

**PENGUJIAN KEAMANAN SISTEM INFORMASI BERBASIS WEB
MENGUNAKAN METODE
PTES (PENETRATION TESTING EXECUTION STANDARD)
(STUDI KASUS: SISTEM INFORMASI PORTAL AKADEMIK
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA)**

Tugas Akhir

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-1
Program Studi Teknologi Informasi



Disusun oleh
Achmad Alief
192104001

**FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA
Juli, 2023**

HALAMAN PENGESAHAN

**PENGUJIAN KEAMANAN SISTEM INFORMASI BERBASIS WEB
MENGUNAKAN METODE**

PTES (PENETRATION TESTING EXECUTION STANDARD)
**(STUDI KASUS: SISTEM INFORMASI PORTAL AKADEMIK
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA)**

dipersiapkan dan disusun oleh

Achmad Alief
192104001

telah dipertahankan di hadapan dewan penguji
pada tanggal 17 Juli 2023

Susunan Dewan Penguji

Pembimbing I

Alfina Rizqi Lahitani S.Kom., M.Eng.
NPP: 2017.13.0105

Pembimbing II

Adkhan Sholeh, S.Si., M.Cs.
NPP: 2003.13.0007

Penguji I

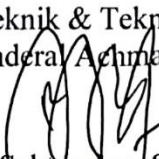
Chanief Budi Setiawan, S.T., M.Eng.
NPP: 2008.13.0021

Penguji II

Dedy Hariyadi, S.T., M.Kom.
NPP: 2019.13.0157

Tugas akhir ini telah diterima sebagai
salah satu persyaratan untuk memperoleh gelar Sarjana
pada tanggal 1. Agustus 2023.

Ketua Program Studi S-1 Teknologi Informasi
Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta


Rama Sahtyawan, S.T., M.Cs.
NPP: 2019.13.0150



PERNYATAAN


Saya yang bertanda tangan di bawah ini, adalah mahasiswa Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta,

Nama : Achmad Alief
NPM : 192104001
Program Studi : Teknologi Informasi (S-1)
Judul Tugas Akhir : Pengujian Keamanan Sistem Informasi Berbasis Web Menggunakan Metode *PTES* (*Penetration Testing Execution Standards*) (Studi Kasus: Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta)

Saya menyatakan dengan sesungguhnya bahwa Tugas Akhir ini seluruhnya merupakan karya kami sendiri, bebas dari peniruan terhadap karya orang lain. Bagian-bagian tertentu dari karya tulis ini yang merupakan kutipan dari hasil karya orang lain telah dituliskan sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam Tugas Akhir ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka kami bersedia menerima sanksi atas perbuatan tersebut.

Yogyakarta, 1 Juli 2023



Achmad Alief

KATA PENGANTAR

Puji Syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat dan hidayah Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul: “Pengujian Keamanan Informasi Berbasis Web Menggunakan Metode PTES (*Penetration Testing Execution Standards*) (Studi Kasus : Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta)”. Shalawat serta salam tidak lupa senantiasa kita panjatkan kepada Nabi Muhammad Shallahu ‘Allaihi Wasallam, yang telah membawa Islam sampai ke kita dari zaman jahiliyah sampai zaman terang benderang seperti serkarang. Penyusunan laporan ini merupakan salah satu syarat untuk menyelesaikan studi di Program Studi Teknologi Informasi (S-1) Fakultas Teknik & Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan Ini dapat diselesaikan atas bimbingan, arahan, dan bantuan dari berbagai pihak. Berbagai rintangan dan hambatan juga penulis temui dalam menyelesaikan penelitian ini. Namun dengan bimbingan, motivasi, bantuan dan do’a yang telah diberikan, penulis yakin bisa melewati rintangan dan hambatan yang ditemui. Dengan penuh kesadaran dan kerendahan hati penulis mengucapkan terima kasih setulus – tulusnya kepada:

1. Kedua orang tua yang sudah mengizinkan, merestui dan meridhoi penulis untuk melanjutkan pendidikan di Universitas Jenderal Achmad Yani Yogyakarta dan seluruh keluarga yang selalu memberi dukungan kepada penulis.
2. Ustadz Adi Hidayat Lc., M.A yang sudah memberikan motivasi, nasihat, arahan dalam penguatan spiritualitas.
3. Bapak Aris Wahyu Murdiyanto, S.Kom., M.Cs. selaku Dekan Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
4. Bapak Rama Sahtyawan, S.T., M.Cs. selaku Ketua Program Studi Teknologi Informasi (S-1) Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;

