

**PENGUJIAN KEAMANAN SISTEM INFORMASI
UJAY MENGGUNAKAN *PENETRATION TESTING***

Tugas Akhir

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



Dibuat Oleh:

NICOLAS IVAN ASPRIANTAMA

170709279

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ATMA JAYA YOGYAKARTA
2021**

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

PENGUJIAN KEAMANAN SISTEM INFORMASI UAJY MENGGUNAKAN PENETRATION TESTING

yang disusun oleh

Nicolas Ivan Aspriantama

170709279

dinyatakan telah memenuhi syarat pada tanggal 25 Juli 2021

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

Yogyakarta, 25 Juli 2021

Universitas Atma Jaya Yogyakarta

Teknologi Industri

Dekan

ttt.

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 : Nicolas Ivan Aspriantama
NPM : 170709279
Program Studi : Informatika
Fakultas : Teknologi Industri
Judul Penelitian : Pengujian Keamanan Sistem Informasi UAJY
Menggunakan *Penetration Testing*

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, 22 Juli 2021

Yang menyatakan,



Nicolas Ivan Aspriantama

170709279

PERNYATAAN PERSETUJUAN DARI INSTANSI ASAL PENELITIAN

Saya yang bertanda tangan di bawah ini:

Nama Lengkap Pembimbing : Paulus Mudjihartono S.T., M.T., Ph.D.

Jabatan : Kepala Kantor Sistem Informasi

Departemen : Kantor Sistem Informasi

Menyatakan dengan ini:

Nama Lengkap : Nicolas Ivan Aspriantama

NPM : 170709279

Program Studi : Informatika

Fakultas : Teknologi Industri

Judul Penelitian : Pengujian Keamanan Sistem Informasi UAJY

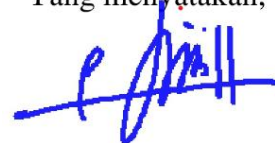
Menggunakan *Penetration Testing*

1. Penelitian telah selesai dilaksanakan pada perusahaan.
2. Perusahaan telah melakukan sidang internal berupa kelayakan penelitian ini dan akan mencantumkan lembar penilaian secara tertutup kepada pihak universitas sebagai bagian dari nilai akhir mahasiswa.
3. Memberikan kepada Instansi Penelitian dan Universitas Atma Jaya Yogyakarta atas penelitian ini, berupa hak untuk menyimpan, mengelola, mendistribusikan, dan menampilkan hasil penelitian selama tetap mencantumkan nama penulis.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 26 Juli 2021

Yang menyatakan,



Paulus Mudjihartono S.T., M.T., Ph.D.

Kepala Kantor Sistem Informasi

HALAMAN PERSEMBAHAN

**Keep
Up
the
Spirit**

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 KEAMANAN SISTEM INFORMASI UAJY MENGGUNAKAN *PENETRATION TESTING*” tersebut dengan baik.

Penulisan tugas akhir ini bertujuan untuk memenuhi salah satu syarat untuk 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 Siswanto, M.Sc., selaku Dekan Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta.
3. Bapak Eduard Rusdianto, S.T., M.T., selaku dosen pembimbing I yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
4. Bapak Paulus Mudjihartono, S.T., M.T., Ph.D., 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, 22 Juli 2021

A handwritten signature in black ink, consisting of several overlapping, stylized strokes that form a cursive representation of the name.

Nicolas Ivan Aspriantama

170709279

DAFTAR ISI

PENGUJIAN KEAMANAN SISTEM INFORMASI	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.....	xiv
INTISARI.....	xv
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	5
BAB II. TINJAUAN PUSTAKA.....	7
BAB III. LANDASAN TEORI.....	12
3.1. Sistem.....	12
3.2. Sistem Informasi	12
3.3. Peretasan (<i>Hacking</i>)	13
3.4. <i>Vulnerability</i>	15
3.5. Keamanan Sistem Informasi	15
3.6. <i>Penetration Testing</i>	16

3.6.1.	<i>Black Box Testing</i>	16
3.6.2.	Metasploit.....	17
3.6.3.	Low Orbit Ion Cannon	17
3.6.4.	DirBuster	17
3.6.5.	NMAP	18
3.6.6.	Whois	18
3.6.7.	Nessus	19
3.6.8.	WhatWeb.....	19
BAB IV. ANALISIS DAN PERANCANGAN PENGUJIAN		20
4.1.	Deskripsi Masalah.....	20
4.2.	Analisis Kebutuhan Pengujian	20
4.3.	Perancangan Pengujian	22
4.3.1.	Nmap.....	22
4.3.2.	Whois	28
4.3.3.	Nessus	34
4.3.4.	WhatWeb.....	44
4.3.5.	Google Directives.....	45
BAB V. IMPLEMENTASI DAN PENGUJIAN SISTEM		49
5.1.	Implementasi	49
5.2.	Implementasi Penyerangan	49
5.2.1.	SNMP <i>Exploit</i>	49
5.2.2.	Metasploit.....	51
5.2.3.	XSS (Cross Site Scripting).....	61
5.2.4.	DoS (Denial of Service)	81
5.2.5.	DirBuster	87

