ANALISIS KERENTANAN APLIKASI WEB DENGAN TEKNIK SQL INJECTION (STUDI KASUS VULNWEB.COM)

Rolan Firnando[1],Momon Muzakkar[2]
Teknik Komputer, Stmik El Rahma Yogyakarta

INTISARI

Teknik SQL injection merupakan salah satu serangan yang umum dilakukan oleh para penyerang untuk mengakses, mengubah, atau menghapus data dari database yang digunakan oleh aplikasi web. Penelitian ini bertujuan untuk menganalisis kerentanan pada aplikasi web vulnweb.com menggunakan teknik SQL injection.

Untuk mengatasi kerentanan ini, diperlukan implementasi pengamanan yang tepat, seperti penggunaan parameterized query dan validasi input yang ketat. Selain itu, pemilihan bahasa pemrograman dan kerangka kerja yang memperhatikan keamanan juga dapat membantu mengurangi risiko serangan SQL injection.

Hasil penelitian menunjukkan bahwa aplikasi web vulnweb.com memiliki tingkat kerentanan yang cukup tinggi terhadap serangan SQL injection. Beberapa parameter input pada aplikasi web tidak divalidasi dengan baik, sehingga memungkinkan penyerang untuk menginjeksikan kode SQL yang berbahaya.

Kata kunci: *Sql Injection, DVWA, vulnweb.com, SqlMap*

ABSTRACT

The rapid advancement of web applications across multiple domains has raised concerns about their vulnerability to security attacks. One of the most common and dangerous threats is SQL injection attack, which is a technique used by attackers to manipulate web application databases by inserting malicious SQL code. This research focuses on analyzing the vulnerability of the vulnweb.com web application against SQL injection attacks.

To overcome this vulnerability, it is very important to implement proper security measures, such as the use of parameterized queries and strict input validation. In addition, choosing a safe programming language and framework can also help reduce the risk of SQL injection attacks.

The results show that vulnweb.com has a significant vulnerability to SQL injection attacks. Lacking input validation on some parameters allows attackers to successfully inject malicious SQL code.

Keywords: Sql Injection, DVWA, vulnweb.com, SqlMap.

1. Latar Belakang

Dalam era digitalisasi yang semakin berkembang, penggunaan aplikasi web sebagai salah satu media dalam berinteraksi di dunia maya semakin meningkat. Aplikasi web menjadi alat yang efektif dalam mempermudah dan mempercepat akses informasi serta layanan yang disediakan oleh suatu sistem. Namun, keamanan aplikasi web menjadi perhatian utama dalam pengembangan aplikasi web karena aplikasi web rentan terhadap serangan keamanan yang berbagai macam bentuknya. Salah satu serangan keamanan yang sering terjadi pada aplikasi web adalah serangan SQL

Injection(Nursapdahi, 2022). . Dengan menyuntikkan kode SQL yang jahat ke dalam masukan, seorang penyerang dapat memanipulasi perilaku query dan melakukan tindakan yang tidak dimaksudkan pada database(Deni Danuarta, 2018).

2. METODE PENELITIAN

Metode Penelitian merupakan tahapan dan instrumen yang digunakan untuk memilih dan menyusun teknik penelitian, maka setiap penelitian pasti memiliki metode yang khas sesuai masalah dan tujuan penelitiannya. Sesuai pandangan positivistik, bila suatu Metode Penelitian dilakukan ulang oleh peneliti lain, maka akan diperoleh hasil yang sama (prinsip objektivitas). Teknik pengumpulan data suatu penelitian mungkin bisa sama dengan penelitian lain, misal teknik wawancara, tetapi Metode Penelitiannya pasti tidak sama.

Adapun Metode penelitian dilakukan sebagai berikut.

A. Metode Deskriptif

1. Peneliti fokus pada teknik SQL Injection untuk menguji kerentanan pada aplikasi web vulnweb
2. Pengujian cara manual dengan memanfaatkan celah keamanan dalam aplikasi web untuk memungkinkan penyerang menyisipkan perintah SQL berbahaya kedalam pernyataan SQL yang dieksikusi oleh database.
3. Pengujian menggunakan framewor SqlMap dengan cara otomatis menggunakan tool atau software khusus.

