JURNAL PENGABDIAN SOSIAL
e-ISSN : 3031- 0059
Volume 2, No. 3, Tahun 2025
https://ejournal.jurnalpengabdiansosial.com/index.php/jps

Pengujian Keamanan Website JDIH Kab.Tegal Menggunakan *Acunetix* dengan Standar ISO/IEC/27001:2013

Fitriasih[1], Muhamad Ainurrohman[2], Fahrudin[3], Yuli Nurasri[4]
[1,2,3,4] *Politeknik Purbaya, Indonesia*

Corresponding Author
Nama Penulis: Fitriasih
E-mai: pipit.qolbu@gmail.com

Abstrak

Pengujian penetrasi pada website Jaringan Dokumentasi dan Informasi Hukum (JDIH) bertujuan untuk mengevaluasi dan meningkatkan keamanan sistem guna melindungi informasi hukum yang sensitif dari potensi ancaman siber. Kegiatan ini dilakukan sebagai bagian dari pengabdian masyarakat yang berfokus pada pemberdayaan kelembagaan di bidang teknologi informasi, khususnya dalam penerapan standar keamanan informasi ISO/IEC 27001:2013 menggunakan Acunetix. Metode pengujian meliputi analisis kerentanan, simulasi serangan, dan pemantauan akses sistem. Hasil dari pengujian menunjukkan adanya tingkat kerentanan rendah hingga sedang, yang memerlukan peningkatan pada pen gelolaan hak akses, pengamanan layanan aplikasi jaringan publik, serta kontrol terhadap kode sumber program. Rekomendasi perbaikan meliputi penerapan kebijakan keamanan yang lebih ketat, pembaruan sistem secara berkala, dan pelatihan teknis kepada tim pengelola JDIH. Dengan implementasi tersebut, diharapkan website JDIH dapat berfungsi secara optimal dalam menyediakan akses hukum yang aman dan terpercaya bagi Masyarakat
Kata kunci - *penetration test, keamanan sistem, dokumentasi,website JDIH*

Abstract

The penetration testing of the Legal Documentation and Information Network (JDIH) website aims to evaluate and enhance system security to protect sensitive legal information from potential cyber threats. This activity is conducted as part of community service focused on institutional empowerment in information technology, particularly in implementing the ISO/IEC 27001:2013 information security standard using Acunetix. The testing methods include vulnerability analysis, attack simulations, and system access monitoring. The results of the testing revealed low to medium levels of vulnerabilities, requiring improvements in access rights management, securing public network application services, and controlling program source codes. Recommendations for improvement include implementing stricter security policies, regularly updating systems, and providing technical training to the JDIH management team. With the implementation of these measures, the JDIH website is expected to function optimally in providing secure and reliable legal access to the public.
Keywords - *penetration test, system security, documentation, JDIH website*

PENDAHULUAN

Pemanfaatan platform digital dalam pelayanan publik semakin meningkat, namun di sisi lain menimbulkan kekhawatiran terkait keamanan siber, terutama untuk situs web yang menangani informasi hukum sensitif. Website Jaringan Dokumentasi dan Informasi Hukum (JDIH) memiliki peran penting sebagai platform untuk menyediakan akses publik terhadap dokumentasi dan informasi hukum. Namun, fungsionalitas dan kredibilitasnya dapat terganggu oleh potensi ancaman siber, sehingga diperlukan evaluasi berkala terhadap infrastruktur keamanannya.

Penelitian sebelumnya juga melakukan Keamanan Webserver Menggunakan Metode Penetrasi Testing mau. maka pentingnya pengujian penetrasi sebagai langkah proaktif untuk mengidentifikasi dan mengurangi kerentanan sistem. Penelitian yang dilakukan oleh penulis dari Politeknik Purbaya menunjukkan efektivitas pengujian penetrasi dalam mengungkap celah keamanan dan memperkuat pertahanan sistem, terutama jika dikombinasikan dengan penerapan standar internasional seperti ISO/IEC 27001:2013. ISO/IEC 27001 adalah standar sistem manajemen keamanan informasi (ISMS) yang diterbitkan pada bulan September 2013 oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC).

Standar ini menyediakan kerangka kerja komprehensif untuk mengelola keamanan informasi, memastikan sistem siap menghadapi ancaman saat ini maupun di masa depan.

Namun, masih terdapat celah dalam penerapan metode tersebut pada platform pemerintahan di tingkat regional. Website JDIH tidak terkecuali, karena memerlukan pendekatan yang disesuaikan untuk mengatasi tantangan operasional dan keamanannya yang unik.

