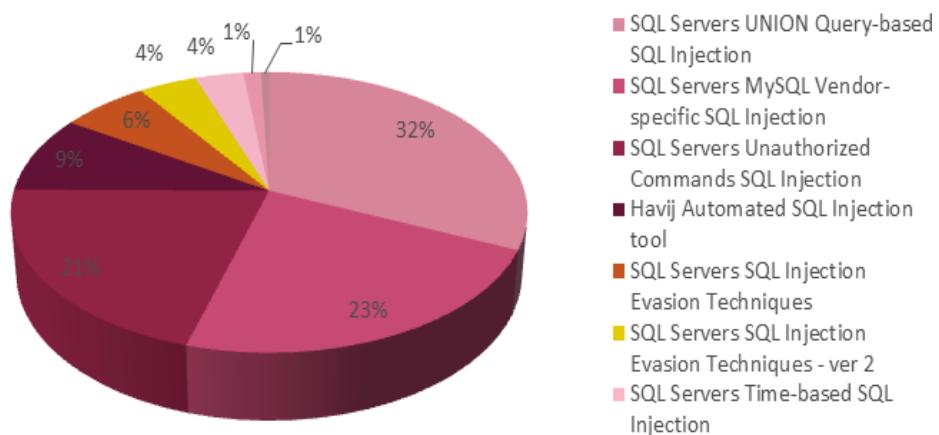
Uji keamanan dilakukan dengan menggunakan perangkat *Smartphone* yang memakai sistem operasi Android dengan program aplikasi *Termux* sebagai sebuah terminal berbasis linux. Tujuan penelitian ini adalah untuk menguji keamanan atau kerentanan *database* di *web server* dan membantu pengelola atau admin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

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 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 kualitas sistem (*system quality*), kualitas layanan (*service quality*) dan kualitas informasi (*information quality*) [3]. Kualitas *website* dipengaruhi oleh beberapa faktor kualitas, kualitas informasi dapat mendeskripsikan 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.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
[1.3.4.44#dev]
http://sqlmap.org

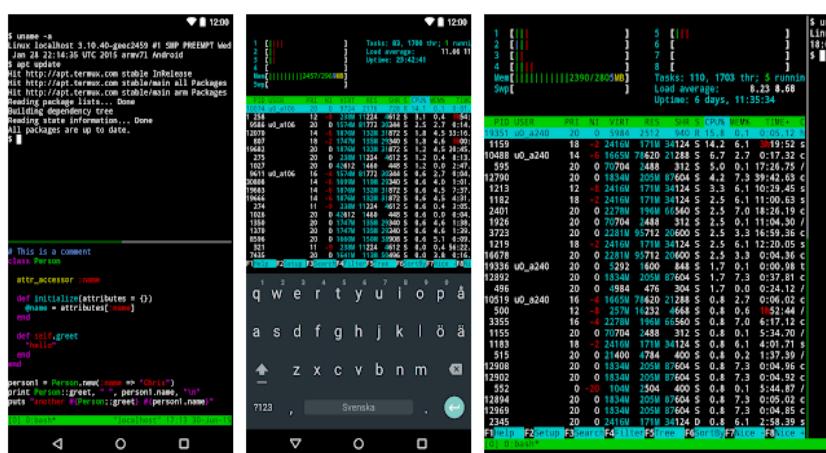
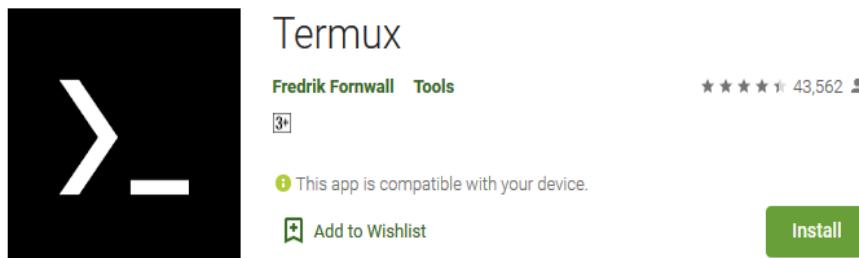
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:44:53 /2019-04-30/

