

PENETRATION TESTING PADA WESITE MAIL SERVER
DENGAN MENGGUNAKAN METODE OWASP

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar
Sarjana Komputer

DISUSUN OLEH:
ALI ZAINAL ABIDIN
1911102441087



PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
SAMARINDA
2023

***Penetration Testing pada Wesite Mail Server dengan
menggunakan Metode Owasp***

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar
Sarjana Komputer

Disusun Oleh:

Ali Zainal Abidin

1911102441087



**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR
SAMARINDA**

2023

HALAMAN PENGESAHAN

PENETRATION TESTING PADA WEBSITE MAIL SERVER DENGAN MENGUNAKAN METODE OWASP

DISUSUN OLEH :

ALI ZAINAL ABIDIN

1911102441097

Telah melaksanakan ujian skripsi dan dinyatakan lulus,

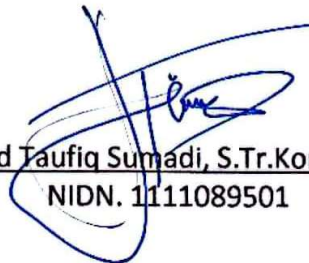
Pada tanggal 05 Juli 2023

Dosen Pembimbing



Faldi, S.Kom., M.TI
NIDN. 1121079101

Penguji



Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom
NIDN. 1111089501

Dekan



Prof. Ir. Sarjito, MT., Ph.D
NIDN. 0610116204

Ketua Program Studi



Asslia Johar Latipah, M.Cs
NIDN. 1124098902

SURAT PERNYATAAN KEASLIAN SKRIPSI

Assalamualaikum Warahmatullahi Wabarakatuh

Saya yang bertanda tangan dibawah ini :

Nama : ALI ZAINAL ABIDIN
NIM : 1911102440187
Program Studi : S1 TEKNIK INFORMATIKA
Judul Penelitian : PENETRATION TESTING PADA WESITE MAIL SERVER DENGAN
MENGGUNAKAN METODE OWASP

Menyatakan bahwa penelitian yang saya tulis ini benar-benar hasil karya saya sendiri, bukan merupakan pengambil alihan tulisan atau pikiran orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri.

Apabila dikemudian hari dapat dibuktikan bahwa terdapat plagiat dalam penelitian ini, maka saya bersedia menerima sanksi sesuai ketentuan perundangundangan (Permendiknas No.17, tahun 2010).

Samarinda, 05 Juli 2023



Ali Zainal Abidin
1911102441087

PRAKATA

Alhamdulillah, puji syukur kehadirat Allah SWT yang telah melimpahkan Rahmat dan Karunia-Nya, sehingga peneliti dapat menyelesaikan skripsi dengan judul “Penetration Testing Pada *Website Mail Server* Dengan Menggunakan Metode OWASP”. Dalam penyusunan skripsi ini,peneliti banyak mendapatkan bantuan dari beberapa pihak. Oleh karena itu, pada kesempatan ini peneliti ingin mengucapkan terima kasih kepada:

1. Orang tua penulis, Ibu, Bapak dan Kakak tercinta yang selalu memberikan doa serta dukungan dan juga telah membiayai kuliah penulis.
2. Yth. Prof. Dr. H. Bambang Setiaji, selaku Rektor Universitas Muhammadiyah Kalimantan Timur.
3. Yth. Prof. Ir. Sarjito, M.T., Ph.D selaku Dekan Fakultas Sains & Teknologi.
4. Yth. Bapak Faldi, S.Kom., M.TI selaku Dosen Pembimbing sekaligus penguji yang memberikan masukan dan arahan dalam menyusun skripsi ini.
5. Yth. Bapak Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom selaku Dosen Penguji yang telah memberikan masukan dan arahan dalam revisi skripsi ini.
6. Yth. Seluruh Bapak dan Ibu Dosen Program Studi Teknik Informatika Universitas Muhammadiyah Kalimantan Timur yang penulis banggakan dan hormati.
7. Perpustakaan Daerah, Kota Samarinda, dan Perpustakaan Universitas Muhammadiyah Kalimantan Timur
8. Tim KDM : Kikin, Putri, Dinamita, Afna, Trisha calon S.kom yang menjadi partner selama masa skripsi
9. Tim Bidin Lovers, teman-teman kampus, tim project tiga serangkai dan Putri Amanda yang telah mensupport dan menemani saya sampai sekarang.

