JURNAL INFORMATIKA DAN TEKONOLOGI KOMPUTER
Halaman Jurnal: https://journal.amikveteran.ac.id/index.php/jitek
Halaman UTAMA Jurnal : https://journal.amikveteran.ac.id/index.php

PENGUKURAN EFEKTIVITAS SQL *INJECTION* PADA *WEBSITE* DENGAN MENGGUNAKAN *TOOLS* JSQL, HAVIJ, dan THE MOLE

Aprilia Monica Sari[a], Trihana Santhi[b], Dewa Ketut Alit Maha Putra[c],Muhamad Bintang Haekal[d], I Made Edy Listartha[e], Gede Arna Jude Saskara[f]

[a] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, aprilia.monica@undiksha.ac.id, Universitas Pendidikan Ganesha
[b] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, trihana@undiksha.ac.id, Universitas Pendidikan Ganesha
[c] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, alit.maha@undiksha.ac.id, Universitas Pendidikan Ganesha
[d] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, muhamad.bintang@undiksha.ac.id, Universitas Pendidikan Ganesha
[e] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, listartha@undiksha.ac.id, Universitas Pendidikan Ganesha
[f] Fakultas Teknik dan Kejuruan / Jurusan Teknik Informatika, jude.saskara@undiksha.ac.id, Universitas Pendidikan Ganesha

ABSTRACT

Along with current technological developments, security for data information residing on websites is very vulnerable to crimes in the internet world such as attacks on security holes in the database layer or often known as SQL Injection. SQL Injection attack is a method to insert SQL commands as input through an application, namely Kali Linux, in order to gain access to the database. This attack can find out usernames, passwords, and other data that is in the database. So that the SQL Injection attack is one of the most popular attacks and is often used to take advantage of security holes in the system because of how easy it is to use it. This study aims to test the level of effectiveness of SQL Injection attacks using the tools in it against a website. Testing the effectiveness is done by doing a comparison between the three tools that are in SQL Injection. The results of the research on the effectiveness of the tools in SQL Injection are the accuracy of database search times and the accuracy of information from the database.

Keywords: *Database, Security, Attack, SQL Injection, Vulnerability.*

Abstrak

Seiring perkembangan teknologi saat ini, keamanan terhadap informasi data yang berada di dalam *website* sangat rentan dengan kejahatan di dunia internet seperti serangan terhadap celah keamanan pada lapisan databases atau sering dikenal dengan istilah SQL *Injection*. Serangan SQL *Injection* merupakan metode untuk menyisipkan perintah SQL sebagai input melalui suatu aplikasi yaitu Kali Linux agar mendapatkan akses masuk ke dalam database. Serangan ini dapat mengetahui username, password, dan data lainnya yang berada di dalam database. Sehingga serangan SQL *Injection* merupakan salah satu serangan yang popular dan sering digunakan untuk memanfaatkan celah keamanan pada system karena cara menggunakannya yang mudah . Penelitian ini memiliki tujuan untuk menguji tingkat efektifitas serangan SQL *Injection* dengan menggunakan *tools* di dalamnya terhadap suatu *website*. Pengujian efektifitas dilakukan dengan melakukan perbandingan antara ketiga *tools* yang berada di dalam SQL *Injection*. Hasil dari penelitian efektifitas *tools* dalam SQL *Injection* adalah akurasi waktu pencarian database dan ketepatan informasi dari database.

Kata Kunci: Database, Keamanan, Serangan, SQL *Injection*, Kerentanan.

