E-ISSN : 2722-0346

IMPLEMENTASI SECURITY SISTEM BLACK ARCH LINUX

Gregorius Hendita Artha Kusuma[1]
Program Studi Teknik Informatika
Fakultas Teknik Universitas Pancasila
gregorius@univpancasila.ac.id[1]

***Abstrak*—Dalam era digital yang semakin berkembang, keamanan sistem dan data menjadi fokus utama dalam dunia teknologi informasi. Banyak ancaman dan juga peluang yang muncul sekarang terutama di bidang siber. Adapun Ancaman seperti kejahatan siber, pencurian data, dan peretasan situs web semakin merajalela, memaksa organisasi dan individu untuk menghadapinya. Paper ini menjelaskan penggunaan security sistem menggunakan dua alat penting dalam keamanan siber,yaitu SQLMap dan John The Ripper, dalam lingkungan BlackArch Linux. SQLMap digunakan untuk mendeteksi dan mengeksploitasi kerentanan SQL injection dalam aplikasi web, sementara John The Ripper digunakan untuk melihat nilai dari password yang terenkripsi. Penelitian ini mengikuti metode Action Research yang melibatkan langkah-langkah untuk mengevaluasi kerentanan SQL injection pada situs web target, mengakses data sensitif dari database, dan mencoba melihat nilai password yang terenkripsi. Hasil penelitian mengungkapkan bahwa SQLMap efektif dalam mendeteksi dan mengeksploitasi kerentanan, sementara John The Ripper membantu dalam menguji kekuatan password. Hal ini juga bisa mengetahui kerentanan dalam sebuah website melalui kekuatan password yang digunakan dalam pengamanan datanya.**

***Kata Kunci*— Security Sistem, SQLMap, Black Arch Linux, SQL injection, John The Ripper**

I. PENDAHULUAN

Pada era digital yang semakin berkembang, keamanan sistem dan data menjadi salah satu aspek paling penting dalam dunia teknologi informasi. Kejahatan siber, pencurian data, dan peretasan situs web semakin menjadi ancaman yang harus dihadapi oleh organisasi dan individu. Oleh karena itu, penting bagi para profesional keamanan siber, administrator sistem, dan pelajar dengan bidang IT untuk memahami alat-alat yang dapat digunakan untuk mengidentifikasi dan mengatasi potensi kerentanan dalam sistem mereka.

Salah satu alat yang sangat berguna dalam dunia keamanan siber adalah SQLMap. SQLMap adalah sebuah open-source yang dirancang khusus untuk mendeteksi dan mengeksploitasi kerentanan SQL injection dalam aplikasi web [1]. Kerentanan SQL injection adalah salah satu kerentanan paling umum yang dieksploitasi oleh peretas untuk mengakses dan memanipulasi database situs web [2]. Dalam jurnal ini, penulis akan membahas cara penggunaan dasar SQLMap untuk mengeksploitasi kerentanan SQL injection.

Selain SQLMap, kita juga akan melihat alat lain yang penting dalam dunia keamanan siber, yaitu John The Ripper. John The Ripper adalah adalah sebuah alat uji penetrasi open source yang digunakan untuk memecahkan password pada sistem UNIX (termasuk Linux) dan menguji kekuatan password [3]. Dalam jurnal ini, kita akan membahas cara penggunaan dasar John The Ripper untuk melihat password pada sistem yang kita amankan.

Penting untuk dicatat bahwa kedua alat ini akan digunakan dalam lingkungan BlackArch Linux, sebuah distribusi Linux yang didedikasikan untuk keperluan pengujian keamanan siber. BlackArch Linux menyediakan beragam alat keamanan siber yang siap digunakan untuk pengujian dan pengevaluasian sistem.

Melalui pemahaman dasar tentang SQLMap dan John The Ripper, pembaca diharapkan dapat lebih siap menghadapi ancaman keamanan siber dan dapat mengidentifikasi kerentanan dalam aplikasi web. Dengan begitu, kita dapat mewujudkan dunia siber yang lebih aman dan terlindungi.

