

**ANALISIS KEAMANAN WEBSITE MENGGUNAKAN
OWASP TOP 10 TAHUN 2021 DAN NIST SP 800-115
STUDI KASUS SISTEM INFORMASI CALON MAHASISWA BARU**

TUGAS AKHIR

Diajukan sebagai salah satu syarat memperoleh gelar Sarjana
Program Studi S-1 Teknologi Informasi



Disusun oleh:

AHMAD NURHIDAYAT

202104001

**PROGRAM STUDI S-1 TEKNOLOGI INFORMASI
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA
2024**

HALAMAN PENGESAHAN

TUGAS AKHIR

**ANALISIS KEAMANAN *WEBSITE* MENGGUNAKAN
OWASP TOP 10 TAHUN 2021 DAN NIST SP 800-115
STUDI KASUS SISTEM INFORMASI CALON MAHASISWA BARU**

Diajukan oleh:

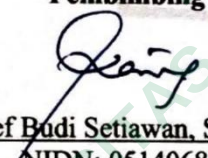
AHMAD NURHIDAYAT
202104001

Telah dipertahankan di depan dewan penguji dan dinyatakan sah
sebagai salah satu syarat untuk memperoleh gelar Sarjana
di Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta

Tanggal: 4 Juli 2024

Mengesahkan:

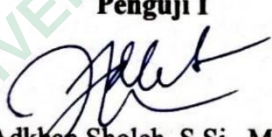
Pembimbing I


Chanief Budi Setiawan, S.T., M.Eng.
NIDN: 0514068101

Pembimbing II


Alfina Rizqi Lahitani, S.Kom., M.Eng.
NIDN: 0506019202

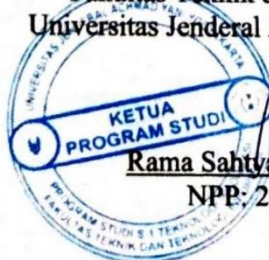
Penguji I

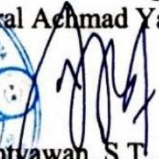

Adkhan Sholeh, S.Si., M.Cs.
NIDN: 0510127501

Penguji II


Rama Sahtyawan, S.T., M.Cs.
NIDN: 0518058001

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 : Ahmad Nurhidayat
NPM : 202104001
Program Studi : S-1 Teknologi Informasi
Judul Tugas Akhir : Analisis Kerentanan *Website* Menggunakan OWASP TOP 10 dan NIST SP 800-115 Studi Kasus Sistem Informasi Calon Mahasiswa Baru

Menyatakan bahwa hasil penelitian dengan judul tersebut di atas adalah asli karya saya sendiri dan bukan hasil plagiarisme. Semua referensi dan sumber terkait yang dikutip dalam karya ilmiah ini telah ditulis sesuai kaidah penulisan ilmiah yang berlaku. Dengan ini, saya menyatakan untuk menyerahkan hak cipta penelitian kepada Universitas Jenderal Achmad Yani Yogyakarta guna kepentingan ilmiah.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya tanpa ada paksaan dari pihak mana pun. Apabila terdapat kekeliruan atau ditemukan adanya pelanggaran akademik di kemudian hari, maka saya bersedia menerima konsekuensi yang berlaku sesuai ketentuan akademik.

Yogyakarta, 10 Juli 2024



KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul: “Analisis Keamanan *Website* Menggunakan OWASP TOP 10 Tahun 2021 Dan NIST SP 800-115 Studi Kasus Sistem Informasi Calon Mahasiswa Baru”. Penyusunan laporan ini merupakan salah satu persyaratan untuk menyelesaikan studi di Program Studi S-1 Teknologi Informasi Fakultas Teknik & Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat diselesaikan atas bimbingan, arahan, dan bantuan dari berbagai pihak. Pada kesempatan ini penulis dengan rendah hati mengucapkan terima kasih dengan setulus-tulusnya kepada:

1. Bapak Aris Wahyu Murdiyanto, S.Kom., M.Cs. selaku Dekan Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
2. Bapak Rama Sahtyawan, S.T., M.Cs. selaku Ketua Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
3. Bapak Chanief Budi Setiawan, S.T., M.Eng. selaku Dosen Pembimbing Tugas Akhir;
4. 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;
5. 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;
6. Rekan-rekan mahasiswa Prodi S-1 Teknologi Informasi di Universitas Jenderal Achmad Yani Yogyakarta yang sudah memberi dukungan dan kerja sama selama pembuatan tugas akhir.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kata sempurna. Maka dari itu dengan segala kerendahan hati penulis sangat menghargai adanya kritik dan saran yang membangun dari semua pihak yang bersedia meluangkan waktu untuk membaca laporan tugas akhir ini.

