IMPLEMENTASI SQL INJECTION DALAM PENETRATION TESTING UNTUK DETEKSI CELAH KEAMANAN WEB

Aristya Miftahun Nur Rizky, Muhlis Tahir, Tania Adela Sapitri, Muhammad Fajrul Islam
Pendidikan Informatika, Universitas Trunojoyo Madura
Jalan Raya Telang, PO.Box. 2 Kamal,Bangkalan - Madura
220631100044@student.trunojoyo.ac.id

ABSTRAK

Aplikasi web keamanan adalah aspek penting dalam menangani ancaman cyber yang semakin kompleks. Salah satu metode serangan yang sering digunakan adalah serangan injeksi SQL yang mengeksploitasi celah input pengguna untuk mengakses basis data secara ilegal. . Penelitian ini bertujuan untuk mengimplementasikan teknik SQL Injection dalam penetration testing untuk mendeteksi celah-celah keamanan pada situs legal testphp.vulnweb.com. Metodologi yang digunakan mencakup investigasi manual terhadap celah keamanan serta tinjauan otomatis menggunakan alat SQLMAP. Hasil pengujian menunjukkan bahwa situs target rentan terhadap SQL Injection, memungkinkan pengambilan data informasi sensitif seperti nama pengguna dan kata sandi. Penelitian ini menegaskan pentingnya validasi input dan penggunaan perintah SQL dengan parameter sangat penting untuk mencegah serangan serupa pada website. Dengan menerapkan penertation testing berbasis SQL Injection telah terbukti efektif dalam mendeteksi dan mengevaluasi kelemahan dalam sistem web.

Kata kunci : *SQL Injection, Penetration Testing, Keamanan Web, SQLMap, testphp.vulnweb.com*

1. PENDAHULUAN

Perkembangan teknologi informasi semakin pesat seiring dengan meningkatnya kebutuhan akan teknologi dan jaringan komputer[1]. Keamanan merupakan elemen yang sangat penting dalam mewujudkan stabilitas dan kenyamanan dalam berbagai aspek kehidupan. Di zaman modern yang serba digital ini, fokus keamanan bukan hanya pada perlindungan fisik, tetapi juga melibatkan pelindungan data dan informasi dari ancaman yang semakin kompleks. Salah satu aspek keamanan yang kini semakin mendesak adalah keamanan web. Dengan meningkatnya penggunaan situs web dan aplikasi berbasis internet, risiko serangan siber, pencurian data pengguna, serta eksploitasi celah keamanan dalam sistem web juga meningkat. Keamanan web mencakup serangkaian langkah pencegahan yang bertujuan untuk melindungi situs web dan data yang dikelola dari ancaman yang ditimbulkan oleh pihak-pihak yang tidak bertanggung jawab. Oleh sebab itu penting adanya keamanan website dimana nanti bisa diketahui celah yang dapat masuk ke dalam website tersebut[2].

Keamanan website menjadi hal yang sangat penting, mengingat website menyimpan berbagai data sensitif seperti informasi pribadi pengguna, data transaksi, dan berbagai data penting lainnya [3]. Dibalik banyaknya manfaat dan kelebihan penggunaan website tidak menutup kemungkinan terdapat kelemahan yang membahayakan[4]. Untuk melindungi data tersebut, pengujian keamanan merupakan langkah yang krusial. Salah satu metode yang umum digunakan dalam pengujian keamanan web adalah teknik serangan SQL Injection. SQL Injection merupakan sebuah aksi hacking yang dilakukan di web client dengan cara memodifikasi perintah SQL yang ada di memori web client [5]. Serangan ini terjadi ketika penyerang memanfaatkan celah keamanan pada input web untuk menyisipkan perintah SQL berbahaya kedalam sistem[6]. Teknik ini digemari oleh penyerang karena efektivitasnya dalam mengakses informasi sensitif secara ilegal. Berdasarkan laporan tahunan Acunetix, serangan SQL Injection masih tergolong sebagai salah satu kerentanan paling umum, dengan angka kejadian sekitar 8% pada tahun 2019 dan menurun menjadi 7% pada tahun 2020 [7].