Received Desember 28, 2022; Revised Januari 16, 2023; Accepted Maret 27, 2023

1. PENDAHULUAN

Di era modernisasi, perkembangan akan teknologi informasi dan komunikasi kian meningkat dan selalu mengalami perubahan seiring dengan perkembangan zaman. Teknologi informasi dan komunikasi merupakan suatu teknologi yang dimanfaatkan untuk mengolah data, memproses data, mendapatkan data, menyusun data, dan menyimpan data dengan menggunakan berbagai cara agar menghasilkan suatu informasi yang berkualitas dan sesuai dengan fakta. Dengan meningkatnya perkembangan teknologi informasi dan komunikasi, dapat membuat masyarakat memperoleh informasi dari berbagai sumber dengan cepat, mudah, dan tepat Pemberian kemudahan dan kenyamanan yang diberikan teknologi ke masyarakat membawa dampak negatif dalam hal keamanan informasi. Keamanan informasi adalah upaya perlindungan terhadap segala jenis informasi dari penyalahgunaan pihak yang tidak bertanggungjawab[1]. Keamanan terhadap informasi merupakan salah satu faktor penting yang harus diperhatikan. Hal ini menjadi suatu tantangan tersendiri bagi masyarakat dan juga pengembang *website*, ini dikarenakan tidak adanya jaminan yang pasti terkait definisi "tidak ada system yang aman" karena realitanya masih banyak terdapat cara ataupun celah untuk melakukan serangan pada suatu sistem *website* yang menimbulkan kerugian bagi pengembang.

Website adalah suatu kumpulan laman dari beberapa web yang saling berkaitan untuk memberikan informasi berbasis digital dalam bentuk teks, gambar, audio, berkas, dan juga berupa file lainnya yang dapat diakses melalui internet. *Website* mencakup halaman web dalam suatu domain informasi, domain merupakan nama dari salah satu institut yang dapat diakses, seperti yahoo.com dan google.com[2]. *Website* memiliki 2 sifat yaitu bersifat statis jika isi dari informasi di dalam *website* tetap tidak berubah serta isi dari informasinya searah hanya dari pemiliki *website* itu sendiri dan bersifat dinamis jika informasi yang ada di dalam *website* berubah-ubah, serta isinya interaktif dua arah yang berarti informasinya berasal dari pemiliki *website* dan pengguna *website*. Saat ini *website* tidak hanya dijadikan sebagai layanan untuk memberikan informasi tetapi sudah berkembang dengan ditambahkannya fitur-fitur untuk dapat melakukan transaksi secara online. Sehingga dengan perkembangan *website* yang semakin maju maka untuk keamanan terhadap data di dalam *website* harus tetap terjaga dari serangan-serangan luar agar tidak menimbulkan kerugian dari berbagai pihak.

SQL *Injection* adalah suatu tindakan kerentanan yang terjadi apabila penyerang memiliki kemampuan untuk mempengaruhi *Structured Query Language* (SQL). Kemampuan yang dimiliki penyerang dalam mempengaruhi *Structured Query Language (*SQL) membuat penyerang dapat memanfaatkan sintaks dari SQL dan mendapatkan informasi database dari sistem *website*. SQL *Injection* dapat terjadi ketika seorang penyerang memasukkan serangkaian pernyataan SQL ke query dengan melakukan manipulasi data input ke aplikasi[3]. Berdasarkan pernyataan diatas, dapat disimpulkan bahwa serangan SQL *Injection* sangatlah berbahaya karena penyerang yang telah berhasil memasuki database sistem dapat melakukan manipulasi data yang terdapat di dalam database sistem. Proses manipulasi data yang dilakukan penyerang yang seharusnya tidak dilakukan dapat menimbulkan kerugian bagi pemilik *website* yang terinjeksi.

Pada penelitian [3] telah menjelaskan penelitian menggunakan metode serangan possibility SQL *Injection* pada keamanan *website* server dengan menganalisis aktifitas yang berusaha masuk ke sistem jaringan melalui notifikasi alert IDS Snort (ping). IDS Snort merupakan sumber informasi yang akan mendeteksi baik atau tidaknya suatu paket. IDS prinsipnya sebagai suatu perangkat yang didesain khusus untuk dapat mengidentifikasi seluruh paket data yang masuk ke jaringan. Adanya IDS Snort seluruh aktifitas jaringan yang berjalan di web server dapat dipantau setiap saat dan pemberitahuan mengenai aturan/rule sebagai alternatif yang akan memberikan peringatan dari serangan(intruder) yang masuk ke jaringan.

