



**PENETRATION TESTING MENGGUNAKAN OWASP TOP 10 2021
PADA *WEBSITE* MALA TOURS AND TRAVEL**

SKRIPSI

MUHAMMAD SATRIO JOYO LUKMONO

1810511047

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2023



**PENETRATION TESTING MENGGUNAKAN OWASP TOP 10 2021
PADA *WEBSITE* MALA TOURS AND TRAVEL**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana
Komputer**

MUHAMMAD SATRIO JOYO LUKMONO

1810511047

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2023

PERNYATAAN ORISINALITAS

Tugas Skripsi ini adalah hasil karya sendiri , dan semua sumber yang dikutip maupun yang dirujuk saya nyatakan dengan benar

Nama : Muhammad Satrio Joyo Lukmono

NIM : 1810511047

Tanggal : 1 Januari 2023

Bilamana dikemudian hari ditemukan ketidak sesuaian dengan pernyataan saya ini , maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 1 Januari 2023

Yang Menyatakan,



(Muhammad Satrio Joyo Lukmono)

PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Muhammad Satrio Joyo Lukmono
NIM : 1810511047
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-Exchange Royalty Free Right*) atas karya ilmiah saya yang berjudul:

Penetration Testing Menggunakan OWASP Top 10 2021 Pada Website Mala Tours And Travel

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti di Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formalitas, mengelola dalam bentuk pengkalan data (Basis Data), merawat dan mempublikasi Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta, Demikian Pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada Tanggal : 4 Januari 2023
Yang Menyatakan,



(Muhammad Satrio Joyo Lukmono)

LEMBAR PENGESAHAN

Lembar Pengesahan

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama : Muhammad Satrio Joyo Lukmono

NIM : 1810511047

Program Studi : S1 Informatika

Judul Skripsi : Penetration Testing Menggunakan Owasp Top 10 2021 Pada Website Mala Tours And Travel

Telah berhasil dipertahankan dihadapan tim penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Javanta, S.Kom., M.Si.
Penguji 1

Bayu Hananto, S.Kom., M.Kom.
Penguji 2

Henki Bayu Seta, S.Kom., MTI.
Pembimbing 1

I Wawan Widi P., S.Kom., MTI
Pembimbing 2

Dr. Ermatita, M.Kom.
Dekan

Dr. Widva Cholil, S.Kom., M.I.T.
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Pengesahan : 1 Januari 2023



**PENETRATION TESTING MENGGUNAKAN OWASP TOP 10 2021
PADA *WEBSITE* MALA TOURS AND TRAVEL
MUHAMMAD SATRIO JOYO LUKMONO**

ABSTRAK

Pertumbuhan jumlah penduduk masyarakat Indonesia mengakibatkan peningkatan yang sebanding dengan jumlah pengguna internet dan *social media* di Indonesia. Maka dari itu jumlah data dan informasi yang ada di internet akan bertambah dan privasi data tiap orang akan berkurang. Informasi juga digunakan dalam berbagai bidang, misalnya pariwisata atau travel untuk memesan tiket perjalanan atau paket perjalanan wisata. Mala Tours adalah operator ekowisata inbound dan outbound yang berbasis di Indonesia dan menggunakan *web* sebagai media promosi dan tempat transaksi penyimpanan data bagi pengguna seperti KTP. Tentunya dengan informasi ini akan sangat berbahaya apabila *web* milik Mala Tours diserang oleh pihak ilegal yang tidak bertanggung jawab. Untuk menghindari hal tersebut penulis memutuskan untuk melakukan *penetration testing* dengan metode OWASP Top 10 2021 yang masih sangat relevan dan populer. OWASP Top 10 adalah metode pengujian keamanan yang dibuat oleh OWASP (*Open Web Application Security*) yang berisikan 10 kategori celah keamanan. Setelah proses uji keamanan dilakukan perhitungan untuk menghitung hasil tingkat celah keamanan yang didapat menggunakan *OWASP Risk Rating Methodology* dan kemudian dibuat hasil *report*-nya. Pada hasil report ditemukan 8 celah keamanan dari 5 kategori celah keamanan dari 10 kategori OWASP Top 10 dengan tingkat skor *medium* dan *low*.

