NASKAH PUBLIKASI *(MANUSCRIPT)*

PENETRATION TESTING PADA WEBSITE MAIL SERVER DENGAN MENGGUNAKAN METODE OWASP

OWASP METHODOLOGY FOR CONDUCTING PENETRATION TESTING ON MAIL SERVER WEBSITES

Ali Zainal Abidin[1], Faldi[2], and Muhammad Taufiq Sumadi[3]

DISUSUN OLEH:

ALI ZAINAL ABIDIN

1911102441087

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

2023

Naskah Publikasi *(Manuscript)*

Penetration Testing pada Website Mail Server dengan menggunakan Metode Owasp

Owasp Methodology for Conducting Penetration Testing on Mail Server Websites

Ali Zainal Abidin[1], Faldi[2], and Muhammad Taufiq Sumadi[3]

Disusun Oleh:

Ali Zainal Abidin

1911102441087

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

2023

HALAMAN PENGESAHAN

PENETRATION TESTING PADA WESITE MAIL SERVER DENGAN MENGGUNAKAN METODE OWASP

NASKAH PUBLIKASI

DISUSUN OLEH:

ALI ZAINAL ABIDIN

1911102441087

Pembimbing

Faldi, S.kom., M.TI
NIDN: 1121079101

Penguji

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

Dekan

Prof. Ir. Sarjito, M.T., Ph.D., IPM
NIDN: 0610116204

Ketua Program Studi

Assila Johar Latipah, S.Kom., M.Cs
NIDN: 1124098902

Penetration Testing pada *Wesite Mail Server d*engan menggunakan Metode OWASP

Ali Zainal Abidin[1], Faldi[2], dan Muhammad Taufiq Sumadi[3]
[1]Teknik Informatika, [1,2,3] Universitas Muhammadiyah Kalimantan Timur, Samarinda, Indonesia
*e-mail *Corresponding: 1911102441087@umkt.ac.id*

Abstract

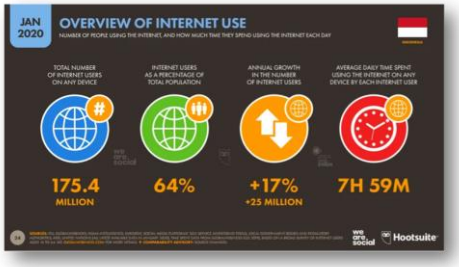
The development of technology has a positive impact in various fields, including the internet. Awareness of system security is crucial for application developers. The solution to protect networks from disruptions or hacker attacks can be done through self-testing, such as Penetration test (Pentest). This research conducted a penetration test on the mail server domain, mail.umtk.sch.id, using OWASP Zap and Acunetix tools. The test results revealed the detection of 9 vulnerabilities, categorized according to OWASP Top 10 2017, with 5 identified categories: Broken Authentication, Sensitive Data Exposure, Broken Access Control, Security Misconfiguration, and Using Components with Known Vulnerabilities.
Keywords: *Penetration Testing; Mail Server; OWASP Top 10 2017*

Abstrak

Perkembangan teknologi berdampak positif di berbagai bidang, termasuk internet. Kesadaran tentang keamanan sistem menjadi perhatian penting bagi pengembang aplikasi. Solusi melindungi jaringan dari gangguan atau serangan hacker dapat dilakukan dengan self-test, seperti Penetration test (Pentest). Penelitian ini melakukan uji penetrasi pada domain mail server yaitu mail.umtk.sch.id dengan menggunakan tools OWASP Zap dan Acunetix. Hasil dari pengujian ini menunjukkan bahwa terdapat 9 kerentanan yang terdeteksi dan berdasarkan kategori kerentanan OWASP Top 10 2017 terdapat 5 kategori yang terdeteksi yaitu *Broken Authentication, Sensitive Data Exposure, Broken Access Control, Security Misconfiguration, dan Using Components with Known Vulnerabilities*.
Kata kunci: Penetration Testing; Mail Server; OWASP TOP 10 2017

1. Pendahuluan

Perkembangan teknologi saat ini memberikan dampak positif di berbagai bidang, termasuk internet. Situs website adalah alternatif bagi korporasi untuk berkomunikasi, media promosi dan berinteraksi. Website ini dapat dengan mudah diakses oleh banyak orang dari mana saja dan kapan saja. Menurut laporan digital We Are Social (Hootsuite), jumlah pengguna internet di Indonesia mencapai 175 juta pengguna pada awal Januari 2020. Jumlah pengguna yang menggunakan internet meningkat 17 persen atau 25 juta pengguna dalam setahun terakhir[1].



