

**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 Penguji 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

Penguji 1



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

Penguji 2



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

Dosen Pembimbing I



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

Dosen Pembimbing II



Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM

Dekan Fakultas Ilmu Komputer



Dr. Widya Cholita, 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
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
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
<b>BAB II TINJAUAN PUSTAKA .....</b>	<b>5</b>
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	<i>Firewall</i> .....8
2.7	<i>Web Application Firewall (WAF)</i> .....8
2.8	<i>Application Programming interface (API)</i> .....8
2.9	<i>Web Application Programming Interface (API)</i> .....8
2.10	<i>Eksploitasi Kerentanan</i> .....9
2.11	<i>Monitoring</i> .....9
2.12	<i>Deteksi</i> .....9
2.13	<i>Mitigasi</i> .....9
2.14	<i>Damn Vulnerable Web Service (DVWS-Node)</i> .....9
2.15	<i>Machine Learning</i> .....10
2.16	<i>OPEN-APPSEC</i> .....10
2.17	<i>DOCKER</i> .....11
2.18	<i>Diagram Sequence</i> .....11
2.19	<i>Windows Subsystem For Linux</i> .....12
2.20	<i>Burp Suite Community Edition</i> .....12
2.21	<i>Common Vulnerability Scoring System (CVSS)</i> .....12
2.22	<i>OWASP Top 10 API Security Risk 2023</i> .....13
2.23	<i>Kajian Literatur</i> .....15
<b>BAB III</b>	<b>METODOLOGI PENELITIAN</b> .....17



	x
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 Eksploitasi 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 <i>Path Traversal</i> .....	53
4.6.8 <i>JSON Hijacking</i> .....	57
4.6.9 <i>Command Injection</i> .....	60

	xi
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

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

	xiii
<b>Gambar 4.43 Kerentanan IDOR .....</b>	<b>64</b>
<b>Gambar 4.44 Perancangan keamanan IDOR .....</b>	<b>67</b>
<b>Gambar 4.45 Uji ulang kerentanan .....</b>	<b>67</b>

**DAFTAR TABEL**

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