PENETRATION TEST PADA WEBSITE SMKMN.SCH.ID MENGGUNAKAN OWASP 10

TUGAS AKHIR

Diajukan sebagai syarat untuk mendapat gelar Ahli Madya pada Prodi

Manajemen Informatika

oleh:

WILI PRIMA
NPM. 201000457401022

FAKULTAS EKONOMI
MANAJEMEN INFORMATIKA
UNIVERSITAS MAHAPUTRA MUHAMMAD YAMIN SOLOK

2023

ABSTRAK

WILI PRIMA.2023. Penetration Test pada Website smkmn.sch.id Menggunakan OWASP 10. Tugas Akhir. Fakultas Ekonomi. Manajemen Informatika. Univeraitas Mahaputra Muhammad Yamin Solok. Solok.

Tujuan dari penelitian ini adalah untuk menguji keamanan dari web yang berdomain smkmn.sch.id terhadap serangan dari luar oleh orang yang tidak bertanggung jawab yang dapat merugikan Sekolah SMK Maritim Nusantara, melakukan pengujian terhadap website smkmn.sch.id, membuat hasil laporan penetration testing terhadap website smkmn.sch.id. Tahapan dalam pengumpulan data ini dari beberapa sumber yaitu melalui jurnal, buku, paper ilmiah, tugas akhir, skripsi dan media digital seperti internet.

Dari hasil analisis ditemukan sebanyak 22 kerentangan yaitu yang berpotensi memiliki tingkat kerusakan tinggi (Hight) ada 6 yaitu Remote OS Command Injection sebanyak 6%, SQL Injection di anka 15%, SQL Injection - MySQL sebanyak 1%, SQL Injection - PostgreSQL - Time Based juga 1% dan SQL Injection - SQLite diangka 38%. Selanjutnya, langkah-langkah perbaikan dan pemantauan berkelanjutan akan menjadi prioritas untuk menjaga keamanan sistem yang dianalisis.

Untuk itu penulis menyarankan perlunya dilaksanakan kembali pengujian pada seluruh sistem yang memiliki domain smkmn.sch.id supaya mudah melihat kerentan secara keseluruhan, server smkmn.sch.id perlu di lakukan konfigurasi kembali supaya hanya user yang diberika akses yang dapat mereques data terentu, serta menutup port-port yang tidak digunakan, plugin dan wordpres perlu di lakukan updata secara rutin, melakuukan penangamanan data menggunakan encryption terhadap data yang penting untuk mengurangi resiko terjadinya kebocoran informasi yang penting, masih kurangnya kesadaran pengelola untuk selalu rutin melakukan pembaruan pada sistem mereka untuk mengurangi resiko adanya celah keamanan.

Kata kunci: Penetration Test, Website, OWASP 10

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Banyak aspek kehidupan kita bergantung pada sistem komputer dan jaringan, mulai dari komunikasi hingga bisnis. Gangguan dalam sistem ini dapat mempengaruhi produktivitas, layanan publik, dan bahkan kehidupan sehari-hari. Keamanan sistem juga memengaruhi persepsi pelanggan, di mana konsumen cenderung lebih percaya pada perusahaan atau organisasi yang menjaga keamanan data. Keamanan informasi sangat penting karena ada potensi pihak yang tidak berhak mengakses dan menyalahgunakan informasi, yang dapat merugikan organisasi. Prinsip dasar keamanan jaringan melibatkan kerahasiaan, integritas, dan ketersediaan informasi, dikenal sebagai CIA TRIAD. Jika prinsip-prinsip ini tidak terpenuhi, jaringan dapat dianggap tidak aman dan rentan terhadap penyusupan. Salah satu tindakan untuk mengatasi masalah ini adalah dengan menganalisis sistem dan jaringan dari perspektif luar atau jaringan publik, seperti yang dilakukan di smkmn.sch.id menggunakan OWASP ZAP 10, WPScan dan nmap. Dengan menggunkan alat bantu ini saya menemukan kerentanan pada website smk.sch.id seperti port-port yang terbuka.

B. Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan di atas maka rumusan masalah yang ditetapkan pada website smkmn.sch.id menunjukkan perhatian terhadap keamanan informasi di smkmn.sch.id dan usaha untuk mengidentifikasi, pengujian, dan melakukan evaluasi keamanan yang bertujuan untuk melindungi proses bisnis dan data sekolah.

C. Batasan Masalah

Untuk memfokuskan masalah yang ada, perlu adanya batasan-batasan agar penulis dapat lebih terfokus pada masalah yang ada. Oleh karena itu, dalam kasus ini, batasan masalah dapat didefinisikan sebagai:

1. Web yang akan diuji dengan url https://smkmn.sch.id
2. Penetration testing ini mengacu pada OWASP ZAP 10, wpscan dan nmap

D. Tujuan Penelitian

Tujuan yang diharapkan tercapai dalam melakukan penelitian pengujian celah keamanan ini adalah sebagai berikut:

1. Menguji keamanan dari web yang berdomain smkmn.sch.id terhadap serangan dari luar oleh orang yang tidak bertanggung jawab yang dapat merugikan Sekolah SMK Maritim Nusantara.
2. Melakukan pengujian terhadap website smkmn.sch.id
3. Membuat hasil laporan penetration testing terhadap website smkmn.sch.id

E. Manfaat Penelitian

Manfaat yang diharapkan didapatkan dari penelitian ini adalah sebagai berikut:

1. Bagi Peneliti
    a. Dapat mengimplementasikan ilmu pengetahuan yang selama ini diperoleh di perkuliahan
    b. Mendapatkan pembelajaran baru tentang OWASP ZAP 10, wpscan, dan nmap
2. Bagi SMK Maritim Nusantara
    a. Mengetahui kerentanan website smkmn.sch.id dari pihak luar yang tidak bertanggung jawab
    b. Mengetahui seberapa rentang website smkmn.sch.id sehingga dapat melakukan langkah-langkah penanggulangan dapat dilakukan sejak dini.

F. Metodologi Penelitian

Metodologi penelitian digunakan untuk mengarahkan pengujian agar sesuai rencana dan mencapai tujuan yang diinginkan. Berikut adalah metodologi yang diterapkan dalam tugas akhir ini:

1. Pendaftaran Alamat IP: Pendaftaran alamat IP diperlukan sebagai syarat utama untuk melakukan penetration testing pada domain smkmn.sch.id. Ini memerlukan akses yang diberikan oleh admin/pengelola, dalam hal ini admin selaku lembaga pengelola domain smkmn.sch.id admin telah mendaftarkan alamat IP komputer yang dipakai untuk melakukan pentes.

2. Footprinting: Tahap awal dalam penguasaan sistem adalah mengumpulkan segala informasi terkait dengan situs web berdomain smkmn.sch.id yang akan diuji penetrasi.
3. Scanning: Setelah memperoleh informasi mengenai web target, langkah selanjutnya adalah melakukan scanning, yaitu mencari port atau celah keamanan lain pada web yang dapat dieksploitasi.
4. Uji Penetrasi: Dilakukan pengujian pada web berdomain smkmn.sch.id dengan metode OWASP10, WPScan, dan NMAP.

G. Sistematika Penulisan

Untuk memberikan gambaran secara menyeluruh mengenai masalah yang akan dibahas dalam penulisan laporan tugas akhir ini, maka sistematika laporan ini dibagi menjadi 5 bab. Adapun penjabarannya sebagai berikut:

1. BAB I PENDAHULUAN Bab pendahuluan berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan laporan penetration testing pada domain smkmn.sch.id menggunakan metode OWASP10, WPSCAN, dan NMAP
2. BAB II LANDASAN TEORI Bab ini membahas tentang gambaran umum tentang teori yang diterapkan dalam pengujian penetration testing, menggunakan OWASP 10. Selain itu, dalam bab ini juga terdapat penjelasan tentang metode dan tools yang digunakan untuk melakukan penetration testing.