Gambar 1. Jumlah Pengguna Internet di Indonesia menurut We Are Social dan Hootsuite pada Januari 2020

Setiap instansi harus memperhatikan keamanan data informasi yang tersimpan pada jaringan internet untuk mencegah gangguan dan tindak kejahatan. Gangguan tersebut dapat berupa serangan *Eksploitasi, Malware dan Injeksi database*. Pada dasarnya keamanan data sangat penting karena berkaitan dengan data pribadi *(privacy)*, hak akses atau verifikasi *(autentication),* integritas *(integritiy),* ketersediaan *(availability)* dan kerahasiaan *(confidentiality).* 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 *hacke*r salah satu metode *selftest* ini adalah *Penetration test (Pentest)*. Pengujian penetrasi aplikasi web adalah metode komprehensif untuk mendeteksi kerentanan sistem dalam pengujian penetrasi. Ada Beberapa metode dapat digunakan, salah satunya adalah Open Web Application Security Project (OWASP). Pada penelitian ini menggunakan metode OWASP Top 10 sebagai metode implementasi untuk pengujian penetrasi, OWASP Top 10 adalah daftar yang dirilis oleh komunitas OWASP yang berisi 10 celah keamanan teratas yang dapat mengancam keamanan sebuah website. Daftar ini terus berkembang dan mengikuti perkembangan teknologi website. Pertama kali dirilis pada tahun 2003, OWASP Top 10 telah mengalami pembaruan minor pada tahun 2004, 2007, 2010, dan 2017[2]. metode OWASP dipilih karena bersifat open source dan gratis untuk semua orang. Mengingat keamanan website cukup penting untuk mencegah dari tindak kejahatan yang dilakukan oleh pihak yang tidak bertanggung jawab, Penelitian ini dilakukan uji penetrasi testing Mail Server lokal, Mail server adalah sebuah server yang bertugas untuk mengelola dan mengirimkan email di dalam suatu jaringan[3]. Fungsi utama dari mail server adalah menerima, menyimpan dan mengirimkan pesan email antara pengguna yang menggunakan aplikasi email atau klien email. Penelitian ini dilaksanakan di Universitas Muhammadiyah Kalimantan Timur (UMKT). Hasil dari penelitian akan direkomendasikan sebagai saran dan langkah-langkah untuk meminimalisir tingkat kerentanan pada sistem yang ada.

2. Tinjauan Pustaka

Berdasarkan penelitian yang berjudul "Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademi" dengan *metode Open Web Application Security Project (OWASP),* hasil dari Penelitian menemukan 19 kerentanan pada website Sistem Informasi Akademik Universitas Pancasila melalui penetration test. Website ini berada pada level sedang dalam kualitasnya dan memerlukan perbaikan lebih lanjut oleh pengembang system[4].

Penelitian kedua yang berjudul “Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode *OWASP (Open Web Application Security Project)* untuk Penilaian Risk Rating”, Hasil dari penelitian ini terdapat 7 risiko dengan 3 risiko memiliki risk severity high, 2 risiko memiliki risk severity medium, 2 risiko memiliki risk severity low pada domain http://202.91.11.42/CI dan Terdapat 8 risiko dengan 3 risiko memiliki risk severity high, 2 risiko memiliki risk severity medium, 3 risiko memiliki risk severity low pada domain http://202.91.11.42/ [5].

Selanjutnya penelitian yang berjudul “Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Gratis Terhadap Serangan *Packet Sniffing*” dengan menggunakan metode *Information System Security Assessment Framework (ISSAF),* sebagai salah satu metode implementasi penetrasi testing, dengan target yang diuji adalah wifi di Universitas Siliwangi hasil yang diperoleh dari penelitian ini adalah Universitas Siliwangi secara keseluruhan memiliki jaringan wifi dan keamanan sistem pengguna komputer yang sangat rentan dengan tingkat kerawanan yang tinggi, kesadaran pengguna komputer terhadap keamanan sistem masih rendah, dan gratis. Pengguna wifi tidak memahami banyaknya serangan hacker pada jaringan yang lemah[6]. Berdasarkan dari hasil penelitian terkait yang dilakukan pengujian dengan metode *Information System Security Assessment Framework (ISSAF)* dan *Open Web Application Security Project (OWASP)* diperoleh bahwa, kerentanan pada sistem informasi website atau aplikasi masih memiliki sistem keamanan yang lemah. Penelitian terkait penggunaan metode ISSAF dan OWASP telah dilakukan dalam pengujian keamanan sistem.