Pada penelitian [4] telah menjelaskan penelitian menggunakan firewall pfsense beserta komponennya yang berfungsi untuk menanggulangi serangan DDoS ataupun DoS pada web server. Agar snort dapat mengenali jenis serangan maka harus mengaktifkan automatic update untuk dapat melakukan pembaharuan database snort. Snort mampu mengenali jenis serangan pada port tep dan DDoS dengan jenis serangan slowloris, setiap serangan yang dikenali akan tersimpan di log snort dengan itu pfsense akan mengambil tindakan untuk melakukan pemblokiran dalam durasi yang telah ditetapkan. Supaya web server terlindungi maka cukup mengaktifkan port yang lazim digunakan pada web server yaitu port 80 dan port 443, sedangkan untuk upload dokumen menggunakan FTP dengan port 21 tetapi harus juga menggunakan SSL yang berfungsi untuk mengenkripsi user dan password pada saat login dan mentransfer data.

Pada penelitian [5] telah menjelaskan penelitian analisis forensik serangan SQL *Injection* menggunakan metode statis forensik. Serangan SQL *Injection* menggunakan metode statis forensik maka dilakukan pada saat komputer tidak terkoneksi dengan internet, saat proses menginstalasi suatu variabel di kode pemrograman dari database query dilakukan validasi terhadap karakter berbahaya, membatasi input yang panjang sehingga penyerang tidak dapat melakukan injeksi ke dalam form login dan penyerang hanya dapat melihat isi data belum dapat mengubah database yang ada di *website*.

Penelitian yang akan dilakukan berbeda dengan penelitian sebelumnya, pada penelitian ini lebih spesifik menguji efektifitas *tools* yang berada di dalam SQL *Injection*. Perbedaan yang mendasar antara penelitian ini dengan penelitian sebelumnya yaitu pada penelitian ini menguji efektifitas tool SQL *Injection* dan jenis analisa yang akan dilakukan. Penelitian ini memiliki tujuan untuk menguji akurasi waktu, ketepatan, dan fitur *tools* yang berada di dalam SQL *Injection*, dan menguji diantara *tools* SQL *Injection* yang lebih efektif untuk digunakan dalam melakukan peretasan database *website*..

2. TINJAUAN PUSTAKA

2.1. Keamanan Informasi

Keamanan informasi adalah upaya perlindungan terhadap segala jenis informasi dari penyalahgunaan pihak yang tidak berwenang. Keamanan informasi merupakan salah satu faktor penting yang harus diperhatikan dalam membangun suatu *website*.

2.2. *Website*

Website merupakan suatu cara untuk menampilkan kumpulan halaman yang didalamnya akan berisi informasi digital dalam bentuk teks, gambar, audio dan lain sebagainya yang bersifat dinamis dan statis yang dihubungkan dan dapat diakses melalui jaringan internet maupun jaringan wilayah lokal (LAN). Saat ini *website* tidak hanya dijadikan sebagai layanan untuk memberikan informasi tetapi sudah berkembang dengan ditambahkannya fitur-fitur untuk dapat melakukan transaksi secara online.

2.3. SQL *Injection*

SQL *Injection* adalah suatu tindakan kerentanan yang terjadi apabila penyerang memiliki kemampuan untuk mempengaruhi *Structured Query Language* (SQL). SQL *Injection* dapat terjadi ketika seorang penyerang memasukkan serangkaian pernyataan SQL ke query dengan melakukan manipulasi data input ke aplikasi.

