ANALISIS KEAMANAN SISTEM MENGGUNAKAN METODE *PENETRATION TESTING* PADA *WEBSITE*

Chincio Putri Simanjuntak [1*], Uskha Dyah Arsanti[2], Landung Sudarmana[3]
[123]Universitas Proklamasi 45
[123]Yogyakarta-Indonesia

Email: [1]chincioputri0354@gmail.com, [2]dyahuskha@gmail.com,
[3]willerkasani@gmail.com

Abstract

This research analyzes the security of the website using the Penetration Testing method. The purpose of the research is to evaluate the effectiveness of Penetration Testing in assessing the security system of the website, identify vulnerabilities, and analyze the risks of successfully exploited vulnerabilities. The results show that the vulnerabilities found include Blind SQL Injection and vulnerabilities in the HTTP Trace method, which have the potential to be exploited by attackers to access sensitive information, data manipulation, and unauthorized access. The analysis showed a distribution of vulnerabilities by severity, with Informational (14%), Low (43%), Medium (29%), and High (14%) categories. In addition, the Acunetix scan identified one critical vulnerability, namely SQL Injection, with a confidence level of 100%, which can open access to the database and reveal sensitive information such as usernames and passwords.

Keywords: *Acunetix, Website Security, Penetration Testing, SQL Injection.*

Abstraksi

Penelitian ini menganalisis keamanan Website menggunakan metode *Penetration Testing*. Tujuan penelitian adalah untuk mengevaluasi efektivitas *Penetration Testing* dalam menilai sistem keamanan website, mengidentifikasi kerentanan, serta menganalisis risiko dari kerentanan yang berhasil dieksploitasi. Hasil penelitian menunjukkan bahwa kerentanan yang ditemukan mencakup Blind *SQL Injection* dan kerentanan pada metode *HTTP Trace*, yang memiliki potensi dieksploitasi oleh penyerang untuk mengakses informasi sensitif, manipulasi data, dan akses tidak sah. Analisis menunjukkan distribusi kerentanan berdasarkan tingkat keparahan, dengan kategori *Informational* (14%), *Low* (43%), *Medium* (29%), dan *High* (14%). Selain itu, pemindaian Acunetix mengidentifikasi satu kerentanan kritis, yaitu *SQL Injection*, dengan tingkat keyakinan 100%, yang dapat membuka akses ke database dan mengungkapkan informasi sensitif seperti *username* dan *password.*

Kata Kunci: *Acunetix, Keamanan Website, Penetration Testing, SQL Injection.*

1. PENDAHULUAN

Keamanan sistem informasi adalah aspek fundamental dalam menjaga integritas, kerahasiaan, dan ketersediaan data di era digital yang terus berkembang. Keamanan

informasi menjadi hal yang sangat penting karena bertujuan untuk melindungi data digital dari ancaman yang dapat merusak atau mengakses informasi sensitif tanpa izin. Keamanan ini juga mencakup perlindungan terhadap sistem yang menyimpan dan mengelola data yang memiliki nilai tinggi, terutama bagi instansi pemerintah yang berperan dalam memberikan pelayanan publik. Menurut beberapa penelitian, ancaman terhadap sistem informasi terus berkembang seiring kemajuan teknologi, memunculkan serangan siber yang semakin canggih dan terstruktur, seperti injeksi SQL, XSS, dan akses tidak sah, yang berpotensi merusak integritas dan kerahasiaan data [1][2].

Salah satu aspek yang penting untuk diamati adalah keamanan website, yang sering menjadi target serangan karena perannya sebagai sumber informasi yang terbuka untuk umum. Website pemerintah, sebagai media informasi dan komunikasi antar lembaga, rentan terhadap serangan yang dapat mengeksploitasi celah-celah di dalam sistem, seperti kerentanannya terhadap SQL injection atau akses tidak sah. Hal ini mengharuskan adanya pengujian dan evaluasi berkala terhadap keamanan website untuk mengidentifikasi dan mengurangi risiko yang mungkin terjadi, sehingga dapat menjaga kepercayaan publik [3]. Salah satu metode yang umum digunakan dalam pengujian keamanan adalah Penetration Testing, yaitu suatu teknik untuk mengeksploitasi dan menemukan kerentanannya sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab [4].

