

**PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK
(SIAMIK) UPN "VETERAN" JAWA TIMUR
MENGUNAKAN TEKNIK PENETRATION TESTING
DENGAN OWASP TOP 10**

SKRIPSI



Oleh:

FERNANDA TINAMBUNAN

19081010179

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

JAWA TIMUR

2024

LEMBAR PENGESAHAN

**Judul : PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK
(SIAMIK) UPN "VETERAN" JAWA TIMUR MENGGUNAKAN
TEKNIK PENETRATION TESTING DENGAN OWASP TOP 10**

Oleh : Fernanda Tinambunan

NPM : 19081010179

Telah Diseminarkan Dalam Ujian Skripsi

Pada : Hari Jumat, 05 Januari 2024

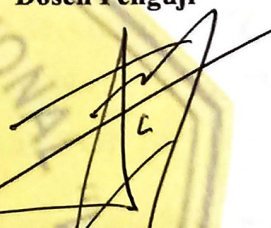
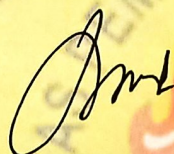
Mengetahui,

Dosen Pembimbing

Dosen Penguji

1.

1.

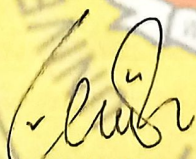


Achmad Junaidi, S.Kom, M.Kom
NPT. 3 7811 04 0199 1

Firza Prima Aditiawan, S.Kom, M.T.I
NIP. 19860523 2021211 003

2.

2.



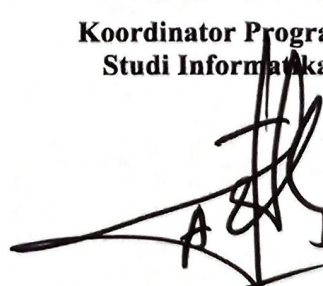
Agung Mustika Rizki, S.Kom, M.Kom
NIP. 199307252022031008

Andreas Nugroho Sihananto, S.Kom., M.Kom.
NPT. 211199 00 412271

Menyetujui,

**Dekan
Fakultas Ilmu Komputer,**

**Koordinator Program
Studi Informatika**



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

Fetty Tri Anggraeny, S.Kom, M.Kom
NIP. 19820211 2021212 005

SURAT PERNYATAAN ORISINALITAS

Saya, mahasiswa Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur, yang bertandatangan dibawah ini :

Nama : Fernanda Tinambunan

NPM : 19081010179

Menyatakan bahwa judul skripsi/tugas akhir yang saya ajukan dan dikerjakan, yang berjudul :

**“PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK
(SIAMIK) UPN “VETERAN” JAWA TIMUR MENGGUNAKAN TEKNIK
PENETRATION TESTING DENGAN OWASP TOP 10”**

Bukan merupakan plagiat dari skripsi/tugas akhir/penelitian orang lain dan juga merupakan produk dan atau software yang saya beli dari pihak lain. Saya juga menyatakan bahwa skripsi ini adalah pekerjaan saya sendiri, kecuali yang dinyatakan dalam daftar pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN “Veteran” Jawa Timur maupun di institusi Pendidikan lain. Apabila nanti terungkap bahwa pernyataan ini terbukti tidak benar, maka saya siap menerima segala konsekuensinya.

Surabaya, 5 Januari 2024

Hormat Saya,



Fernanda Tinambunan

NPM. 19081010179

PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK (SIAMIK) UPN "VETERAN" JAWA TIMUR MENGGUNAKAN TEKNIK PENETRATION TESTING DENGAN OWASP TOP 10

Nama Mahasiswa : Fernanda Tinambunan

NPM : 19081010179

Program Studi : Informatika

Dosen Pembimbing : Achmad Junaidi, S.Kom, M.Kom

Agung Mustika Rizki, S.Kom, M.Kom

ABSTRAK

Universitas Pembangunan Nasional "Veteran" Jawa Timur memiliki beberapa situs web yang menjadi sarana penting untuk mendukung, menyimpan, dan mengelola data krusial terkait proses perkuliahan. Namun, seiring dengan kemajuan teknologi informasi yang semakin kompleks, juga muncul ancaman dan tantangan keamanan siber yang meningkat. Oleh karena itu, diperlukan pengujian keamanan yang cermat terhadap situs web UPN "Veteran" Jawa Timur untuk mencegah kemungkinan terjadinya serangan peretasan yang dapat dilakukan oleh pihak yang tidak bertanggung jawab.

Penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi, dan menyoroti kerentanan keamanan yang mungkin ada dalam Sistem Informasi Akademik (SIAMIK), dengan menggunakan teknik *Penetration Testing* dengan fokus pada OWASP Top 10. OWASP (Open Web Application Security Project) Top 10 adalah daftar kerentanan keamanan yang umum pada aplikasi web yang diterbitkan oleh OWASP, organisasi yang mengkhususkan diri dalam keamanan aplikasi web. Penelitian ini mencakup analisis mendalam terhadap SIAMIK dengan pendekatan *Penetration Testing* yang mencakup tahapan pengumpulan data, analisa celah keamanan, pengujian, dan penulisan laporan.

Hasil pemindaian terhadap website SIAMIK mengungkapkan adanya 23 celah keamanan yang teridentifikasi, dimana sebanyak 20 celah tersebut masuk ke dalam kategori yang telah diidentifikasi oleh OWASP TOP 10. Temuan ini

memberikan gambaran yang signifikan bahwa sebagian besar celah keamanan yang terdeteksi sejalan dengan kategori kerentanan utama yang telah didefinisikan oleh standar OWASP TOP 10. Dari hasil ini, dapat disimpulkan bahwa penerapan OWASP TOP 10 sebagai acuan standar keamanan dalam melakukan uji penetrasi terbukti efektif dalam mengidentifikasi dan mengevaluasi celah keamanan yang signifikan pada sistem, serta memberikan arah yang tepat dalam meningkatkan tingkat keamanan pada website SIAMIK.

Kata kunci : Penetration Testing, OWASP Top 10, Sistem Informasi Akademik, Keamanan Sistem, UPN "Veteran" Jawa Timur

KATA PENGANTAR

Terimakasih kepada Tuhan Yang Maha Esa, yang telah memberikan kekuatan, kesabaran, dan hal-hal yang tidak diduga selama pengerjaan skripsi ini. Atas kasih karunia-Nya penulis dapat menyelesaikan skripsi dengan judul :


**“Pengujian Keamanan Sistem Informasi Akademik (SIAMIK) UPN
"Veteran" Jawa Timur Menggunakan Teknik Penetration Testing Dengan
OWASP Top 10”**

Tak lupa, penulis juga mengucapkan rasa terima kasih kepada orang-orang baik disekitar penulis yang senantiasa memberikan doa, dukungan moral, dan motivasi dalam setiap langkah perjalanan penulisan skripsi ini. Penulis sadar bahwa skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, segala kritik, saran, dan masukan dari pembaca serta pihak-pihak yang peduli akan sangat penulis hargai guna perbaikan di masa yang akan datang.

Akhir kata, penulis berharap bahwa skripsi ini dapat memberikan manfaat, kontribusi, serta pengetahuan yang bermanfaat bagi perkembangan ilmu pengetahuan di bidang yang terkait. Semoga skripsi ini dapat menjadi awal perjalanan pengetahuan yang lebih luas dan bermanfaat bagi pembaca.