2.4. JSQL

J SQL merupakan salah satu tool SQL *Injection* yang berguna sebagai alat penguji peretas serbaguna sama seperti *tools* lainnya. J SQL memiliki fungsi menemukan dan mengeksploitasi kerentanan database serta dapat melakukan encode atau decode string

2.5. Havij SQL

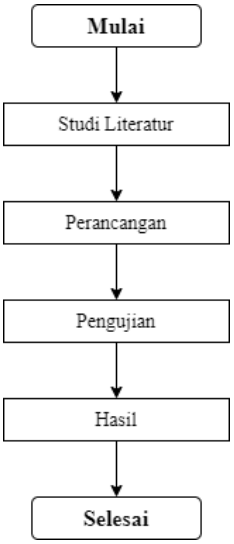
Havij SQL adalah salah satu *tools* SQL *Injection* yang berguna untuk membantu menguji penetrasi untuk dapat menemukan dan mengeksploitasi kerentanan SQL *Injection* pada suatu halaman Web. *Tools* Havij SQL diuraikan dengan GUI yang mudah dipahami. Havij SQL masih sering digunakan baik oleh penguji penetrasi maupun peretas tingkat rendah.

2.6. The Mole

The Mole adalah salah satu *tools* SQL *Injection* yang berguna untuk membantu menguji penetrasi untuk dapat menemukan dan mengeksploitasi kerentanan SQL *Injection* pada suatu halaman Web. Diantara ketiga *tools* ini The Mole memiliki interface yang berbeda karena *tools* ini aplikasi masih dalam bentuk CLI atau command line interface.

3. METODOLOGI PENELITIAN

Alur penelitian merupakan sistematika yang menjelaskan mengenai proses kerja dari sebuah penelitian sehingga penelitian ini tersusun secara sistematis dan dapat diterima oleh segala pihak. Metode penelitian yang kami gunakan adalah studi literatur. Alur penelitian ini dapat dilihat pada gambar 1. berikut ini.



Gambar 1. Alur Metode Penelitian

3.1 Studi Literatur
Studi literatur atau Literature review dimulai dengan pengamatan dari hasil penelitian sebelumnya yang dianggap sekuensi dengan penelitian kali ini yang memperhatikan kerelevannya[6]. Pada penelitian ini peneliti akan mencari dan memahami penelitian sebelumnya yang berasal dari jurnal periode 5 tahun ke belakang. Studi literatur ini dimulai dari pencarian kata kunci penelitian sebelumnya yang meninjau mengenai serangan SQL *Injection* diantaranya "Keamanan *Website*", "*Tools* SQL *Injection*", "Efektivitas serangan *tools* SQL *Injection*". Dilanjutkan dengan identifikasi sumber-sumber penelitian sebelumnya sesuai dengan kriteria penelitian

3.2 Perancangan
Menurut Adi Nugroho perancangan merupakan sebuah strategi untuk memecahkan masalah dan mengembangkan solusi terbaik bagi permasalahan. Sehingga dapat diartikan perancangan merupakan kegiatan yang digunakan untuk dapat menyelesaikan serta memecahkan masalah sehingga mendapatkan solusi terbaik untuk penelitian ini. Perancangan penelitian ini akan dilakukan pada *website* http://testphp.vulnweb.com.

Website http://testphp.vulnweb.com merupakan suatu situs *website* yang dirancang untuk dapat digunakan dalam mendemonstrasikan kemampuan dalam memindai kerentanan *website*. Terdapat beberapa cara yang digunakan untuk melakukan pengujian terhadapan *website* http://testphp.vulnweb.com, salah satunya yaitu dengan melakukan percobaan SQL *Injection*. Untuk melakukan serangan pada *website* ini menggunakan tiga *tools* diantaranya JSQL, HAVIJ, dan The Mole.