ABSTRAK

Perkembangan teknologi saat ini memberikan dampak positif di berbagai bidang, termasuk internet. Seiring meningkatnya sumber daya manusia pemahaman dan kesadaran akan masalah keamanan sistem selalu menjadi ancaman setiap saat, terutama bagi pengembang aplikasi. Solusi untuk melindungi jaringan dari gangguan atau serangan hacker dapat dilakukan dengan *self-test*, yaitu pengujian yang dilakukan pada web server dengan tindakan yang sah seperti hacker salah satu metode *selftest* ini adalah *Penetration test* (Pentest). Pada penelitian ini dilakukan uji penetrasi testing berdasarkan ketentuan OWASP *Top 10* 2017 pada domain mail server Lokal yaitu mail.umtk.sch.id. Pengujian dilakukan dengan menggunakan aplikasi OWASP *Zap* dan Acunetix aplikasi ini dirancang untuk mensimulasikan tindakan seorang peretas dalam menemukan kerentanan pada *website*. Berdasarkan pengujian menggunakan OWASP *ZAP* dan Acunetix menunjukkan bahwa *website server local* yang berdomain mail.umkt.sch.id memiliki 9 kerentanan dan berdasarkan OWASP *TOP 10* 2017 memiliki 5 kategori kerentanan yaitu (A2) *Broken Authentication*, (A3) *Sensitive Data Exposure*, (A5) *Broken Access Control*, (A6) *Security Misconfiguration* dan (A9) *Using Components with Known Vulnerabilities*.

Kata Kunci : *Penetration Testing, Mail Server, OWASP TOP 10 2017*

ABSTRACT

The current technological advancements have had a positive impact in various fields, including the internet. With the increasing human resources, understanding, and awareness, security issues in systems have always been a threat, especially for application developers. Solutions to protect networks from disruptions or hacker attacks can be done through self-testing, which involves testing the web server with legitimate actions like a hacker. One of these self-testing methods is Penetration Testing (Pentest). In this research, a penetration testing was conducted based on the OWASP Top 10 2017 guidelines on the local mail server domain, mail.umtk.sch.id. The testing was performed using OWASP Zap and Acunetix applications, which are designed to simulate the actions of a hacker in discovering vulnerabilities on a website. Based on the testing using OWASP ZAP and Acunetix, it was found that the local server website with the domain mail.umkt.sch.id has 9 vulnerabilities and falls into 5 vulnerability categories according to OWASP TOP 10 2017: (A2) Broken Authentication, (A3) Sensitive Data Exposure, (A5) Broken Access Control, (A6) Security Misconfiguration, and (A9) Using Components with Known Vulnerabilities.

Keywords: Penetration Testing, Mail Server, OWASP Top 10 2017

DAFTAR ISI

HALAMAN JUDUL	HAL
HALAMAN PENGESAHAN	ii
PERNYATAAN KEASLIAN SKRIPSI	iii
PRAKATA	iv
ABSTRAK	v
<i>ABSTRACT</i>	vi
DAFTAR ISI	vii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN	xii
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	4
BAB 2 TINJAUAN PUSTAKA	5
2.1 Penelitian Terkait	5
2.2 Kajian Teori	7
2.2.1 Jaringan Komputer	7
2.2.2 Keamanan Jaringan komputer	8
2.2.3 Website	8
2.2.4 Web Server	8
2.2.5 Mail Server	8
2.2.6 SquirrelMail	9
2.2.7 POP3	9
2.2.8 IMAP	9
2.2.9 SMTP	9
2.2.10 DNS	9

2.2.11 IPAddress	9
2.2.12 Virtualbox	10
2.2.13 Linux.....	10
2.2.14 Acunetix.....	11
2.2.15 Common Vulnerability Scoring System (CVSS).....	11
2.2.16 Common Weakness Enumeration (CWE).....	11
2.2.17 Common Vulnerability and Exposures (CVE).....	12
2.2.18 Penetration Testing	12
2.2.19 Open Web Application Security Project (OWASP)	13
2.2.20 OWASP ZAP.....	13
2.2.21 OWASP TOP 10	13
BAB 3 METODE PENELITIAN.....	16
3.1 Subjek dan Objek Penelitian.....	16
3.1.1 Subjek Penelitian	16
3.1.2 Objek Penelitian	17
3.2 Metode Penelitian	17
3.2.1 Studi Literatur	17
3.2.2 Identifikasi Website	18
3.2.3 Penetration Testing	18
3.2.4 Alur Pengujian	18
3.2.5 Analisis dan Laporan.....	18
3.3 Jadwal Penelitian	19
BAB 4 HASIL dan PEMBAHASAN	20
4.1 Identifikasi Kerentanan.....	20
4.1.1 Absence of Anti-CSRF Tokens	21
4.1.2 Content Security Policy (CSP) Header Not Set	22
4.1.3 Cookie No HttpOnly Flag	23
4.1.4 Cookie without SameSite Attribute.....	24
4.1.5 Server Leaks Version Information via "Server" HTTP Response Header Field 25	

