https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

# Analisis Keamanan Informasi Bagi Pengguna Website Menggunakan Kalilinux Melalui Teknik SQL Injection

[1]Yehezkiel Natanael, [2]Rangga Felicia, [3]Essy Malays Sari Sakti
[123] Informatika, Universitas Persada Indonesia Y.A.I, Jakarta Pusat

E-mail: [1]natanaelyehezkiel3@gmail.com, [2]ranggafulfian@gmail.com,
[3]emalays67@gmail.com

## ABSTRAK

Keamanan informasi menjadi aspek penting di era digital, khususnya bagi pengguna website. Salah satu ancaman utamanya adalah serangan injeksi SQL, di mana penyerang dapat menyuntikkan kode SQL berbahaya melalui input pengguna untuk mengakses dan memanipulasi database. Penelitian ini bertujuan untuk menganalisis masalah keamanan informasi bagi pengguna situs web yang menggunakan Kali Linux untuk mendeteksi dan mengeksploitasi kerentanan injeksi SQL. Metode yang digunakan melibatkan eksplorasi alat yang tersedia di Kali Linux, seperti sqlmap, serta simulasi serangan di lingkungan web yang terkendali. Hasil studi menunjukkan pentingnya menerapkan langkah-langkah keamanan yang baik untuk mencegah serangan injeksi SQL dan melindungi data pengguna.

## *ABSTRACT*

*Information security is an important aspect in the digital era, especially for website users. One of the main threats is SQL injection attacks, where attackers can inject malicious SQL code via user input to access and manipulate the database. This research aims to analyze information security problems for website users who use Kali Linux to detect and exploit SQL injection vulnerabilities. The methods used involve exploring tools available in Kali Linux, such as sqlmap, as well as simulating attacks in a controlled web environment. The study results demonstrate the importance of implementing good security measures to prevent SQL injection attacks and protect user data..*

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

## 1. PENDAHULUAN

Pesatnya perkembangan teknologi informasi telah mempengaruhi kehidupan sehari-hari, termasuk sektor korporasi, dan dalam implementasinya banyak perusahaan yang menggunakan aplikasi web sebagai sarana pembelajaran online dan untuk keperluan lainnya.(Sari Sakti & Wagiyati.P, 2022)

Keamanan informasi bagi pengguna website menjadi pertimbangan penting. Ini karena situs web sering kali menyimpan data sensitif pengguna seperti informasi pribadi, detail keuangan, dan informasi lainnya. (Dahlan et al., 2015)

Perkembangan teknologi telah memunculkan banyak alat yang dapat digunakan untuk melakukan pengujian penetrasi dan pengujian keamanan. Kali Linux adalah distribusi Linux yang populer di kalangan pakar keamanan. Kali Linux menyediakan banyak alat yang dapat digunakan untuk mendeteksi dan mengeksploitasi kerentanan dalam aplikasi web, termasuk sqlmap, alat otomatisasi untuk mendeteksi dan mengeksploitasi injeksi SQL. Dengan menggunakan Kali Linux, peneliti dan pakar keamanan dapat mengidentifikasi kerentanan sebelum dieksploitasi oleh penyerang.

Selain itu, pertumbuhan Internet dan meningkatnya pengguna Internet juga meningkatkan risiko serangan. Seiring bertambahnya jumlah pengguna, semakin banyak data sensitif yang disimpan dan diproses oleh aplikasi web. Data ini mencakup informasi pribadi, keuangan, dan medis yang berharga. Oleh karena itu, sangat penting untuk melindungi data ini dari serangan cyber, termasuk injeksi SQL. Melalui penelitian ini, kami berharap dapat memberikan wawasan lebih jauh mengenai ancaman SQL injection dan langkah-langkah yang dapat dilakukan untuk mencegahnya.