Tools HAVIJ merupakan *tools* yang dijalankan untuk menemukan titik lemah dan mengeksploitasi halaman *web* dan berfokus pada pengaksesan file sistem[7]. *Tools* JSQL merupakan *tools* pengujian serangan SQL yang tersedia pada sistem operasi kali *linux*, *tools* ini memiliki *interface* grafis yang dikembangkan pada java yang mendukung pemindaian terhadap kerentanan basis data URL[8]. Dari ketiga *tools* ini hasil yang diharapkan dari penelitian ini berupa akurasi waktu diantara ketiga *tools* ini, ketepatan hasil yang didapatkan dari ketiga *tools* ini serta fitur-fitur yang ada didalam tiga *tools* ini. Proses mendapatkan ketiga hasil ini akan dilakukan sebanyak enam kali yang berguna untuk menghasilkan keakuratan output yang dihasilkan oleh *tools* - *tools* ini.

3.3 Pengujian
Melakukan pengujian keefektifitasan serangan SQL *Injection* pada *website* dengan menggunakan *tools* yang berada di dalam SQL *Injection*. *Tools* tersebut yaitu JSQL, HAVIJ, dan The Mole. Adapun perangkat yang membantu pengujian serangan *tools* SQL *Injection* yaitu dengan menggunakan perangkat bersistem operasi kali linux. Kali linux adalah suatu sistem operasi open source berbasis linux debian yang dikembangkan oleh Office Security. Tampilan dari kali linux terbilang cukup sederhana dan tidak mencolok, untuk kemudahan dari penggunaannya tergolong cukup mudah. Hal ini membuat kali linux

menjadi perangkat yang baik untuk pemula yang sedang belajar dalam melakukan penetrasi pada sistem, jaringan, dan aplikasi[9], karena di dalam kali linux terdapat lebih dari 300 *tools* dengan fungsinya masing-masing yang dapat dimanfaatkan untuk melakukan pengujian keamanan pada suatu sistem[10].

3.4 Hasil

Tahap terakhir dari penelitian ini, setelah melakukan pengujian pada *website* http://testphp.vulnweb.com menggunakan *tools* JSQL, HAVIJ, dan The Mole untuk mengetahui keamanan yang dimiliki *website* ini, selain itu untuk mengetahui kerentanan *website* terhadap serangan yang dilakukan oleh ketiga *tools* ini. Jika *website* ini mudah untuk melakukan serangan maka akan didapatkan akurasi waktu dari enam kali percobaan, ketepatan data dari enam percobaan dan fitur yang dimiliki oleh masing-masing *tools*. Hasil ini akan disampaikan dalam bentuk perbandingan diantara *tools-tools* baik dalam bentuk kelebihan maupun kekurangan

4. HASIL DAN PEMBAHASAN

4.1 Pembahasan

Dalam melakukan uji efektifitas tool SQL *Injection* yang perlu dilakukan yaitu dengan menyiapkan perangkat elektronik (laptop) untuk menjalankan *tools* SQL *Injection* di Kali Linux, kemudian menyiapkan *website* yang akan dijadikan target penyerangan dan teknik serangan menggunakan teknik SQL *Injection* menggunakan 3 *tools* yaitu JSQL, HAVIJ, dan The Mole. Penelitian ini dilakukan untuk mengetahui perbedaan dari ketiga *tools* SQL *Injection* untuk dapat menyerang database pada suatu URL *website* yang sama. *Website* yang kami gunakan adalah http://testphp.vulnweb.com merupakan suatu situs *website* yang dirancang untuk dapat digunakan dalam mendemonstrasikan kemampuan dalam memindai kerentanan *website*

4.2 Hasil

Hasil dari proses penelitian ini dilakukan pada ruang perpustakaan Universitas Pendidikan Ganesha dengan menggunakan wifi Undiksha Harmoni dengan setiap *tools* pada laptop yang berbeda, laptop yang digunakan diantaranya dua laptop asus dan satu laptop lenovo. Hal ini dilakukan untuk mencegahnya perbedaan yang cukup signifikan baik pada kecepatan jaringan, network dan sebagainya. Rata-rata diatas didapatkan dari percobaan sebanyak enam kali dengan menyerang *website*. Menggunakan database Acuart pada tabel usur dengan memilih kolom uname,pass dan email.