5. Ibu Alfirna Rizqi Lahitani, S.Kom., M.Eng selaku Dosen Pembimbing Tugas Akhir;
6. Para dosen yang telah memberikan banyak bekal ilmu pengetahuan kepada penulis selama menjadi mahasiswa di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
7. Kak Ismail A Hakim S.T selaku Mentor Tugas Akhir;
8. Teman – teman seperjuangan yaitu Bambang Sadewo, Ahmad Gofiansah, Velysia Amanda Khafid, Bagas Saktiawan Prasajo, Dimas Pratama, Indah Sari, Niko Agus Setiawan, Muhammad Yusuf Murdadlo, Violita Indar Pramutia, Reskiyanti, Ayu Widya Astuti, Milna Asmarita Tri Utami, Molesy Fransina Tanesib, Indri Mustika Rahmawati, Sela Banzira dan lainnya yang telah memberikan motivasi dan semangat selama masa kuliah saya.
9. Rekan – rekan mahasiswa Teknologi Informasi (S-1) di Universitas Jenderal Achmad Yani Yogyakarta yang sudah memberikan dukungan dan kerja sama selama penyusunan tugas akhir.
10. Sahabat SMA sampai sekarang merangkap menjadi saudara dan keluarga yaitu, Yuyun Setiawati S.M, Anggriawan Ragil Abi Yoga, Saeful Ismail yang selalu memberikan motivasi, mendampingi dari tahun 2017- sekarang.

Yogyakarta, 1 Juli 2023



Achmad Alief

DAFTAR ISI

Halaman Pengesahan.....	ii
Pernyataan.....	iii
Kata Pengantar	iv
Daftar Isi	vi
Daftar Tabel.....	viii
Daftar Gambar	ix
Daftar Lampiran	xii
Daftar Singkatan	xiii
Intisari.....	xv
Abstract.....	xvi
Bab 1 Pendahuluan	1
1.1 Latar Belakang	1
1.1.1 Perumusan Masalah.....	4
1.1.2 Manfaat Hasil Penelitian	4
1.2 Tujuan Penelitian	5
Bab 2 Tinjauan Pustaka dan Landasan Teori.....	6
2.1 Tinjauan Pustaka	6
2.2 Landasan Teori.....	9
2.3 Pertanyaan Penelitian	14
Bab 3 Metode Penelitian.....	15
3.1 Tahap Penetration Testing PTES	16
3.2 Bahan Penelitian.....	18
3.3 Alat Penelitian.....	18
3.3.1 <i>Tools Hardware</i>	18
3.3.2 <i>Tools Software</i>	18
3.4 Metode Pengujian.....	19
3.4.1 Jenis Pengujian.....	19
3.4.2 Alur Pengujian.....	21

3.5 Jalan Penelitian.....	22
Bab 4 Hasil Penelitian.....	23
4.1 Ringkasan Hasil Penelitian	23
4.2 Pembahasan.....	23
4.2.1 <i>Pre - engagement</i>	23
4.2.2 <i>Reconnaissance</i>	23
4.2.2.1 <i>Passive Reconnaissance</i>	24
4.2.2.2 <i>Active reconnaissance</i>	44
4.2.3 <i>Vulnerability Assesment</i>	58
4.2.4 <i>Exploitation</i>	66
4.2.5 <i>Reporting</i>	70
Bab 5 Kesimpulan dan Saran	72
5.1 Kesimpulan	72
5.2 Saran.....	73
Daftar Pustaka.....	75
Lampiran	81

DAFTAR TABEL

Tabel 2.1 Daftar penelitian sebelumnya.....	7
Tabel 3.1 Komponen Tools Hardware	18
Tabel 4.1 Tabel Google Dork List	39
Tabel 4.2 List Vulnerability Assement	59
Tabel 4.3 Hasil Pengujian Penetration Testing	70
Tabel 4.4 Hasil Pengkategorian Referensi OWASP TOP 10 2021	70

PEPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR GAMBAR

Gambar 3.1 Tahapan PTES (Penetration Testing Execution Standard)	15
Gambar 3.2 Jenis Pengujian OSSTMM (Open Source Security Testing Methodology Manual).....	20
Gambar 3.3 Alur Pengujian pendekatan Standards PTES	21
Gambar 3.4 Jalan Penelitian.....	22
Gambar 4.1 Informasi Arsitektur Objek Penelitian WappalyzerTools	24
Gambar 4.2 General Information, Open Port Objek Penelitian Shodan Tools.....	25
Gambar 4.3 Informasi Background, Hosting History, Site Technology Objek Penelitian Netcraft Tools.....	26
Gambar 4.4 Informasi Teknologi Pada Blog dan Web Browser Targeting Objek Penelitian Netcraft Tools.....	27
Gambar 4.5 Informasi Detection dan Ip Address owner Domain Objek Penelitian Virus Total Tools	29
Gambar 4.6 Informasi Detail dan Basic Properties PT Selaras Citra Terabit Virus Total Tools	29
Gambar 4.7 Informasi Relations dan Passive DNS Replication PT Selaras Citra Terabit Virus Total Tools.....	30
Gambar 4.8 Informasi Detection dan Analysis keamanan Vendor Objek Penelitian Virus Total Tools	32
Gambar 4.9 Informasi Link pada Objek Penelitian Virus Total Tools.....	32
Gambar 4.10 Informasi Details Categories, Body SHA -256 Public Virus Total Tools.....	33
Gambar 4.11 Informasi Pemilik Domain PT Selaras Citra Terabit Whois Tools. 35	
Gambar 4.12 Enumerasi Cheatsheet Google Dork Tools	38
Gambar 4.13 Enumerasi Login pada Objek Penelitian Google Dork Tools	39
Gambar 4.14 Enumerasi Login Pada Layanan Web Unjaya 1.....	40
Gambar 4.15 Enumerasi Login Pada Layanan Web Unjaya 2.....	41

Gambar 4.16 Informasi Black hat SEO Google Dork Tools	42
Gambar 4.17 Informasi Index.of Pada Objek Penelitian 1	43
Gambar 4.18 Informasi Index.of Pada Objek Penelitian 2	43
Gambar 4.19 Informasi Port Terbuka pada Objek Penelitian Nmap Tools	44
Gambar 4.20 memeriksa sistem operasi dan versi, pemeriksaan skrip Pada Objek Penelitian Nmap Tools	44
Gambar 4.21 Hasil Vulnerability Scanner Pada Port 80 Objek Penelitian Nmap Tools.....	45
Gambar 4.22 Hasil Vulnerability Scanner Pada Port 443 Objek Penelitian Nmap Tools.....	45
Gambar 4.23 Hasil Vulnerability Scanner Pada Port 53 Objek Penelitian Nmap Tools.....	45
Gambar 4.24 List Hidden Directory Pada Objek Penelitian 1 Dirb Tools.....	47
Gambar 4.25 List Hidden Directory Pada Objek Penelitian 2 Dirb Tools.....	47
Gambar 4.26 List Hidden Directory Pada Objek Penelitian 3 Dirb Tools.....	48
Gambar 4.27 Menemukan Vulnerable Breach Attack Pada Content Encoding Header Objek Penelitian Nikto Tools	49
Gambar 4.28 Melihat Proses Debugging Pada Objek Penelitian Nikto Tools	49
Gambar 4.29 Melihat Kerentanan SQL Injection Attack Pada Port 80 Nikto Tools	50
Gambar 4.30 Melihat Kerentanan Injection Attack Pada Port 80 Nikto Tools ..	50
Gambar 4.31 Melihat Kerentanan Denial of Services , SQL Injection Attack Pada Port 80 Nikto Tools.....	50
Gambar 4.32 Vulnerable Scanner Pada Port 443	51
Gambar 4.33 Menemukan Informasi Sensitive Wp-admin Objek Penelitian Dirsearch Tools	53
Gambar 4.34 Analisa Hidden Directory Objek Penelitian 1 Dirhunt Tools	55
Gambar 4.35 Analisa Hidden Directory Objek Penelitian 2 Dirhunt Tools	56
Gambar 4.36 Hasil Analisa Hidden Directory Objek Penelitian Dirhunt 3 Tools	56
Gambar 4.37 Hasil Report Pemindaian 1 Objek Penelitian Nessus Tools	62
Gambar 4.38 Hasil Report Pemindaian 2 Objek Penelitian Nessus Tools	63

Gambar 4.39 Hasil Scanning 1 Objek Penelitian WPScan	63
Gambar 4.40 Hasil Scanning 2 Objek Penelitian WPScan	64
Gambar 4.41 Cartegory OWASP TOP 10 Update 2021	64
Gambar 4.42 Vulnerability Scanner 1 Objek Penelitian Burp Suite Tools	65
Gambar 4.43 Vulnerability Scanner 2 Objek Penelitian Burp Suite Tools	65
Gambar 4.44 Exploit , Sensitive Information 1 Objek Penelitian NIKto Tools ...	66
Gambar 4.45 Exploit , Sensitive Information 2 Objek Penelitian Burpsuite Tools	67
Gambar 4.46 Exploit, Vektor(Payload) XSS Attack Objek Penelitian Technical Tools.....	67
Gambar 4.47 Exploit, Result XSS Attack Objek Penelitian.....	68
Gambar 4.48 Exploit, Result Business Logic Attack Objek Penelitian Burp Suite Tools.....	68
Gambar 4.49 Exploit, Result unrestricted attack Objek Penelitian Burp Suite Tools	69
Gambar 4.50 OWASP Risk Assement Calc pada objek penelitian	71