3. BAB III METODOLOGI Bab ini membahas tentang metode yang dilakukan dalam penelitian. Metode tersebut adalah pengumpulan data, analisis kebutuhan serta perancangan pembangunan sistem dan termasuk didalamnya perancangan pengujian yang dilakukan secara sistematis.
4. BAB IV IMPLEMENTASI DAN HASIL Bab ini berisi tentang langkah-langkah proses pengujian yang dilakukan dan hasil yang didapatkan dari proses pengujian yang dilakukan terhadap beberapa target yang ditentukan.
5. BAB V KESIMPULAN DAN SARAN Bab ini berisi penutup yang meliputi kesimpulan-kesimpulan dari hasil pengujian yang telah dilakukan sebelumnya yang berupa hasil analisis pengujian yang telah dilakukan dan terdapat saran-saran dari hasil pengujian.

BAB V

KESIMPULAN

A. Kesimpulan

Setelah dilakukan pengujian penetrasi menggunakan berbagai alat seperti OWASP Top 10, WPScan, dan Nmap, bersama dengan penerapan teknik pengumpulan informasi yang relevan. Hasil pengujian ini mengungkapkan sejumlah kerentanan keamanan yang signifikan dalam sistem atau aplikasi yang ditinjau, termasuk masalah serius seperti SQL injection, kerentanan autentikasi yang melibatkan akses ilegal ke akun pengguna, dan potensi paparan data sensitif. Selain itu, penggunaan alat seperti WPScan telah membantu mengidentifikasi kerentanan spesifik terkait dengan platform WordPress, sementara Nmap memberikan wawasan tentang topologi jaringan dan potensi kerentanan di dalamnya. Dari hasil analisis ditemukan sebanyak 22 kerentangan diantaranya yang berpotensi meiliki tingkat kerusakan tinggi (Hight) ada 6 buah yaitu Remote OS Command Injection sebanyak 6%, SQL Injection di anka 15%, SQL Injection - MySQL sebanyak 1%, SQL Injection - PostgreSQL - Time Based juga 1% dan SQL Injection - SQLite diangka 38%. Selanjutnya, langkah-langkah perbaikan dan pemantauan berkelanjutan akan menjadi prioritas untuk menjaga keamanan sistem yang dianalisis. Kesimpulannya, pengujian penetrasi adalah langkah esensial dalam mengidentifikasi dan mengatasi potensi risiko keamanan yang dapat mengancam aset informasi di sekolah.

B. Saran

Berdasarkan penelitian yang sudah dilakukan terdapat beberapa saran yang dapat diterapkan pada penelitian berikutnya serta terdapat beberapa kekurangan pada pengembangan otomatisasi OWASPZap yang dapat dikembangkan lebih lanjut pada peneletian berikutnya yang antara lain:

1. Perlunya dilaksanakan kembali pengujian pada seluruh sistem yang memiliki domain smkmn.sch.id supaya mudah melihat kerentan secara keseluruhan.
2. Server smkmn.sch.id perlu di lakukan konfigurasi Kembali supaya hanya user yang diberika akses yang dapat mereques data terentu, serta menutup port-port yang tidak digunakan
3. Plugin dan wordpres perlu di lakukan updata secara rutin
4. Melakuukan penangamanan data menggunakan encryption terhadap data yang penting untuk mengurangi resiko terjadinya kebocoran informasi yang penting.
5. Masih kurangnya kesadaran pengelola untuk selalu rutin melakukan pembaruan pada sistem mereka untuk mengurangi resiko adanya celah keamanan.

