

**PENGUJIAN KEAMANAN WEBSITE DENGAN
TEKNIK PENETRATION TESTING BERBASIS
OWASP TOP 10
STUDI KASUS SUBDOMAIN UPNJATIM**

SKRIPSI



Oleh :

MOCHAMMAD DZAKI AL VRIANO

NPM. 19081010138

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

JAWA TIMUR

2023

**LEMBAR PENGESAHAN
SKRIPSI**

**Judul : PENGUJIAN KEAMANAN WEBSITE DENGAN TEKNIK
PENETRATION TESTING BERBASIS OWASP TOP 10 STUDI
KASUS SUBDOMAIN UPNJATIM**

Oleh : MOCHAMMAD DZAKI AL VRIANO

NPM : 19081010138

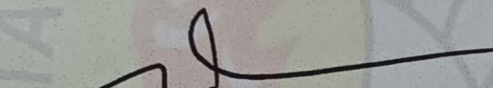
Telah Diseminarkan Dalam Ujian Skripsi, pada :

Hari Jumat, Tanggal 10 November 2023

Mengetahui

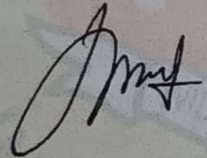
Dosen Pembimbing

1.


Dr. Ir. Mohammad Idhom, SP, S.Kom, MT.

NIP : 19830310 2021211 006

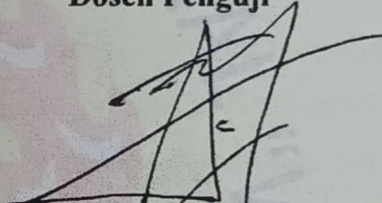
2.


Achmad Junaidi, S.Kom, M.Kom.

NIP : 3 7811 04 0199 1

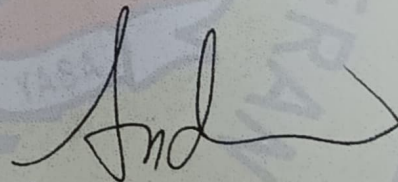
Dosen Penguji

1.


Firza Prima Aditiawan, S.Kom, M.TI.

NIP : 19860523 2021211 003

2.


Andreas Nugroho S., S.Kom., M.Kom.

NPT : 211199 00 412271

Menyetujui

Dekan

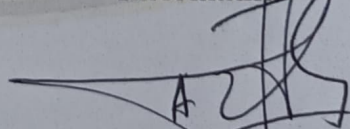
Fakultas Ilmu Komputer


Prof. Dr. Ir. Novirina Hendrasarie, M.T.

NIP : 19681126 199403 2 001

Koordinator Program Studi

Informatika


Fetty Tri Anggraeny, S.Kom., M.Kom.

NIP : 19820211 2021212 005

SURAT PERNYATAAN ORISINALITAS

Saya mahasiswa Program Studi Informatika UPN “Veteran” Jawa Timur, yang bertanda tangan di bawah ini:

Nama : Mochammad Dzaki Al Vriano

NPM : 19081010138

Dengan ini menyatakan bahwa judul skripsi yang Saya ajukan dan kerjakan, dengan judul:

**“PENGUJIAN KEAMANAN WEBSITE DENGAN TEKNIK
PENETRATION TESTING BERBASIS OWASP TOP 10
STUDI KASUS SUBDOMAIN UPNJATIM”**

Bukan merupakan plagiat dari skripsi atau tugas akhir maupun penelitian orang lain dan juga bukan merupakan produk atau *software* yang saya beli dari pihak lain. Saya juga menyatakan bahwa skripsi ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam daftar pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN “Veteran” Jawa Timur maupun institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, 10 November 2023
Format Saya,



Mochammad Dzaki Al Vriano
NPM. 19081010138

PENGUJIAN KEAMANAN WEBSITE DENGAN TEKNIK PENETRATION TESTING BERBASIS OWASP TOP 10 STUDI KASUS SUBDOMAIN UPNJATIM

Nama Mahasiswa : Mochammad Dzaki Al Vriano
NPM : 19081010138
Program Studi : Informatika
Dosen Pembimbing : Mohammad Idhom, SP, S.Kom, MT.
Achmad Junaidi, S.Kom, M.Kom.

