

**SKRIPSI**



**UJI KEAMANAN PADA *WEBSITE* JKL MENGGUNAKAN METODE  
*PENETRATION TESTING EXECUTION STANDARD***

**Gito Putro Wardana**

**NIM. 1910511042**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA  
2023**

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana**



**UJI KEAMANAN PADA *WEBSITE* JKL MENGGUNAKAN  
METODE *PENETRATION TESTING EXECUTION STANDARD***

**Gito Putro Wardana**

**NIM. 1910511042**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA  
2023**

## PERNYATAAN ORISINALITAS

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

Nama : Gito Putro Wardana

NIM : 1910511042

Tanggal : 12 Juli 2023

Judul Skripsi : *Uji Keamanan Website JKL Menggunakan Metode Penetration Testing Execution Standard*

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

Jakarta, 12 Juli 2023

Yang Menyatakan,



Gito Putro Wardana

# PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

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

Nama : Gito Putro Wardana  
NIM : 1910511042  
Fakultas : Ilmu Komputer  
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan karya ilmiah saya kepada Universitas Pembangunan Nasional "Veteran" Jakarta Hak Bebas Royalti Non-Eksklusif (*Non-Exchange Royalty Free Right*) untuk dipublikasikan dengan judul:

## **Uji Keamanan Website JKL Menggunakan Metode *Penetration Testing Execution Standard***

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media atau memformatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta  
Pada tanggal : 12 Juli 2023

Yang Menyatakan,



Gito Putro Wardana

# LEMBAR PENGESAHAN

## LEMBAR PENGESAHAN


Tugas Akhir ini diajukan oleh:


Nama : Gito Putro Wardana  
NIM : 1910511042  
Program Studi : S1 Informatika  
Judul Tugas Akhir : Uji Keamanan Website JKL Menggunakan Metode Penetration Testing Execution Standard

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

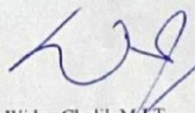
  
Bayu Hananto, S.Kom, M.Kom.

Penguji I

  
I Wayan Widi P., S.Kom., MTI  
Penguji II

  
Henki Bayu Seta, S.Kom, MTI  
Pembimbing

  
  
Dr. Emajita, M.Kom.  
Dekan

  
Dr. Widya Cholil, M.IT.  
Kepala Program Studi

Ditetapkan di : Jakarta  
Tanggal Ujian : Kamis, 6 Juli 2023



## KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadiran Allah SWT atas segala karuniaNya sehingga Skripsi ini berhasil diselesaikan. Dalam penyelesaian Tugas Akhir ini tidak lepas dari bantuan banyak pihak yang telah memberikan bantuan dan dukungan. Untuk itu peneliti mengucapkan banyak terima kasih kepada.

1. Bapak Dr. Anter Venus, M.A., Comm. selaku Rektor UPN Veteran Jakarta
2. Dr. Ermatita, M.Kom., selaku dekan Fakultas Ilmu Komputer
3. Dr. Widya Cholil, M.I.T. selaku Ketua Program Studi Sarjana Jurusan Informatika
4. Henki Bayu Seta, S.Kom, MTI. selaku Dosen Pembimbing
5. UPT TIK UPN Veteran Jakarta dan LPPM UPN Veteran Jakarta, yang telah membantu dan memberi izin dalam penelitian ini
6. Ibu saya yang telah memberikan dukungan baik secara moral maupun materil
7. Raihan Kemmy Rachmansyah, Eliana Rosa Evelyn, Ajeng Arifa Chantika Rindu, Galuh Widiana, Muhammad Taufiqurahman, dan Intern IT Nusantara Infrastructure Kampus Merdeka Batch 3 yang telah memberikan dukungan dan semangat dalam penyelesaian skripsi ini

Peneliti menyadari bahwa masih banyaknya kekurangan secara materi maupun teknik penulisan dari Tugas Akhir ini, mengingat kurangnya pengetahuan dan pengalaman peneliti. Oleh karena itu, kritik dan saran yang membangun akan sangat berarti bagi peneliti

Penulis



Gito Putro Wardana

**Uji Keamanan Website JKL Menggunakan Metode *Penetration Testing Execution Standard***

**Gito Putro Wardana**

**ABSTRAK**

*Website* adalah sekumpulan halaman *web* yang saling berhubungan yang umumnya berada pada peladen yang sama berisikan kumpulan informasi yang disediakan secara perorangan, kelompok, atau organisasi. Pada zaman sekarang perkembangan dunia Teknologi informasi semakin pesat yang mengakibatkan banyak orang yang mengakses internet khususnya mengunjungi sebuah *website*, dari anak kecil hingga orang dewasa. *Website* yang memiliki sistem keamanan yang lemah akan rentan oleh serangan-serangan ancaman yang dapat terjadi sewaktu-waktu. Berdasarkan data yang diperoleh dari Badan Siber dan Sandi Negara (BSSN) Terdapat 148 kasus peretasan *website* pada bulan agustus 2022. Pada penulisan skripsi ini, akan dilakukan uji keamanan terhadap *website* JKL. Hal ini dilakukan untuk menganalisis keamanan *website* tersebut dan cara untuk mengatasi jika terdapat celah yang ditemukan. Metode yang akan digunakan pada penulisan skripsi ini adalah *Penetration Testing Execution Standard (PTES)*.