Yogyakarta, 10 Juli 2024



Ahmad Nurhidayat

DAFTAR ISI

Judul.....	i
Halaman Pengesahan.....	ii
Pernyataan.....	iii
Kata Pengantar	iv
Daftar Isi	vi
Daftar Tabel.....	viii
Daftar Gambar	ix
Daftar Lampiran	x
Daftar Singkatan	xi
Intisari.....	xii
Abstract.....	xiii
Bab 1 Pendahuluan	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	5
1.3 Pertanyaan Penelitian	5
1.4 Tujuan Penelitian	5
1.5 Manfaat Hasil Penelitian	6
Bab 2 Tinjauan Pustaka dan Landasan Teori.....	7
2.1 Tinjauan Pustaka	7
2.2 Landasan Teori.....	11
2.2.1 Keamanan Informasi	12
2.2.2 Kerentanan	13
2.2.3 <i>Open Web Application Security Project (OWASP) TOP 10</i>	13
2.2.4 <i>NIST SP 800-115 Methodology</i>	19
2.2.5 <i>Website</i>	20
2.2.6 <i>Transmission Control Protocol/ Internet Protocol (TCP/IP)</i>	21
2.2.7 <i>Port</i>	22
2.2.8 <i>Vulnerability Identification</i>	24
2.2.9 <i>Sistem Informasi Calon Mahasiswa Baru</i>	25

Bab 3 Metode Penelitian.....	27
3.1 Bahan dan Alat Penelitian.....	29
3.2 Jalan Penelitian.....	30
Bab 4 Hasil Penelitian.....	33
4.1 Ringkasan Hasil Penelitian	33
4.2 Perencanaan (<i>Planning</i>)	34
4.3 Penemuan (<i>Discovery</i>)	34
4.3.1 <i>Information Gathering</i>	34
4.3.2 <i>Vulnerability Scanning</i>	39
4.4 Pengujian (<i>Attacking</i>).....	43
4.4.1 <i>Helium Security</i>	43
4.4.2 ZAP (<i>Zed Attack Proxy</i>) 2.14.0.....	49
4.5 Pembahasan.....	57
4.5.1 <i>Nikto Scanner</i>	57
4.5.2 <i>Helium Security</i>	60
4.5.3 ZAP (<i>Zed Attack Proxy</i>) 2.14.0.....	66
4.5.4 <i>Report OWASP TOP 10</i>	75
4.5.5 Pencegahan (<i>Preventing</i>) berdasarkan OWASP TOP 10.....	82
Bab 5 Kesimpulan dan Saran	91
5.1 Kesimpulan	91
5.2 Saran.....	92
Daftar Pustaka.....	93
Lampiran	96

DAFTAR TABEL

Tabel 2.1 <i>Literature Review</i>	9
Tabel 2.2 <i>TCP/IP Layer</i>	22
Tabel 2.3 <i>Jenis Port dan Fungsinya</i>	23
Tabel 3.1 <i>Software yang digunakan beserta fungsinya</i>	29
Tabel 4.1 <i>Hasil Information Gathering menggunakan Netcraft</i>	35
Tabel 4.2 <i>Hasil TCP Scan</i>	38
Tabel 4.3 <i>Hasil UDP Scan</i>	38
Tabel 4.4 <i>Informasi umum hasil Nikto Scanner</i>	40
Tabel 4.5 <i>Hasil kerentanan Nikto Scanner</i>	41
Tabel 4.6 <i>Informasi Umum Hasil Helium Security</i>	45
Tabel 4.7 <i>Informasi Umum Hasil Helium Security</i>	47
Tabel 4.8 <i>Celah kerentanan hasil Helium Security</i>	48
Tabel 4.9 <i>Hasil Kerentanan ZAP (Zed Attack Proxy)</i>	56
Tabel 4.10 <i>Kerentanan Nikto Scanner dan acuan OWASP TOP 10</i>	59
Tabel 4.11 <i>Absence of Anti-CSRF Tokens</i>	61
Tabel 4.12 <i>CSP Wildcard Directive Vulnerabilities</i>	62
Tabel 4.13 <i>Sub Resource Integrity Attribute Missing Vulnerabilities</i>	63
Tabel 4.14 <i>Kerentanan Helium Security dan acuan OWASP TOP 10</i>	65
Tabel 4.15 <i>SQL Injection</i>	68
Tabel 4.16 <i>CSP (Content Security Policy)</i>	69
Tabel 4.17 <i>Vulnerable JS Library</i>	70
Tabel 4.18 <i>Absence of Anti-CSRF Tokens - ZAP</i>	71
Tabel 4.19 <i>Hidden File Found</i>	72
Tabel 4.20 <i>Hasil pemindaian ZAP dengan Kategori OWASP TOP 10</i>	73
Tabel 4.21 <i>Daftar Kerentanan berdasarkan Kategori OWASP TOP 10</i>	76
Tabel 4.22 <i>Daftar Kerentanan berdasarkan Kategori OWASP TOP 10</i>	80
Tabel 4.23 <i>Persentase Kerentanan yang ditemukan</i>	82