[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
(possible DBMS: 'MySQL')
```

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

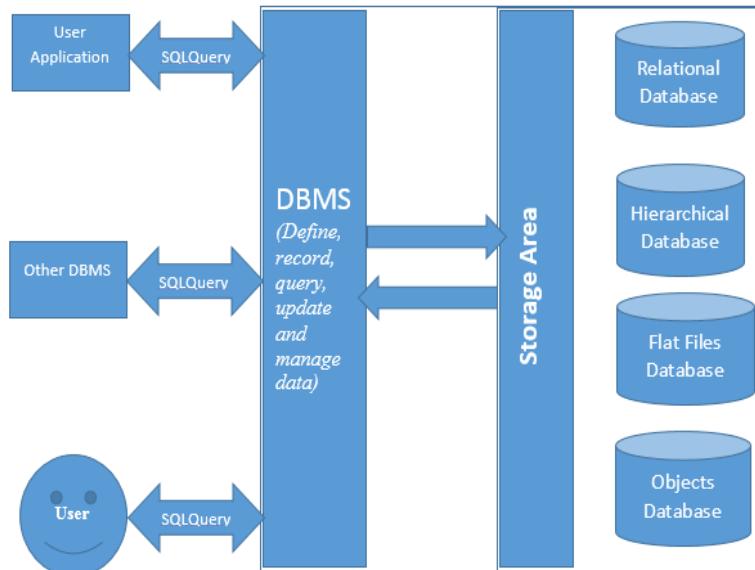
Termux adalah aplikasi gratis yang dapat diunduh melalui PlayStore, *Termux* merupakan *emulator terminal Android* yang juga merupakan *environment Linux*. Aplikasi ini dapat dijalankan secara langsung tanpa harus dilakukan *rooting* sehingga dapat langsung di *install* dan digunakan. Kegunaan aplikasi 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

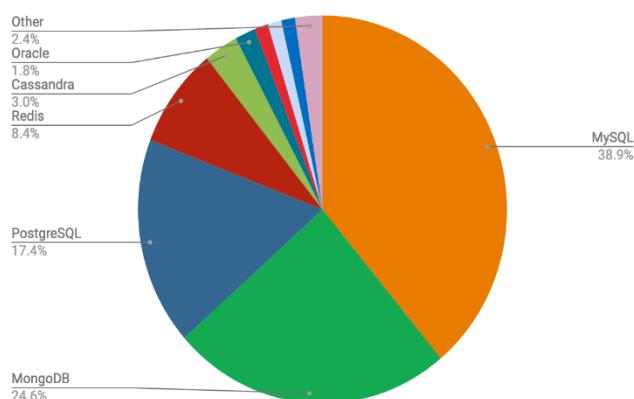
pada suatu media, data disimpan dengan cara tertentu sehingga mudah untuk digunakan sehingga proses modifikasi data dapat dilakukan dengan mudah dan terkontrol [6]. Perancangan *database* difungsikan untuk menentukan struktur tabel dan relasi tabel yang akan diimplementasi ke dalam basis data MySQL [7].



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.



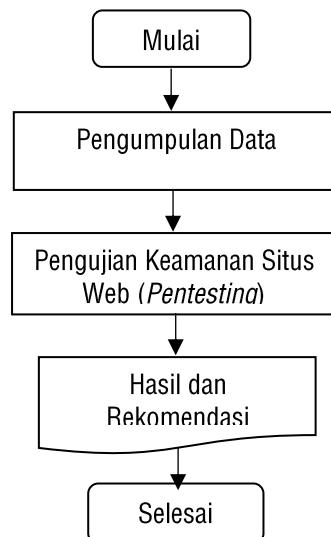
Gambar 6. *DBMS Trends*
(<http://highscalability.com>)

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 IJAI (Indonesian Journal of Applied Informatics) | 5

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.