**Kata Kunci:** *Website*, Keamanan *Website*, *Penetration Testing*, *Penetration Testing Execution Standard*, Peretasan

*Security Testing of Website JKL Using Penetration Testing Execution Standard  
Method*

**Gito Putro Wardana**

***ABSTRACT***

*A website is a collection of interconnected web pages that are generally located on the same server containing a collection of information provided by individuals, groups, or organizations. In today's world, the development of information technology is growing rapidly which has resulted in many people accessing the internet, especially visiting a website, from small children to adults. Websites that have a weak security system will be vulnerable to threat attacks that can occur at any time. Based on data obtained from the National Cyber and Crypto Agency (BSSN), there were 148 cases of website hacking in August 2022. In writing this thesis, a security test will be conducted on the JKL website. This is done to analyze the security of the website and how to overcome if any gaps are found. The method that will be used in writing this thesis is the Penetration Testing Execution Standard (PTES)*

***Keywords:*** Website, Website Security, Penetration Testing, Penetration Testing Execution Standard, Hacking



## DAFTAR ISI

	Halaman
PERNYATAAN ORISINALITAS .....	iii
PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS .....	iv
LEMBAR PENGESAHAN .....	v
KATA PENGANTAR .....	vi
ABSTRAK .....	vii
<i>ABSTRACT</i> .....	viii
DAFTAR ISI .....	ix
DAFTAR TABEL .....	xii
DAFTAR GAMBAR .....	xiii
DAFTAR LAMPIRAN .....	xv
BAB 1 PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	3
1.3. Tujuan Penelitian .....	3
1.4. Batasan Masalah .....	3
1.5. Manfaat Penelitian .....	4
1.6. Luaran yang Diharapkan .....	4
1.7. Sistematika Penulisan .....	4
BAB 2 TINJAUAN PUSTAKA .....	6
2.1. Website .....	6
2.2. Website JKL .....	6
2.3. Vulnerability Website .....	8
2.4. STRIDE .....	9
2.5. Cross-site scripting (XSS) .....	9
2.5.1. Serangan XSS Persistent .....	10
2.5.2. Serangan XSS Non-Persistent .....	10
2.5.3. Serangan XSS Berbasis Document Object Model (DOM)	

2.6.	SQL Injection .....	11
2.7.	Broken Access Control .....	12
2.8.	Vulnerability Assessment .....	12
2.9.	Common Vulnerability and Exposures (CVE) .....	13
2.9.1.	Common Vulnerability Scoring System (CVSS).....	13
2.10.	Penetration Testing.....	16
2.11.	Penetration Testing Execution Standard (PTES).....	17
2.11.1.	Pre-engagement Interactions .....	17
2.11.2.	Intelligence Gathering .....	17
2.11.3.	Threat Modelling.....	17
2.11.4.	Vulnerability Analysis.....	18
2.11.5.	Exploitation .....	18
2.11.6.	Post Exploitation .....	18
2.11.7.	Reporting .....	19
2.12.	Tools yang digunakan .....	19
2.12.1.	Nmap 7.93 .....	19
2.12.2.	Wappalyzer.....	19
2.12.3.	OWASP Threat Dragon.....	20
2.12.4.	OWASP ZAP .....	20
2.12.5.	Nikto .....	21
2.12.6.	Burp Suite.....	21
2.12.7.	Dirb.....	22
2.12.8.	SQLMap .....	22
2.13.	Penelitian Terdahulu .....	22
<b>BAB 3 METODOLOGI PENELITIAN.....</b>		<b>25</b>
3.1.	Tahapan Penelitian .....	25
3.2.	Pre-engagement Interactions.....	25
3.3.	Intelligence Gathering.....	26
3.3.1.	Nmap .....	26
3.3.2.	Wappalyzer.....	26
3.4.	Threat Modelling.....	26