Penelitian ini bertujuan untuk mengevaluasi keamanan website JDIH dari ancaman ancaman cyber, Adanya permukaan serangan yang mengekspos serangan jaringan bisa pasif atau aktif. Permukaan serangan ini dapat membuat layanan jaringan runtuh, membuatnya tidak tersedia untuk sementara, memungkinkan akses tidak sah dari data yang mengalir melalui jaringan, dan sebagainya. Jika terjadi serangan pasif, jaringan dapat dipantau oleh musuh untuk menangkap kata sandi, atau untuk menangkap informasi yang bersifat sensitif. Selama serangan pasif, seseorang dapat memanfaatkan lalu lintas jaringan untuk mencegat komunikasi antara 5 sistem sensitif dan mencuri informasi. Melalui pengujian penetrasi, dengan fokus pada identifikasi kerentanan, pemberian rekomendasi perbaikan, dan penguatan sistem secara keseluruhan guna melindungi informasi hukum yang sensitif. Temuan penelitian ini diharapkan dapat mendukung terciptanya platform pelayanan publik yang lebih aman dan andal, serta memberikan wawasan praktis untuk inisiatif serupa di wilayah lain.

Keamanan database merupakan proses yang sangat krusial untuk menjaga data dalam basis data tetap aman dan tersedia. Proses ini mencakup berbagai langkah untuk memastikan bahwa data hanya dapat diakses oleh pihak yang memiliki wewenang, sekaligus mencegah akses oleh pihak yang tidak berhak.

Aspek keamanan database meliputi kebijakan keamanan, pengelolaan akses, enkripsi data, pencadangan dan pemulihan, serta pengawasan dan pemantauan. Kebijakan keamanan berfungsi sebagai pedoman dan aturan yang dirancang untuk melindungi data agar tidak disalahgunakan. Sementara itu, pengelolaan akses melibatkan pengaturan hak akses pengguna, sehingga hanya individu yang memiliki otoritas yang dapat mengakses data yang tersimpan. Sehingga dengan dilakukannya penetration test dapat diketahui tingkat keamanan dari data yang ada di website di JDIH Pemerintah Kabupaten Tegal.

METODE

Kegiatan ini menggunakan metode pengujian penetrasi *(penetration testing)* dengan pendekatan berbasis standar internasional ISO/IEC 27001:2013. Tujuan SNI ISO/IEC 27001:2013 adalah mengadopsi pendekatan menyeluruh untuk melindungi serta menjaga keamanan informasi yang

mencakup tiga aspek utama, yaitu Kerahasiaan *(Confidentiality),* Integritas (*Integrity),* dan Ketersediaan *(Availability).* Tahapan pelaksanaan penelitian meliputi:

1. Persiapan dan Perencanaan
   a. Mengumpulkan informasi awal terkait arsitektur dan infrastruktur website JDIH.
   b. Menentukan ruang lingkup pengujian, termasuk area sistem yang akan diuji.
   c. Menyusun rencana pengujian sesuai dengan kebutuhan sistem dan kerangka kerja ISO/IEC 27001:2013.
2. Identifikasi Kerentanan
   a. Menggunakan alat pemindai kerentanan *(vulnerability scanner)* untuk mengidentifikasi celah keamanan potensial, seperti celah akses, validasi input, dan konfigurasi server.
   b. Melakukan analisis terhadap hasil pemindaian untuk menentukan prioritas risiko berdasarkan tingkat keparahannya.
3. Simulasi Serangan Siber
   a. Mensimulasikan berbagai jenis serangan, seperti injection, *cross-site scripting* (XSS), dan *brute force*, untuk menguji efektivitas pertahanan sistem.
   b. Mengevaluasi kemampuan sistem dalam mendeteksi dan menangkal serangan.
4. Pemantauan dan Analisis
   a. Melakukan pemantauan aktivitas akses sistem selama simulasi serangan.
   b. Menganalisis data log untuk menemukan pola akses mencurigakan dan potensi pelanggaran keamanan.
5. Rekomendasi dan Implementasi
   a. Menyusun laporan hasil pengujian yang mencakup temuan kerentanan, tingkat risiko, dan rekomendasi perbaikan.
   b. Memberikan pelatihan teknis kepada pengelola JDIH untuk menerapkan langkah-langkah perbaikan, seperti peningkatan pengelolaan hak akses, pembaruan sistem berkala, dan implementasi kebijakan keamanan yang lebih ketat.

