



**ANALISIS KEAMANAN *WEBSITE* SMAN 77 JAKARTA
MENGUNAKAN METODE *WEB SECURITY TESTING GUIDE***

**MUHAMAD SAFAR ASTAKUSUMA
2110511048**

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
JAKARTA
2025**



**ANALISIS KEAMANAN *WEBSITE* SMAN 77 JAKARTA
MENGUNAKAN METODE *WEB SECURITY TESTING GUIDE***

**MUHAMAD SAFAR ASTAKUSUMA
2110511048**

SKRIPSI

Sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
JAKARTA
2025**

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Muhamad Safar Astakusuma

NIM : 2110511048

Tanggal : 7 Juli 2025

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 7 Juli 2025

Yang Menyatakan



Muhamad Safar Astakusuma

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Muhamad Safar Astakusuma
NIM : 2110511048
Fakultas : Ilmu Komputer
Program Studi : S1 Informatika

Demi Pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (Non – exclusive Royalty Free Right) atas skripsi saya yang berjudul:

**ANALISIS KEAMANAN *WEBSITE* SMAN 77 JAKARTA
MENGUNAKAN METODE *WEB SECURITY TESTING GUIDE***

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/memformatkan, mengelola dalam bentuk pangkalan data (basis data), merawat dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Jakarta

Pada tanggal: 07 Juli 2025

Yang menyatakan,



Muhamad Safar Astakusuma

LEMBAR PENGESAHAN

Judul : Analisis Keamanan *Website* SMAN 77 Jakarta
Menggunakan Metode *Web Security Testing Guide*
Nama : Muhamad Safar Astakusuma
NIM : 2110511048
Program Studi : S1 Informatika

Disetujui oleh :

Penguji 1:

Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM.



Penguji 2:

Novi Trisman Hadi, S.Pd., M.Kom



Pembimbing 1:

Henki Bayu Seta, S.Kom., MTL



Pembimbing 2:

Hamonangan Kinantan Prabu, S.T., M.T.



Diketahui oleh:

Koordinator Program Studi:

Dr. Widya Cholil, M.I.T

NIP. 221112080

Dekan Fakultas Ilmu Komputer:

Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM

NIP. 197605082003121002





Tanggal Ujian Tugas Akhir:

04 Juli 2025

ANALISIS KEAMANAN *WEBSITE* SMAN 77 JAKARTA MENGUNAKAN METODE *WEB SECURITY TESTING GUIDE*

Muhamad Safar Astakusuma

ABSTRAK

Pesatnya perkembangan teknologi informasi di era digital membawa berbagai kemudahan, namun di sisi lain juga meningkatkan risiko keamanan siber yang dapat merugikan banyak pihak. Website sekolah sebagai salah satu media informasi publik dan layanan administratif tidak terlepas dari ancaman tersebut, termasuk kemungkinan adanya serangan siber seperti injeksi SQL, kontrol akses yang lemah, serta kebijakan kata sandi yang tidak memadai. Oleh karena itu, penelitian ini dilakukan dengan tujuan untuk menganalisis tingkat keamanan website SMAN 77 Jakarta terhadap serangan yang paling umum, yaitu kerentanan terhadap kontrol akses file atau direktori, *Injection*, kegagalan identifikasi dan otentikasi, dan kesalahan konfigurasi keamanan. Metode yang digunakan mengacu pada panduan OWASP Web Security Testing Guide (WSTG) dengan pendekatan penetration testing yang dilakukan pada salinan lokal website menggunakan akun admin untuk memeriksa form login dan halaman admin secara spesifik. Terdapat beberapa kerentanan dari hasil pengujian yang dilakukan analisis dengan bantuan CVSS pada aspek base score metrics untuk mengukur tingkat keparahan kerentanan.

Kata Kunci: *Website*, Burp Suite, OWASP WSTG, *Penetration Testing*, CVSS

SECURITY ANALYSIS OF THE SMAN 77 JAKARTA WEBSITE USING THE WEB SECURITY TESTING GUIDE METHOD

Muhamad Safar Astakusuma

ABSTRACT

The rapid development of information technology in the digital era brings various conveniences, but on the other hand also increases cybersecurity risks that can harm many parties. School websites as one of the public information media and administrative services are not free from these threats, including the possibility of cyber attacks such as SQL injection, weak access control, and inadequate password policies. Therefore, this study was conducted with the aim to analyze the security level of SMAN 77 Jakarta's website against the most common attacks, namely vulnerabilities to file or directory access control, Injection, identification and authentication failures, and security configuration errors. The method used refers to the OWASP Web Security Testing Guide (WSTG) with a penetration testing approach conducted on a local copy of the website using an admin account to check the login form and admin page specifically. There are several vulnerabilities from the test results that are analyzed with the help of CVSS on the base score metrics aspect to measure the severity of the vulnerability.

