Analisis Vulnerability Sistem Manajemen Tugas Akhir (Simanta) Universitas Muhammadiyah Malang

Laporan Tugas Akhir

Diajukan Untuk Memenuhi

Persyaratan Guna Meraih Gelar Sarjana

Informatika Universitas Muhammadiyah Malang

Yanuar Ardiansah 201910370311411

Bidang Minat:

Sistem Keamanan Jaringan

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2024

LEMBAR PERSETUJUAN

Analisis Vulnerability Sistem Manajemen Tugas Akhir (Simanta) Universitas Muhammadiyah Malang

TUGAS AKHIR

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

Menyetujui,
Malang, *22 November 2024*

Dosen Pembimbing 1	Dosen Pembimbing 2
Luqman Hakim S.Kom., M.Kom.	**Ir Denar Regata Akbi S.Kom., M.Kom.**
NIP. 10819030658PNS.	**NIP. 10816120591PNS.**

LEMBAR PENGESAHAN

Analisis Vulnerability Sistem Manajemen Tugas Akhir (Simanta)
Universitas Muhammadiyah Malang

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

Yanuar Ardiansah
201910370311411

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji
pada tanggal 22 November 2024

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Diah Risqiwati ST., MT.	**Ir. Wildan Suharso S.Kom., M.Kom**
NIP. 10814100545PNS.	**NIP. 10817030596PNS.**

Mengetahui,
Ketua Jurusan Informatika

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : YANUAR ARDIANSAH

NIM : 201910370311411

FAK./JUR. : TEKNIK / INFORMATIKA

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Analisis Vulnerability Sistem Manajemen Tugas Akhir (Simanta) Universitas Muhammadiyah Malang"** 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.

Malang, 22 November 2024

Yang membuat pernyataan

Yanuar Ardiansah

Mengetahui,

Pembimbing 1	Pembimbing 2
Luqman Hakim S.Kom., M.Kom.	**Ir. Denar Regata Akbi S.Kom., M.Kom.**
NIP. 10819030658PNS.	**NIP. 10816120591PNS.**

ABSTRAK

Keamanan website akademik merupakan tindakan dan praktik yang diterapkan untuk melindungi situs web yang berhubungan dengan institusi pendidikan, seperti universitas atau sekolah, dari berbagai ancaman dan serangan. Sebuah sistem yang dapat membantu proses pelaksanaan kegiatan penyusunan Tugas Akhir (TA) oleh mahasiswa mulai dari proses pendaftaran sampai dengan proses kelulusan atau yudisium. Penelitian ini bertujuan untuk memberikan informasi terhadap pihak institusi web terkait untuk lebih meingkatkan segi keamanan agar tidak terjadinya kebocoran data. Penelitian ini menggunakan metode *penetration testing* sekaligus untuk mengukur tingkatan keamanan dari tertingga hingga terendah dengan OWASP Top 10. Hasil dari penelitian ini berupa *reporting* atau laporan yang telah di analisa mengenai kerentanan ditemukan. Hasil yang ditemukan pada *vulnerability scanning* dengan *tools nessus* berjumlah 34 kerentanan, OWASP ZAP berjumlah 19 yang dikategorikan menjadi 4 yaitu *critical*, *high*, *medium*, *low*, dan *info*. Pada serangan *penetration testing* yang dilakukan berupa file tersembunyi yang terpbuka tercara publik.

Kata kunci: Penetration Testing, Web Akademik, Hidden File Found, Nessus, Pemindaian Kerentanan Web

ABSTRACT

Academic website security is an action and practice implemented to protect websites related to educational institutions, such as universities or schools, from various threats and attacks. A system that can assist the process of implementing the Final Assignment (TA) preparation activities by students starting from the registration process to the graduation or graduation process. This study aims to provide information to related web institutions to further improve security aspects so that data leakage does not occur. This study uses the penetration testing method as well as to measure the level of security from the highest to the lowest with OWASP Top 10. The results of this study are in the form of reporting or reports that have been analyzed regarding the vulnerabilities found. The results found in vulnerability scanning with the nessus tool amounted to 34 vulnerabilities, OWASP ZAP amounted to 19 which were categorized into 4, namely critical, high, medium, low, and info. In the penetration testing attack carried out in the form of hidden files that are open to the public.

