

SKRIPSI



**ANALISIS KERENTANAN WEB API STUDI KASUS : DAMN
VULNERABLE WEB SERVICES-NODE YANG MENGGUNAKAN WEB
APPLICATION FIREWALL OPEN-APPSEC**

MUHAMMAD THORIQ AL-FATIH

2010511025

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
2024**

SKRIPSI



**ANALISIS KERENTANAN WEB API STUDI KASUS : DAMN
VULNERABLE WEB SERVICES-NODE YANG MENGGUNAKAN WEB
APPLICATION FIREWALL OPEN-APPSEC**

MUHAMMAD THORIQ AL-FATIH

2010511025

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Komputer**

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
2024**

PERNYATAAN ORISINALITAS

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

Nama : Muhammad Thoriq Al-fatih

NIM : 2010511025

Tanggal : 10 Juli 2024

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

Jakarta, 10 Juli 2024

Yang Menyatakan



Muhammad Thoriq Al-fatih

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama : Muhammad Thoriq Al-fatih
NIM : 2010511025
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 :

ANALISIS KERENTANAN WEB API STUDI KASUS : DAMN VULNERABLE WEB SERVICES-NODE YANG MENGGUNAKAN WEB APPLICATION FIREWALL OPEN-APPSEC

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 : Jakarta

Pada Tanggal : 10 Juli 2024

Yang menyatakan,



Muhammad Thoriq Al-Fatih)

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Skripsi ini diajukan oleh:

Nama : Muhammad Thoriq Al-fatih
NIM : 2010511025
Program Studi : S-1 Informatika
Judul Skripsi/TA : Analisis Kerentanan Web API Studi Kasus : Damn Vulnerable Web Service-Node Yang Menggunakan Web Application Firewall OPEN-APPSEC

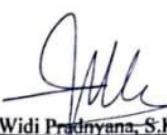
Telah berhasil dipertahankan dihadapan Tim Pengaji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.


Theresia Wati, S.Kom.,M.TI

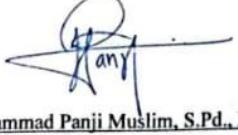
Pengaji 1


Hamonangan Kinantan Prabu, S.T., M.T.

Pengaji 2

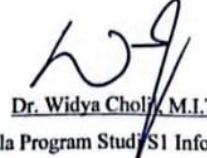

I Wayan Widi Pradnyana, S.Kom., M.TI

Dosen Pembimbing I


Muhammad Panji Muslim, S.Pd., M.Kom.

Dosen Pembimbing II




Dr. Widya Cholif, M.I.T
Kepala Program Studi S1 Informatika

Ditetapkan di : Jakarta
Tanggal Persetujuan : 10 Juli 2024

KATA PENGANTAR

Assalamu'alaikum wr,wb. Puji dan syukur penulis panjatkan kepada Allah SWT atas berkat dan rahmat-Nyalah sehingga penulis dapat menyelesaikan skripsi ini tepat pada waktunya. Skripsi ini berjudul " Analisis Kerentanan Web API Studi Kasus : Damn Vulnerable Web Services-Node yang Menggunakan Web Application Firewall Open-appsec". Penulis ingin menyampaikan terima kasih kepada :

1. Ayah dan Ibu yang selalu mendoakan, mendukung penuh penyelesaian tugas skripsi ini, dengan memberikan semangat dan motivasi.
2. Bapak I Wayan Pradnyana, S.Kom., MTI selaku Dosen Pembimbing 1, atas bimbingan dan dukungan yang diberikan selama proses penyusunan skripsi ini.
3. dan Bapak Muhammad Panji Muslim, S.Pd.,M., Kom. selaku Dosen Pembimbing 2, atas bimbingan dan dukungan yang diberikan selama proses penyusunan skripsi ini.
4. Ibu Widya Cholil, M.I.T selaku ketua prodi informatika yang telah memberikan kemudahan dan kelancaran dalam pelaksanaan tugas akhir skripsi ini.
5. Muhammad Ferdiansyah yang telah meminjamkan laptopnya kepada saya sehingga saya bisa mencapai pada target tugas akhir ini.
6. Dan untuk semua sahabat saya yang selalu memberikan motivasi, dukungan serta doanya yang selalu dipanjatkan untuk kemudahan dalam mengerjakan tugas akhir skripsi ini.

