SKRIPSI

ANALISIS KEAMANAN WEBSITE SIPATCA MENGGUNAKAN METODE PENETRATION TESTING BERBASIS ISSAF dan OWASP WSTG v4.2

Muhammad Rafi Arganta

NPM 21082010061

DOSEN PEMBIMBING

Eka Dyar Wahyuni, S.Kom., M.Kom

Iqbal Ramadhani Mukhlis, S.Kom., M.Kom

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI SISTEM INFORMASI
SURABAYA
2026

LEMBAR PENGESAHAN

ANALISIS KEAMANAN WEBSITE SIPATCA MENGGUNAKAN METODE PENETRATION TESTING BERBASIS ISSAF dan OWASP WSTG v4.2

Oleh :
MUHAMMAD RAFI ARGANTA
NPM. 21082010061

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi Prodi Sistem Informasi Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jawa Timur Pada tanggal .... Mei 2026

Eka Dyar Wahyuni, S.Kom, M.Kom
NIP. 19841201 2021212 005 ..... (Pembimbing I)

Iqbal Ramadhani Mukhlis, S.Kom., M.Kom
NIP. 199303052024061002 ..... (Pembimbing II)

Nur Cahyo Wibowo, S.Kom, M.Kom
NIP. 19790317 2021211 002 ..... (Penguji I)

Nambi Sembilu, S.Kom., M.Kom.
NIP. 199005162024061003 ..... (Penguji II)

Mohammad Al Hafidz, S.Kom., M.Kom.
NIP. 199109222025061003 ..... (Penguji III)

Mengetahui,
Dekan Fakultas Ilmu Komputer

Prof. Dr. Ir. Novirina Hendrasarie, MT
NIP. 19681126 199403 2 001

LEMBAR PERSETUJUAN

ANALISIS KEAMANAN WEBSITE SIPATCA MENGGUNAKAN METODE PENETRATION TESTING BERBASIS ISSAF dan OWASP WSTG v4.2

Oleh:
Muhammad Rafi Arganta
NPM. 21082010061

Telah disetujui untuk mengikuti Ujian Skripsi

Mengetahui,
Koordinator Program Studi Sistem Informasi
Fakultas Ilmu Komputer

Siti Mukaromah, S.Kom., M.Kom
NIP. 19810704 2021212011

SURAT PERNYATAAN BEBAS PLAGIASI

Saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Rafi Arganta
NPM	: 21082010061
Program	: Sarjana(S1)
Program Studi	: Sistem Informasi
Fakultas	: Fakultas Ilmu Komputer

Menyatakan bahwa dalam dokumen ilmiah Skripsi ini tidak terdapat bagian dari karya ilmiah lain yang telah diajukan untuk memperoleh gelar akademik di suatu lembaga Pendidikan Tinggi, dan juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang/lembaga lain, kecuali yang secara tertulis disitasi dalam dokumen ini dan disebutkan secara lengkap dalam daftar pustaka.

Dan saya menyatakan bahwa dokumen ilmiah ini bebas dari unsur-unsur plagiasi. Apabila dikemudian hari ditemukan indikasi plagiat pada Skripsi ini, saya bersedia menerima sanksi sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya tanpa ada paksaan dari siapapun juga dan untuk dipergunakan sebagaimana mestinya.

Surabaya, .. Mei 2026

Yang Membuat Pernyataan,

Muhammad Rafi Arganta

NPM. 21082010061

ABSTRAK

Nama Mahasiswa/ NPM	:	Muhammad Rafi Arganta / 21082010061
Judul Skripsi	:	ANALISIS KEAMANAN WEBSITE SIPATCA MENGGUNAKAN METODE PENETRATION TESTING BERBASIS ISSAF dan OWASP WSTG v4.2
Dosen Pembimbing	:	1. Eka Dyar Wahyuni, S.Kom, M.Kom. 2.Iqbal Ramadhani Mukhlis, S.Kom., M.Kom

Website SIPATCA (Sistem Informasi Pelayanan Administrasi Terpadu Civitas Akademik) Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jawa Timur digunakan sebagai layanan administrasi surat-menyurat yang berpotensi mengelola data sensitif. Oleh karena itu, diperlukan pengujian keamanan untuk mengidentifikasi potensi kerentanan yang dapat menimbulkan risiko seperti kebocoran data dan akses tidak sah. Penelitian ini bertujuan untuk menganalisis keamanan Website SIPATCA menggunakan metode penetration testing dengan pendekatan black box berbasis Information System Security Assessment Framework (ISSAF) dan OWASP Web Security Testing Guide (WSTG) v4.2.

Hasil penelitian menunjukkan bahwa sistem masih memiliki beberapa kerentanan keamanan pada konfigurasi server dan keamanan sisi klien, seperti tidak diterapkannya security headers, fitur autocomplete pada field password, kelemahan cache browser, serta pengungkapan informasi versi server dan struktur internal Website. Kerentanan tersebut berpotensi meningkatkan risiko kebocoran informasi dan serangan berbasis browser. Namun, tidak ditemukan kerentanan kritis seperti SQL Injection, Cross Site Scripting (XSS), maupun authentication bypass. Berdasarkan hasil analisis, Website SIPATCA berada pada tingkat risiko rendah hingga sedang dan memerlukan peningkatan konfigurasi keamanan secara berkala.

