

SKRIPSI



**IMPLEMENTASI DAN OPTIMASI TERHADAP SERANGAN *BRUTE-FORCE*
PADA KEAMANAN WEB APLIKASI REGISTRASI MAHASISWA BARU UPN
VETERAN JAKARTA MENGGUNAKAN *PENETRATION TESTING***

FIQRI FADILLAH

NIM. 2010511023

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

2024

SKRIPSI

**Diajukan sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer
pada Fakultas Ilmu Komputer**



**IMPLEMENTASI DAN OPTIMASI TERHADAP SERANGAN *BRUTE-FORCE*
PADA KEAMANAN WEB APLIKASI REGISTRASI MAHASISWA BARU UPN
VETERAN JAKARTA MENGGUNAKAN *PENETRATION TESTING***

FIQRI FADILLAH

NIM. 2010511023

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

2024

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Fiqri Fadillah

NIM : 2010511023

Tanggal : 17 Agustus 2024

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 17 Agustus 2024

Yang menyatakan,



(Fiqri Fadillah)

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Fiqri Fadillah

NIM : 2010511023

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Non Eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

IMPLEMENTASI DAN OPTIMASI TERHADAP SERANGAN *BRUTE-FORCE* PADA KEAMANAN WEB APLIKASI REGISTRASI MAHASISWA BARU UPN VETERAN JAKARTA MENGGUNAKAN *PENETRATION TESTING*.

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/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.

Dibuat di : Tangerang

Pada tanggal : 17 Agustus 2024

Yang menyatakan,



(Fiqri Fadillah)

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Skripsi ini diajukan oleh:

Nama : Fiqri Fadillah
NIM : 2010511023
Program Studi : S-1 Informatika
Judul Skripsi/TA : IMPLEMENTASI DAN OPTIMASI TERHADAP
SERANGAN *BRUTE-FORCE* PADA KEAMANAN
WEB APLIKASI REGISTRASI MAHASISWA BARU
UPN VETERAN JAKARTA MENGGUNAKAN
PENETRATION TESTING

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.


Bayu Hananto, S.Kom, M.Kom
Penguji I


Kraugusteeliana, S.Kom., M.Kom., MM.
Penguji 2


Henki Bayu Seta, S.Kom., M.TI
Dosen Pembimbing I


Hamonangan Kinantan Prabu, S.T., M.T.
Dosen Pembimbing II


Prof. Dr. Ir. Sapriyanto, ST., M.Sc., IPM
Dekan Fakultas Ilmu Komputer


Dr. Widya Cholil, M.T
Kepala Program Studi S1 Informatika

Ditetapkan di : Jakarta

Tanggal Persetujuan : 16 Agustus 2024

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur senantiasa penulis panjatkan atas kehadiran ALLAH ﷻ, yang selalu melimpahkan rahmat dan karunia-NYA, sehingga Penulis dapat menyelesaikan penyusunan laporan Tugas Akhir atau Skripsi ini yang berjudul “IMPLEMENTASI DAN OPTIMASI TERHADAP SERANGAN *BRUTE-FORCE* PADA KEAMANAN WEB APLIKASI REGISTRASI MAHASISWA BARU UPN VETERAN JAKARTA MENGGUNAKAN *PENETRATION TESTING*”.

Dalam penyusunan skripsi ini, penulis tidak luput dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih kepada:

1. Ayah dan Ibu selaku orang tua dan saudara saudari dari penulis yang selalu memberikan dukungan dalam bentuk moral dan materil hingga saat ini.
2. Bapak Henki Bayu Seta, S.Kom, MTI, selaku Dosen Pembimbing 1 Skripsi yang telah banyak memberi masukan, arahan, dan saran yang sangat berguna dan berarti bagi Penulis dalam menyelesaikan Skripsi ini.
3. Bapak Hamonangan Kinantan Prabu, S.T, MT, selaku Dosen Pembimbing 2.
4. Bapak Jayanta, S.Kom., M.Si, selaku Dosen Pembimbing Akademik.
5. Bapak Sigit Pradana, S.T., M.T. yang telah memberikan izin penelitian kepada Penulis.
6. Bapak Fariz Setiawan., S.Kom selaku penanggung jawab sidang skripsi.
7. Kepada teman – teman seperjuangan saya dari tahun 2020 hingga sekarang Endow Bonapen, Rizky Firmansyah, dan Rizki Firmansyah yang selalu memberi dukungan dan berproses bersama baik suka maupun dukaselama proses perkuliahan dan penyelesaian Skripsi ini.
8. Kepada teman – teman yang baru saya jumpai di tengah masa perkuliahan Muhammad Thoriq Alfatih, Raffi Ramdhani, Arif Rahman Hakim, Muhammad Ronald Lullah, Muhammad Fadhillah Akbar, Muhammad Fhandika Rafif, Muhammad Ferdi, Adam Fauzan, Nisa Silaen, Nauval Laudza Munadjat Pattinggi, dan Annisa Nur Iksan.