Penelitian ini bertujuan untuk mengevaluasi keamanan website yang digunakan oleh lembaga pemerintah dalam mengelola dan menyediakan data ekonomi kepada publik. Website tersebut sangat penting bagi kebijakan ekonomi dan pelayanan publik, sehingga perlu dilindungi dari potensi ancaman siber. Dengan menggunakan metode Penetration Testing, penelitian ini berfokus pada identifikasi potensi kerentanan yang ada dalam sistem dan memberikan rekomendasi untuk meningkatkan perlindungannya. Diharapkan hasil penelitian ini dapat memberikan kontribusi dalam meningkatkan sistem keamanan website pemerintah serta memperkuat kepercayaan publik terhadap layanan digital yang disediakan.

2. TINJAUAN PUSTAKA

Pada penelitian pertama yang menganalisis keamanan *Website* dengan metode *Penetration Testing* dan *Framework* ISSAF. Pada penelitian ini tentang "Analisis Keamanan Web Server *Open* Journal System (OJS) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)". Fokus penelitian adalah web server OJS Universitas Lancang Kuning, menggunakan *Framework* ISSAF. Hasilnya menunjukkan bahwa sistem OJS tersebut tergolong aman, namun disarankan untuk menerapkan sistem monitoring seperti *Firewall* untuk meningkatkan keamanan lebih lanjut [5].

Penelitian kedua yang mengevaluasi keamanan *Website* Lembaga X menggunakan *framework* ISSAF. Hasilnya mengungkapkan celah keamanan serius seperti *SQL Injection* dan XSS. Rekomendasi yang diajukan adalah melakukan validasi pada level php untuk mencegah serangan yang merugikan. Evaluasi memberikan wawasan penting tentang

pentingnya memperkuat keamanan *Website*, terutama dalam konteks serangan siber yang semakin canggih dan berbahaya [6].

Penelitian ketiga yang berjudul " Penetration Testing Information System Security AssessmentFramework (ISSAF)" bahwa penelitian ini berfokus pada penerapan empat dari sembilan tahap dalam Framework ISSAF dengan menggunakan strategi blackbox, di mana penguji hanya diberikan akses pada domain website target. Penelitian ini dilatarbelakangi oleh permasalahan yang sering terjadi pada salah satu sistem informasi Universitas Muhammadiyah Riau (UMRI), khususnya pada website *https://kekampus.umri.ac.id/*. Hasil penelitian mengidentifikasi beberapa kerentanan pada website tersebut, termasuk serangan *SQL injection*, *cross-site scripting (XSS)*, dan kelemahan pada konfigurasi *cookie secure flag*[7].

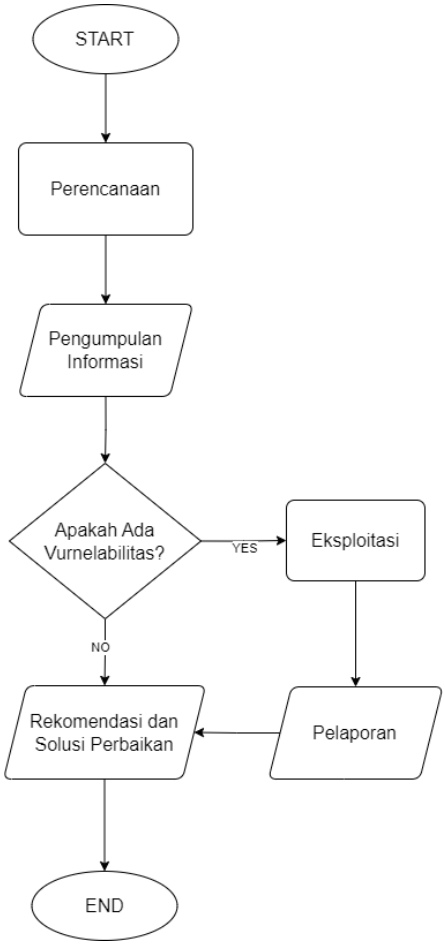
Dalam penelitian keempat melakukan penelitian berjudul "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test dan ISSAF" pada Sistem Informasi MTsN 8 Bantul. Hasil pengujian menggunakan Kali Linux menunjukkan bahwa tidak terdapat celah yang terdeteksi, menyoroti tingkat keamanan sistem informasi sekolah tersebut. Analisis menunjukkan bahwa sistem tersebut memiliki perlindungan yang baik terhadap penetrasi yang berpotensi merugikan [8].

