



**STT TERPADU  
NURUL FIKRI**

**SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI**

**ANALISIS KERENTANAN KEAMANAN APLIKASI  
MANAJEMEN ASSET BERBASIS WEB  
MENGUNAKAN METODE ISSAF (INFORMATION  
SYSTEMS SECURITY ASSESSMENT FRAMEWORK)  
STUDI KASUS PT.XYZ**

**TUGAS AKHIR**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar  
Sarjana Komputer**

**STT - NF**

**RAIHAN SABIQ RABBANI  
0110217040**

**PROGRAM STUDI TEKNIK INFORMATIKA  
JEMBER  
OKTOBER 2021**

**HALAMAN PERNYATAAN ORISINALITAS**

**Tugas Akhir ini adalah hasil karya penulis,  
dan semua sumber baik yang dikutip maupun dirujuk  
telah saya nyatakan dengan benar.**



**Nama : Raihan Sabiq Rabbani**

**NIM : 0110217040**

**Tanda Tangan : .....**

**Tanggal : 22 Oktober 2021**

**STT - NF**

## HALAMAN PENGESAHAN

**Tugas Akhir ini diajukan oleh:**

**Nama:** Raihan Sabiq Rabbani

**NIM:** 0110217040

**Program Studi:** Teknik Informatika

**Judul Skripsi:** ANALISIS KERENTANAN KEAMANAN APLIKASI

MANAJEMEN ASSET BERBASIS WEB

MENGGUNAKAN METODE ISSAF (INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK) STUDI KASUS PT.XYZ

**Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri**

**DEWAN PENGUJI**

Pembimbing I

Sirojul Munir, S. Si, M. Kom

Penguji I **S TT - NF** Penguji II

Tubagus Rizky Darmawan, S.T, M. Sc Hilmy Abidzar Tawakal, S.T, M. Kom

Ditetapkan di : .....

Tanggal : .....