B. Metode Korelasional/ Asosiasi

1. Sistem ini menggunakan fitur dari teknologi antara lain SQL Injection, Aplikasi web, SqlMap.

C. Metode Kausal Komparatif

1. Penelitian bersifat ec post facto, artinya data yang dikumpulkan semua setelah kejadian yang dipersoalkan langsung (lewat).
2. Peneliti mengambil satu atau lebih akibat (sebagai “dependent Variabels”) dan menguji data itu dengan menelusuri kembali ke masa lampau unntuk mencari sebab-sebab, saling berhubungan dan maknanya.

   Berikut ini beberapa kebutuhan perangkat dalam pengujian.

   a) Sebuah Komputer/Laptop yang berfungsi sebagai server.
   b) Sebuah personal Komputer/Laptop yang berfungsi sebagai penguji.
   c) Alat dan bahan yang digunakan dalam penelitian ini sebagai berikut.
      1. Laptop Acer 3 intel
      2. Laptop Lenovo intel core i5
      3. Aplikasi Web
      4. MySQLMap
      5. Klik Linux

3. TABLE DAN GAMBAR

- **Table**

Table 2.1 Ringkasan Penelitian

No	Nama, Tahun	Judul	Persamaan dan Perbedaan
1	Deni Danuarta, 2018	Analsis keamanan dan DVWA terhadap serangan SQL Injection	Mengalami kesulitan mengevaluasi keamanan aplikasi web terhadap serangan SQL injection, dalam penelitian nya dilakukan analisis keamanan dan DVWA untuk mencegah beberapa aplikasi web yang rentan terhadap serangan SQL injection.
2	Mochamad Alfan Rosid, 2022	Serangan SQL Injection terhadap server snort IDS melalui aplikasi DVWA	Dalam penelitiannya mengenali adanya penyusup yaitu dengan cara menyadap paket data dan kemudian membandingkannya dengan database rule sehingga dilakukan serangan SQL injection terhadap server snort IDS melalui aplikasi DVWA, snort dan juga wireshark agar dapat meningkatkan keamanan didalam jaringan dan secara otomatis untuk menghambat semua serangan yang akan menggangu sebuah jaringan.
3	Lelly Hidayah Anggraini, 2015	Pengujian terhadap keamanan website UMK	Dalam penelitiannya peneliti melakukan pengujian terhadap keamanan website UMK dengan melakukan SQL Injection sehingga Dapat mengetahui kelemahan website UMK apakah sistem rentan terhadap serangan.

- Gambar

A. Penetration Testing

Gambar Penetration Testing

Penetration testing (pentest) adalah kegiatan untuk mengevaluasi keamanan dari suatu sistem jaringan komputer.

B. SQL Injection

Gambar SQL Injection

SQL (Structured Query Language) adalah bahasa yang digunakan untuk berkomunikasi dengan basis data dan melakukan manipulasi data di dalamnya. SQL injection adalah sebuah teknik serangan pada sistem basis data yang memanfaatkan kelemahan pada aplikasi atau sistem yang menggunakan SQL untuk mengakses dan memanipulasi data.

C. Aplikasi Web

Gambar Aplikasi Web

Aplikasi web adalah program komputer yang dirancang untuk diakses melalui jaringan internet dengan menggunakan browser web.

D. My SQL

Gambar MySQL

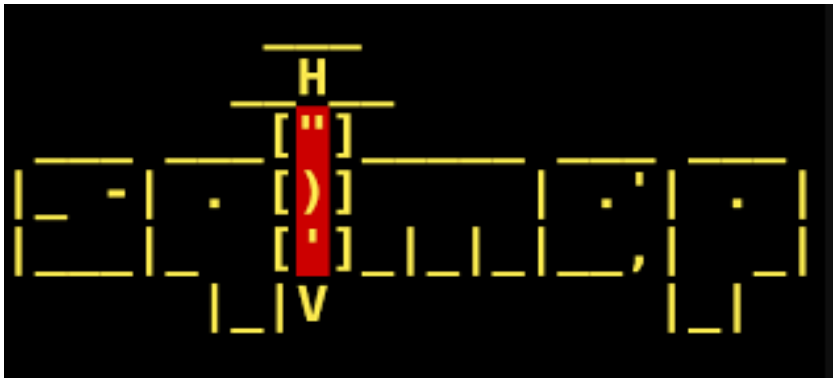
MySQL adalah Relational Database Management System (RDBMS) yang didistribusikan secara gratis dibawah lisensi GPL (General Public License). Dimana setiap orang bebas untuk menggunakan MySQL, namun tidak boleh dijadikan produk turunan yang bersifat komersial.