Dengan demikian, penelitian sebelumnya dapat disimpulkan bahwa secara konsisten menyoroti pentingnya analisis keamanan *Website* menggunakan metode *Penetration Testing* dan *Framework* ISSAF. Dari studi kasus yang berbeda, ditemukan beragam kerentanan keamanan, mulai dari celah keamanan serius seperti *SQL Injection* dan XSS hingga risiko DDoS. Penelitian ini bertujuan memperluas kajian tersebut dengan menganalisis keamanan *Website* menggunakan metode yang sama, untuk mengidentifikasi potensi kerentanan spesifik pada konteks pemerintahan. Berbeda dengan fokus pada situs pendidikan dan lembaga swasta dalam penelitian sebelumnya, penelitian ini memberikan perspektif baru dalam pengamanan data pemerintahan, khususnya untuk perlindungan data sensitif terkait pengendalian inflasi daerah, serta strategi mitigasi yang sesuai.

3. METODE PENELITIAN

3.1. *Flowchart*

Tahapan analisis keamanan sistem menggunakan metode Penetration Testing pada website dapat dilihat pada **Gambar 1**:



Gambar 1. Alur Analisa Keamanan Sistem

Pada **Gambar 1** merupakan Proses analisis keamanan sistem dimulai dengan tahap awal yang mencakup analisis keamanan menggunakan metode *Penetration Testing* pada *Website*. Pada tahap perencanaan, dilakukan persiapan yang cermat dan teliti, termasuk pemilihan alat-alat yang diperlukan untuk pemindaian serta pembuatan *proof of concept* (PoC) sebagai langkah awal dalam proses penetrasi. Selanjutnya, dilakukan pengumpulan informasi terkait *Website* untuk memahami struktur dan fitur-fitur yang ada. Jika dalam analisis ditemukan adanya kerentanan, proses dilanjutkan ke tahap eksploitasi untuk menguji potensi ancaman dengan menjalankan PoC untuk mengeksploitasi kerentanan tersebut. Hasil dari analisis dan eksploitasi ini kemudian dilaporkan kepada pihak terkait, seperti pengelola *Website* atau tim keamanan informasi. Berdasarkan laporan tersebut, diberikan rekomendasi dan solusi perbaikan yang disarankan untuk meningkatkan keamanan sistem secara keseluruhan. Setelah semua tahapan dilaksanakan dan rekomendasi perbaikan disampaikan, proses analisis keamanan sistem pada *Website* dianggap selesai.

3.2. Metode Pengumpulan Data

Metode penelitian yang digunakan dalam melakukan penelitian ini adalah dengan menggunakan metode penelitian deskriptif kuantitatif dan kualitatif. Metode penelitian

kuantitatif menekankan pada hipotesis yang spesifik, berupa angka, analisis statistik, fokus pada hasil, dan bersifat deduktif [9]. Sedangkan, kualitatif berfokus pada perspektif, pengalaman, dan perilaku responden dalam suatu kajian penelitian [10]. Metode pengumpulan data yang digunakan pada penelitian ini, sebagai berikut:

1. **Studi Literatur**

   Mengumpulkan dan mengkaji literatur yang relevan dengan keamanan sistem, teknik *Penetration Testing*, dan standar keamanan web. Sumber literatur dapat berupa buku, artikel jurnal, dan dokumen standar keamanan seperti *Acunetix*.