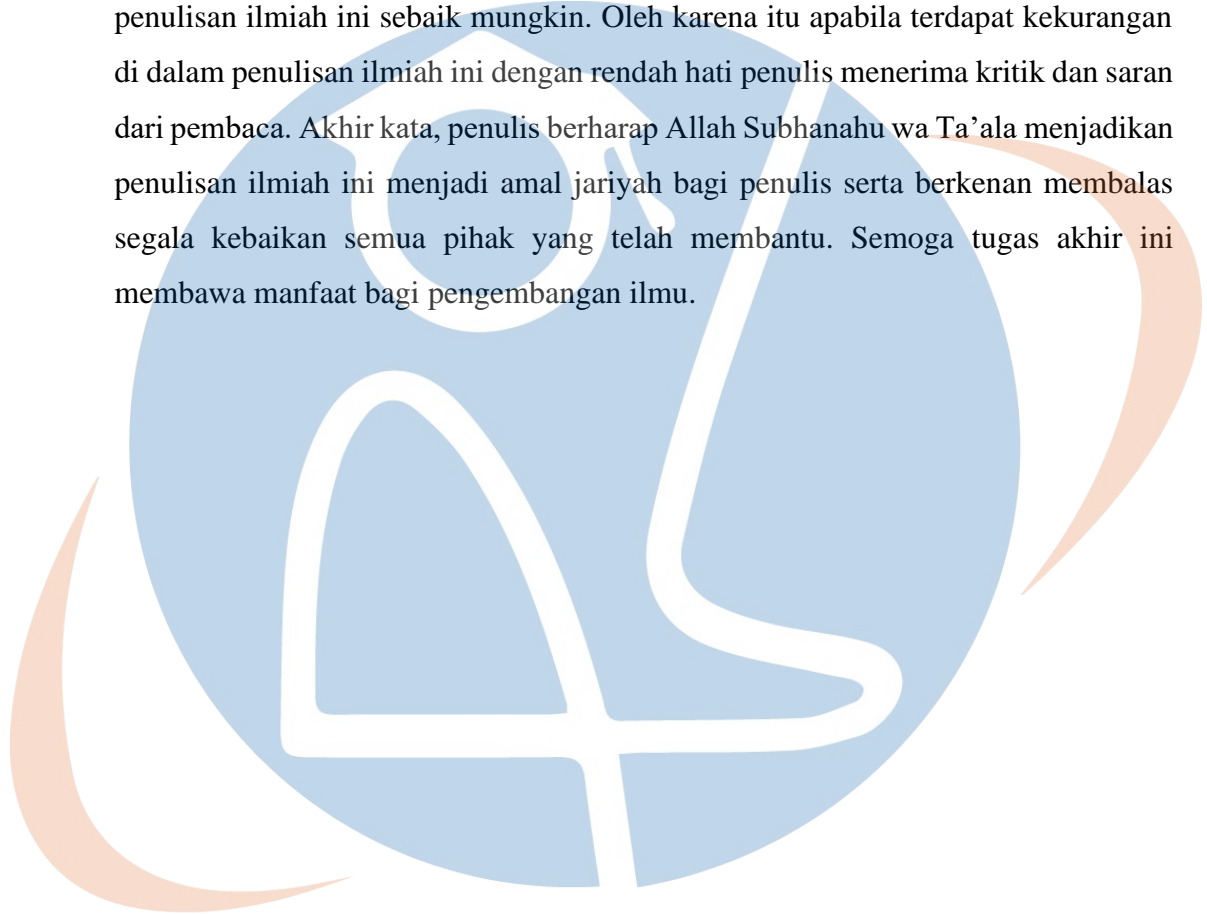
## KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah Subhanahu Wa Ta'ala, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Tugas Akhir ini. Shalawat dan salam semoga senantiasa tercurahkan untuk Rasulullah Shallallahu 'Alaihi wa Sallam, keluarga dan para sahabatnya. Penulisan Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer Program Studi Teknik Informatika pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri. Penulis menyadari bahwa, tanpa bantuan Allah dan bimbingan dari berbagai pihak dari masa perkuliahan sampai pada penyusunan Tugas Akhir ini, sangatlah sulit bagi penulis untuk menyelesaikan tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah Subhanahu wa Ta'ala.
2. Orang tua dan semua anggota keluarga yang telah memberikan dorongan baik secara moril maupun materil dalam penyelesaian tugas ini.
3. Bapak Lukman Rosyidi, ST. MM. MT., selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Bapak Ahmad Rio Adriansyah, S. Si M.Si., selaku Wakil Ketua 1 Akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
5. Bu Tifanny Nabarian, S. Kom, M.T.i., selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
6. Bapak Sirojul Munir, S.Si. M.Kom., selaku Dosen Pembimbing Akademik dan selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan tugas akhir ini.
7. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
8. Karyawan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah meluangkan waktunya untuk memberikan data yang diperlukan bagi penulisan ilmiah ini.
9. Teman-teman Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah mendukung penulis dalam menyelesaikan penulisan ilmiah ini.
10. Seluruh pihak yang telah membantu secara langsung maupun tidak

langsung, yang tidak dapat penulis sertakan satu persatu namun tidak mengurangi rasa terima kasih penulis.

Dalam penulisan ilmiah ini tentu saja masih banyak terdapat kekurangan-kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan yang penulis miliki. Namun, penulis telah berusaha menyelesaikan penulisan ilmiah ini sebaik mungkin. Oleh karena itu apabila terdapat kekurangan di dalam penulisan ilmiah ini dengan rendah hati penulis menerima kritik dan saran dari pembaca. Akhir kata, penulis berharap Allah Subhanahu wa Ta'ala menjadikan penulisan ilmiah ini menjadi amal jariyah bagi penulis serta berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tugas akhir ini membawa manfaat bagi pengembangan ilmu.



STT - NF

Jember, 22 Oktober 2021

Raihan Sabiq Rabbani

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI  
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS**

---

---

Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini:

Nama : Raihan Sabiq Rabbani

NIM : 0110217040

Program Studi : Teknik Informatika

Jenis Karya : Tugas Akhir

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STT-NF **Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty – Free Right)** atas karya ilmiah saya yang berjudul:

ANALISIS KERENTANAN KEAMANAN APLIKASI MANAJEMEN ASSET  
BERBASIS WEB MENGGUNAKAN METODE ISSAF (INFORMATION  
SYSTEMS SECURITY ASSESSMENT FRAMEWORK)  
STUDI KASUS PT.XYZ

Dengan Hak Bebas Royalti Noneksklusif ini STT-NF berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

STT - NF

Dibuat di: Jember  
Pada tanggal: 22 Oktober 2021

Yang Menyatakan

(Raihan Sabiq Rabbani)