SQL Injection umumnya terjadi akibat kelalaian pengembang dalam menerapkan pembatas atau filter terhadap karakter-karakter khusus (seperti &, ;, ', `, , ", |, *, ?, ~, <, >, ^, (,), [,], {, }, $, \n, \r) yang digunakan dalam sintaks SQL pada form input. Celah ini memungkinkan penyerang untuk memasukkan karakter tersebut disertai script query untuk menjalankan aksi berbahaya, seperti melewati autentikasi atau membaca data sensitif [8]. Salah satu tools yang umum digunakan untuk menguji kerentanan aplikasi terhadap SQL Injection adalah SQLMap, yaitu aplikasi sumber terbuka yang dapat secara otomatis mendeteksi dan mengeksploitasi celah SQL Injection dalam situs web. SQLMap bekerja dengan menyisipkan perintah query tertentu melalui parameter URL atau form input untuk menguji respons dari sistem basis data, sehingga dapat digunakan untuk menilai seberapa rentan sebuah situs web terhadap serangan SQL Injection [9].

Penelitian ini bertujuan untuk mengimplementasikan teknik SQL Injection dalam penetration testing untuk mendeteksi celah-celah keamanan pada aplikasi web *testphp.vulnweb.com.* Penelitian ini juga akan mengevaluasi efektivitas SQLMap sebagai alat untuk mengidentifikasi dan mengatasi potensi celah SQL Injection pada aplikasi web. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan

metodologi penetration testing yang lebih efektif dalam mengamankan aplikasi web.

2. TINJAUAN PUSTAKA

Injeksi SQL adalah salah satu teknologi serangan tertua, tetapi masih dikaitkan dengan aplikasi web di dunia keamanan. Teknik ini menggunakan celah dalam parameter input pengguna yang tidak disaring dengan benar sehingga penyerang dapat memasukkan perintah SQL berbahaya. menurut [10] SQL Injection merupakan teknik penyerangan yang ditunjukan ke webserver dengan menggunakan kode SQL untuk memanipulasi database. Laporan Acunetix juga menunjukkan bahwa meskipun ada penurunan, injeksi SQL adalah yang tertinggi pada daftar keselamatan umum, sebesar 7% pada tahun 2020. Untuk mendeteksi dan mengevaluasi kerentanan semacam ini, digunakan pendekatan penetration testing, yaitu metode pengujian keamanan dengan mensimulasikan serangan aktual pada sistem target secara legal dan terkontro. Salah satu alat yang efektif untuk praktik ini adalah SQLMAP. Ini adalah perangkat lunak open source yang dapat digunakan untuk mengotomatisasi proses pembelajaran dan eksploitasi injeksi SQL. Studi literatur ini menunjukkan bahwa metode dan alat ini menjadi lebih luas dalam berbagai studi kasus untuk meningkatkan keamanan sistem dan meningkatkan daya tahan digital.

SQLmap adalah alat open source yang mampu menganalisis, mendeteksi, dan melakukan eksploistasi (kode yang secara khusus dapat menyerang keamanan sistem komputer) pada kesalahan injecsi SQL[11]. SQLmap digunakan untuk membantu peneliti keamanan atau penyerang (peretas) dengan cepat dan efisien untuk menemukan dan mengekspoitasi kerentanan injeksi SQL[12]. Dalam pengujian penetration testing, SQLmap berguna untuk mensimulasikan serangan secara otomatis, sehingga mempermudah mengidentifikasi titik kelemahan situs web.

Penetration testing adalah salah satu cara untuk mensimulasikan metode yang mungkin akan digunakan oleh penyerang untuk menghindari atau menerobos mekanisme keamanan dan mendapatka akses secara ilegal ke suatu sistem[13]. Tujuan utama dalam penetration testing ini yaitu untuk mengidentifikasi selah keamanan sebelum dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab.

