Jurnal Informatika Medis (J-INFORMED)
Universitas Muhammadiyah Muara Bungo
DOI: https://doi.org/10.52060/im.v1i2.1629
Vol. 1, No. 2, November-2023, hlm. 68-72
e-ISSN: 2987-4661

DATABASE VULNERABILITY TESTING MEMANFAATKAN SQLMAP PADA UBUNTU 22.04 (STUDI KASUS : ANTARATECH.NET)

Sidik Praptomo[1]
[1]Universitas Muhammadiyah Muara Bungo
[1]sidikmdj@gmail.com

Suryanto[2]
[2]Pascasarjana Sistem Informasi UTDI
[2]student.suryanto23@mti.utdi.ac.id

Jefdy Kurniawan[3]
[3]Universitas Muhammadiyah Muara Bungo
[3]jefdykurniawan@gmail.com

ABSTRAK

Vulnerability trial of database using SQLMap on Ubuntu 22.04 is an important process to identify security vulnerabilities in database systems running on the Ubuntu 22.04 platform. This study discusses the importance of vulnerability Uji coba in the information security space, with a focus on SQL-based database systems and the Ubuntu 22.04 platform. We describe a vulnerability Uji coba methodology that involves the use of SQLMap, a penetration tool specifically designed to identify SQL injection vulnerabilities. This research covers the basic concepts of SQL injection, the steps of implementing SQLMap on the Ubuntu 22.04 platform, and how to interpret the test results. We also discuss the benefits of using SQLMap, including an in-depth understanding of database vulnerabilities that can help organizations improve the security of their systems. The result of this research is a practical guide to performing database vulnerability testing with SQLMap on the Ubuntu 22.04 platform, thus helping security professionals and system administrators to identify and address potential vulnerabilities that could compromise data integrity and confidentiality. This research makes an important contribution in the effort to maintain the security of database systems in the challenging digital era.

Kata kunci: ***Vulnerability, SQLMap, Ubuntu***

1. PENDAHULUAN

Uji coba *vulnerability* pada basis data adalah praktik yang sangat penting dalam dunia teknologi informasi saat ini. Hal ini seiring dengan fakta bahwa basis data merupakan komponen sentral dalam hampir semua aplikasi dan sistem, yang menyimpan data yang sangat berharga dan sensitif. Uji coba vulnerabiliti basis data adalah proses untuk mengidentifikasi dan mengatasi potensi masalah keamanan yang dapat memengaruhi basis data. Salah satu alasan utama mengapa uji coba *vulnerability* basis data sangat penting adalah untuk melindungi data sensitif. Basis data sering kali berisi informasi yang sangat penting, termasuk data pribadi pelanggan,

Jurnal Informatika Medis (J-INFORMED)
Universitas Muhammadiyah Muara Bungo
DOI: https://doi.org/10.52060/im.v1i2.1629
Vol. 1, No. 2, November-2023, hlm. 68-72
e-ISSN: 2987-4661

informasi keuangan, dan data perusahaan yang sangat bernilai. Jika basis data tersebut rentan terhadap serangan atau ancaman keamanan, data ini dapat dicuri atau dikompromi, yang dapat mengakibatkan kerugian finansial yang signifikan dan merusak reputasi perusahaan.

Selain melindungi data, uji coba *vulnerability* basis data juga membantu dalam mematuhi peraturan dan undang-undang yang berkaitan dengan privasi dan keamanan data. Banyak negara dan yurisdiksi memiliki regulasi ketat yang mengatur perlindungan data pribadi, seperti regulasi umum perlindungan data *(general data protection regulation/gdpr)* di uni eropa. Organisasi yang tidak mematuhi regulasi ini dapat menghadapi sanksi berat. Oleh karena itu, dengan mengidentifikasi dan mengatasi *vulnerability* basis data, perusahaan dapat memastikan bahwa mereka tetap mematuhi regulasi yang berlaku. Selanjutnya, uji coba *vulnerabiliy* basis data adalah langkah proaktif untuk mencegah kerugian. Dengan mengidentifikasi potensi kerentanan dan kelemahan dalam basis data sebelum serangan terjadi, organisasi dapat mengambil tindakan preventif untuk mengurangi risiko keamanan. Ini dapat mencakup peningkatan kebijakan keamanan, perbaikan kelemahan teknis, dan pelatihan staf.