Kata kunci: OWASP, *Website*, *Penetration Testing*, OWASP TOP 10

ABSTRACT

The growth in the population of Indonesian people has resulted in a proportional increase in the number of internet and social media users in Indonesia. Therefore the amount of data and information on the internet will increase and the privacy of each person's data will decrease. Information is also used in various fields, for example tourism or travel to order travel tickets or travel packages. Mala Tours is an inbound and outbound ecotourism operator based in Indonesia and uses the web as a promotional medium and a place for data storage transactions for users such as national Identity Cards. Of course, this information will be very dangerous if Mala Tours' website is attacked by irresponsible illegal parties. To avoid this, the authors decided to do penetration testing using the OWASP Top 10 2021 method, which is still very relevant and popular. OWASP Top 10 itself is a security testing method created by OWASP (Open Web Application Security) which contains 10 categories of security holes. After the security test process, calculations are carried out to calculate the results of the level of security gaps obtained using the OWASP Risk Rating Methodology and then a report is made. The results of the report found 8 security vulnerabilities from 5 categories of security vulnerabilities from 10 OWASP Top 10 categories with medium and low score levels.

Keywords: OWASP, Website, Penetration Testing, OWASP TOP 10

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala Nikmat-Nya, sehingga skripsi dengan judul “Penetration Testing Menggunakan OWASP Top 10 2021 Pada *Website* Mala Tours and Travel” berhasil diselesaikan. Penulis ingin mengucapkan terima kasih kepada:

1. Kedua orang tua, keluarga dan kerabat saudara penulis yang selalu memberikan do’a, dukungan, dan semangat kepada penulis sehingga penulis dapat menyelesaikan skripsi ini.
2. Pak Henki Bayu Seta, S.Kom, M.T.I. dan Bapak I Wayan Widi P., S.Kom, M.T.I. selaku dosen pembimbing yang senantiasa membimbing, mengarahkan, dan memberi masukan dan saran pada penulis untuk menyelesaikan skripsi ini.
3. Dosen penguji yang menguji pada sidang tugas akhir skripsi.
4. Seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah memberikan ilmu yang bermanfaat kepada penulis.
5. Teman-teman Fakultas Ilmu Komputer yang telah memberikan dukungan dan do’a.
6. Bu Melissa sebagai pemilik dari Mala Tours and Travel yang *website* nya bersedia digunakan sebagai penelitian penulis.
7. Seluruh pihak yang terlibat dan mendukung dalam proses pembuatan skripsi yang belum disebutkan diatas dan tidak dapat disebutkan satu persatu penulis ucapkan terimakasih.

DAFTAR ISI

PERNYATAAN ORISINALITAS.....	iii
PERNYATAAN PERSETUJUAN PUBLIKASI.....	iv
LEMBAR PENGESAHAN	v
ABSTRAK.....	vi
ABSTRACT.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL.....	xvi
DAFTAR LAMPIRAN.....	xvii
DAFTAR SIMBOL	xviii
BAB I.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah.....	4
1.3. Batasan Masalah.....	4
1.4. Tujuan Penelitian	4
1.5. Manfaat Penelitian	5
1.6. Luaran Yang Diharapkan.....	5
1.7. Sistematika Penelitian.....	5
BAB II.....	7
2.1. Keamanan Informasi.....	7
2.2. <i>Website</i>	9
2.3. <i>Content Management System (CMS)</i>	10
2.4. <i>WordPress</i>	10
2.5. <i>Penetration Testing</i>	12
2.6. <i>Vulnerability Assesment</i>	13
2.7. <i>Black Box Testing</i>	14
2.8. <i>Open Web Application Security Project(OWASP)</i>	14