ABSTRAK

Seiring dengan perkembangan teknologi informasi keamanan merupakan suatu faktor vital yang harus ada dan terjamin dalam penerapan dan penggunaannya. Aplikasi berbasis *web* seperti pada *subdomain* upnjatim.ac.id merupakan salah satu *platform* yang mungkin memiliki kerentanan dalam keamanan siber. Kerentan ini kemungkinan dapat terjadi terhadap berbagai ancaman maupun serangan maupun eksploitasi umum seperti SQL *injection*, DoS, CSRF, *Cross Site Scripting* (XSS), dan lain-lain yang tercantum dalam OWASP TOP 10.

Pada penelitian ini metode *penetration testing* ini berfungsi untuk analisis kerentanan dengan mengidentifikasi dan eksploitasi dari pengujian keamanan yang dapat dijadikan sebagai laporan pengembangan keamanan pada *website subdomain* upnjatim.ac.id. *Penetration testing* dilakukan melalui 5 tahapan *ethical hacking* yaitu *Reconnaissance*, *scanning & enumeration*, *gaining access* (*exploitation*), *maintaining access*, *covering tracks*, dan *pentest report*. Dari hasil pengujian didapat bahwa *website* target dengan *subdomain* upnjatim.ac.id. tidak memiliki kerentanan yang bersifat *critical*. Kerentanan yang ditemukan seperti DoS hanya mengakibatkan gangguan pada *web load time* dan tidak berpengaruh secara signifikan. Adapun langkah preventif yang dapat diterapkan terhadap potensi serangan adalah dengan melakukan *update* dan *maintenance* secara berkala.

Kata kunci : OWASP TOP 10, *Pentesting subdomain* upnjatim,
Cyber Security

KATA PENGANTAR

Segala puji bagi Allah SWT, berkat limpahan rahmat, nikmat dan karunianya penulis dapat menyelesaikan laporan skripsi yang berjudul “PENGUJIAN KEAMANAN WEBSITE DENGAN TEKNIK PENETRATION TESTING BERBASIS OWASP TOP 10 STUDI KASUS SUBDOMAIN UPNJATIM”. Penyusunan laporan ini dilakukan untuk memenuhi persyaratan kelulusan mata kuliah skripsi salah satu persyaratan kelulusan dari Program Studi Informatika, Fakultas Ilmu Komputer, UPN “Veteran” Jawa Timur.

Penulis menyadari adanya kekurangan dalam proses penulisan laporan ini. Sebagai bentuk perbaikan, penulis terbuka pada saran dan masukan dari pembaca.

Semoga laporan skripsi ini dapat bermanfaat dan dapat menjadi referensi yang baik bagi pembaca khususnya mahasiswa yang hendak melaksanakan mata kuliah skripsi baik di instansi yang sama maupun instansi yang berbeda.

Surabaya, 10 November 2023
Penulis,

Mochammad Dzaki Al Vriano
NPM. 19081010138

UCAPAN TERIMA KASIH

Ucapan terima kasih dan bersyukur kehadirat Allah SWT yang telah memberikan segala rahmat dan hidayah-Nya sehingga penyusunan laporan skripsi ini dapat terselesaikan. Penulis menyadari bahwa dalam penyusunan laporan skripsi ini melibatkan orang-orang yang sangat berjasa bagi penulis. Oleh karena itu, penulis menyampaikan rasa hormat serta ucapan terima kasih yang sebesar-besarnya kepada :

1. Kedua orang tua penulis yang selalu memberikan doa serta dukungan baik secara moril maupun materil.
2. Bapak Prof. Dr. Ir. Akhmad Fauzi, M.MT selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Ibu Prof. Dr. Ir. Novirina Hendrasarie, S.T., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Ibu Fetty Tri Anggraeny S.Kom., M.Kom., selaku Koordinator Program Studi Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Bapak Mohammad Idhom, SP, S.Kom, MT., selaku dosen pembimbing I yang telah memberikan arahan, petunjuk serta bimbingan sejak penyusunan usulan hingga penyelesaian laporan skripsi.
6. Bapak Achmad Junaidi, S.Kom, M.Kom., selaku dosen pembimbing II penulis yang telah banyak memberikan arahan dan bimbingan kepada penulis selama proses penyelesaian skripsi.
7. Seluruh dosen, staff, dan pihak tenaga pendidik program studi Informatika UPN “Veteran” Jawa Timur yang telah mengajar dan memberikan ilmu serta pengalaman selama masa perkuliahan.

