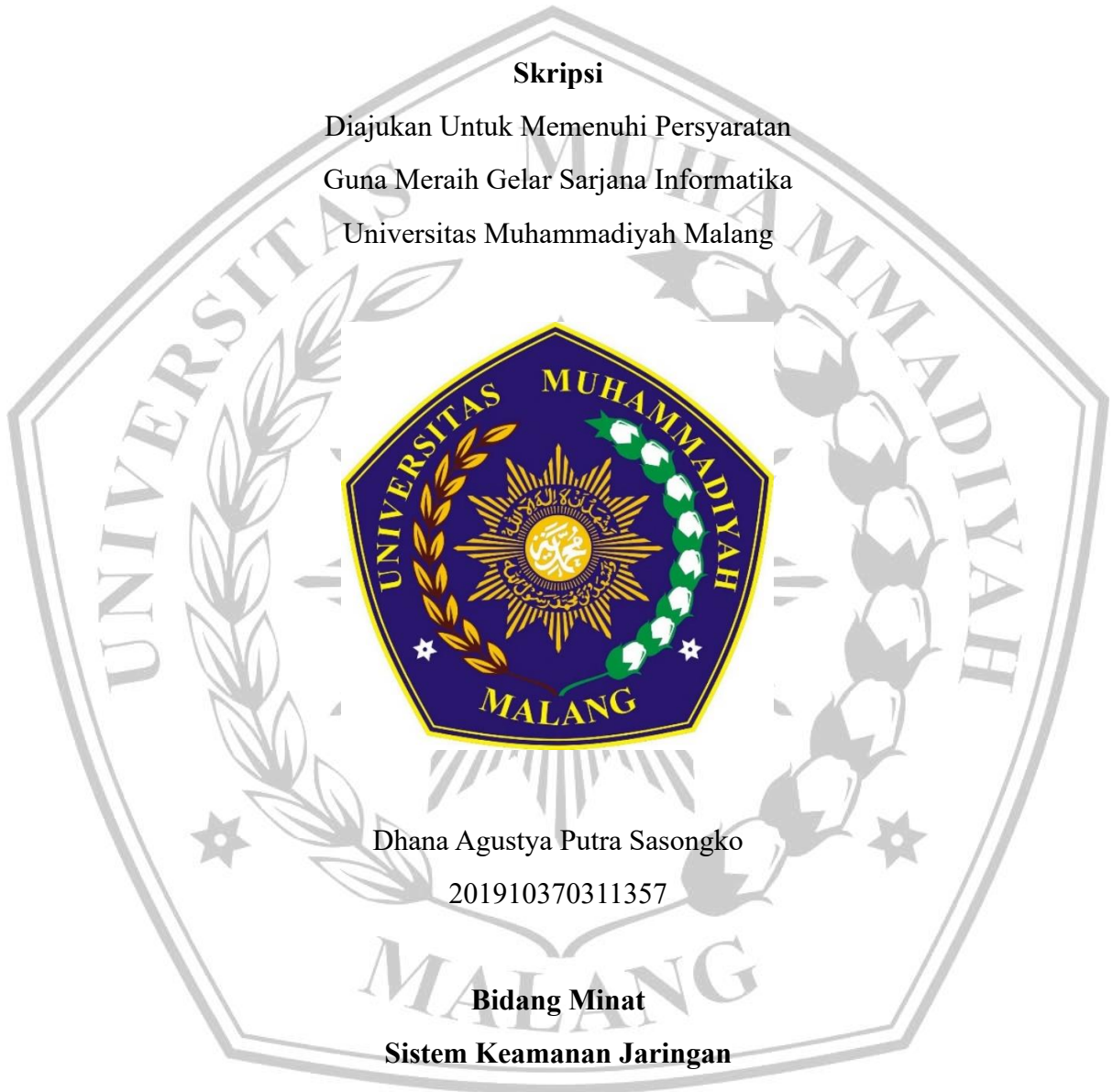


**ANALISIS METODE VULNERABILITY SCANNING  
DAN PERBANDINGAN PENETRATION TESTING DENGAN  
INTRUSION DETECTION SYSTEM TERHADAP  
VULNERABLE WEBSITE**

**Skripsi**

Diajukan Untuk Memenuhi Persyaratan  
Guna Meraih Gelar Sarjana Informatika  
Universitas Muhammadiyah Malang



Dhana Agustya Putra Sasongko

201910370311357

**Bidang Minat**

**Sistem Keamanan Jaringan**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH MALANG**

**2024**

## LEMBAR PERSETUJUAN

# ANALISIS METODE VULNERABILITY SCANNING DAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE

## TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Informatika Universitas Muhammadiyah Malang

Menyetujui,

Malang, 22 November 2024

Dosen Pembimbing 1



Luqman Hakim S.Kom., M.Kom.