2. **Observasi**

   Mengamati dan memeriksa konfigurasi sistem *website* TPID DIY secara online. Ini termasuk pengamatan terhadap *server*, aplikasi web, dan komponen-komponen jaringan yang terkait.

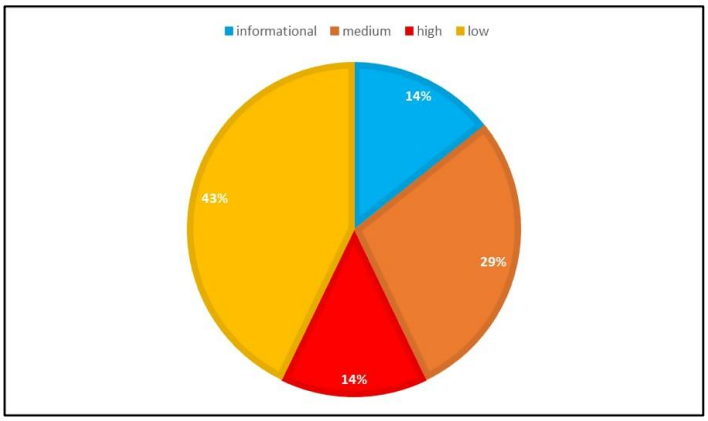
3. **Pengujian Manual**

   Melakukan pengujian manual terhadap aplikasi web untuk menemukan kerentanan yang mungkin tidak terdeteksi oleh alat otomatis. Ini termasuk teknik seperti injection, *cross-site scripting (XSS),* dan uji coba otentikasi serta otorisasi.

4. HASIL DAN PEMBAHASAN

4.1. Ringkasan Grafis *(Graphical summary)*

Graphical summary dari laporan pentest pada *Website* tpid.jogjaprov.go.id memberikan gambaran yang informatif mengenai hasil pengujian keamanan. Grafik ini mencakup elemen visual seperti diagram batang untuk menampilkan tingkat kerentanan berdasarkan keparahannya, yang menggunakan warna berbeda untuk menyoroti area yang memerlukan perhatian segera. Selain itu, grafik lingkaran digunakan untuk menunjukkan distribusi kerentanan berdasarkan jenis, seperti *SQL Injection* dan XSS, yang memberikan wawasan mengenai jenis serangan yang dihadapi oleh situs tersebut. Grafik *Graphical Summary* dapat dilihat pada **Gambar 2** sebagai berikut:



Gambar 2. *Graphical summary tpid.jogjaprov.go.id*

Pada Gambar 2 diatas menunjukkan distribusi kerentanan pada *website* TPID DIY berdasarkan tingkat keparahannya.

1. ***Informational* (14%):** Kerentanan informasi ini mencakup kelemahan yang tidak menyebabkan ancaman langsung terhadap keamanan sistem. Namun, informasi ini bisa membantu penyerang untuk merencanakan serangan yang lebih serius di masa depan.
2. ***Low* (43%):** Kerentanan tingkat rendah ini adalah kelemahan yang memiliki dampak minimal terhadap keamanan sistem. Kerentanan ini tetap perlu diperbaiki untuk mencegah kemungkinan penyalahgunaan di masa depan.
3. ***Medium* (29%):** Kerentanan tingkat menengah ini mencakup kelemahan yang dapat dieksploitasi untuk mendapatkan akses terbatas atau merusak fungsi sebagian dari sistem. Kerentanan ini mungkin memerlukan kombinasi dengan kelemahan lain untuk menyebabkan dampak yang lebih serius.
4. ***High* (14%):** Kerentanan tingkat tinggi ini mencakup kelemahan yang bisa dieksploitasi dengan mudah oleh penyerang dan dapat menyebabkan dampak signifikan, seperti kehilangan data atau akses tidak sah ke sistem. Contoh kerentanan ini termasuk *SQL Injection*, di mana penyerang bisa mendapatkan akses langsung ke basis data sistem.

