JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/e4rhmk70

PENGUJIAN PENETRASI JARINGAN MENGGUNAKAN OWASP ZAP DAN SQLMAP UNTUK MENGIDENTIFIKASI KERENTANAN KEAMANAN WEBSITE

Rakhmadi Rahman [a*], Danang Fatkhur Razak [b]
[a] Program Studi Sistem Informasi, rakhmadi.rahman@ith.ac.id, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[b] Program Studi Sistem Informasi, danangfatkhurrazak@gmail.com, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[*]Korespondensi

ABSTRACT

Web application security is becoming increasingly critical amidst increasing cyber threats that can result in data leakage and other losses. This research aims to identify and exploit security vulnerabilities in a web application using two popular tools, OWASP ZAP and SQLMAP. OWASP ZAP is used to find various vulnerabilities such as Cross-Site Scripting (XSS) and insecure configuration, while SQLMAP is focused on the detection and exploitation of SQL Injection vulnerabilities. Through a series of automated scans and in-depth analysis, this research successfully identified several vulnerabilities with medium and low risk levels. The test results show that both tools are effective in identifying vulnerabilities, providing important insights into mitigation steps that need to be taken to improve web application security. This research also emphasizes the importance of input validation and sanitization, the use of parameterized queries, and security configuration updates as key mitigation measures. The findings are expected to contribute to improved security practices in web application development and reduce the risk against cyberattacks.

Keywords: *OWASP ZAP, SQLMAP, Vulnerabilities*

Abstrak

Keamanan aplikasi web menjadi semakin kritis di tengah meningkatnya ancaman siber yang dapat mengakibatkan kebocoran data dan kerugian lainnya. Penelitian ini bertujuan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan pada sebuah aplikasi web menggunakan dua alat populer, OWASP ZAP dan SQLMAP. OWASP ZAP digunakan untuk menemukan berbagai kerentanan seperti Cross-Site Scripting (XSS) dan konfigurasi yang tidak aman, sedangkan SQLMAP difokuskan pada deteksi dan eksploitasi kerentanan SQL Injection. Melalui serangkaian pemindaian otomatis dan analisis mendalam, penelitian ini berhasil mengidentifikasi beberapa kerentanan dengan tingkat risiko sedang dan rendah. Hasil pengujian menunjukkan bahwa kedua alat ini efektif dalam mengidentifikasi kerentanan, memberikan wawasan penting tentang langkah-langkah mitigasi yang perlu diambil untuk meningkatkan keamanan aplikasi web. Penelitian ini juga menekankan pentingnya validasi dan sanitasi input, penggunaan parameterized queries, dan pembaruan konfigurasi keamanan sebagai langkah-langkah mitigasi utama. Temuan ini diharapkan dapat berkontribusi pada peningkatan praktik keamanan dalam pengembangan aplikasi web dan mengurangi risiko terhadap serangan siber.

Kata Kunci: OWASP ZAP, SQLMAP, Kerentanan

1. PENDAHULUAN

Keamanan aplikasi web merupakan aspek yang sangat penting dalam era digital saat ini, di mana semakin banyak data sensitif yang dipertukarkan melalui internet. Serangan terhadap aplikasi web dapat menyebabkan kebocoran data, kehilangan kepercayaan pengguna, dan kerugian finansial yang signifikan. Oleh karena itu, pengujian penetrasi menjadi salah satu metode yang krusial dalam mengidentifikasi dan

Received Juli 6, 2024; Revised Agustus 9, 2024; Accepted September 26, 2024; Published Oktober 2, 2024

mengatasi kerentanan keamanan pada aplikasi web. OWASP ZAP (Zed Attack Proxy) dan SQLMAP adalah dua alat populer yang digunakan dalam pengujian penetrasi. OWASP ZAP adalah alat open-source yang dirancang untuk menemukan berbagai kerentanan keamanan dalam aplikasi web secara otomatis, Seperti Cross-Site Scripting (XSS), Insecure Configurations, dan banyak lagi. Di sisi lain, SQLMAP adalah alat open-source yang khusus digunakan untuk mendeteksi dan mengeksploitasi kerentanan SQL Injection. SQL Injection adalah salah satu serangan paling umum dan berbahaya yang dapat digunakan oleh penyerang untuk mendapatkan akses tidak sah ke basis data aplikasi. SQLMAP tidak hanya mendeteksi kerentanan ini, tetapi juga dapat digunakan untuk mengambil data sensitif dari basis data yang tereksploitasi.