2.9.	OWASP TOP 10	14
2.9.1.	<i>Broken Control Access</i>	15
2.9.2.	<i>Cryptographic Failures</i>	15
2.9.3.	<i>Injection</i>	15
2.9.4.	<i>Insecure Design</i>	16
2.9.5.	<i>Security Misconfiguration</i>	16
2.9.6.	<i>Vulnerable and Outdated Components</i>	16
2.9.7.	<i>Identification and Authentication</i>	16
2.9.8.	<i>Software and Data Integrity Failures</i>	17
2.9.9.	<i>Security Logging and Monitoring Features</i>	17
2.9.10.	<i>Server-Side Request Forgery</i>	17
2.10.	<i>Fingerprinting Tools</i>	17
2.10.1.	<i>Wappalyzer</i>	17
2.11.	<i>Scanning Tools</i>	18
2.11.1.	OWASP ZAP	18
2.11.2.	NMAP	21
2.12.	<i>OWASP Risk Rating Methodology</i>	22
2.12.1.	<i>Likelihood factors</i>	22
2.12.2.	<i>Impact factors</i>	25
2.13.	<i>Exploit Tools</i>	28
2.13.1.	<i>WPScan</i>	28
2.13.2.	<i>BurpSuite</i>	28
2.13.3.	<i>XSSer</i>	28
2.13.4.	<i>SQLMap</i>	29
2.13.5.	<i>Metasploit Framework</i>	29
2.9.	Penelitian Terkait	29
BAB III.....		32
3.1.	Kerangka Pikir.....	32
3.1.1.	Identifikasi Masalah	33
3.1.2.	Studi Literatur	33
3.1.3.	Pengumpulan data	33
3.1.4.	Analisis Celah Keamanan	34
3.1.5.	Uji Keamanan	34

3.1.6.	Pembuatan Laporan	34
3.2.	Kebutuhan Aplikasi	34
3.2.1.	Otomatisasi OWASP ZAP	35
3.2.2.	Pseudocode	36
3.3.	Perangkat Penelitian.....	42
3.4.	Jadwal Penelitian.....	44
BAB IV	45
4.1.	Pengumpulan Data	45
4.1.1.	<i>Wappalyzer</i>	45
4.2.	Analisis Celah Keamanan.....	47
4.2.1.	OWASP ZAP	47
4.2.2.	NMAP	51
4.3.	Uji Keamanan	52
4.3.1.	<i>Broken Access Control</i>	52
4.3.1.1.	<i>Absence of Anti-CSRF Tokens</i>	52
4.3.1.2.	<i>Cookies without SameSite Attribute</i>	54
4.3.1.3.	<i>Server Leaks Information via 'X-Powered-By' HTTP Response header Field(s)</i>	57
4.3.1.4.	<i>Timestamp Disclosure - Unix</i>	59
4.3.1.5.	<i>Information Disclosure - Suspicious Comments</i>	62
4.3.2.	<i>Cryptographic Failures</i>	64
4.3.3.	<i>Injection</i>	67
4.3.3.1.	<i>Cross Site Scripting</i>	67
4.3.3.2.	<i>SQL Injection</i>	69
4.3.4.	<i>Insecure Design</i>	70
4.3.5.	<i>Security Misconfiguration</i>	73
4.3.6.	<i>Vulnerable and Outdated Components</i>	74
4.3.7.	<i>Identification and Authentication Failure</i>	75
4.3.7.1.	<i>User Enumeration</i>	76
4.3.7.2.	<i>Brute Force</i>	80
4.3.8.	<i>Software and Data Integrity Failures</i>	81
4.3.9.	<i>Security Logging and Monitoring Failures</i>	82
4.3.10.	<i>Server-Side Request Forgery</i>	83
4.4.	Hasil Report.....	85