Keamanan website merupakan upaya untuk melindungi web dari peretasan iligal, perusakan data, dan pencurian tada yang dilakukan oleh pihak yang tidak bertaanggung jawab. Selain itu keamanan website juga mengelola hak akses pengguna dan perlindungan terhadap serangan berbahaya. Dengan adanya sistem keamanan website yang baik, resiko kerugian akibat serangan siber dapat meminimalkan maupun meningkatkan kepercayaan pengguna terhadap layanan website.

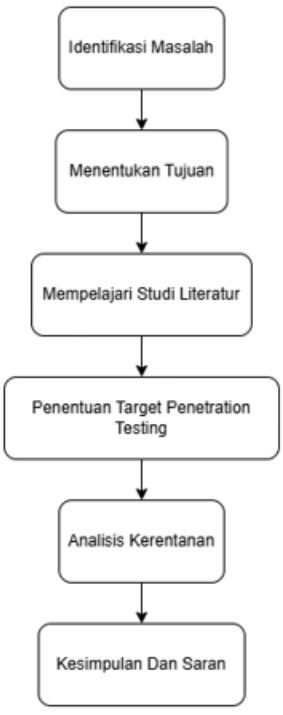
testphp.vulnweb.com merupakan situs uji coba yang di sediakan oleh Acunetix secara ilegal. Situs ini di rancang khusus untuk mengujian keamanan yang dimana *user* dapat melakukan uji coba penetration testing seperti SQL Injection dan serangan web lainnya tanpa melanggar hukum.

Penelitian ini menunjukan bahwa serangan SQL Injection tetap menjadi salah satu ancaman yang paling umum digunakan dalam keamanan aplikasi web. Melalui pengujian yang dilakukan menggunakan tools SQLMap, didapatkan bahwa data seperti username dan password dapat terdeteksi, selain itu ditemukan pada situs yang tampaknya tidak relevan terhadap SQLi [6].

Hal ini menunjukan bahwa metode penetration testing menggunakan serangan SQL Injection merupakan ancaman serius terhadap keamanan website. Pendekatan dan tools, seperti SQLMap, telah dikembangkan untuk mengidentifikasi dan mengatasi celah keamanan. Oleh karena itu, penting bagi pengembangan aplikasi untuk melakukan penetration agar mampu membangun sistem yang lebih aman.

3. METODE PENELITIAN

Metodologi penelitian ini disusun untuk memberikan pendekatan sistematis dalam mengeksplorasi dan menguji celah keamanan pada aplikasi web menggunakan teknik SQL Injection. Seluruh tahapan dirancang untuk mendukung proses penetrasi yang sah dan etis, dengan tujuan akhir mengidentifikasi kerentanan serta memberikan solusi yang relevan. Penelitian ini menggunakan situs uji dari *Acunetix Vulnerable Web Application (Vulnweb)* sebagai lingkungan pengujian yang legal dan aman untuk simulasi serangan.



Gambar 1. Metodelogi Penelitian

3.1. Fase Kajian Awal (Review Steps)

Penelitian dimulai dengan pengumpulan informasi umum mengenai ancaman keamanan pada aplikasi web, dengan fokus khusus pada teknik SQL Injection. Kajian awal ini mencakup analisis terhadap tren serangan terkini, serta penyusunan batasan agar penelitian tetap relevan pada ruang lingkup yang ditentukan. Masalah dirumuskan dari sudut pandang kerentanan sistem input data pada web modern, yang sering kali menjadi titik masuk utama eksploitasi.

3.2. Menentukan Tujuan

Langkah selanjutnya adalah merumuskan tujuan penelitian secara terarah. Fokus utama ditetapkan pada penerapan teknik SQL Injection untuk mengidentifikasi dan menguji kelemahan pada parameter input aplikasi web. Dengan tujuan ini, penelitian diharapkan mampu mengukur seberapa efektif teknik injeksi digunakan dalam konteks uji penetrasi, serta memetakan potensi risiko terhadap keamanan data dalam sistem web.