Tahapan ini dilakukan secara sistematis untuk memastikan bahwa seluruh potensi ancaman terhadap keamanan sistem dapat diidentifikasi dan diatasi dengan solusi yang tepat, sehingga mendukung operasional website JDIH yang aman dan andal.

HASIL DAN PEMBAHASAN

Berdasarkan hasil pengujian yang dilakukan, pada pengujian Website JDIH pada pengujian ini menunjukkan bahwa situs web Jaringan Dokumentasi dan Informasi Hukum (JDIH) telah melalui pemindaian keamanan dan kepatuhan terhadap standar keamanan ISO 27001:2013. Beberapa temuan utama meliputi:

1. Kepatuhan Kategori Kontrol Akses: Tidak ada peringatan terkait manajemen hak akses istimewa, kontrol akses ke kode sumber, akses ke jaringan, dan lingkungan pengembangan, pengujian, serta operasional. Ini menunjukkan bahwa JDIH memiliki kebijakan dan implementasi keamanan yang cukup baik dalam menjaga keamanan akses.
2. Manajemen Autentikasi dan Informasi Sensitif: Tidak ditemukan peringatan pada kategori penggunaan informasi autentikasi rahasia dan prosedur log-on aman. Hal ini menunjukkan bahwa kebijakan keamanan terkait akses dan autentikasi telah dipatuhi.
3. Keamanan Layanan Aplikasi dan Jaringan: Tidak ada peringatan mengenai pengamanan layanan aplikasi pada jaringan publik, perlindungan data uji, dan kebijakan kontrol kriptografi. Ini menandakan bahwa aplikasi dan layanan JDIH telah mengikuti standar perlindungan data dan kerahasiaan.

Secara keseluruhan, hasil uji menunjukkan bahwa situs JDIH Tegal memenuhi sebagian besar standar keamanan dan tidak terdapat peringatan signifikan. Namun, pemantauan dan pemeliharaan terus diperlukan untuk memastikan keberlanjutan keamanan sesuai standar ISO 27001:2013

Gambar 1.
Penyerahan Laporan Hasil Penetration Test JDIH
oleh Ibu Fitriasih kepada Bapak

KESIMPULAN

Kesimpulan dari pengujian penetrasi pada website Jaringan Dokumentasi dan Informasi Hukum (JDIH) adalah bahwa pengujian ini berhasil mengidentifikasi beberapa kerentanannya, dengan tingkat kerentanan yang bervariasi dari rendah hingga sedang. Meskipun demikian, pengujian ini memberikan gambaran jelas mengenai area-area yang memerlukan perbaikan, seperti pengelolaan hak akses, pengamanan layanan aplikasi jaringan publik, serta kontrol terhadap kode sumber program. Untuk meningkatkan keamanan sistem dan melindungi informasi hukum yang sensitif, disarankan untuk menerapkan kebijakan keamanan yang lebih ketat, melakukan pembaruan sistem secara berkala, dan memberikan pelatihan teknis kepada tim pengelola JDIH. Langkah-langkah ini diharapkan dapat meningkatkan performa dan memastikan keamanan akses hukum yang disediakan oleh website JDIH bagi masyarakat.

UCAPAN TERIMA KASIH

Terimakasih kepada semua Kerjasama team penulis yang berkontribusi dalam penulisan pengabdian ini, serta bekerjasama dalam melakukan pengujian keamanan Website JDIH. Terimakasih kepada Pemerintah Kabupaten Tegal yang telah mempercayakan pengujian keamanan website JDIH kepada Politeknik Purbaya.

DAFTAR PUSTAKA

A. M. Ujung, M. Irwan, and P. Nasution, "Pentingnya Sistem Keamanan Database untuk melindungi data pribadi," JISKA J. Sist. Inf. Dan Inform., vol. 1, no. 2, p. 44, 2023, [Online]. Available: http://jurnal.unidha.ac.id/index.php/jteksis

Fachri, F. (2023). Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing. Jurnal Teknologi Informasi Dan Ilmu Komputer, 10(1), 51-58.

Hanafi, "Dasar Cyber Security dan Forensic," p. 236, 2022, [Online]. Available: https://eprints.amikom.ac.id/id/eprint/10688/

Pongdatu, G. A. N., Michael, A., & Patalo, E. E. (2022). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing di SMK Xyz Tana Toraja. INFINITY: UKI Toraja Journal of Information Technology, 2(2).

Yunanri, Riadi, and Yudnana. (2018.) "Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing," Annu. Res. Semin., vol. 2, no. 1, pp. 300–304,