Jakarta, 12 Juli 2024



Fiqri Fadillah

IMPLEMENTASI DAN OPTIMASI TERHADAP SERANGAN *BRUTE-FORCE* PADA KEAMANAN WEB APLIKASI REGISTRASI MAHASISWA BARU UPN VETERAN JAKARTA MENGGUNAKAN *PENETRATION TESTING*

FIQRI FADILLAH

ABSTRAK

Web aplikasi registrasi mahasiswa baru tahun 2024 UPN Veteran Jakarta adalah aplikasi berbasis web yang berfungsi untuk melayani pendaftaran mahasiswa baru di Universitas. Sebagai aplikasi berbasis pelayanan akademik, aplikasi ini mengandung data-data penting tentang mahasiswa baru seperti nama, nomor telepon, dan informasi lainnya. Namun, masalah keamanan pada aplikasi ini masih kurang mendapat perhatian dari pihak pengembang yang seharusnya segera ditangani agar tidak terjadi kebocoran data. Tujuan dari penelitian ini adalah untuk melakukan analisis dari segi keamanan pada web aplikasi registrasi mahasiswa baru tahun 2024 UPN Veteran Jakarta dan membuktikan kerentanan yang ditemukan. Penelitian ini menggunakan *Nessus* dan *OWASP* untuk menganalisa dan menguji potensi kerentanan pada aplikasi. Hasilnya, terdapat 389 akun mahasiswa baru yang berhasil diretas dengan memanfaatkan teknik *Brute Force* dengan total 1400 username yang di uji coba. Durasi Brute Force dalam meretas akun target berbeda-beda tergantung tanggal lahir mahasiswa.

Kata Kunci: Keamanan Web Aplikasi, Kerentanan, *Brute-Force*.

***IMPLEMENTATION AND OPTIMIZATION OF BRUTE-FORCE ATTACKS ON THE
WEB SECURITY OF THE NEW STUDENT REGISTRATION APPLICATION UPN
VETERAN JAKARTA USING PENETRATION TESTING***

FIQRI FADILLAH

ABSTRACT

Web application for new student registration in 2024 UPN Veteran Jakarta is a web-based application that serves to serve new student registration. web-based application that serves to serve new student registration at the University. As an academic service based application, this application contains important data about new students such as names, telephone numbers, and other information. However, security issues in this application still receive less attention from the developer which should be addressed immediately to prevent data leakage. The purpose of this research is to analyze the security of the 2024 UPN Veteran Jakarta new student registration web application and prove the vulnerabilities found. This research uses Nessus and OWASP to analyze and test potential vulnerabilities in the application. and test potential vulnerabilities in the application. As a result, there were 389 new student accounts that were successfully breached by utilizing Brute Force techniques with a total of 1400 usernames tested. usernames that were tested. Duration of Brute Force in breaking into the target account varies depending on the student's date of birth.