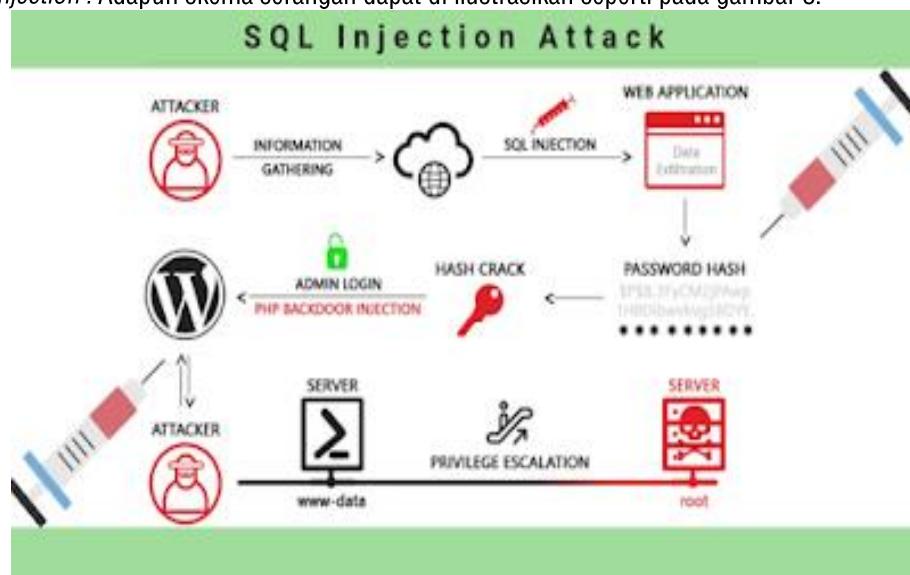
Pada penelitian ini, pengumpulan data berupa data utama yang didapat dari studi lapangan yang terdiri dari hasil observasi terhadap situs web target. Selain itu pengumpulan data yang diperoleh dari penelitian sebelumnya berupa jurnal dan sumber referensi lain seperti buku.



Gambar 7. Alur Penelitian

3. HASIL DAN PEMBAHASAN

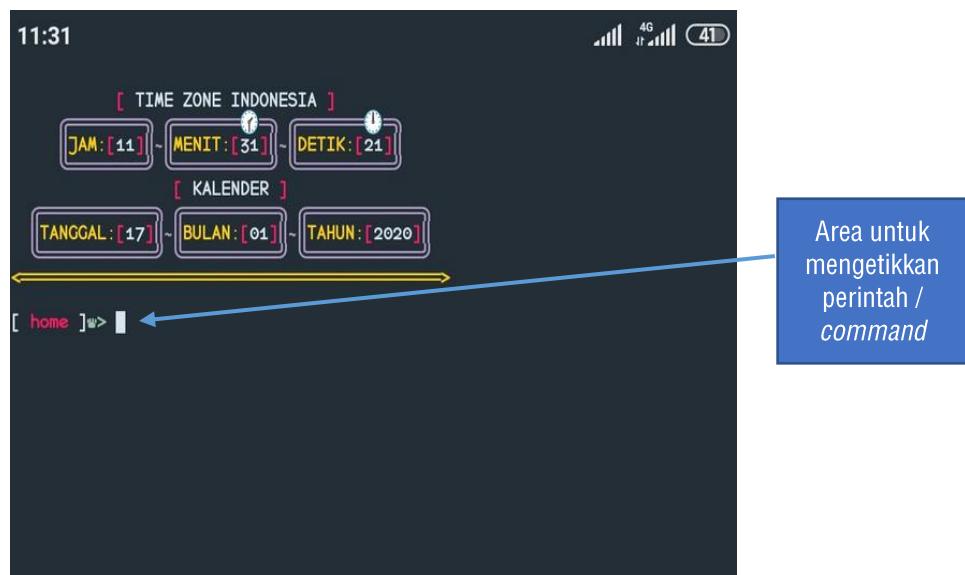
Pada penelitian ini, adapun perangkat atau alat-alat yang digunakan seperti *Smartphone* bersistem operasi *Android*, *Termux* sebagai *emulator terminal Android* dan *SQLMap* untuk menganalisa dan mengeksekusi bug *SQL Injection*. Adapun skema serangan dapat di ilustrasikan seperti pada gambar 8.



Gambar 8. *SQL Injection Attack*
(lamhek1337.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 bisa cloning
\$apt install git
4. Perintah / *command* untuk clone *SQLMap Tool*
\$git clone <https://github.com/SQLMapProject/SQLMap>
5. Perintah atau *command* untuk masuk ke direktori *SQLMap*
\$cd SQLMap
6. *Command* atau perintah untuk dapat menjalankan *SQLMap Tool*
\$python2 SQLMap.py



Proses Update Packaaes

Perintah Update Packaaes

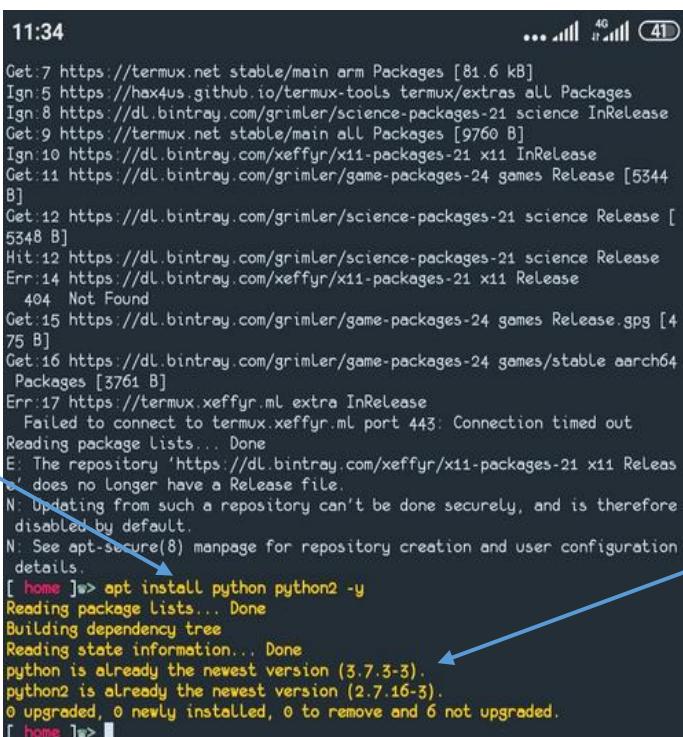
```

