Tesis

Analisis Keamanan dan Penilaian Kerentanan Sistem Informasi Akademik Berbasis Web Menggunakan *Framework* OWASP dan ISSAF

Muhammad Ihya Aulia Elfatiha
2008048045

Program Studi S2 Informatika
Fakultas Teknologi Industri
Universitas Ahmad Dahlan
Yogyakarta
2024

Tesis

Analisis Keamanan dan Penilaian Kerentanan Sistem Informasi Akademik Berbasis Web Menggunakan *Framework OWASP* dan *ISSAF*

Muhammad Ihya Aulia Elfatiha
2008048045

Dipertahankan di depan Dewan Penguji
Tanggal 05 Agustus 2024

Rusydi Umar, S.T., M.T., Ph.D.
Ketua Penguji

Prof. Dr. Ir. Imam Riadi, M.Kom.
Penguji 1

Prof. Drs. Ir. Abdul Fadlil, M.T., Ph.D.
Penguji 2

Herman, S.Kom., M.Sc., Ph.D.
Penguji 3

Mengetahui,

Prof. Dr. Ir. Siti Jamilatun, M.T.
Dekan Fakultas Teknologi Industri

Pernyataan Tidak Plagiat

Saya yang bertanda tangan di bawah ini:

Nama	:	Muhammad Ihya Aulia Elfatiha
NIM	:	2008048045
Email	:	elfatih2008048045@webmail.uad.ac.id
Program Studi	:	S2 Informatika
Fakultas	:	Teknologi Industri
Judul Tesis	:	Analisis Keamanan dan Penilaian Kerentanan Sistem Informasi Akademik Berbasis Web Menggunakan *Framework* OWASP dan ISSAF

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar magister, baik di Universitas Ahmad Dahlan maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan nara sumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Ahmad Dahlan.

Yogyakarta, 05 Agustus 2024

ang Menyatakan

Muhammad Ihya Aulia Elfatiha

Pernyataan Persetujuan Akses

Saya yang bertanda tangan di bawah ini:

Nama	:	Muhammad Ihya Aulia Elfatiha
NIM	:	2008048045
Email	:	elfatih2008048045@webmail.uad.ac.id
Program Studi	:	S2 Informatika
Fakultas	:	Teknologi Industri
Judul Tesis	:	Analisis Keamanan dan Penilaian Kerentanan Sistem Informasi Akademik Berbasis Web Menggunakan *Framework* OWASP dan ISSAF

Dengan ini saya menyerahkan hak sepenuhnya kepada Pusat Sumber Belajar Universitas Ahmad Dahlan untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tesis elektronik sebagai berikut (beri tanda pada kotak):

☑ Saya mengijinkan karya tersebut diunggah ke dalam aplikasi *repository* perpustakaan Universitas Ahmad Dahlan.

Demikian pernyataan ini saya buat dengan sebenarnya.

Yogyakarta, 05 Agustus 2024

Yang Menyatakan

Muhammad Ihya Aulia Elfatiha

Mengetahui,

Pembimbing Tesis 1

Rusydi Umar, ST., MT., Ph.D.

Pembimbing Tesis 2

Prof. Ir. Dr. Imam Riadi, M.Kom.

Motto dan Persembahan

“Keberuntungan adalah ketika kesempatan bertemu dengan kemampuan. Kesempatan bisa dicari dan kemampuan bisa diasah, maka pada dasarnya keberuntungan itu bisa diciptakan.” -Muhammad Ihya Aulia Elfatiha

“Jangan bersedih atas apa yang telah berlalu, kecuali jika itu bisa membuatmu bekerja lebih keras untuk masa depan (yang lebih baik).” -Umar bin Khattab

Tesis ini kupersembahkan untuk:

1. Orang tua tersayang, ibu anda dan bapak anda

   Terima kasih atas kepercayaan dan kesempatan yang diberikan selama ini.
2. Para pembaca semua.

Kata Pengantar

Bismillahirrahmaanirrahiim,

Assalaamu'alaikum warahmatullaahi wabarakaatuh

Segala puji bagi Allah swt yang telah memberikan rahmat, hidayah, dan inayah kepada hamba-Nya sehingga penulis dapat menyelesaikan Tesis ini.

Penulis menyadari bahwa keberhasilan dalam menyelesaikan laporan ini berkat dorongan dan bimbingan berbagai pihak. Oleh karena itu, dalam kesempatan ini penulis menghaturkan terima kasih dan penghargaan kepada Bapak Prof. Dr. Muchlas, M.T. Rektor Universitas Ahmad Dahlan, Ibu Prof. Dr. Ir. Siti Jamilatun, M.T. Dekan Fakultas Teknologi Industri, Bapak Prof. Drs. Ir. Abdul Fadlil, M.T., Ph.D. selaku Kaprodi S2 Informatika, Bapak Prof. Rusydi Umar, MT., Ph.D. selaku Pembimbing Tesis 1 dan Bapak Prof. Dr. Ir. Imam Riadi, M.Kom. selaku Pembimbing Tesis 2 yang rela diganggu setiap saat selama proses penulisan tesis. Terima kasih juga penulis haturkan kepada seluruh dosen S2 Informatika yang telah memberikan banyak ilmu dan wawasan.

Selanjutnya penulis juga menyampaikan terima kasih kepada rekan-rekan angkatan 11 di S2IF UAD dan berbagai pihak yang tidak dapat disebutkan satu persatu.