BAB VI. PENUTUP	92
6.1. Kesimpulan	92
6.2. Saran.....	93
DAFTAR PUSTAKA	94

DAFTAR GAMBAR

Gambar 4. 1. Port yang Terbuka Pada kuliah.uajy.ac.id.....	24
Gambar 4. 2. Port yang Terbuka Pada ortu.uajy.ac.id	25
Gambar 4. 3. Port yang Terbuka Pada ortu.uajy.ac.id (2).....	26
Gambar 4. 4. Pengintaian Domain uajy.ac.id Menggunakan Whois	29
Gambar 4. 5. Pengintaian kuliah.uajy.ac.id Menggunakan Whois	30
Gambar 4. 6. Pengintaian kuliah.uajy.ac.id Menggunakan Whois (2)	31
Gambar 4. 7. Pengintaian kuliah.uajy.ac.id Menggunakan Whois (3)	32
Gambar 4. 8. Hasil Pemindaian kuliah.uajy.ac.id Menggunakan Aplikasi Nessus (1).....	34
Gambar 4. 9. Hasil Pemindaian kuliah.uajy.ac.id Menggunakan Aplikasi Nessus (2).....	35
Gambar 4. 10. Hasil Pemindaian kuliah.uajy.ac.id Menggunakan Aplikasi Nessus (3).....	36
Gambar 4. 11. Hasil Pemindaian ortu.uajy.ac.id Menggunakan Aplikasi Nessus.	41
Gambar 4. 12. Hasil Pengintaian kuliah.uajy.ac.id Menggunakan WhatWeb.....	44
Gambar 4. 13. Hasil Pengintaian ortu.uajy.ac.id Menggunakan WhatWeb	44
Gambar 4. 14. Hasil Dari https://www.exploit-db.com/google-hacking-database Menggunakan Kata Kunci Moodle	46
Gambar 4. 15. Dorking site:moodle.*.*/login.....	47
Gambar 4. 16. Dorking inurl:"/moodle/login/index.php"	48
Gambar 5. 1. Hasil Exploit Menggunakan Alat Metasploit.....	50
Gambar 5. 2. Informasi Tambahan Menggunakan Use auxiliary/scanner/http/http_version.....	52
Gambar 5. 3. Hasil Menggunakan Modul auxiliary/scanner/http/dir_scanner	53
Gambar 5. 4. Hasil Menggunakan Modul auxiliary/scanner/http/dir_listing	54
Gambar 5. 5. Hasil Menggunakan Modul auxiliary/scanner/http/files_dir	55
Gambar 5. 6. Hasil Searchsploit.....	56
Gambar 5. 7. User dan Password Guessing Brute Force Port 22.....	57

Gambar 5. 8. Hasil dari Brute Force	58
Gambar 5. 9. Hasil dari Modul SSL Port 443	59
Gambar 5. 10. Melakukan Login pada Website kuliah.uajy.ac.id	62
Gambar 5. 11. Melakukan Stored XSS Untuk Memunculkan Alert.....	63
Gambar 5. 12. Hasil Stored XSS.....	63
Gambar 5. 13. Melakukan Variasi Script.....	64
Gambar 5. 14. Hasil Variasi Script	64
Gambar 5. 15. Melakukan Store XSS Kolom ‘Skype ID’	65
Gambar 5. 16. Hasil Store XSS Kolom ‘Skype ID’	65
Gambar 5. 17. Melakukan Variasi Script Kolom ‘Skype ID’	66
Gambar 5. 18. Hasil Variasi Script Kolom ‘Skype ID’	67
Gambar 5. 19. Injeksi Kolom ‘AIM ID’	68
Gambar 5. 20. Injeksi Kolom ‘Yahoo ID’	68
Gambar 5. 21. Injeksi Kolom ‘MSN ID’	68
Gambar 5. 22. Injeksi Kolom ‘ID number’	68
Gambar 5. 23. Injeksi Kolom ‘Institution’	69
Gambar 5. 24. Injeksi Kolom ‘Department’	69
Gambar 5. 25. Injeksi Kolom ‘Address’	69
Gambar 5. 26. Hasil Injeksi Kolom ‘Yahoo ID’, ‘AIM ID’, ‘MSN ID’, ‘ID number’, ‘Institution’, ‘Department’, dan ‘Address’	70
Gambar 5. 27. Melakukan Variasi Injeksi Kolom ‘MSN ID’	71
Gambar 5. 28. Melakukan Variasi Injeksi Kolom ‘AIM ID’	71
Gambar 5. 29. Melakukan Variasi Injeksi Kolom ‘Yahoo ID’	71
Gambar 5. 30. Melakukan Variasi Injeksi Kolom ‘ID number’	72
Gambar 5. 31. Melakukan Variasi Injeksi Kolom ‘Institution’	72
Gambar 5. 32. Melakukan Variasi Injeksi Kolom ‘Department’	72
Gambar 5. 33. Melakukan Variasi Injeksi Kolom ‘Address’	72
Gambar 5. 34. Hasil Variasi Injeksi	73
Gambar 5. 35. Melakukan Store XSS Kolom Deskripsi.....	74
Gambar 5. 36. Hasil Injeksi Store XSS.....	74
Gambar 5. 37. Hasil pada Kolom Deskripsi	75