II. LANDASAN TEORI

A. SQL Injection

SQL injection adalah sebuah kerentanan keamanan siber yang memungkinkan peretas untuk memanipulasi perintah SQL yang dijalankan oleh aplikasi web [2]. Kerentanan ini terjadi ketika aplikasi web tidak memvalidasi input pengguna dengan benar sebelum menggunakannya dalam perintah SQL. Sebagai akibatnya, peretas dapat menyisipkan kode SQL berbahaya ke dalam input yang dimasukkan ke dalam aplikasi, yang kemudian dieksekusi oleh database.

SQL injection dapat memiliki dampak yang sangat serius, termasuk akses tidak sah ke data sensitif, perusakan database, atau bahkan pengendalian sistem secara keseluruhan. Serangan SQL injection dapat menyebabkan kerugian finansial, reputasi yang buruk, dan masalah hukum bagi organisasi yang terkena dampak.

 E-ISSN : 2722-0346

SQL injection bekerja dengan memanfaatkan kurangnya validasi input pengguna dalam aplikasi web. Peretas memasukkan input berbahaya yang mengandung perintah SQL ke dalam formulir atau parameter URL yang kemudian diolah oleh aplikasi. Perintah SQL berbahaya ini akan dijalankan oleh sistem database, yang berarti peretas dapat mengakses atau memanipulasi data dalam cara yang tidak diinginkan.

Beberapa teknik umum yang digunakan dalam serangan SQL injection, termasuk:

1. Union-based SQL Injection: Peretas memanfaatkan operasi SQL UNION untuk menggabungkan hasil dari beberapa perintah SQL dan mengambil data yang tidak seharusnya diakses.
2. Blind SQL Injection: Dalam serangan ini, peretas mencoba mengumpulkan informasi dengan mengajukan pertanyaan ya/tidak kepada database. Mereka mencari tahu informasi terkait struktur tabel atau data sensitif dengan mengamati respon yang diberikan oleh aplikasi.
3. Time-based Blind SQL Injection: Serangan ini memanfaatkan keterlambatan dalam eksekusi perintah SQL untuk mengidentifikasi informasi yang sensitif.

Dampak serangan SQL injection dapat beragam, tergantung pada tingkat kerentanannya dan sejauh mana peretas dapat mengelolanya. Dampak umum dari serangan SQL injection meliputi:

1. Akses tidak sah ke data sensitif, seperti informasi pengguna, informasi kartu kredit, atau data bisnis penting.
2. Kerusakan database, termasuk penghapusan atau perusakan data.
3. Pengambilalihan kontrol atas aplikasi atau sistem.
4. Kerugian finansial dan dampak reputasi yang dapat merugikan organisasi.

B. SQLMap

SQLMap adalah salah satu alat keamanan siber yang sangat berguna untuk mendeteksi dan mengeksploitasi kerentanan SQL injection dalam aplikasi web [1]. Alat ini dibangun menggunakan Python dan berfungsi dengan mengotomatisasi proses pengujian keamanan aplikasi web, terutama dalam hal SQL injection.

SQLMap secara otomatis mengidentifikasi kerentanan SQL injection dalam aplikasi web dengan menguji parameter input dan mengamati respon dari server. Hal ini akan menghemat waktu dan usaha dalam mengidentifikasi kerentanan. SQLMap mendukung berbagai jenis database, termasuk MySQL, PostgreSQL, Oracle, dan banyak lainnya, alat ini dapat menyesuaikan teknik serangan berdasarkan jenis database yang digunakan. SQLMap mampu mengidentifikasi tabel, kolom, dan data dalam database yang diserang, hal Ini berguna bagi peretas untuk mengambil informasi sensitif. Setelah kerentanan SQL injection terdeteksi, SQLMap dapat digunakan untuk mengeksploitasi kerentanan tersebut, termasuk mengambil data dari database, menambahkan, mengubah, atau menghapus data, dan bahkan menjalankan perintah pada server yangterpengaruh. SQLMap juga menyediakan berbagai opsi pemindaian yang dapat dikustomisasi, seperti penggunaan proxy, penggunaan cookie, dan pengujian login.

