Eksplorasi Keamanan Website Dinas XY di Jawa Timur dalam Pendekatan Pengujian Brute Force untuk mendeteksi kerentanan

Laporan Tugas Akhir

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana
Informatika Universitas Muhammadiyah Malang

Muchammad Zaidan
(201810370311025)

Bidang Minat
Keamanan Jaringan

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2023

LEMBAR PERSETUJUAN

Website Vulnerability Analysis of AB and XY Office in East Java (Analisa Kerentanan Website Dinas AB dan XY di Jawa Timur)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,
Malang, *13 Januari 2024*

Dosen Pembimbing 1	Dosen Pembimbing 2
	
Zamah Sari ST., MT.	**Ir Denar Regata Akbi S.Kom., M.Kom.**
NIP. 10814100555PNS.	**NIP. 10816120591PNS.**

LEMBAR PENGESAHAN

Website Vulnerability Analysis of AB and XY Office in East Java (Analisa Kerentanan Website Dinas AB dan XY di Jawa Timur)

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

Muchammad Zaidan

201810370311025

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 13 Januari 2024

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Briansyah Setio Wiyono S.Kom., M.Kom	**Ir. Wildan Suharso S.Kom., M.Kom**
NIP. 190913071987PNS.	**NIP. 10817030596PNS.**

Mengetahui,
Ketua Jurusan Informatika

Ir. Galih Wasis Wicaksono S.kom. M.Cs.
NIP. 10814100541PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : Muchammad Zaidan

NIM : 201810370311025

FAK./JUR. : Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Website Vulnerability Analysis of AB and XY Office in East Java (Analisa Kerentanan Website Dinas AB dan XY di Jawa Timur)"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Zamah Sari ST., MT.

Malang, 13 Januari 2024
Yang Membuat Pernyataan

Muchammad Zaidan

ABSTRAK

Penelitian ini bertujuan untuk melakukan analisis kerentanan terhadap website Kantor XY yang berlokasi di Jawa Timur. Website ini merupakan salah satu platform penting yang digunakan oleh kantor untuk berinteraksi dengan publik, menyediakan informasi, dan melakukan transaksi online. Keamanan website adalah aspek kritis yang harus diperhatikan, mengingat meningkatnya ancaman siber dalam beberapa tahun terakhir. Metode analisis kerentanan digunakan untuk mengidentifikasi potensi celah keamanan yang dapat dieksploitasi oleh penyerang. Berbagai alat keamanan siber, termasuk Burp Suite, Unicornscan, dan Whatweb, digunakan dalam penelitian ini untuk mengidentifikasi kerentanan potensial. Selain itu, pengujian penetrasi dilakukan untuk memeriksa kerentanan secara menyeluruh. Hasil analisis kerentanan menunjukkan beberapa temuan kritis yang perlu segera diperbaiki oleh Kantor XY. Temuan tersebut mencakup kerentanan terhadap injeksi SQL, serangan XSS (Cross-Site Scripting), serta masalah terkait konfigurasi server dan aplikasi. Selain itu, ditemukan kerentanan terkait CSRF (Cross-Site Request Forgery) yang dapat memengaruhi integritas data. Studi ini memberikan gambaran mendalam tentang kerentanan website Kantor XY dan memberikan rekomendasi keamanan yang dapat membantu mengatasi masalah tersebut. Melindungi website dari serangan siber adalah langkah krusial dalam menjaga data sensitif dan reputasi institusi. Kesimpulannya, analisis kerentanan ini bertujuan untuk meningkatkan keamanan website Kantor XY dan membantu melindungi informasi yang tersimpan di dalamnya dari ancaman siber.

Kata kunci : Website, Analisis Kerentanan, Keamanan Siber, XSS (Corss-Site Scripting), CSRF (Corss-Site Request Forgery).

ABSTRACT

This research aims to conduct a vulnerability analysis of the XY Office website located in East Java. This website is one of the important platforms used by the office to interact with the public, provide information and carry out online transactions. Website security is a critical aspect that must be considered, considering the increase in cyber threats in recent years. Vulnerability analysis methods are used to identify potential security gaps that can be exploited by attackers. Various cybersecurity tools, including Burp Suite, Unicornscan, and Whatweb, were used in this research to identify potential vulnerabilities. Additionally, penetration testing is performed to thoroughly check vulnerabilities. The results of the vulnerability analysis showed several critical findings that needed to be immediately corrected by XY Office. The findings include vulnerabilities to SQL injection, XSS (Cross-Site Scripting) attacks, as well as issues related to server and application configuration. Additionally, a vulnerability related to CSRF (Cross-Site Request Forgery) was discovered that could affect data integrity. This study provides an in-depth look at the vulnerabilities of the XY Office website and provides security recommendations that can help resolve the issue. Protecting a website from cyberattacks is a crucial step in safeguarding sensitive data and an institution's reputation. In conclusion, this vulnerability analysis aims to improve the security of the XY Office website and help protect the information stored on it from cyber threats.

