

SKRIPSI

**ANALISIS KERENTANAN DAN PENGUJIAN KEAMANAN
PADA WEBSITE PROFIL SMKN 1 JAKARTA
MENGUNAKAN STANDAR NIST SP 800-115**



KHANSA SYAFIQ ABRARY

1512621077

PROGRAM STUDI

PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER

FAKULTAS TEKNIK

UNIVERSITAS NEGERI JAKARTA

2025

LEMBAR PENGESAHAN SKRIPSI

Judul : ANALISIS KERENTANAN DAN PENGUJIAN KEAMANAN PADA
WEBSITE PROFIL SMKN 1 JAKARTA MENGGUNAKAN STANDAR
NIST SP 800-115

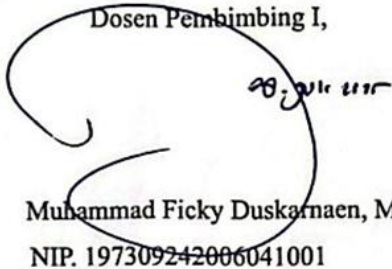
Penyusun : Khansa Syafiq Abrary

NIM : 1512621077

Disetujui oleh:

Tanggal, 25 Juli 2025

Dosen Pembimbing I,



Muhammad Ficky Duskarnaen, M.Sc
NIP. 197309242006041001

Tanggal, 25 Juli 2025

Dosen Pembimbing II,



Ali Idrus, S.Kom., M.Kom.
NIP. 198802262019031010

PENGESAHAN PANITIA UJIAN SKRIPSI

NAMA DOSEN	TANDA TANGAN	TANGGAL
Diat Nurhidayat, S.Pd, M.TI Ketua Penguji		25 Juli 2025
Murien Nugraheni, S.T., M.C Sekretaris		25 Juli 2025
Nur Elah, S.Kom., M.T Penguji Ahli		25 Juli 2025

HALAMAN PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini merupakan Karya asli dan belum pernah diajukan untuk mendapatkan gelar akademik sarjana, baik di Universitas Negeri Jakarta maupun di Perguruan Tinggi lain.
2. Skripsi ini belum dipublikasikan, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
3. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Universitas Negeri Jakarta.

Jakarta, 1 Juli 2025

Yang membuat pernyataan



Khansa Syafiq Abrary

NIM. 1512621077



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS NEGERI JAKARTA
UPT PERPUSTAKAAN

Jalan Rawamangun Muka Jakarta 13220
Telepon/Faksimili: 021-4894221
Laman: lib.unj.ac.id

**LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitas akademika Universitas Negeri Jakarta, yang bertanda tangan di bawah ini, saya:

Nama : Khansa Syafiq Abrary
NIM : 1512621077
Fakultas/Prodi : Teknik/Pendidikan Teknik Informatika dan Komputer
Alamat email : khansasyafiq40@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UPT Perpustakaan Universitas Negeri Jakarta, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah:

☒ Skripsi ☐ Tesis ☐ Disertasi ☐ Lain-lain (.....)

yang berjudul :

ANALISIS KERENTANAN DAN PENGUJIAN KEAMANAN PADA WEBSITE PROFIL SMKN
1 JAKARTA MENGGUNAKAN STANDAR NIST SP 800-115

Dengan Hak Bebas Royalti Non-Eksklusif ini UPT Perpustakaan Universitas Negeri Jakarta berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/mempublikasikannya di internet atau media lain secara *fulltext* untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan Universitas Negeri Jakarta, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 31 Juli 2025

Penulis

Khansa Syafiq Abrary

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan atas kehadiran Allah SWT yang telah memberikan limpahan rahmat, anugrah, karunia, hidayah, serta kuasa-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Kerentanan dan Pengujian Keamanan Pada Website Profil SMKN 1 Jakarta Menggunakan Standar NIST SP 800-115” yang bertujuan untuk mendapatkan gelar Sarjana Pendidikan di Universitas Negeri Jakarta serta sebagai sarana untuk mengimplementasikan kemampuan dan pengetahuan yang telah peneliti dapatkan selama menempuh pendidikan di bangku perkuliahan.

