



**PENGUJIAN CELAH KEAMANAN MENGGUNAKAN
METODE OWASP *WEB SECURITY TESTING GUIDE* (WSTG)
PADA *WEBSITE XYZ***

SKRIPSI

**ALBESTTY ISLAMYATI RAFELI
1810511110**

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN
JAKARTA
2022**



**PENGUJIAN CELAH KEAMANAN MENGGUNAKAN
METODE OWASP *WEB SECURITY TESTING GUIDE* (WSTG)
PADA *WEBSITE XYZ***

SKRIPSI

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

**ALBESTTY ISLAMYATI RAFELI
1810511110**

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN
JAKARTA
2022**

PERNYATAAN ORISINALITAS

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

Nama : Albestty Islamyati Rafeli

NIM : 1810511110

Tanggal : 26 Maret 2022

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

Jakarta, 26 Maret 2022

yang menyatakan.



Albestty Islamyati Rafeli

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

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

Nama : Albestty Islamyati Rafeli

NIM : 1810511110

Fakultas : Ilmu Komputer

Program Studi : S1 Infomatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

PENGUJIAN CELAH KEAMANAN MENGGUNAKAN METODE OWASP *WEB SECURITY TESTING GUIDE (WSTG) PADA WEBSITE XYZ*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 26 Maret 2022

Yang menyatakan,

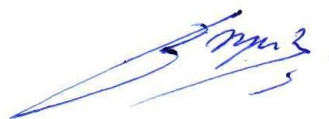
(Albestty Islamyati Rafeli)

PENGESAHAN

Dengan ini dinyatakan bahwa skripsi berikut :

Nama : Albesty Islamyati Rafeli
NIM : 1810511110
Program Studi : Informatika
Judul : Pengujian Celah Keamanan Menggunakan Metode
OWASP *Web Security Testing Guide* (WSTG) pada
Website XYZ.

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



Bayu Hananto, S.Kom., M.Kom.

Penguji I



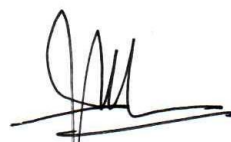
Noor Falih., S.Kom., M.T

Penguji II



Henki Bayu Seta, S.Kom, MTI.

Dosen Pembimbing I



I Wyan Widi P., S.Kom, MTI.

Dosen Pembimbing II



Dr. Ermatita, M.Kom.

Dekan



Desta Sandya Prasvita, S.Komp., M.Kom.

Ketua Program Studi

Ditetapkan di : Jakarta
Tanggal Persetujuan : 18 Juli 2022



Pengujian Celah Keamanan Menggunakan Metode OWASP *Web Security Testing Guide* (WSTG) pada *Website XYZ*

Albestty Islamyati Rafeli

Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta

Email: albestty@gmail.com

ABSTRAK

XYZ sebagai *website research* tentunya memiliki banyak data sensitif seperti data pribadi pengguna baik *researcher* ataupun responden dan data hasil *research*. Data ini rentan akan kebocoran data ataupun dicuri dan disalah gunakan oleh oknum yang tidak bertanggung jawab dan merugikan banyak pihak. *Penetration Testing* merupakan cara untuk mensimulasikan metode yang sekiranya akan digunakan oleh penyerang atau oknum tidak bertanggung jawab untuk dapat mengakses data secara ilegal kedalam sistem. WSTG merupakan singkatan dari *Web Security Testing Guide*, yaitu sebuah panduan *project* pengujian keamanan *Cyber* terutama dibidang pengembang aplikasi *web* dan keamanan professional. Pada penelitian ini dilakukan tujuh teknik yaitu *Information gathering*, *Configuration and Deployment Management Testing*, *Identity Management Testing*, *Input Validation Testing*, *Testing For Error Handling*, *Business Logic Testing* dan *Client Side Testing*. Teknik tersebut diterapkan pada *website XYZ* sehingga mendapatkan *vulnerability* dari *website XYZ*. Pada penelitian ini ditemukan delapan *vulnerability* pada *website XYZ*. Setelah dilakukan penilaian resiko secara menyeluruh resiko dari *vulnerability* pada *website XYZ* termasuk dalam kategori *medium*.

Kata Kunci : *Website, Penetration Testing, WSTG.*

ABSTRACT

XYZ as a *research website*, of course, has a lot of sensitive data, such as personal data of users, both researchers and respondents, and data from *research* results. This data is vulnerable to data leakage or being stolen and misused by irresponsible people and harming many parties. Penetration Testing is a way to simulate a method that would be used by an attacker or irresponsible person to be able to illegally access data into the system. WSTG stands for Web Security Testing Guide, which is a Cyber security testing project guide, especially in the field of web application developers and professional security. In this study, seven techniques were carried out, namely Information gathering, Configuration and Deployment Management Testing, Identity Management Testing, Input Validation Testing, Testing For Error Handling, Business Logic Testing and Client Side Testing. The technique is applied to the XYZ *website* so that it gets a vulnerability from the XYZ *website*. In this study, eight vulnerabilities were found on the XYZ *website*. After a thorough risk assessment, the risk of the vulnerabilities on the XYZ *website* is included in the medium category.

