SQL Injection: Analisis Efektivitas Uji Penetrasi dalam Aplikasi Web

by Luthfi Arian Nugraha

Submission date: 23-May-2024 11:07PM (UTC+0800)
Submission ID: 2376066964
File name: _Archive_Artikel_Ilmiah.pdf (1.46M)
Word count: 5033
Character count: 30984

SQL Injection: Analysis of Penetration Testing Effectiveness in Web Applications
[SQL Injection: Analisis Efektivitas Uji Penetrasi dalam Aplikasi Web]

Luthfi Arian Nugraha [1)], Irwan Alnarus Kautsar*[,2)]

[1)]Program Studi Informatika, Universitas Muhammadiyah Sidoarjo, Indonesia
[2)] Program Studi Informatika, Universitas Muhammadiyah Sidoarjo, Indonesia
*Email Penulis Korespondensi: irwan@umsida.ac.id

Abstract. *In this era of digital advancement, information system security becomes crucial, especially against SQL Injection attacks that threaten data integrity. This study aims to evaluate SQL Injection vulnerabilities in web applications and assess the effectiveness of penetration testing methods as a security measurement tool. By utilizing literature reviews and previous studies, this study identifies various attack techniques and defense strategies used to protect data. Through systematic penetration testing on ten websites, this study generates performance data that reflects the success rate of attacks and the time required for penetration. The results show variations in the effectiveness of penetration testing tools, with some sites showing significant vulnerabilities. To improve web application security, this study recommends updating programming languages, applying OOP and MVC paradigms, using Rest API, implementing WAF, and using CAPTCHA. These findings provide insights for developing more robust and adaptive security strategies in the face of cyber threats.*

Keywords – *Cybersecurity, SQL Injection, Penetration Testing, Web Vulnerability*

Abstrak. *Penelitian ini mengevaluasi kerentanan SQL Injection dalam aplikasi web dan menilai efektivitas metode pengujian penetrasi. Dengan tinjauan literatur dan studi terdahulu, penelitian ini mengidentifikasi berbagai teknik serangan dan strategi pertahanan. Pengujian penetrasi pada sepuluh situs web menghasilkan data performa yang menunjukkan variasi dalam efektivitas tools pengujian penetrasi. Penelitian ini menyarankan beberapa rekomendasi untuk meningkatkan keamanan aplikasi web, seperti pembaruan bahasa pemrograman, penerapan paradigma OOP dan MVC, penggunaan Rest API, implementasi WAF, dan penggunaan CAPTCHA. Temuan ini memberikan wawasan untuk pengembangan strategi keamanan yang lebih tangguh dan adaptif dalam menghadapi ancaman siber.*

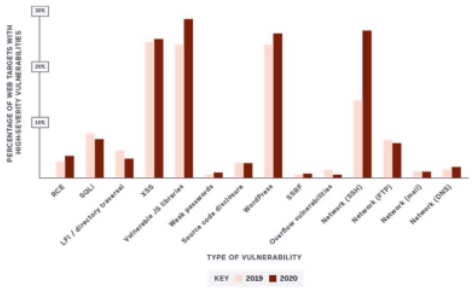
Kata Kunci – *Keamanan Siber, Injeksi SQL, Uji Penetrasi, Kerentanan Web*

I. PENDAHULUAN

Teknologi sistem informasi saat ini berkembang sangat pesat. Informasi yang mudah diakses di internet secara gratis dan cepat tanpa batasan membuat banyak data terbuka yang mudah diakses oleh semua orang. Hal ini menyebabkan lemahnya integritas data asli yang dipresentasikan, menjadi tidak otentik atau telah diubah oleh pengguna yang tidak bertanggung jawab [1].

Sistem informasi menjadi suatu kebutuhan sehari-hari masyarakat, salah satu contohnya yaitu situs web berita, media sosial, dan blog yang bersifat individu. Informasi yang disuguhkan ialah hasil olah data dari setiap pemilik atau instansi yang menyediakan platform tersebut [2].

SQL Injection merupakan teknik serangan eksploitasi pada basis data yang terintegrasi dengan situs web, yang memungkinkan penghancuran dan manipulasi data [3]. Serangan eksploitasi tersebut menyebabkan kerusakan bahkan kehilangan data yang disimpan pada situs web. Implementasi teknik serangan ini dapat dilakukan melalui *Uniform Resource Locator* (URL) pada situs web menggunakan tools yang bersifat sumber terbuka [4].



Gambar 1. Statisk Acunetix pada Musim Semi Tahun 2021

Laporan tahunan Acunetix yang terbit di awal tahun 2021 menunjukkan bahwa serangan *SQL Injection* masih menjadi kerentanan yang sering ditemui, dengan angka kejadian sekitar 8% di tahun 2019 dan menurun sedikit menjadi 7% di tahun 2020. Informasi ini tergambar dalam Gambar 1 yang menampilkan daftar kerentanan tersebut. Kendati mengalami penurunan sebesar 1% antara tahun 2019 dan 2020, serangan *SQL Injection* tetap berada di urutan kelima dalam daftar 14 jenis serangan yang paling umum [5].

Penetrasi merupakan salah satu metode uji pengukuran terjadinya kerentanan sebuah aplikasi yang telah dibangun atau dalam tahapan pembuatan [6]. Uji penetrasi dapat menjaga integritas sebuah data setiap pengguna dari aplikasi yang digunakan [7].