NIP. 10819030658PNS.

Dosen Pembimbing 2



=

NIP.

**LEMBAR PENGESAHAN**  
**ANALISIS METODE VULNERABILITY SCANNING DAN**  
**PENETRATION TESTING DENGAN INTRUSION**  
**DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE**  
**TUGAS AKHIR**

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Informatika Universitas Muhammadiyah Malang

Disusun Oleh :

**DHANA AGUSTYA PUTRA SASONGKO**  
**201910370311357**

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji  
pada tanggal 22 November 2024

Menyetujui,

Dosen Penguji 1



**Diah Risqiwati ST., MT.**  
**NIP. 10814100545PNS.**

Dosen Penguji 2



**Ir. Wildan Suharso S.Kom., M.Kom**  
**NIP. 10817030596PNS.**

Mengetahui,  
Ketua Jurusan Informatika



**Galih Wasis Wicaksono S.kom. M.Cs.**  
**NIP. 10814100541PNS.**



## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

**NAMA : DHANA AGUSTYA PUTRA SASONGKO**

**NIM : 201910370311357**

**FAK./JUR. : Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul “ANALISIS METODE VULNERABILITY SCANNING DAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE” beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,  
Dosen Pembimbing



Luqman Hakim S.Kom., M.Kom.

Malang, 22 November 2024  
buat Pernyataan



**DHANA AGUSTYA PUTRA  
SASONGKO**

## ABSTRAK

Kemajuan teknologi jaringan, termasuk internet, telah mendorong perkembangan website sebagai wadah informasi yang mudah diakses dan digunakan untuk berbagai aktivitas. Namun, peningkatan jumlah website juga membuka peluang bagi hacker dan cracker untuk mengeksploitasi kerentanan sistem keamanan, seperti pencurian data dan serangan sistem. Berbagai metode pengujian keamanan, seperti white box dan black box testing, digunakan untuk mendeteksi kerentanan pada aplikasi web. Salah satu teknologi keamanan yang banyak digunakan adalah Intrusion Detection System (IDS) berbasis Snort, yang memiliki kemampuan mendeteksi ancaman dengan ribuan aturan keamanan. Penelitian ini bertujuan untuk mengembangkan sistem keamanan berbasis Snort melalui pengujian menggunakan metode Vulnerability Scanning dan Penetration Testing. Dengan menganalisis hasil identifikasi terhadap berbagai pola serangan, penelitian ini diharapkan dapat meningkatkan kemampuan Snort dalam mendeteksi serangan secara lebih mendetail dan memberikan kontribusi terhadap perancangan sistem keamanan website yang lebih stabil dan efektif.

**Kata Kunci:** Keamanan Website, Snort, Intrusion Detection System (IDS), Vulnerability Scanning, Penetration Testing, Kerentanan Aplikasi Web.

## ABSTRACT

The advancement of network technology, including the internet, has driven the rapid growth of websites as accessible platforms for information and various activities. However, the increasing number of websites also presents opportunities for hackers and crackers to exploit system vulnerabilities, such as data theft and system attacks. Various security testing methods, including white box and black box testing, are utilized to detect vulnerabilities in web applications. One widely used security technology is the Snort-based Intrusion Detection System (IDS), known for its ability to detect threats using thousands of security rules. This study aims to enhance the Snort-based security system through testing methods such as Vulnerability Scanning and Penetration Testing. By analyzing the identification results against various attack patterns, this research seeks to improve Snort's capability in detecting attacks more comprehensively and contribute to designing a more stable and effective web security system.

**Keywords:** Website Security, Snort, Intrusion Detection System (IDS), Vulnerability Scanning, Penetration Testing, Web Application Vulnerabilities.

## KATA PENGANTAR

Dengan memanjatkan puji syukur ke hadirat Allah SWT atas limpahan rahmat dan hidayah-Nya, sehingga peneliti dapat menyelesaikan tugas akhir yang berjudul:

### **“ANALISIS METODE VULNERABILITY SCANNING DAN PERBANDINGAN PENETRATION TESTING DENGAN INTRUSION DETECTION SYSTEM TERHADAP VULNERABLE WEBSITE”**

Di dalam tulisan ini disajikan pokok-pokok bahasan yang meliputi teori dasar mengenai teknologi jaringan dan sistem keamanan, analisis kerentanan aplikasi web, metode pengujian keamanan menggunakan Snort, serta pengujian menggunakan metode vulnerability scanning dan penetration testing untuk mengidentifikasi dan mengatasi ancaman terhadap keamanan website. Penelitian ini bertujuan untuk memberikan solusi dalam meningkatkan keamanan website melalui teknologi IDS berbasis Snort.