Penulis mengucapkan terima kasih kepada berbagai pihak terkait yang telah memberikan bantuan, baik secara langsung maupun dukungan moril, serta bimbingan kepada penulis dalam menyelesaikan penelitian skripsi. Dengan demikian, maka peneliti ingin mengucapkan banyak terima kasih kepada :

1. Keluarga penulis, baik ayah, ibu, dan adik penulis serta sanak famili yang selalu mendukung dan mendoakan agar selalu diberikan kelancaran dan kekuatan dalam menyelesaikan skripsi .
2. Muchammad Ficky Duskarnaen, M.Sc. selaku Koordinator Program Studi Pendidikan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Jakarta dan selaku Dosen Pembimbing I yang selalu memberikan bimbingan, arahan, dukungan, serta masukan kepada peneliti dalam proses penyusunan skripsi ini.
3. Ali Idrus, S.Kom.,M.Kom selaku Dosen Pembimbing II yang selalu memberikan bimbingan, arahan, dukungan, serta masukan kepada peneliti dalam proses penyusunan skripsi ini.
4. Segenap Bapak dan Ibu Dosen Pendidikan Teknik Informatika dan Komputer yang telah memberikan ilmu, dukungan, dan motivasi selama studi di bangku perkuliahan.
5. Bapak dan Ibu guru serta peserta didik SMK Negeri 1 Jakarta yang telah memberikan bantuan kepada penulis dalam bentuk data, sarana, dan prasarana selama penelitian;

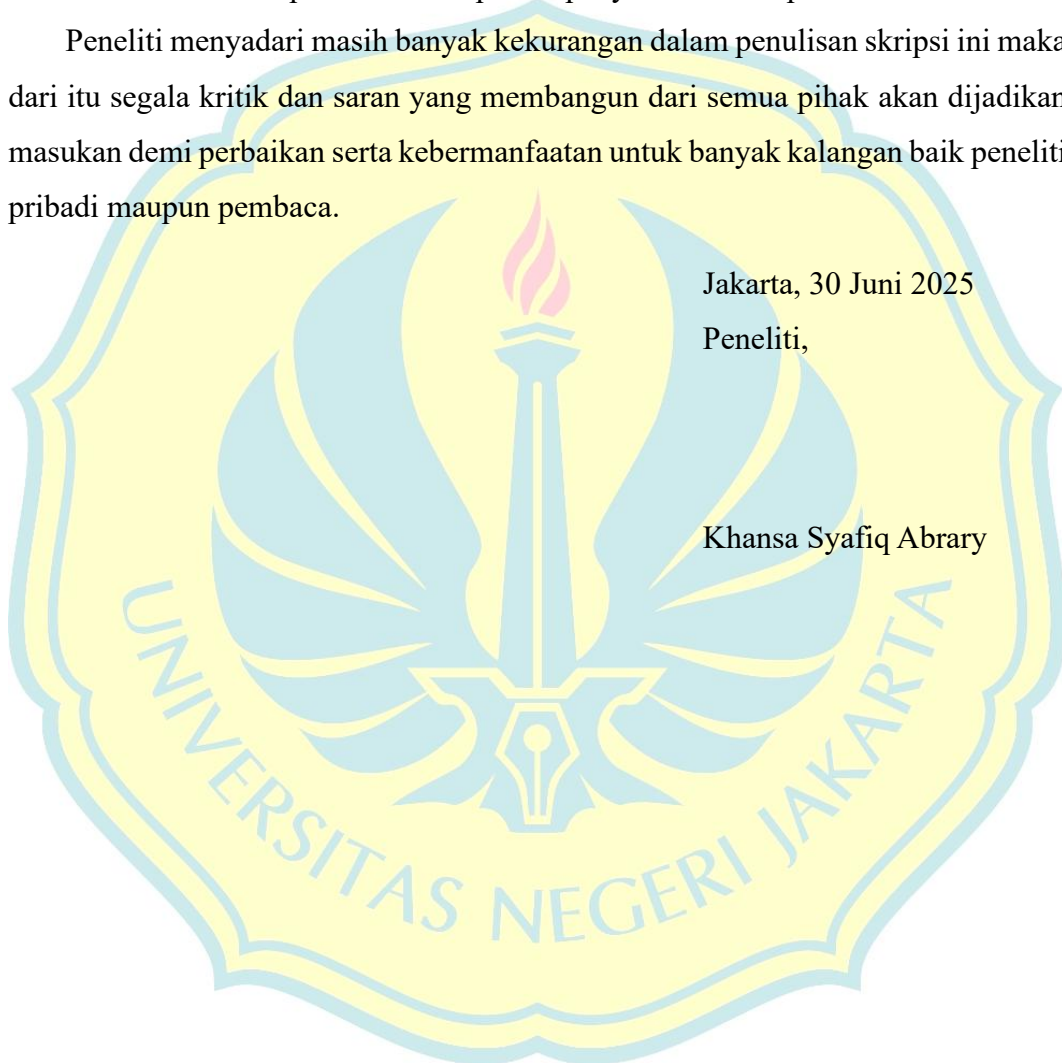
6. Viqri Ramadhani, Akhdiyat Rifky Iqbal, dan Muhammad Irfan Pratama sebagai sahabat penulis yang tidak bosan mendengarkan keluh kesah serta memberikan semangat dan motivasi untuk menyelesaikan skripsi ini.
7. Seluruh rekan PTIK angkatan 2021 yang sudah bersama-sama menempuh perkuliahan selama ini;
8. Serta berbagai pihak yang terlibat secara langsung maupun tidak langsung untuk membantu penulis dalam proses penyelesaian skripsi ini.