4.5. Pengamanan Celah.....	88
4.6. Aplikasi Otomatisasi <i>Vulnerability Scanning</i>	89
4.6.1. Kebutuhan Aplikasi.....	89
4.6.1.1. OWASP ZAP	89
4.6.1.2. Python.....	89
4.6.1.2.1. ZAPv2 library	89
4.6.2. Tampilan Program.....	89
BAB V.....	100
5.1. KESIMPULAN	100
5.2. SARAN	100
DAFTAR PUSTAKA	102
RIWAYAT HIDUP.....	104
LAMPIRAN.....	105
LAMPIRAN 1	106
LAMPIRAN 2	110
LAMPIRAN 3	141

DAFTAR GAMBAR

Gambar 1. 1 Laporan Digital 2022.....	1
Gambar 1. 2 Laporan Digital 2021 Dengan Digital 2022.....	2
Gambar 1. 3 Malatours.com	3
Gambar 1. 4 Laman data diri	3
Gambar 2. 1 CIA Triad	7
Gambar 2. 2 Fase <i>Penetration Testing</i>	13
Gambar 2. 3 OWASP Top 10 2021.....	15
Gambar 2. 4 <i>Crawler</i>	19
Gambar 2. 5 Scanner rule alert	20
Gambar 2. 6 Detil rule alert	20
Gambar 3. 1 Kerangka Penelitian.....	32
Gambar 3. 2 <i>Flow chart</i> aplikasi Otomatisasi OWASP ZAP	35
Gambar 4. 1 Hasil <i>Wappalyzer</i>	46
Gambar 4. 2 Hasil OWASP ZAP	48
Gambar 4. 3 Form review	53
Gambar 4. 4 HTTP History Burp	53
Gambar 4. 5 HTTP Request.....	53
Gambar 4. 6 Hasil SameSite Cookies	54
Gambar 4. 7 X-Powered-By pada Header	57
Gambar 4. 8 Response header	59
Gambar 4. 9 Keyword Admin pada Source code	62
Gambar 4. 10 Form Login	64
Gambar 4. 11 Form Login terisi.....	64
Gambar 4. 12 Response HTTP Form Login.....	65
Gambar 4. 13 Tampilan <i>XSSer</i>	67
Gambar 4. 14 WAF Imunify360	70
Gambar 4. 15 Hasil SQL Map	70
Gambar 4. 16 form ganti password	71
Gambar 4. 17 Hasil SSL Scan	74
Gambar 4. 18 Hasil PureFTP.....	75
Gambar 4. 19 Hasil Scan <i>WPScan</i>	78

Gambar 4. 20 Hasil Bruteforce <i>WPScan</i>	81
Gambar 4. 21 Hasil Java Deserialization.....	82
Gambar 4. 22 Hasil Litespeed	83
Gambar 4. 23 Hasil SSRFMap	84
Gambar 4. 24 Risk severity	85
Gambar 4. 25 Tampilan ZAP	90
Gambar 4. 26 Menu Setting.....	90
Gambar 4. 27 Menu Options	90
Gambar 4. 28 API key.....	91
Gambar 4. 29 apikey.txt.....	91
Gambar 4. 30 Folder Program	91
Gambar 4. 31 Direktori program.....	91
Gambar 4. 32 Running Program.....	92
Gambar 4. 33 pilihan pada aplikasi	92
Gambar 4. 34 Ya tidak	92
Gambar 4. 35 Proses berjalan	92
Gambar 4. 36 Input durasi	93
Gambar 4. 37 Durasi Active Scan berubah.....	93
Gambar 4. 38 Durasi <i>Spider</i> berubah.....	93
Gambar 4. 39 Full Scan durasi	93
Gambar 4. 40 Full Scan active scan	94
Gambar 4. 41 Full Scan <i>Spider</i> scan	94
Gambar 4. 42 Input filter durasi	94
Gambar 4. 43 input thread	94
Gambar 4. 44 Active scan thread	95
Gambar 4. 45 <i>Spider</i> thread	95
Gambar 4. 46 Durasi Ajax	95
Gambar 4. 47 Durasi Ajax Zap.....	95
Gambar 4. 48 Ajax <i>Spider</i> pilihan.....	96
Gambar 4. 49 <i>Spider</i> Running	96
Gambar 4. 50 Zap <i>Spider</i> scan.....	96
Gambar 4. 51 Ajax Running.....	97