Pentingnya uji coba *vulnerability* basis data juga sangat relevan dalam era serangan siber yang semakin kompleks. Serangan siber dapat mengancam basis data dengan berbagai metode, seperti *sql injection, denial of service (dos)*, dan ancaman *malware.* Dengan menguji *vulnerability* basis data secara berkala, organisasi dapat mengidentifikasi potensi masalah keamanan sebelum serangan terjadi, yang memungkinkan mereka untuk mengambil tindakan yang diperlukan. Selain itu, uji coba *vulnerability* basis data dapat membantu meningkatkan kualitas aplikasi dan sistem. Dengan mengidentifikasi masalah keamanan pada tahap awal pengembangan, organisasi dapat memastikan bahwa aplikasi yang dihasilkan lebih aman dan andal. Ini pada gilirannya dapat meningkatkan kepercayaan pelanggan dan reputasi perusahaan. Pentingnya uji coba *vulnerability* basis data juga terlihat dalam kerentanan internal. Beberapa ancaman keamanan berasal dari dalam organisasi, baik disengaja atau tidak. Dengan menguji *vulnerability* basis data, organisasi dapat mengidentifikasi akses yang tidak sah atau aktivitas yang mencurigakan. Sehingga uji coba *vulnerability* basis data adalah praktik penting yang tidak boleh diabaikan. Hal ini melindungi data sensitif, mematuhi regulasi, mencegah kerugian, dan meningkatkan keamanan serta kualitas sistem. Oleh karena itu, organisasi harus mengintegrasikan uji coba *vulnerability* basis data sebagai bagian integral dari strategi keamanan mereka.

2. METODOLOGI PENELITIAN

Kebutuhan *Software*

Software atau perangkat lunak adalah sebuah perangkat yang menghubungkan suatu komputer dengan pengguna atau bisa dikatakan sebagai perangkat yang umumnya digunakan untuk mengontrol perangkat keras atau bisa juga digunakan untuk menghasilkan data informasi. Penelitian ini memerlukan beberapa *software* antara lain:

1. Distro Linux Ubuntu versi 22.04

2. SQLMap

3. Terminal

Jurnal Informatika Medis (J-INFORMED)
Universitas Muhammadiyah Muara Bungo
DOI: https://doi.org/10.52060/im.v1i2.1629
Vol. 1, No. 2, November-2023, hlm. 68-72
e-ISSN: 2987-4661

Uji Vulnerabiliti
Menurut GOV-CSIRT (Goverment Computer Security Incident Response Team), vulnerability assessment adalah melakukan identifikasi vulnerability dari suatu aplikasi, sistem operasi dan infrastruktur jaringan. Vulnerability assessment tidak melakukan eksploitasi celah atau kelemahan dari suatu sistem. Sedangkan vulnerability adalah suatu kelemahan dalam desain sistem, implementasi sistem atau operasi dan manajemen yang dapat dimanfaatkan untuk melanggar kebijakan kemanan sistem. Vulnerability assessment lebih fokus untuk menemukan beragam public vulnerability pada seluruh sistem komputer dalam jaringan target. Dalam vulnerability assessment tidak menuju ke proses eksploitasi namun memiliki potensi untuk di eksploitasi sehingga harus ditutup kerentanan yang ditemukan tersebut.

Hasil Uji Vulnerabiliti

Hasil uji coba vulnerabiliti dikategorikan menjadi 3 yaitu:

1. Level *High*

Pada level ini merepresentasikan uji coba vulnerabiliti yang menghasilkan kerentanan yang beresiko signifikan bagi sistem yang telah dibuat dan memerlukan penanganan sesegera mungkin

2. Level *Medium*

Pada level ini hasil uji coba vulnerabiliti merepresentasikan kerentanan yang bersifat lokal, dan memerlukan penanganan yang bersifat lokal.

3. Level *Low*

Pada level ini tidak representasi hasil uji coba bersifat rendah dan tidak mempengaruhi sistem yang telah dibuat namun tetap memerlukan penanganan.