Tabel 1. Rata-rata akurasi waktu percobaan

Parameter	**Link ke *Database* Acuart**	***Database*s ke Tabel *User***	**Tabel *User* ke Kolom *Database*s**	**Hasil Kolom Uname**	**Hasil Kolom Pass**	**Hasil Kolom Email**
HAVIJ	10,3 Detik	2,2 Detik	3,1 Detik	2,8 Detik	2,5 Detik	1,9 Detik
THE MOLE	19,5 Detik	3,3 Detik	56,7 Detik	3,5 Detik	2,5 Detik	2,5 Detik
JSQL	60,9 Detik	0 Detik	0 Detik	3,8 Detik	4,1 Detik	2,6 Detik

Berdasarkan data diatas dapat dilihat pada *tools* JSQL menghasilkan akurasi yang lebih cepat. Terlihat dari parameter yang digunakan JQL tidak perlu harus melakukan pemilihan tabel user dan kolom karena pada saat memasukan link akan langsung muncul kolom-kolom dan tabel-tabel yang ada pada databases *website* tersebut. Penelitian selanjutnya mendapatkan ketepatan data yang diperoleh oleh masing-masing *tools*. Hasil dari proses penelitian ini dilakukan pada ruang perpustakaan Universitas Pendidikan Ganesha dengan menggunakan wifi Undiksha Harmoni dengan setiap *tools* pada laptop yang berbeda, laptop yang digunakan diantaranya dua laptop asus dan satu laptop lenovo. Dengan sasaran serangan masih sama yaitu pada *website* http://testphp.vulnweb.com dengan target kolom uname,pass dan email yang terdapat pada tabel user di database Acuart.

Tabel 2. Hasil ketepatan data

Parameter	*User*name (test)	Pass (test)	Email (testing@example.com)

HAVIJ	Pada percobaan pertama hingga ke terakhir menghasilkan data yang sama yaitu menghasilkan *user*name test	Pada percobaan pertama hingga ke terakhir menghasilkan data yang sama yaitu menghasilkan *password* test	Pada percobaan pertama hingga kelima menghasilkan data yang sama yaitu menghasilkan email testing@example.com. Namun pada percobaan keenam hasil yang ditampilkan berubah menjadi array
THE MOLE	Pada percobaan pertama hingga ke terakhir menghasilkan data yang sama yaitu menghasilkan *user*name test	Pada percobaan pertama hingga ke terakhir menghasilkan data yang sama yaitu menghasilkan *password* test	Pada percobaan pertama hingga ke lima menghasilkan data yang sama yaitu menghasilkan email testing@example.com. Namun pada percobaan keenam hasil yang ditampilkan berubah menjadi array
JSQL	Pada percobaan pertama hingga ke terakhir menghasilkan data yang sama yaitu menghasilkan *user*name test	Pada percobaan pertama hingga ke terakhir menghasilkan data yang sama yaitu menghasilkan *password* test	Percobaan pertama hingga kelima menghasilkan data yang sama yaitu menghasilkan email testing@example.com. Namun pada percobaan keenam hasil yang ditampilkan berubah menjadi number87

Dari hasil penelitian diatas dapat terlihat bahwa setiap *tools* memiliki ketepatan penyerangan sangat baik sehingga hasil yang dihasilkan sama. Namun di lain sisi terdapat pada beberapa percobaan yang menghasilkan data yang berbeda seperti halnya pada bagian email setiap *tools* menghasilkan email yang berbeda pada percobaan terakhir atau keenam yang dimana pada percobaan sebelumnya muncul testing@example.com berubah menjadi array atau <h1>number87</h1>. Hal ini dikarenakan data user yang terdapat pada database *website* dipastikan tidak hanya satu user namun terdapat beberapa data user didalamnya. Dari data yang didapatkan yaitu username dan password itu dapat digunakan untuk melakukan sign in pada *website* tersebut. Serta data yang didapatkan sama dengan data yang ada pada *website* tersebut. Penelitian selanjutnya melihat perbedaan yang terlihat dari tampilannya saja yaitu perbedaan fitur yang dihasilkan oleh masing-masing *tools*.

