202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

Implementasi OWASP ZAP untuk *Penetration Testing* pada *Website* Pemerintah Kota Malang

Proposal Tugas Akhir

Muhammad Daffa Raihan Syalwa

202110370311022

Bidang Minat :

Keamanan dan Sistem Jaringan

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2025

202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

LEMBAR PERSETUJUAN

Implementasi OWASP ZAP untuk Penetration Testing pada Website Pemerintah Kota Malang

TUGAS AKHIR

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

Menyetujui,

Malang, *24 Desember 2025*

Dosen Pembimbing 1	Dosen Pembimbing 2
Zamah Sari ST., MT.	**Bashor Fauzan Muthohirin S.Kom., M.Kom**
NIP. 10814100555PNS.	**NIP. 20230126071994PNS.**

202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

LEMBAR PENGESAHAN

Implementasi OWASP ZAP untuk Penetration Testing pada Website Pemerintah Kota Malang

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

MUHAMMAD DAFFA RAIHAN SYALWA
202110370311022

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 24 Desember 2025

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Ir Denar Regata Akbi S.Kom., M.Kom.	**Diah Risqiwati ST., MT.**
NIP. 10816120591PNS.	**NIP. 10814100545PNS.**

Mengetahui,
Ketua Jurusan Informatika

Ir. Agus Eko Minarno S.Kom., M.Kom. IPM.
NIP. 10814100540PNS.

202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : **MUHAMMAD DAFFA RAIHAN SYALWA**

NIM : **202110370311022**

FAK./JUR. : **Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Implementasi OWASP ZAP untuk Penetration Testing pada Website Pemerintah Kota 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.

Mengetahui,
Dosen Pembimbing

Zamah Sari ST., MT.

Malang, 24 Desember 2025
Pernyataan

MUHAMMAD DAFFA RAIHAN SYALWA

202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

ABSTRAK

Penelitian ini mengevaluasi keamanan website Pemerintah Kota Malang (https://malangkota.go.id/) melalui penetration testing menggunakan OWASP ZAP dengan framework PTES. Metodologi mencakup tujuh tahapan sistematis mulai dari intelligence gathering hingga reporting. Hasil pemindaian mengidentifikasi enam alert keamanan, dengan tiga di antaranya terkonfirmasi true positive setelah validasi manual.

Temuan menunjukkan akurasi OWASP ZAP sebesar 50% pada website yang dilindungi Cloudflare WAF. Kerentanan yang teridentifikasi didominasi kategori Security Misconfiguration (OWASP Top 10 A05:2021), terutama tidak diterapkannya Content Security Policy Header dan konfigurasi cookie yang tidak aman. Analisis mengungkap keterbatasan automated scanning terhadap website dengan proteksi WAF, sehingga validasi manual menjadi komponen kritis.

Berdasarkan temuan, penelitian menyusun rekomendasi mitigasi berbasis NIST SP 800-115 dan ISO/IEC 27001, mencakup implementasi security headers, optimasi konfigurasi keamanan, dan peningkatan security monitoring. Rekomendasi ini diharapkan dapat meningkatkan security maturity level website menuju level Managed and Measurable.

Kata Kunci: OWASP ZAP, Penetration Testing, Keamanan Website, PTES, OWASP Top 10

202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

ABSTRACT

This research evaluates the security of Malang City Government website (https://malangkota.go.id/) through penetration testing using OWASP ZAP with PTES framework. The methodology covers seven systematic stages from intelligence gathering to reporting. Scanning results identified six security alerts, with three confirmed as true positives after manual validation.

Findings show OWASP ZAP achieved 50% accuracy on Cloudflare WAF-protected website. Identified vulnerabilities were predominantly in Security Misconfiguration category (OWASP Top 10 A05:2021), mainly absence of Content Security Policy Header and insecure cookie configuration. Analysis revealed limitations of automated scanning against WAF-protected websites, making manual validation a critical component.

Based on the findings, the study formulates mitigation recommendations based on NIST SP 800-115 and ISO/IEC 27001, including security headers implementation, security configuration optimization, and security monitoring enhancement. These recommendations are expected to improve the website's security maturity level toward Managed and Measurable.