Peneliti menyadari masih banyak kekurangan dalam penulisan skripsi ini maka dari itu segala kritik dan saran yang membangun dari semua pihak akan dijadikan masukan demi perbaikan serta kebermanfaatan untuk banyak kalangan baik peneliti pribadi maupun pembaca.

Jakarta, 30 Juni 2025

Peneliti,

Khansa Syafiq Abrary



ANALISIS KERENTANAN DAN PENGUJIAN KEAMANAN PADA WEBSITE PROFIL SMKN 1 JAKARTA MENGUNAKAN STANDAR NIST SP 800-115

Khansa Syafiq Abrary

Dosen Pembimbing : Muhammad Ficky Duskarnaen, M.Sc dan Ali
Idrus, S.Kom.,M.Kom.

ABSTRAK

Perkembangan teknologi informasi dan komunikasi yang pesat telah menjadikan website sebagai media utama dalam distribusi informasi, termasuk dalam sektor pendidikan. Namun, tingginya tingkat pemanfaatan website publik tidak diimbangi dengan kesadaran keamanan yang memadai, sehingga meningkatkan potensi serangan siber. Fenomena serangan siber menimbulkan risiko kebocoran data pribadi dan pelanggaran terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Penelitian ini bertujuan untuk mengidentifikasi dan mendokumentasikan kerentanan pada website xxx.jkt.xxx.id melalui pendekatan *black box-testing* berbasis standar NIST SP 800-115. Metodologi yang digunakan terdiri dari empat tahap utama yaitu *planning*, *discovery*, *attack*, dan *reporting*. Parameter evaluasi dalam penelitian ini meliputi identifikasi risiko menggunakan tools seperti OWASP ZAP, Nmap, validasi eksploitasi, dan analisis terhadap tingkat risiko berdasarkan kategori OWASP Top 10. 2021 Hasil pengujian menunjukkan terdapat 24 temuan celah keamanan, dengan lima di antaranya divalidasi sebagai kerentanan aktif berisiko sedang hingga tinggi. Beberapa di antaranya adalah ketiadaan *Content-Security-Policy*, *Cross-Domain Misconfiguration*, dan *Missing Anti-clickjacking Header*, yang memungkinkan terjadinya serangan seperti XSS dan *clickjacking*. Empat dari lima *confidence* yang diuji terbukti valid dalam pengujian adalah *content security policy*, *cross-domain misconfiguration*, *HTTP to HTTPS Insecure Transition in Form Post*, dan *missing anti-clickjacking header*. Dari hasil pengujian dapat disimpulkan bahwa website SMKN 1 Jakarta masih memiliki banyak celah keamanan yang belum terdokumentasi dan tervalidasi secara sistematis.

Kata kunci : Website, serangan siber, *black-box testing*, NIST SP 800-115, *vulnerability scanning*, OWASP 2021 .

VULNERABILITY ANALYSIS AND SECURITY TESTING ON THE SMKN 1 JAKARTA PROFILE WEBSITE USING THE NIST SP 800-115 STANDARD

Khansa Syafiq Abrary

Thesis Advisor : Muhammad Ficky Duskarnaen, M.Sc and Ali
Idrus, S.Kom.,M.Kom.