C. John The Ripper

John The Ripper, sering disebut sebagai John, adalah salah satu alat paling terkenal dan powerfull untuk membobol dan melihat password [3]. Alat ini dapat digunakan untuk menguji kekuatan password dalam berbagai skenario, dan membuat john menjadi alat primadona dalam keamanan siber. John The Ripper dirancang untuk melakukan serangan password, yang melibatkan mencoba berbagai kombinasi password untuk mengidentifikasi password yang benar. Alat ini dapat digunakan untuk menguji password pengguna, baik secara online (menghubungi server langsung) maupun offline (dengan menguji database password yang telah dicuri). John mendukung berbagai algoritma hashing password, termasuk DES, MD5, SHA-1, dan banyak lainnya. Alat ini juga dapat digunakan untuk menguji kekuatan password dalam berbagai format. John mendukung dua jenis serangan utama, yaitu serangan brute force (mencoba semua kemungkinan password) dan serangan dictionary (mencoba kata-kata dari daftar kata yang telah ada). John juga dapat digunakan untuk mengidentifikasi password yang lemah, yang dapat membantu administrator sistem dalam meningkatkan keamanan sistem mereka.

John The Ripper bekerja dengan mencoba berbagai kombinasi password untuk mengidentifikasi password yang benar. Alat ini menggunakan teknik-teknik seperti serangan brute force, serangan dictionary, dan serangan rule-based untuk mencoba password secara efisien.

III. METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini mengunakan metode penelitian Action Research [4]. Metode penelitian Action Research dipilih karena penelitian ini langsung berfokus pada objek penelitian yang merupakan percobaan seranganSQL injection pada situs web yang dipilih dan percobaan untuk melihat nilai password yang didapatkan. Penelitian akan dimulai dengan proses injeksi pada situs web yang menjadi target, lalu akan dilanjutkan dengan pengambilan data sensitif dari situs web tersebut seperti username dan password. Proses penelitian ini akan melibatkan langkah-langkah berikut:

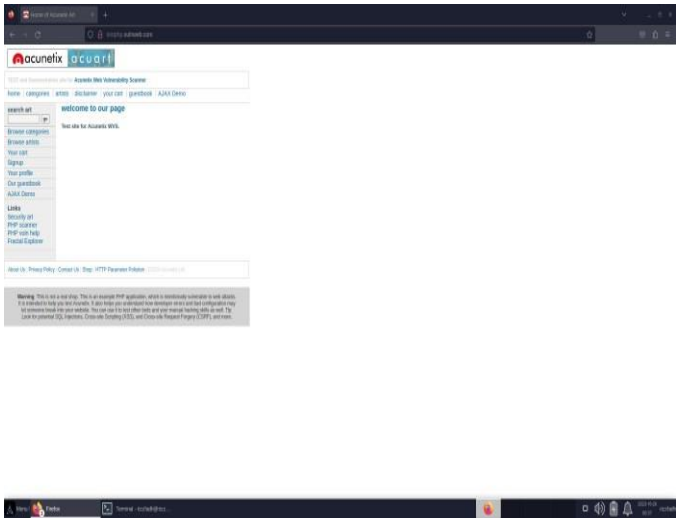
1. Mencari database yang terdapat pada situs web yang menjadi target.
2. Melakukan serangan SQL injection untuk mendapatkan data-data yang terdapat pada database tersebut.
3. Mencari serta mendapatkan data sensitif (username dan password) dari situs web tersebut.
4. Mencoba melihat nilai dari password yang terenkripsi.

IV. HASIL DAN PEMBAHASAN

A. Vulnerable Scanning

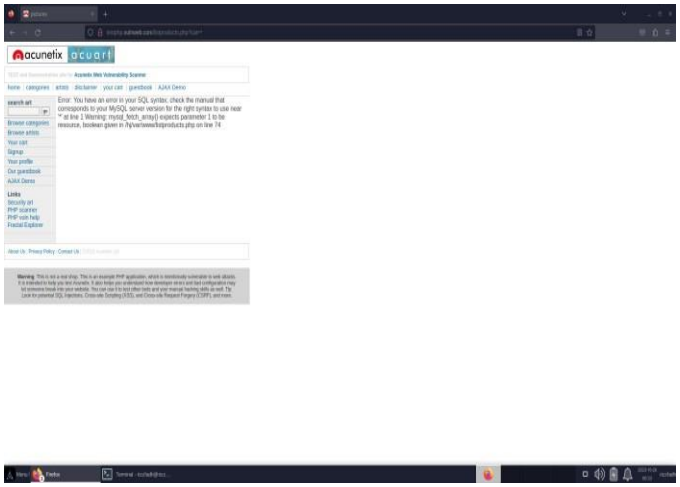
Langkah pertama yang akan dilakukan adalah mengecek apakah situs web yang menjadi target memiliki kerentanan terhadap SQL injection atau tidak. Pada penelitian ini, penulis menargetkan sebuah website khusus untuk testing kerentanan pada URL berikut http://testphp.vulnweb.com.