E. Vullenweb.Com

Gambar Vullenweb.Com

vulnwab adalah salah satu lab publik yang terdapat banyak jenis website seperti online shop, blog, forum dll untuk di coba kerentanannya terhadap beberapa metode pengujian seperti SQL Injection, Cross-site Scrpting (XSS), Cross-site Request Forgery (CSRF) dan metode pengujian lainya. Pada dasarnya vulnweb di bangun oleh sebuah perusahaan software khusus Vulnerability Scanner yang berlokasi di Austin Texax, Amerika Serikat (SoftwareTestingHelp, 2023).

F. SQLMap



Gambar SQLMap

SQLmap adalah alat otomatis untuk melakukan serangan SQL injection pada sebuah website atau aplikasi. Alat ini dapat mendeteksi kerentanan pada sebuah aplikasi web, mengeksploitasi kelemahan tersebut, dan memperoleh akses ke database yang mendasarinya(Sukma Aji, 2022).

SQLmap dapat melakukan berbagai macam jenis serangan, termasuk serangan bertingkat (multi-level), serangan blind (tidak menghasilkan output langsung), dan serangan waktu berbasis respons (time-based response)(Sukma Aji,2022)..

Selain itu, SQLmap juga mendukung berbagai jenis database, termasuk MySQL, Oracle, PostgreSQL, dan Microsoft SQL Server. Alat ini tersedia secara gratis dan open-source, dan tersedia dalam berbagai platform, termasuk Windows, Linux, dan MacOS(Arif Senja Fitrani, 2022).

Namun, penting untuk diingat bahwa penggunaan SQLmap untuk melakukan serangan tanpa izin adalah ilegal dan dapat berakibat serius. Alat ini sebaiknya digunakan hanya untuk tujuan pengujian keamanan pada website atau aplikasi yang telah diberi izin oleh pemiliknya(Nursapdahi, 2012).

4. HASIL DAN PEMBAHASAN

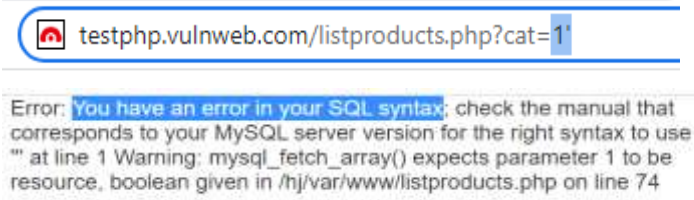
Implementasi merupakan dan pembahasan merupakan tahap yang berisi tentang pengoprasian dan pengujian pada keadaan yang sebenarnya. Berikut implementasi dan pembahasan serangan SQL injection pada website vulnweb.com.

Gambar 5. 1 Halaman Produk

Pada Gambar 5.1 pilih salah satu kategori yang tersedia kemudia cek parameter yang dikirim di url untuk memastikan apakah bisa melakukan serangan sql injection dihalaman kategori.

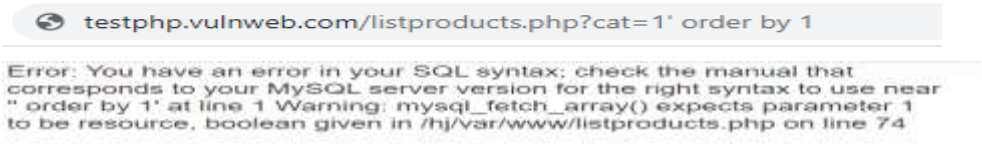
Gambar 5. 2 Tampilan Kategori

Pada Gambar 5.2 terdapat parameter cat=1, langkah selanjutnya memasukkan petik satu (‘) untuk mendapatkan pesan error pada website ini.



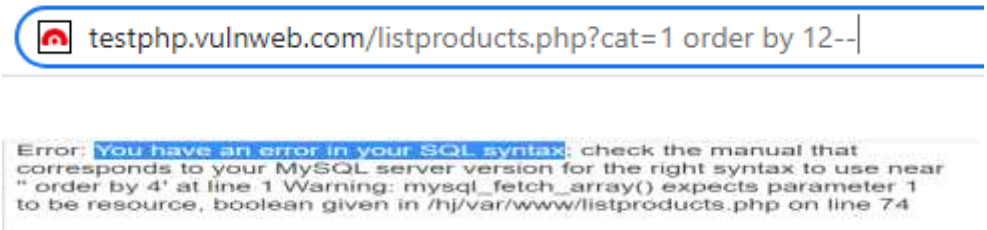
Gambar 5. 3 Pesan Error

Pada Gambar 5.3 melihat pesan error yang keluar dengan ini situs vulnweb.com terdapat kerentanan sql injection, langkah selanjutnya mencari jumlah table yang terdapat pada database menggunakan query order by.