DAFTAR PUSTAKA

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A., & Mooduto, H. A. (2021). Web application penetration testing using sql injection attack. *International Journal on Informatics Visualization*, *5*(3), 320–326. https://doi.org/10.30630/joiv.5.3.470

Fahlevi, M. R., & Putri, D. R. D. (2021). Analisis Monitoring & Kinerja Sistem Keamanan Jaringan Komputer Menggunakan Nmap (Studi Kasus: Raz Hotel & Convention Medan). *It (Informatic Technique) Journal*, *9*(1), 35. https://doi.org/10.22303/it.9.1.2021.35-43

Hasibuan, M., & Elhanafi, A. M. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. *Sudo Jurnal Teknik Informatika*, *1*(4), 171–177. https://doi.org/10.56211/sudo.v1i4.160

Herdiana, Y., & Saepudin, D. S. (2023). *Perancangan Sistem Informasi Penjualan Menggunakan Cms Wordpress Berbasis Web (Di Sandallaku Majalaya)*. *05*, 55–62.

Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, *18*(1), 77–86. https://doi.org/10.33364/algoritma/v.18-1.827

Jannati, A. (2019). *Rancang Bangun Website PT. Tendri Dharma Samudra*. http://repo.palcomtech.ac.id/id/eprint/141/1/PKL Ataya.pdf

Kurniawan, M. A., & Makin, S. (2023). *Dosen Tetap, Universitas Insan Pembangunan Indonesia *Penulis Korespondensi : Awan.insanpembangunan*. *11*(1).

Mulyanto, Y., Herfandi, H., & Kirana, randi chadra. (2022). ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR). *Jurnal Informatika Teknologi Dan Sains*, *4*(1), 26–35. https://doi.org/10.51401/jinteks.v4i1.1528

Mushlih, M., Fitri, R., & Wardiah, I. (2019). Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web. *Seminar Nasional Riset ...*, *5662*(November), 41–47. http://e-prosiding.poliban.ac.id/index.php/snrt/article/view/409

Pangestu, T., & Liza, R. (2022). Analisis Keamanan Jaringan Pada Jaringan Wireless Dari Serangan Man In The Middle Attack DNS Spoofing. *JiTEKH*, *10*(2), 60–67. https://doi.org/10.35447/jitekh.v10i2.571

Patricia, C. O. S. (2021). *JENIS KEJAHATAN PADA MASA PANDEMI COVID-19 DALAM PERSPEKTIF CYBER SECURITY NASIONAL DI INDONESIA*. *3*(2), 6.

Putra, Y., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Web

Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. *Jurnal Sistim Informasi Dan Teknologi*, *3*, 56–63. https://doi.org/10.37034/jsisfotek.v3i2.44

Rahardjo, B. (2015). Keamanan Sistem Informasi Berbasis Internet. In *PT Insan Infonesia* (Vol. 0).

Ramaddan Julianti, M., Akas Suwandara, J., Ali Akbar Jufri, M., Nabili Akbar, R., Abdul Hakim, R., & Diva Wardana, R. P. (2022). *Membuat Blog Dengan Wordpress (Hosting Dan Domain Gratis) Pada Siswa Smkn 2 Kab. Tangerang Article History*. *1*(2), 1.

Riasetiawan, M., Wisnuaji, A., Hariyadi, D., & Febrianto, T. (2021). Pengembangan Aplikasi Information Gathering Menggunakan Metode Hybrid Scan Berbasis Graphical User Interface. *Cyber Security Dan Forensik Digital*, *4*(1), 44–48. https://doi.org/10.14421/csecurity.2021.4.1.2449

Sari, E. P., Febrianti, D. A., & ... (2022). Fenomena Penipuan Transaksi Jual Beli Online Melalui Media Baru Berdasarkan Kajian Space Transition Theory. *Deviance Jurnal ...*, *6*, 153–168. https://journal.budiluhur.ac.id/index.php/deviance/article/view/1882%0Ahttps://journal.budiluhur.ac.id/index.php/deviance/article/download/1882/1272