Tabel 3. Fitur setiap *tools*.

Parameter	*User*name (test)
HAVIJ	Pada *tools* ini disediakan dua metode yaitu get dan post, untuk get menghasilkan semua bentuk tulisan sedangkan post untuk sebuah postingan, kemudian pada *database* dapat dipilih sesuai dengan MYSQL atau jenis SQL lainnya dan dapat juga memilih auto detect. Terdapat juga type yang digunakan untuk memilih tipe data apa yang ingin diserang integer atau string dan dapat juga memilih auto detect
THE MOLE	Pada *tools* ini aplikasi masih dalam bentuk CLI atau command line interface yang artinya *user* harus tidak dapat mengetahui fitur yang dimiliki oleh *tools*
JSQL	Pada *tools* ini disediakan strategy untuk melakukan sebuah penyerangan yaitu Normal, Blind, Error dan Time yang artinya *user* dapat memilih cara untuk menyerang *website* baik hanya untuk melihat error, blind atau time atau juga semua dengan strategy normal

Dari hasil penelitian diatas dilihat pada HAVIJ memiliki banyak fitur disediakan namun sayangnya *tools* ini bukanlah *tools* asli dari kali linux namun dapat digunakan di linex menggunakan wine. JSQL dapat menjadi alternatif lain untuk melakukan serangan karena memiliki pilihan strategi, memiliki interface yang baik dan juga merupakan *tools* asli dari linux.

5. KESIMPULAN

Berdasarkan hasil dan analisis dari penelitian ini dapat disimpulkan bahwa, dalam penelitian ini menjelaskan cara menginjeksi kerentanan *website* dengan menggunakan tiga *tools* yang berada di dalam SQL *Injection* yaitu JSQL, HAVIJ, dan The Mole. Analisis menggunakan *website* http://testphp.vulnweb.com merupakan suatu situs *website* yang dirancang untuk dapat digunakan dalam mendemonstrasikan kemampuan dalam memindai kerentanan *website*. Dari hasil penelitian yang dilakukan seorang penyerang hanya akan dapat melihat isi database dalam suatu *website* dan belum dapat untuk mengubah database yang berada di dalam *website*, dan dari hasil penelitian yang dilakukan dari ketika *tools* tersebut, masing-masing *tools* memiliki kelebihan dan kekurangannya masing-masing. Ketiga *tools* SQL *Injection*, *tools* yang paling efektif digunakan untuk melakukan peretasan database *website* yaitu *tools* JSQL ini dikarenakan cukup dengan memasukkan URL *website* ke kolom yang sudah disediakan kemudian melakukan enter dan tunggu beberapa saat (50 detik sampai 1 menit) maka akan muncul pilihan database dari *website* tersebut. *Tools* JSQL sangat praktis digunakan karena sudah berbasis aplikasi. Pada penelitian ini peneliti menyarankan untuk proses penyerangan sebuah *website* atau ingin belajar mengenai serangan SQL dapat menggunakan JSQL karena mudah untuk diinstal dan merupakan aplikasi asli dari linux dan Pada penelitian selanjutnya dapat mengembangkan parameter perbandingan yang digunakan untuk melakukan analisis serangan dalam bentuk database.