Gambar 4. 52 Ajax Chrome	97
Gambar 4. 53 Ajax Zap.....	97
Gambar 4. 54 Proses <i>Spider</i> selesai	98
Gambar 4. 55 Tampilan Ajax <i>Scanning</i> Selesai.....	98
Gambar 4. 56 Proses <i>Scanning</i> dimulai	98
Gambar 4. 57 Active <i>Scanning</i> zap.....	99
Gambar 4. 58 Tampilan saat Proses selesai.....	99
Gambar 4. 59 Tampilan Hasil Report	99


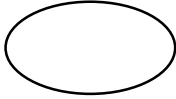


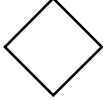
DAFTAR TABEL

Tabel 3. 1 Library	36
Tabel 3. 2 Pseudocode Aplikasi Otomatisasi OWASP ZAP	37
Tabel 3. 3 Spesifikasi Perangkat Keras	42
Tabel 3. 4 Jadwal Penelitian	44
Tabel 4. 1 Scanner Rule Alert OWASP ZAP	48
Tabel 4. 2 Command NMAP	51
Tabel 4. 3 Hasil NMAP	51
Tabel 4. 4 Command <i>XSSer</i>	67
Tabel 4. 5 Command <i>SQL Injection</i>	69
Tabel 4. 6 Command <i>SSLScan</i>	73
Tabel 4. 7 Command Exploit PureFTPd	74
Tabel 4. 8 Command User Enumerate	76
Tabel 4. 9 Command <i>Brute Force</i>	80
Tabel 4. 10 Command Litespeed scan	83
Tabel 4. 11 Command <i>SSRFmap</i>	84
Tabel 4. 12 Perhitungan risk severity	85
Tabel 4. 13 Command Samesite Cookies	88
Tabel 4. 14 Command XSS .htaccess	88
Tabel 1. 15 Scanner Rule Alert OWASP ZAP	113
Tabel 1. 16 <i>Command</i> NMAP	116
Tabel 1. 17 Hasil NMAP	116
Tabel 1. 18 <i>Command XSSer</i>	124
Tabel 1. 19 <i>Command SQL Injection</i>	125
Tabel 1. 20 <i>Command SSLScan</i>	126
Tabel 1. 21 Command Exploit PureFTPd	127
Tabel 1. 22 <i>Command User Enumerate</i>	129
Tabel 1. 23 <i>Command Brute Force</i>	131
Tabel 1. 24 <i>Command Litespeed scan</i>	134
Tabel 1. 25 <i>Command SSRFmap</i>	134
Tabel 1. 26 <i>Command Samesite Cookies</i>	139
Tabel 1. 27 <i>Command XSS .htaccess</i>	139

DAFTAR LAMPIRAN

Lampiran 1 Source Code	106
Lampiran 2 Hasil Report.....	110
Lampiran 3 Hasil Scanning OWASP ZAP	141
Lampiran 4 HASIL TURNITIN.....	185

DAFTAR SIMBOL

SIMBOL	Nama Simbol	Keterangan
	Simbol Proses	Menggambarkan Proses
	Simbol Terminator	Simbol untuk permulaan atau akhir dari suatu kegiatan
	Simbol Arah Data	Simbol untuk penunjuk arah data pada proses
	Simbol Manual Input	Simbol yang menandakan input manual
	Simbol Decision	Simbol untuk pilihan antara dua atau lebih proses