

SKRIPSI

**ANALISIS KEAMANAN WEBSITE *REPOSITORY* INSTITUT
TEKNOLOGI TELKOM PURWOKERTO MENGGUNAKAN
METODE *VULNERABILITY ASSESSMENT***

***ANALYSIS OF INSTITUTION OF TECHNOLOGY TELKOM
PURWOKERTO REPOSITORY WEBSITE SECURITY USING
VULNERABILITY ASSESSMENT METHOD***



Disusun Oleh:

SHAFIRA KHAIRUNNISA

18101139

**PROGRAM STUDI SARJANA TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2022

**ANALISIS KEAMANAN WEBSITE *REPOSITORY* INSTITUT
TEKNOLOGI TELKOM PURWOKERTO MENGGUNAKAN METODE
*VULNERABILITY ASSESSMENT***

***ANALYSIS OF INSTITUTION OF TECHNOLOGY TELKOM
PURWOKERTO REPOSITORY WEBSITE SECURITY USING
VULNERABILITY ASSESSMENT METHOD***

**Skripsi digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)**

Di Institut Teknologi Telkom Purwokerto

2022

Disusun oleh :

Shafira Khairunnisa

18101139

DOSEN PEMBIMBING

Nanda Iryani, S.T.,M.T.

Eko Fajar Cahyadi, S.T.,M.T., Ph.D.

**PROGRAM STUDI SARJANA TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2022

HALAMAN PENGESAHAN
SKRIPSI

**ANALISIS KEAMANAN WEBSITE *REPOSITORY* INSTITUT
TEKNOLOGI TELKOM PURWOKERTO MENGGUNAKAN METODE
*VULNERABILITY ASSESSMENT***

***ANALYSIS OF INSTITUTION OF TECHNOLOGY TELKOM
PURWOKERTO REPOSITORY WEBSITE SECURITY USING
VULNERABILITY ASSESSMENT METHOD***

Disusun oleh :
Shafira Khairunnisa
18101139

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 22 Agustus
2022

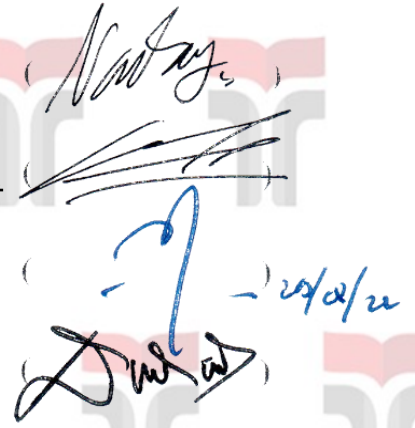
Susunan Tim Penguji

Pembimbing Utama : Nanda Iryani, S.T., M.T.
NIDN. 0604059302

Pembimbing Pendamping : Eko Fajar Cahyadi, S.T., M.T., Ph.D.
NIDN. 0616098703

Penguji 1 : Fauza Khair, S.T., M.Eng.
NIDN. 0622039001

Penguji 2 : Dadiek Pranindito, S.T., M.T.
NIDN. 0626108502



Handwritten signatures of the examiners and supervisors, including the date 22/08/22.

Mengetahui,
Ketua Program Studi S1 Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto



Prasetyo Yuliantoro, S.T., M.T.
NIDN. 0620079201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **SHAFIRA KHAIRUNNISA**, menyatakan bahwa skripsi dengan judul “**ANALISIS KEAMANAN WEBSITE *REPOSITORY* INSTITUT TEKNOLOGI TELKOM PURWOKERTO MENGGUNAKAN METODE *VULNERABILITY ASSESSMENT***” adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 29 Juli 2022

Yang menyatakan,



(Shafira Khairunnisa)

PRAKATA

Puji dan syukur kehadirat Allah SWT yang telah memberikan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Keamanan Website Repository Institut Teknologi Telkom Purwokerto Menggunakan Metode *Vulnerability Assessment*”. Skripsi ini diajukan untuk memenuhi syarat kelulusan mata kuliah Skripsi Teknik Telekomunikasi di Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto. Dalam pembuatan skripsi ini, berbagai pihak telah membantu penulis dalam berbagai hal. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Ahmad Jubaedi dan Ibu Devi Melani selaku orang tua penulis.
2. Ananda Danish Hisham Ahmad, Saudara Penulis
3. Ibu Nanda Iryani, S.T., M.T. sebagai Dosen Pembimbing I
4. Bapak Eko Fajar Cahyadi, S.T., M.T., Ph.D. sebagai Dosen Pembimbing II
5. Bapak Prasetyo Yuliantoro, S.T., M.T. selaku Ketua Program Studi S1 Teknik Telekomunikasi.
6. Bapak Dr. Arfianto Fahmi, S.T., M.T. selaku Rektor Institut Teknologi Telkom Purwokerto.
7. Seluruh dosen dan staf Program Studi S1 Teknik Telekomunikasi Institut Teknologi Telkom Purwokerto.
8. Teman-teman S1TT-06-D dan anggota Astralik yang selalu mendukung saya.