Keywords: *Website*, Penetration Testing, WSTG.

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas kehadiran Allah SWT atas segala nikmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Pengujian Celah Keamanan Menggunakan Metode OWASP *Web Security Testing Guide* (WSTG) pada *Website XYZ*” dengan baik. Pada kesempatan ini penulis ingin mengucapkan rasa terima kasih kepada:

1. Orang tua, keluarga dan kerabat penulis yang selalu memberikan do’a dan dukungan setiap waktu untuk kesuksesan penulis dalam menyelesaikan skripsi ini.
2. Bapak Henki Bayu Seta, S.Kom, M.T.I. dan Bapak I Wayan Widi P., S.Kom, M.T.I. selaku dosen Pembimbing serta Bapak Bagus Tri Mahardika, S.Kom., M.M.S.I. selaku dosen Pembimbing dari luar kampus Universitas Pembangunan Nasional Veteran Jakarta yang telah bersedia untuk meluangkan waktunya untuk memberikan bimbingan, masukan, kritik, saran dan dukungan selama penulis melakukan penelitian tugas akhir penulis.
3. Seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah mendidik dan memberikan ilmu yang bermanfaat kepada penulis.
4. Seluruh sahabat dan teman Program Studi Informatika angkatan 2018 Fakultas Ilmu Komputer yang telah memberikan dukungan dan do’a.
5. Seluruh pihak yang terlibat dalam kelancaran pembuatan skripsi ini yang belum disebutkan di atas dan tidak dapat disebutkan satu persatu yang telah memberikan dukungan, penulis ucapkan terima kasih.

Jakarta, 26 Maret 2022



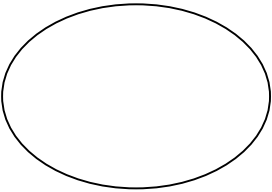



Albestty Islamyati Rafeli

DAFTAR ISI

SKRIPSI.....	i
SKRIPSI.....	i
PERNYATAAN ORISINALITAS	ii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	iii
PENGESAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR SIMBOL.....	x
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xii
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian	2
1.4 Manfaat Penelitian	3
1.5 Batasan Masalah	3
1.6 Luaran yang Diharapkan	4
1.7 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA.....	6
2.1 Vulnerability Assessment	6
2.2 Penetration Testing	6
2.2.1 Black Box Testing	8
2.2.2 Gray Box Testing	8
2.2.3 White Box Testing	8
2.3 Web Security Testing Guide	9
2.3.1 Information Gathering	9
2.3.2 Configuration dan Deployment Management Testing	10
2.3.3 Identity Management Testing	11
2.3.4 Input Validation Testing	11
2.3.5 Testing For Error Handling	12
2.3.6 Business Logic Testing	12
2.3.7 Client-side Testing	13
2.4 BURP Suite	14
2.4.1 BURP Tools	14
2.5 Dirb	15
2.6 Common Vulnerability Scoring System (CVSS)	15
2.7 Website	21
2.8 Website XYZ	21
2.9 Penelitian Terkait	21
BAB III METODELOGI PENELITIAN	26

3.1	Tahapan Penelitian.....	26
3.2	Metode Penelitian	27
3.2.1	Identifikasi Masalah	27
3.2.2	Studi Literatur.....	27
3.2.3	<i>Information Gathering</i>	27
3.2.4	<i>Configuration and Deployment Management Testing</i>	27
3.2.5	<i>Identity Management Testing</i>	28
3.2.7	<i>Testing For Error Handling</i>	28
3.2.8	<i>Business Logic Testing</i>	28
3.2.9	<i>Client Side Testing</i>	28
3.2.10	<i>Report</i>	29
3.3	Alat Bantu Penelitian	29
3.3.1	Perangkat Keras (<i>Hardware</i>)	29
3.3.2	Perangkat Lunak (<i>Software</i>)	29
3.4	Jadwal Penelitian.....	30
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....		31
4.1	<i>Information Gathering</i>	31
4.1.1	<i>Conduct Search Engine Discovery Reconnaissance for Information Leakage</i>	31
4.1.2	<i>Fingerprint Web Server</i>	32
4.1.3	<i>Review Web Server Metafiles for Information Leakage</i>	33
4.2	<i>Configuration and Deployment Management Testing</i>	37
4.2.1	<i>Review Old Backup and Unreferenced Files for Sensitive Information</i>	37
4.2.2	<i>Test HTTP Methods</i>	42
4.3	<i>Identity Management Testing</i>	43
4.3.1	<i>Test User Registration Process</i>	43
4.4	<i>Input Validation Testing</i>	46
4.4.1	<i>Testing For Stored Cross Site Scripting</i>	46
4.5	<i>Testing For Error Handling</i>	48
4.5.1	<i>Testing For Improper Error Handling</i>	48
4.6	<i>Business Logic Testing</i>	50
4.6.1	<i>Test Integrity Check</i>	50
4.7	<i>Client Side Testing</i>	53
4.7.1	<i>Testing For DOM-Based Cross Site Scripting</i>	53
4.7.2	<i>Testing Cross Origin Resource Sharing</i>	53
4.8	<i>Report</i>	54
4.9	Rekomendasi Perbaikan.....	58
BAB V PENUTUP.....		61
5.1	Kesimpulan	61
5.2	Saran.....	63
DAFTAR PUSTAKA		65
RIWAYAT HIDUP.....		67
LAMPIRAN.....		68