A. Penelitian Terdahulu

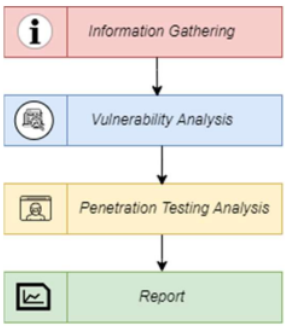
Penelitian pertama [8] dengan judul "*Web Application Penetration Testing Using SQL Injection Attack*" melakukan penelitian dengan menggunakan metode injeksi SQL digunakan untuk mengidentifikasi kerentanan injeksi SQL dalam aplikasi web. Metode ini mengeksploitasi kerentanan keamanan dalam aplikasi web untuk mengirimkan perintah SQL yang tidak valid. Jika kerentanan ini ada maka perintah SQL yang tidak valid akan dijalankan oleh database, yang dapat menyebabkan serangan injeksi SQL. Tujuan umum pada penelitian tersebut adalah mengidentifikasi dan mengeksploitasi kerentanan *SQL injection* pada aplikasi web.

Penelitian kedua [9] dengan judul "*SQL Injection Attacks Countermeasures Assessment*" dengan menggunakan metode identifikasi countermeasure pada serangan eksploitasi injeksi SQL. Tujuan umum pada penelitian tersebut adalah mengevaluasi efektivitas countermeasure terhadap serangan SQL injection.

Penelitian Keempat [10] dengan judul "*Query Response Time Comparison SQL and No SQL for Contact Tracing Application*" menggunakan metode eksperimen untuk melakukan komparasi terhadap dua jenis basis data relasional (SQL) dan non-relasional (NoSQL). Tujuan penelitian yang terkait yaitu menginformasikan pada pengembang tentang perbandingan basis data relasional memiliki struktur data yang lebih kompleks dan efisien untuk merepresentasikan hubungan antar data, sedangkan basis data non-relasional memiliki struktur data yang lebih sederhana dan efisien untuk merepresentasikan data dalam jumlah besar.

II. METODE

Penelitian ini menggunakan metode pengujian penetrasi. Gambar 2 menunjukkan tahapan dalam melakukan penelitian [11].



Gambar 2. Tahapan Metode Uji Penetrasi

Information gathering adalah fase awal untuk mendapatkan sebuah informasi pada platform yang dituju. Tujuan dari pengumpulan informasi adalah untuk mendapatkan data sensitif dari target yang akan diteliti [12].

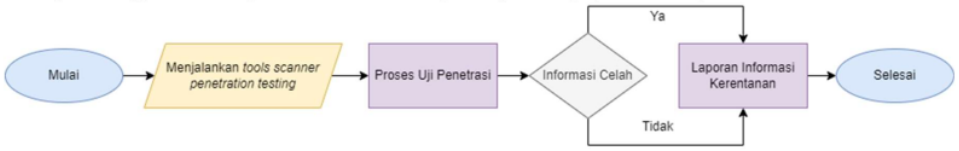
Vulnerability analysis tahapan penting analisis dalam melakukan pengujian penetrasi. Tahapan ini menentukan metode pengujian yang akan digunakan. Dengan demikian, akan diperoleh data mentah yang dapat diproses menggunakan *tools* yang telah disediakan [13].

Penetration testing analysis merupakan tahapan implementasi pengujian penetrasi pada platform yang dituju Tahapan ini akan menghasilkan data kinerja sebagai hasil dari laporan pengujian penetrasi [14].

Report atau penyusunan laporan adalah tahapan terakhir yang melibatkan penyajian data yang telah diproses sehingga dapat dipahami oleh pembaca. Tahapan ini juga melibatkan penyajian informasi yang berasal dari data yang telah diperoleh [15].

A. Desain Alur Uji Penetrasi

Diagram alir atau *flowchart* merupakan representasi alur prosedur penelitian ini yang dilakukan secara sistematis [16]. Dengan menggunakan diagram alir tersebut, rangkaian proses uji penetrasi dapat dilakukan lebih mudah.



Gambar 3. Diagram Alir Pengujian Penetrasi

Gambar 3 adalah diagram alir yang menunjukkan alur pengujian penetrasi, diikuti dengan pelaksanaan pengujian penetrasi pada platform yang dituju. Selanjutnya, informasi tentang celah keamanan diperoleh dan dicatat dalam laporan yang mencakup status keberhasilan dan waktu yang diperlukan selama pengujian penetrasi [17].

III. HASIL DAN PEMBAHASAN

A. Pengumpulan Informasi dan Analisis Kerentanan

Peneliti akan melakukan simulasi serangan pada 10 situs web, terdiri dari 5 situs web sumber terbuka yang sudah memiliki izin dan 5 situs web secara acak seperti pada tabel 1 tersebut untuk menemukan kelemahan atau celah keamanan yang dapat dimanfaatkan oleh penyerang untuk melakukan tindakan berbahaya, seperti mencuri data sensitif, merusak sistem, atau mengganggu operasi situs web [15].