Peneliti menyadari sepenuhnya bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dan keterbatasan. Oleh karena itu, peneliti mengharapkan saran yang membangun agar tulisan ini bermanfaat bagi perkembangan ilmu pengetahuan, khususnya dalam bidang keamanan jaringan dan aplikasi web.

Malang, 07 Desember 2024

Dhana Agustya Putra Sasongko

## DAFTAR ISI

LEMBAR PERSETUJUAN.....	ii
LEMBAR PERNYATAAN .....	iii
KATA PENGANTAR.....	iv
ABSTRAK .....	v
ABSTRACT.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR .....	xiv
BAB I.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Tujuan Penelitian.....	3
1.4 Batasan Masalah.....	4
BAB II.....	5
2.1 Sistem Keamanan Jaringan.....	5
2.1.1 <i>Firewall</i> .....	5
2.1.2 Enkripsi.....	5
2.1.3 <i>Virtual Private Network (VPN)</i> .....	5
2.1.4 Keamanan Nirkabel .....	5
2.1.5 Pemantauan Jaringan .....	6
2.2 Serangan <i>Website</i> .....	6
2.2.1 SQL Injection.....	6

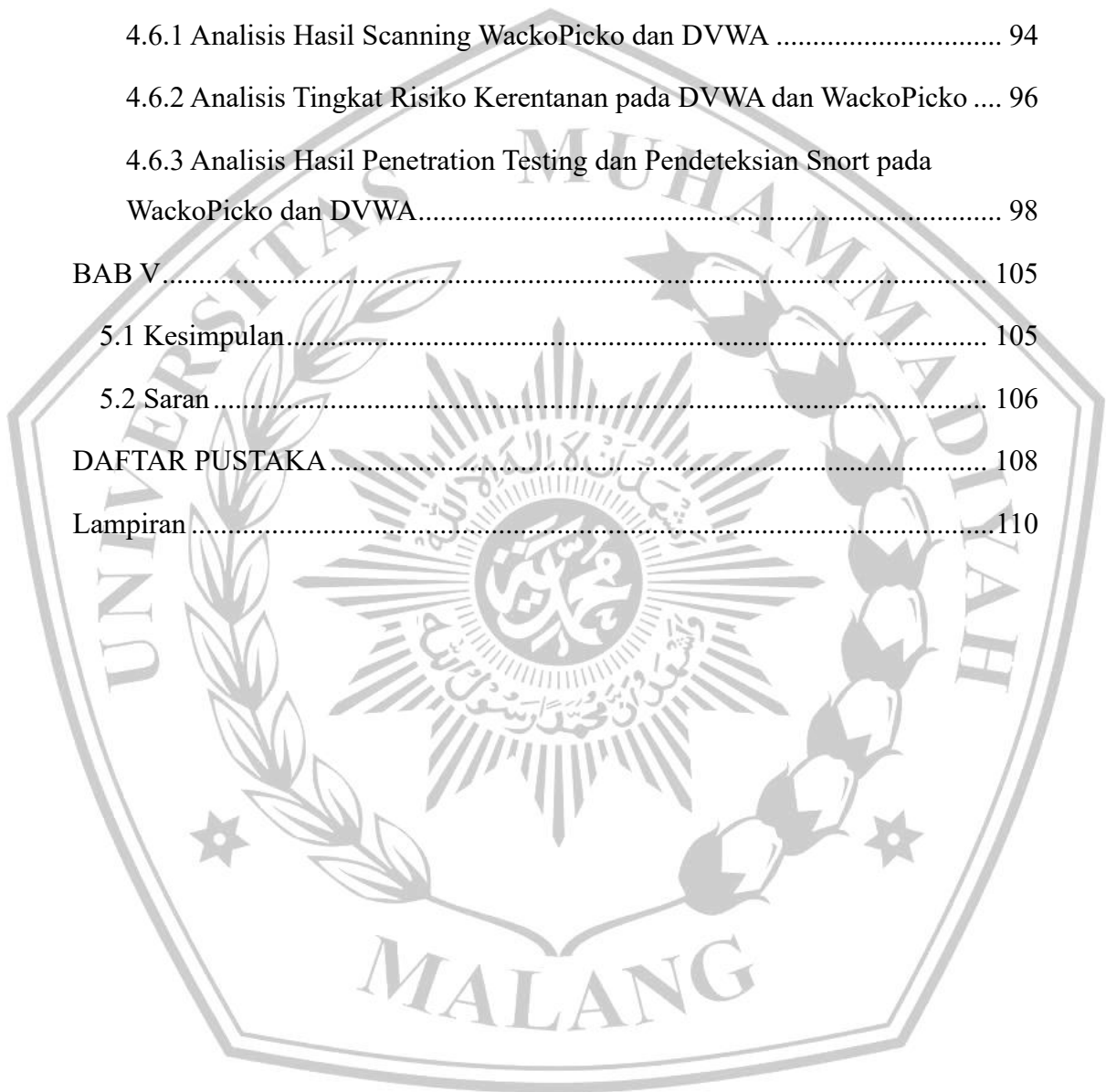


2.2.2 DoS .....	6
2.2.3 XSS .....	7
2.3 <i>Vulnerable Website</i> .....	7
2.3.1 DVWA .....	8
2.3.2 WackoPicko .....	8
2.4 <i>Intrusion Detection System (IDS)</i> .....	9
2.4.1 <i>Host-based Intrusion Detection System (HIDS)</i> .....	9
2.4.2 <i>Network-based Intrusion Detection System (NIDS)</i> .....	9
2.5 Snort .....	10
2.6 Penelitian Terdahulu .....	11
2.7 <i>Vulnerability Scanning</i> .....	13
2.7.1 Identifikasi Kelemahan .....	13
2.7.2 Skanning Otomatis.....	13
2.7.3 Analisis Hasil .....	14
2.8 <i>Penetration Testing</i> .....	14
2.8.1 Tujuan Pengujian .....	14
2.8.2 Skenario Serangan Nyata.....	15
2.8.3 Rekomendasi Perbaikan.....	15
BAB III .....	16
3.1 Tahap Perencanaan .....	17
3.2 Tahap Desain .....	17
3.3 Tahap Implementasi.....	18
3.4 Tahap Uji Coba.....	18
3.5 Tahap Analisis.....	18
3.6 Framework Pengujian.....	19

3.6.1 Vulnerability Scanning .....	19
3.6.2 Penetration Testing.....	20
3.6.3 Hasil Pengujian (Report) .....	20
BAB IV .....	21
4.1 Model Sistem.....	21
4.1.1 Perangkat Keras .....	21
4.1.2 Perangkat Lunak .....	22
4.2 Instalasi <i>Software</i> .....	24
4.2.1 Snort.....	24
4.2.2 Wapiti .....	26
4.2.3 Burp Suite .....	26
4.2.4 <i>Acunetix Manual Tools</i> .....	27
4.2.5 OWASP ZAP .....	28