Gambar 5. 38. Malformed a Tags Store XSS Injection	76
Gambar 5. 39. Hasil Store XSS Menggunakan Metode Malformed a Tags	76
Gambar 5. 40. Hasil yang Ditampilkan pada Profile	77
Gambar 5. 41. Percobaan Injeksi Kolom ‘Search’	78
Gambar 5. 42. Hasil Percobaan Injeksi XSS Kolom ‘Search’	79
Gambar 5. 43. Percobaan Penyerangan DoS Menggunakan Low Orbit Ion Cannon	81
Gambar 5. 44. Melakukan DoS pada Domain uajy.ac.id.....	83
Gambar 5. 45. Kondisi Situs kuliah.uajy.ac.id (1)	84
Gambar 5. 46. Kondisi Situs kuliah.uajy.ac.id (2)	85
Gambar 5. 47. Melakukan Pengaturan Pada Aplikasi DirBuster.....	88
Gambar 5. 48. Hasil dari DirBuster	89
Gambar 5. 49. Isi dari View Response.....	90

DAFTAR TABEL

Tabel 2. 1. Perbandingan Penelitian Terdahulu dengan Penelitian Saat Ini	10
Tabel 4. 1. Perangkat Keras Pengujian	21
Tabel 4. 2. Perangkat Lunak Pengujian	21
Tabel 4. 3. Hasil Pemindaian kuliah.uajy.ac.id Menggunakan Aplikasi Nessus ...	37
Tabel 4. 4. Hasil Pemindaian ortu.uajy.ac.id menggunakan Nessus.....	42
Tabel 5. 1. Hasil Metasploit.....	61
Tabel 5. 2. Hasil XSS	80
Tabel 5. 3. Hasil Pengujian DoS	87

INTISARI

PENGUJIAN KEAMANAN SISTEM INFORMASI UAJY MENGUNAKAN *PENETRATION TESTING*

Intisari

Nicolas Ivan Aspriantama

170709279

Sebanyak 171,17 juta jiwa dari total 264,16 juta jiwa masyarakat Indonesia tercatat pada Asosiasi Penyelenggara Jasa Internet (APJII) sebagai pengguna internet. Terlebih lagi pada tahun 2020, pandemi COVID-19 membuat pengguna internet bertambah pesat. Hal tersebut terjadi karena masyarakat dipaksa untuk melakukan *Work from Home* (WFH) dan para pelajar diminta untuk mengikuti kelas secara *online* yang berakibat pada penggunaan internet yang semakin bertambah.

Dalam masa pandemi seperti saat ini, *website* kampus akan sangat diperlukan untuk mengelola administrasi kampus dan kegiatan akademik secara *online*. Adapun Universitas Atma Jaya Yogyakarta juga menggunakan *website* untuk mengelola berbagai data untuk menunjang kegiatan akademik yang dilakukan. Oleh karena itu, diperlukan uji penetrasi untuk menjaga informasi yang terdapat pada *website* tersebut. Uji penetrasi dilakukan untuk mengetahui tingkat keamanan dan celah keamanan apa saja yang terdapat pada *website* kuliah.uajy.ac.id. *Website* tersebut merupakan salah satu *website* yang digunakan untuk mengelola tugas dan nilai mahasiswa.

Berdasarkan pengujian yang telah dilakukan, diperoleh bahwa *website* kuliah.uajy.ac.id memiliki dua kerentanan pada tingkat '*HIGH*', tiga kerentanan pada tingkat '*MEDIUM*', satu kerentanan pada tingkat '*LOW*', dan 18 kerentanan pada tingkat '*INFO*'. Adapun pemindaian juga dilakukan terhadap *website* ortu.uajy.ac.id. Akan tetapi, dari hasil pemindaian yang diperoleh diketahui bahwa kerentanan yang terdapat pada *website* ortu.uajy.ac.id lebih sedikit dibandingkan dengan *website* kuliah.uajy.ac.id, yaitu dua kerentanan pada tingkat '*MEDIUM*' dan 15 kerentanan pada tingkat '*INFO*'. Dari pemindaian tersebut dapat diketahui beberapa simulasi penyerangan yang dapat dilakukan terhadap *website* kuliah.uajy.ac.id yaitu, *exploit*, *cross-site scripting* (XSS), dan DoS.

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

Dosen Pembimbing I : Eduard Rusdianto S.T., M.T.

Dosen Pembimbing II : Paulus Mudjihartono S.T., M.T., Ph.D.

Jadwal Sidang Tugas Akhir : Kamis, 22 Juli 2021