DAFTAR GAMBAR

Gambar 2.1 <i>Update data OWASP TOP 10 tahun 2017-2021</i>	14
Gambar 3.1 <i>Alur Penelitian</i>	28
Gambar 4.1 <i>Pemindaian dengan Netcraft</i>	35
Gambar 4.2 <i>Check konektivitas dengan server</i>	37
Gambar 4.3 <i>Hasil TCP Scan</i>	37
Gambar 4.4 <i>Hasil UDP Scan</i>	38
Gambar 4.5 <i>Hasil Maimon Scan</i>	39
Gambar 4.6 <i>Hasil pemindaian Nikto Scanner</i>	40
Gambar 4.7 <i>Hasil pemindaian target Helium Security</i>	44
Gambar 4.8 <i>Hasil Scan Helium Security</i>	46
Gambar 4.9 <i>Hasil kerentanan Helium Security</i>	47
Gambar 4.10 <i>Tampilan awal ZAP (Zed Attack Proxy) 2.14.0</i>	50
Gambar 4.11 <i>Parameters ZAP (Zed Attack Proxy) 2.14.0</i>	51
Gambar 4.12 <i>Result Scan ZAP (Zed Attack Proxy) 2.14.0</i>	52
Gambar 4.13 <i>Summary Scan ZAP (Zed Attack Proxy) 2.14.0</i>	53
Gambar 4.14 <i>Alerts Counts ZAP (Zed Attack Proxy) 2.14.0</i>	54
Gambar 4.15 <i>Daftar hasil kerentanan ZAP (Zed Attack Proxy) 2.14.0</i>	55

DAFTAR LAMPIRAN

Lampiran 1 Jadwal Penelitian	96
Lampiran 2 Surat Izin Penelitian.....	97
Lampiran 3 Kartu Bimbingan Skripsi	98
Lampiran 4 Hasil Cek Plagiarisme.....	99

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR SINGKATAN

ACL	<i>Access Control List</i>
CDN	<i>Content Delivery Network</i>
DBMS	<i>Database Management System</i>
DNS	<i>Domain Name Server</i>
HTML	<i>Hypertext Markup Language</i>
HTTP	<i>Hypertext Transfer Protocol</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
IMAP	<i>Internet Message Access Protocol</i>
IP	<i>Internet Protocol</i>
NIST	<i>National Institute of Standards and Technology</i>
NMAP	<i>Network Mapper</i>
OWASP	<i>Open Web Application Security Project</i>
SICAMA	<i>Sistem Calon Mahasiswa Baru</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SNMP	<i>Simple Network Management Protocol</i>
SQL	<i>Structure Query Language</i>
SSH	<i>Secure Shell</i>
TCP/IP	<i>Transfer Control Protocol/ Internet Protocol</i>
TLS	<i>Transport Layer Security</i>
UDP	<i>User Datagram Protocol</i>
UNJAYA	<i>Universitas Jenderal Achmad Yani Yogyakarta</i>
URL	<i>Uniform Resource Locator</i>
VPN	<i>Virtual Private Network</i>
WAN	<i>Wide Area Network</i>
ZAP	<i>Zed Attack Proxy</i>