Dengan demikian, *graphical summary* memberikan wawasan mendalam tentang jenis-jenis kerentanan yang ada di *website* TPID DIY. Dengan mengetahui distribusi ini, tim keamanan dapat menyusun strategi peningkatan keamanan yang lebih spesifik dan sesuai dengan risiko yang dihadapi. Informasi ini sangat penting untuk mengalokasikan sumber daya keamanan secara efektif dan meningkatkan ketahanan sistem terhadap serangan siber.

4.2. *Vulnerability Assesment*

4.2.1. *Information Gathering*

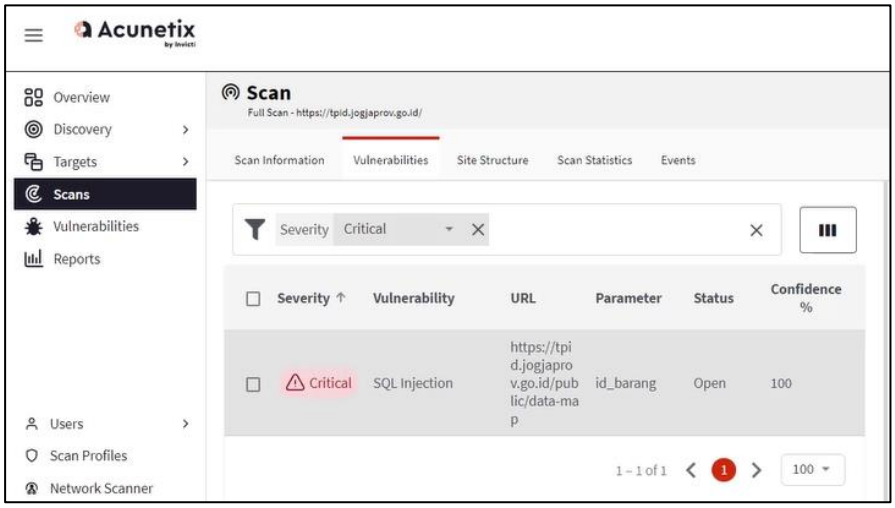
Information Gathering merupakan tahapan awal dalam melakukan pengujian keamanan sistem dan jaringan komputer. Tujuan dari *Information Gathering* adalah untuk mengumpulkan dan memperoleh informasi mengenai ekosistem yang diterapkan oleh pengguna, termasuk kepemilikan domain dan informasi sensitif lainnya [11]. TPID Daerah Istimewa Yogyakarta, yang dikelola melalui situs resmi *tpid.jogjaprov.go.id*, merupakan inisiatif pemerintah setempat untuk mengendalikan inflasi di wilayah tersebut. Dalam upaya transparansi, informasi teknis terkait dengan situs dapat ditemukan sebagai berikut:

a. Server HTTP: Apache
b. Alamat IP: 103.255.15.93
c. Script: text/javascript
d. Email: support@*tpid.jogjaprov.go.id*.

Dengan demikian, pemerintah Daerah Istimewa Yogyakarta berupaya memberikan akses dan informasi yang jelas terkait dengan langkah-langkah pengendalian inflasi di wilayah tersebut melalui *platform online.*

4.2.2. *Acunetix*

Acunetix adalah salah satu aplikasi pemindai web terkemuka yang sangat efektif sebagai solusi untuk mengatasi masalah keamanan situs web. *Acunetix* mampu mendeteksi lebih banyak kerentanan keamanan web dibandingkan dengan alat pemindai lainnya yang tersedia di internet [12]. *Website* TPID DIY yang akan dianalisis menggunakan Acunetix adalah langkah krusial sebelum memasuki proses *scan*ning, karena hal ini berfungsi untuk memahami potensi kelemahan keamanan yang ada dalam sebuah sistem atau aplikasi web. Hasil *scan* acunetix dapat dilihat pada gambar 3.