E-ISSN : 2722-0346



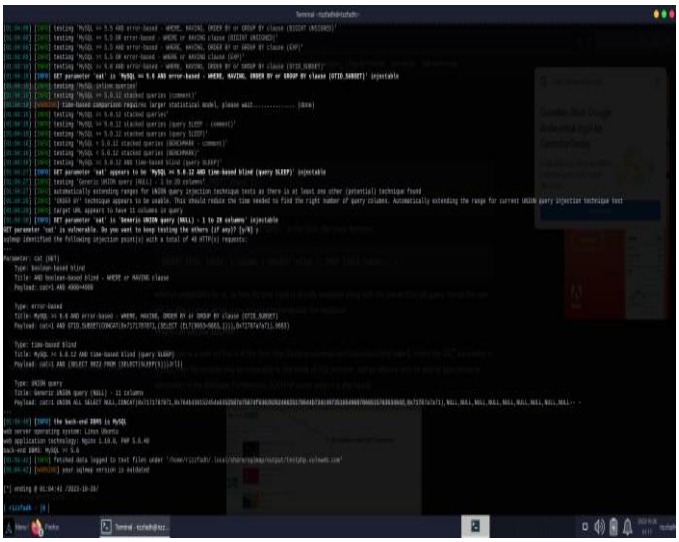
Gambar 1 Check Vulnarablity

Bila diperhatikan, kita akan memasukkan URL dalam bentuk GET request seperti berikut http://testphp.vulnweb.com/listproducts.php?cat=1 dimana parameter GET adalah cat=1. Cara sederhana untuk memeriksa apakah website yang menjadi target kita memiliki kerentanan atau tidak adalah dengan cara mengganti nilai dari parameter GET request menjadi asterisk (*), contoh http://testphp.vulnweb.com/listproducts.php?cat=* jika hasil dari GET request tersebut adalah error, maka dapat dikatakan website tersebut memiliki kerentanan.



Gambar 2 Check Kerentanan

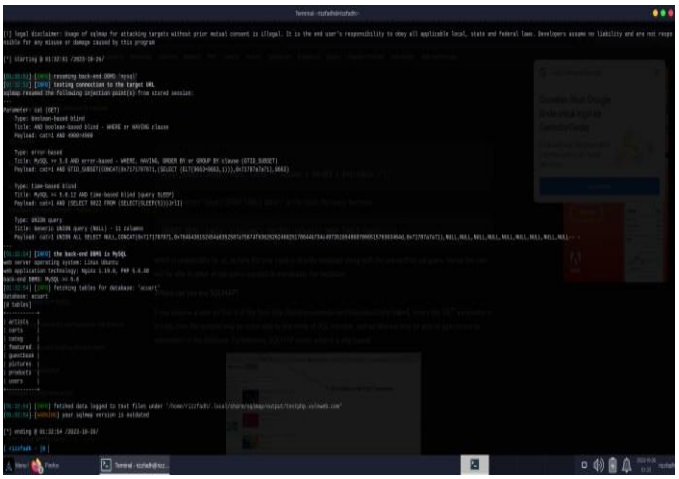
Selanjutnya kita akan mencoba melakukan pengecekan kerentanan melalui SQLMap dengan cara memasukkan perintah `sqlmap -u <target url>` contoh `sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1` lalu ketik “y” saja apabila ada pertanyaan yang muncul, maka akan terlihat hasil dari sqlmap yang berupa detail dari proses SQL injection beserta informasi dari server dan database website tersebut.