Keywords: Website, Burp Suite, OWASP WSTG, Penetration Testing, CVSS

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa, atas segala rahmat-Nya sehingga skripsi dengan judul “Analisis Keamanan Website SMAN 77 Jakarta Menggunakan Metode Web Security Testing Guide” berhasil diselesaikan. Penulis berharap skripsi ini dapat menambah wawasan dan pengetahuan tentang pengujian keamanan terhadap website. Penyelesaian skripsi ini tidak luput dari bantuan, arahan, dorongan, saran, bimbingan, serta kritik baik secara langsung maupun tidak langsung dari pihak manapun. Maka dari itu, pada kesempatan kali ini penulis ingin mengucapkan banyak terima kasih kepada:

1. Kedua orang tua, Imam Cahyadi dan Ratih Rahmawati yang telah memberikan dukungan penuh, doa disetiap ibadahnya, dan kasih sayang yang tulus kepada penulis dalam penyelesaian skripsi skripsi ini;
2. Kedua kakak, Tri Sutrisno Adri dan Frida Caturima Darojati yang telah memberikan dukungan secara materi dan pengertian terhadap penulis;
3. Bapak Dr. Anter Venus, MA., Comm. selaku Rektor Universitas Pembangunan Nasional Veteran Jakarta;
4. Bapak Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta;
5. Ibu Dr. Widya Cholil, M.I.T. selaku Koordinator Program Studi Sarjana Jurusan Informatika Fakultas Ilmu Komputer UPN Veteran Jakarta;
6. Bapak Henki Bayu Seta, S.Kom., MTI., selaku Dosen Pembimbing pertama yang telah memberikan bimbingan dan arahan kepada penulis dalam menyelesaikan skripsi ini;
7. Bapak Hamonangan Kinantan Prabu, S.T., M.T., selaku Dosen Pembimbing kedua yang telah memberikan bimbingan dan arahan kepada penulis dalam menyelesaikan skripsi ini;
8. Bapak Indra Permana Solihin, M.Kom., selaku Dosen Pembimbing Akademik program studi Informatika program sarjana;
9. Seluruh teman, sahabat, serta pacar yang selalu mendukung, menemani, bertukar pikiran, dan memberikan semangat kepada penulis dari awal perkuliahan hingga penyelesaian skripsi ini.

Penulis menyadari bahwa skripsi ini masih belum sempurna dan memiliki beberapa kekurangan. Oleh karena itu, dengan penuh kerendahan hati, penulis memohon maaf atas segala kekurangan yang ada serta sangat menghargai kritik dan saran yang membangun dari para pembaca. Masukan yang diberikan diharapkan dapat menjadi bahan berharga untuk perbaikan di masa mendatang.

Jakarta, 7 Juli 2025



Muhamad Safar Astakusuma

DAFTAR ISI

PERNYATAAN ORISINALITAS	i
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN	xiv
BAB 1. PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian	5
1.6 Sistematika Penulisan.....	6
BAB 2. TINJAUAN PUSTAKA	8
2.1 <i>Website</i>	8
2.2 <i>Penetration Testing</i>	8
2.3 <i>SQL</i>	9
2.4 <i>SQL Injection</i>	10
2.5 SQLMap.....	16
2.6 Dirb.....	20
2.7 DirSearch	21
2.8 WPScan	21
2.9 BurpSuite	23
2.10 OWASP Top 10 2021.....	24
2.11 <i>Web Security Testing Guide</i>	27
2.12 <i>Database</i>	32