Dalam beberapa tahun terakhir, serangan injeksi SQL terus meningkat frekuensi dan kompleksitasnya. Penyerang menjadi lebih canggih dalam menyembunyikan serangan mereka, sehingga membuat deteksi menjadi lebih sulit. Kasus-kasus besar seperti pelanggaran data di perusahaan besar seringkali disebabkan oleh kerentanan yang dapat dieksploitasi melalui injeksi SQL. Dampak finansial dan reputasi dari pelanggaran semacam itu bisa sangat parah, hal ini menunjukkan pentingnya pencegahan dan respons proaktif.

Teknik injeksi SQL juga telah berkembang dengan munculnya varian penyisipan SQL yang lebih kompleks seperti penyisipan SQL buta. , yang lebih sulit dideteksi karena tidak memberikan respons langsung yang jelas kepada penyerang. Penggunaan teknik ini menunjukkan bahwa situs web yang telah menerapkan keamanan berlapis pun masih bisa rentan jika tidak diterapkan dengan benar. Oleh karena itu, perlu dipahami dan diuji secara berkala untuk menjaga keamanan aplikasi web.

Selain dampak langsung dari pelanggaran data, serangan injeksi SQL juga dapat dijadikan titik awal untuk serangan yang lebih besar. Misalnya, setelah mendapatkan akses awal melalui injeksi SQL, penyerang dapat memasang pintu belakang atau meningkatkan hak istimewa untuk mengambil kendali seluruh sistem. Hal ini menunjukkan bahwa kerentanan injeksi SQL tidak hanya berbahaya dalam konteks pencurian data tetapi juga dapat membahayakan seluruh infrastruktur TI.

Salah satu ancaman keamanan informasi yang umum di situs web adalah SQL Injection (Dahlan et al., 2015). SQL Injection adalah teknik serangan yang

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

mengeksploitasi kerentanan dalam aplikasi web untuk memasukkan perintah SQL berbahaya. Perintah SQL ini dapat digunakan untuk mencuri data sensitif pengguna, merusak database, atau mengambil kendali situs web (Supartini & Parenreng, 2023).

Sadar akan potensi bahaya ini, penting bagi pengguna situs web untuk memahami dan mengambil tindakan keamanan yang tepat. Salah satu cara untuk meningkatkan keamanan website adalah dengan melakukan pengujian penetrasi menggunakan Kali Linux. Kali Linux adalah sistem operasi sumber terbuka yang biasa digunakan untuk pengujian keamanan informasi dan menyediakan banyak alat untuk mendeteksi dan mengeksploitasi kerentanan injeksi SQL.

Oleh karena itu, penting untuk melakukan analisis keamanan informasi pengguna situs web untuk mengetahui tingkat kerentanan pada situs web yang telah dibuat terhadap serangan SQL Injection dan untuk mengidentifikasi jenis data yang dapat dicuri menggunakan teknik ini.

Kali Linux adalah sistem operasi sumber terbuka populer yang digunakan untuk pengujian penetrasi dan analisis keamanan informasi (Dewa Made Julijati Putra et al., 2022).

Kali Linux menyediakan beberapa tools yang dapat digunakan untuk melakukan tes SQL Injection, antara lain SQLMap dan Burp Suite.

## 2. LANDASAN TEORI

### 2.1 Keamanan Informasi

Keamanan informasi adalah suatu proses yang bertujuan untuk melindungi informasi dari akses, penggunaan, pengungkapan, modifikasi, dan penghancuran yang tidak sah (Agustina et al., n.d.). Keamanan informasi penting untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi (Kelrey & Muzaki, 2019)..

Keamanan informasi melibatkan perlindungan data dari akses, modifikasi, atau penghancuran yang tidak sah. Aspek kunci keamanan informasi mencakup kerahasiaan, integritas, dan ketersediaan (CIA Triad). Kerahasiaan berarti bahwa data hanya dapat diakses oleh pihak yang berwenang, integritas memastikan bahwa data tidak diubah tanpa izin, dan ketersediaan memastikan bahwa data dapat diakses tersedia saat dibutuhkan. Dalam konteks aplikasi web, memastikan ketiga aspek tersebut memerlukan berbagai mekanisme keamanan seperti enkripsi, kontrol akses, dan pemantauan aktivitas. Tanpa perlindungan yang memadai, data sensitif dapat terekspos, diubah, atau dihapus, yang dapat menyebabkan kerugian finansial dan reputasi yang signifikan bagi organisasi.