Tabel 1. Daftar Sirus Web dan Analisis Kerentanannya

Nama Situs Web	Jenis Situs Web	Sasaran	Metode
Situs-A	Pendidikan Negeri	Form	POST
Situs-B	Pendidikan Swasta	Form	POST
Situs-C	Hiburan	Login Admin	POST
Situs-D	Pekerja Lepas A	Form	POST
Situs-E	Pekerja Lepas B	Form	POST
Situs-F	Bisnis	Pencarian	GET
Situs-G	Penyedia Layanan	Pencarian	GET
Situs-H	Blog Komersial	Pencarian	POST
Situs-I	Blog Individu	Form	GET
Situs-J	Forum Komunitas	Form	GET

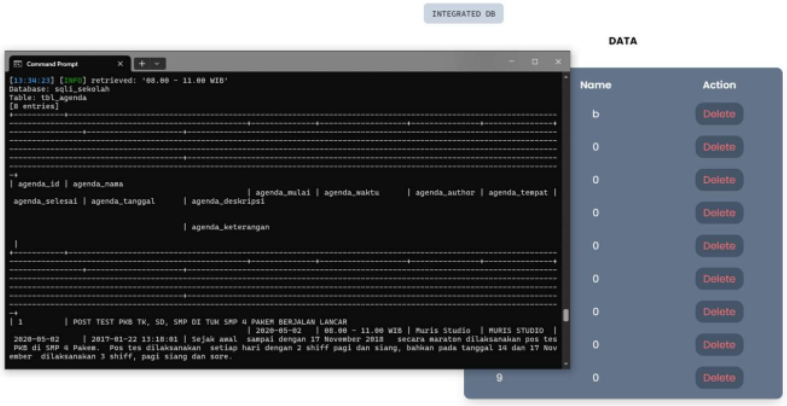
Situs web yang telah dikumpulkan, kemudian dilakukan analisis terhadap sasaran yang digunakan dan metode yang diterapkan, sebagaimana dirangkum dalam Tabel 1 [18].

B. Analisis Uji Penetrasi

Penelitian ini mengimplementasikan tiga alat uji penetrasi yang bersifat sumber terbuka. Pemilihan alat-alat ini didasarkan pada beberapa pertimbangan krusial. Pertama, sifat sumber terbuka dari alat-alat ini memungkinkan kemudahan dalam implementasi, yang vital dalam konteks penelitian keamanan siber. Kedua, dokumentasi yang lengkap untuk setiap alat memastikan bahwa proses uji penetrasi dapat dilakukan dengan standar yang konsisten dan dapat diulang. Terakhir, dukungan komunitas yang kuat untuk alat-alat ini memberikan jaminan tambahan dalam hal pembaruan keamanan dan resolusi masalah yang cepat. Berikut analisis dari setiap *Tools* dalam pengujian penetrasi pada 10 situs web pada tabel 1.

a. Analisis *Tools* A

Data penetrasi merupakan komponen penting dalam pengujian, khususnya pada pengujian penetrasi yang bertujuan untuk mengidentifikasi kerentanan dan celah keamanan dalam sistem informasi. Data ini diperoleh melalui penggunaan berbagai *tools*, salah satunya adalah *Tools* A yang tercantum dalam tabel 2.



Gambar 4. Contoh Uji Penetrasi Menggunakan *Tools* A

Tabel 2. Hasil Uji Penetrasi *Tools* A

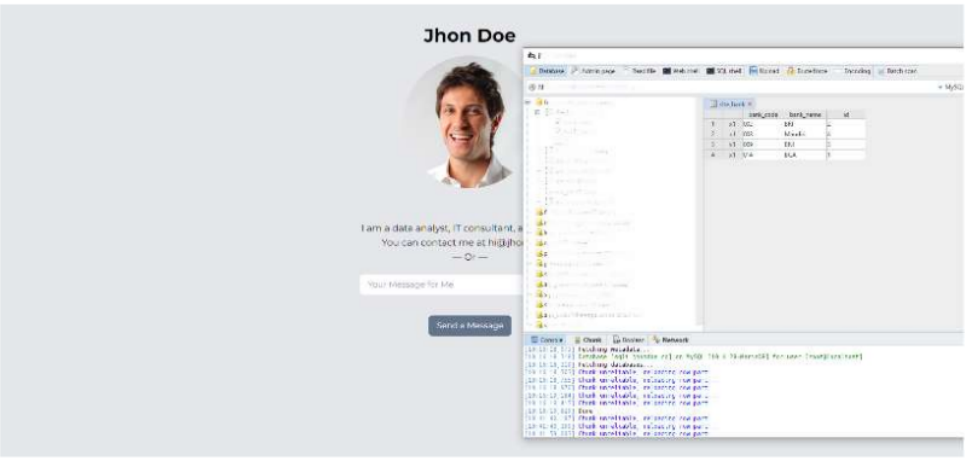
Nama Situs Web	Waktu	Status Keberhasilan
Situs-A	2 menit 23 detik	Ya
Situs-B	1 menit 36 detik	Ya
Situs-C	8 menit 27 detik	Tidak
Situs-D	28 menit 22 detik	Tidak
Situs-E	7 menit 13 detik	Tidak
Situs-F	1 menit 27 detik	Tidak
Situs-G	7 menit 24 detik	Tidak
Situs-H	2 menit 44 detik	Tidak
Situs-I	49 Detik	Ya
Situs-J	10 menit 45 detik	Ya

b. Analisis *Tools* B

Pengujian selanjutnya, penetrasi dilakukan menggunakan *Tools* B. Data penetrasi yang dihasilkan kemudian dianalisis untuk mengevaluasi ketahanan sistem terhadap serangan siber.