Penulis juga ingin menyampaikan terima kasih kepada semua pihak yang telah memberikan dukungan moril maupun materil sehingga skripsi ini dapat diselesaikan. Semoga skripsi ini dapat memberikan manfaat dan kontribusi pada bidang keamanan siber.

Jakarta 20 Juni 2024



Muhammad Thoriq Al-fatih

DAFTAR ISI

SKRIPSI	i
SKRIPSI	i
PERNYATAAN ORISINALITAS.....	ii
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	iii
LEMBAR PENGESAHAN.....	iv
ABSTRAK.....	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xiv
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan Penelitian	3
1.4 Manfaat Penelitian	3
1.5 Batasan Masalah	3
1.6 Luaran yang diharapkan.....	4
BAB II TINJAUAN PUSTAKA	5
2.1 Analisis	5
2.2 Kerentanan	5
2.2.1 Cross-Site Scripting (XSS).....	5
2.2.2 NoSQL <i>Injection</i> - Remote Code Execution (RCE).....	5
2.2.3 SQL <i>Injection</i>	5
2.2.4 Hidden API Functionality Exposure.....	6
2.2.5 XML RPC (Remote Procedure Call) User Enumeration.....	6

	ix	
2.2.6	<i>Mass Assignment</i>	6
2.2.7	<i>Path Traversal</i>	6
2.2.8	<i>JSON Hijacking</i>	6
2.2.9	<i>Command Injection -Remote Code Execution (RCE)</i>	6
2.2.10	<i>Insecure Direct Object Reference (IDOR)</i>	7
2.3	<i>Website (web)</i>	7
2.4	<i>Application (Aplikasi)</i>	7
2.5	<i>Web Application (Aplikasi Web)</i>	7
2.6	Firewall	8
2.7	Web Application Firewall (WAF)	8
2.8	<i>Application Programming interface (API)</i>	8
2.9	<i>Web Application Programming Interface (API)</i>	8
2.10	Eksloitasi Kerentanan.....	9
2.11	Monitoring.....	9
2.12	Deteksi.....	9
2.13	Mitigasi.....	9
2.14	Damn Vulnerable Web Service (DVWS-Node)	9
2.15	<i>Machine Learning</i>	10
2.16	OPEN-APPSEC	10
2.17	DOCKER	11
2.18	<i>Diagram Sequence</i>	11
2.19	Windows Subsystem For Linux	12
2.20	Burp Suite Community Edition.....	12
2.21	<i>Common Vulnerability Scoring System (CVSS)</i>	12
2.22	OWASP Top 10 API Security Risk 2023	13
2.23	Kajian Literatur	15
	BAB III METODOLOGI PENELITIAN	17

3.1	Tahapan Penelitian.....	17
3.1.1	Identifikasi Masalah	18
3.1.2	Studi Literatur.....	18
3.1.3	Persiapan lingkungan dan Perancangan sistem	18
3.1.4	Melakukan Uji Kerentanan.....	18
3.1.5	Analisis Kerentanan.....	19
3.1.6	Melakukan Perancangan Keamanan.....	19
3.1.7	Alat Bantu Penelitian.....	19
3.2	Jadwal Kegiatan.....	19
	BAB IV PEMBAHASAN DAN HASIL.....	21
4.1	Identifikasi Masalah.....	21
4.2	Studi Literatur	22
4.3	Persiapan Lingkungan dan Perancangan Sistem.....	23
4.3.1	Persiapan Lingkungan	23
4.3.2	Perancangan Sistem.....	24
4.4	Identifikasi Kerentanan.....	27
4.5	Activity Diagram	28
4.6	Eksplorasi Kerentanan	30
4.6.1	<i>Cross-Site Scripting (XSS)</i>	30
4.6.2	<i>NoSQL Injection - Remote Code Execution (RCE)</i>	34
4.6.3	<i>SQL Injection</i>	38
4.6.4	<i>Hidden API Functionality Exposure</i>	42
4.6.5	<i>XML RPC (Remote Procedure Call) user enumeration</i>	45
4.6.6	<i>Mass Assignment</i>	49
4.6.7	Path Traversal.....	53
4.6.8	JSON Hijacking.....	57
4.6.9	<i>Command Injection</i>	60