ABSTRACT

The rapid development of information and communication technology has made websites the primary medium for information dissemination, including in the education sector. However, the high level of public website utilization is not accompanied by adequate security awareness, thereby increasing the potential for cyberattacks. These attacks pose *risks* of personal data leakage and violations of Law No. 27 of 2022 on Personal Data Protection (PDP Law). This study aims to identify and document vulnerabilities on the website xxx.jkt.xxx.id using a *black-box testing* approach based on the NIST SP 800-115 standard. The methodology consists of four main stages: planning, discovery, attack, and reporting. Evaluation parameters include *risk* identification using tools such as OWASP ZAP and Nmap, *exploitation* validation, and *risk* level analysis based on the OWASP Top 10 (2021). The results reveal 24 security vulnerabilities, five of which are validated as active *threats* with medium to high *risk* levels. Some of these include the absence of a Content-Security-Policy, Cross-Domain Misconfiguration, and Missing Anti-Clickjacking Header, which enable attacks such as XSS and *clickjacking*. Four out of five *confidences* that were tested and confirmed as valid include Content Security Policy, Cross-Domain Misconfiguration, HTTP to HTTPS Insecure Transition in Form Post, and Missing Anti-Clickjacking Header. Based on these findings, it can be concluded that the SMKN 1 Jakarta website still contains numerous undocumented and unvalidated security gaps, highlighting the need for systematic security evaluation.

Keywords : Website, *cyber attack*, *black-box testing*, NIST SP 800-115, *vulnerability scanning*, OWASP 2021.

DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI.....	i
HALAMAN PERNYATAAN.....	ii
LEMBAR PERNYATAAN PUBLIKASI	iii
KATA PENGANTAR	iv
ABSTRAK.....	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
LAMPIRAN	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Identifikasi Masalah	6
1.3 Pembatasan masalah.....	7
1.4 Perumusan masalah.....	7
1.5 Tujuan penelitian.....	7
1.6 Manfaat penelitian.....	7
BAB II TINJAUAN PUSTAKA	9
2.1 Kerangka Teoritik.....	9
2.1.1 Keamanan informasi	9
2.1.2 Website	10
2.1.3 Website SMKN 1 Jakarta	12
2.1.4 Open System Interconnection (OSI) Layer.....	13
2.1.5 <i>Penetration testing</i>	15

2.1.6 National Institute of Standards and Technology (NIST) SP 800-115	15
2.1.7 Open Web Application Security Project (OWASP) TOP 10	20
2.1.8 CMS Wordpress	25
2.1.9 Port	26
2.1.10 VMware Workstation	28
2.1.11 Serangan Siber	29
2.1.12 Kali linux tools	31
2.2 Penelitian Relevan	35
2.3 Kerangka Berpikir	49
BAB III METODOLOGI PENELITIAN.....	51
3.1 Tempat dan Waktu Penelitian	51
3.2 Alat dan Bahan Penelitian	51
3.2.1 Alat Penelitian	51
3.2.2 Bahan Penelitian	52
3.3 Diagram Alir Penelitian	53
3.4 Teknik Pengumpulan Data	55
3.5 Prosedur Penelitian	56
3.5.1 Planning	57
3.5.2 Discovery	60
3.5.3 Attack	62
3.5.4 Reporting	67
3.6 Metode Evaluasi Data	67
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	71
4.1 Discovery	71
4.1.1 Information gathering	71

4.1.2	<i>Vulnerability Scanning</i>	79
4.2	Attack	86
4.2.1	Cloud Metadata Potentially Exposed	86
4.2.2	Content Security Policy (CSP) Header Not Set	88
4.2.3	Cross-Domain Misconfiguration.....	90
4.2.4	HTTP to HTTPS Insecure Transition in Form Post	92
4.2.5	Missing Anti- <i>clickjacking</i> Header	95
4.3	Reporting.....	97
4.3.1	Hasil Pengujian Cloud Metadata Potentially Exposed.....	97
4.3.2	Hasil Pengujian Content Security Policy (CSP) Header Not Set...	98
4.3.3	Hasil Pengujian Cross-Domain Misconfiguration	99
4.3.4	Hasil Pengujian HTTP to HTTPS Insecure Transition in Form Post	99
4.3.5	Hasil Pengujian Missing Anti- <i>clickjacking</i> Header	100
BAB V KESIMPULAN DAN SARAN		106
5.1	Kesimpulan	106
5.2	Saran.....	107
DAFTAR PUSTAKA.....		109
LAMPIRAN		117
DAFTAR RIWAYAT HIDUP		132