Keywords: *Web Application Security, Brute-Force.*

DAFTAR ISI

IMPLEMENTASI DAN OPTIMASI TERHADAP SERANGAN BRUTE-FORCE PADA KEAMANAN WEB APLIKASI REGISTRASI MAHASISWA BARU UPN VETERAN JAKARTA MENGGUNAKAN PENETRATION TESTING.....	ii
PERNYATAAN ORISINALITAS	iii
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	iv
LEMBAR PENGESAHAN	v
KATA PENGANTAR	vi
ABSTRAK.....	vii
<i>ABSTRACT</i>	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian	3
1.5 Batasan Masalah.....	4
1.6 Luaran Yang Diharapkan.....	4
1.7 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA.....	7
2.1 Keamanan Informasi	7
2.2 Web Aplikasi	8
2.2.1 Regmaba UPN Veteran Jakarta	9
2.3 <i>Web Application Attack</i>	10
2.4 Skema Mahasiswa baru UPN Veteran Jakarta	11
2.4.1 SNBP	11
2.4.2 SNBT	11
2.4.3 SEMA UPN Veteran Jakarta	12
2.5 Penetration Testing.....	12
2.5.1 Pendekatan <i>Penetration Testing</i>	13
2.6 Tahap <i>Penetration Testing</i>	14

2.7	<i>Vulnerability Assessment</i>	16
2.7.1	<i>CVSS Based-Severity Nessus</i>	16
2.7.2	<i>Vulnerability Priority Rating</i>	17
2.7.3	<i>VPR Key Driver</i>	18
2.8	<i>Open Web Application Security Project (OWASP)</i>	19
2.8.1	<i>OWASP Top 10</i>	20
2.8.2	<i>Perbandingan OWASP dan Metode lainnya</i>	24
2.9	<i>Alat yang digunakan</i>	25
2.10	<i>HTTP Status Codes</i>	33
2.10.1	<i>HTTP Status Code 1xx : Informational</i>	33
2.10.2	<i>HTTP Status Code 2xx: Success</i>	33
2.10.3	<i>HTTP Status Code 3xx : Redirection</i>	33
2.10.4	<i>HTTP Status Code 4xx: Client Error</i>	34
2.10.5	<i>HTTP Status Code 5xx: Server Error</i>	35
2.11	<i>Review Penelitian Terdahulu</i>	35
BAB III METODELOGI PENELITIAN		39
3.1	<i>Tahapan Penelitian</i>	39
3.1.1	<i>Identifikasi Masalah</i>	39
3.1.2	<i>Studi Literatur</i>	40
3.1.3	<i>Fase Planning (Perencanaan)</i>	40
3.1.4	<i>Fase Discovery (Penemuan)</i>	40
3.1.5	<i>Fase Attack (Serangan)</i>	41
3.1.6	<i>Fase Reporting (Pelaporan)</i>	41
3.2	<i>Alat Bantu Penelitian Penelitian</i>	41
3.2.1	<i>Perangkat Keras</i>	41
3.2.2	<i>Perangkat Lunak</i>	41
3.2.3	<i>Jadwal Penelitian</i>	42
BAB IV		44
HASIL DAN PEMBAHASAN		44
4.1	<i>Tahap Planning</i>	44
4.1.1	<i>Topologi dan arsitektur serangan</i>	45
4.1.2	<i>Jadwal Kerja Penelitian</i>	46
4.2	<i>Fase Discovery</i>	46
4.2.1	<i>Genelify</i>	46
4.2.2	<i>Nslookup</i>	49
4.2.3	<i>DNS Analysis</i>	50

4.2.4	Live Host Identification	54
4.2.5	Whatweb	55
4.2.6	Whois	57
4.2.7	<i>Httpprint</i>	59
4.2.8	NMAP	62
4.2.9	Nessus	63
4.2.10	OWASP ZAP.....	72
4.3	<i>Fase Attack</i>	77
4.3.1	<i>Apache Unsupported Version</i>	78
4.3.2	<i>PHP Unsupported Version</i>	78
4.3.3	<i>SSL Version 2 and 3 Protocol Detection</i>	79
4.3.4	SSL Medium Strength Cipher Suites Supported (SWEET32)	80
4.3.5	Missing HTTP Strict Transport Security Policy	81
4.3.6	<i>Content Security Policy not Set</i>	82
4.3.7	<i>DDOS Resource Availability</i>	83
4.3.8	OSINT.....	83
4.3.9	<i>Brute Force Attack</i>	85
4.4	<i>Fase Reporting</i>	97
BAB V		100
KESIMPULAN DAN SARAN		100
5.1	Kesimpulan	100
5.2	Saran.....	101
DAFTAR PUSTAKA		xiv
LAMPIRAN		xvii