2.13	SMAN 77 Jakarta	33
2.14	Kali Linux	34
2.15	<i>Common Vulnerability Scoring System (CVSS)</i>	34
2.15.1	<i>CVSS Base Score Metrics</i>	34
2.15.2	<i>CVSS Base Score Equations</i>	35
2.16	Penelitian Terdahulu	38
BAB 3. METODE PENELITIAN.....		49
3.1	Tahapan Penelitian.....	49
3.2	Rancangan Solusi	53
3.3	Alat Bantu Penelitian.....	55
3.4	Tempat dan Waktu Penelitian	56
BAB 4. PEMBAHASAN		57
4.1	Profil Perusahaan.....	57
4.2	Hasil <i>Information Gathering</i>	57
4.3	Hasil <i>Configuration and Deployment Management Testing</i>	66
4.4	Hasil <i>Identity Management Testing</i>	70
4.5	Hasil <i>Authentication Testing</i>	74
4.6	Hasil <i>Authorization Testing</i>	86
4.7	Hasil <i>Session Management Testing</i>	92
4.8	Hasil <i>Input Validation Testing</i>	100
4.9	Report.....	102
BAB 5. PENUTUP.....		107
5.1	Kesimpulan.....	107
5.2	Saran.....	108
DAFTAR PUSTAKA		109
RIWAYAT HIDUP		113
LAMPIRAN.....		114

DAFTAR TABEL

Tabel 2.1 Deskripsi Nilai Metrik	36
Tabel 2.2 Nilai Numerik untuk Metrik Skor Dasar.....	37
Tabel 2.3 Skala Penilaian Tingkat Keparahan Kualitatif.....	37
Tabel 2.4 Studi Literatur	41
Tabel 3.1 Rancangan Solusi.....	46
Tabel 4.1 Evaluasi Hasil Penelitian	104

DAFTAR GAMBAR

Gambar 2.1 Ilustrasi alur kerja serangan <i>SQL Injection</i>	11
Gambar 2.2 Klasifikasi <i>SQL Injection</i>	12
Gambar 2.3 Cara Kerja <i>Error-Based SQLi</i>	13
Gambar 2.4 Contoh Method Post.....	14
Gambar 2.5 Contoh Perintah SQLMap.....	17
Gambar 2.6 Contoh Perintah WPScan	22
Gambar 2.7 Fokus kategori OWASP Top 10 2021.....	24
Gambar 2.8 OWASP Top 10 2021	24
Gambar 2.9 Fokus kategori <i>web security testing guide</i>	28
Gambar 2.10 Metriks CVSS <i>base score</i>	35
Gambar 2.11 Persamaan skor dasar CVSS v3	38
Gambar 3.1 Diagram alur penelitian.....	49
Gambar 4.1 Hasil pencarian menggunakan operator “site”	58
Gambar 4.2 Hasil pencarian dengan menambahkan operator “filetype”	58
Gambar 4.3 Hasil pencarian dengan penambahan operator “inurl”.....	59
Gambar 4.4 Hasil pencarian menggunakan operator “cache”	59
Gambar 4.5 Hasil pencarian pesan “error”	60
Gambar 4.6 Hasil intercept request pada <i>website</i> SMAN 77 Jakarta	60
Gambar 4.7 Hasil pencarian robots.txt.....	61
Gambar 4.8 Hasil pencarian META Tags view-source	62
Gambar 4.9 Hasil pencarian sitemap.xml	62
Gambar 4.10 Hasil pencarian security.txt.....	63
Gambar 4.11 Hasil pencarian humans.txt	64
Gambar 4.12 Hasil Pencarian humans.txt dengan penambahan .well-known	64
Gambar 4.13 Halaman login <i>website</i>	65
Gambar 4.14 Hasil <i>intercept</i> halaman login	65
Gambar 4.15 Hasil WhatWeb	66
Gambar 4.16 Hasil nmap.....	66
Gambar 4.17 Hasil <i>Directory Discovery</i>	67
Gambar 4.18 Akses file dengan ekstensi .php	67