Keywords: Penetration Testing, Academic Web, Hidden File Found, Nessus, Web Vulnerability Scanning

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT. Atas limpahan rahmat dan hidayah-NYA sehingga peneliti dapat menyelesaikan tugas akhir yang berjudul: "**Analisis Vulnerability Sistem Manajemen Tugas Akhir (Simanta) Universitas Muhammadiyah Malang**".

Peneliti menyadari bahwa penyusunan skripsi ini jauh dari sempurna, itu semua berkat doa, bantuan dan dukungan yang selalu diberikan oleh orang-orang terdekat saya dan pihak yang bersangkutan. Semoga Allah SWT memberikan balasan yang berlipat ganda pada semua pihak yang telah turut membantu penulis dalam menyelesaikan penulisan skripsi ini.

Oleh karena itu, penulis berharap atas saran dan kritik yang bersifat membangun dari pembaca. Akhir kata penulis mengucapkan terima kasih sebesarbesarnya kepada semua pihak yang bersangkutan dalam membantu proses penelitian ini. Peneliti berharap tujuan dari pembuatan skripsi ini dapat tercapai sesuai yang diharapkan.

Malang, 22 November 2024

Yanuar Ardiansah

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

[1] S. Hidayatulloh dan D. Saptadiaji, “Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP),” *Jurnal Algoritma*, vol. 18, no. 1, pp. 77-86, 2021.

[2] S. R. A. Dalimuthe dan M. Amin, “Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus,” *Prosiding Seminar Nasional Riset Information Science (SENARIS)*, vol. 1, p. 994, 2019.

[3] F. Fachri, A. Fadlil and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *Jurnal Informatika*, vol. 8, no. 2, pp. 183190, September 2021.

[4] Y. W, I. Riadi and A. Yudhana, "Analisis Deteksi Vulnerability Pada Web Server Open Journal System Menggunakan OWASP Scanner," *Jurnal Rekayasa Teknologi Informasi (JURTI)*, vol. 2, no. 1, p. 1, Juni 2018.

[5] A. Zirwan, “Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner,” *Jurnal Informasi dan Teknologi*, vol. 4, no. 1, pp. 70-75, 2022.

[6] A. M. Ibrahim, T. Defisa, H. B. Seta and I. W. Widi P, "Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT)," *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)*, 14 April 2022.

[7] M. A. Mu'min, A. Fadlil and I. Riadi, "Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 3, pp. 1468-1475, 2022.

[8] Y. A. Elanda and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan

OWASP Top 10," *CESS (Journal of Computer Engineering, System and Science)*, vol. 6, no. 2, pp. 185-191, 31 Juli 2021.

[9] I. Mukhopadhyay, S. Goswami and E. Mandal, "Web Penetration Testing using Nessus and Metasploit Tool," *IOSR Journal of Computer Engineering*, vol. 16, no. 3, pp. 126-129, 2014.

[10] Hendra and E. Budhy, "Peningkatan Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Jakarta Melalui Klasifikasi Serangan Cyber Dalam Menunjang WFH," *Seminar Nasional Sains dan Teknologi*, 2021.

[11] A. W. Kuncoro and F. Rahma, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," *AUTOMATA*, vol. 3, no. 1, 2022.

[12] I. K. Bayu, M. Yamin and L. F. Aksara, "ANALISA KEAMANAN JARINGAN WLAN DENGAN METODE PENETRATION TESTING (STUDI KASUS : LABORATORIUM SISTEM INFORMASI DAN PROGRAMMING TEKNIK INFORMATIKA UHO)," *semanTIK*, vol. 3, no. 2, pp. 69-78, 2017.