Penelitian ini bertujuan untuk mengidentifikasi kerentanan keamanan pada sebuah aplikasi web menggunakan OWASP ZAP dan SQLMAP. Fokus utama dari penelitian ini adalah untuk mengevaluasi efektivitas kedua alat tersebut dalam menemukan dan mengeksploitasi kerentanan, serta memberikan rekomendasi mitigasi yang dapat diterapkan untuk meningkatkan keamanan aplikasi web.

2. TINJAUAN PUSTAKA

Penelitian ini menggunakan metode studi kasus untuk mengidentifikasi dan mengeksploitasi kerentanan pada sebuah aplikasi web yang dipilih sebagai target. Proses pengujian dilakukan dengan memanfaatkan dua alat utama, yaitu OWASP ZAP dan SQLMAP. OWASP ZAP digunakan untuk melakukan pemindaian otomatis pada aplikasi web, dengan tujuan menemukan berbagai jenis kerentanan seperti Cross-Site Scripting (XSS) dan konfigurasi yang tidak aman. Teknik pemindaian yang digunakan termasuk spidering, AJAX spidering, dan active scanning [1].

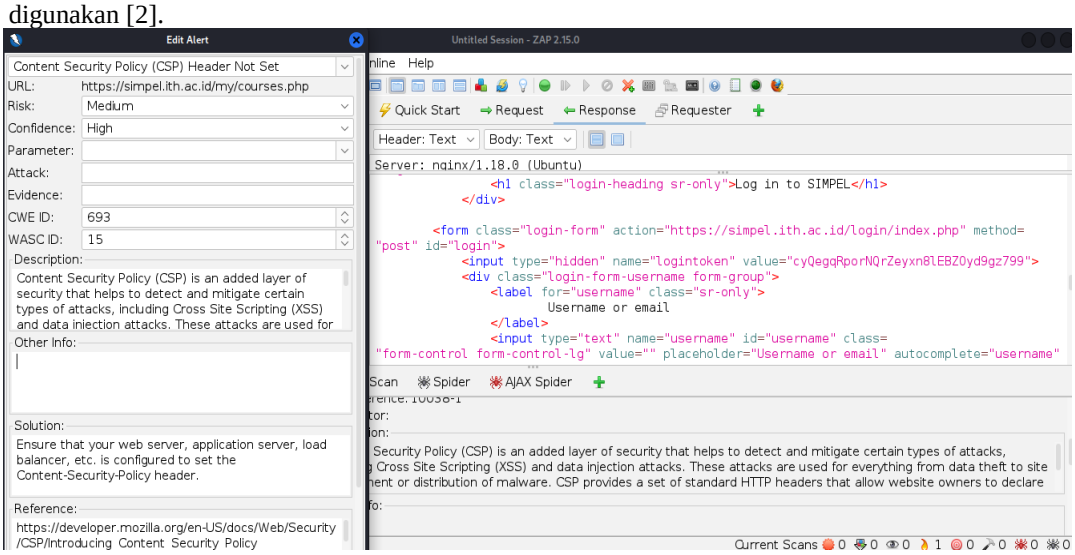
Selanjutnya, SQLMAP digunakan untuk mengidentifikasi dan mengeksploitasi kelemahan SQL Injection. Tahap ini mencakup pemindaian URL target guna menemukan parameter yang rentan terhadap injeksi SQL, diikuti dengan upaya eksploitasi kerentanan tersebut untuk mengakses serta mengambil data dari basis data yang telah disusupi. Setiap kerentanan yang ditemukan dianalisis secara detail untuk menilai dampaknya terhadap keamanan aplikasi, dan rekomendasi perbaikan yang tepat diberikan. Penelitian ini menyoroti efektivitas kedua alat dalam mendeteksi kerentanan dan menawarkan wawasan praktis tentang langkah-langkah mitigasi yang dapat diterapkan.