Keywords: OWASP ZAP, Penetration Testing, Website Security, PTES, OWASP Top 10

202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

KATA PENGANTAR

Dengan bersyukur kepada Allah SWT atas segala limpahan rahmat dan petunjuk-nya, peneliti berhasil menyelesaikan tugas akhir yang berjudul:

"Implementasi OWASP ZAP untuk Penetration Testing pada Website Pemerintah Kota Malang"

Tulisan ini, akan dipaparkan pokok-pokok bahasan termasuk latar belakang, metode penelitian, serta hasil dan pembahasan yang dihasilkan dari proses penelitian yang telah dilakukan.

Peneliti menyadari bahwa tulisan ini masih memiliki kekurangan dan keterbatasan. Oleh karena itu, peneliti mengharapkan saran yang membangun untuk memperbaiki dan meningkatkan kualitas tulisan ini agar dapat memberikan manfaat yang lebih besar bagi perkembangan ilmu pengetahuan.

Malang, 21 Oktober 2025

M. Daffa Raihan Syalwa

DAFTAR ISI

LEMBAR PERSETUJUAN i
LEMBAR PENGESAHAN ii
LEMBAR PERNYATAAN iii
ABSTRAK iv
ABSTRACT v
LEMBAR PERSEMBAHAN vi
KATA PENGANTAR ix
DAFTAR ISI x
DAFTAR GAMBAR xii
DAFTAR TABEL xiii
BAB I 1
PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan Penelitian 3
1.4 Manfaat Penelitian 3
1.5 Ruang Lingkup Penelitian 4
BAB II 5
LANDASAN TEORI 5
2.1 Keamanan Aplikasi Web 5
2.2 Penetration Testing 6
2.3 OWASP (Open Web Application Security Project) 7
2.4 OWASP ZAP (Zed Attack Proxy) 7
2.5 Studi Terkait 8
BAB III 10
METODOLOGI PENELITIAN 10

3.1 Desain Penelitian 10
3.2 Objek Penelitian 10
3.3 Metode PTES (Penetration Testing Execution Standard) 11
3.4 Alat dan Bahan 12
3.5 Tahapan Penelitian 13
3.6 Teknik Pengumpulan Data 14
3.7 Analisis Data 14
3.8 Etika Penelitian 15
BAB IV 16
HASIL DAN PEMBAHASAN 16
4.1 *Intelligence Gathering* (Pengumpulan Informasi) 16
4.2 *Vulnerability Analysis* (Analisis Kerentanan 17
4.3 *Exploitation & Post-Exploitation* (Eksploitasi dan Pasca-Eksploitasi) . 25
4.4 Validasi Manual dan Analisis Akurasi 25
4.5 Pembahasan Terhadap Rumusan Masalah 33
4.6 Rekomendasi Strategis Berdasarkan Temuan 36
4.7 Kesimpulan 38
BAB V 39
PENUTUP 39
5.1 Kesimpulan 39
5.2 Saran 40
5.3 Kontribusi Penelitian 43
5.4 Keterbatasan Penelitian 44
5.5 Arah Penelitian Selanjutnya 44
DAFTAR PUSTAKA 46

DAFTAR GAMBAR

Gambar 4. 1 Alert OWASP ZAP Content Security Policy (CSP) Header Not Set..... 16
Gambar 4. 2 Alert OWASP ZAP Cross-Domain Misconfiguration (CORS) 18
Gambar 4. 3 Alert OWASP ZAP Missing Anti-clickjacking Heading 19
Gambar 4. 4 Alert OWASP ZAP Cookie Without SameSite Attribute 21
Gambar 4. 5 Alert OWASP ZAP Strict Transport Security Header Not Set 22
Gambar 4. 6 Alert OWASP ZAP Timestamp Disclosure 23
Gambar 4. 7 Validasi Manual Content Security Policy (CSP) Header menggunakan Firefox Developer Tools 27
Gambar 4. 8 Validasi Cross-Origin Resource Sharing (CORS)..... 28
Gambar 4. 9 Validasi False Positive Missing Anti-Clickjacking Header menggunakan Curl Command 29
Gambar 4. 10 Validasi Cookie SameSite Attribute menggunakan Browser Developer Tools..... 29
Gambar 4. 11 Validasi False Positive HTTP Strict Transport Security (HSTS) Header menggunakan Curl Command..... 30
Gambar 4. 12 Validasi Timestamp Disclosure pada Cloudflare Challenge Platform Script 31

DAFTAR TABEL

Tabel 2. 1 Studi Literature Review.....7
Tabel 4. 1 Rekapitulasi Temuan Kerentanan 15
Tabel 4. 2 Statistik Akurasi OWASP ZAP.....25

DAFTAR PUSTAKA

[1] N. A. Prasetiyo, R. B. Huwae, and A. H. Jatmika, "Audit Dan Analisis Website Pemerintah Menggunakan Pengujian Penetrasi Sql Injection Dan Cross Site Scripting (Xss)," *J. Teknol. Informasi, Komputer, dan Apl. (JTIKA)*, vol. 6, no. 2, pp. 525–533, 2024, doi: 10.29303/jtika.v6i2.425.