3.4.1.	OWASP Threat Dragon.....	27
3.5.	Vulnerability Analysis .....	27
3.5.1.	CVE .....	27
3.5.2.	Nikto .....	27
3.5.3.	OWASP ZAP .....	27
3.6.	Exploitation .....	28
3.6.1.	Dirb.....	28
3.6.2.	Burp Suite.....	28
3.6.3.	SQLMap .....	28
3.7.	Post Exploitation .....	28
3.8.	Reporting.....	29
3.9.	Alat dan Bahan yang Digunakan.....	29
3.10.	Tahapan Kegiatan.....	30
BAB 4 HASIL DAN PEMBAHASAN.....		31
4.1.	Pre-engagement.....	31
4.2.	Intelligence Gathering.....	31
4.3.	Threat Modelling.....	32
4.4.	Vulnerability Analysis .....	34
4.5.	Exploitation .....	42
4.6.	Post Exploitation .....	53
4.7.	Reporting.....	54
BAB 5 Kesimpulan dan Saran .....		58
5.1.	Kesimpulan .....	58
5.2.	Saran.....	59
DAFTAR PUSTAKA .....		60
RIWAYAT HIDUP.....		63
LAMPIRAN.....		64

## DAFTAR TABEL

	<b>Halaman</b>
Tabel 2.1. Sepuluh Risiko Keamanan Aplikasi Web Paling Penting .....	8
Tabel 2.2 Kategori Ancaman STRIDE .....	9
Tabel 2.3. Skor CVSS berdasarkan peringkat kerentanan .....	13
Tabel 3.1. Tahapan Kegiatan .....	30
Tabel 4.1 Klasifikasi Ancaman .....	33
Tabel 4.2 Tabel hasil skor CVSS .....	55
Tabel 4.3 Solusi dan langkah – langkah pengerjaan solusi.....	56

## DAFTAR GAMBAR

	<b>Halaman</b>
Gambar 1.1. Data Statistik Kasus Peretasan .....	2
Gambar 2.1 Topologi Jaringan Website JKL.....	7
Gambar 2.2. Ilustrasi Tahapan <i>Vulnerability Assessment</i> .....	12
Gambar 2.3. Ilustrasi Tahapan <i>Penetration Testing</i> .....	16
Gambar 3.1. Tahapan Penelitian .....	25
Gambar 4.1. Hasil <i>Scanning port Nmap</i> .....	31
Gambar 4.2. Hasil <i>Scan</i> dari <i>Wappalyzer</i> .....	32
Gambar 4.3 Diagram <i>Flow Website JKL</i> .....	33
Gambar 4.4 Hasil <i>vulnerability</i> dari <i>website cvedetail.com</i> .....	35
Gambar 4.5 Hasil <i>scanning</i> menggunakan <i>nikto</i> .....	36
Gambar 4.6 Hasil <i>scanning</i> menggunakan <i>nikto</i> .....	38
Gambar 4.7 <i>Scanning</i> dengan <i>OWASP ZAP</i> .....	39
Gambar 4.8 Hasil <i>scanning OWASP ZAP</i> .....	39
Gambar 4.9 Proses <i>brute force</i> direktori menggunakan <i>dirb</i> .....	43
Gambar 4.10 Hasil direktori yang didapat pada <i>website JKL</i> .....	44
Gambar 4.11 Isi direktori “ <i>_db</i> ”.....	45
Gambar 4.12 Isi dari direktori <i>08</i> .....	45
Gambar 4.13 Isi file <i>adodb_0834db5d842d1330bf75a97222d23452.cache</i> .....	46
Gambar 4.14 Isi direktori <i>site</i> .....	47
Gambar 4.15 file <i>o.jpg</i> .....	47
Gambar 4.16 proses <i>SQL injection</i> menggunakan <i>SQLMap</i> .....	48
Gambar 4.17 proses <i>SQL injection</i> menggunakan <i>SQLMap</i> .....	48
Gambar 4.18 proses <i>SQL injection</i> menggunakan <i>SQLMap</i> .....	49
Gambar 4.19 List payload.....	50
Gambar 4.20 Hasil serangan <i>XSS</i> pada <i>search field</i> .....	50
Gambar 4.21 Hasil serangan <i>XSS</i> pada <i>username</i> dan <i>password field</i> .....	51
Gambar 4.22 pengisian kode <i>XSS via host header</i> dengan <i>burp suite</i> .....	52
Gambar 4.23 Hasil dari serangan <i>XSS via Host Header</i> .....	52

Gambar 4.24 direktori <i>public/site</i> .....	53
Gambar 4.25 informasi pengguna <i>website</i> JKL .....	54

## DAFTAR LAMPIRAN

	<b>Halaman</b>
LAMPIRAN 1. SURAT IZIN.....	63
LAMPIRAN 2. HASIL TURNITIN.....	64