DAFTAR GAMBAR

Gambar 1.1 Data Pengguna TIK di Indonesia 2020 – 2023 (Badan Pusat Statistik, 2024).....	1
Gambar 1.2 Rekapitulasi dugaan kebocoran data 2024 (BSSN, 2025).....	3
Gambar 2.1 (Whitman & Mattord, 2022).....	9
Gambar 2.2 Cara Kerja Website (Lesmidayarti dkk., 2023)	11
Gambar 2.3 Beranda website xxx.jkt.xxx.id	12
Gambar 2.4 Four – Step NIST SP 800-115 Methodology (Scarfone dkk., 2008)	16
Gambar 2.5 <i>Attack Phase Steps with Loopback to Discovery Phase</i> (Scarfone dkk., 2008).....	19
Gambar 2.6 (OWASP (Open Web Application Security Project), 2021)	21
Gambar 2.7 Kerangka teoritis	50
Gambar 3.1 Diagram alir penelitian	53
Gambar 3.2 Perintah whois pada kali linux	60
Gambar 3.3 Perintah nmap pada kali linux	61
Gambar 3.4 Tampilan Owasp Zap 2.1.16.....	62
Gambar 4.1 Hasil <i>scanning</i> dengan <i>tools</i> whois	71
Gambar 4.2 Informasi IP publik dan IP server	71
Gambar 4.3 Hasil pengecekan wapplyzer	72
Gambar 4.4 Hasil pemindaian nmap	74
Gambar 4.5 Hasil pemindaian nmap	75
Gambar 4.6 Hasil pemindaian nmap	75
Gambar 4.7 Hasil pemindaian <i>whatweb</i>	77
Gambar 4.8 Hasil pemindaian WAF	78
Gambar 4.9 Hasil <i>scanning</i> zap	79
Gambar 4.10 Detail <i>confidence cloud metada potentially exposed</i>	87

Gambar 4.11 Hasil pengujian <i>curl</i> dan <i>grep</i> pada metadata.....	88
Gambar 4.12 Hasil <i>response</i> CSP	89
Gambar 4.13 Hasil <i>report securityheaders.com</i>	89
Gambar 4.14 Hasil peninjauan <i>request header</i>	90
Gambar 4.15 Hasil <i>response Cross-Domain Misconfiguration</i>	91
Gambar 4.16 Hasil pengujian <i>Cross-Domain Misconfiguration</i>	91
Gambar 4.17 Hasil <i>response</i> HTTP to Insecure Transition in Form Post	92
Gambar 4.18 Hasil pengujian <i>curl</i> pada aler HTTPS	93
Gambar 4.19 Hasil pengecekan <i>HSTS preload list</i>	94
Gambar 4.20 Hasil peninjauan pada <i>browser</i> Microsoft Edge.....	94
Gambar 4.21 Hasil <i>clickjaker.io</i>	95
Gambar 4.22 Hasil pengujian <i>clickjacking</i>	96



DAFTAR TABEL

Tabel 2.1 Daftar port dan keterangannya (Kurose & Ross, 2017)	26
Tabel 2.2 Penelitian Relevan	44
Tabel 3.1 Perangkat keras.....	51
Tabel 3.2 Perangkat lunak	52
Tabel 3.3 Komponen perencanaan	57
Tabel 3.4 Pengkategorian terhadap <i>scanning</i> OWASP ZAP	62
Tabel 3.5 Skema serangan terhadap kerentanan.....	63
Tabel 3.6 Format tabel <i>reporting</i>	67
Tabel 3.7 Analisis risiko kerentanan Owasp Zap	69
Berdasarkan hasil <i>scanning</i> , maka data yang diperoleh akan ditampilkan pada tabel 4.1	72
Tabel 4.1 Data informasi website	72
Tabel 4.2 Data <i>network mapping</i>	76
Tabel 4.3 Informasi komponen website.....	77
Tabel 4.4 Daftar kerentanan pada website.....	80
Tabel 4.5 Daftar kerentanan yang akan diuji.....	86
Tabel 4.6 Reporting hasil pengujian berdasarkan parameter OWASP Top-10 2021	101

LAMPIRAN

Lampiran 1. Instrumen wawancara	117
Lampiran 2. Dokumentasi wawancara dengan administrator IT.....	119
Lampiran 3. Surat Izin Penelitian Skripsi	120
Lampiran 4. <i>Rules of Engagement</i> (ROE).....	123
Lampiran 5. Surat Tugas Dosen Pembimbing.....	127
Lampiran 6 Lembar Konsultasi Konsultasi Bimbingan	128
Lampiran 7 Surat Permohonan Sidang Skripsi	128
Lampiran 8. Surat Persetujuan Dosen Pembimbing.....	130
Lampiran 9. Surat Pernyataan Kelayakan Judul	131