Gambar 4.19 Percobaan request <i>HTTP method</i> pertama	68
Gambar 4.20 Hasil percobaan request <i>HTTP method</i> pertama	69
Gambar 4.21 Percobaan request <i>HTTP method</i> kedua.....	69
Gambar 4.22 Hasil percobaan request <i>HTTP method</i> kedua	70
Gambar 4.23 Daftar peranan pada <i>Website</i>	71
Gambar 4.24 Peranan administrator.....	71
Gambar 4.25 Peranan editor.....	72
Gambar 4.26 Pembatasan hak akses peranan.....	72
Gambar 4.27 Verifikasi identitas pengguna.....	73
Gambar 4.28 <i>Percobaan Username</i>	73
Gambar 4.29 <i>Percobaan Sandi</i>	73
Gambar 4.30 Halaman login admin <i>website</i>	74
Gambar 4.31 Tampilan <i>burp intruder</i>	75
Gambar 4.32 Payload <i>username</i>	75
Gambar 4.33 Payload <i>password</i>	75
Gambar 4.34 Hasil pengujian menggunakan <i>burp intruder</i>	76
Gambar 4.35 Pengujian melalui permintaan langsung	76
Gambar 4.36 Perubahan kredensial menggunakan <i>cookie administrator</i>	77
Gambar 4.37 Percobaan pada parameter URL.....	77
Gambar 4.38 Laman <i>add user</i>	78
Gambar 4.39 Kategori sandi sangat lemah	79
Gambar 4.40 Kategori sandi lemah.....	79
Gambar 4.41 Kategori sandi sedang	80
Gambar 4.42 Kategori sandi kuat.....	80
Gambar 4.43 Kategori sandi kuat hanya dengan 12 karakter	81
Gambar 4.44 Penggunaan simbol yang dilarang.....	81
Gambar 4.45 Fitur buat kata sandi otomatis	82
Gambar 4.46 Laman fitur lupa kata sandi.....	82
Gambar 4.47 Tampilan laman tambah akun setelah perubahan kebijakan.....	83
Gambar 4.48 Laman pengaturan ulang kata sandi	85
Gambar 4.49 Fitur otentikasi dua faktor	86
Gambar 4.50 Opsi otentikasi dua faktor	86

Gambar 4.51 Penelusuran parameter url website.....	87
Gambar 4.52 Modifikasi parameter	87
Gambar 4.53 Payload 0-100.....	88
Gambar 4.54 Hasil pencarian jumlah user	89
Gambar 4.55 Parameter user_id=17.....	89
Gambar 4.56 Perubahan nilai parameter user_id	90
Gambar 4.57 Parameter <i>cookie</i> dan x-wp-nonce	90
Gambar 4.58 Perubahan nilai parameter <i>cookie</i> dan x-wp-nonce.....	90
Gambar 4.59 Parameter user_id pada <i>burp intruder</i>	91
Gambar 4.60 Paylaod untuk nilai user_id.....	91
Gambar 4.61 Hasil <i>burp intruder</i> parameter user_id	92
Gambar 4.62 <i>Cookies website</i>	92
Gambar 4.63 Atribut keamanan <i>cookies website</i>	93
Gambar 4.64 Pengujian atribut <i>secure</i>	94
Gambar 4.65 Simulasi CSRF	94
Gambar 4.66 Percobaan simulasi CSRF	95
Gambar 4.67 <i>Session ID</i> sebelum login	96
Gambar 4.68 <i>Session ID</i> setelah login	96
Gambar 4.69 <i>Session ID</i> login	97
Gambar 4.70 <i>Session ID</i> logout	97
Gambar 4.71 Percobaan <i>session id</i> login lama.....	98
Gambar 4.72 Percobaan <i>backward</i> pada browser	99
Gambar 4.73 Respon ketika berhasil login	99
Gambar 4.74 Halaman dasbor.....	100
Gambar 4.75 <i>Plugin idle timeout</i>	100
Gambar 4.76 <i>Payload reflected XSS</i>	101
Gambar 4.77 URL Target	101
Gambar 4.78 Hasil eksekusi <i>payload</i>	101
Gambar 4.79 Perintah SQLMap.....	102
Gambar 4.80 Hasil SQLMap.....	102

DAFTAR LAMPIRAN

Lampiran 1. Hasil Wawancara Wakil Kepala Sekolah SMAN 77 Jakarta	114
Lampiran 2. Hasil Wawancara Admin Website Sekolah SMAN 77 Jakarta	117
Lampiran 3. Surat Riset Penelitian.....	121
Lampiran 4. Kode menghilangkan baris tombol konfirmasi <i>password</i>	122
Lampiran 5. Kode untuk membuat kebijakan <i>password</i> kuat.....	123
Lampiran 6. Kode untuk memeriksa ketentuan <i>password</i>	124
Lampiran 7. Kode untuk tampilan ketentuan <i>password</i> kuat.....	125
Lampiran 8. Kode simulasi CSRF	126
Lampiran 9. Hasil Turnitin.....	127