4.2.6 Postman.....	29
4.3 <i>Vulnerable Web Application</i> .....	29
4.4 <i>Vulnerability Scanning</i> .....	31
4.4.1 Hasil Tools Scanning .....	31
4.4.2 Hasil <i>Scanning</i> Wapiti pada WackoPicko .....	34
4.4.3 Hasil Scanning Wapiti pada DVWA .....	34
4.5 <i>Penetration Testing</i> .....	35
4.5.1 Hasil SQL Injection Dengan Burp Suite pada DVWA .....	35
4.5.2 Hasil Pendeteksian Snort Terhadap Serangan SQL Injection .....	38
4.5.3 Hasil XSS Stored Dengan Burp Suite pada DVWA .....	38
4.5.4 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	41
4.5.5 Hasil SQL Injection Dengan Burp Suite pada WackoPicko .....	42

4.5.6 Hasil Pendeteksian Snort Terhadap Serangan SQL Injection .....	45
4.5.7 Hasil XSS Stored Dengan Burp Suite pada WackoPicko .....	46
4.5.8 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	50
4.5.9 Hasil <i>SQL Injection</i> Dengan OWASP ZAP pada DVWA .....	51
4.5.10 Hasil Pendeteksian Snort Terhadap Serangan SQL Injection .....	54
4.5.11 Hasil XSS OWASP ZAP pada DVWA .....	55
4.5.12 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	58
4.5.13 Hasil SQL Injection Dengan OWASP ZAP pada WackoPicko .....	58
4.5.14 Hasil Pendeteksian Snort Terhadap Serangan SQL Injection .....	62
4.5.15 Hasil XSS Stored Dengan OWASP ZAP pada WackoPicko .....	62
4.5.16 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	67
4.5.17 Hasil SQL Injection Pada DVWA dengan Acunetix Manual Tools ....	67
4.5.18 Hasil Pendeteksian Snort Terhadap Serangan SQL .....	71
4.5.19 Hasil XSS Pada DVWA dengan Acunetix Manual Tools .....	71
4.5.20 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	74
4.5.21 Hasil SQL Injection Pada WackoPicko dengan Acunetix Manual Tools .....	75
4.5.22 Hasil Pendeteksian Snort Terhadap Serangan SQL .....	78
4.5.23 Hasil XSS Pada WackoPicko dengan Acunetix Manual Tools .....	78
4.5.24 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	80
4.5.25 SQL Injection Dengan Postman pada DVWA .....	80
4.5.26 Hasil Pendeteksian Snort Terhadap Serangan SQL Injection .....	84
4.5.27 XSS Dengan Postman pada DVWA .....	85
4.5.28 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	88
4.5.29 SQL Injection Dengan Postman pada WackoPicko .....	88