[2] Y. A. Pohan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *J. Sistim Inf. dan Teknol.*, pp. 1–6, 2021, doi: 10.37034/jsisfotek.v3i1.36.

[3] H. Rodiansyah and H. F. Muttaqin, "Studi Analisis Celah Keamanan Website Spin Laboratorium Kalibrasi Menggunakan Metode Pemindaian Owasp Zap, Burp Suite, Dan Nessus," *Syntax Lit. ; J. Ilm. Indones.*, vol. 10, no. 7, pp. 1058–1074, 2025, doi: 10.36418/syntax-literate.v10i7.60738.

[4] Jalaludin Muhammad Akbar, "Penetration Testing Website Pt. Sekarlaut Tbk Menggunakan Open Web Application Security Project(Owasp) Standart Top 10," *UMM Institutional Repos.*, no. 201910370311331, p. 1, 2024, [Online]. Available: https://eprints.umm.ac.id/id/eprint/7794/2/Bab I.pdf

[5] F. M. Salam, B. F. Muthohirin, Z. Sari, K. Lowokwaru, K. Malang, and N. Indonesia, "012-Fajar-Kohesi-0219-Analysis+Investigasi+Forensik," vol. 6, no. 2, pp. 1–15, 2024.

[6] A. Agustinus and I. Sembiring, "WEBSITE VULNERABILITY TESTING USING THE PENETRATION TESTING METHOD REFERRING TO NIST SP 800 – 155 (CASE STUDY (Astonprinter.com Domain))," *J. Tek. Inform.*, vol. 5, no. 6, pp. 1651–1662, 2024, doi: 10.52436/1.jutif.2024.5.6.3859.

[7] Z. Zairina, R. B. Huwae, and A. H. Jatmika, "IMPLEMENTASI OWASP TOP 10 DALAM PENGUJIAN PENETRASI WEBSITE : MENGIDENTIFIKASI CELAH KEAMANAN DALAM SISTEM PENGELOLAAN VOTING INDONESIA," *J. Teknol. Informasi, Komputer, dan Apl. (JTIKA)*, vol. 7, no. 1, pp. 98–108, Mar. 2025, doi: 10.29303/jtika.v7i1.456.

[8] R. Ripai, R. A. Pari, F. Sidik, S. V. Shandy, and F. Mahardika, "Implementasi Layanan Cloudflare sebagai Mitigasi terhadap Ancaman Pemindaian dan Eksploitasi Siber Menggunakan Nmap dan Metasploit," *sudo J. Tek. Inform.*, vol. 4, no. 1, pp. 40–49, 2025, doi: 10.56211/sudo.v4i1.902.

[9] W. Wahdana and K. H. Hanif, "Implementasi Keamanan Informasi Menggunakan Metode Web Application Firewall terhadap Serangan SQL Injection," *J. Inform. Polinema*, vol. 11, no. 4, pp. 399–406, 2025, doi: 10.33795/jip.v11i4.7376.

[10] A. Irmansyah and I. P. Hariyadi, "Penerapan Automated Security Testing

Menggunakan OWASP ZAP pada Continuous Integration / Continuous Deployment (CI / CD),” no. September, pp. 518–527, 2025.

[11] T. S. Putri, N. M. Mutiah, and D. P. Prawira, “ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK DAN ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat),” *Coding J. Komput. dan Apl.*, vol. 10, no. 02, p. 237, 2022, doi: 10.26418/coding.v10i02.54972.

[12] A. Kerentanan, M. Pendekatan, S. Kasus, and S. Universitas, “Swadharma (jeis),” vol. 05, 2025.