Keywords: Website, Vulnerability Analysis, Cyber Security, XSS (Corss-Site Scripting), CSRF (Corss-Site Request Forgery).

.

LEMBAR PERSEMBAHAN

Puji syukur kepada Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini. Penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Kedua orang tua saya yaitu papa dan mama yang sudah mendukung, medoakan dan selalu memberitahu supaya segera menyelesaikan tugas akhir.
2. Bapak Zamah Sari, S.T, M.T dan Bapak Denar Regata Akbi, S.Kom, M.Kom selaku pembimbing tugas akhir yang sudah bersedia meluangkan waktu untuk membantu dalam terkait tugas akhir.
3. Ibu Dekan Fakultas Teknik Universitas Muhammadiyah Malang.
4. Bapak Ketua Jurusan Informatika Universitas Muhammadiyah Malang.
5. Teman-temanku yang sudah selalu mengingatkan untuk mengerjakan dan membantu walaupun hanya memberikan saran saja.

Malang, 7 Juli 2023

Muchammad Zaidan

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT. Atas limpahan rahmat dan hidah-NYA sehingga peneliti dapat menyelesaikan tugas akhir yang berjudul :

"Eksplorasi Keamanan Website Dinas XY di Jawa Timur dalam Pendekatan Pengujian Brute Force untuk mendeteksi kerentanan"

Di dalam tulisan ini disajikan pokok – pokok bahasan yang meliputi pendahuluan, studi literatur, metode penelitian dan hasil penelitian yang telah didapatkan dari hasil penelitian dan disimpulkan berdasarkan hasil yang telah di dapat oleh peneliti. Peneliti menyadari sepenuhnya bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dan keterbatasan. Oleh karena itu, peneliti mengharapkan saran yang membangun agar tulisan ini bermanfaat bagi perkembangan ilmu pengetahuan.

Malang, 7 Juli 2023

Muchammad Zaidan

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

[1] A. Jamil, K. Asif, R. Ashraf, S. Mehmood, and G. Mustafa, "A comprehensive study of cyber attacks & counter measures for web systems," in Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, Amman Jordan: ACM, Jun. 2018, pp. 1–7. doi: 10.1145/3231053.3231116.

[2] A. A. Ali and M. Zamri Murah, "Security Assessment of Libyan Government Websites," Proceedings of the 2018 Cyber Resilience Conference, CRC 2018, pp. 1–4, 2019, doi: 10.1109/CR.2018.8626862.

[3] A. F. Maskur and Y. Dwi Wardhana Asnar, "Static Code Analysis Tools with the Taint Analysis Method for Detecting Web Application Vulnerability," Proceedings of 2019 International Conference on Data and Software Engineering, ICoDSE 2019, 2019, doi: 10.1109/ICoDSE48700.2019.9092614.

[4] G. Dong, F. Liu, and G. Wu, "A Website's Network Attack Analysis and Security Countermeasures," Procedia Comput Sci, vol. 208, pp. 577–582, 2022, doi: 10.1016/j.procs.2022.10.080.

[5] D. Arnaldy and A. R. Perdana, "Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack," Proceedings - 2019 2nd International Conference of Computer and Informatics Engineering: Artificial Intelligence Roles in Industrial Revolution 4.0, IC2IE 2019, pp. 188–192, 2019, doi: 10.1109/IC2IE47452.2019.8940872.

[6] A. Goutam and V. Tiwari, "Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application," 2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019, pp. 601–605, 2019, doi: 10.1109/ISCON47742.2019.9036175.

[7] R. S. Devi, "Testing for Security Weakness of Web Applications using Ethical Hacking," Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020, pp. 354–361, 2020, doi: 10.1109/ICOEI48184.2020.9143018.

[8] I. G. N. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman, “Web vulnerability assessment and maturity model analysis on Indonesia higher education,” Procedia Comput Sci, vol. 161, pp. 1165– 1172, 2019, doi: 10.1016/j.procs.2019.11.229.

[9] P. Pant et al., “Authentication and Authorization in Modern Web Apps for Data Security Using Nodejs and Role of Dark Web,” Procedia Comput Sci, vol. 215, pp. 781–790, 2022, doi: 10.1016/j.procs.2022.12.080.