3. HASIL DAN PEMBAHASAN

3.1 Penelitian Analisis Hasil Pemindaian OWASP ZAP

Setelah spidering selesai, ZAP melakukan pemindaian aktif (Active Scan) dengan mengirimkan permintaan berbahaya ke server web untuk menemukan kerentanan. Kerentanan yang terdeteksi oleh OWASP ZAP meliputi:

a. Cross-Site Scripting (XSS): Parameter input yang rentan terhadap XSS ditemukan, memungkinkan injeksi skrip berbahaya yang dapat dieksekusi di browser pengguna.
b. Insecure Configurations: Beberapa konfigurasi server yang tidak aman terdeteksi, seperti header server yang terlalu informatif, yang dapat memberikan informasi kepada penyerang mengenai teknologi yang digunakan [2].



Gambar 1. Detail kerentanan pada target Content Security Policy (CSP) Header Not Set.

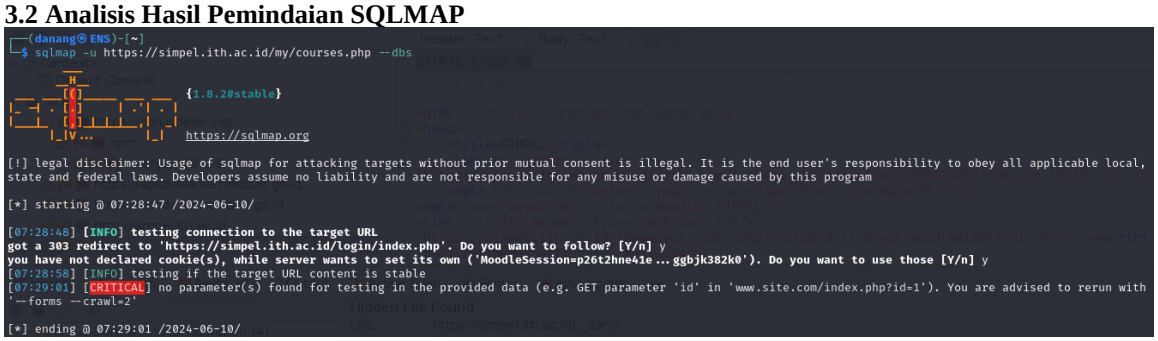
Setelah pemindaian selesai, kerentanan yang ditemukan diklasifikasikan berdasarkan tingkat risiko (High, Medium, Low). Kerentanan dengan tingkat risiko sedang dan rendah dianalisis untuk menentukan dampak potensial terhadap keamanan aplikasi web. Setiap kerentanan diberi rekomendasi mitigasi yang spesifik, seperti melakukan sanitasi input dan memperbarui konfigurasi server untuk meningkatkan keamanan.

Tabel 1 Persentase kerentanan confidence dan risk.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (6.2%)	0 (0.0%)	1 (6.2%)	2 (12.5%)
	Low	0 (0.0%)	2 (12.5%)	5 (31.2%)	1 (6.2%)	8 (50.0%)
	Informational	0 (0.0%)	1 (6.2%)	2 (12.5%)	3 (18.8%)	6 (37.5%)
	Total	0 (0.0%)	4 (25.0%)	7 (43.8%)	5 (31.2%)	16 (100%)

Berdasarkan hasil yang dijabarkan, terdapat beberapa kerentanan dengan risk (risiko) rendah dan menengah diikuti tingkat confidence yang bervariasi. Hal ini menunjukkan bahwa situs yang menjadi target perlu untuk melakukan peningkatan pada sistem keamanan, karena risk menengah sudah cenderung rawan untuk dipenetrasi.

3.2 Analisis Hasil Pemindaian SQLMAP



Gambar 2. Mengeksploitasi kerentanan dengan mencantumkan database menggunakan perintah sqlmap -u (target) --dbs

Hasil eksploitasi menunjukkan bahwa beberapa parameter input tidak rentan terhadap SQL Injection, tidak memungkinkan bagi penyerang untuk mengakses dan mengambil data sensitif dari basis data. Data yang diambil dianalisis untuk menentukan dampaknya terhadap keamanan aplikasi web.