4.1.6 X-Content-Type-Options Header Missing.....	26
4.1.7 GET for POST.....	27
4.1.8 Modern Web Application	28
4.1.9 User Agent Fuzzer.....	28
4.2 Penetrasi OWASP Top 10.....	29
4.2.1 (A2) Broken Authentication.....	30
4.2.2 (A3) Sensitive Data Exposure	32
4.2.3 (A5) Broken Access Control	37
4.2.4 (A6) Security Misconfiguration.....	38
4.2.5 (A9) Using Components with Known Vulnerabilities	41
4.3 Penjelasan Hasil Penetrasi.....	44
4.3.1 Clickjacking: X-Frame-Options header missing	44
4.3.2 Cookie(s) without HttpOnly flag set (verified)	45
4.3.3 Cookie(s) without Secure flag set (verified)	46
4.3.4 Documentation file (verified)	47
4.3.5 Login page password-guessing attack.....	48
4.3.6 Possible sensitive files	49
4.3.7 Unencrypted connection (verified)	50
4.3.8 Content Security Policy (CSP) not implemented	52
4.3.9 Content type is not specified (verified).....	53
4.3.10 Error page web server version disclosure	54
4.3.11 Password type input with auto-complete enabled.....	55
4.4 Analisis dan Laporan hasil Uji Penetrasi.....	57
BAB 5 PENUTUP	60
5.1 Kesimpulan	60
5.2 Saran	60
DAFTAR PUSTAKA.....	61
LAMPIRAN	64

DAFTAR TABEL

Table 2.1 Penelitian Terkait	5
Table 2.2 Bilangan <i>biner</i> dan <i>desimal</i>	10
Table 2.3 Skor kerentanan CVSS	11
Table 3.1 Pengujian Penetrasi OWASP <i>Top 10</i>	18
Table 3.2 Jadwal penelitian.....	19
Table 4.1 Hasil Kerentanan	20
Table 4.2 Kategori A2	31
Table 4.3 Kategori A3	32
Table 4.4 Kategori A5	37
Table 4.5 Kategori A6	38
Table 4.6 Kategori A9	41
Table 4.7 Kategori kerentanan A3 dan A5	45
Table 4.8 Kategori kerentanan A3, A6, A9	46
Table 4.9 Kategori kerentanan A3, A6, A9	46
Table 4.10 Kategori A3	47
Table 4.11 Katergori A2, A3, A5, A6, A9.....	48
Table 4.12 kategori kerentanan A3.....	49
Table 4.13 Kategori kerentanan A2	51
Table 4.14 Kategori kerentanan A3,A6,A9.....	53
Table 4.15 Kategori kerentanan A3, A6 dan A9.....	53
Table 4.16 Kategori kerentanan A3,A6,A9.....	54
Table 4.17 kategori kerentanan A3.....	55
Table 4.18 Hasil Pengujian OWASP <i>TOP 10</i> 2017	56
Table 4.19 Hasil Analisis dan Laporan.....	57

DAFTAR GAMBAR

Gambar 1.1 Jumlah Pengguna Internet di Indonesia menurut <i>We Are Social</i> dan <i>Hootsuite</i> pada Januari 2020	1
Gambar 1.2 Indeks keamanan siber	2
Gambar 2.1 OWASP <i>Top 10</i> 2017	14
Gambar 3.1 Halaman Login.....	16
Gambar 3.2 Halaman Dashboard.....	17
Gambar 3.3 Tahapan Penelitian.....	17
Gambar 4.1 Hasil <i>Scan</i> OWASP ZAP	20
Gambar 4.2 <i>Absence of Anti-CSRF Tokens</i>	21
Gambar 4.3 Solusi <i>Absence of Anti-CSRF Tokens</i>	22
Gambar 4.4 <i>Content Security Policy (CSP) Header Not Set</i>	22
Gambar 4.5 Solusi <i>Content Security Policy (CSP) Header Not Set</i>	23
Gambar 4.6 <i>Cookie No HttpOnly Flag</i>	23
Gambar 4.7 Solusi <i>Cookie No HttpOnly Flag</i>	24
Gambar 4.8 <i>Cookie without SameSite Attribute</i>	24
Gambar 4.9 <i>Cookie without SameSite Attribute</i>	25
Gambar 4.10 <i>Server Leaks Version Information via "Server" HTTP Response Header Field</i>	25
Gambar 4.11 Solusi <i>Server Leaks Version Information via "Server" HTTP Response Header Field</i>	26
Gambar 4.12 <i>X-Content-Type-Options Header Missing</i>	26
Gambar 4.13 Solusi <i>X-Content-Type-Options Header Missing</i>	27
Gambar 4.14 <i>Get For Post</i>	27
Gambar 4.15 <i>Modern Web Application</i>	28
Gambar 4.16 <i>User Agent Fuzzer</i>	29
Gambar 4.17 Detail kerentanan OWASP <i>Top 10</i> 2017	30
Gambar 4.18 Contoh penerapan CSP	53

DAFTAR LAMPIRAN

Lampiran 1: Riwayat Hidup.....	65
Lampiran 2: Hasil <i>Acunetix</i>	66
Lampiran 3: Surat Ijin Penelitian.....	96
Lampiran 4: Lembar Bimbingan	98
Lampiran 5: Hasil Uji Turnitin.....	100