Gambar 3. Hasil *Scan* Acunetix

Pada **Gambar 3**, hasil *scan* Acunetix menunjukkan adanya satu kerentanan (*vulnerability*) pada situs web yang di*scan*. Berikut adalah penjelasan hasil *scan* acunetix, sebagai berikut:

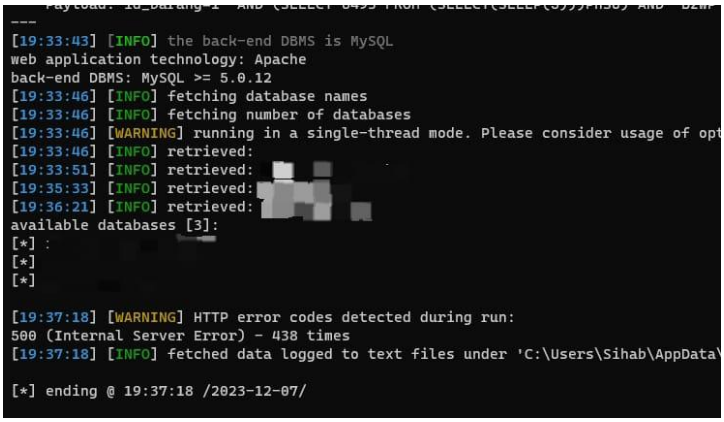
1. ***Severity* (Keparahan):** Kategori ini menunjukkan tingkat keparahan dari kerentanan yang ditemukan. Pada gambar tersebut, tingkat keparahan yang terdeteksi adalah "*Critical*" (Kritis). Hasil *scan* menunjukkan bahwa kerentanan yang ditemukan memiliki potensi dampak yang sangat tinggi dan perlu segera diperbaiki.
2. ***Vulnerability* (Kerentanan):** Jenis kerentanan yang ditemukan adalah "*SQL Injection*". *SQL Injection* adalah jenis serangan di mana penyerang dapat menyisipkan atau "menyuntikkan" kode SQL berbahaya ke dalam *query* SQL yang digunakan oleh aplikasi web. Penyerang bisa mengakses atau memodifikasi data dalam basis data yang mendasarinya.
3. ***URL:*** URL menunjukkan alamat spesifik di mana kerentanan ditemukan. Pada gambar tersebut, kerentanan ditemukan.
4. ***Parameter*:** Parameter ini menunjukkan parameter spesifik yang rentan terhadap serangan. Parameter yang ditemukan adalah id_barang.
5. **Status:** Status menunjukkan keadaan terkini dari kerentanan yang ditemukan. Pada gambar tersebut, statusnya adalah "*Open*" (Terbuka), yang berarti kerentanan ini belum diperbaiki atau ditangani.

6. ***Confidence*** % (Tingkat Keyakinan): Persentase keyakinan menunjukkan seberapa yakin alat pemindai dalam mendeteksi kerentanan tersebut. Pada gambar tersebut, tingkat keyakinannya adalah 100%, yang berarti Acunetix sangat yakin bahwa kerentanan ini benar adanya.

Dengan demikian, hasil ini menunjukkan pentingnya pemindaian keamanan web secara rutin untuk mendeteksi dan memperbaiki kerentanan yang mungkin ada, guna mencegah serangan yang dapat merugikan.