3.3. Mempelajari Studi Literatur

Untuk memperkuat fondasi metodologis, dilakukan kajian pustaka dari berbagai sumber terpercaya. Materi yang ditinjau mencakup jurnal keamanan siber, dokumentasi teknik SQL Injection, standar keamanan OWASP, serta praktik terbaik dalam pengujian penetrasi. Hasil studi literatur ini digunakan sebagai pedoman dalam menyusun skenario pengujian dan menginterpretasikan hasil eksploitasi terhadap sistem target.

3.4. Penentuan Target

Target pengujian ditentukan secara spesifik, yakni situs *testphp.vulnweb.com* milik Vulnweb, yang memang disediakan sebagai sarana uji coba keamanan aplikasi web. Situs ini dipilih karena menyediakan berbagai parameter input yang sengaja dirancang rentan, seperti kolom pencarian, ID produk dalam URL, dan formulir login. Penetapan target dilakukan secara legal untuk menjamin bahwa seluruh pengujian berada dalam batas etis dan tidak menimbulkan dampak negatif terhadap sistem pihak ketiga.

3.5. Analisis Kerentanan

Proses utama dalam penelitian ini adalah melakukan injeksi kode SQL pada parameter input yang tersedia di situs target. Peneliti mencoba berbagai jenis payload, seperti ' OR '1'='1 atau UNION SELECT, untuk mengamati respon sistem terhadap input tak terduga. Reaksi seperti munculnya error SQL, perubahan konten halaman, atau keberhasilan menampilkan data sensitif menjadi indikator adanya celah keamanan. Setiap hasil dicatat dan dianalisis untuk mengetahui sejauh mana injeksi berhasil menembus sistem.

3.6. Kesimpulan Dan Saran

Tahapan terakhir adalah menyusun simpulan dari hasil eksploitasi dan analisis terhadap respon sistem selama pengujian. Kesimpulan menjelaskan tingkat keberhasilan SQL Injection dalam mengakses atau memanipulasi data, sekaligus menunjukkan kelemahan spesifik pada sistem target. Peneliti juga memberikan rekomendasi teknis seperti implementasi *parameterized query*, *input validation*, dan *web application firewall (WAF)* untuk mencegah potensi serangan serupa di aplikasi web yang sesungguhnya.

4. HASIL DAN PEMBAHASAN

4.1. Target

Proses pengujian dimulai dengan mengakses halaman login dari situs uji legal testphp.vulnweb.com, yang disediakan untuk simulasi keamanan aplikasi web. Peneliti mencoba mengeksplorasi respon sistem terhadap input abnormal dengan menyisipkan karakter tunggal tanda kutip (') pada bagian akhir URL. Langkah ini bertujuan untuk mengamati apakah sistem memunculkan pesan kesalahan yang berkaitan dengan query SQL, yang menandakan adanya celah untuk serangan injeksi SQL. Teknik dasar ini sering digunakan untuk mengidentifikasi kerentanan pada parameter input.

4.2. Analisis Kerentanan

Setelah ditemukan respon yang mengindikasikan potensi celah, peneliti melanjutkan dengan menjalankan berbagai perintah SQL menggunakan terminal Linux. Tahapan ini bertujuan untuk memperoleh akses lebih dalam terhadap struktur database situs. Hasil eksploitasi awal memperlihatkan keberadaan tabel bernama acuart, yang berhasil ditampilkan sebagai bagian dari struktur database. Peneliti kemudian mengeksekusi perintah tambahan untuk menampilkan data pada tabel-tabel lainnya, termasuk tabel user, yang menyimpan informasi penting seperti akun pengguna dan kata sandi yang semestinya bersifat rahasia.

4.3. Hasil verivikasi SQLMap

Meskipun informasi login sebenarnya telah tersedia secara terbuka di situs target, peneliti tetap melibatkan penggunaan alat otomatis seperti SQLMap untuk melakukan verifikasi atas data yang ditemukan sebelumnya. Alat ini bekerja dengan menyuntikkan query SQL secara otomatis untuk mengekstrak informasi dari basis data. Hasil dari penggunaan SQLMap membuktikan bahwa kredensial yang ditampilkan memang benar dan dapat digunakan untuk mengakses sistem secara tidak sah, memperkuat bukti bahwa celah tersebut benar-benar bisa dieksploitasi oleh pihak yang tidak bertanggung jawab.