Akhir kata, semoga dengan adanya laporan ini dapat bermanfaat bagi penulis, pembaca serta memberikan ilmu dan pemikiran yang baru bagi pihak yang membutuhkan.

DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI	i
LEMBAR PERNYATAAN ORISINALITAS.....	ii
ABSTRAK.....	iii
KATA PENGANTAR	iv
UCAPAN TERIMA KASIH.....	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR.....	ix
DAFTAR TABEL	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
BAB II TINJAUAN PUSTAKA	5
2.1 Penelitian Terdahulu	5
2.1.1 Visi Dan Misi	8
2.1.2 Program Sarjana.....	8
2.2 Sistem Informasi yang Diuji	9
2.3 Keamanan Informasi.....	10
2.4 Website.....	11
2.5 Penetration Testing	12
2.5.1 Black Box Testing	13
2.5.2 White Box Testing.....	13
2.5.3 Gray Box Testing	13
2.6 OWASP	14
2.7 OWASP TOP 10	14
2.8 Domain Website	15
2.9 Kali Linux & Tools	16
2.9.1 Kali Linux	16

2.9.2	Metasploit	17
2.9.3	Nmap	18
2.9.4	Burp Suite	19
2.9.5	Shell	20
2.9.6	GoWitness.....	20
2.9.7	SQLMap	21
2.9.8	WPScan.....	22
2.9.9	Joomscan.....	22
2.9.10	DoS Tools	23
BAB III METODOLOGI		24
3.1	Studi Literatur	24
3.2	Tahapan Penelitian	25
3.3	Ethical Hacking	24
3.3.1	Reconnaissance	27
3.3.2	Scanning & Enumeration	32
3.3.3	Gaining Access	42
3.3.4	Maintaining Access	46
3.3.5	Covering Tracks	47
3.3.6	Pentest Report	48
BAB IV HASIL & PEMBAHASAN.....		49
4.1	Temuan.....	49
4.1.1	User Login.....	50
4.1.2	Web Fingerprinting Results	51
4.1.3	Vulnerabilities Scan Results	55
4.2	Exploitation	60
4.2.1	Subdomain fasilkom.upnjatim.ac.id	60
4.2.2	Subdomain fad.upnjatim.ac.id	65
4.2.3	Subdomain faperta.upnjatim.ac.id	68
4.2.4	Subdomain febis.upnjatim.ac.id.....	70
4.2.5	Subdomain fisip.upnjatim.ac.id	76
4.2.6	Subdomain ft.upnjatim.ac.id	79
4.3	Pentest Report	84
BAB V PENUTUP		85