### 2.2 SQL Injection

SQL Injection adalah Teknik serangan yang mengeksploitasi kerentanan keamanan dalam aplikasi web untuk memasukkan perintah SQL berbahaya. Perintah SQL ini dapat digunakan untuk mencuri data sensitive pengguna, merusak database, atau mengambil kendali situs web.

Kerentanan SQL Injection biasanya disebabkan oleh aplikasi web yang tidak memvalidasi input pengguna dengan benar (Al Fajar, 2020). Penyerang dapat mengekspliotasi kerentanan ini dengan memasukkan perintah SQL berbahaya ke dalam input pengguna, seperti formular login atau URL situs web (Haikal Muhammad et al., 2023).

### 2.3 Ancaman Keamanan Informasi

Ancaman keamanan informasi adalah suatu peristiwa atau tindakan yang dapat membahayakan keamanan informasi.

Ancaman keamanan informasi dapat diklasifikasikan menjadi beberapa jenis:

- Ancaman fisik: Ancaman fisik adalah ancaman yang dapat menyebabkan kerusakan fisik pada perangkat keras atau

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

perangkat lunak, seperti pencurian, kebakaran dan bencana alam.

- Ancaman logis: Ancaman logis adalah ancaman yang berpotensi merusak data atau perangkat lunak.
- Ancaman Manusia : Ancaman manusia adalah ancaman yang disebabkan oleh tindakan manusia baik disengaja maupun tidak disengaja, seperti: Kesalahan Pengguna, Akses Tidak Sah atau Sabotase.

## 2.4 Kalilinux

Kalilinux adalah sistem operasi open source yang biasa digunakan untuk pengujian penetrasi dan analisis keamanan informasi.

Salah satu fitur utama Kali Linux adalah kehadiran lebih dari 600 alat keamanan yang sudah diinstal sebelumnya dan tersedia secara default. Ini mencakup alat untuk melakukan analisis jaringan, eksploitasi kerentanan, analisis forensik, dan banyak lagi. Dengan mengakses alat-alat ini secara langsung, pengguna dapat dengan mudah melakukan berbagai jenis pengujian penetrasi tanpa harus menginstal dan mengkonfigurasi setiap alat secara manual.

Selain itu, Kali Linux juga dikenal karena kemampuannya mendukung banyak perangkat keras dan perangkat virtual yang berbeda. lingkungan, termasuk dukungan untuk mesin virtual seperti VMware dan VirtualBox. Hal ini memungkinkan pengguna untuk menginstal Kali Linux di berbagai platform dan menggunakannya di lingkungan yang sesuai dengan kebutuhan mereka. Kemampuan ini menjadikan Kali Linux pilihan populer bagi profesional keamanan yang bekerja dengan berbagai jenis infrastruktur TI. Kali Linux juga menawarkan banyak sumber tambahan seperti dokumentasi, tutorial, dan forum komunitas yang aktif. Hal ini memungkinkan pengguna untuk mempelajari lebih lanjut tentang berbagai alat dan teknik keamanan yang tersedia di Kali Linux, serta berbagi pengalaman dan pengetahuan mereka dengan profesional keamanan lainnya. Dengan komunitas yang aktif dan dukungan luas, Kali Linux terus berkembang dan menjadi salah satu distro Linux yang paling banyak digunakan di dunia keamanan informasi.

## 2.5 Keamanan Website

Keamanan website adalah proses yang bertujuan untuk melindungi website Anda dari berbagai ancaman keamanan seperti serangan hacker, malware, dan injeksi SQL.

Salah satu aspek keamanan situs web yang paling rentan adalah kerentanan terhadap serangan injeksi SQL. Serangan ini dapat memungkinkan penyerang mengakses atau mengubah data yang disimpan dalam database yang terhubung ke situs web. Oleh karena itu, informasi sensitif seperti informasi pengguna, informasi kartu kredit, atau informasi rahasia bisnis dapat diretas dan disalahgunakan oleh penyerang. Selain itu, serangan injeksi SQL juga dapat digunakan sebagai titik awal serangan yang lebih besar terhadap infrastruktur TI perusahaan.