Mencari Jumlah Table

Pada Gambar 5.4 dengan mengganti angka 1 menjadi 2/3/4/5/6/7/8/9/10/11/12 dan seterusnya sampai muncul pesan error lagi.



Gambar 5. 4 Pesan Error

Pada Gambar 5.5 ketika memasukkan angka 12 muncul pesan error yang artinya jumlah table pada database adalah 11, langkah selanjutnya adalah mencari no unik atau no injeksi yang dimana no unik tersebut berguna untuk menempatkan payload atau injeksi kita, gunakan query union select untuk menemukan no unik tersebut.

Query Union Select Untuk Mencari No Injeksi

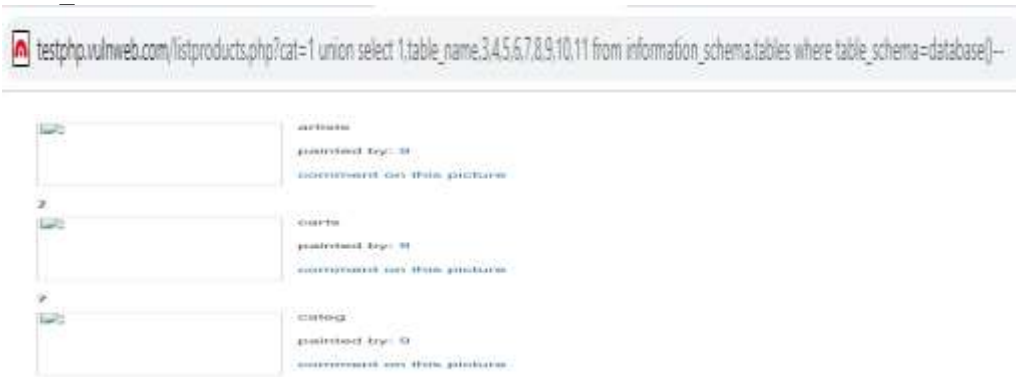
Pada Gambar 5.6 mendapatkan angka 7,2,9 dimana kolom ini rentan terhadap serangan sql injection, sekarang gunakan angka tersebut untuk mendapatkan informasi tentang nama database dengan query database() pada diangka 2.

Query Union Select Untuk Mencari Database

Pada Gambar 5.7 hal yang sama untuk mendapatkan informasi versi database menggunakan query version() diangka 7.

Query Union Select Untuk Mencari Database Version

Pada Gambar 5.8 mencari nama table pada database acuart menggunakan query table_nama.



Query Union Select Untuk Mencari Nama Table

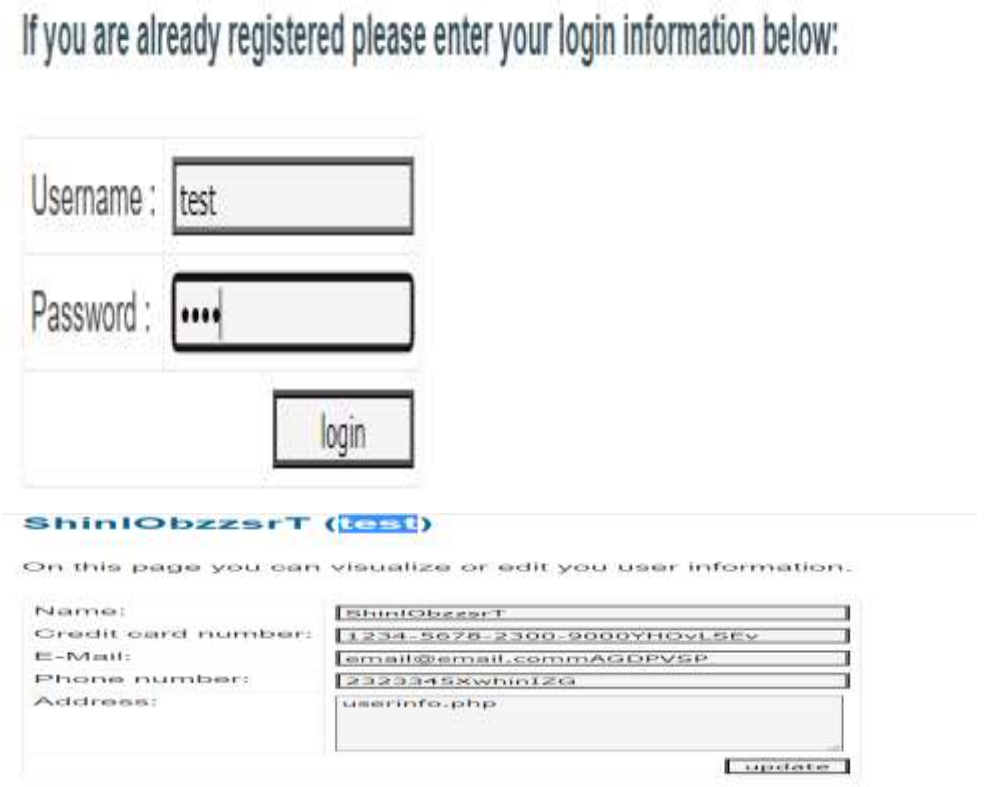
Pada Gambar 5.9 mencari nama kolom pada table ‘users’ menggunakan query column_name.