Pada penelitian selanjutnya, akan dilakukan penetrasi testing dengan menggunakan metode penelitian yaitu metode OWASP Top 10 2017. Analisis keamanan dengan menggunakan metode ini akan dibandingkan untuk dijadikan rekomendasi perbaikan pada website.

Adapun teori pendukung sebagai dasar teori pada penelitian selanjutnya adalah sebagai berikut.

1) Website

Website adalah sebuah alamat (URL) yang berfungsi sebagai tempat menyimpan data dan informasi berdasarkan topik tertentu. Website dapat dikategorikan menjadi dua jenis yaitu Web Statis, Web yang berisi atau menampilkan informasi yang sifatnya statis (tetap). Web dinamis,

Web yang menampilkan informasi dan juga dapat berinteraksi dengan user yang bersifat dinamis[7].

2) Web Server

Web Server adalah perangkat lunak penerima permintaan (request) halaman website melalui HTTP atau HTTPs dari client (browser) dan mengirimkan respons berupa halaman web HTML. Fungsi web server tidak hanya mengolah data, tetapi juga mengirimkan file, foto, dan video sesuai permintaan client. Web server dapat dijalankan secara online[8].

3) Mail Server

Mail server adalah aplikasi pengelola pengiriman pesan email. Server ini menerima pesan dari email client atau server email lainnya. Sebagai pusat kendali sistem email, mail server memiliki area penyimpanan, konfigurasi user, daftar user, dan modul komunikasi [3].

4) *Squirrelmail*

SquirrelMail adalah webmail standar yang ditulis dalam PHP4. Dalam pemrograman PHP-nya, *SquirrelMail* mendukung protokol POP, IMAP, dan SMTP. Instalasi dan konfigurasi *SquirrelMail* sederhana. Aplikasi ini interaktif dan dapat dikonfigurasi sesuai keinginan pengguna [9].

5) VirtualBox

VirtualBox adalah perangkat lunak virtualisasi yang memungkinkan eksekusi sistem operasi tambahan di dalam sistem operasi utama. Contohnya, Anda bisa menjalankan sistem operasi lain di dalam Windows yang ada di komputer Anda [10].

6) Penetrasi testing

Penetrasi testing adalah simulasi serangan untuk menemukan kelemahan pada sistem jaringan organisasi/perusahaan [11].

7) OWASP

OWASP adalah framework open source yang fokus pada keamanan software aplikasi. Organisasi ini berupaya menemukan celah keamanan pada aplikasi website [12].

8) OWASP Zap

Zed Attack Proxy (ZAP) adalah tools scanner kerentanan dari OWASP yang aktif dan terus dikembangkan secara open-source. ZAP berfungsi sebagai server proxy, memungkinkan pengguna memanipulasi lalu lintas termasuk HTTPS [4].

9) Acunetix

Acunetix adalah perangkat lunak scanner aplikasi web yang mengidentifikasi kelemahan pada website. Kelebihannya adalah memberikan solusi untuk kelemahan yang ditemukan dan melacak setiap kerentanan. Acunetix juga memiliki fungsi tambahan untuk pengujian lanjutan pada website yang diuji [13].

10) *Common Vulnerability Scoring* System (CVSS)

CVSS adalah kerangka terbuka untuk mengkomunikasikan karakteristik dan dampak kerentanan aplikasi. Terdiri dari tiga kelompok pengukuran: Base, Temporal, dan Environmental. Base menggambarkan kualitas intrinsik kerentanan, Temporal mencerminkan perubahan karakteristik kerentanan seiring waktu, dan Environmental mencerminkan karakteristik kerentanan yang unik untuk lingkungan pengguna[14].