Gambar 3 Hasil Check SQL Injection

B. Database Scanning

Setelah mengetahui terdapatnya kerentanan pada website target, maka langkah selanjutnya kita akan mencari tahu nama dari database yang tersedia pada website tersebut dengan parameter `--dbs` contoh `sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs` penulis mendapatkan nama yaitu acuartdan information_schema. Dari sini kita bisa melangkah lebihlanjut dengan melihat nama-nama tables dari database yang kitamau menggunakan parameter `-D <nama database> --tables` contoh `sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables` dengan hasil berupa list nama-nama table pada database tersebut

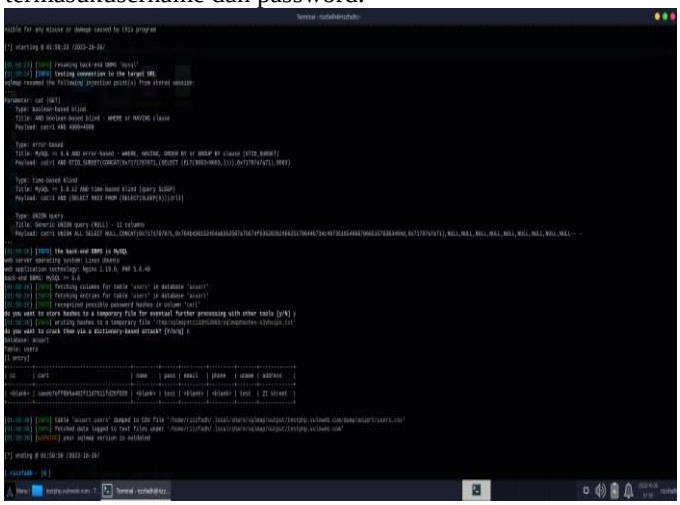


Gambar 4 Hasil Check Vulnarablity

Dari hasil tersebut kita bisa langsung mengambil data dari column table tersebut dengan parameter `-T <nama table> --dump` contoh `sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --dump` maka akan

E-ISSN : 2722-0346

terlihat hasil dari sqlmap yang berupa columns yang ada di tableusers. Dari sini kita sudah sukses memanfaatkan celah keamaanpada website tersebut, melakukan serangan SQL injection, danberhasil mendapatkan data sensitif pengguna termasukusername dan password.



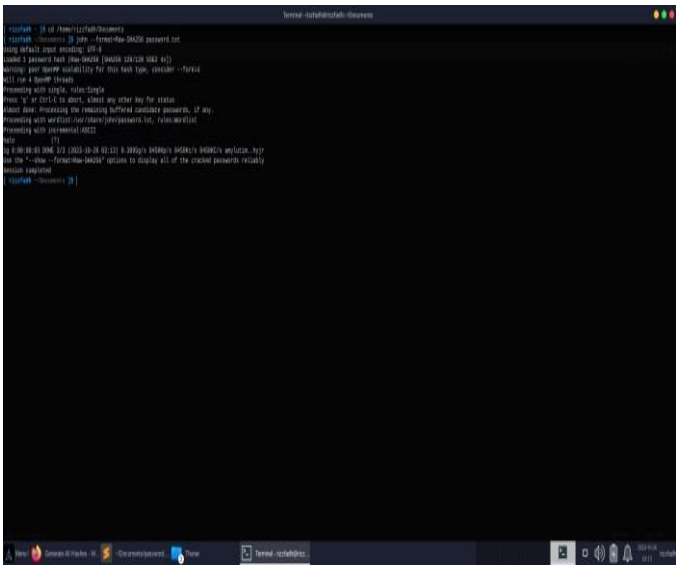
Gambar 5 Hasil Username dan Password

C. *Password cracking*

Tidak selamanya pengambilan data menggunakan SQLMap berjalan sesuai dengan yang kita mau, seringkali terdapat hambatan seperti password yang kita dapatkan masih dalam bentuk yang terenkripsi. Untuk mengatasi masalah tersebut, kita akan memanfaatkan alat yang bernama John The Ripper untuk melihat nilai asli dari password yang terenkripsi. Caranya yaitu kita buat file txt baru yang berisi nilai dari password tersebut