4.5.30 Hasil Pendeteksian Snort Terhadap Serangan SQL Injection .....	90
4.5.31 XSS Dengan Postman pada WackoPicko .....	90
4.5.32 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	93
4.6 Analisis Hasil.....	94
4.6.1 Analisis Hasil Scanning WackoPicko dan DVWA .....	94
4.6.2 Analisis Tingkat Risiko Kerentanan pada DVWA dan WackoPicko ....	96
4.6.3 Analisis Hasil Penetration Testing dan Pendeteksian Snort pada WackoPicko dan DVWA.....	98
BAB V.....	105
5.1 Kesimpulan.....	105
5.2 Saran.....	106
DAFTAR PUSTAKA.....	108
Lampiran.....	110



## DAFTAR TABEL

Tabel 1 Sintaks Snort Untuk Deteksi Serangan .....	11
Tabel 2 Ringkasan Penelitian Terdahulu .....	11
Tabel 3 Spesifikasi Perangkat Keras .....	21
Tabel 4 Tabel Spesifikasi Perangkat Lunak .....	22
Tabel 5 Hasil Scanning Dengan Wapiti.....	34
Tabel 6 Hasil Scanning Dengan Wapiti.....	35
Tabel 7 Hasil Scanning Wapiti Untuk Wackopicko Dan DVWA.....	95
Tabel 8 Jumlah Temuan Dan Selisih Antara Kedua Website .....	95
Tabel 9 Tingkat Risiko Kerentanan DVWA dan WackoPicko .....	96
Tabel 10 Hasil Penetration Testing SQL Injection dan Pendeteksian Snort pada DVWA.....	98
Tabel 11 Hasil Penetration Testing SQL Injection dan Pendeteksian Snort pada Wacko Picko.....	99
Tabel 12 Hasil Penetration Testing XSS dan Pendeteksian Snort pada DVWA .	100
Tabel 13 Hasil Penetration Testing XSS dan Pendeteksian Snort pada Wacko Picko.....	100
Tabel 14 Hasil Serangan SQL Injection pada WackoPicko .....	101



## DAFTAR GAMBAR

Gambar 3.1 Diagram Alur Untuk Metode Pengujian .....	16
Gambar 3.2.1 Diagram Tahap Desain Penelitian[5] .....	17
Gambar 3.6.1 Framework Pengujian .....	19
Gambar 4.2.1 Proses Instalasi Snort Pada Sistem Operasi .....	24
Gambar 4.2.2 Konfigurasi Snort Untuk Deteksi Serangan .....	25
Gambar 4.2.3 Proses Instalasi Wapiti Sebagai Scanning Tool.....	26
Gambar 4.2.4 Tampilan UI Utama Burp Suite.....	26
Gambar 4.2.5 Proses Instalasi Acunetix Untuk Penetration Testing Tool.....	27
Gambar 4.2.6 Proses Instalasi ZAP Sebagai Pentration Testing Tool.....	28
Gambar 4.2.7 Proses Instalasi Postman Untuk Penetration Testing Tool .....	29
Gambar 4.3.1 Tampilan UI DVWA ( <i>Damn Vulnerable Web Application</i> ) Untuk Target Testing .....	30
Gambar 4.3.2 Tampilan UI WackoPicko Untuk Target Testing .....	30
Gambar 4.4.1 Proses <i>Scanning</i> pada DVWA Menggunakan Wapiti.....	31
Gambar 4.4.2 Proses <i>Scanning</i> pada WackoPicko Menggunakan Wapiti.....	32
Gambar 4.4.3 Hasil <i>Scanning</i> pada WackoPicko Dengan Wapiti .....	32
Gambar 4.4.4 Hasil Scanning pada DVWA Dengan Wapiti .....	33
Gambar 4.5.1 Penggunaan Fitur “ <i>Send to Intruder</i> ” Pada BurpSuite.....	36
Gambar 4.5.2 Penambahan File Fuzz Untuk Simulasi SQL Injection Pada BurpSuite .....	37
Gambar 4.5.3 Hasil SQL Injection Menggunakan Burp Suite pada DVWA .....	37
Gambar 4.5.4 Hasil Pendeteksian Snort Terhadap SQL Injection .....	38
Gambar 4.5.5 Request HTTP Untuk Simulasi XSS Pada BurpSuite.....	39
Gambar 4.5.6 Menampilkan Respons Server di Browser Setelah Payload Dikirim .....	40
Gambar 4.5.7 Hasil XSS Stored Menggunakan Burp Suite pada DVWA.....	40
Gambar 4.5.8 Hasil Pendeteksian Snort Terhadap XSS.....	41
Gambar 4.5.9 Proses Awal Serangan Injection Pada WackoPicko Dengan BurpSuite .....	42