Tabel 3. Hasil Uji Penetrasi *Tools* B

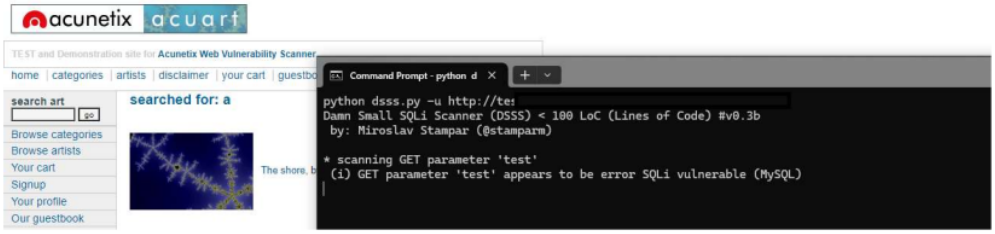
Nama Situs Web	Waktu	Status Keberhasilan
Situs-A	8 detik	Tidak
Situs-B	4 menit 18 detik	Ya
Situs-C	1 detik	Tidak
Situs-D	4 menit 12 detik	Tidak
Situs-E	2 detik	Tidak
Situs-F	4 menit 51 detik	Tidak
Situs-G	6 menit 8 detik	Tidak
Situs-H	1 detik	Tidak
Situs-I	1 menit 22 detik	Ya
Situs-J	52 detik	Ya



Gambar 5. Contoh Implementasi *Tools* B

c. Analisis *Tools* C

Pengujian terakhir dilakukan dengan memanfaatkan *Tools* C, sebuah perangkat lunak yang dikembangkan untuk memindai situs web dengan cara menulis dalam kurang dari 100 baris kode berbahaya.



Gambar 6. Contoh Uji Penetrasi Menggunakan *Tools* C

Tabel 4. Hasil Uji Penetrasi *Tools* C

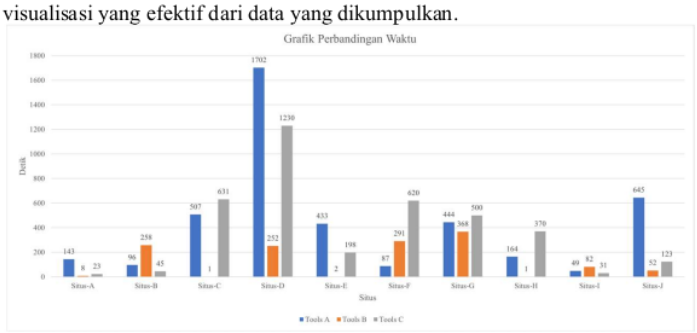
Nama Situs Web	Waktu	Status Keberhasilan
Situs-A	23 detik	Ya
Situs-B	45 detik	Ya
Situs-C	10 menit 31 detik	Tidak
Situs-D	20 menit 30 detik	Tidak
Situs-E	3 menit 18 detik	Tidak
Situs-F	10 menit 20 detik	Tidak
Situs-G	8 menit 20 detik	Tidak
Situs-H	6 menit 10 detik	Tidak
Situs-I	31 detik	Ya
Situs-J	2 menit 3 detik	Ya

C. Analisis Hasil Uji Penetrasi

Data uji penetrasi yang presentasikan pengujian menggunakan *Tools* A menunjukan bahwa 4 dari 10 situs web berhasil melemahkan (Situs-A, Situs-B, Situs-I, dan Situs-J). *Tools* B menunjukkan bahwa 3 dari 10 situs web berhasil ditembus (Situs-B, Situs-I, dan Situs-J). *Tools* C menunjukkan bahwa 4 dari 10 situs web berhasil ditembus (Situs-A, Situs-B, Situs-I, dan Situs-J).

Situs-C hingga Situs-H menunjukkan ketahanan yang baik terhadap serangan siber, karena berhasil lolos dalam semua pengujian penetrasi, ketahanan ini dapat diatributkan kepada implementasi proteksi berlapis yang terintegrasi selama fase pengembangan situs web. Situs-B, Situs-I, dan Situs-J menunjukkan kerentanan yang tinggi terhadap serangan siber, yang sebagian besar disebabkan oleh penggunaan teknik pengembangan prosedural sehingga memudahkan uji penetrasi.

Fokus utama dari penelitian ini adalah untuk mengidentifikasi dan mengeksplorasi titik celah yang memungkinkan serangan siber untuk menyusup dan mengirimkan kode berbahaya. Tujuan akhir adalah untuk mendapatkan akses ke basis data situs web yang ditargetkan melalui *Tools* yang digunakan dalam penelitian ini. Sebagai bagian dari analisis penelitian, gambar 7 menyajikan grafik perbandingan waktu yang dibutuhkan untuk menembus masing-masing situs web, memberikan visualisasi yang efektif dari data yang dikumpulkan.



Gambar 7. Grafik Hasil Uji Penetrasi Bedasarkan Waktu

D. Solusi Hasil Uji Penetrasi

1. Menggunakan Bahasa Pemrograman dengan Versi Terbaru

Dalam konteks pengembangan perangkat lunak, pembaruan bahasa pemrograman merupakan salah satu strategi krusial untuk mengamankan aplikasi dari serangan injeksi SQL. Pembaruan ini tidak hanya memperbaiki kerentanan yang telah dikenali, tetapi juga memperkenalkan fitur keamanan yang lebih canggih. Versi terbaru bahasa pemrograman, seperti PHP 8.3 yang dirilis pada 11 April 2024, kerap dilengkapi dengan mekanisme pertahanan yang ditingkatkan, termasuk sanitasi input yang lebih efektif dan dukungan yang lebih baik untuk *prepared statements*. Fitur-fitur ini secara signifikan mengurangi risiko serangan injeksi SQL dengan membatasi kemungkinan eksekusi perintah SQL yang berbahaya [19]. Selain itu, pembaruan bahasa pemrograman memastikan kepatuhan terhadap standar keamanan terkini dan mendukung inisiatif pemantauan keamanan yang berkelanjutan. Oleh karena itu,

pembaruan ke versi terbaru tidak hanya merupakan praktik keamanan yang baik, tetapi juga bagian integral dari manajemen risiko yang proaktif dalam pengembangan aplikasi web.