Terakhir, penulis sangat mengharapkan saran dan kritik yang membangun, karena Tesis ini sangat jauh dari sempurna. Semoga Allah meridhoi langkah kita. Amin.

Wassalaamu'alaikum warahmatullaahi wabarakaatuh

Yogyakarta, 05 Agustus 2024

Muhammad Ihya Aulia Elfatiha

Daftar Isi

Daftar Gambar

Daftar Tabel

Elfatiha, M. I. A. (2024). **Analisis Keamanan dan Penilaian Kerentanan Sistem Informasi Akademik Berbasis Web Menggunakan *Framework OWASP* dan *ISSAF*.** Tesis, Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta.

Abstrak

Penggunaan teknologi informasi dalam dunia pendidikan telah menjadi kebutuhan utama untuk meningkatkan kinerja institusi. Institut Bisnis Muhammadiyah Bekasi telah memanfaatkan IT dalam seluruh kegiatan operasionalnya yang diberi nama Sistem Informasi Akademik Terpadu. Penelitian bertujuan untuk menganalisis dan membandingkan *framework OWASP* dan *ISSAF* dalam melakukan penilaian kerentanan pada Sistem Informasi Akademik Institut Bisnis Muhammadiyah Bekasi.

Penelitian ini menggunakan metode *Vulnerability Assessment and Penetration Testing* dengan menggunakan *framework OWASP* dan *ISSAF*. *Framework OWASP* meliputi proses tahapan *Recconaisance, Scanning, Exploitation, Maintaining Access*, dan *Reporting*. *Framework ISSAF* meliputi tahapan *Information Gathering, Network Mapping, Vulnerbility Identification, Penetration*, dan *Reporting*. Hasil pengujian kemudian didokumentasikan dan dibuatkan rekomendasi tindakan mitigasi atas temuan yang didapat.

Dari penelitan yang telah dilakukan, Pengujian menggunakan *framework OWASP* berdasarkan daftar risiko keamanan *OWASP Top 10* mendapatkan hasil bahwa sistem aman dari percobaan serangan *SQL Injection, XXE, XSS, Insecure Deserialization, dan Insufficient Logging and Monitoring*. Namun sistem memiliki kerentanan pada *Broken Authentication, Sensitive Data Exposure, Broken Access Control, Security Missconfiguration,* dan *Using Component with Known Vurnelabilities*. Kemudian pengujian menggunakan *framework ISSAF*, ditemukan kerentanan pada sistem yaitu *Sensitive Data Exposure dan Session Hijacking with Cookie*, namun sistem aman dari percobaan serangan *SQL Injection, XSS, dan Broken Access Control*. Dari hasil yang didapat, penelitian menyimpulkan bahwa sistem informasi akademik Institut Bisnis Muhammadiyah Bekasi masih dalam kategori aman, namun terdapat beberapa bagian yang harus segera diperbaiki. Adapun rekomendasi tindakan mitigasi yang disarankan dalam penelitian ini adalah sistem hendaknya dilakukan pembaruan pada versi *JS Library* dan *Bootstrap* yang digunakan untuk mencegah munculnya celah keamanan baru, konfigurasi *server* lebih diperketat, dan rutin memonitoring sistem agar jika terdapat aktivitas mencurigakan dapat segera diantisipasi.

Kata kunci: *OWASP*, *ISSAF*, *Penetration Testing*, Penilaian Kerentanan, Sistem Informasi Akademik

Elfatiha, M. I. A. (2024). ***Security Analysis and Vulnerability Assessment of Web-Based Academic Information Systems Using OWASP and ISSAF Frameworks****. Thesis, Master Program of Informatics, Universitas Ahmad Dahlan, Yogyakarta.*

Abstract

In the modern educational landscape, the use of information technology has become a crucial requirement for enhancing institutional performance. Institut Bisnis Muhammadiyah Bekasi has utilized IT in all its operational activities under the name Integrated Academic Information System. This research aims to analyze and compare the OWASP and ISSAF frameworks in assessing vulnerabilities in the Academic Information System of Institut Bisnis Muhammadiyah Bekasi.

This research employs the Vulnerability Assessment and Penetration Testing method using the OWASP and ISSAF frameworks. The OWASP framework includes stages of Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting. The ISSAF framework involves stages of Information Gathering, Network Mapping, Vulnerability Identification, Penetration, and Reporting. The testing results are then documented, and mitigation recommendations are provided based on the findings.

From the research conducted, testing using the OWASP framework based on the OWASP Top 10 security risks revealed that the system is secure against attempted SQL Injection, XXE, XSS, Insecure Deserialization, and Insufficient Logging and Monitoring attacks. However, the system is vulnerable to Broken Authentication, Sensitive Data Exposure, Broken Access Control, Security Misconfiguration, and Using Components with Known Vulnerabilities. Meanwhile, testing using the ISSAF framework identified vulnerabilities in the system, such as Sensitive Data Exposure and Session Hijacking with Cookies, but the system is secure against attempted SQL Injection, XSS, and Broken Access Control attacks. Based on the results obtained, the research concludes that the academic information system of Institut Bisnis Muhammadiyah Bekasi is generally secure, though some areas need immediate improvement. The recommended mitigation actions include updating the JS Library and Bootstrap versions used to prevent new security gaps, tightening server configuration, and regularly monitoring the system to promptly address any suspicious activities.

Keywords: OWASP, ISSAF, Penetration Testing, Vulnerability Assessment, Academic Information System.