Untuk mengurangi risiko serangan injeksi SQL dan melindungi keamanan Situs Web, pengembang web harus menerapkan keamanan yang baik praktik. dari awal siklus pengembangan. Langkah-langkah ini termasuk menggunakan kueri berparameter atau pernyataan yang disiapkan untuk menghindari injeksi SQL, memvalidasi dan memfilter input pengguna, dan menerapkan firewall aplikasi web (WAF) untuk memantau dan memfilter lalu lintas HTTP yang masuk. Selain itu, pengujian kerentanan rutin dan pemindaian keamanan berkala juga penting untuk

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

mendeteksi dan memperbaiki kerentanan sebelum penyerang dapat mengeksploitasinya.

Tidak hanya memperhatikan aspek teknis, kesadaran dan edukasi Keamanan Cyber juga penting. Melibatkan seluruh pemangku kepentingan dalam upaya menjaga keamanan situs. Pelatihan rutin bagi pengembang web dan staf TI tentang praktik keamanan yang baik serta peningkatan kesadaran tentang jenis serangan yang dapat terjadi dan cara mengatasinya dapat membantu mencegah serangan siber dan keamanan situs web. Melalui pendekatan komprehensif yang melibatkan teknologi, proses, dan manusia, keamanan situs web dapat ditingkatkan dan risiko serangan dunia maya dapat diminimalkan.

Keamanan website penting untuk melindungi kerahasiaan data pengguna, integritas website, dan reputasi pemilik website.

### 2.6 Keamanan Database

Keamanan basis data merupakan aspek penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data yang disimpan dalam sistem informasi. Basis data sering kali menjadi target utama penyerang karena berisi informasi sensitif seperti informasi pengguna, informasi keuangan, dan rahasia dagang. Ancaman keamanan basis data mencakup serangan injeksi SQL, eksfiltrasi data, dan serangan malware yang bertujuan untuk merusak atau mencuri informasi. Oleh karena itu, perlindungan basis data sangat penting untuk melindungi aset informasi organisasi.

Salah satu langkah penting dalam menjaga keamanan basis data adalah menerapkan langkah-langkah kontrol akses yang ketat. Hal ini melibatkan pengaturan izin akses yang sesuai untuk pengguna dan peran tertentu, serta penggunaan autentikasi yang kuat seperti penggunaan kata sandi yang rumit dan beberapa mekanisme autentikasi. Selain itu, enkripsi data pada tingkat penyimpanan dan transmisi dapat membantu melindungi data sensitif dari akses tidak sah, bahkan jika database diserang.

Pengawasan Pemantauan dan audit aktivitas database juga penting untuk mendeteksi dan merespons ancaman keamanan dengan cepat. Dengan menganalisis log aktivitas database, organisasi dapat mengidentifikasi pola aneh atau aktivitas mencurigakan yang mungkin mengindikasikan serangan atau penyalahgunaan. Memantau aktivitas pengguna juga dapat membantu mendeteksi perilaku tidak biasa atau upaya akses tidak sah ke data sensitif.

Selain itu, manajemen dan pemulihan bencana merupakan bagian penting dari 'strategi keamanan database'. Organisasi harus memiliki rencana darurat yang jelas dan teruji untuk menangani insiden keamanan seperti pencurian data atau gangguan sistem. Hal ini mencakup prosedur pemulihan data secara rutin, cadangan yang disimpan di lokasi yang aman, serta pembaruan sistem dan perangkat lunak secara berkala untuk mengatasi kerentanan baru yang mungkin timbul. Dengan mengambil langkah-langkah ini, organisasi dapat meningkatkan keamanan basis data dan melindungi informasi sensitif dari ancaman dunia maya yang semakin kompleks dan parah.