11:32
[ JAM:[11] - MENIT:[31] - DETIK:[21]
[ KALENDER ]
[ TANGGAL:[17] - BULAN:[01] - TAHUN:[2020]

[ home ]$> apt update -y
Get:1 https://termux.net stable InRelease [1720 B]
Ign:2 https://hex4us.github.io/termux-tools termux InRelease
Ign:3 https://hex4us.github.io/termux-tools termux Release
Ign:4 https://hex4us.github.io/termux-tools termux/extras arm Packages
Ign:5 https://hex4us.github.io/termux-tools termux/extras all Packages
Ign:4 https://hex4us.github.io/termux-tools termux/extras arm Packages
Ign:5 https://hex4us.github.io/termux-tools termux/extras all Packages
Ign:4 https://hex4us.github.io/termux-tools termux/extras arm Packages
Ign:6 https://dl.bintray.com/grimler/game-packages-24 games InRelease
Ign:5 https://hex4us.github.io/termux-tools termux/extras all Packages
Err:4 https://hex4us.github.io/termux-tools termux/extras arm Packages
        404
Get:7 https://termux.net stable/main arm Packages [81.6 kB]
Ign:5 https://hex4us.github.io/termux-tools termux/extras all Packages
Ign:8 https://dl.bintray.com/grimler/science-packages-21 science InRelease
Get:9 https://termux.net stable/main all Packages [9760 B]
Ign:10 https://dl.bintray.com/xeffyr/x11-packages-21 x11 InRelease
Get:11 https://dl.bintray.com/grimler/game-packages-24 games Release [5344 B]
Get:12 https://dl.bintray.com/grimler/science-packages-21 science Release [5348 B]
Hit:12 https://dl.bintray.com/grimler/science-packages-21 science Release
0% [Working]
    
```

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.



Perintah instalasi Packaaes

Package Terinstall

```

11:34
[ JAM:[11] - MENIT:[31] - DETIK:[21]
[ KALENDER ]
[ TANGGAL:[17] - BULAN:[01] - TAHUN:[2020]

[ home ]$> apt update -y
Get:7 https://termux.net stable/main arm Packages [81.6 kB]
Ign:5 https://hex4us.github.io/termux-tools termux/extras all Packages
Ign:8 https://dl.bintray.com/grimler/science-packages-21 science InRelease
Get:9 https://termux.net stable/main all Packages [9760 B]
Ign:10 https://dl.bintray.com/xeffyr/x11-packages-21 x11 InRelease
Get:11 https://dl.bintray.com/grimler/game-packages-24 games Release [5344 B]
Get:12 https://dl.bintray.com/grimler/science-packages-21 science Release [5348 B]
Hit:12 https://dl.bintray.com/grimler/science-packages-21 science Release
Err:14 https://dl.bintray.com/xeffyr/x11-packages-21 x11 Release
        404 Not Found
Get:15 https://dl.bintray.com/grimler/game-packages-24 games Release.gpg [475 B]
Get:16 https://dl.bintray.com/grimler/game-packages-24 games/stable aarch64 Packages [3761 B]
Err:17 https://termux.xeffyr.ml extra InRelease
Failed to connect to termux.xeffyr.ml port 443: Connection timed out
Reading package lists... Done
E: The repository 'https://dl.bintray.com/xeffyr/x11-packages-21 x11 Release' does no longer have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
[ home ]$> apt install python python2 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
python is already the newest version (3.7.3-3).
python2 is already the newest version (2.7.16-3).
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
[ home ]$>
    
```

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.

The screenshot shows a Termux session at 11:49. The user runs `cd sqlmap` and `python3 sqlmap.py -u http://[REDACTED]` to target a MySQL database. The output shows SQLMap identifying the database as MySQL 5.6.21, PHP 5.6.21, and Apache 2.4.39. It lists available databases: information_schema, [REDACTED], and test. A blue box labeled "Proses pentesting" points to the command line. Another blue box labeled "URL Address situs web target" points to the URL in the command. A third blue box labeled "Database yang terdapat pada server" points to the listed databases.

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 eksplorasi oleh *hacker*/peretas sehingga dapat menampilkan dan mengakses struktur *database* yang terdapat di *web server*. Hal tersebut tentu sangat risikan 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 tidak 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.