Gambar Query Union Select Untuk Mencari Nama Kolom

Pada Gambar 5.10 dump data pada table ‘users’ sesuai dengan kolom yang ada menggunakan query group concat.

Gambar Query Group_Concat Untuk Dump Database

Pada Gambar 5.11 mendapatkan username dan password sekarang coba login menggunakan username dan password tersebut.



Gambar 5. 5 Login

5. KESIMPULAN

a. Vulnweb.com rentan terhadap serangan SQL Injection: Hasil uji penetrasi menunjukkan bahwa aplikasi web vulnweb.com memiliki tingkat kerentanan yang signifikan terhadap serangan SQL injection. Kondisi ini mengindikasikan bahwa penggunaan teknik SQL injection pada aplikasi yang tidak memperhatikan keamanan dapat menyebabkan risiko yang serius.

b. Pengamanan aplikasi web perlu ditingkatkan: Kesimpulan ini menunjukkan perlunya meningkatkan pengamanan aplikasi web dalam menghadapi serangan SQL injection. Pengembang perangkat lunak perlu memastikan bahwa parameter input di-validasi dengan baik dan menggunakan teknik parameterized query untuk mencegah potensi eksploitasi melalui penyisipan kode SQL berbahaya.

c. Peran bahasa pemrograman dan kerangka kerja: Pilihan bahasa pemrograman dan kerangka kerja dalam pengembangan

aplikasi web dapat mempengaruhi tingkat kerentanannya terhadap serangan SQL injection. Penggunaan bahasa pemrograman dan kerangka kerja yang lebih aman dan terpercaya dapat membantu mengurangi risiko serangan ini.

d. Pentingnya uji keamanan secara berkala: Penelitian ini menekankan pentingnya melakukan uji keamanan secara berkala terhadap aplikasi web. Uji penetrasi dapat membantu mengidentifikasi celah keamanan dan memungkinkan perbaikan tepat waktu sebelum celah tersebut dieksploitasi oleh penyerang.
e. Kesadaran keamanan pengembang: Kesimpulan ini menegaskan bahwa pengembang aplikasi web harus meningkatkan kesadaran mereka terhadap masalah keamanan, termasuk risiko serangan SQL injection. Pengetahuan dan pemahaman yang lebih mendalam tentang teknik-teknik keamanan dapat membantu mencegah dan mengurangi kerentanan pada aplikasi web.

6. SARAN

a. Perbaiki dan tingkatkan engamanan aplikasi: Dalam menghadapi kerentanan SQL injection, perlu dilakukan perbaikan pada aplikasi web vulnweb.com. Implementasikan validasi input yang ketat dan gunakan teknik parameterized query untuk menghindari celah penyisipan kode SQL yang berbahaya.
b. Uji keamanan secara berkala: Melakukan uji penetrasi secara berkala pada aplikasi web sangat penting untuk mengidentifikasi dan mengatasi celah keamanan sebelum penyerang melakukannya. Selain itu, uji keamanan secara berkala juga membantu memastikan bahwa setiap perubahan pada aplikasi tidak mengenalkan kerentanan baru.
c. Tingkatkan kesadaran keamanan pengembang: Peningkatan kesadaran keamanan di antara pengembang aplikasi web adalah kunci untuk mengurangi risiko serangan SQL injection. Dengan meningkatkan pemahaman mereka tentang teknik-teknik keamanan dan mengikuti praktik terbaik dalam pengembangan perangkat lunak, pengembang dapat membantu melindungi aplikasi dari ancaman keamanan.
d. Gunakan bahasa pemrograman dan kerangka kerja yang aman: Pemilihan bahasa pemrograman dan kerangka kerja yang aman dapat membantu mengurangi tingkat kerentanan terhadap serangan SQL injection. Pilihlah bahasa pemrograman dan kerangka kerja yang memiliki fitur keamanan yang kuat dan memiliki sejarah yang baik dalam menghadapi serangan keamanan.
e. Pertahankan aplikasi web dengan pembaruan terbaru: Pastikan aplikasi web DVWA selalu diperbarui dengan versi terbaru dari bahasa pemrograman, kerangka kerja, dan perangkat lunak lainnya. Pembaruan sering kali mencakup perbaikan keamanan dan kerentanan baru yang ditemukan,