SQL Injection

SQL Injection merupakan sebuah teknik serangan yang memanfaatkan celah keamanan pada sebuah *web application*. Serangan ini termasuk ke dalam jenis serangan *Password Attack*. Akibat dari serangan SQL Injection adalah dapat memanipulasi *database* melalui aktifitas yang tidak sah. Dengan menggunakan media berupa *Uniform Resource Location* (URL) dan *Uniform Resource Identifier* (URI), serangan *SQL Injection* ini dapat melakukan proses retrieving data.

3. HASIL DAN PEMBAHASAN

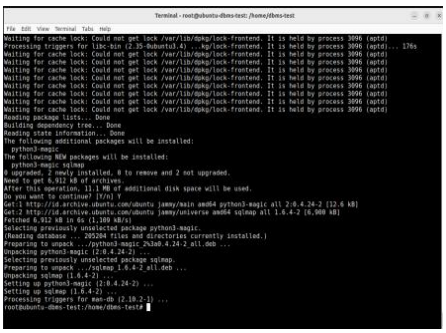
Uji Coba Vulnerabiliti dengan Studi Kasus *Web Application* "antaratech.net"

Langkah pertama yang harus dilakukan adalah melakukan installasi sistem operasi distro linux ubuntu versi terbaru 22.04, sistem operasi tersebut bisa didapatkan dari website berikut ini "https://ubuntu.com/download/desktop"

Gambar 1. *Install Ubuntu 22.04*

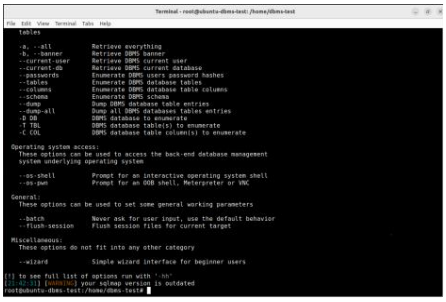
Setelah melakukan installasi *Ubuntu 22.04,* selanjutnya adalah melakukan installasi *software SQLMap,* dengan cara buka jendela aplikasi "terminal", kemudian ketikkan perintah "sudo su" untuk masuk kedalam *root folder ubuntu 22.04,* kemudian akan diminta memasukkan *password user,* lalu jalankan perintah "sudo apt update", setelah selesai melakukan update repository, selanjutnya masukkan perintah "sudo apt install sqlmap".

Jurnal Informatika Medis (J-INFORMED)
Universitas Muhammadiyah Muara Bungo
DOI: https://doi.org/10.52060/im.v1i2.1629
Vol. 1, No. 2, November-2023, hlm. 68-72
e-ISSN: 2987-4661



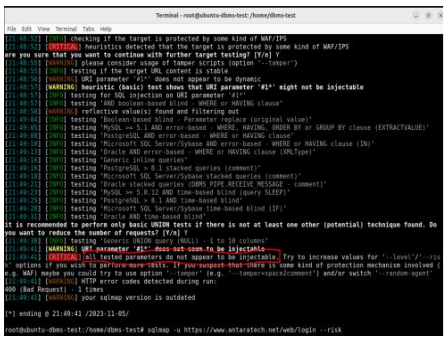
Gambar 2. *Install Sqlmap*

Langkah selanjutnya adalah memahami perintah yang perlu digunakan untuk melakukan uji coba vulnerabiliti menggunakan perintah "sqlmap -h". Perintah tersebut dapat menjelaskan semua fungsi yang dapat digunakan untuk melakukan uji coba. Terdapat berbagai macam perintah yang dapat dilihat pada Gambar 3. *Sqlmap Feature Function.*



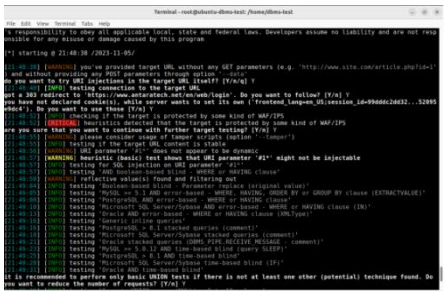
Gambar 3. *Sqlmap Feature Function*

Setelah memahapi perintah apa saja yang dapat digunakan dalam sqlmap, masukkan perintah "sqlmap -u https://www.antaratech.net/web/login --dbs", didapatkan hasil uji coba sebagai berikut