11) Common Weakness Enumeration (CWE)

CWE adalah proyek komunitas yang berisi katalog kelemahan dan kerentanan perangkat lunak. Tujuannya adalah memahami kelemahan perangkat lunak dan menciptakan alat otomatis untuk mengidentifikasi, memperbaiki, dan mencegah kerentanan. Proyek ini disponsori oleh Mitre [15].

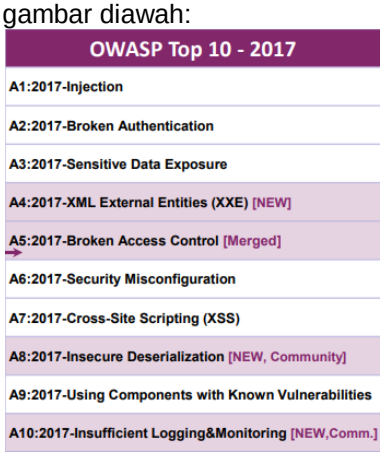
12) Common Vulnerability and Exposures (CVE)

CVE adalah kamus publik yang berisi identitas kerentanan keamanan informasi. Ini memfasilitasi berbagi data di database tentang keamanan informasi di jaringan yang berbeda dan menyediakan dasar untuk mengevaluasi alat keamanan organisasi. Identitas CVE memungkinkan penanganan yang lebih cepat dan mudah jika laporan alat evaluasi keamanan dilengkapi dengan identitas tersebut [14].

13) OWASP Top 10

OWASP Top 10 adalah daftar yang dirilis oleh komunitas OWASP yang berisi 10 celah keamanan teratas yang dapat mengancam keamanan sebuah website. Daftar ini terus berkembang dan mengikuti perkembangan teknologi website. Pertama kali dirilis pada tahun 2003, OWASP Top 10 telah mengalami pembaruan minor pada tahun 2004, 2007, 2010, dan 2017. Tujuan dari OWASP Top 10 adalah untuk meningkatkan kesadaran tentang keamanan aplikasi dengan mengidentifikasi risiko celah keamanan yang sering dihadapi dalam banyak

kasus. Dalam versi terbaru, OWASP Top 10 2017 menyajikan beberapa perubahan dalam struktur pengujian keamanan yang disarankan [2] Berikut adalah beberapa saran pengujian yang disajikan bisa dilihat pada gambar diawah:



Gambar 2. OWASP Top 10 2017

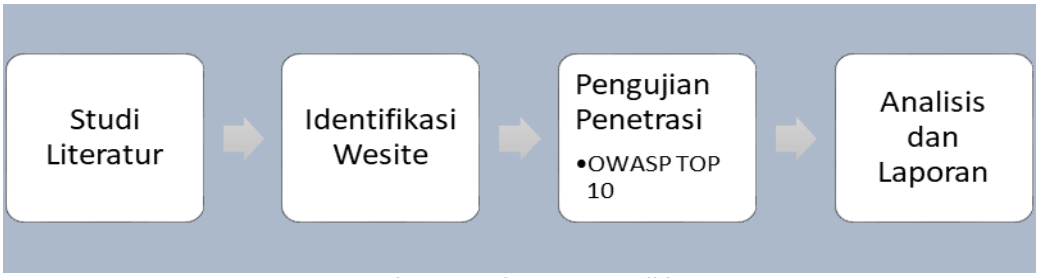
Sumber : **https://owasp.org/www-project-top-ten/2017/Top_10**