Gambar 6 File Text baru untuk Password

Lalu kita perlu menentukan tipe dari hash pada password tersebut untuk meningkatkan keberhasilan crack pada john, salah satu cara ialah dengan menggunakan online tool seperti pada website https://hashes.com/en/tools/hash_identifier. Setelah itu kita arahkan terminal ke direktori file password berada dan kita bisa mulai menggunakan john untuk mengcrack password tersebut dengan perintah `john --format=<tipe hash> <nama file password>` contoh `john --format=Raw-SHA256 password.txt` maka john akan mulai tugasnya, proses akan memakan waktu sesuai dengan panjang dan kerumitan password. Jika sudah selesai maka john akan menampilkan nilai dari password yang terenkripsi seperti gambar dibawah, penulis mendapatkan hasil enkripsi dari "a4e63bcacf6c172ad84f9f4523c8f1acaf33676fa76d3258c67b7e7bbf16d777" berupa "helo"



Gambar 7 Hasil Enkripsi Password

V. PENUTUP

A. *Kesimpulan*

SQLMap merupakan alat yang sangat berguna untuk mendeteksi dan mengeksploitasi kerentanan SQL injection dalam aplikasi web. Alat ini dapat secara otomatis mengidentifikasi kerentanan, mengakses data dalam database, dan menjalankan perintah pada server yang terpengaruh. Penggunaan SQLMap dapat membantu para pakar keamanan siber dalam mengidentifikasi potensi kerentanan dalam sistem mereka.

John The Ripper adalah alat yang powerfull untuk menguji kekuatan password dalam berbagai skenario. Alat ini mendukung berbagai algoritma hashing password dan dapat digunakan untuk mencoba kombinasi password yang berbeda. John The Ripper juga dapat membantu administrator sistem dalam meningkatkan keamanan sistem mereka dengan mengidentifikasi password yang lemah.

B. *Saran*

Para pakar keamanan siber, administrator sistem, dan pelajar bidang IT sebaiknya memahami dan menguasai penggunaan alat-alat seperti SQLMap dan John The Ripper. Pengetahuan ini akan membantu mereka dalam menghadapi ancaman keamanan siber dan meningkatkan keamanan sistem mereka. Penting untuk selalu melakukan pengujian keamanan secara berkala pada aplikasi web dan sistem untuk mengidentifikasi potensi kerentanan, terutama terhadap serangan SQL injection. Alat seperti SQLMap dapat digunakan dalam pengujian ini. Administrator sistem sebaiknya menggunakan alat seperti John The Ripper untuk menguji kekuatan password dalam sistem mereka dan secara berkala

mengidentifikasi password yang lemah yang perlu ditingkatkan.

Selalu perhatikan etika dalam penggunaan alat-alat keamanan siber. Penggunaan alat-alat ini harus selalu dilakukan dengan izin yang sah dan tidak boleh disalahgunakan untuk aktivitas ilegal.

VI. DAFTAR PUSTAKA

[1] B. Bin Halib, E. Budiman, dan H. J. Setyadi, "Teknik Hacking Web Server Dengan Sqlmap Di Kali Linux," *Jurnal Rekayasa Teknologi Informasi (JURTI)*, vol. 1, no. 1, hlm. 67, Jun 2017, doi: 10.30872/jurti.v1i1.642.

[2] S. Lika, R. D. P. Halim, dan I. Verdian, "ANALISA SERANGAN SQL INJEKSI MENGGUNAKAN SQLMAP," *POSITIF : Jurnal Sistem dan Teknologi Informasi*, vol. 4, no. 2, hlm. 88, Nov 2018, doi: 10.31961/positif.v4i2.610.

[3] I. H. D. Nugroho, K. Pebriawan, K. G. T. M. Jati, I. G. *C.* A. Diptha, I. M. E. Listartha, dan G. A. J. Saskara, "ANALISA EVALUASI KINERJA SOFTWARE PASSWORD ATTACKER PADA BERKAS FILE ZIP," *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, vol. 3, no. 1, hlm. 14–23, 2023.

[4] R. Davison, M. G. Martinsons, dan N. Kock, "Principles of canonical action research," *Information Systems Journal*, vol. 14, no. 1, hlm. 65–86, Jan 2004, doi: 10.1111/j.1365-2575.2004.00162.x.