DAFTAR SIMBOL

Simbol	Nama Simbol	Keterangan
	Simbol <i>Terminator</i>	Menggambarkan Proses
	Simbol Proses	Dokumen yang dibutuhkan dalam proses sistem
	Simbol arah data atau arus data	Sebagai petunjuk arah data dan arus data pada proses
	Simbol Data	Sebagai masukan atau keluaran data untuk suatu proses

DAFTAR GAMBAR

Gambar 3. 1 <i>Flowchart penelitian</i>	26
Gambar 4.1 Pencarian situs <i>websiteXYZ</i> menggunakan <i>search engine google</i> ...	32
Gambar 4.2 Hasil <i>intercept request</i> terhadap situs <i>websiteXYZ</i>	32
Gambar 4.3 Tampilan awal atau <i>Home</i> dari <i>demo.websiteXYZ.id</i>	34
Gambar 4.4 URL <i>robots.txt</i>	34
Gambar 4.5 <i>View source</i> untuk melihat <i>tag meta</i>	35
Gambar 4.6 URL <i>sitemap.xml</i>	35
Gambar 4.7 URL <i>security.txt</i>	36
Gambar 4.8 URL <i>humans.txt</i>	36
Gambar 4.9 Hasil <i>Dirb</i>	37
Gambar 4.10 Hasil <i>Dirb</i>	38
Gambar 4.11 <i>https://websiteXYZ/admin</i>	38
Gambar 4.12 <i>https://websiteXYZ/controlpanel</i>	39
Gambar 4.13 <i>https://websiteXYZ/form</i>	40
Gambar 4.14 <i>https://websiteXYZ/web.config</i>	40
Gambar 4.15 Hasil download <i>https://websiteXYZ/web.config</i>	41
Gambar 4.16 Isi dari <i>file web.config</i>	41
Gambar 4.17 <i>https://websiteXYZ/webmail</i>	42
Gambar 4.18 Tampilan <i>tools Burp Suite HTTP Method</i>	43
Gambar 4.19 Tampilan interface pada saat mencek <i>HTTP Method</i>	43
Gambar 4.20 <i>Interface</i> percobaan pertama membuat akun	44
Gambar 4.21 <i>Interface</i> percobaan kedua membuat akun.....	44
Gambar 4.22 <i>Interface e-mail verifikasi</i>	45
Gambar 4.23 <i>Interface</i> pada saat mengklik <i>e-mail verifikasi</i>	45
Gambar 4.24 <i>Interface</i> saat <i>request</i> mengirimkan <i>e-mail verifikasi</i> ulang	46
Gambar 4.25 <i>Interface</i> saat membuat akun menggunakan <i>email</i> yang salah	47
Gambar 4.26 <i>Interface</i> saat setelah peneliti mengklik tombol lanjutkan.....	47
Gambar 4.27 <i>Interface tools Burp Suite</i>	48
Gambar 4.28 <i>Interface intercept error</i>	49
Gambar 4.29 <i>Interface intercept error</i>	49
Gambar 4.30 <i>Interface intercept register</i> tanpa <i>checklist</i>	50
Gambar 4.31 <i>Interface intercept</i> tidak ada validasi input	51
Gambar 4.32 <i>Interface intercept question number one</i>	52
Gambar 4.33 <i>Interface intercept question number eight</i>	52
Gambar 4.34 <i>Interface BURP Suite XSS</i>	53
Gambar 4.35 <i>Interface BURP Suite CORS</i>	54

DAFTAR TABEL

Tabel 3. 1 Jadwal Penelitian.....	30
Tabel 4. 1 Hasil Penelitian.....	54

DAFTAR LAMPIRAN

Lampiran 1 CVSS	A-1
Lampiran 2 WSTG <i>Checklist</i>	A-4
Lampiran 3 Hasil <i>Turnitin</i>	A-15