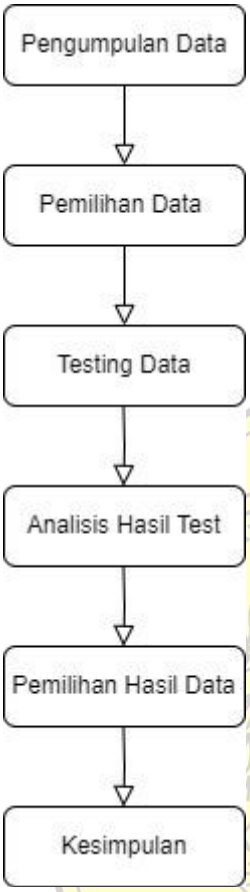
## 3. METODOLOGI

Penelitian ini menggunakan metode penelitian kuantitatif dengan pendekatan eksperimen. Data dikumpulkan dengan menjalankan tes SQL Injection di situs web yang rentan terhadap serangan SQL Injection. Alat untuk melakukan SQL Injection adalah SQLMap (Celvine Adi Putra et al., 2023).

Data yang dikumpulkan dianalisis untuk mengetahui Tingkat kerentanan website terhadap serangan SQL Injection dan untuk mengidentifikasi jenis data

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

yang dapat dicuri menggunakan Teknik SQL Injection.




Gambar 1. Proses Analisis Data

### 3.1 Pengumpulan Data

Langkah ini merupakan fase permulaan dalam pelaksanaan penelitian, dimana peneliti melakukan pengumpulan data batasan permasalahan yang diinvestigasi untuk memberikan arah yang jelas. Pengumpulan data juga penting untuk dilakukan karena peneliti dapat mengetahui data apa saja yang ada dalam suatu website.

### 3.2 Pemilihan Data

Pada tahapan selanjutnya peneliti melakukan pemilihan data untuk menentukan data yang akan dilakukan pengetesan lanjut. Data-data yang dipilih juga akan menjadi pertimbangan selanjutnya jika data yang pertama gagal dilakukan pengetesan uji SQL Injection.

### 3.3 Testing Data

Pada tahapan ini peneliti akan melakukan testing data. Setiap data yang terkumpul akan diuji kerentanannya supaya dapat mengetahui website tersebut aman atau tidaknya dari serangan-serangan hacker. Testing data juga sangatlah penting untuk bisa menguji keamanan dalam suatu website.

### 3.4 Analisis Hasil Test

Pada tahapan ini, peneliti menganalisis hasil test yang sudah dilakukan testing data untuk bisa mengetahui data-data yang telah berhasil dicuri atau didapatkan.

### 3.5 Pemilihan Hasil Data

Pada tahapan ini, peneliti menampilkan hasil data yang sudah didapatkan. Hasil data ini merupakan keberhasilan peneliti dalam melakukan pengujian website untuk mengetahui apakah website tersebut memiliki kertenanan atau tidak sehingga data pengguna dapat dicuri.

### 3.6 Kesimpulan

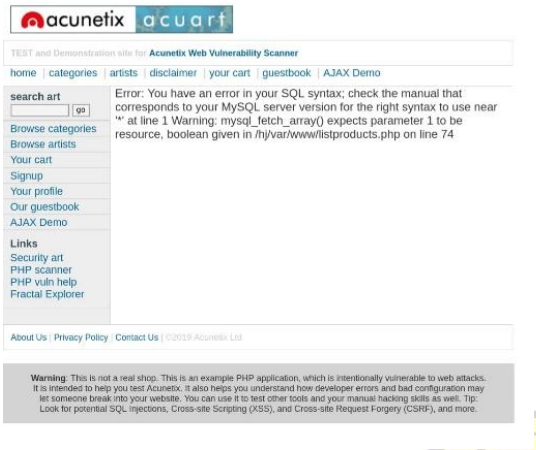
Pada tahapan ini, peneliti akan merangkum temuan-temuan utama yang ditemukan selama penelitian. Ini semua mencakup jawaban terhadap landasan teori yang telah ditetapkan sebelumnya.

## 4. HASIL DAN PEMBAHASAN

### 3.7 Pembahasan

Dalam pengujian kali ini untuk melalukan uji SQL Injection, peneliti menyiapkan perangkat elektronik(Laptop) untuk menjalankan tools SQL Injection di Kalilinux. Website yang dipilih adalah testphp.vulnweb.com.

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

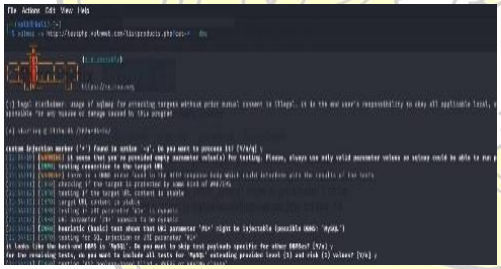



Gambar1. Website yang akan diserang

## 3.8 Teknik perancangan

### 4.1.1 Vulnerable Scanning

pada SQLMAP memasukkan URL yang akan diserang dan mencoba masuk kedalam database website

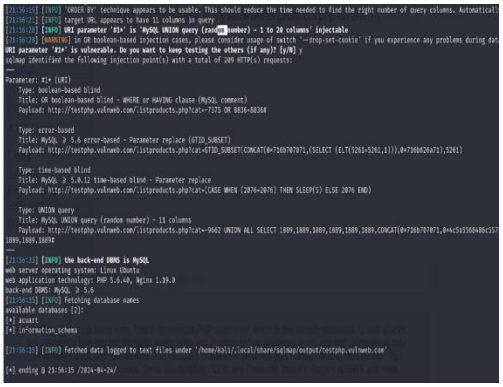


Gambar2. Melakukan vulnerable Scanning

Hasil menunjukan bahwa situs website sangat rentan dan berhasil masuk ke dalam database web.

### 4.1.2 Database Scanning

Pada database yang didapat dari vurnable scanning. Maka selanjutnya, melakukan pengecekan table terhadap setiap informasi database yang tersedia.



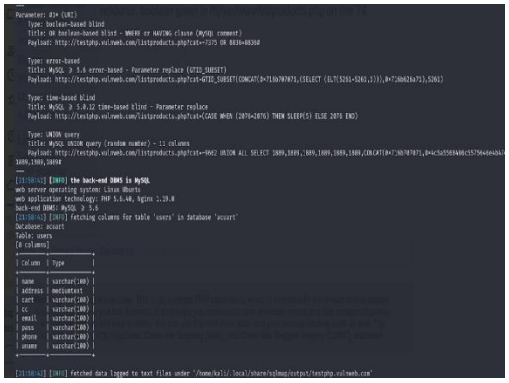
Gambar3. Memilih database yang akan discanning

Pada gambar3 peneliti mendapatkan 2 database yang didapatkan, lalu peneliti melakukan pemilihan terhadap database yang akan discanning. Peneliti memilih database nomor 1 yaitu ‘acuart’. Untuk melihat isi dari database ‘acuart’ tersebut.

Gambar4. Database acuart

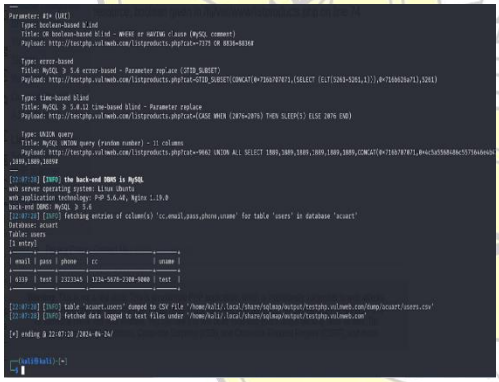
Pada gambar4, terdapat database dari ‘acuart’ yang berhasil diketahui. peneliti mendapatkan 8 tabel dalam database acuart. Dan didalam database acuart peneliti memilih users untuk melihat table SQL dan pengecekan email, username, password.