Kata kunci: keamanan website, penetration testing, ISSAF, OWASP WSTG v4.2

ABSTRACT

Nama Mahasiswa/ NPM	:	Muhammad Rafi Arganta / 21082010061
Judul Skripsi	:	WEBSITE SECURITY ANALYSIS OF SIPATCA USING PENETRATION TESTING METHOD BASED ON ISSAF AND OWASP WSTG v4.2
Dosen Pembimbing	:	1. Eka Dyar Wahyuni, S.Kom, M.Kom. 2.Iqbal Ramadhani Mukhlis, S.Kom., M.Kom

The SIPATCA Website (Integrated Academic Community Administrative Service Information System) of the Faculty of Computer Science, Universitas Pembangunan Nasional "Veteran" East Java, is used as an administrative correspondence service that potentially manages sensitive data. Therefore, security testing is required to identify potential vulnerabilities that may cause risks such as data leakage and unauthorized access. This research aims to analyze the security of the SIPATCA Website using a penetration testing method with a black box approach based on the Information System Security Assessment Framework (ISSAF) and the OWASP Web Security Testing Guide (WSTG) v4.2.

The results of the study indicate that the system still has several security vulnerabilities related to server configuration and client-side security, such as the absence of security headers implementation, the use of autocomplete features in password fields, browser cache weaknesses, and disclosure of server version information and internal website structure. These vulnerabilities may increase the risk of information leakage and browser-based attacks. However, no critical vulnerabilities such as SQL Injection, Cross Site Scripting (XSS), or authentication bypass were found. Based on the analysis results, the SIPATCA Website is categorized as having a low to medium risk level and requires periodic improvements in security configuration, server hardening, and overall website security

Kata kunci: website security, penetration testing, ISSAF, OWASP WSTG v4.2

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis Keamanan Website SIPATCA Menggunakan Metode Penetration Testing Berbasis ISSAF dan OWASP WSTG v4.2" dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur. Dalam proses penyusunan skripsi ini, penulis menyadari bahwa banyak pihak telah memberikan dukungan, bantuan, doa, serta bimbingan baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Orang tua tercinta, kakak, dan keluarga besar yang selalu memberikan doa, kasih sayang, dukungan, motivasi, serta pengorbanan yang tidak ternilai selama penulis menempuh pendidikan hingga menyelesaikan skripsi ini.
2. Ibu Eka Dyar Wahyuni, S.Kom., M.Kom., selaku dosen pembimbing pertama yang telah memberikan arahan, bimbingan, kesabaran, serta masukan yang sangat berarti selama proses penyusunan skripsi.
3. Bapak Iqbal Ramadhani Mukhlis, S.Kom., M.Kom., selaku dosen pembimbing kedua yang telah memberikan kritik, saran, motivasi, dan dukungan sehingga penelitian ini dapat diselesaikan dengan baik.
4. Bapak Doddy Ridwandono, S.Kom., M.Kom., selaku dosen wali yang telah memberikan arahan dan bimbingan selama masa perkuliahan.
5. Seluruh dosen dan tenaga pengajar Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur yang telah memberikan ilmu, pengalaman, dan pembelajaran yang bermanfaat selama masa studi.
6. Bapak Dr. I Gede Susrama Mas Diyasa, S.T., M.T., selaku pihak yang telah memberikan izin dan akses terhadap objek penelitian sehingga penelitian ini dapat dilaksanakan dengan baik.
7. Teman-teman seperjuangan dan sahabat terdekat, yaitu Farras Hafish, Naufal Nur Ahmad, Dhiya' Ulhaq, Hadyan Alhafiz, Hanif Izzul, Hafiz Ilham Ardana, serta pihak lainnya yang tidak dapat disebutkan satu per satu,

atas dukungan, semangat, bantuan, dan kebersamaan selama proses penyusunan skripsi ini.

8. Seluruh pihak lain yang telah membantu dan mendukung penulis, baik secara teknis, moral, maupun spiritual, sehingga skripsi ini dapat terselesaikan.

Penulis menyadari bahwa penelitian ini masih memiliki berbagai keterbatasan, baik dari segi ruang lingkup pengujian maupun teknik analisis yang digunakan. Oleh karena itu, penulis berharap penelitian ini dapat menjadi referensi dan bahan evaluasi dalam meningkatkan keamanan website, khususnya pada sistem informasi berbasis web di lingkungan akademik. Selain itu, penulis juga berharap penelitian ini dapat dikembangkan lebih lanjut dengan metode maupun tools pengujian keamanan yang lebih luas dan mendalam. Penulis juga menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi perbaikan di masa mendatang. Semoga penelitian ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya pada bidang keamanan sistem informasi dan pengujian keamanan website.

Surabaya, Mei 2026

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN