

**PENGUJIAN CELAH KEAMANAN PADA  
WEBSITE MENGGUNAKAN *FRAMEWORK* ISSAF**

**Tugas Akhir**

**Diajukan untuk Memenuhi Salah Satu Persyaratan Mencapai Derajat  
Sarjana Komputer**



Dibuat Oleh:

**CORNELIUS PHILLIPO JULIANTO**

**180709605**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS ATMA JAYA YOGYAKARTA  
2022**

## HALAMAN PENGESAHAN

Tugas Akhir Berjudul

PENGUJIAN CELAH KEAMANAN PADA WEBSITE MENGGUNAKAN FRAMEWORK ISSAF

yang disusun oleh

Cornelius Phillipu Julianto

180709605

dinyatakan telah memenuhi syarat pada tanggal 03 Juni 2022

		Keterangan
Dosen Pembimbing 1	: Dr. Ir. Alb. Joko Santoso, M.T.	Telah Menyetujui
Dosen Pembimbing 2	: Th. Adi Purnomo Sidhi, S.T., M.T.	Telah Menyetujui
Tim Penguji		
Penguji 1	: Dr. Ir. Alb. Joko Santoso, M.T.	Telah Menyetujui
Penguji 2	: Joseph Eric Samodra, S.Kom., MIT	Telah Menyetujui
Penguji 3	: Paulus Mudjihartono, S.T.,M.T., Ph. D	Telah Menyetujui

Yogyakarta, 03 Juni 2022

Universitas Atma Jaya Yogyakarta

Teknologi Industri

Dekan

ttd.

Dr. A. Teguh Siswanto, M.Sc.

Dokumen ini merupakan dokumen resmi UAJY yang tidak memerlukan tanda tangan karena dihasilkan secara elektronik oleh Sistem Bimbingan UAJY. UAJY bertanggung jawab penuh atas informasi yang tertera di dalam dokumen ini

# PERNYATAAN ORISINALITAS & PUBLIKASI ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama Lengkap : Cornelius Phillipio Julianto  
NPM : 180709605  
Program Studi : Informatika  
Fakultas : Teknologi Industri  
Judul Penelitian : Pengujian Celah Keamanan Pada *Website*  
Menggunakan *Framework ISSAF*

Menyatakan dengan ini:

1. Tugas Akhir ini adalah benar tidak merupakan salinan sebagian atau keseluruhan dari karya penelitian lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta atas penelitian ini, berupa Hak untuk menyimpan, mengelola, mendistribusikan, dan menampilkan hasil penelitian selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum atas pelanggaran Hak Cipta dalam pembuatan Tugas Akhir ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 16 Juni 2022

Yang menyatakan,



Cornelius Phillipio Julianto

180709605

# PERNYATAAN PERSETUJUAN DARI INSTANSI ASAL PENELITIAN



## KANTOR SISTEM INFORMASI UNIVERSITAS ATMA JAYA YOGYAKARTA

No : 034/In/KSI/2022  
Hal : Pemberitahuan  
Lamp :

Kepada Yth.  
**Dr. Ir. Albertus Joko Santoso, MT**  
Universitas Atma Jaya Yogyakarta  
di Yogyakarta

Dengan Hormat,

Menindaklanjuti surat dari dosen pembimbing I tentang permohonan untuk melakukan scan terhadap website [sikma.uajy.ac.is](http://sikma.uajy.ac.is) yang merupakan langkah dari pengujian framework ISSAF, dengan ini kami sampaikan bahwa permohonan tersebut dikabulkan hanya untuk keperluan tugas akhir.

Demikian pemberitahuan kami, atas perhatiannya diucapkan terimakasih.

Yogyakarta, 7 Maret 2022

Hormat kami



KANTOR  
**Paulus Mudi Hartono, ST., MT. PhD**  
UNIVERSITAS ATMA JAYA YOGYAKARTA  
Kepala Kantor Sistem Informasi-UAJY

**HALAMAN PERSEMBAHAN**

**Don't**

**Give**

**Up**



## KATA PENGANTAR

Puji dan syukur penulis haturkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya, sehingga dapat menyelesaikan pembuatan tugas akhir “PENGUJIAN CELAH KEAMANAN PADA *WEBSITE* MENGGUNAKAN *FRAMEWORK* ISSAF” ini dengan baik.

Penulisan tugas akhir ini bertujuan untuk memenuhi salah satu syarat dalam mencapai derajat sarjana komputer dari Program Studi Informatika, Fakultas Teknologi Industri di Universitas Atma Jaya Yogyakarta.

Penulis menyadari bahwa dalam pembuatan tugas akhir ini penulis telah mendapatkan bantuan, bimbingan, dan dorongan dari banyak pihak. Untuk itu, pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Tuhan Yesus Kristus yang selalu membimbing dalam iman-Nya, memberikan berkat-Nya, dan menyertai penulis selalu.
2. Bapak Dr. A. Teguh Siswantoro, M.Sc., selaku Dekan Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta.
3. Bapak Dr. Ir. Alb. Joko Santoso MT. selaku dosen pembimbing I yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
4. Bapak Thomas Adi Purnomo Sidhi, ST., MT selaku dosen pembimbing II yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.

