

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
Yang 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):

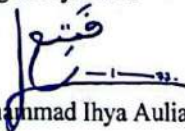


Saya mengizinkan karya tersebut diunggah ke dalam aplikasi *repository* perpustakaan Universitas Ahmad Dahlan.

Demikian pernyataan ini saya buat dengan sebenarnya.

Yogyakarta, 05 Agustus 2024

Yang Menyatakan



Muhammad Ihya Aulia Elfatiha

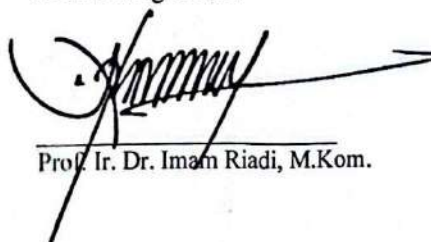
Mengetahui,

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

Pernyataan Tidak Plagiat.....	iii
Pernyataan Persetujuan Akses	iv
Motto dan Persembahan	v
Kata Pengantar	vi
Daftar Isi	vii
Daftar Gambar	ix
Daftar Tabel.....	x
Abstrak.....	xi
Abstract.....	xii
Bab 1 Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah	6
1.3 Batasan Masalah	6
1.4 Rumusan Masalah.....	6
1.5 Tujuan Penelitian.....	7
1.6 Manfaat Penelitian.....	7
Bab 2 Tinjauan Pustaka	8
2.1 Kajian Penelitian Terdahulu	8
2.2 Landasan Teori	37
2.2.1 Digital Forensik	38
2.2.2 Analisis Keamanan Sistem.....	39
2.2.3 <i>Vulnerability Assessment and Penetration Testing</i>	41
2.2.4 <i>Open Web Application Security Project (OWASP)</i>	46
2.2.5 <i>Information Systems Security Application Frameworks (ISSAF)</i>	52
2.2.6 <i>Tools</i> Evaluasi Keamanan Sistem Informasi	53
2.2.7 Sistem Informasi Akademik.....	55
Bab 3 Metodologi	59
3.1 Objek Penelitian	59
3.2 Alat dan Bahan	59
3.3 Kerangka Penelitian.....	60

3.3.1 Analisis dan Pengujian Sistem Menggunakan OWASP	62
3.3.2 Analisis dan Pengujian Sistem Menggunakan ISSAF	66
3.3.3 Review Hasil Pengujian.....	69
Bab 4 Hasil dan Pembahasan.....	71
4.1 Pengujian Menggunakan <i>Framework</i> OWASP.....	72
4.1.1 <i>Reconnaissance</i>	72
4.1.2 <i>Scanning</i>	77
4.1.3 <i>Exploitation</i>	82
4.1.4 <i>Maintaining Access</i>	97
4.1.5 <i>Reporting</i>	98
4.2 Pengujian Menggunakan <i>Framework</i> ISSAF	101
4.2.1 <i>Information Gathering</i>	101
4.2.2 <i>Network Mapping</i>	106
4.2.3 <i>Vulnerability Identification</i>	107
4.2.4 <i>Penetration</i>	109
4.2.5 <i>Reporting</i>	113
4.3 Review Hasil Pengujian	117
Bab 5 Penutup	123
5.1 Kesimpulan.....	123
5.2 Saran	124
Daftar Acuan	126
Daftar Lampiran	135
Lampiran 1 Daftar Riwayat Hidup	136
Lampiran 2 Nama Dosen dan Afiliasi	137
Lampiran 3 OWASP ZAP Report	138
Lampiran 4 Pentest-tool Report.....	145

