PENETRATION TESTING WEBSITE PT. SEKARLAUT TBK MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT(OWASP) STANDART TOP 10

Tugas Akhir

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

Jalaludin Muhammad Akbar
(201910370311331)

Bidang Minat
(Jaringan)

PROGRAM STUDI INFORMATIKAFAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2024

LEMBAR PERSETUJUAN

PENETRATION TESTING WEBSITE PT. SEKARLAUT TBK MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT(OWASP) STANDART TOP 10

TUGAS AKHIR

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

Menyetujui,
Malang, *7 Juni 2024*

Dosen Pembimbing 1	Dosen Pembimbing 2
Luqman Hakim S.Kom., M.Kom.	**-**
NIP. 10819030658PNS.	**NIP.**

LEMBAR PENGESAHAN

PENETRATION TESTING WEBSITE PT. SEKARLAUT TBK MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT(OWASP) STANDART TOP 10

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

Jalaludin Mohammad Akbar

201910370311331

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 7 Juni 2024

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Ir. Mahar Faiqurahman S.Kom., M.T.	**Diah Risqiwati ST., MT.**
NIP. 10808110462PNS.	**NIP. 10814100545PNS.**

Mengetahui,
Ketua Jurusan Informatika

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : **JALALUDIN MUHAMMAD AKBAR**
NIM : **201910370311331**
FAK./JUR. : **Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Penetration Testing Website Pt. Sekarlaut TBK Menggunakan Open Web Application Security Project(OWASP) Standart top 10"** 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

Luqman Hakim S.Kom., M.Kom.

Malang, 26 April 2024
Yang [illegible]an

JALALUDIN MUHAMMAD AKBAR

ABSTRAK

Perkembangan ini teknologi menunjukkan perkembangannya yang begitu pesat dan penggunanya dituntut untuk semakin berkembang. Tentunya berbagai pihak yang tidak bertanggung jawab memakai internet dengan tidak bijak terutama pada website di sebuah perusahaan maupun sekolah. PT. Sekar Laut Tbk. ialah perusahaan yang bergerak di berbagai bidang khususnya industri di sektor makanan dan minuman. PT. Sekar Laut Tbk. mempunyai website sistem informasi yang didalamnya terdapat data-data penting perusahaan, namun dari sisi keamanannya masih belum diperhatikan. Berdasarkan latar belakang tersebut, perlu evaluasi mengenai celah keamanan(*vulnerability*) pada website sistem informasi PT. Sekar Laut Tbk. Metode penelitian yang digunakan penetrations testing dengan standar OWASP dengan memakai sejumlah tools yang ada di sistem operasi linux dan windows. Hasil pengujian penetration testing mendapatkan beberapa kelemahan, injection, sensitive data Exposure, cross site scripting (XSS).

Kata kunci— vulnerability; OWASP; penetration testing

KATA PENGANTAR

Puji syukur ke hadirat Allah Yang Maha Pengasih Lagi Maha Penyayang atas rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir. Shalawat serta salam tidak lupa penulis hanturkan kepada junjungan kita, Nabi Muhammad Shallallahu 'alaihi wasallam. Laporan ini dibuat untuk memenuhi persyaratan kelulusan di Fakultas Teknik Informatika, Universitas Muhammadiyah Malang dengan judul "Penetration Testing Website Pt. Sekarlaut TBK Menggunakan Open Web Application Security Project(OWASP) Standart top 10". Penulis bersyukur dapat mengerjakan dengan maksimal dan menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu dan memberikan dukungan selama proses pengerjaan, penulis juga mengucapkan terima kasih kepada:

1. Seluruh dosen Prodi Informatika yang telah mendampingi selama perkuliahan
2. Bapak Luqman Hakim, S.Kom., M.Kom. selaku Dosen Pembimbing Tugas Akhir
3. Kedua Orang Tua tercinta dan keluarga yang selalu mendukung dan mendoakan penulis
4. Teman seperjuangan Abdur, Yusuf, Hadid, Rafi dan Moriz yang telah berjuang bersama selama perkuliahan
5. Teman-teman kelas G dan lainnya yang selalu membersamai penulis selama perkuliahan

Semoga segala kebaikan dan dukungan semuanya mendapat balasan dari Allah Subhanahu wa ta'ala, dan akhirnya penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna, karena keterbatasan ilmu yang penulis miliki. Untuk itu penulis dengan kerendahan hati mengharapkan saran dan kritik yang sifatnya membangun dari semua pihak demi membangun laporan penelitian.