## ABSTRAK

Nama : Raihan Sabiq Rabbani  
NIM : 0110217040  
Program Studi : Teknik Information  
Judul : ANALISIS KERENTANAN KEAMANAN APLIKASI  
MANAJEMEN ASSET BERBASIS WEB MENGGUNAKAN METODE ISSAF  
(INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK)  
STUDI KASUS PT.XYZ

Tugas Akhir/Skripsi ini membahas tentang kerentanan keamanan menjadi topik penelitian ini dikarenakan setiap produk informatika yang dibangun/dibuat seperti website, aplikasi android dan lainnya memiliki kerentanan keamanan. Penelitian ini dalam mencari kerentanan keamanan menggunakan ISSAF (Information System Security Assessment Framework) versi 0.2.1B untuk menganalisa apa saja kemungkinan kerentanan keamanan pada aplikasi web manajemen asset milik PT.XYZ dengan berbasis framework laravel versi 8. Pendekatan penelitian ini menggunakan blackbox testing dan whitebox testing, adapun alat bantu yang digunakan sistem operasi Windows dan Windows Subsystem Linux versi 2 (WSL2) sehingga membantu masyarakat yang kurang familiar dengan sistem operasi sumber terbuka. Hasil dari penelitian ini bahwa aplikasi manajemen asset berbasis web PT.XYZ memiliki kerentanan keamanan yang tinggi.

Kata kunci: Web, ISSAF, Kerentanan, Keamanan, Laravel, WSL2



## ABSTRACT

Name : Raihan Sabiq Rabbani  
NIM : 0110217040  
Study Program : Informatics  
Title : ANALYSIS OF WEB-BASED ASSET MANAGEMENT APPLICATION SECURITY VULNERABILITY USING THE ISSAF (INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK) METHOD CASE STUDY OF PT.XYZ.

The focus of final research is about security vulnerabilities which is the topic of this research because every informatics product that is built/made such as websites, android applications and others has security vulnerabilities. This research is looking for security vulnerabilities using ISSAF (Information System Security Assessment Framework) version 0.2.1B to analyze what are the possible security vulnerabilities in PT. XYZ's asset management web application based on the Laravel version 8 framework. This research approach uses blackbox testing and whitebox testing, as for the tools used by the Windows operating system and Windows Subsystem Linux version 2 (WSL2) to help people who are less familiar with open-source operating systems. The results of this final research show that PT. XYZ's web-based asset management application has a high security vulnerability.

Keywords: Web, ISSAF, Vulnerability, Security, Laravel, WSL2



# DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS.....	ii
HALAMAN PENGESAHAN.....	iii
KATA PENGANTAR .....	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI.....	vi
ABSTRAK .....	vii
ABSTRACT.....	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR .....	xii
DAFTAR TABEL.....	xiv
BAB I.....	1
PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Perumusan Masalah .....	2
1.3. Tujuan dan Manfaat Penelitian .....	2
1.4. Batasan Masalah.....	3
1.5. Sistematika Penulisan .....	3
BAB II.....	5
KAJIAN LITERATUR.....	5
2.1. Kajian Pustaka.....	5
2.1.1. Aplikasi Manajemen .....	5
2.1.2. Framework Laravel .....	5
2.1.3. Kerentanan Keamanan .....	5
2.1.4. Jenis Penetrasi .....	6
2.1.4.1. Black Box Testing .....	7
2.1.4.2. White Box Testing .....	7
2.1.4.3. Grey Box Testing.....	7
2.1.5. ISSAF.....	7
2.1.5.1. PHASE 1 - PLANNING AND PREPARATION.....	8
2.1.5.2. PHASE 2 - ASSESSMENT .....	9