2. Penerapan Metode *Object Oriented Programming* (OOP)

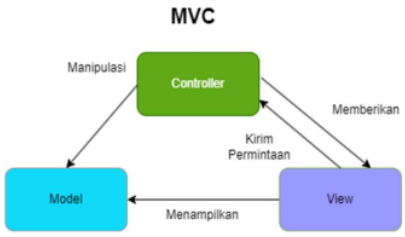
Pemrograman yang berorientasi pada objek adalah metode pengembangan perangkat lunak yang memusatkan fokus pada objek sebagai elemen kunci dalam proses pembuatan program. Dalam OOP, objek didefinisikan oleh atributnya, yang berupa data, dan metodenya adalah fungsi yang menentukan perilaku objek tersebut. Peningkatan keamanan aplikasi dengan enkapsulasi data, pemisahan kepentingan, dan pola desain seperti DAO dan *Repository* yang memfasilitasi penggunaan *prepared statements* dan *parameterized queries*. Pendekatan ini memungkinkan kontrol akses yang ketat dan validasi input yang efektif, mengurangi risiko serangan *SQL Injection* secara signifikan, seperti contoh kode PHP OOP sederhana pada Gambar 9 [20], [21].

```php
<?php

class Hewan {
  public $nama;

  function __construct($nama) {
    $this->nama = $nama;
  }

  function suara() {
    echo "Suara hewan ini tidak diketahui";
  }
}

class Kucing extends Hewan {
  function suara() {
    echo "Meaong!";
  }
}

class Anjing extends Hewan {
  function suara() {
    echo "Guk! Guk!";
  }
}

$kucing = new Kucing("Garfield");
$anjing = new Anjing("Siberian Husky");

echo "Hewan bernama " . $kucing->nama . " bersuara: "; $kucing->suara();

echo "\nHewan bernama " . $anjing->nama . " bersuara: "; $anjing->suara();
```

Gambar 8. Contoh Kode Bahasa Pemrogaman PHP OOP Sederhana

3. Penerapan Metode *Model-View-Controller* (MVC)

MVC adalah model arsitektur perangkat lunak yang efektif dan dapat diadaptasi, yang tidak hanya berguna untuk mengembangkan berbagai jenis aplikasi tetapi juga menawarkan keuntungan seperti pemisahan fungsi yang jelas, keterkaitan yang minimal antar komponen, kemudahan dalam pengujian, dan sederhana untuk digunakan. MVC mendukung keamanan aplikasi dengan memungkinkan pemisahan yang jelas antara logika bisnis dan antarmuka pengguna, yang dapat membantu meminimalisir risiko serangan, sehingga memperkuat aplikasi terhadap ancaman keamanan [22]. Gambar 10 menunjukkan berkas tampilan, kontrol, dan komunikasi dengan basis data secara terpisah. Hal ini mencegah *tools* mendeteksi instruksi kode pada komunikasi terhadap basis data yang dituju.

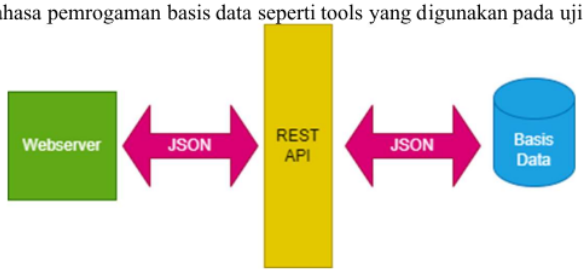


Gambar 9. Diagram MVC

4. Penerapan Rest API

Representational State Transfer Application Programming Interface (Rest API) adalah sebuah antarmuka pemrograman aplikasi yang digunakan untuk memfasilitasi komunikasi dan pertukaran data antar berbagai perangkat lunak atau sistem dalam jaringan komputer seperti diagram pada Gambar 11. Rest API berfungsi sebagai perantara yang mengikuti seperangkat aturan dan batasan untuk memastikan komunikasi yang handal dan mudah digunakan. Rest API merupakan gaya arsitektur yang umum digunakan dalam pengembangan perangkat lunak untuk memungkinkan aplikasi berinteraksi satu sama lain melalui protokol *Hypertext Transfer Protocol* (HTTP), yang merupakan protokol dasar yang digunakan untuk komunikasi web. Rest API menggunakan metode HTTP standar seperti *get, post, put*, dan *delete* untuk melakukan *operasi create, read, update, delete* (CRUD) pada data [23]. Rest

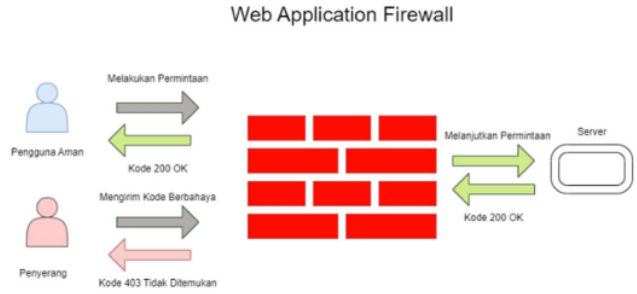
API juga dapat menggunakan format data umum seperti *Javascript Object Notation* (JSON) atau *Extensible Markup Language* (XML) untuk bertukar data dengan mudah antara aplikasi yang berbeda. Hal ini menjadikan rest api sebagai pilihan yang populer untuk membangun layanan web yang fleksibel dan dapat diskalakan dan tidak dapat mengeksekusi intruksi bahasa pemrogaman basis data seperti tools yang digunakan pada uji penetrasi [24].