4. KESIMPULAN DAN SARAN

Evaluasi Penelitian ini sukses mengidentifikasi dan mengeksploitasi kerentanan keamanan pada sebuah aplikasi web menggunakan dua alat utama, yaitu OWASP ZAP dan SQLMAP. Hasil pengujian menunjukkan bahwa aplikasi web yang diuji memiliki beberapa kerentanan dengan tingkat risiko sedang dan rendah, seperti Cross-Site Scripting (XSS), konfigurasi yang tidak aman, dan SQL Injection. Kedua alat ini terbukti efektif dalam menemukan kerentanan yang bisa dimanfaatkan oleh penyerang, menekankan pentingnya alat-alat tersebut dalam pengujian penetrasi. Kesimpulan utama dari penelitian ini adalah bahwa OWASP ZAP dan SQLMAP sangat berguna dalam pengujian penetrasi untuk mengidentifikasi kerentanan keamanan pada aplikasi web.

OWASP ZAP mampu menemukan berbagai jenis kerentanan, sedangkan SQLMAP khususnya efektif dalam mendeteksi dan mengeksploitasi SQL Injection. Kombinasi kedua alat ini memberikan pendekatan yang menyeluruh dalam pengujian keamanan aplikasi web [3]. Berdasarkan temuan penelitian ini, beberapa saran dapat diberikan untuk meningkatkan keamanan aplikasi web: Sanitasi dan Validasi Input: Semua input dari pengguna harus divalidasi dan disanitasi untuk mencegah injeksi skrip dan perintah berbahaya. Ini adalah langkah penting untuk mencegah serangan XSS dan SQL Injection. Penggunaan Parameterized Queries: Implementasi parameterized queries atau prepared statements untuk semua interaksi dengan basis

data adalah kunci untuk mencegah SQL Injection. Pembaruan Konfigurasi Keamanan: Server web harus dikonfigurasi dengan pengaturan keamanan yang tepat untuk mengurangi informasi yang terekspos dan memperketat aturan akses. Pengujian Penetrasi Rutin: Melakukan pengujian penetrasi secara berkala dengan menggunakan alat seperti OWASP ZAP dan SQLMAP untuk memastikan bahwa aplikasi web tetap aman terhadap ancaman baru yang muncul.

DAFTAR PUSTAKA

[1] Fajarino, Y. N. Kunang, H. M. Yudha, E. S. Negara, and N. R. Damayanti, "Evaluasi dan Peningkatan Keamanan Pada Sistem Informasi Akademik Universitas XYZ Palembang," J-SAKTI (Jurnal Sains Komputer dan Informatika), vol. 7, no. 2, pp. 991–1005, Sep. 2023, doi: https://doi.org/10.30645/j-sakti.v7i2.702.

[2] A. Fadlil, I. Riadi, and M. A. Mu'min, "Mitigation from SQL Injection Attacks on Web Server using Open Web Application Security Project Framework," International Journal of Engineering, vol. 37, no. 4, pp. 635–645, Apr. 2024, doi: https://doi.org/10.5829/ije.2024.37.04a.06.

[3] S. K. Rakshit, Ethical Hacker's Penetration Testing Guide: Vulnerability Assessment and Attack Simulation on Web, Mobile, Network Services and Wireless Networks (English Edition). BPB Publications, 2022. Accessed: Jun. 18, 2024. [Online]. Available: https://books.google.co.id/books?hl=en&lr=&id=ZetwEAAAQBAJ&oi=fnd&pg=PP26&dq=OWASP+ZAP+%26+SQLMAP&ots=THf_TEK1o_&sig=3-32OQm4eY7lW6iUlXBjGJGtO0M&redir_esc=y#v=onepage&q=OWASP%20ZAP%20%26%20SQLMAP&f=false

[4] Rezshal Hidayah. "Hardening Web Aplikasi Dengan Menggunakan OWASP Security Testing Guide (WSTG) Pada Website ABC." 2021.

[5] Rafeli, A. I., Seta, H. B., & Widi, I. W. "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ." Informatik: Jurnal Ilmu Komputer, 18(2), 97-103. 2022.

[6] M. Rizki, "POLITEIA : Jurnal Ilmu Politik Perkembangan Sistem Pertahanan / Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi," vol. 14, no. 1, pp. 54–62, 2022.

[7] Kho, Y., & Hernawan, F. Y. (2019). Bug Hunting 101 - Web Application Security Testing. AlFursanID.