ANALISIS KEAMANAN WEBSITE MENGGUNAKAN METODE VULNERABILITY ASSESSMENT (STUDI KASUS: WEBSITE PEMERINTAH KABUPATEN BIMA)

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

MUHAMMAD IMAM GAFIRIN

21.83.0590

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

ANALISIS KEAMANAN WEBSITE MENGGUNAKAN METODE VULNERABILITY ASSESSMENT (STUDI KASUS: WEBSITE PEMERINTAH KABUPATEN BIMA)

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

MUHAMMAD IMAM GAFIRIN

21.83.0590

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS KEAMANAN WEBSITE MENGGUNAKAN METODE VULNERABILITY ASSESSMENT (STUDI KASUS: WEBSITE PEMERINTAH KABUPATEN BIMA)

yang disusun dan diajukan oleh

Muhammad Imam Gafirin

21.83.0590

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Juli 2025

Dosen Pembimbing,

Muhammad Rudyanto Arief, S.T, M.T
NIK. 190302098

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS KEAMANAN WEBSITE MENGGUNAKAN METODE VULNERABILITY ASSESSMENT (STUDI KASUS: WEBSITE PEMERINTAH KABUPATEN BIMA)

yang disusun dan diajukan oleh

Muhammad Imam Gafirin

21.83.0590

Telah dipertahankan di depan Dewan Penguji
pada tanggal 28 Juli 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	
Melwin Syafrizal, S.Kom., M.Eng., Ph.D. **NIK. 190302105**	
Muhammad Rudyanto Arief, ST., M.T **NIK. 190302098**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 28 Juli 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini., M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Imam Gafirin
NIM : 21.83.0590

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Keamanan *Website* Menggunakan Metode *Vulnerability Assessment* (Studi Kasus: *Website* Pemerintah Kabupaten Bima)

Dosen Pembimbing : Muhammad Rudyanto Arief, S.T, M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 28 Juli 2025

Yang Menyatakan,

Muhammad Imam Gafirin

HALAMAN PERSEMBAHAN

Alhamdulilahi rabbil'alamin puji syukur kehadirat Allah SWT. Atas limpahan dan rahmatnya sehingga penulisan skripsi ini membawa keberkahan dan manfaat tersendiri bagi penulis dan juga dapat memberikan manfaat kepada orang lain.

Dengan adanya karya ini tidak lepas dari bantuan dan dukungan dari berbagai pihak, untuk itu penulis mengucapkan terima kasih kepada:

1. Allah SWT Yang senantiasa memberikan kemudahan, kebaikan, anugerah kepada penulis sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
2. Teruntuk cinta pertama, Almarhumah Ibu Sitti Hajrah, dan Motivator hidup saya, Ayah Ramli. Terima kasih atas segala, doa, kasih sayang, dukungan moral, materi, serta pengorbanan yang tak ternilai. Semua itu menjadi kekuatan besar hingga saya dapat menyelesaikan skripsi ini dan meraih gelar Sarjana Teknik Komputer.
3. Teruntuk dua saudara saya, Kakak laki-laki Muhammad Izzul Islam dan Adik laki-laki Muhammad Fathurrahman, terima kasih atas dukungan dan semangat yang kalian berikan kepada penulis sehingga dapat menyelesaikan skripsi ini dan meraih gelar Sarjana Teknik Komputer.
4. Terima kasih kepada Bapak Muhammad Rudyanto Arief, S.T, M.T. Selaku Dosen Pembimbing, yang telah memberikan arahan selama proses penyusunan skripsi.
5. Terima kasih kepada Sri Wahyuni, yang telah menjadi sumber semangat selama proses penulisan skripsi ini. Kehadirannya saat-saat sulit, serta dukungan yang tak henti, menjadi bagian penting yang menguatkan penulis untuk menyelesaikan skripsi.

KATA PENGANTAR

Puji Syukur atas kehadirat Allah SWT yang telah memberikan Rahmat dan karuniaNya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Keamanan *Website* Menggunakan Metode *Vulnerability Assessment* (Studi Kasus: *Website* Pemerintah Kabupaten Bima)" yang diajukan sebagai salah satu syarat untuk menyelesaikan Program Strata Satu (S1) di program studi Teknik Komputer Universitas Amikom Yogyakarta.

Adapun penyusunan skripsi ini digunakan sebagai bukti bahwa penulis telah melaksanakan dan menyelesaikan penelitian skripsi. Dalam proses penyusunan skripsi ini, penulis mendapatkan bantuan dari berbagai pihak. Oleh karena itu penulis mengucapkan terima kasih banyak kepada:

1. Prof. Dr. M. Suyanto, M.M. Selaku Rektor Universitas Amikom Yogyakarta.
2. Prof. Dr. Kusrini, M.Kom. Selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Dr. Dony Ariyus, M.Kom. Selaku Ketua Program Studi Teknik Komputer Universitas Amikom Yogyakarta.
4. M. Rudyanto Arief, S.T, M.T. Selaku Dosen Pembimbing, yang telah memberikan arahan selama proses penyusunan skripsi.
5. Teman-teman sperjuangan dan seluruh pihak yang telah membantu baik secara langsung maupun tidak langsung dalam proses penyelesaian skripsi ini.