Gambar 10. Diagram Komunikasi Rest API

5. Implementasi Perangkat Lunak *Web Application Firewall* (WAF)

WAF merupakan sistem pengamanan yang secara khusus dikembangkan untuk mengamankan aplikasi web dari ancaman serangan siber seperti *SQL Injection, Cross Site Scripting* (XSS), dan *Distributed Denial-of-Service* (DDoS). Berfungsi sebagai penyaring, WAF mengawasi serta mengevaluasi lalu lintas data yang menuju aplikasi web, mengidentifikasi kegiatan yang mencurigakan, serta menghalanginya agar tidak sampai ke tujuan [25]. Seperti yang dicontohkan pada gambar 11, tools yang digunakan dalam uji penetrasi terdeteksi sebagai penyerangan kedalam sistem situs web.



Gambar 11. Diagram Kerja WAF

6. Implementasi Metode Captcha

Serangan SQL Injection, XSS, dan DDoS dapat dicegah menggunakan metode *Completely Automated Public Turing test to tell Computers and Humans Apart* (CAPTCHA). Captcha adalah sebuah fitur keamanan pada situs web yang berfungsi sebagai pendeteksi pengguna manusia dan komputer, jika sistem mendeteksi adanya kecurangan seperti menggunakan *tools* berbahaya, maka yang terjadi yaitu memblokir *Internet Protocol* (IP) pada pengguna yang melakukan kecurangan [26].

E. Diskusi Hasil Uji Penetrasi

1. Efektivitas *Tools* dalam Mengidentifikasi Kerentanan

Pengujian yang dilakukan, *Tools* A, B, dan C menunjukkan variasi dalam efektivitas mereka. *Tools* A tampaknya lebih efektif dalam menembus sejumlah situs web, sementara *Tools* B dan C memiliki tingkat keberhasilan yang lebih rendah. Hal ini dapat menunjukkan bahwa *Tools* A memiliki kemampuan yang lebih baik dalam mengidentifikasi dan mengeksploitasi kerentanan yang ada.

2. Konsistensi Keberhasilan Uji Penetrasi

Situs-A dan Situs-B menunjukkan konsistensi dalam keberhasilan penetrasi menggunakan *Tools* A dan B, namun *Tools* C gagal menembus Situs-A. Ini menimbulkan pertanyaan tentang keandalan dan metodologi yang digunakan oleh *Tools* C dalam pengujian.

3. Kerentanan Situs Web

Situs-I dan Situs-J berhasil ditembus oleh semua *tools*, yang menandakan bahwa kedua situs ini memiliki kerentanan yang lebih serius. Ini memerlukan tindakan segera untuk menambal celah keamanan yang ada.

4. Waktu Penetrasi

Waktu yang dibutuhkan untuk menembus setiap situs web sangat bervariasi, yang menunjukkan perbedaan dalam tingkat keamanan dan kompleksitas setiap situs. Situs dengan waktu penetrasi yang lebih singkat mungkin memiliki kerentanan yang lebih mudah diidentifikasi atau kurangnya langkah-langkah keamanan yang efektif.

5. Implikasi untuk Pengembangan Peningkatan Keamanan

Hasil pengujian ini juga memberikan wawasan penting untuk pengembangan *tools* penetrasi di masa depan. *Tools* yang dapat menyesuaikan pendekatannya berdasarkan karakteristik unik dari setiap situs web mungkin lebih efektif dalam mengidentifikasi kerentanan.

6. Perbandingan Keamanan Teknologi dalam Pengembangan Situs Web

Teknologi yang digunakan untuk pengembangan di setiap situs web memiliki pengaruh besar dalam penelitian ini. Sebagaimana contohnya dalam Situs-A dan Situs-I menggunakan teknologi pengembangan prosedural yang memiliki kerentanan sangat tinggi, dibandingkan dengan Situs-D dan Situs-E yang menerapkan teknologi pengembangan MVC sebagai pemrosesan data yang akan ditampilkan kepada pengguna situs dan Rest API sebagai cara kerja komunikasi aplikasi web dengan basis data.

7. Batasan Situs Web dalam Penelitian

Penelitian ini melibatkan uji penetrasi yang dilakukan pada 10 situs web terpilih. Langkah ini diambil untuk menguji efektivitas metode penetrasi dalam mengidentifikasi kerentanan sistem. Meskipun waktu yang tersedia untuk uji penetrasi ini terbatas, prosedur yang digunakan telah dirancang untuk memastikan bahwa hasil yang diperoleh dapat memberikan wawasan yang signifikan mengenai keamanan situs web yang diuji.

8. Batasan Variasi *Tools* dalam Penelitian

Penelitian ini membatasi penggunaan *tools* penetrasi ke tiga *tools* utama. Pembatasan ini dilakukan dengan pertimbangan khusus untuk memastikan konsistensi dan keandalan data. Ketiga tools tersebut dipilih berdasarkan kemampuan *tools* untuk memberikan wawasan komprehensif tentang keefetivitasan terhadap serangan *SQL Injection*. Selain itu, penggunaan alat yang lebih terbatas memungkinkan peneliti untuk melakukan analisis yang lebih mendalam dan spesifik, yang pada gilirannya meningkatkan kualitas hasil penelitian. Meskipun penggunaan lebih banyak alat dapat memberikan variasi data yang lebih luas, namun hal itu juga dapat menyebabkan kompleksitas dan variabilitas yang tidak diinginkan, yang dapat mengaburkan temuan utama penelitian.