Surabaya, 5 Januari 2024

Hormat Saya,


Fernanda Tinambunan

NPM. 19081010179

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan atas kehadiran Tuhan Yang Maha Esa telah memberikan rahmat, ridha, dan karunia-Nya. Dengan tulus dan penuh rasa syukur, penulis mengucapkan terima kasih yang tak terhingga atas bantuan, dukungan, dan bimbingan yang luar biasa selama proses penulisan skripsi ini. Takkan ada kata yang cukup mampu menggambarkan seberapa berharga kontribusi dalam membantu mengatasi setiap tantangan dan hambatan yang muncul. Ini adalah tonggak berharga dalam perjalanan akademik saya yang tak akan pernah saya lupakan. Pada kesempatan ini penulis menyampaikan rasa terimakasih yang sebesar-besarnya kepada :

1. Orang Tua, Adik, dan Keluarga yang telah memberikan dukungan secara materi dan non-materi sehingga penulis dapat menyelesaikan perkuliahan dari awal hingga akhir dengan baik.
2. Bapak Prof. Dr. Ir. Akhmad Fauzi, MMT. selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Ibu Dr. Novirina Hendrasarie, S.T, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Ibu Fetty Tri Anggraeny, S.Kom, M.Kom. selaku Koordinator Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Bapak Pratama Wiryana Atmaja, S.Kom, M.Kom selaku dosen wali yang membantu dalam perwalian dari awal sampai akhir perkuliahan.
6. Bapak Achmad Junaidi, S.Kom, M.Kom selaku dosen pembimbing pertama yang sangat membantu dan memberikan arahan sehingga dapat menyelesaikan tugas akhir ini dengan baik
7. Bapak Agung Mustika Rizki, S.Kom, M.Kom selaku pembimbing kedua yang telah membimbing dalam melakukan memberikan arahan pada tugas akhir ini dengan maksimal.
8. Bapak Firza Prima Aditiawan, S.Kom, M.T.I dan Bapak Andreas Nugroho Sihananto, S.Kom., M.Kom. selaku dosen penguji skripsi saya. Bimbingan,

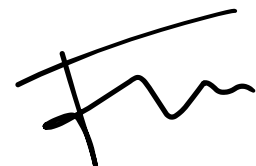
saran, dan pertanyaan yang diberikan sangat berarti bagi perkembangan dan penyempurnaan skripsi ini.

9. Seluruh Dosen dan Staf Tata usaha Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur yang telah memberikan ilmu yang bermanfaat selama perkuliahan.
10. Seluruh Staf Biro Akademik Kemahasiswaan Perencanaan & Kerjasama (BAKPK) UPN "Veteran" Jawa Timur yang telah memberikan kesempatan penulis untuk melakukan penelitian pada Sistem Informasi Akademik (SIAMIK) UPN “Veteran” Jawa Timur.
11. Agata, Agung, Erlin, Farra, Firman, Hermas, Jessica, Nadia, Nael, Niisa, Pab, Zara, dan seluruh teman-teman Informatika angkatan 2019 yang selalu menemani, memberikan dukungan, serta menawarkan bantuan sejak memasuki perkuliahan sampai saat ini.
12. Janji Jiwa Jilid 358 - Rungkut Madya yang telah menjadi saksi setiap langkah pengerjaan tugas akhir saya. Kenyamanan dan layanan baik yang diberikan Janji Jiwa membuat pengalaman saya di sini begitu berkesan.
13. Semua pihak yang penulis tidak sebutkan satu persatu.
14. Terakhir, terima kasih untuk diri sendiri, karena telah berusaha keras dan berjuang sejauh ini. Mampu menyelesaikan skripsi ini dengan baik dan semaksimal mungkin.

Akhir kata, penulis mengharapkan skripsi ini dapat memberikan manfaat bagi penulis khususnya dan bagi pembaca pada umumnya. Semoga Tuhan memberikan balasan yang berlipat ganda atas kebaikan yang telah diberikan.

Surabaya, 5 Januari 2024

Hormat Saya,



Fernanda Tinambunan

NPM. 19081010179

DAFTAR ISI

LEMBAR PENGESAHAN	i
SURAT PERNYATAAN ORISINALITAS	ii
ABSTRAK	iii
KATA PENGANTAR	v
UCAPAN TERIMA KASIH.....	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan.....	3
1.4 Manfaat.....	3
1.5 Batasan Masalah.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Penelitian Terdahulu.....	5
2.2 Gambaran Umum Instansi.....	7
2.2.1 Profil Instansi.....	7
2.2.2 Struktur Organisasi	8
2.3 Penetration Testing	9
2.3.1 Reconnaissance dan Information Gathering	12
2.3.2 Vulnerability Analysis	12
2.3.3 Vulnerability Exploits.....	12
2.3.4 Reporting	13