Gambar 4.5.10 Request HTTP WackoPicko Pada BurpSuite .....	43
Gambar 4.5.11 Penambahan File Fuzzing Untuk Simulasi Serangan SQL Injection .....	43
Gambar 4.5.12 Hasil SQL Injection Menggunakan Burp Suite pada WackoPicko .....	44
Gambar 4.5.13 Fitur Unggah Foto Pada WackoPicko .....	45
Gambar 4.5.14 Hasil Pendeteksian Snort Terhadap SQL Injection .....	45
Gambar 4.5.15 Proses Awal Serangan XSS Stored Pada WackoPicko .....	46
Gambar 4.5.16 Request HTTP WackoPicko Pada BurpSuite .....	47
Gambar 4.5.17 Penggunaan Fitur Send to Repeater pada Request yang Tertangkap .....	48
Gambar 4.5.18 Modifikasi Parameter Dengan Script Injection .....	48
Gambar 4.5.19 Opsi "Show Respon in Browser" .....	49
Gambar 4.5.20 Hasil XSS Stored Burp Suite pada WackoPicko .....	50
Gambar 4.5.21 Hasil Pendeteksian Snort Terhadap XSS .....	50
Gambar 4.5.22 Damn Vulnerable Web Application (DVWA) .....	51
Gambar 4.5.23 Request DVWA Yang Tertangkap Pada OWASP ZAP .....	52
Gambar 4.5.24 Pengubahan Parameter Untuk Serangan Injection .....	53
Gambar 4.5.25 Hasil SQL Injection OWASP ZAP pada DVWA .....	53
Gambar 4.5.26 Hasil Pendeteksian Snort Terhadap Serangan SQL Injection .....	54
Gambar 4.5.27 Proses Awal Untuk XSS Pada DVWA .....	55
Gambar 4.5.28 Pemilihan Opsi "Fuzz" .....	56
Gambar 4.5.29 Penambahan File Fuzz .....	56
Gambar 4.5.30 File XSS 101 .....	56
Gambar 4.5.31 Salah Satu Respon Proses Fuzz .....	56
Gambar 4.5.32 Pemilihan Opsi "URL in Browser" .....	57
Gambar 4.5.33 Hasil XSS Stored OWASP ZAP pada DVWA .....	57
Gambar 4.5.34 Hasil Pendeteksian Snort Terhadap Serangan XSS .....	58
Gambar 4.5.35 Proses Awal Serangan SQL Injection .....	59
Gambar 4.5.36 Pemilihan Opsi "Fuzz" Pada OWASP ZAP .....	60
Gambar 4.5.37 Penambahan File Fuzz Pada OWASP ZAP Untuk SQL Injection .....	60

Gambar 4.5.38 Hasil SQL Injection OWASP ZAP pada WackoPicko .....	61
Gambar 4.5.39 Hasil Pendeteksian Snort Terhadap SQL Injection .....	62
Gambar 4.5.40 Proses Awal Serangan XSS Stored.....	63
Gambar 4.5.41 Hasil Request WackoPicko Pada OWASP ZAP.....	63
Gambar 4.5.42 Parameter Yang Diuji .....	64
Gambar 4.5.43 Penambahan File Fuzz .....	64
Gambar 4.5.44 Hasil Respon Fuzz OWASP ZAP .....	65
Gambar 4.5.45 Opsi URL in Browser Pada WackoPicko .....	65
Gambar 4.5.46 Hasil XSS Stored OWASP ZAP pada WackoPicko .....	66
Gambar 4.5.47 Hasil Pendeteksian Snort Terhadap XSS.....	67
Gambar 4.5.48 Penambahan Target Pada Acunetix Manual Tools .....	68
Gambar 4.5.49 Penambahan Cookies dan Tingkat Security .....	68
Gambar 4.5.50 Penambahan Payload SQL Injection.....	69
Gambar 4.5.51 Hasil Serangan SQL Injection Dengan Acunetix .....	70
Gambar 4.5.52 Hasil Pendeteksian Snort Terhadap SQL Injection .....	71
Gambar 4.5.53 Penambahan Targer URL DVWA .....	71
Gambar 4.5.54 Percobaan Untuk Serangan XSS .....	72
Gambar 4.5.55 Respon Data XSS Menggunakan Acunetix.....	73
Gambar 4.5.56 Percobaan di Browser Untuk Verifikasi XSS menggunakan Acunetix .....	74
Gambar 4.5.57 Laporan Hasil Snort Terhadap XSS .....	74
Gambar 4.5.58 Penambahan Url WackoPicko Pada Acunetix.....	75
Gambar 4.5.59 Penambahan Cookies PHPSESSID.....	76
Gambar 4.5.60 Pengubahan Request Data dan Respon View Page.....	76
Gambar 4.5.61 Respon Data SQL Injection pada Acunetix.....	77
Gambar 4.5.62 Hasil Pendeteksian Snort Terhadap SQL Injection .....	78
Gambar 4.5.63 Penambahan Url WackoPicko Pada WackoPicko .....	79
Gambar 4.5.64 Respon Setelah Pengujian XSS Pada Acunetix.....	79
Gambar 4.5.65 Hasil Pendeteksian Snort Terhadap XSS.....	80
Gambar 4.5.66 Penambahan Url Target DVWA Pada Postman.....	81
Gambar 4.5.67 Penambahan Cookies dan Tingkat Keamanan .....	82