Malang, 30 April 2024

Jalaludin Muhammad A

Daftar Isi

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

[1] R. Pangalila, A. Noertjahyana, and J. Andjarwirawan, "Penetration Testing Server Sistem Informasi Manajemen," *Penetration Test. Serv. Sist. Inf. Manaj. dan Website Univ. Kristen Petra*, pp. 1–6, 2015.

[2] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *J. Inf. dan Teknol.*, vol. 4, no. 1, pp. 70–75, 2022, doi: 10.37034/jidt.v4i1.190.

[3] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[4] Y. Yudiana, 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 Comput. Eng. Syst. Sci.*, vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.

[5] M. A. Mu'min, A. Fadlil, and I. Riadi, "Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework," *J. Media Inform. Budidarma*, vol. 6, no. 3, p. 1468, 2022, doi: 10.30865/mib.v6i3.4099.

[6] M. Rafi Ramdani, N. Heryana, and A. Susilo Yuda Irawan, "Penetration Testing pada Website Universitas Singaperbangsa Karawang Menggunakan Open Web Application Security Project (OWASP)," *J. Pendidik. dan Konseling*, vol. 4, no. 4, pp. 5522–5529, 2022.

[7] V. Varma Vegesna, "Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks," vol. XII, no. Vii, pp. 81–94, [Online]. Available: https://ssrn.com/abstract=4612524

[8] A. M. Ibrahim, T. Defisa, and H. B. Seta, "Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT)," *… Mhs. Bid. Ilmu …*, no. April, pp. 312–325, 2022, [Online]. Available: https://conference.upnvj.ac.id/index.php/senamika/article/view/2002%0Ahttps://conference.upnvj.ac.id/index.php/senamika/article/download/2002/1544

[9] OWASP, "The ten Most Critical Web Application Security Risk," 2017. http://www.owasp.org

[10] I. Chalvatzis, "Reproducible modelling and simulating security vulnerability scanners evaluation framework towards risk management assessment of small and medium enterprises business networks," *Indian J. Sci. Technol.*, vol. 13, no. 37, pp. 3910–3943, 2020, doi: 10.17485/ijst/v13i37.868.

[11] O. ZAP, "ZAPping the OWASP Top 10," 2020. https://www.zaproxy.org/docs/guides/zappingthe-top-10/

[12] E. A. Altulaihan, A. Alismail, and M. Frikha, "A Survey on Web Application Penetration Testing," *Electron.*, vol. 12, no. 5, 2023, doi: 10.3390/electronics12051229.

[13] H. Haeruddin and A. Kurniadi, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6)," Comb. Manag. …, vol. 1, no. 1, pp. 508–515, 2021, [Online]. Available:

[14] K. Paulina, "Penetration Testing Open Journal Systems (Ojs) Pada Aplikasi Web Jurnal Ji-Tech," vol. 1, no. 1, pp. 37–45, 2023.

[15] A. W. Wasis Wardana, Ahmad Almaarif, “Vulnerability Assessment and Penetration Testing On the xyz Website Using NIST 800-115 Standard,” J. Ilm. Indones. p–ISSN 2541-0849 e-ISSN 2548-1398, vol. Vol. 7, 2022.

[16] E. Hacker, “Certifi ed Ethical Hacker.”

[17] S. A. Rahalkar, Certified Ethical Hacker (CEH) Foundation Guide

UNIVERSITAS MUHAMMADIYAH MALANG

FAKULTAS TEKNIK

INFORMATIKA

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

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **Jalaludin Mohammad Akbar**

NIM : **201910370311331**

Judul TA : **PENETRATION TESTING WEBSITE PT. SEKARLAUT TBK MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT(OWASP) STANDART TOP 10**

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	7%
2.	Bab 2 – Daftar Pustaka	25 %	19%
3.	Bab 3 – Analisis dan Perancangan	25 %	20%
4.	Bab 4 – Implementasi dan Pengujian	15 %	8%
5.	Bab 5 – Kesimpulan dan Saran	5 %	0%
6.	Makalah Tugas Akhir	20%	17%

Mengetahui,

Pemeriksa (Staff TU)

(.....)

Kampus I
Jl. Bandung 1 Malang, Jawa Timur
P: +62 341 551 253 (Hunting)
F: +62 341 460 435

Kampus II
Jl. Bendungan Sutami No.188 Malang, Jawa Timur
P: +62 341 551 149 (Hunting)
F: +62 341 582 060

Kampus III
Jl. Raya Tlogomas No.246 Malang, Jawa Timur
P: +62 341 464 318 (Hunting)
F: +62 341 460 435
E: webmaster@umm.ac.id