A1 Injection:
Melakukan pengujian terhadap celah keamanan seperti SQL Injection, NoSQL Injection, OS Injection, dan LDAP Injection yang terjadi saat data yang tidak diverifikasi dikirim ke intepreter sebagai perintah atau query.
A2 Broken Authentication:
Melakukan pengujian terhadap fungsi otentikasi dan manajemen sesi yang sering kali tidak diimplementasikan dengan benar, memungkinkan penyerang untuk mengeksploitasi password, kunci, atau token sesi untuk masuk ke sistem dengan identitas pengguna yang ada.
A3 Sensitive Data Exposure:
Melakukan pengujian terhadap perlindungan data sensitif pengguna seperti data keuangan, kesehatan, dan identitas pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.
A4 XML External Entities:
Melakukan pengujian terhadap website yang masih menggunakan XML untuk menangani dokumen, karena dapat memungkinkan penyerang mendapatkan informasi tentang server website, file internal, mengeksekusi perintah pada server, atau menyebabkan serangan denial of service.
A5 Broken Access Control:
Melakukan pengujian terhadap pengaturan akses yang tidak tepat, yang memungkinkan penyerang untuk mengubah hak akses mereka dan mengakses informasi sensitif atau melakukan tindakan yang seharusnya tidak diizinkan.
A6 Security Misconfiguration:
Melakukan pengujian terhadap kesalahan dalam konfigurasi sistem seperti pesan error yang terlihat, pengaturan HTTP header yang tidak terenkripsi, atau pengaturan default yang tidak aman.
A7 Cross-Site Scripting (XSS):
Melakukan pengujian terhadap celah keamanan yang memungkinkan penyerang untuk menyisipkan skrip JavaScript dalam input pengguna, yang dapat menyebabkan deface pada website atau mengarahkan pengguna ke website berbahaya.
A8 Insecure Deserialization:
Melakukan pengujian terhadap celah keamanan yang terjadi ketika aplikasi membaca string tanpa melakukan filter, yang dapat mengakibatkan eksekusi perintah yang tidak diinginkan dan serangan privilege escalation atau injection.
A9 Using Components with Known Vulnerabilities:
Melakukan pengujian terhadap penggunaan komponen dalam aplikasi (seperti framework, library, dan modul) yang diketahui memiliki celah keamanan, karena penyerang dapat mengeksploitasi celah tersebut untuk menyerang sistem.
A10 Insufficient Logging and Monitoring:

Melakukan pengujian terhadap sistem logging dan monitoring yang tidak memadai, yang dapat menyebabkan kesulitan dalam menganalisis serangan yang terjadi pada aplikasi.

3. Metodologi

Metode Penelitian akan dilakukan dengan beberapa tahapan yaitu diawali dengan tahap studi literatur dan diakhiri dengan tahapan analisis dan pelaporan. Tahapan yang digunakan sesuai dengan gambar dibawah.



Gambar 3. Tahapan Penelitian

1) Studi Literatur

Tahap ini dilakukan survey literatur tujuanya untuk menjelaskan tentang teori pendukung yang digunakan sebagai bahan penelitian. literatur rievew ini diperoleh dari buku, artikel penelitian dan internet.

2) Identifikasi Website

Website yang akan diuji adalah website server lokal yang berdomain mail.umkt.sch.id dengan ip address 192.168.20.17 dibuat dengan menggunakan virtualbox yang beroperasi pada sistem operasi windows 10 dan nantinya akan diuji tingkat kerentanan website server tersebut dengan beberapa tools yang berfungsi sebagai penetrasi testing. Berikut gambar dari tampilan website.

Gambar 4. Halaman Login dan Dahsboard Web Mail server

Pada gambar diatas menampilkan tampilan halaman login dan halaman dahsboard dari web mail server berbasis SquirrelMail yang berdomain mail.umkt.sch.id yang beroperasi pada sistem operasi linux debian 8.11.0.

3) Penetration Testing

Pengujian akan dilakukan dengan menggunakan metode OWASP Top 10.Pengujian metode OWASP Top 10 bisa dilihat pada tabel dibawah:

Tabel 1. Pengujian Penetrasi OWASP Top 10

OWASP TOP 10	***TOOLS***
A1-Injection	*Acunetix*
A2-Broken Authentication	*Acunetix*
A3-Sensitive Data Exposure	*Acunetix*

A4-XML External Entities (XXE)	*Acunetix*
A5-Broken Access Control	*Acunetix*
A6-Security Misconfiguration	*Acunetix*
A7-Cross-Site Scripting (XSS)	*Acunetix*
A8-Insecure Deserialization	*Acunetix*
A9-Using Components with Known Vulnerabilities	*Acunetix*
A10-Insufficient Logging & Monitoring	*Acunetix*