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1



Gambar5. Table SQL

Pada gambar5 merupakan hasil table SQL dari ‘users’. Dalam hasil pengujian testing ini Peneliti menemukan terdapat 8 kolom table SQL. Dan saat program melakukan proses, peneliti menargetkan username dan password. Tujuannya adalah untuk mengetahui username login dan password login beserta email pada saat sign-up.



Gambar6. Hasil pembongkaran

Pada gambar6, peneliti berhasil menemukan beberapa data yang berhasil dicuri yaitu email, username, dan password. Dan ini merupakan hasil table SQL dari users terdapat 8 kolom table SQL. Data pengguna dalam website berhasil dicuri dan didapatkan sehingga dapat mengetahui data pengguna. Hasil ini juga merupakan keberhasilan peneliti dalam melakukan teknil SQL Injection.

## 5. KESIMPULAN

penelitian ini menunjukkan bahwa teknik injeksi SQL masih menjadi ancaman serius terhadap keamanan informasi pengguna situs web. Dengan alat yang tersedia di Kali Linux, peneliti dapat dengan mudah mendeteksi dan mengeksploitasi kerentanan injeksi SQL. Hal ini menunjukkan bahwa banyak aplikasi web tetap rentan terhadap serangan ini, karena kelemahan dalam kode aplikasi atau kurangnya langkah-langkah keamanan yang memadai. Selama pengujian, sqlmap terbukti efektif dalam mengidentifikasi kerentanan dan mengeksploitasi data database sensitif.

Pentingnya implementasi tidak dapat diabaikan. Validasi dan sanitasi input adalah langkah pertama yang penting dalam mencegah serangan injeksi SQL. Pengembang harus memastikan bahwa semua masukan pengguna divalidasi dan dibersihkan dengan benar untuk menghapus karakter atau perintah berbahaya. Selain itu, penggunaan kueri berparameter dan pernyataan yang disiapkan akan menjadi norma dalam pengembangan aplikasi web untuk memastikan bahwa kueri SQL tidak dapat diubah oleh informasi yang dimasukkan.

Selain langkah-langkah teknis, penerapan alat pengujian penetrasi secara teratur seperti sqlmap Cyclical Web Application Development dapat membantu mendeteksi kerentanan terlebih dahulu ketika aplikasi diterapkan di lingkungan produksi. Penggunaan alat ini memungkinkan pengembang dan pakar keamanan mengidentifikasi potensi kelemahan dan memperbaikinya sebelum penyerang dapat mengeksploitasinya. Oleh karena itu, pengujian keamanan proaktif dapat meminimalkan risiko dan meningkatkan ketahanan aplikasi web terhadap serangan.

Kesadaran dan pendidikan juga berperan penting dalam meningkatkan keamanan informasi. Banyak serangan

P-ISSN: 1411-3635
E-ISSN: 2962-5645

injeksi SQL berhasil karena pengembang dan staf TI tidak terlatih dengan baik dalam aspek keamanan. Program pelatihan rutin dan kesadaran akan teknik serangan dan praktik terbaik keamanan sangat penting untuk memastikan bahwa semua pihak yang terlibat dalam pengembangan aplikasi dan pemeliharaan web memahami risiko dan cara memitigasinya. Hal ini mencakup pelatihan tentang cara menggunakan alat pengujian penetrasi dan memahami hasilnya untuk meningkatkan keamanan aplikasi.

Singkatnya, menjaga keamanan informasi dalam aplikasi web memerlukan pendekatan komprehensif yang mencakup tindakan teknis, penggunaan alat pengujian penetrasi, dan tindakan yang sesuai. dan langkah-langkah pendidikan yang berkelanjutan. Serangan injeksi SQL dapat menimbulkan konsekuensi serius, namun dengan penerapan langkah-langkah keamanan yang tepat dan alat yang efektif seperti Kali Linux, risiko ini dapat dikelola dan diminimalkan. Penelitian ini diharapkan dapat memberikan informasi dan panduan praktis kepada pengembang web dan profesional keamanan dalam menangani ancaman injeksi SQL, serta menyoroti pentingnya kesadaran dan pendidikan dalam menjaga keamanan informasi.Keamanan informasi website adalah tanggung jawab bersama antara pengembang dan pengguna website. Peningkatan kesadaran dan upaya proaktif dari kedua pihak sangatlah penting untuk melindungi data pengguna dan menjaga privasi mereka di dunia digital.