Purwokerto , 29 Juli 2022



(Shafira Khairunnisa)

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN ORISINALITAS	v
PRAKATA	vi
ABSTRAK	vii
<i>ABSTRACT</i>	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Perumusan Masalah	2
1.3. Tujuan Penelitian	2
1.4. Ruang Lingkup dan Batasan Masalah	2
1.5. Manfaat Penelitian	3
1.6. Sistematika Penulisan	3
BAB 2 LANDASAN TEORI	5
2.1. Tinjauan Pustaka	5
2.2. <i>Network Security</i> (Keamanan Jaringan)	11
2.3. <i>Web Server</i>	11
2.4. <i>Vulnerability Assessment</i>	12
2.5. Jenis <i>Vulnerability Assessment</i>	12
2.6. Kategori <i>Vulnerability Assessment Scan</i>	12
2.7. Alat <i>Vulnerability Assessment</i>	13
2.7.1. Kali Linux	13
2.7.2. Nmap	13
2.7.3. Zenmap	13
2.7.4. Nessus	13
2.8. Tipe Ancaman <i>Web Vulnerability</i>	14
2.8.1. <i>SQL Injection Vulnerability Attack</i>	14

2.8.2. <i>Broken Authentication and Session Management Vulnerability Attack</i>	15
2.8.3. <i>Cross-Site Scripting Attack</i>	15
2.9. <i>Vulnerability Assessments Vs. Penetration Testing</i>	16
BAB 3 METODOLOGI PENELITIAN	17
3.1. Studi Literatur	17
3.2. <i>Planning and Preparation</i>	18
3.3. <i>Footprinting</i>	20
3.4. <i>Vulnerabilities Scanning</i>	21
3.5. Analisa dan Rekomendasi	21
3.6. <i>Reporting</i> (Dokumentasi)	21
BAB 4 HASIL DAN PEMBAHASAN	23
4.1. <i>Footprinting</i>	23
4.2. <i>Vulnerabilities Scanning</i>	27
4.3. Analisis dan Rekomendasi	29
BAB 5 KESIMPULAN DAN SARAN	39
5.1. KESIMPULAN	39
5.2. SARAN	40
DAFTAR PUSTAKA	41
Lampiran	44

DAFTAR GAMBAR

Gambar 3.1 Diagram Alir Penelitian	17
Gambar 3.2 Topologi Jaringan	19
Gambar 3.4 Pengujian Whois	20
Gambar 3.5 Pengujian Nslookup	20
Gambar 3.6 Pengujian <i>Scanning Port</i>	21
Gambar 4.1 Hasil pengujian <i>IP Address Repository</i> IT Telkom Purwokerto	23
Gambar 4.2 (a) Hasil pengujian <i>Domain info 1 (Domain)</i> , (b) Hasil Pengujian <i>Domain info 2</i> (kontak administratif dan teknisi) dan (c) Hasil pengujian <i>Domain info 3</i> (kontak administratif dan teknisi)	25
Gambar 4.3 Hasil Pengujian <i>Domain Name Server lookup</i>	26
Gambar 4.4 Hasil Pengujian <i>Scanning Port</i>	26
Gambar 4.5 Hasil <i>Vulnerabilities Scan IP Repository</i> di Nessus	27
Gambar 4.6 <i>Scan</i> jaringan dengan Zenmap	29
Gambar 4.7 Hasil pengujian <i>HTTP methods</i>	31
Gambar 4.8 Hasil pengujian <i>HTTP proxy scanning</i>	31
Gambar 4.9 Hasil pengujian <i>Cross-site scripting</i>	32
Gambar 4.10 Hasil pengujian <i>SQL Injection</i>	32
Gambar 4.11 Hasil <i>Vulnerabilities</i> terdeteksi di Nessus	33
Gambar 4.12 <i>Vulnerabilities Apache 2.4.x < 2.4.54 Multiple Vulnerabilities</i>	34
Gambar 4.13 <i>DNS Server Spoofed Request Amplification DDoS</i>	34
Gambar 4.14 <i>DNS Server Recursive Query Cache Poisoning Weakness</i>	35
Gambar 4.15 <i>Vulnerabilities Web Application Potentially Vulnerable to Clickjacking</i>	35
Gambar 4.16 <i>Vulnerabilities Apache mod_status /server-status Information Disclosure</i>	36

DAFTAR TABEL

Tabel 2.1 Rangkuman Tinjauan Pustaka	7
Tabel 3.1 Spesifikasi <i>Hardware</i> yang digunakan	18
Tabel 3.2 Spesifikasi <i>Software</i> yang akan digunakan	18
Tabel 4.1 Hasil <i>Scanning Port</i> menggunakan Zenmap	26
Tabel 4.2 <i>Alert</i> ditemukan Nessus berdasarkan kategori <i>vulnerability</i>	28
Tabel 4.3 Hasil Pengujian di Zenmap	32
Tabel 4.4 Kerentanan <i>critical</i> , <i>high</i> , dan <i>medium</i> yang didapat	36