4.4. Penilaian Terhadap Tingkat Kerentanan

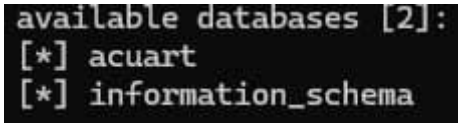
Dari keseluruhan proses yang dilakukan, diperoleh pemahaman bahwa situs testphp.vulnweb.com mengandung kelemahan

keamanan serius pada sisi input pengguna. Teknik SQL Injection terbukti efektif untuk menyusup ke dalam database dan memperoleh akses ke informasi penting tanpa otorisasi. Hasil ini menunjukkan pentingnya penerapan pengamanan pada parameter input, seperti validasi data dan penggunaan query terparameterisasi, guna mencegah penyalahgunaan yang serupa pada sistem produksi yang sesungguhnya.

a. Pengguna mencoba mengakses salah satu menu kategori yang tersedia di situs web. Setelah berhasil masuk ke halaman tersebut, pengguna menambahkan karakter tanda kutip satu (') di akhir URL untuk menguji apakah sistem rentan terhadap kesalahan SQL

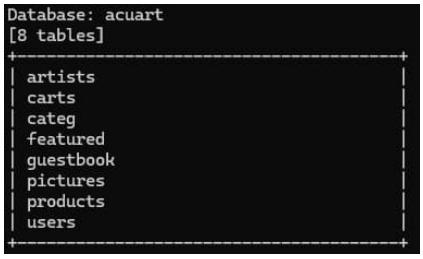
Gambar 2. Akses ke dalam situs web

b. Setelah itu, jalankan perintah *root@Monarch:/mnt/c/Users/arism# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs* di terminal Linux untuk mulai .Akses ini dilakukan dengan memanfaatkan celah keamanan pada tautan yang telah diketahui sebelumnya, sehingga muncul sebuah database.



Gambar 3. Akses Database

c. Kemudian menjalankan perintah SQL yang digunakan untuk menampilkan data yang terdapat di dalam tabel pada database dengan perintah *root@Monarch:/mnt/c/Users/arism# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 acuart --tables* , sehingga memunculkan data acuart.

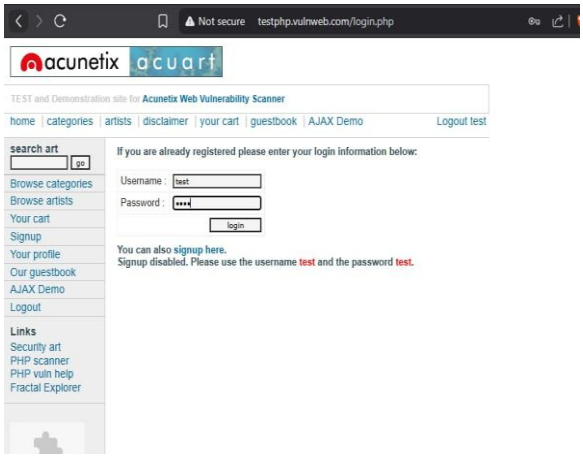


Gambar 4. Akses Table Database

d. Kemudian menjalankan perintah SQL yang digunakan untuk menampilkan tabel user dengan perintah *root@Monarch:/mnt/c/Users/arism# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 acuart users --dump*.

Gambar 5. Akses Table User

e. Meskipun informasi mengenai username dan password sebenarnya sudah tersedia langsung di situs webnya, kami tetap melakukan pengujian menggunakan SQLMap untuk memastikan kebenaran data tersebut. Hasil dari proses tersebut menunjukkan bahwa kredensial yang diberikan memang valid, sehingga membuktikan bahwa metode otomatis ini mampu memverifikasi informasi yang sudah ada dengan akurat.