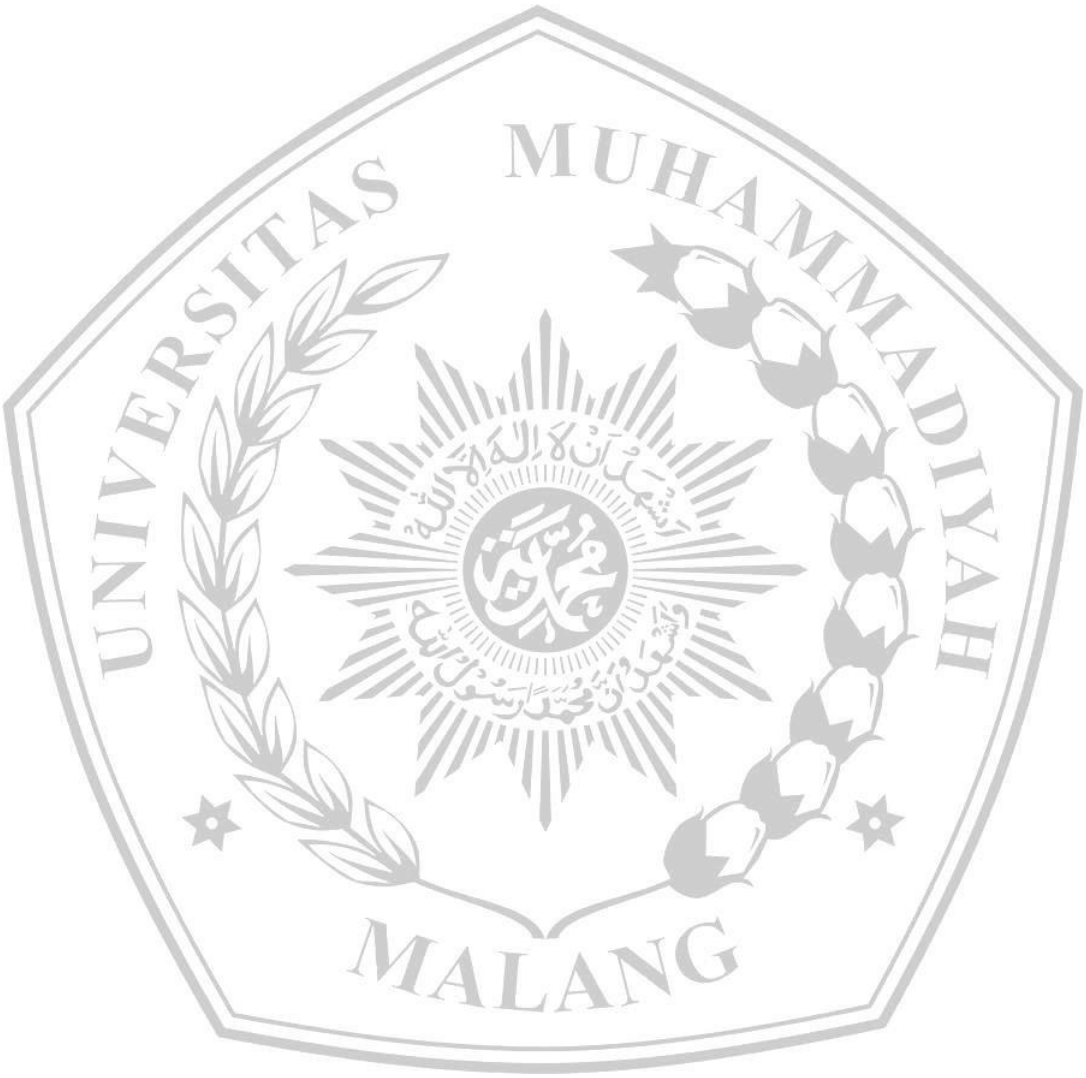
[13] B. T. K. Dewi and M. A. Setiawan, "Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web," *AUTOMATA*, vol. 3, no. 1, 2022.

[14] F. Wibowo, Harjono and A. P. Wicaksono, "Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS," *JURNAL INFORMATIKA*, vol. 6, no. 2, pp. 212-218, 2019.

[15] M. Orisa and M. Ardita, "VULNERABILITY ASSESMENT UNTUK MENINGKATKAN KUALITAS KEMANAN WEB," *Jurnal MNEMONIC*, vol. 4, no. 1, pp. 16-19, 2021.

[16] E. I. Alwi and L. B. Ilmawan, "Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment," *INFORMATICS JOURNAL (INFORMAL)*, vol. 6, no. 3, pp.

131-135, 20 12 2021.
[17] Nessus, “Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing,” 2001. https://www.tenable.com/plugins/nessus/10756.



UNIVERSITAS
MUHAMMADIYAH
MALANG

FAKULTAS TEKNIK

INFORMATIKA
informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **Yanuar Ardiansah**

NIM : **201910370311411**

Judul TA : **Analisis Vulnerability Sistem Manajemen Tugas Akhir (Simanta) Universitas Muhammadiyah Malang**

Hasil Cek Plagiarisme dengan Turnitin

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

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

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

Mengetahui,

Pemeriksa (Staff TU)

(.....)