Ucapan Terima Kasih

Terimakasih penulis ucapkan kepada :

1) Bapak I Made Edy Listartha, S.Kom., M.Kom. dan Bapak Gede Arna Jude Saskara, S.T.,M.T atas bimbingan yang sudah diberikan dalam penyusunan jurnal yang berjudul "Pengukuran Efektivitas Serangan SQL *Injection* Pada *Website* Dengan Menggunakan *Tools* JSQL, Havij, Dan The Mole" sehingga dapat diselesaikan dengan tepat waktu.
2) Dewan Editor yang telah menelaah dan mereview naskah jurnal yang berjudul "Pengukuran Efektivitas Serangan SQL *Injection* Pada *Website* Dengan Menggunakan *Tools* JSQL, Havij, Dan The Mole " sehingga menjadi sempurna.
3) Universitas Pendidikan Ganesha yang telah memfasilitasi dan membantu berjalannya penelitian ini.
4) Dan yang terakhir kepada para rekan-rekan yang membantu dalam menlancarkan penelitia ini dan menyelesaikan jurnal yang berjudul "Pengukuran Efektivitas Serangan SQL *Injection* Pada *Website* Dengan Menggunakan *Tools* JSQL, Havij, Dan The Mole".

DAFTAR PUSTAKA

[1] RAMADHANI, Aditya. Keamanan Informasi. Nusantara Journal of Information and Library Studies (N-JILS), 2018, 1.1: 39-51. [Accessed Nov. 11, 2022].

[2] METKONO, Akhis Mistus. PERANCANGAN SISTEM PENGARSIPAN SURAT MENYURAT GEREJA GMIT EFATA SOE BERBASIS WEB MENGGUNAKAN FRAMEWORK CODEIGNITER. JIKO (Jurnal Informatika dan Komputer), 2022, 5.1: 69-77. [Accessed Nov. 11, 2022]

[3] INDRIANI, Yuni Wardatul. ANALISA KEAMANAN WEB SERVER TERHADAP SERANGAN POSSIBILITY SQL INJECTION Studi Kasus: Web Server UMK (Yuni Wardatul Indriani). 2020. [Accessed Nov. 11, 2022].

[4] ARMAN, Molavi; RACHMAT, Nur. Implementasi Sistem Keamanan Web Server Menggunakan Pfsense. Jusikom: Jurnal Sistem Komputer Musirawas, 2020, 5.1: 13-23. [Accessed Nov. 29, 2022].

[5] Riadi, I., Umar, R. and Sukarno, W., 2016. Analisis Forensik Serangan Sql Injection Menggunakan Metode Statis Forensik. In Pros. Interdiscip. Postgrad. Student Conf. 1st (Vol. 1, pp. 102-103). [Accessed Nov. 29, 2022].

[6] PRATAMA, Tino Imam Maulana, et al. Analisis Serangan dan Keamanan pada SQL Injection: Sebuah Review Sistematik. JIIFKOM (Jurnal Ilmiah Informatika dan Komputer), 2022, 1.2: 27-32. [Accessed Nov. 29, 2022].

[7] Baklizi, M., Atoum, I., Abdullah, N., Al-Wesabi, O. A., Otoom, A. A., & Hasan, M. A. S. (2022). A Technical Review of SQL Injection Tools and Methods: A Case Study of SQLMap. International

Journal of Intelligent Systems and Applications in Engineering, 10(3), 75-85. [Accessed Nov. 29, 2022].

[8] Mishra, A. K., & Kumar, A. (2020, July). Performance-based Comparative Analysis of Open Source Vulnerability Testing Tools for Web Database Applications. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE. [Accessed Nov. 29, 2022].

[9] Hermawan, Rudi. "Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux." STRING (Satuan Tulisan Riset dan Inovasi Teknologi) 6, no. 2 (2021): 210-216. [Accessed Nov. 29, 2022].

[10] Andria, Andria. "Website Security Gap Analysis Using WEBPWN3R Tools at Kali Linux." Generation Journal 4, no. 2 (2020): 69-76. [Accessed Nov. 29, 2022].