DAFTAR TABEL

Tabel 2.1 CVSS Based Severity	17
Tabel 2.2 VPR Range.....	18
Tabel 2.3 VPR Key Driver.....	18
Tabel 2.4 Perbandingan OWASP dan Metode Lainnya	24
Tabel 2.5 Tools yang digunakan	26
Tabel 2.6 Perbandingan Tools.....	28
Tabel 2.7 Penelitian terdahulu	35
Tabel 3.1 Tahapan Penelitian	43
Tabel 4.1 Hasil DNS Enumerasi	51
Tabel 4.2 Informasi umum whois terdahulu	57
Tabel 4.3 Informasi Alamat hasil whois	58
Tabel 4.4 Informasi pemilik web aplikasi.....	59
Tabel 4.5 Port Open NMAP.....	62
Tabel 4.6 Vulnerability assessment Nessus	63
Tabel 4.7 Vulnerability OWASP ZAP.....	72
Tabel 4.8 Generate Username	86
Tabel 4.9 Brute Force Percobaan 1	87
Tabel 4.10 Brute Force hasil 1	88
Tabel 4.11 Brute Force Percobaan 2	88
Tabel 4.12 Brute Force Hasil 2	89
Tabel 4.13 Brute Force Percobaan 3	89
Tabel 4.14 Brute Force Hasil 3	90
Tabel 4.15 Brute Force Percobaan 4	90
Tabel 4.16 Brute Force Hasil 4	91
Tabel 4.17 Brute Force Percobaan 5	92
Tabel 4.18 Brute Force Hasil Keseluruhan	92
Tabel 4.19 Rekomendasi Mitigasi	97

DAFTAR GAMBAR

Gambar 2.1 Halaman depan regmaba.....	10
Gamba 2.2 Perbandingan OWASP 2017 dan 2021	20
Gambar 3.1 Alur Penelitian	39
Gambar 4.1 Surat permohonan izin penelitian	44
Gambar 4.2 Topologi Serangan	45
Gambar 4.3 Infrastruktur web server.....	44
Gambar 4.4 Hasil Genelify 1	47
Gambar 4.5 Hasil Genelify 2	47
Gambar 4.6 Hasil NSLookup.....	49
Gambar 4.7 Hasil DNS Enumeration	50
Gambar 4.8 Hasil Enumerasi IPv6	52
Gambar 4.9 Hasil DNSenum	52
Gambar 4.10 Name Server.....	53
Gambar 4.11 Hasil Subdomain Finder.....	53
Gambar 4.12 Hasil DNS Mapper.....	54
Gambar 4.13 Hasil Fping.....	54
Gambar 4.14 Tes Koneksi ke host	55
Gambar 4.15 Whatweb 1	56
Gambar 4.16 Hasil Whatweb 2	56
Gambar 4.17 Hasil whatweb 3.....	57
Gambar 4.18 Hasil httpprint	60
Gambar 4.19 Hasil httpprint informasi server	61
Gambar 4.20 Hasil httpprint informasi ssl.....	61
Gambar 4.21 Apache HTTP Unsupported	78
Gambar 4.22 Versi Apache usang	78
Gambar 4.23 Versi PHP tidak support	79
Gambar 4.24 SSL.....	79
Gambar 4.25 Hasil SSL CIPHER 22	80
Gambar 4.26 CSP Broken.....	82
Gambar 4.27 DDOS Timeout	83
Gambar 4.28 Contoh Hasil OSINT.....	84
Gambar 4.29 Hasil OSINT Username	84

Gambar 4.30 Skema Brute Force Attack	85
Gambar 4.31 Percobaan serangan brute force	87
Gambar 4.32 Halaman Utama regmaba.....	96
Gambar 4.33 Dokumen sensitive regmaba	96
Gambar 4.34 Informasi akun mahasiswa.....	97

DAFTAR LAMPIRAN

Lampiran 1. Surat Pengajuan Penelitian

Lampiran 2. Balasan Surat Penelitian

Lampiran 3. Surat Pakta Integritas

Lampiran 4. Hasil *Brute-Force Attack*

Lampiran 5. Turnitin