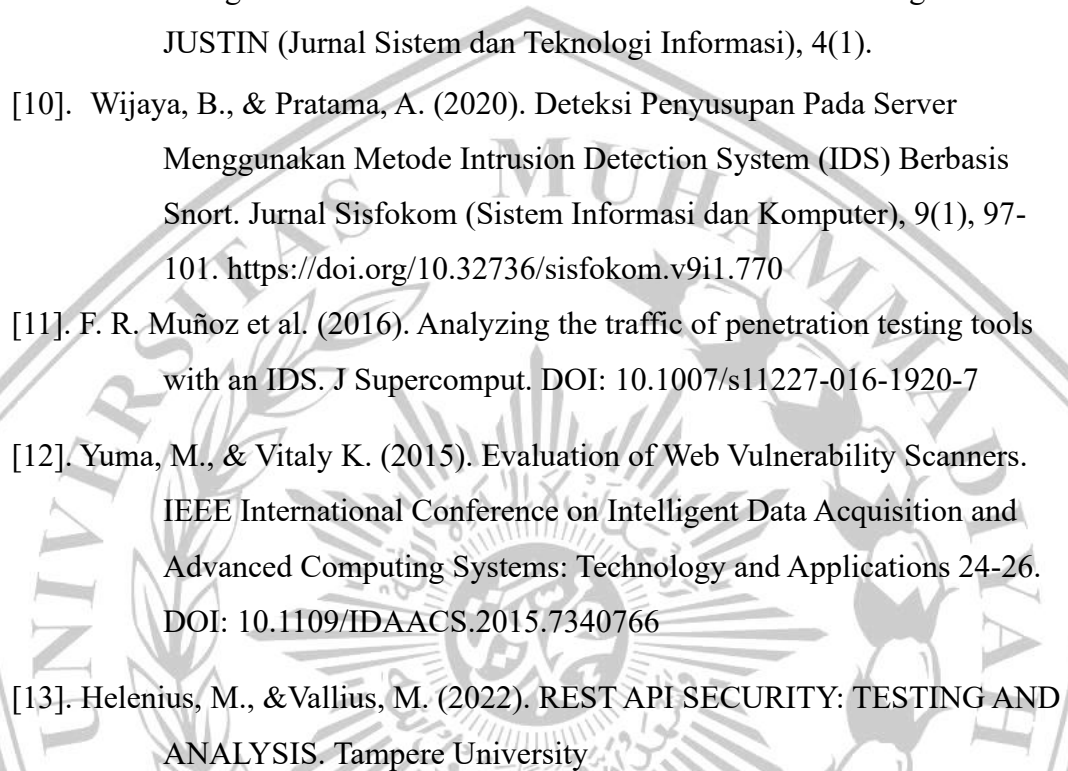
Gambar 4.5.68 Perubahan Nilai Parameter Pada Postman .....	82
Gambar 4.5.69 Hasil Preview SQL Injection Pada Postman .....	83
Gambar 4.5.70 Body HTML SQL Injection Pada Postman.....	84
Gambar 4.5.71 Laporan Snort Terhadap SQL Injection .....	84
Gambar 4.5.72 Penambahan Target Url DVWA Pada Postman.....	85
Gambar 4.5.73 Perubahan Nilai Parameter Pada Postman .....	86
Gambar 4.5.74 Hasil Preview XSS Pada Postman .....	86
Gambar 4.5.75 Body HTML Untuk XSS Pada Postman .....	87
Gambar 4.5.76 Laporan Alert Snort Terhadap XSS.....	88
Gambar 4.5.77 Penambahan Target Url WackoPicko .....	88
Gambar 4.5.78 Hasil Body Preview SQL Injection Pada Postman .....	89
Gambar 4.5.79 Hasil Body HTML Pada Postman .....	90
Gambar 4.5.80 Alert Snort Terhadap SQL Injection.....	90
Gambar 4.5.81 Penambahan Url WackoPicko Pada Postman .....	91
Gambar 4.5.82 Perubahan Nilai Parameter Pada Postman .....	91
Gambar 4.5.83 Hasil Body Preview Pada Acunetix Untuk XSS .....	92
Gambar 4.5.84 Hasil Body HTML Pada Acunetix Untuk XSS .....	93
Gambar 4.5.85 Snort Alert Terhadap Serangan XSS .....	93