Demikian laporan tugas akhir ini dibuat, dan penulis mengucapkan terima kasih kepada semua pihak. Semoga laporan ini dapat bermanfaat bagi pembaca.

Yogyakarta, 16 Juni 2022

*CPJ*

Cornelius Phillipo Julianto

180709605



# DAFTAR ISI

PENGUJIAN CELAH KEAMANAN <i>WEBSITE</i> .....	i
LEMBAR PENGESAHAN.....	ii
PERNYATAAN ORISINALITAS & PUBLIKASI ILMIAH.....	iii
PERNYATAAN PERSETUJUAN DARI INSTANSI ASAL PENELITIAN.....	iv
HALAMAN PERSEMBAHAN .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI .....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xii
INTISARI.....	xiii
BAB I. PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	3
1.3. Batasan Masalah.....	3
1.4. Tujuan Penelitian.....	3
1.5. Metode Penelitian.....	3
1.6. Sistematika Penulisan .....	4
BAB II. TINJAUAN PUSTAKA .....	6
BAB III. LANDASAN TEORI .....	14
3.1. Sistem .....	14
3.2. Informasi.....	14
3.3. Sistem Informasi .....	15
3.4. Peretasan ( <i>Hacking</i> ).....	15
3.4.1. <i>Vulnerability Testing</i> .....	15
3.4.2. <i>Penetration Testing</i> .....	16



3.4.3.	<i>Black Box Testing</i> .....	16
3.5.	Keamanan Sistem Informasi .....	16
3.6.	Framework .....	17
3.6.1.	ISSAF.....	17
3.6.2.	NIST.....	17
3.6.3.	OWASP.....	17
3.7.	Whois.....	18
3.8.	Spiderfoot.....	18
3.9.	WhatWeb .....	18
3.10.	NMAP.....	19
3.11.	Nessus.....	19
3.12.	Burp Suite .....	19
3.13.	Metasploit .....	20
<b>BAB IV.</b>	<b>ANALISIS DAN PERANCANGAN PENGUJIAN</b> .....	<b>21</b>
4.1.	Deskripsi Masalah .....	21
4.2.	Analisis Kebutuhan Pengujian .....	21
4.3.	Perancangan Pengujian.....	23
4.3.1.	<i>Information Gathering</i> .....	23
4.3.2.	<i>Network Mapping</i> .....	43
<b>BAB V.</b>	<b>IMPLEMENTASI DAN PENGUJIAN SISTEM</b> .....	<b>48</b>
5.1.	Implementasi.....	48
5.2.	<i>Vulnerability Identification</i> .....	48
5.2.1.	Nessus.....	48
5.2.2.	Burp Suite .....	54
5.2.3.	Metasploit .....	60

5.2.4. Microsoft IIS .....	65
BAB VI. PENUTUP .....	68
6.1. Kesimpulan .....	68
6.2. Saran .....	69
DAFTAR PUSTAKA .....	70



## DAFTAR GAMBAR

Gambar 4. 1. Hasil Subdomain Finder Pada Domain uajy.ac.id.....	24
Gambar 4. 2. Hasil Whois Pada Domain uajy.ac.id .....	25
Gambar 4. 3. Hasil Whois Pada sikma.uajy.ac.id.....	27
Gambar 4. 4. Hasil Whois Pada sikma.uajy.ac.id (2) .....	28
Gambar 4. 5. Hasil Whois Pada sikma.uajy.ac.id (3) .....	29
Gambar 4. 6. Domain Whois Pada sikma.uajy.ac.id Menggunakan Spiderfoot ...	32
Gambar 4. 7. Domain Parent Pada sikma.uajy.ac.id Menggunakan Spiderfoot ...	33
Gambar 4. 8. Domain Registrar Pada sikma.uajy.ac.id Menggunakan Spiderfoot .....	33
Gambar 4. 9. Open Port Pada sikma.uajy.ac.id Menggunakan Spiderfoot .....	34
Gambar 4. 10. Country Name Pada sikma.uajy.ac.id Menggunakan Spiderfoot .	35
Gambar 4. 11. Email Address Pada sikma.uajy.ac.id Menggunakan Spiderfoot...	35
Gambar 4. 12. Hasil WhatWeb Pada sikma.uajy.ac.id .....	37
Gambar 4. 13. Hasil Fiddler Pada sikma.uajy.ac.id.....	41
Gambar 4. 14. Hasil Developer Toolbar (Mozilla Firefox) Pada sikma.uajy.ac.id .....	42
Gambar 4. 15. Port yang Terbuka pada uajy.ac.id.....	44
Gambar 4. 16. Port yang Terbuka pada uajy.ac.id (2) .....	45
Gambar 4. 17. IP Address sikma.uajy.ac.id .....	45
Gambar 5. 1. Hasil Nessus Pada sikma.uajy.ac.id.....	49
Gambar 5. 2. Hasil Burp Suite Pada sikma.uajy.ac.id .....	55
Gambar 5. 3. Query yang digunakan pada Metasploit.....	60
Gambar 5. 4. Query yang digunakan pada Metasploit (2) .....	60
Gambar 5. 5. Query yang digunakan pada Metasploit (3) .....	61
Gambar 5. 6. Hasil Metasploit Pada sikma.uajy.ac.id .....	62