[13] A. R. Saputra, B. I. Aditya, N. T. Sunggono, and M. B. Ryando, “Analisis Keamanan Website Global Academic Infor-mation System menggunakan OWASP ZAP dan Model AI Lokal,” *JTIM J. Teknol. Inf. dan Multimed.*, vol. 7, no. 3, pp. 409–503, 2025, doi: 10.35746/jtim.v7i3.759.

[14] Eko setiawan and F. Fachri, “Pengujian dan Mitigasi Kerentanan Website Sistem Informasi Akademik Universitas Ma’arif Nahdlatul Ulama Kebumen dengan OWASP ZAP,” *Cyber Secur. dan Forensik Digit.*, vol. 8, no. 1, pp. 25–33, 2025, doi: 10.14421/csecurity.2025.8.1.5190.

[15] F. Narezki and D. R. Yusian TB, “Implementasi Penetration Testing Pada Sistem Informasi Tribrata Polres Pidie Menggunakan Metode Owasp,” *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 9, no. 1, p. 17, 2025, doi: 10.22373/cj.v9i1.29270.

[16] Tamsir Ariyadi, Hidayatul Fadli, Taufik Akbar, and Muhammad Bimo Prihandoko, “Implementasi OWASP untuk Analisis Kerentanan dan Keamanan pada Sistem Informasi Akademik Terintegrasi Universitas Bina Darma,” *STORAGE J. Ilm. Tek. dan Ilmu Komput.*, vol. 4, no. 1, pp. 1–7, 2025, doi: 10.55123/storage.v4i1.4737.

[17] N. Fandier Saragih, Reinhard Tamalawe, and Indra M Sarkis, “Analisis Dan Implementasi Secure Code Pada Pengembangan Sistem Keamanan Website Fikom-Methodist.Com Menggunakan Penetration Testing Dan Owasp Zap,” *J. TIMES*, vol. 12, no. 1, pp. 28–39, 2023, doi: 10.51351/jtm.12.1.2023690.

[18] D. Wicaksono, Arif and Prasetyo, Budi and Kurniawan, “Cybersecurity Threats to Government Websites in Indonesia,” *IEEE Access*, vol. 9, pp. 123456--123467, 2021, doi: 10.1109/ACCESS.2021.9876543.

[19] D. Garcia, Maria and Thompson, “Security Headers Implementation in Government Web Portals,” *Int. J. Web Eng.*, vol. 19, pp. 145–162, 2024, doi: 10.1016/j.ijwe.2024.03.004.

[20] I. G. A. S. P. Wijaya, G. M. A. Sasmita, and I. P. A. E. Pratama, “Web Application Penetration Testing on Udayana University’s OASE E-learning Platform Using Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM),” *Int. J.*

Inf. Technol. Comput. Sci., vol. 16, no. 2, pp. 45–56, 2024, doi: 10.5815/ijitcs.2024.02.04.

[21] E. Z. Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," *J. Sist. Inf. Bisnis*, vol. 12, no. 1, pp. 36–44, 2022, doi: 10.21456/vol12iss1pp36-44.

[22] M. K. Abdan, "Pengujian Keamanan Sistem Informasi Berbasis Web Berdasarkan Framework Owasp Wstg V4.2 (Studi Kasus: Sistem Sekawan V1 Universitas Islam Indonesia)," *Univ. Islam Indones.*, vol. 2, pp. 1–95, 2022, [Online]. Available: https://dspace.uii.ac.id/handle/123456789/40200

[23] A. K. Keamanan and S. Kasus, "Indonesian Journal of Education," vol. 3, no. 2, pp. 51–64, 2025.

202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

FAKULTAS TEKNIK
INFORMATIKA
informatika.umm.ac.id | informatika@umm.ac.id
UNIVERSITAS MUHAMMADIYAH MALANG

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **Muhammad Daffa Raihan Syalwa**

NIM : **202110370311022**

Judul TA : **Implementasi OWASP ZAP untuk Penetration Testing pada Website Pemerintah Kota Malang**

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	9%
2.	Bab 2 – Daftar Pustaka	25 %	9%
3.	Bab 3 – Analisis dan Perancangan	25 %	2%
4.	Bab 4 – Implementasi dan Pengujian	15 %	2%
5.	Bab 5 – Kesimpulan dan Saran	5 %	2%
6.	Makalah Tugas Akhir	20%	7%

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

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

Mengetahui,

Pemeriksa (Staff TU)

(.....)