2.4 Vulnerability Scanning.....	13
2.5 OWASP Top 10.....	14
2.5.1 A01:2021-Broken Access Control.....	15
2.5.2 A02:2021-Cryptographic Failures	17
2.5.3 A03:2021-Injection.....	19
2.5.4 A04:2021-Insecure Design	21
2.5.5 A05:2021-Security Misconfiguration.....	23
2.5.6 A06:2021-Vulnerable and Outdated Components.....	24
2.5.7 A07:2021-Identification and Authentication Failures	25
2.5.8 A08:2021-Software and Data Integrity Failures.....	26
2.5.9 A09:2021-Security Logging and Monitoring Failures	27
2.5.10 A10:2021-Server-Side Request Forgery.....	28
2.6 Alat Bantu.....	29
2.6.1 Netcraft	29
2.6.2 Whois Lookup.....	30
2.6.3 Zenmap (Nmap GUI).....	31
2.6.4 OWASP Zed Attack Proxy (ZAP).....	34
2.6.5 Burp Suite	36
BAB III METODOLOGI PENELITIAN.....	38
3.1 Alur Penelitian.....	38
3.2 Cara Kerja Sistem.....	42
3.3 Alat Bantu Penelitian.....	44
BAB IV HASIL DAN PEMBAHASAN	45
4.1 Information Gathering	45
4.1.1 Netcraft	45
4.1.2 Whois	47

4.1.3 Nmap – Zenmap GUI	49
4.2 Vulnerability Scanning	53
4.3 Exploitation	57
4.3.1 Cross Site Scripting (Reflected)	57
4.3.2 Hash Disclosure - Mac OSX salted SHA-1	60
4.3.3 SQL Injection - Oracle - Time Based	61
4.3.4 SQL Injection – SQLite	63
4.3.5 Path Traversal	66
4.3.6 Content Security Policy (CSP) Header Not Set.....	68
4.3.7 Missing Anti-clickjacking Header	70
4.3.8 Vulnerable JS Library	72
4.3.9 Absence of Anti-CSRF Tokens	73
4.4 Laporan.....	74
4.4.1 Hasil	74
4.4.2 Rekomendasi Perbaikan.....	77
BAB V KESIMPULAN DAN SARAN.....	81
5.1 Kesimpulan.....	81
5.2 Saran	82
DAFTAR PUSTAKA	83
LAMPIRAN SURAT.....	86
LAMPIRAN.....	87

DAFTAR TABEL

Tabel 3.1 Perencanaan pengumpulan data	39
Tabel 4.1 Riwayat Hosting SIAMIK	46
Tabel 4.2 Hasil Pemindaian OWASP ZAP	54
Tabel 4.3 Kesimpulan Information Gathering	74
Tabel 4.4 Laporan Hasil Pengujian	76
Tabel 4.5 Hasil Payload XSS Reflected.....	87
Tabel 4.6 Hasil Payload SQL Injection - Oracle - Time Based	92
Tabel 4.7 Hasil Payload SQL Injection - SQLite.....	98
Tabel 4.8 Hasil Payload Path Traversal	105