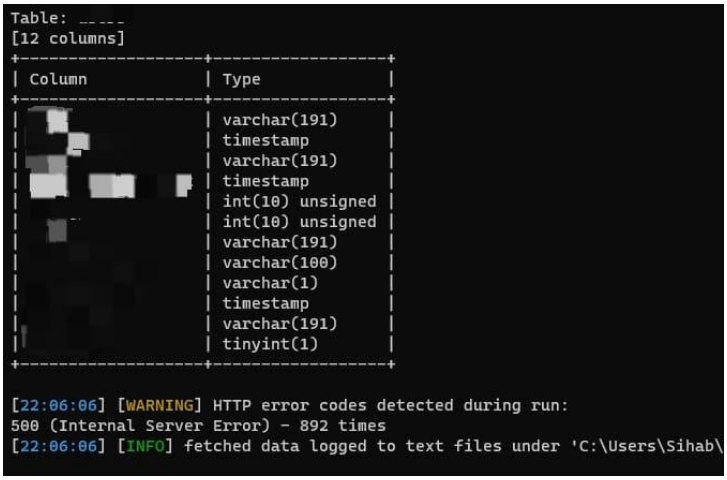
4.2.3. *SQL Injection*

Serangan *SQL Injection* adalah metode untuk menyisipkan perintah *SQL* sebagai input melalui aplikasi, seperti *Kali Linux*, dengan tujuan mendapatkan akses ke dalam *database*. Serangan ini dapat mengungkapkan informasi sensitif, seperti *username*, *password*, dan data lainnya yang tersimpan dalam *database* [13]. Tahap selanjutnya adalah pemberian laporan temuan kepada pihak terkait, termasuk otoritas yang bertanggung jawab atas keamanan *Website https://tpid.jogjaprov.go.id/*. Rekomendasi perbaikan konkret diajukan agar dapat diimplementasikan segera guna menutup celah keamanan yang ditemukan. Selain itu, dukungan teknis ditawarkan untuk membantu dalam pelaksanaan perbaikan-perbaikan tersebut, demi memastikan peningkatan keamanan sistem yang berkelanjutan. Kerja sama erat antara tim keamanan dan pihak terkait dipandang sebagai langkah penting untuk memastikan keberlanjutan keamanan *Website* serta melindungi data sensitif yang ada. Hasil *SQL Injection* dapat dilihat pada **Gambar 4** sebagai berikut:



Gambar 4. *SQL Injection tpid.jogjaprov.go.id*

Tindakan penetrasi dilakukan semata-mata untuk keperluan uji keamanan dan telah dilakukan dengan izin tertulis dari pihak berwenang yang bertanggung jawab terhadap keamanan *Website* tersebut. Laporan lengkap beserta rekomendasi keamanan yang diberikan kepada pihak terkait agar dapat mengatasi celah keamanan yang telah ditemukan, dengan tujuan meningkatkan keamanan dan melindungi integritas data pada *Website* tersebut. Hasil *database* dapat dilihat pada **Gambar 5** sebagai berikut:



Gambar 5. Kolom *Database tpid.jogjaprov.go.id*

Setelah melakukan analisis mendalam terhadap temuan keamanan, sejumlah perbaikan diusulkan untuk segera meningkatkan perlindungan sistem. Dalam pembaruan keamanan *database*, sangat penting untuk menutup celah *SQL Injection* yang terdeteksi. Implementasi *Parameterized Queries* atau penggunaan *Prepared Statements* menjadi langkah krusial yang akan membantu mencegah serangan *SQL Injection* di masa depan. Selain itu, diperlukan peninjauan ulang terhadap kebijakan akses ke *database*. Evaluasi hak akses, pengelolaan kata sandi yang lebih kuat, serta pembaruan kata sandi secara berkala merupakan langkah-langkah efektif untuk mengurangi risiko akses tidak sah. Penerapan sistem monitoring keamanan aktif juga didorong untuk mendeteksi dan memberikan peringatan dini atas aktivitas mencurigakan atau serangan yang sedang terjadi. Langkah-langkah perbaikan ini penting dilakukan sesegera mungkin guna mengurangi risiko serangan dan melindungi data sensitif yang tersimpan dalam *database*.

5. KESIMPULAN

Kerentanan keamanan pada *Website tpid.jogjaprov.go.id* yang ditemukan termasuk *Blind SQL Injection*, dan kerentanan pada metode *HTTP Trace*. Setiap jenis kerentanan memiliki potensi untuk dieksploitasi oleh penyerang, yang dapat menyebabkan pengungkapan informasi sensitif, manipulasi data, dan akses tidak sah.

1. Grafik menunjukkan tingkat kerentanan berdasarkan tingkat keparahan, yaitu: Informational (14%), Low (43%), Medium (29%), dan High (14%). Selain itu, grafik juga menunjukkan distribusi kerentanan berdasarkan jenis, seperti *SQL Injection* dan XSS.
2. Hasil pemindaian Acunetix menunjukkan satu kerentanan dengan kategori “Critical,” yaitu “*SQL Injection*,” dengan tingkat keyakinan 100%. Kerentanan ini ditemukan pada URL dengan parameter “id_barang” dan berstatus “Open,” yang berarti belum diperbaiki.
3. Serangan *SQL Injection* berhasil memperoleh akses ke database dan mengungkapkan informasi sensitif, seperti username dan password.