Penulis menyadari bahwa dengan keterbatasan wawasan dan serta penglaman penulis, membuat Tugas Akhir ini masih jauh dari kata sempurna. Oleh karena itu, mengharapkan kritik dan saran yang bersifat membangun. Semoga skripsi ini dapat memberikan manfaat. Akhir kata, semoga kita semua mendapatkan rahmat dan selalu ada dalam lindungan Allah SWT.

Yogyakarta, 28 Juli 2025

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

CIA	*Confidentiality, Integrity, Availability* (Triad keamanan informasi)
OWASP	*Open Web Application Security Project*
ZAP	*Zed Attack Proxy* (tool pengujian keamanan dari OWASP)
NIST	*National Institute of Standards and Technology*
SSRF	*Server Side Request Forgery*
DNS	*Domain Name System*
PII	*Personally Identifiable Information* (Informasi Identitas Pribadi)
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
SQL	*Structured Query Language*
XSS	*Cross-Site Scripting*

DAFTAR ISTILAH

Vulnerability Assessment	Proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi celah keamanan pada sistem informasi.
Non-intrusive	Pendekatan pengujian keamanan yang tidak mengeksploitasi celah secara aktif atau merusak sistem.
Information Gathering	Tahap awal dalam *vulnerability assessment* untuk mengumpulkan informasi target secara pasif.
OWASP Top 10	Daftar sepuluh kerentanan keamanan aplikasi web paling umum yang dirilis oleh OWASP sebagai standar internasional.
Cross-Domain JavaScript	Pemanggilan file JavaScript dari domain luar, yang dapat membuka potensi serangan seperti XSS.
PII Disclosure	Terbukanya informasi identitas pribadi pengguna, seperti BIN kartu atau data sensitif lainnya.
Security Misconfiguration	Pengaturan keamanan sistem yang kurang tepat atau tidak optimal, sehingga membuka potensi celah.
WHOIS	Protokol yang digunakan untuk melihat informasi pendaftaran domain, seperti nama pemilik, registrar, dan DNS server.
CVSS	Sistem standar untuk mengukur tingkat keparahan kerentanan keamanan berdasarkan sejumlah parameter teknis.

INTISARI

Perkembangan teknologi informasi telah mendorong instansi pemerintah untuk menyediakan layanan publik melalui *website* resmi. Namun, keterbukaan informasi tersebut meningkatkan risiko terhadap serangan siber. *Website* Pemerintah Kabupaten Bima sebagai sarana layanan publik digital belum memiliki dokumentasi formal mengenai pengujian keamanannya, sehingga berpotensi mengalami kebocoran data atau serangan terhadap sistem.

Penelitian ini bertujuan untuk mengidentifikasi kerentanan keamanan pada *website* tersebut menggunakan metode *Vulnerability Assessment* berbasis pendekatan *non-intrusive*, tanpa eksploitasi langsung terhadap sistem. Tools yang digunakan yaitu WHOIS dan NSLookup untuk tahap information gathering, serta OWASP ZAP versi 2.16.1 untuk melakukan pemindaian kerentanan berdasarkan acuan OWASP Top 10 Tahun 2021. Hasil pemindaian menunjukkan terdapat 13 jenis kerentanan, terdiri dari 1 kerentanan risiko tinggi (*PII Disclosure*), 3 risiko sedang, dan 9 risiko rendah, seperti konfigurasi header yang tidak aman dan *Cross-Domain JavaScript Inclusion*.

Penelitian ini memberikan kontribusi nyata dalam evaluasi awal keamanan aplikasi web pemerintah dan menyajikan rekomendasi teknis sebagai upaya mitigasi risiko. Hasil ini dapat dimanfaatkan oleh pengelola sistem informasi pemerintah daerah dan praktisi keamanan siber untuk memperkuat pertahanan digital. Penelitian lanjutan dapat dikembangkan dengan pendekatan penetration testing guna mendapatkan hasil yang lebih komprehensif.

Kata kunci: *Vulnerability Assessment*. Keamanan *Website*, OWASP, *Website*, Pemerintah Bima, Kerentanan Siber.

ABSTRACT

The advancement of information technology has encouraged government institutions to provide public services through official websites. However, such openness of information also increases the risk of cyberattacks. The official website of the Bima Regency Government, as a platform for digital public services, lacks formal documentation of security testing, which may lead to data breaches or system compromise.

This research aims to identify security vulnerabilities on the website using a non-intrusive Vulnerability Assessment approach, without actively exploiting any detected flaws. The tools used include WHOIS and NSLookup for the information gathering stage, and OWASP ZAP version 2.16.1 for vulnerability scanning based on the OWASP Top 10 2021 standard. The scanning results revealed 13 types of vulnerabilities, consisting of 1 high-risk vulnerability (PII Disclosure), 3 medium-risk, and 9 low-risk vulnerabilities, such as insecure header configurations and Cross-Domain JavaScript Inclusion.

This study contributes significantly to the initial evaluation of government web application security and provides technical recommendations as a mitigation effort. The results may be utilized by regional government IT administrators and cybersecurity practitioners to strengthen digital defenses. Future research is encouraged to adopt penetration testing approaches to obtain more comprehensive results.

Keyword**:** *Vulnerability Assessment, Website Security, OWASP, Website, Bima Government, Cyber Vulnerability*