4.6.10 <i>Insecure Direct Object Reference (IDOR)</i>	64
4.7 Analisis dan Evaluasi	67
BAB V KESIMPULAN DAN SARAN	71
5.1 KESIMPULAN	71
5.2 SARAN	71
DAFTAR PUSTAKA	72
LAMPIRAN	77
DAFTAR RIWAYAT HIDUP	90

DAFTAR GAMBAR

Gambar 2.1 Infrastruktur Docker 1(sumber : (Docker Overview Docker Docs, n.d.))	11
Gambar 3.1 Tahapan Penelitian	17
Gambar 4.5 Diagram Sequence	28
Gambar 4.6 Kerentanan XSS	30
Gambar 4.7 Monitoring deteksi kerentanan oleh WAF open-appsec	31
Gambar 4.8 Perancangan keamanan WAF open-appsec	33
Gambar 4.9 Uji ulang Kerentanan XSS	34
Gambar 4.10 Log Details Pencegahan XSS	34
Gambar 4.11 Kerentanan NoSQL-RCE	35
Gambar 4.12 Log Details Deteksi oleh WAF open-appsec	35
Gambar 4.13 Perancangan kemaanan WAF open-appsec	38
Gambar 4.17 Uji Ulang kerentanan SQL Injection	39
Gambar 4.19 Kerentanan Hidden API Functionality Exposure	42
Gambar 4.20 Perancangan keamanan WAF open-appsec	44
Gambar 4.21 Pencegahan oleh WAF open-appsec	45
Gambar 4.23 Kerentanan XML RPS (Remote Procedure Call) user enumeration	46
Gambar 4.24 Perancangan keamanan WAF open-appsec	48
Gambar 4.25 Uji ulang Kerentanan XML RPC	48
Gambar 4.27 Kerentanan Mass Assignment	49
Gambar 4.28 Perancangan Keamanan	52
Gambar 4.29 Pencegahan oleh WAF open-appsec	52
Gambar 4.31 Kerentanan Path Traversal	53
Gambar 4.32 Log details deteksi path Traversal	53
Gambar 4.33 Perancangan Keamanan Path Traversal	56
Gambar 4.34 Uji ulang Kerentanan	56
Gambar 4.35 Log details pencegahan kerentanan	57
Gambar 4.36 Kerentanan JSON Hijacking	57
Gambar 4.37 Perancangan keamanan	59
Gambar 4.38 Uji Ulang kerentanan	60
Gambar 4.39 Monitoring log details pencegahan	60
Gambar 4.40 Kerentanan Command Injection	61
Gambar 4.41 Uji ulang kerentanan	63
Gambar 4.42 Monitoring Log details pencegahan	64

Gambar 4.43 Kerentanan IDOR	64
Gambar 4.44 Perancangan keamanan IDOR	67
Gambar 4.45 Uji ulang kerentanan	67

DAFTAR TABEL

Table 2.1 Qualitative severity rating scale	12
Tabel 2.2 OWASP Top 10 API security risks 20231sumber: (OWASP, 2023).....	13
Tabel 2.3 Kajian Literatur	15
Tabel 3.2 Jadwal Kegiatan	20
Tabel 4.4. Identifikasi Kerentanan	27
Tabel 4.6 Nilai Risiko Kerentanan XSS	32
Tabel 4.7 Nilai Risiko Kerentanan NoSQL Injection	37
Tabel 4.8 Penilaian Risiko Kerentanan SQL Injection	41
Tabel 4.9 Penilaian Risiko Kerentanan Hidden API Functionality Exposure	43
Tabel 4.10 Penilaian Risiko Kerentanan XML RPC	47
Tabel 4.11 Penilaian Risiko Kerentanan Mass Assignment	51
Tabel 4.12 Penilaian Risiko Kerentanan Path Traversal	55
Tabel 4.13 Penilaian Risiko Kerentanan JSON Hijacking.....	59
Tabel 4.14 Nilai Risiko kerentanan Command Injection	62
Tabel 4.15 Nilai Risiko kerentanan IDOR	66

DAFTAR LAMPIRAN

Lampiran 1. Halaman Login DVWS-Node

Lampiran 2. Halaman Home DVWS-Node

Lampiran 3. Dashboard OPEN-APPSEC

Lampiran 4. Monitoring OPEN-APPSEC

Lampiran 5. Hasil Turnitin