9. Masalah dalam Uji Penetrasi

Peneliti menghadapi beberapa tantangan, termasuk keterbatasan informasi mengenai teknologi yang digunakan selama pengembangan situs web yang diuji secara acak. Akibatnya, pendekatan yang diterapkan adalah *Blackbox Testing*, di mana berfokus pada analisis input dan output dari berbagai alat tanpa akses ke struktur kode internal situs. Metode ini memungkinkan kami untuk menilai keamanan eksternal situs web tanpa memerlukan pengetahuan mendalam tentang arsitektur sistemnya.

10. Pengalaman Pengguna pada Setiap *Tools* Uji Penetrasi

Penelitian ini menggunakan 3 *tools* dan setiap penggunaan *tools* tersebut memiliki tingkatnya masing-masing. *Tools* A memiliki tingkat menengah dalam melakukan uji penetrasi, tidak ada tampilan yang ramah pengguna seperti *Graphic User Interface* (GUI). *Tools* B memiliki tingkat menengah dan lanjut, meskipun *tools* ini terdapat GUI untuk melakukan uji penetrasi, tetapi butuh pengaturan khusus untuk menjalankan *tools* tersebut. *Tools* C memiliki pengalaman yang ramah pengguna, tidak memiliki GUI bukan menjadi masalah pada *tools* tersebut, dengan satu kali instruksi tools tersebut melakukan tugasnya dengan mudah.

IV. SIMPULAN

Serangan *SQL Injection* masih menjadi ancaman serius bagi situs web. Penelitian ini menunjukkan bahwa pengujian penetrasi merupakan metode yang efektif untuk mengidentifikasi kerentanan dan celah keamanan dalam sistem informasi. Namun, efektivitas *tools* penetrasi bervariasi, dan beberapa situs web memiliki kerentanan yang lebih serius dibandingkan situs web lainnya.

Penerapan langkah-langkah keamanan seperti penggunaan bahasa pemrograman terbaru, metode OOP, MVC, Rest API, WAF, dan Captcha dapat membantu meningkatkan keamanan situs web terhadap serangan *SQL Injection*. Diperlukan penelitian lebih lanjut untuk mengembangkan *tools* penetrasi yang lebih efektif dan metode pencegahan serangan *SQL Injection* yang lebih canggih.

Hasil penelitian ini diharapkan dapat membantu pengembang situs web untuk meningkatkan keamanan situs web mereka dan para peneliti keamanan untuk mengembangkan metode pencegahan serangan *SQL Injection* yang lebih efektif.

V. SARAN

Dalam penelitian ini, metode pengujian penetrasi yang sistematis telah berhasil mengungkap kerentanan terhadap serangan *SQL Injection* pada aplikasi web, menyoroti pentingnya pembaruan keamanan dan penerapan paradigma pemrograman modern. Sebagai saran untuk penelitian selanjutnya, akan bermanfaat untuk mengeksplorasi integrasi teknologi kecerdasan buatan dalam pengujian penetrasi untuk respons yang lebih dinamis terhadap ancaman siber. Meskipun penelitian ini memberikan wawasan berharga, terdapat keterbatasan dalam variasi *tools* pengujian dan sampel situs web yang terbatas, yang menyarankan perlunya pendekatan yang lebih inklusif dan diversifikasi alat pengujian untuk memperoleh perspektif yang lebih luas dalam keamanan siber. Keberhasilan dalam identifikasi kerentanan ini menegaskan kontribusi signifikan penelitian terhadap pengembangan strategi keamanan yang lebih tangguh, sementara keterbatasannya membuka peluang untuk peningkatan dan inovasi berkelanjutan dalam bidang keamanan informasi.

REFERENSI

[1] B. Baharuddin, H. Wakkang, dan B. Irianto, "IMPLEMENTASI WEB SERVICE DENGAN METODE REST API UNTUK INTEGRASI DATA COVID 19 DI SULAWESI SELATAN," *J. Sintaks Log.*, vol. 2, no. 1, Art. no. 1, Feb 2022, doi: 10.31850/jsilog.v2i1.1035.

[2] M. A. Z. Risky dan Y. Yuhandri, "Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS," *J. Sistim Inf. Dan Teknol.*, hlm. 215–220, Sep 2021, doi: 10.37034/jsisfotek.v3i4.68.

[3] A. D. Djayali, "Analisa Serangan SQL Injection pada Server pengisian Kartu Rencana Studi (KRS) Online," *JAMINFOKOM - J. Manaj. Inform. Dan Komput.*, vol. 1, no. 1, Art. no. 1, Sep 2020.

[4] P. G. S. Adinata, I. P. W. P. Putra, N. P. A. I. Juliantari, dan K. D. A. Sutrisna, "Analisis Perbandingan Tools SQL Injection Menggunakan SQLmap, SQLsus dan The Mole," *Inform. J. Ilmu Komput.*, vol. 18, no. 3, hlm. 286, Des 2022, doi: 10.52958/iftk.v18i3.5373.

[5] "The Invicti AppSec Indicator Spring 2021 Edition: Acunetix Web Vulnerability Report," Acunetix. Diakses: 29 Desember 2023. [Daring]. Tersedia pada: https://www.acunetix.com/white-papers/acunetix-web-application-vulnerability-report-2021/

[6] A. Faidlatul Habibah, F. Shabira, dan I. Irwansyah, "Pengaplikasian Teori Penetrasi Sosial pada Aplikasi Online Dating," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 3, no. 1, hlm. 44–53, Jan 2021, doi: 10.47233/jteksis.v3i1.183.

[7] S. U. Sunaringtyas, "Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On," 2021.