Gambar 4. Hasil uji coba

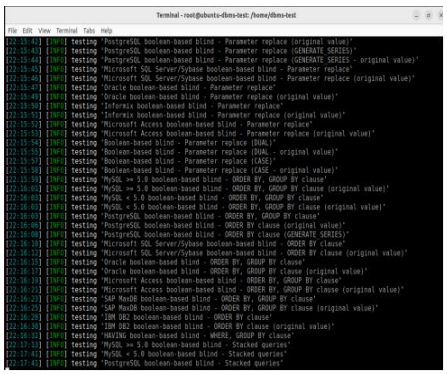
Gamrar 4 menjelaskan bahwa website antaratech.net sudah menerapkan proteksi terhadap berbagai macam jenis penetrasi yang dapat dilakukan melalui sqlmap, dapat dibuktikan melalui penjelasan *"all tested parameters do not appear to be injected".* Pada percobaan tersebut sqlmap melakukan testing menggunakan beberapa macam DBMS yang dapat dijelaskan melalui Gambar 5. Parameter testing SQLMap



Gambar 5. Parameter testing SQLMap

Setelah melakukan uji coba dasar terhadap website Antara Tech, dapat dilakukan ujicoba lanjutan dengan menambahkan level risk kepada perintah di sqlmap, level risk yang diipakai dalam penelitian ini menggunakan level risk = 5 yang bisa dijabarkan adalah penetrasi menggunakan dan menambahkan header host untuk melakukan penetrasi, didapatkan hasil sebagai berikut

Jurnal Informatika Medis (J-INFORMED)
Universitas Muhammadiyah Muara Bungo
DOI: https://doi.org/10.52060/im.v1i2.1629
Vol. 1, No. 2, November-2023, hlm. 68-72
e-ISSN: 2987-4661



Gambar 6. Parameter uji coba level risk 5

Pada ujicoba dengan menggunakan level risk 5, didapatkan hasil website antaratech.net tidak dapat dilakukan penetrasi dengan menggunakan SQLMap, pada level risk 5, terdapat lebih banyak parameter tes yang digunakan.

4. SUMBER PUSTAKA/RUJUKAN

[1] M. ULA, "Evaluasi Kinerja Software Web Penetration Testing," TECHSI - J. Tek. Inform., vol. 11, no. 3, p. 336, Oct. 2020, doi: 10.29103/TECHSI.V11I3.1996.

[2] A. RICO AGARTA, "Analisa Keamanan Website Pada Universitas Gunadarma Terhadap Serangan Sql Injection," Apr. 2021, Accessed: Oct. 06, 2021. [Online]. Available: https://www.binadarma.ac.id/.

[3] B. BIN HALIB, E. BUDIMAN, and H. J. SETYADI, "Teknik Hacking Web Server Dengan Sqlmap Di Kali Linux," J. Rekayasa Teknol. Inf., vol. 1, no. 1, pp. 67–72, Jun. 2020, doi: 10.30872/JURTI.V1I1.642.

[4] R. U. PUTRI and J. E. ISTIYANTO, "Analisis Forensik Jaringan Studi Kasus Serangan Sql injection pada Server Universitas Gadjah Mada," IJCCS (Indonesian J. Comput. Cybern. Syst., vol. 6, no. 2, pp. 101– 112, Jul. 2021, doi: 10.22146/IJCCS.2157.

[5] "Kalilinux Penetration Testing Bible - GoogleBooks."https://www.google.co.id/books/edition/Kali_Linux_Penetration_Testing_Bible/0EkrEAAAQBAJ?hl=en&gbpv=1&dq=kali+linux&printsec=fron tcover (accessed Oct. 12, 2021).

[6] S. S. ARDIANSYAH, S. RAHARJO, and J. TRIYONO, "Analisis Keamanan Serangan Sql Injection Berdasarkan Metode Koneksi Database," J. Scr., vol. 4, no. 2, pp. 72–80, Dec. 2016, Accessed: Oct. 06, 2021. [Online]. Available: https://journal.akprind.ac.id/index.php/script/article/view/742.

[7] S. UTORO et al., "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard."

[8] D. KURNIA, "Analisis Forensik Serangan Sql injection dan DoS Menggunakan Instrution Detection System Pada Server Berbasis Lokal," InfoTekJar J. Nas. Inform. dan Teknol. Jar., vol. 4, no. 2, pp. 208–212, Apr. 2020, doi: 10.30743/INFOTEKJAR.V4I2.2420.