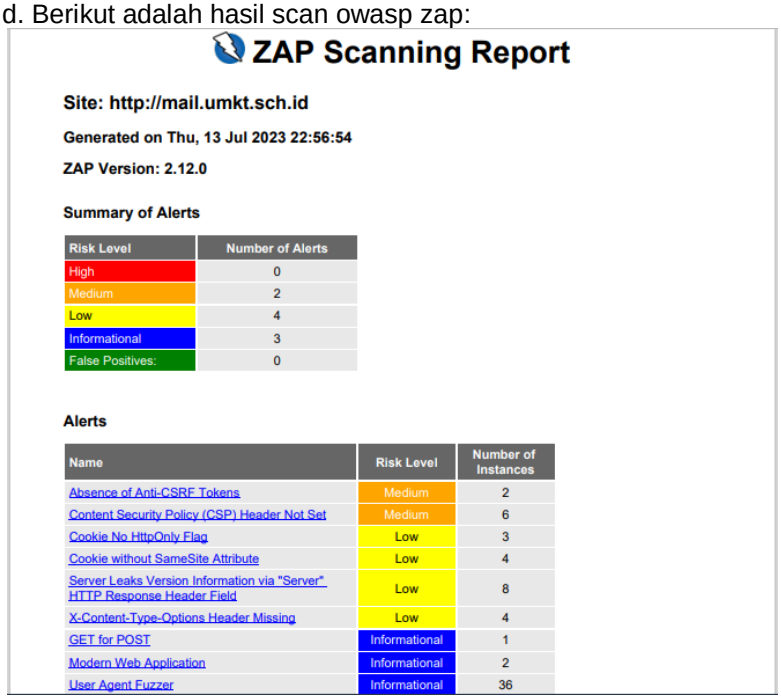
4) Analisis dan Laporan

Tahapan ini dilakukan Analisis dan laporan dari pengujian penetrasi menggunakan metode OWASP Top 10. Analisis dan laporan disajikan dalam bentuk saran atau rekomendasi untuk perbaikan pada website mail server.

4. Hasil dan Pembahasan

4.1 Identifikasi Kerentanan

Identifikasi dalam penelitian ini menggunakan tools owasp zap untuk mengetahui bagaimana tingkat kerentanan yang ada pada web server yang yang memiliki domain server mail.umkt.sch.id. Berikut adalah hasil scan owasp zap:



ZAP Scanning Report

Site: http://mail.umkt.sch.id

Generated on Thu, 13 Jul 2023 22:56:54

ZAP Version: 2.12.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	3
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	6
Cookie No HttpOnly Flag	Low	3
Cookie without SameSite Attribute	Low	4
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	8
X-Content-Type-Options Header Missing	Low	4
GET for POST	Informational	1
Modern Web Application	Informational	2
User Agent Fuzzer	Informational	36

Gambar 5. Hasil Scanning OWASP ZAP

Dari hasil scanning pada domain mail.umkt.sch.id dengan menggunakan tools owasp zap terdapat 9 kerentanan yaitu dapat dilihat pada table dibawah:

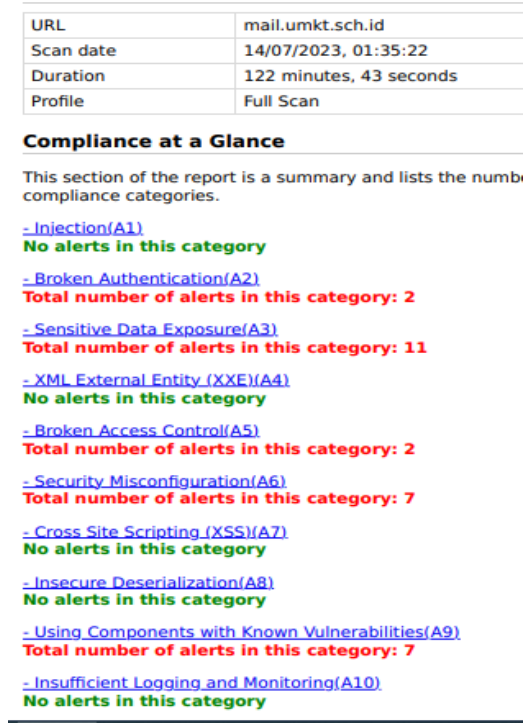
Tabel 2 Hasil Kerentanan

NO	Nama	Level Kerentanan	Jumlah Kerentanan
1	Absence of Anti-CSRF Tokens	Medium	2
2	Content Security Policy (CSP) Header Not Set	Medium	6
3	Cookie No HttpOnly Flag	Low	3
4	Cookie without SameSite Attribute	Low	4
5	Server Leaks Version Information via "Server" HTTP Response Header Field	Low	8
6	X-Content-Type-Options Header Missing	Low	4