[8] A. Alanda, D. Satria, M. I. Ardhana, A. A. Dahlan, dan H. A. Mooduto, "Web Application Penetration Testing Using SQL Injection Attack," *JOIV Int. J. Inform. Vis.*, vol. 5, no. 3, Art. no. 3, Sep 2021, doi: 10.30630/joiv.5.3.470.

[9] M. Alenezi, M. Nadeem, dan R. Asif, "SQL Injection Attacks Countermeasures Assessments," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, Okt 2020, doi: 10.11591/ijeecs.v21.i2.pp1121-1131.

[10] A. B. Setyawan, I. A. Kautsar, dan N. L. Azizah, "Query Response Time Comparison SQL and No SQL for Contact Tracing Application," *Procedia Eng. Life Sci.*, vol. 2, no. 2, Okt 2022, doi: 10.21070/pels.v2i2.1296.

[11] M. Hasibuan dan A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box: Studi Kasus Web Server Diva Karaoke.co.id," *Sudo J. Tek. Inform.*, vol. 1, no. 4, hlm. 171–177, Des 2022, doi: 10.56211/sudo.v1i4.160.

[12] C. B. Setiawan, D. Hariyadi, A. Sholeh, dan A. Wisnuaji, "Pengembangan Aplikasi Information Gathering Berbasis HybridApps," *INTEK J. Inform. Dan Teknol. Inf.*, vol. 5, no. 1, Art. no. 1, Mei 2022, doi: 10.37729/intek.v5i1.1729.

[13] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *J. Inf. Dan Teknol.*, hlm. 70–75, Mar 2022, doi: 10.37034/jidt.v4i1.190.

[14] Y. A. Pohan, Y. Yuhandri, dan S. Sumijan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *J. Sistim Inf. Dan Teknol.*, hlm. 1–6, Sep 2021, doi: 10.37034/jsisfotek.v3i1.36.
[15] J. Panjaitan dan A. F. Pakpahan, "Perancangan Sistem E-Reporting Menggunakan ReactJS dan Firebase," *J. Tek. Inform. Dan Sist. Inf.*, vol. 7, no. 1, Art. no. 1, Apr 2021, doi: 10.28932/jutisi.v7i1.3098.
[16] S. Syamsiah, "Perancangan Flowchart dan Pseudocode Pembelajaran Mengenal Angka dengan Animasi untuk Anak PAUD Rambutan," *STRING Satuan Tulisan Ris. Dan Inov. Teknol.*, vol. 4, no. 1, hlm. 86, Agu 2019, doi: 10.30998/string.v4i1.3623.
[17] S. T. Argaw *dkk.*, "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, hlm. 146, Jul 2020, doi: 10.1186/s12911-020-01161-7.
[18] R. D. E. P. F. D. Hanggara, "Analisis Sistem Antrian Pelanggan SPBU Dengan Pendekatan Simulasi Arena | Jurnal INTECH Teknik Industri Universitas Serang Raya," Des 2020, Diakses: 24 April 2024. [Daring]. Tersedia pada: https://e-jurnal.lppmunsera.org/index.php/INTECH/article/view/2543
[19] "PHP: PHP 8.3.0 Release Announcement." Diakses: 21 April 2024. [Daring]. Tersedia pada: https://www.php.net/releases/8.3/en.php
[20] D. P. Y. Ardiana dan L. H. Loekito, "Gamification design to improve student motivation on learning object-oriented programming," *J. Phys. Conf. Ser.*, vol. 1516, no. 1, hlm. 012041, Apr 2020, doi: 10.1088/1742-6596/1516/1/012041.
[21] M. Fajar, F. Ciuandi, dan A. Munir, "Desain Aplikasi Daily Remainder Menggunakan Model-View Controller Dan Data Access Object," vol. 4, no. 2.
[22] E. Bautista-Villegas, "Metodologías agiles XP y Scrum, empleadas para el desarrollo de páginas web, bajo MVC, con lenguaje PHP y framework Laravel," *Rev. Amaz. Digit.*, vol. 1, no. 1, Art. no. 1, Jan 2022, doi: 10.55873/rad.v1i1.168.
[23] V. Punitha, C. Mala, dan N. Rajagopalan, "A novel deep learning model for detection of denial of service attacks in HTTP traffic over internet," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 33, no. 4, hlm. 240–256, Jan 2020, doi: 10.1504/IJAHUC.2020.106666.
[24] C.-O. Truică, E.-S. Apostol, J. Darmont, dan T. B. Pedersen, "The Forgotten Document-Oriented Database Management Systems: An Overview and Benchmark of Native XML DODBMSes in Comparison with JSON DODBMSes," *Big Data Res.*, vol. 25, hlm. 100205, Jul 2021, doi: 10.1016/j.bdr.2021.100205.
[25] Z. Qu, X. Ling, T. Wang, X. Chen, S. Ji, dan C. Wu, "AdvSQLi: Generating Adversarial SQL Injections Against Real-World WAF-as-a-Service," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, hlm. 2623–2638, 2024, doi: 10.1109/TIFS.2024.3350911.
[26] J. Hansen dan T. Sutabri, "Mendesain Cyber Security Untuk Mencegah Serangan DDoS Pada Website Menggunakan Metode Captcha," vol. 3, no. 1, 2023.

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

SQL Injection: Analisis Efektivitas Uji Penetrasi dalam Aplikasi Web

ORIGINALITY REPORT

18%	17%	17%	17%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Muhammadiyah Sidoarjo Student Paper	15%
2	www.researchgate.net Internet Source	2%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		