5.1	Kesimpulan.....	85
5.2	Saran.....	86
	Daftar Pustaka	87

DAFTAR GAMBAR

Gambar 2.1 Struktur UPN “Veteran” Jawa Timur.....	10
Gambar 2.2 OWASP Top 10 Tahun 2021	15
Gambar 3.1 Tahapan Penelitian	26
Gambar 3.2 Terminal Hasil Whois	29
Gambar 3.3 Daftar Subdomain yang Ditemukan.....	30
Gambar 3.4 Perintah untuk Memulai local DB Gowitness.....	31
Gambar 3.5 Gallery View Gowitness	32
Gambar 3.6 URL Details dalam Gowitness.....	32
Gambar 3.7 Command untuk Scanning dengan WPScan.....	41
Gambar 3.8 Output dari WPScan.....	41
Gambar 3.9 Directory Browsing pada fasilkom.upnjatim.ac.id.....	44
Gambar 3.10 wp-login form fasilkom.upnjatim.ac.id.....	45
Gambar 3.11 login request pada Burp Suite	46
Gambar 4.1 Update dari Versi Wordpress Website FASILKOM.....	61
Gambar 4.2 SQL Injection pada User Login Form pada Website FASILKOM....	61
Gambar 4.3 XMLRPC Response pada Burpsuite	62
Gambar 4.4 XMLRPC Request pada Burpsuite.....	63
Gambar 4.5 Upload Directoy Listing pada subdomain fasilkom.....	63
Gambar 4.6 Kemungkinan Temuan External wp-cron	63
Gambar 4.7 Payload DoS pada wp-cron.php	64
Gambar 4.8 Temuan Admin+ Stored XSS pada subdomain Fasilkom.....	65
Gambar 4.9 Moderasi kolom komentar pada web subdomain fasilkom.....	65
Gambar 4.10 XMLRPC dalam kondisi non aktif pada web FAD	66
Gambar 4.11 Login form pada web FAD	67
Gambar 4.12 Kompleksitas tahapan SSRF with DNS Rebinding	68
Gambar 4.13 Login form pada web FAPERTA.....	70
Gambar 4.14 Penggunaan Modul SMTP Scanner pada Metasploit.....	72
Gambar 4.15 Penggunaan Modul DNS Scanner pada Metasploit	72
Gambar 4.16 Penggunaan Modul DNS Scanner pada Metasploit	73
Gambar 4.17 Penggunaan rsh-grind untuk Menguji Vuln RSH	74
Gambar 4.18 Konfigurasi Payload PHPMailer RCE Script.....	74
Gambar 4.19 Respons HTTP 403 yang Didapat PHPMailer RCE Script.....	75
Gambar 4.20 Penggunaan Modul Akeeba Unserialize Exploit pada Web FEBIS.	75
Gambar 4.21 Penggunaan Modul WP XMLRPC Checker pada Metasploit	77
Gambar 4.22 Restricted user Registration Form pada Website FISIP	78
Gambar 4.23 Deteksi GOTMLS Anti-Malware pada Path Traversal.....	78
Gambar 4.24 Penggunaan Script Integer Overflow terhadap mysql port	79
Gambar 4.25 Contact Form pada web subdomain FT	80
Gambar 4.26 Konfigurasi Variables PHPMailer RCE Script	80
Gambar 4.27 Respons 404 yang didapat dari PHPMailer RCE Script	81
Gambar 4.28 Popup Notice yang Muncul setelah Submit Contact Form	81
Gambar 4.29 Konfigurasi Payload Metasploit untuk Vuln Akeeba.....	82
Gambar 4.30 Penggunaan Modul Akeeba Unserialize Exploit pada Web FT	82

Gambar 4.31 Peenggunaan Script Doser untuk Pengujian DoS Web FT 83
Gambar 4.32 Penggunaan Script KarmaDDoS untuk Pengujian DoS Web FT..... 83

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu Dengan Penulis	7
Tabel 3.1 Versi OS dan Tools Kali Linux.....	25
Tabel 3.2 Daftar Subdomain Target.....	34
Tabel 4.1 Temuan Username pada Target	50
Tabel 4.2 Versi Website Target.....	51
Tabel 4.3 Hasil dari Nmap Scan FASILKOM	52
Tabel 4.4 Hasil dari Nmap Scan FAD.....	52
Tabel 4.5 Hasil dari Nmap Scan FAPERTA.....	53
Tabel 4.6 Hasil dari Nmap Scan FEBIS.....	53
Tabel 4.7 Hasil dari Nmap Scan FISIP	54
Tabel 4.8 Hasil dari Nmap Scan FT	54
Tabel 4.9 Hasil WPScan pada FASILKOM.....	55
Tabel 4.10 Hasil WPScan pada FAD	56
Tabel 4.11 Hasil WPScan pada FAPERTA	56
Tabel 4.12 Hasil WPScan pada FISIP.....	57
Tabel 4.13 Hasil WPScan pada FEBIS & FT	59
Tabel 4.14 Perbandingan KarmaDDoS dan Doser pada Subdomain FIK.....	64
Tabel 4.15 Perbandingan KarmaDDoS dan Doser pada Subdomain FAD.....	66
Tabel 4.16 Perbandingan KarmaDDoS dan Doser pada Subdomain FAPERTA.	69
Tabel 4.17 Perbandingan KarmaDDoS dan Doser pada Subdomain FEBIS.....	76
Tabel 4.18 Perbandingan KarmaDDoS dan Doser pada Subdomain FISIP	77
Tabel 4.19 Perbandingan KarmaDDoS dan Doser pada Subdomain FT	84