sehingga memastikan aplikasi tetap aman dari ancaman terkini.

f. Implementasikan metode autentikasi yang kuat: Memastikan bahwa aplikasi web vulnweb.com memiliki metode autentikasi yang kuat dapat membantu melindungi data sensitif dari akses yang tidak sah. Autentikasi dua faktor atau penggunaan mekanisme otentikasi yang lebih aman dapat meningkatkan keamanan secara keseluruhan.

g. Pelajari dan analisis serangan lainnya: Selain SQL injection, ada banyak teknik serangan lain yang dapat menargetkan aplikasi web. Pelajari dan analisis serangan lainnya, seperti Cross-Site Scripting (XSS) atau Cross-Site Request Forgery (CSRF), untuk memahami celah keamanan yang mungkin ada pada aplikasi dan mengambil langkah-langkah pencegahan yang sesuai.

7. UCAPAN TERIMA KASIH

Terima kasih yang sebesar-besarnya kepada Pak Momon Muzakkar selaku dosen pembimbing saya dalam menyelesaikan Skripsi ini dan tak lupa juga dengan para dosen yang telah ikut serta dalam penyelesain skripsi ini serta semua pihak yang terkait.

Daftar Pustaka

Adinata, P. G, 2022, Analisis Perbandingan Tools SQL Injection Menggunakan SQLmap,*JURNAL INFORMATIK Edisi ke-18, Nomor 3, Desember 2022, 18*, 28-92.

David Axmark, 2022, MySQL. Konsep pengoperasian untuk pemilihan data, 67-70.

Danuarta, D, 2018, Membuat Alat Untuk Mendeteksi Serangan Sql Injection Menggunakan Sonrt IDS Dan Bayesian Network. *DeteksiSeranganSQLInjectionDenganMetodeBayesianNetwork*, 28-41.

Isna Wardiah, 2020, Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web. *Penetration Testing, SQL Injection, Vulnerabilities, Web, 4*.

Keycdn, 2021, Web Security. *Kerentanan SQL Injection*, 35-52.

Lelly Hidayah Anggraini, 2015, Pengujian Dan Analisa Keamanan Website Terhadap Serangan SQL Injection. *M Dahlan · 2014 · Cited by 7 — Volume 7 Nomor 1 Juni 2015, 7*.

Leonardo Pandapotan, 2021, Aplikasi Web. Melindungi Aplikasi Web Dari Serangan Yang Membahayakan Keamanan Dan Privasi Data, 87-102.

Muhamad Musliah, 2019, Penetration Testing. Mengavaluasi Keamanan Suatu Sistem Jaringan Komputer, *JURNAL ARTIKEL*, 73-89.

Mochamad Alfan Rosid, F. S. (2022, Juli). Studi Analisa Serangan Sql. *Seminar Nasional Inovasi Teknologi UN PGRI Kediri, 23 Juli 2022*. Teknik Informatika.

Nursapdahi, (2022). SQL Injection. Penyerangan Pada Sistem Basis Data Dengan Memanfaatkan Kelemahan Website, *JURNAL ARTIKEL*, 34-56.

Saputra, R. I, 2023, Penetration Testing. *Retrieved From https://fourtrezz.co.id/artikel/pengertian-penetration-testing-dan-manfaatnya-bagi-perusahaan-anda/*.

Schevencko, 2023. Vulnweb.com. *Lab publik yang terdapat banyak jenis website*, *JURNAL ARTIKEL*, 5-9.

Sukma Aji, 2022, SQLmap. Mendeteksi kerentanan pada sebuah aplikasi web, *JURNAL INFORMATIK* 43-52

Taufiqul Hidayah, 2017, Penerapan High Availabilyty Web Server Menggunakan Nginx Dan Mode security. Jurnal Informatika Terpadu, 95-102.