Daftar Gambar

Gambar 1.1 Karakteristik <i>World Class University</i> (WCU)	3
Gambar 2.1 Peta kaitan penelitian terdahulu dan penelitian yang dikerjakan	36
Gambar 2.2 Teknik pengujian <i>penetration testing</i>	43
Gambar 2.3 Tahapan <i>framework</i> OWASP	47
Gambar 2.4 OWASP <i>Top 10 Most Critical Web Application Security Risks</i>	49
Gambar 2.5 Tahapan <i>framework</i> ISSAF	52
Gambar 3.1 Kerangka penelitian.....	61
Gambar 3.2 Skenario pengujian menggunakan OWASP	62
Gambar 3.3 Skenario pengujian menggunakan ISSAF.....	66
Gambar 4.1 Hasil pencarian <i>IP Address</i> dengan <i>tool</i> Netcraft	73
Gambar 4.2 <i>Whois domain results</i>	74
Gambar 4.3 <i>Nmap results</i>	75
Gambar 4.4 <i>Whatweb results</i>	76
Gambar 4.5 <i>ZAP scanning result</i>	77
Gambar 4.6 <i>Injection attack</i> menggunakan SQLMap.....	82
Gambar 4.7 <i>Injection attack</i> menggunakan Havij Pro	83
Gambar 4.8 <i>Bruteforce attack</i> menggunakan <i>tool</i> Hydra	84
Gambar 4.9 <i>Sensitive data exposure</i> menggunakan <i>tool</i> dirb	85
Gambar 4.10 <i>Server status sikadu.ibm.ac.id</i>	86
Gambar 4.11 <i>Response XML</i>	87
Gambar 4.12 Percobaan <i>fuzzer ID Access</i>	88
Gambar 4.13 Pemindaian SSL/TLS menggunakan OpenSSL	89
Gambar 4.14 Hasil pengujian SSL/TLS menggunakan <i>pentest-tool</i>	90
Gambar 4.15 <i>Heartbleed attack</i> menggunakan Metasploit.....	91
Gambar 4.16 <i>Payload XSS</i> pada kolom <i>search</i>	92
Gambar 4.17 <i>XSS attack</i> menggunakan <i>tool</i> Burp Suite.....	93
Gambar 4.18 Pengujian <i>rate limiting</i>	94
Gambar 4.19 <i>Insecure deserialization</i> menggunakan <i>tool</i> Burpsuite	95
Gambar 4.20 <i>Component with Known Vulnerability</i>	96
Gambar 4.21 <i>Logging and Monitoring</i>	97
Gambar 4.22 Percobaan <i>maintaining access</i>	98
Gambar 4.23 Hasil identifikasi IP dengan <i>tool</i> Nikto	101
Gambar 4.24 Hasil identifikasi IP menggunakan <i>pentest-tool</i>	102
Gambar 4.25 Hasil pemindaian SSL	103
Gambar 4.26 Pemeriksaan DNS dengan NSLookup	104
Gambar 4.27 Identifikasi <i>website</i> menggunakan whatweb.....	105
Gambar 4.28 Identifikasi <i>website</i> menggunakan <i>pentest-tool</i>	105
Gambar 4.29 Hasil pemindaian <i>port</i> menggunakan <i>tool</i> <i>pentest-tool</i>	106
Gambar 4.30 Hasil <i>vulnerability identification</i> menggunakan <i>pentest-tool</i>	108

Daftar Tabel

Tabel 2.1 Rangkuman penelitian terdahulu	25
Tabel 2.2 Perbandingan penelitian terdahulu	35
Tabel 3.1 Alat dan bahan penelitian	59
Tabel 3.2 <i>Software</i> dan <i>tools</i> pendukung	60
Tabel 4.1 <i>Server specification</i>	71
Tabel 4.2 <i>Tools reconnaissance</i>	72
Tabel 4.3 <i>Whois domain results</i>	74
Tabel 4.4 <i>Nmap results</i>	76
Tabel 4.5 <i>Whatweb results</i>	77
Tabel 4.6 Penjelasan <i>vulnerability</i> yang ditemukan <i>tools</i> ZAP	78
Tabel 4.7 <i>Report on vulnerability identification results</i>	99
Tabel 4.8 <i>Report on penetration testing results</i>	100
Tabel 4.9 Hasil pemindaian SSL melalui terminal	103
Tabel 4.10 Kesimpulan hasil pemindaian <i>port</i>	107
Tabel 4.11 Penjelasan hasil <i>vulnerability identification</i>	108
Tabel 4.12 <i>Exploitation results</i>	109
Tabel 4.13 Hasil pengujian <i>gaining access and privilege escalation</i>	110
Tabel 4.14 Hasil pengujian <i>enumerating further</i>	111
Tabel 4.15 Hasil pengujian <i>compromise remote user/sites</i>	112
Tabel 4.16 Hasil pengujian <i>maintaining access</i>	112
Tabel 4.17 Hasil <i>covering tracks</i>	113
Tabel 4.18 Laporan hasil pengujian berdasarkan <i>framework</i> ISSAF	114
Tabel 4.19 Hasil pemindaian kerentanan pada <i>sikadu.ibm.ac.id</i>	117
Tabel 4.20 Laporan hasil pemindaian dan tindakan mitigasi OWASP	117
Tabel 4.21 Laporan hasil pemindaian beserta tindakan mitigasi ISSAF	119
Tabel 4.22 Laporan hasil pengujian dan rekomendasi mitigasi OWASP	120
Tabel 4.23 Laporan hasil pengujian dan rekomendasi mitigasi ISSAF	121

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 *Reconnaissance*, *Scanning*, *Exploitation*, *Maintaining Access*, dan *Reporting*. *Framework* ISSAF meliputi tahapan *Information Gathering*, *Network Mapping*, *Vulnerability Identification*, *Penetration*, dan *Reporting*. Hasil pengujian kemudian didokumentasikan dan dibuatkan rekomendasi tindakan mitigasi atas temuan yang didapat.

Dari penelitian 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 Misconfiguration*, dan *Using Component with Known Vulnerabilities*. 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.