Gambar 6. Mengakses Password

Gambar 7. Hasil Penetration Testing

5. KESIMPULAN DAN SARAN

Hasil dari penelitian ini menunjukan bahwa teknik SQL Injection sangat relevan dan berbahaya apabil atidak diantisipasi dengan baik oleh pengembang aplikasi. Hasil yang didapat dengan melakukan pengujian pada situs testphp.vulweb.com menunjukan terdapat parameter input yang tidak aman dapat dimanfaatkan untuk memeperoleh akses ilegal ke database, termasuk data sensitif seperti akun

pengguna. Denggan menggunakan SQLMap sebagai alat verifikasi membuktikan bahwa teknik otomatis dapat meningkatkan efisien dan akurasi dalam peroses penetration testing. Maka dari itu penting bagi pengembang aplikasi untuk menerapkan praktik keamanan terbaik seperti validasi input,penggunaan query terparameterisasi agar dapat mengurangi resiko eksploitasi.

DAFTAR PUSTAKA

[1] A. Riyanti, B. M. Rahmanto, D. R. Hardianto, R. D. A. Yuristiawan, and A. Setiawan, "Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 9, Jun. 2024, doi: 10.47134/pjise.v1i4.2623.

[2] M. A. Z. Risky and Y. Yuhandri, "Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS," *Jurnal Sistim Informasi dan Teknologi*, pp. 215–220, Aug. 2021, doi: 10.37034/jsisfotek.v3i4.68.

[3] T. Anugrah, "PENETRATION TESTING KEAMANAN WEBSITE STIE SAMARINDA MENGGUNAKAN TEKNIK SQL INJECTION DAN XSS," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 1, Jan. 2024, doi: 10.23960/jitet.v12i1.3882.

[4] M. Dian Khoiroh *et al.*, "Jurnal Sistem dan Teknologi Informasi (JSTI) PENETRATION TESTING UNTUK MENGUJI KERENTANAN SISTEM INFORMASI PEMERINTAH DAERAH." [Online]. Available: https://journalpedia.com/1/index.php/jsti

[5] A. Bastian, H. Sujadi, and L. Abror, "ANALISIS KEAMANAN APLIKASI DATA POKOK PENDIDIKAN (DAPODIK) MENGGUNAKAN PENETRATION TESTING DAN SQL INJECTION", [Online]. Available: http://www.dapodik.com/contoh.php?id

[6] M. Amirul Mu'min, Z. Alamin, and S. Ramadhan, "Uji Penetrasi Injeksi SQL terhadap Celah Keamanan Website XYZ menggunakan Tools SQLMap", doi: 10.34304/scientific.v1i2.330.

[7] L. A. Nugraha, I. A. Kautsar, and A. S. Fitrani, "SQL Injection: Analisis Efektivitas Uji Penetrasi dalam Aplikasi Web," *SMATIKA JURNAL*, vol. 14, no. 01, pp. 111–123, Jun. 2024, doi: 10.32664/smatika.v14i01.1224.

[8] R. Hermawan, "STRING (Satuan Tulisan Riset dan Inovasi Teknologi) TEKNIK UJI PENETRASI WEB SERVER MENGGUNAKAN SQL INJECTION DENGAN SQLMAP DI KALILINUX."

[9] R. P. Andrian, "Penetration Testing Database Menggunakan Metode SQL Injection Via SQLMap di Termux," *Indonesia Journal of Applied Informatics*, vol. 5, pp. 1–10, Nov. 2020.

[10] F. T. Anugrah *et al.*, "Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection."

[11] M. D. Purnomo and A. Chusyairi, "Sistematis : Jurnal Ilmiah Sistem Informasi Pengujian Keamanan Sistem Mengunakan Metode Penetration Testing di Website Diskominfostandi Kota Bekasi," *Oktober*, vol. 1, no. 1, 2024, doi: 10.69533.

[12] A. Dos Santos, G. S. Pereira, R. A. Syuhada, E. Malays, and S. Sakti, "Uji Coba Keamanan Database Website Menggunakan Python Dan Sqlmap Melalui Command Prompt Pada Sistem Operasi Windows", doi: 10.37817/tekinfo.v25i1.

[13] Y. Thurfah Afifa Rosaliah and B. Hananto, *Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx*. 2021.