[10] Y. Zhuang, Y. Choi, S. He, A. C. M. Leung, G. M. Lee, and A. Whinston, “Understanding Security Vulnerability Awareness, Firm Incentives, and ICT Development in Pan-Asia,” Journal of Management Information Systems, vol. 37, no. 3, pp. 668–693, 2020, doi: 10.1080/07421222.2020.1790185.

[11] A. Tiwari, J. Prakash, S. Groß, and C. Hammer, “A Large Scale Analysis of Android — Web Hybridization,” Journal of Systems and Software, vol. 170, p. 110775, 2020, doi: 10.1016/j.jss.2020.110775.

[12] M. Liu, B. Zhang, W. Chen, and X. Zhang, “A Survey of Exploitation and Detection Methods of XSS Vulnerabilities,” IEEE Access, vol. 7, pp. 182004–182016, 2019, doi: 10.1109/ACCESS.2019.2960449.

[13] K. Kritikos, K. Magoutis, M. Papoutsakis, and S. Ioannidis, “A survey on vulnerability assessment tools and databases for cloud-based web applications,” Array, vol. 3–4, p. 100011, Sep. 2019, doi: 10.1016/j.array.2019.100011.

[14] M. Moniruzzaman, F. Chowdhury, and M. S. Ferdous, “Measuring Vulnerabilities of Bangladeshi Websites,” 2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019, pp. 1–7, 2019, doi: 10.1109/ECACE.2019.8679426.

[15] K. Sinchana, C. Sinchana, H. L. Gururaj, and B. R. Sunil Kumar, “Performance Evaluation and Analysis of various Network Security tools,” Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019, no. Icces, pp. 644–650, 2019, doi: 10.1109/ICCES45898.2019.9002531.

[16] I. Alsmadi and F. Mira, “Website security analysis: Variation of detection methods and decisions,” 21st Saudi Computer Society National Computer Conference, NCC 2018, pp. 1–5, 2018, doi: 10.1109/NCG.2018.8592962.

[17] H. Poston, “Mapping the OWASP Top Ten to Blockchain,” Procedia Comput Sci, vol. 177, pp. 613– 617, 2020, doi: 10.1016/j.procs.2020.10.087.

[18] S. K. Shandilya, C. Ganguli, I. Izonin, and Prof. A. K. Nagar, “Cyber attack evaluation dataset for deep packet inspection and analysis,” Data Brief, vol. 46, p. 108771, Feb. 2023, doi: 10.1016/j.dib.2022.108771.

[19] L. Erdődi, Å. Å. Sommervoll, and F. M. Zennaro, “Simulating SQL injection vulnerability exploitation using Q-learning reinforcement learning agents,” Journal of Information Security and Applications, vol. 61, p. 102903, Sep. 2021, doi: 10.1016/j.jisa.2021.102903.

[20] Md. M. Hassan et al., “Broken Authentication and Session Management Vulnerability: A Case Study of Web Application.” ijssst.info, 2018. doi: 10.5013/ijssst.a.19.02.06.

[21] A. W. Marashdih, Z. F. Zaaba, K. Suwais, and N. A. Mohd, “Web Application Security: An Investigation on Static Analysis with other Algorithms to Detect Cross Site Scripting,” Procedia Comput Sci, vol. 161, pp. 1173–1181, 2019, doi: 10.1016/j.procs.2019.11.230.

[22] G. Kaur, B. Pande, A. Bhardwaj, G. Bhagat, and S. Gupta, “Efficient yet Robust Elimination of XSS Attack Vectors from HTML5 Web Applications Hosted on OSN-Based Cloud Platforms,” Procedia Comput Sci, vol. 125, pp. 669–675, 2018, doi: 10.1016/j.procs.2017.12.086.

[23] F. Caturano, G. Perrone, and S. Pietro Romano, “Discovering reflected cross-site scripting vulnerabilities using a multiobjective reinforcement learning environment,” Comput Secur, vol. 103, p. 102204, Apr. 2021, doi: 10.1016/j.cose.2021.102204.

[24] M. Krishnan, Y. Lim, S. Perumal, and G. Palanisamy, “Detection and defending the XSS attack using novel hybrid stacking ensemble learning-

based DNN approach," Digital Communications and Networks, p. S2352864822001997, Oct. 2022, doi: 10.1016/j.dcan.2022.09.024.

[25] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," 2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017, pp. 1–6, 2018, doi: 10.1109/ICCUBEA.2017.8463920.