2.1.5.3. PHASE 3 - REPORTING, CLEANING UP AND DESTROY ARTIFACTS .....	16
2.1.5.3.1. REPORTING.....	16
2.1.5.3.2. CLEANING UP AND DESTROY ARTIFACTS.....	16
2.2. Penelitian Terkait .....	17
2.3. Posisi Penelitian .....	19
<b>BAB III .....</b>	<b>21</b>
<b>METODOLOGI PENELITIAN.....</b>	<b>21</b>
3.1. Jenis Metode Penelitian.....	21
3.2. Tahapan Penelitian .....	21
3.2.1. Studi Literatur .....	21
3.2.2. Analisa Kebutuhan Sistem .....	22
3.2.3. Pengujian Penetrasi .....	22
3.2.4. Analisis dan Laporan.....	22
3.2.5. Kesimpulan .....	22
3.3. Perancangan Penelitian .....	23
3.3.1. Arsitektur Penelitian.....	23
3.3.2. Lingkungan Penelitian .....	23
<b>BAB IV .....</b>	<b>25</b>
<b>IMPLEMENTASI.....</b>	<b>25</b>
4.1. PHASE I – PLANNING AND PREPARATION .....	25
4.1.1. Persiapan pada Windows .....	25
4.1.2. Persiapan pada Windows Subsystem Linux (WSL).....	27
4.2. PHASE II – ASSESSMENT.....	29
4.2.1. Information Gathering.....	29
4.2.2. Network Mapping .....	30
4.2.2.1. Nmap.....	30
4.2.3. Vulnerability Identification.....	32
4.2.4. Penetration.....	44
4.2.4.1. DoS (Denial of Service).....	44
4.2.5. Gaining Access and Priviledge Escalation.....	46

4.2.6.	Enumerating Further .....	55
4.2.6.1.	SQL Injection.....	55
4.2.6.2.	Man In the Middle .....	57
4.2.7.	Compromise Remote Users/Sites and Maintaining Access .....	59
4.2.8.	Covering Tracks .....	61
4.3.	PHASE III – Reporting, Clean Up and Destroy Artifact.....	62
4.3.1.	Reporting.....	62
4.3.2.	Clean Up and Destroy Artefacts .....	64
BAB V.	.....	65
KESIMPULAN DAN SARAN	.....	65
5.1.	Kesimpulan .....	65
5.2.	Saran.....	65
DAFTAR PUSTAKA	.....	66
LAMPIRAN	.....	68

STT - NF

## DAFTAR GAMBAR

Gambar 1. Metode Dasar Penetrasi Testing.....	6
Gambar 2. Rincian Information System Security Assessment Framework.....	8
Gambar 3. Diagram Tahapan Penelitian .....	21
Gambar 4. Arsitektur Penelitian.....	23
Gambar 5. Web Manajemen Asset (Localhost) .....	25
Gambar 6. Web Manajemen Asset (IPv4 Address) .....	26
Gambar 7. Konfigurasi Firewall dan Private Network .....	26
Gambar 8. Service XRDP Start.....	27
Gambar 9. IPv4 Address Kali Linux.....	27
Gambar 10. Remote Desktop Connection dengan IPv4 WSL .....	28
Gambar 11. Tampilan Login dan GUI Kali Linux via XRDP .....	28
Gambar 12. KeX start dan KeX -s .....	28
Gambar 13. GUI Kali Linux via KeX.....	29
Gambar 14. Halaman Pembuatan Akun Nessus Essentials .....	33
Gambar 15. Login Page Nessus Essentials .....	33
Gambar 16. New Scan Nessus Essentials .....	34
Gambar 17. Advanced Scan Nessus Essentials.....	34
Gambar 18. Konfigurasi Advanced Scan Nessus Essentials .....	35
Gambar 19. Konfigurasi Credentials.....	35
Gambar 20. Automatic Autentication Nessus Essentials.....	36
Gambar 21. Konfigurasi Credentials Username dan Password .....	36
Gambar 22. Jalankan Nessus Essentials .....	37
Gambar 23. Web Manajemen Asset sebelum DoS .....	44
Gambar 24. Slowloris DoS Attack.....	45
Gambar 25. Web Manajemen Asset setelah DoS .....	45
Gambar 26. Slowloris DoS Attack Interupt .....	45
Gambar 27. Web Manajemen Asset Normal Kembali.....	46
Gambar 28. Install Burp Suite.....	46
Gambar 29. Burp Suite Project (Next).....	47
Gambar 30. Use Burp Default and Start Burp .....	47
Gambar 31. Tampilan Dashboard Burp Suite .....	48