7	GET for POST	Low	1
8	Modern Web Application	Informational	2
9	User Agent Fuzzer	Informational	36

4.2 Penetrasi Testing OWASP Top 10

Pada tahap selanjutnya adalah penetrasi testing pada domain mail server mail.umkt.sch.id dengan ketentuan OWASP Top 10, penulis memanfaatkan tools acunetix untuk uji penetrasi.Acunetix *Web Vulnerability Scanner* adalah aplikasi yang digunakan untuk mengaudit keamanan aplikasi web. Aplikasi ini dirancang untuk mensimulasikan tindakan seorang peretas dalam menemukan kerentanan seperti *SQL Injection* dan *serangan Cross Site Scripting*. Acunetix mendeteksi dan melaporkan berbagai kerentanan dalam berbagai arsitektur seperti *WordPress, PHP, ASP.NET, Java Frameworks, Ruby on Rails* dan lainnya. Hasil pemindaian keamanan oleh Acunetix Web Vulnerability Scanner dapat digunakan sebagai laporan yang disampaikan kepada pengembang website atau aplikasi [16]. Berikut beberapa ancaman yang beberapa sesuai ketentuan owasp top 10 dengan menggunakan tools acunetix terlihat pada gambar dibawah.



URL	mail.umkt.sch.id
Scan date	14/07/2023, 01:35:22
Duration	122 minutes, 43 seconds
Profile	Full Scan

Compliance at a Glance

This section of the report is a summary and lists the numb
compliance categories.

- Injection(A1)
No alerts in this category

- Broken Authentication(A2)
Total number of alerts in this category: 2

- Sensitive Data Exposure(A3)
Total number of alerts in this category: 11

- XML External Entity (XXE)(A4)
No alerts in this category

- Broken Access Control(A5)
Total number of alerts in this category: 2

- Security Misconfiguration(A6)
Total number of alerts in this category: 7

- Cross Site Scripting (XSS)(A7)
No alerts in this category

- Insecure Deserialization(A8)
No alerts in this category

- Using Components with Known Vulnerabilities(A9)
Total number of alerts in this category: 7

- Insufficient Logging and Monitoring(A10)
No alerts in this category

Gambar 6. Hasil Acunetix Berdasarkan OWASP Top 10 2017

Berdasarkan hasil pengujian penetrasi pada domain website server mail.umkt.sch.id menggunakan tools acunetix, website server memiliki 11 kerentanan dengan 5 kategori kerentanan sesuai ketentuan OWASP Top 10 2017. Berikut hasil pengujian yang disajikan dalam bentuk tabel, seperti terlihat pada tabel dibawah.

Tabel 3 Hasil Uji OWASP Top 10 2017

OWASP TOP 10	TOOLS	KERENTANAN	JUMLAH KERENTANAN
A1-Injection	Acunetix	Tidak Rentan	0
A2-Broken Authentication	Acunetix	Rentan	2
A3-Sensitive Data Exposure	Acunetix	Rentan	9
A4-XML External Entities (XXE)	Acunetix	Tidak Rentan	-
A5-Broken Access Control	Acunetix	Rentan	2
A6-Security	Acunetix	Rentan	6

Misconfiguration			
A7-Cross-Site Scripting (XSS)	Acunetix	Tidak Rentan	0
A8-Insecure Deserialization	Acunetix	Tidak Rentan	0
A9-Using Components with Known Vulnerabilities	Acunetix	Rentan	6
A10-Insufficient Logging & Monitoring	Acunetix	Tidak Rentan	0

Berdasarkan tabel 4.16 hasil pengujian penetrasi dengan ketentuan OWASP Top 10 2017 pada domain website server mail.umkt.sch.id dengan menggunakan *tools Acunetix* terdapat kerentanan di *A3-Sensitive Data Exposure, A5-Broken Access Control, A6-Security Misconfiguration* dan *A9-Using Components with Known Vulnerabilities.*