DAFTAR PUSTAKA

[1] M. B. Yel and M. K. M. Nasution, 'KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL', *Jurnal Informatika Kaputama (JIK)*, vol. 6, no. 1, pp. 92–101, Jan. 2022, doi: 10.59697/jik.v6i1.144.

[2] R. Vansuri *et al.*, 'Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi', *Jurnal Ilmu Multidisplin*, vol. 2, no. 1, pp. 106–113, Jun. 2023, doi: 10.38035/jim.v2i1.234.

[3] M. Ayyas, A. Fauzi, and S. Widodo, 'Studi Komparatif Teknik Analisis Keamanan Sistem Informasi e-Government: Penetration Testing VS Vulnerability Assessment', *SATIN - Sains Dan Teknologi Informasi*, vol. 10, no. 1, pp. 36–44, 2024, doi: 10.33372/stn.v10i1.1085.

[4] F. Fachri, A. Fadlil, and I. Riadi, 'Analisis Keamanan Webserver menggunakan Penetration Test', *Jurnal Informatika*, vol. 8, no. 2, pp. 183–190, Aug. 2021, doi: 10.31294/ji.v8i2.10854.

[5] G. Guntoro, L. Costaner, and M. Musfawati, 'Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)', *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 5, no. 1, p. 45, Jun. 2020, doi: 10.29100/jipi.v5i1.1565.

[6] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, 'Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF', *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, p. 113, Jul. 2020, doi: 10.24843/JIM.2020.v08.i02.p05.

[7] Z. A. Khan, N. Safaat, M. Irsyad, and T. Darmizal, 'Penetration Testing Information System Security Assessment Framework (ISSAF)', *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 4, no. 3, pp. 1593–1601, 2023, doi: 10.30865/klik.v4i3.1507.

[8] E. P. Silmina, A. Firdonsyah, and R. A. A. Amanda, 'Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan ISSAF', *Transmisi*, vol. 24, no. 3, pp. 83–91, Aug. 2022, doi: 10.14710/transmisi.24.3.83-91.

[9] I. Patonah, M. Sambella, and S. M. Az-Zahra, 'PENDEKATAN PENELITIAN PENDIDIKAN : PENELITIAN KUALITATIF, KUANTITATIF DAN KOMBINASI (MIX METHOD)', *PENDAS: Pendidikan Dasar*, vol. 8, no. 3, pp. 5378–5392, Dec. 2023, doi: 10.23969/jp.v8i3.11671.

[10] C. Schmieder, 'Qualitative data analysis software as a tool for teaching analytic practice: Towards a theoretical framework for integrating QDAS into methods pedagogy', *Qualitative Research*, vol. 20, no. 5, pp. 684–702, Oct. 2020, doi: 10.1177/1468794119891846.

[11] Chanief Budi Setiawan, Dedy Hariyadi, Adkhan Sholeh, and Akas Wisnuaji, 'Pengembangan Aplikasi Information Gathering Berbasis HybridApps', *INTEK : Jurnal Informatika dan Teknologi Informasi*, vol. 5, no. 1, pp. 22–28, May 2022, doi: 10.37729/intek.v5i1.1729.

[12] F. Al Fajar, 'ANALISIS KEAMANAN APLIKASI WEB PRODI TEKNIK INFORMATIKA UIKA MENGGUNAKAN ACUNETIX WEB VULNERABILITY', *INOVA-TIF*, vol. 3, no. 2, p. 110, Dec. 2020, doi: 10.32832/inova-tif.v3i2.4127.

[13] A. Monica, 'Pengukuran Efektivitas Serangan SQL Injection Pada Website Dengan Menggunakan Tools JSQL, Havij, Dan The Mole', *Jurnal Informatika dan Teknologi Komputer (J-ICOM)*, vol. 4, no. 2, Oct. 2023, doi: 10.55377/j-icom.v4i2.6926.