Gambar 32. Burp Suite Browser and Localhost (192.168.61.55).....	48
Gambar 33. Sitemap Burp Suite (192.168.61.55).....	49
Gambar 34. Burp Suite Intercept Off.....	49
Gambar 35. Burp Suite Intercept On.....	49
Gambar 36. Login pada Burp Suite Browser.....	50
Gambar 37. Intercept Web pada Burp Suite.....	50
Gambar 38. Send to Intruder pada Burp Suite.....	51
Gambar 39. Send to Intruder Burp Suite.....	51
Gambar 40. Tampilan Intruder Burp Suite.....	51
Gambar 41. Proses Intruder Add Variabel pada Burp Suite.....	52
Gambar 42. Payload 1 dan Payload 2Burp Suite.....	52
Gambar 43. Wordlist Password.....	53
Gambar 44. Wordlist Email.....	53
Gambar 45. Grep Match Burp Suite.....	54
Gambar 46. Brute Force Burp Suite.....	54
Gambar 47. Pengujian Brute Force Login Web Manajemen Asset.....	55
Gambar 48. Berhasil Masuk pada Web Manajemen Asset.....	55
Gambar 49. Konfigurasi Bettercap.....	58
Gambar 50. Bettercap Spoofing.....	58
Gambar 51. Default Gateway pada Windows PowerShell.....	59
Gambar 52. Cloning Github WeBaCoo.....	60
Gambar 53. Masuk Direktori WeBaCoo.....	60
Gambar 54. Membuat File Backdoor.....	60
Gambar 55. Upload Backdoor.....	61
Gambar 56. Akses Backdoor.....	61
Gambar 57. Serangan Backdoor Gagal.....	61
Gambar 58. Manipulasi File Backdoor.....	62
Gambar 59. Menghapus File Backdoor.....	64

## DAFTAR TABEL

Tabel 1. Klasifikasi Risiko Kerentanan .....	10
Tabel 2. Penelitian Terkait .....	17
Tabel 3. Posisi Penelitian .....	19
Tabel 4. Spesifikasi .....	24
Tabel 5. List Data Web Manajemen Asset .....	29
Tabel 6. Sudo nmap -A 192.168.43.75 .....	30
Tabel 7. Sudo nmap -p '*' 192.168.43.75 .....	32
Tabel 8. Nessus Essential Vulnerability Scanner (Apache) .....	37
Tabel 9. Nessus Essential Vulnerability Scanner (<OpenSSL 1.1.1o) .....	37
Tabel 10. Nessus Essential Vulnerability Scanner (<OpenSSL 1.1.1p) .....	37
Tabel 11. Nessus Essential Vulnerability Scanner (<OpenSSL 1.1.1q) .....	38
Tabel 12. Nessus Essential Vulnerability Scanner (<PHP 8.0.20 Risk High) .....	38
Tabel 13. Nessus Essential Vulnerability Scanner (<PHP 8.0.20 Risk Medium) .....	39
Tabel 14. Nessus Essential Vulnerability Scanner (TLS Protocol Detection) .....	39
Tabel 15. Nessus Essential Vulnerability Scanner (TLS Protocol Detection) .....	40
Tabel 16. Nessus Essential Vulnerability Scanner (SWEET32) .....	40
Tabel 17. Nessus Essential Vulnerability Scanner (SSL Certificate) .....	41
Tabel 18. Nessus Essential Vulnerability Scanner (SSL Self Sign) .....	42
Tabel 19. Nessus Essential Vulnerability Scanner (Apache mod_info) .....	42
Tabel 20. Nessus Essential Vulnerability Scanner (Apache mod_status) .....	43
Tabel 21. Nessus Essential Vulnerability Scanner (Apache multiviews) .....	43
Tabel 22. Nessus Essential Vulnerability Scanner (Trace/Track) .....	43
Tabel 23. Nessus Essential Vulnerability Scanner (SMB) .....	44
Tabel 24. SQLMap --dbs .....	56
Tabel 25. SQLMap --dbs --cookie .....	56
Tabel 26. Hasil MiTM Attack .....	57
Tabel 27. Report Planning and Preparation .....	62
Tabel 28. Report Assessment .....	63
Tabel 29. Fullscan sudo nmap -A 192.168.43.75 .....	68
Tabel 30. Fullxan sudo nmap -p "*" 192.168.43.75 .....	70

Tabel 31. Rincian Pemindaian Kerentanan Apache.....	70
Tabel 32. Rincian Pemindaian Kerentanan OpenSSL1.1.1o .....	73
Tabel 33. Rincian Pemindaian Kerentanan OpenSSL1.1.1p .....	73
Tabel 34. Rincian Pemindaian Kerentanan OpenSSL1.1.1q .....	74
Tabel 35. Rincian SQLMap --dbs .....	75
Tabel 36. Rincian SQLMap --dbs --cookie.....	78



STT - NF