[26] A. Wijayanto, E. Utami, and A. B. Prasetio, "Analysis of Vulnerability Webserver Office Management of Information And Documentation Diskominfo using OWASP Scanner," in 2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS), Manado, Indonesia: IEEE, Oct. 2020, pp. 1–5. doi: 10.1109/ICORIS50180.2020.9320833.

[27] M. Agreindra Helmiawan, E. Firmansyah, I. Fadil, Y. Sofivan, F. Mahardika, and A. Guntara, "Analysis of Web Security Using Open Web Application Security Project 10," 2020 8th International Conference on Cyber and IT Service Management, CITSM 2020, 2020, doi: 10.1109/CITSM50537.2020.9268856.

[28] R. Rojas, A. Muedas, and D. Mauricio, "Security maturity model of web applications for cyber attacks," in Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur Malaysia: ACM, Jan. 2019, pp. 130–137. doi: 10.1145/3309074.3309096.

[29] S. Alazmi and D. C. De Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," IEEE Access, vol. 10, pp. 33200–33219, 2022, doi: 10.1109/ACCESS.2022.3161522.

[30] N. Karangle, A. K. Mishra, and D. A. Khan, "Comparison of Nikto and Uniscan for measuring URL vulnerability," in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India: IEEE, Jul. 2019, pp. 1–6. doi: 10.1109/ICCCNT45670.2019.8944463.

[31] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," in 2020 4th International Conference

on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India: IEEE, Jun. 2020, pp. 354–361. doi: 10.1109/ICOEI48184.2020.9143018.

[32] J. Pauli, “Web Server Hacking,” in The Basics of Web Hacking, Elsevier, 2013, pp. 19–40. doi: 10.1016/B978-0-12-416600-4.00002-2.

[33] K. V. V. N. L. Sai Kiran, R. N. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, “Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques,” Procedia Comput Sci, vol. 171, pp. 2372–2379, 2020, doi: 10.1016/j.procs.2020.04.257.

[34] I. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman, “Web Vulnerability Assessment and Maturity Model Analysis on Indonesia Higher Education,” Procedia Comput Sci, vol. 161, pp. 1165– 1172, 2019, doi: 10.1016/j.procs.2019.11.229.

[35] A. Subasi and E. Kremic, “Comparison of Adaboost with MultiBoosting for Phishing Website Detection,” Procedia Comput Sci, vol. 168, pp. 272–278, 2020, doi: 10.1016/j.procs.2020.02.251.

[36] A. F. Otoom, W. Eleisah, and E. E. Abdallah, “Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks,” Procedia Comput Sci, vol. 220, pp. 291–298, 2023, doi: 10.1016/j.procs.2023.03.038.

[37] Q. Zhou, J. Yu, and D. Li, “A dynamic and lightweight framework to secure source addresses in the SDN-based networks,” Computer Networks, vol. 193, p. 108075, Jul. 2021, doi: 10.1016/j.comnet.2021.108075.

[38] H. Poston, “Mapping the OWASP Top Ten to Blockchain,” Procedia Comput Sci, vol. 177, pp. 613– 617, 2020, doi: 10.1016/j.procs.2020.10.087.

[39] F. Caturano, G. Perrone, and S. Pietro Romano, “Discovering reflected cross-site scripting vulnerabilities using a multiobjective reinforcement learning environment,” Comput Secur, vol. 103, p. 102204, Apr. 2021, doi: 10.1016/j.cose.2021.102204.

[40] G. De Carvalho Bertoli et al., “An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System,” IEEE Access, vol. 9, pp. 106790–106805, 2021, doi: 10.1109/ACCESS.2021.3101188.

[41] E. Filiol, F. Mercaldo, and A. Santone, “A Method for Automatic Penetration Testing and Mitigation: A Red Hat Approach,” Procedia Comput Sci, vol. 192, pp. 2039–2046, 2021, doi: 10.1016/j.procs.2021.08.210.

[42] J.-S. Cho, S.-S. Yeo, and S. K. Kim, “Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value,” Comput Commun, vol. 34, no. 3, pp. 391–397, Mar. 2011, doi: 10.1016/j.comcom.2010.02.029.

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **Muchammad Zaidan**

NIM : **201810370311025**

Judul TA : **Eksplorasi Keamanan Website Dinas XY di Jawa Timur dalam Pendekatan Pengujian Brute Force untuk Mendeteksi Kerentanan**

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	2 %
2.	Bab 2 – Daftar Pustaka	25 %	0 %
3.	Bab 3 – Analisis dan Perancangan	25 %	0 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	9 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	1 %
6.	Makalah Tugas Akhir	20%	2 %

**) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)*

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

(.....)