## DAFTAR PUSTAKA

- [1]. Dar, M. H., & Harahap, S. Z. (2017). IMPLEMENTASI SNORT INTRUSION DETECTION SYSTEM (IDS) PADA SISTEM JARINGAN KOMPUTER. *JURNAL INFORMATIKA*, 6(3), 14–23.  
<https://doi.org/10.36987/informatika.v6i3.1619>
- [2]. Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 4(2), 413.  
<https://doi.org/10.30865/mib.v4i2.2037>
- [3]. Hafiz, A., Kurniawan, T., Sivi, N. A., Ikhsan, F. K., & Andhika, P. (2020). ANALISIS CELAH KEAMANAN JARINGAN DAN SERVER MENGGUNAKAN SNORT INTRUSION DETECTION SYSTEM. *Jurnal Informasi Dan Komputer*, 8(2), 59–66.  
<https://doi.org/10.35959/jik.v8i2.185>
- [4]. Lukman, L., & Suci, M. (2020). Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache. *Respati*, 15(2), 6.  
<https://doi.org/10.35842/jtir.v15i2.343>
- [5]. Prasetyo, H. (2016). Analisa Keamanan Web Server Menggunakan Web Application Firewall Modsecurity
- [6]. Arman, M., & Rachmat, N. (2020). IMPLEMENTASI SISTEM KEAMANAN WEB MENGGUNAKAN PFSENSE. *Jusikom : Jurnal Sistem Komputer Musirawas*, 5(1), 13-23.  
<https://doi.org/10.32767/jusikom.v5i1.752>
- [7]. Hassan, Z., Shahzeb, Odarchenko, R., Gnatyuk, S., Zaman, A., & Shah, M (2018). Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems. 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), 238-288.  
<https://doi.org/10.1109/MSNMC.2018.8576287>



- 
- [8]. Purba, W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI*, 17(2), 143-158.  
<https://doi.org/10.24246/aiti.v17i2.143-158>
- [9]. Mutaqin, A. (2016). Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, 4(1).
- [10]. Wijaya, B., & Pratama, A. (2020). Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (IDS) Berbasis Snort. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, 9(1), 97-101. <https://doi.org/10.32736/sisfokom.v9i1.770>
- [11]. F. R. Muñoz et al. (2016). Analyzing the traffic of penetration testing tools with an IDS. *J Supercomput.* DOI: 10.1007/s11227-016-1920-7
- [12]. Yuma, M., & Vitaly K. (2015). Evaluation of Web Vulnerability Scanners. *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* 24-26. DOI: 10.1109/IDAACS.2015.7340766
- [13]. Helenius, M., & Vallius, M. (2022). REST API SECURITY: TESTING AND ANALYSIS. Tampere University

## Lampiran

Video Dokumentasi :

[https://drive.google.com/drive/folders/14BWcpiy\\_MJFiKPvOXomGHzf5H8yasxdL?usp=sharing](https://drive.google.com/drive/folders/14BWcpiy_MJFiKPvOXomGHzf5H8yasxdL?usp=sharing)



# FAKULTAS TEKNIK

## INFORMATIKA

informatika.umm.ac.id | informatika@umm.ac.id

UMM  
1964

UNIVERSITAS  
MUHAMMADIYAH  
MALANG



### FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : DHANA AGUSTYA PUTRA SASONGKO

NIM : 201910370311357

Judul TA : ANALISIS METODE VULNERABILITY SCANNING DAN  
PENETRATION TESTING DENGAN INTRUSION DETECTION  
SYSTEM TERHADAP VULNERABLE WEBSITE

#### Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	28 %
2.	Bab 2 – Daftar Pustaka	25 %	8 %
3.	Bab 3 – Analisis dan Perancangan	25 %	13 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	0 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	11 %
6.	Makalah Tugas Akhir	20%	20%

\*) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

\*) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)

Mengetahui,

Pemeriksa (Staff TU)

(.....)



#### Kampus I

Jl. Bandung 1 Malang, Jawa Timur  
P. +62 341 551 253 (Hunting)  
F. +62 341 460 435

#### Kampus II

Jl. Bendungan Sutarni No 188 Malang, Jawa Timur  
P. +62 341 551 149 (Hunting)  
F. +62 341 582 060

#### Kampus III

Jl. Raya Tlogomas No.246 Malang, Jawa Timur  
P. +62 341 464 318 (Hunting)  
F. +62 341 460 435  
E. webmaster@umm.ac.id