Analisis keamanan informasi bagi pengguna website menggunakan Kali Linux melalui teknik SQL Injection penting dilakukan untuk mengetahui tingkat kerentanan website terhadap serangan SQL Injection dan untuk mengidentifikasi jenis data yang dapat dicuri dengan menggunakan teknik SQL Injection.

Hasil penelitian ini dapat digunakan untuk meningkatkan keamanan website dan untuk melindungi data pengguna dari akses yang tidak sah

## 6. UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada semua pihak yang telah membantu dalam penyusunan jurnal ini. Semoga informasi ini dapat bermanfaat bagi pengembang dan pengguna website untuk meningkatkan keamanan informasi website dan melindungi data pengguna.

## DAFTAR PUSTAKA

Agustina, D., Nazzilla Pramadista, F., & Fara Regyna, T. (n.d.). *"SISTEM MANAJEMEN KEAMANAN INFORMASI."*

Al Fajar, F. (2020). ANALISIS KEAMANAN APLIKASI WEB PRODI TEKNIK INFORMATIKA UIKA MENGGUNAKAN ACUNETIX WEB VULNERABILITY. *INOVA-TIF*, *3*(2). https://doi.org/10.32832/inova-tif.v3i2.4127

Celvine Adi Putra, Rianda Pratama, & Tata Sutabri. (2023). ANALISIS MANFAAT MACHINE LEARNING PADA NEXT-GENERATION FIREWALL SOPHOS XG 330 DALAM MENGATASI SERANGAN SQL INJECTION. *Jurnal Manajemen Informatika Dan Sistem Informasi*, *6*(2). https://doi.org/10.36595/misi.v6i2.886

Dahlan, M., Latubessy, A., Nurkamid, M., & Hidayah Anggraini, L. (2015). *Pengujian Dan Analisa Keamanan Website Terhadap Serangan SQL Injection (Studi Kasus : Website UMK)* (Vol. 7).

Dewa Made Julijati Putra, I Nyoman Namo Yoga Anantra, Putu Adhitya

kusuma, Putu Damar Jagat Pratama, Gede Arna Jude Saskara, & I Made Edy Listartha. (2022). ANALISIS PERBANDINGAN SERANGAN HYDRA, MEDUSA DAN NCRACK PADA PASSWORD ATTACK. *Jurnal Informatika Teknologi Dan Sains*, *4*(4). https://doi.org/10.51401/jinteks.v4i4.2192

Haikal Muhammad, H., Id Hadiana, A., Ashaury Informatika, H., Jenderal Achmad Yani Cimahi Jl Terusan Jend Sudirman, U., Cimahi Sel, K., Cimahi, K., & Barat, J. (2023). PENGAMANAN APLIKASI WEB DARI SERANGAN SQL INJECTION DAN CROSS SITE SCRIPTING MENGGUNAKAN WEB APPLICATION FIREWALL. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Issue 5).

Kelrey, A. R., & Muzaki, A. (2019). PENGARUH ETHICAL HACKING BAGI KEAMANAN DATA PERUSAHAAN. *Cyber Security Dan Forensik Digital*, *2*(2). https://doi.org/10.14421/csecurity.2019.2.2.1625

Sari Sakti, E. M., & Wagiyati.P, S. (2022). Pengembangan Sistem Informasi Persediaan Barang Berbasis Android ( Kasus Cv Berkah Ananda ). *Ikraith-Informatika*, *7*(1). https://doi.org/10.37817/ikraith-informatika.v7i1.2232

Supartini, R., & Parenreng, J. M. (2023). Deteksi Serangan SQL Injection pada Website dengan Menggunakan Metode Reguler Expression. *Progressive Information, Security, Computer, and Embedded System*, *1*(2). https://doi.org/10.61255/pisces.v1i2.101

.