## DAFTAR TABEL

Tabel 2. 1. Tabel Perbandingan Peneliti Terdahulu dengan Saat Ini.....	10
Tabel 4. 1. Perangkat Keras Pengujian .....	22
Tabel 4. 2. Perangkat Lunak Pengujian .....	22
Tabel 4. 3. Hasil Pemindaian sikma.uajy.ac.id Menggunakan Whois dan Subdomain Finder.....	30
Tabel 4. 4. Hasil Pemindaian sikma.uajy.ac.id Menggunakan Aplikasi Spiderfoot .....	36
Tabel 4. 5. Hasil Pemindaian sikma.uajy.ac.id Menggunakan Aplikasi WhatWeb .....	39
Tabel 4. 6. Tabel Hasil <i>Network Mapping</i> .....	46
Tabel 5. 1. Hasil Pemindaian sikma.uajy.ac.id Menggunakan Aplikasi Nessus...50	
Tabel 5. 2. Pro dan Kontra Aplikasi Nessus.....	53
Tabel 5. 3. Hasil Pemindaian sikma.uajy.ac.id Menggunakan Aplikasi Burp Suite .....	56
Tabel 5. 4. Pro dan Kontra Aplikasi Burp Suite.....	59
Tabel 5. 5. Hasil Pemindaian sikma.uajy.ac.id Menggunakan Aplikasi Metasploit .....	63
Tabel 5. 6. Pro dan Kontra Aplikasi Metasploit.....	64
Tabel 5. 7. Hasil Pencarian Kelemahan Teknologi Microsoft IIS 10.0.....	66

# INTISARI

## PENGUJIAN CELAH KEAMANAN PADA *WEBSITE* MENGUNAKAN *FRAMEWORK* ISSAF

Intisari

Cornelius Phillipa Julianto

180709605

Berdasarkan *HootSuite*, Indonesia mengalami peningkatan pengguna internet dibandingkan dengan tahun 2020 lalu. Hal tersebut disebabkan oleh COVID-19 sehingga masyarakat terpaksa *Work from Home* (WFH). Para pelajar juga terpaksa belajar secara *online* dan mengikuti kelas dari rumah. Hal tersebut tentunya menyebabkan pengguna internet menjadi semakin banyak.

Pelajar dibantu oleh *website* yang telah disediakan oleh sekolah atau kampus untuk. *Website* tersebut memenuhi berbagai macam kebutuhan pelajar sehingga dapat melakukan belajar *online*. Salah satu *website* yang disediakan oleh Universitas Atma Jaya Yogyakarta adalah SIKMA (Sistem Informasi Kemahasiswaan). SIKMA berfungsi untuk mengatur segala macam informasi kemahasiswaan salah satunya adalah SPAMA. SPAMA merupakan salah satu syarat agar mahasiswa UAJY dapat lulus. Oleh karena itu, keamanan *website* SIKMA perlu dijaga dengan cara melakukan pemindaian. Pemindaian dapat dilakukan untuk mengetahui informasi serta kerentanan yang dimiliki sebuah *website*.

Pada Pengujian ini, penguji menggunakan alat Nessus, Burp Suite dan Metasploit sebagai pemindai *website* sikma.uajy.ac.id. Berdasarkan pengujian yang dilakukan, *website* sikma.uajy.ac.id memiliki 33 kerentanan (dua '*HIGH*', enam '*MEDIUM*', 25 '*INFO*') menggunakan alat Nessus. Untuk Burp Suite ditemukan sembilan kerentanan (tiga '*LOW*', enam '*INFORMATION*'). Terakhir, Metasploit menemukan 13 *port* terbuka. Adapun juga dilakukan perbandingan antara ketiga alat yang digunakan oleh penguji. Pertama, ketiga alat memiliki lisensi gratis dan dapat diakses pada berbagai macam *platform*. Kedua, Nessus dan Burp Suite terdapat tipe pemindaian yang ingin dilakukan, Metasploit tidak. Terakhir berdasarkan pengalaman penguji, hasil pemindaian yang didapat dan waktu pemindaian beragam.

Kata Kunci: *Website, Framework ISSAF, Vulnerability Scanning.*

Dosen Pembimbing I : Dr. Ir. Alb. Joko Santoso MT.

Dosen Pembimbing II : Thomas Adi Purnomo Sidhi, ST., MT

Jadwal Sidang Tugas Akhir : Senin, 30 Mei 2022