DAFTAR GAMBAR

Gambar 2.1 Logo UPN "Veteran" Jawa Timur	7
Gambar 2.2 Struktur Organisasi UPN "Veteran" Jawa Timur.....	8
Gambar 2.3 Perubahan OWASP Top 10.....	14
Gambar 2.4 Netcraft.....	29
Gambar 2.5 ICANN	30
Gambar 2.6 Zenmap.....	31
Gambar 2.7 OWASP ZAP	34
Gambar 2.8 Tampilan Scan Otomatis	35
Gambar 2.9 Burp Suite.....	36
Gambar 3.1 Flowchart alur penelitian.....	38
Gambar 3.2 Target Pemindaian	41
Gambar 3.3 Halaman utama SIAMIK	42
Gambar 3. 4 Diagram Use Case SIAMIK.....	43
Gambar 4.1 Hasil Netcraft Pertama	45
Gambar 4.2 Hasil Netcraft Kedua.....	46
Gambar 4.3 Hasil Whois 114.xxx.xxx.xxx	47
Gambar 4.4 Hasil Whois 103.xxx.xxx.xxx	48
Gambar 4.5 Hasil ICANN 103.xxx.xxx.xxx.....	48
Gambar 4.6 Hasil ICANN 114.xxx.xxx.xxx.....	49
Gambar 4.7 Hasil Quick Scan 103.xxx.xxx.xxx.....	50
Gambar 4.8 Hasil Quick Scan 114.xxx.xxx.xxx	50
Gambar 4.9 Hasil Intense Scan 103.xxx.xxx.xxx	51
Gambar 4.10 Informasi Host Intense Scan 103.xxx.xxx.xxx	51

Gambar 4.11 Hasil Intense Scan 114.xxx.xxx.xxx	52
Gambar 4.12 Informasi Host Intense Scan 114.xxx.xxx.xxx	52
Gambar 4.13 Target pemindaian celah	53
Gambar 4.14 Celah yang ditemukan pada OWASP ZAP	53
Gambar 4.15 Perhitungan Jumlah Celah.....	54
Gambar 4.16 Celah Cross Site Scripting (Reflected) pada SIAMIK.....	58
Gambar 4.17 Penyerangan Cross Site Scripting (Reflected)	58
Gambar 4.18 Respon Cross Site Scripting (Reflected).....	59
Gambar 4.19 Hasil Payloads Reflected Cross-Site Scripting	59
Gambar 4.20 Celah Hash Disclosure pada SIAMIK	60
Gambar 4.21 Respon Hash Disclosure	60
Gambar 4.22 Hasil Dekripsi Hash	61
Gambar 4.23 Celah SQL Injection – Oracle – Time Based pada SIAMIK	61
Gambar 4.24 Penyerangan SQL Injection – Oracle – Time Based.....	62
Gambar 4.25 Waktu Respon SQL Injection – Oracle – Time Based.....	63
Gambar 4.26 Hasil Payloads SQL Injection – Time Based.....	63
Gambar 4.27 Celah SQL Injection – SQLite pada SIAMIK	64
Gambar 4.28 Penyerangan SQL Injection – SQLite.....	64
Gambar 4.29 Pengalihan ke Halaman Login	65
Gambar 4.30 Waktu Respon SQL Injection – SQLite.....	65
Gambar 4.31 Respon Payloads SQL Injection – SQLite.....	65
Gambar 4.32 Celah Path Traversal pada SIAMIK.....	66
Gambar 4.33 Penyerangan Path Traversal pada SIAMIK	67
Gambar 4.34 Pengalihan ke Halaman Utama	67
Gambar 4.35 Hasil Payloads Path Traversal.....	68

Gambar 4.36 Celah Content Security Policy (CSP) Header Not Set pada SIAMIK	68
Gambar 4.37 Contoh CSP Pada Web Github	69
Gambar 4.38 Script Tidak Bisa Dijalankan Pada Console	69
Gambar 4.39 Respons Headers SIAMIK	70
Gambar 4.40 Injeksi Script Pada Console SIAMIK	70
Gambar 4.41 Celah Missing Anti-clickjacking Header Pada SIAMIK	71
Gambar 4.42 Script Clickbandit.....	71
Gambar 4.43 Tampilan Burp ClickBandit	71
Gambar 4.44 Hasil Pengujian ClickJacking.....	72
Gambar 4.45 Tampilan Berhasil Menyerang Dengan Clickjacking	72
Gambar 4.46 Celah Vulnerable JS Library pada SIAMIK	72
Gambar 4.47 JQuery yang digunakan pada halaman SIAMIK.....	73
Gambar 4.48 Celah Absence of Anti-CSRF Tokens Pada SIAMIK	73
Gambar 4.49 Mencari Token CSRF.....	74