4.3 Analisis dan Laporan hasil Uji Penetrasi

Pada tahapan ini dilakukan Analisis dan Laporan dalam pengujian penetrasi, dalam bentuk saran ataupun rekomendasi perbaikan website untuk meminimalisir kerentanan yang dihasilkan dalam pengujian sebelumnya. Pada dasarnya ancaman pada website yang terjadi pada tahun 2017 sudah didata oleh OWASP (Open Web Application Security Project) dan sudah tercatat pada OWASP Top 10 Security – 2017. Pada OWASP Top 10 Security, terdapat beberapa ancaman dan tingkat resiko dari dampak serangan yang telah diklasifikasikan oleh OWASP. Tingkat ancaman yang diberi nilai sudah dihitung dengan kalkulator khusus dari NIST (National Institute of Standards and Technology) yang disebut CVSS (Common Vunlnerability Scoring System) dengan rentang score 0.0 sampai 10.0. Dari penilaian kerentanan ini akan dijadikan acuan seberapa parah kerentanan yang dialami. Berikut table dari analisis hasil pengujian beserta saran/rekomendasi yang dibuat beserta tingkat ancaman yang terjadi.

Clickjacking: X-Frame-Options header missing		**Solusi**
Affected item	Web Server	Menambahkan header "X-Frame-Options" pada respons server.
CVSS2	Base Score: 4.3 (medium) Access Vector: Network_accessible Access Complexity: Medium Integrity Impact: Partial	
CWE	CWE-693	
Cookie(s) without HttpOnly flag set (verified)		**Solusi**
Affected item	Web Server	Mengatur flag HttpOnly pada cookie yang dikirimkan oleh server
CVSS2	Base Score: 0.0 (None) Access Vector: Network_accessible Access Complexity: Low	
CWE	CWE-16	
Cookie(s) without Secure flag set (verified)		**Solusi**
Affected item	Web Server	Mengatur flag Secure pada cookie yang dikirimkan oleh server.
CVSS2	Base Score: 0.0 (none) Access Vector: Network_accessible Access Complexity: Low	
CWE	CWE-16	
Documentation file (verified)		**Solusi**
Affected item	/plugins/demo/README	Menghapus/membatasi akses publik terhadap file dokumentasi yang ditemukan
CVSS2	Base Score: 5.0 (medium) Access Vector: Network_accessible Access Complexity: Low Confidentiality Impact: Partial	

CWE	CWE-538	
Login page password-guessing attack		**Solusi**
Affected item	/src/redirect.php	Menerapakan mekanisme pembatasan percobaan login, Menggunakan metode verifikasi Captcha untuk memastikan bahwa manusia, bukan bot otomatis, yang mencoba melakukan login.
CVSS2	Base Score: 5.0 (Medium) Access Vector: Network_accessible Access Complexity: Low Confidentiality Impact: Partial	
CVSS3	Base Score: 5.3 (medium) Attack Vector: Network Attack Complexity: Low Scope: Unchanged Availability Impact: Low	
CWE	CWE-307	
Possible sensitive files		**Solusi**
Affected item	/plugins/test/test.php	Menerapkan proteksi tambahan seperti *firewall*, *IDS (Intrusion Detection System)*, atau *IPS (Intrusion Prevention System)* untuk melindungi file sensitif dari serangan atau akses yang tidak sah.
CVSS2	Base Score: 5.0 (medium) Access Vector: Network_accessible Access Complexity: Low Confidentiality Impact: Partial	
CVSS3	Base Score: 7.5 (High) Attack Vector: Network Attack Complexity: Low Scope: Unchanged Confidentiality Impact: High	
CWE	CWE-200	
Unencrypted connection (verified)		**Solusi**
Affected item	WebServer	Menggunakan protokol enkripsi yang aman seperti HTTPS
CVSS2	Base Score: 5.8 (medium) Access Vector: Network_accessible Access Complexity: Medium Confidentiality Impact: Partial Integrity Impact: Partial	
CVSS3	Base Score: 9.1 (critical) Attack Vector: Network Attack Complexity: Low Scope: Unchanged Confidentiality Impact: High Integrity Impact: High	
CWE	CWE-310	
Content Security Policy (CSP) not implemented		**Solusi**
Affected item	WebServer	Menerapkan dan mengkonfigurasi CSP di server web
CVSS2	Base Score: 0.0 (None) Access Vector: Network_accessible Access Complexity: Low	
CWE	CWE-16	
Content type is not specified (verified)		**Solusi**
Affected item	/plugins/demo/README	Gunakan header "Content-Type" dalam respons server dengan nilai yang sesuai untuk tipe konten yang dikirimkan.
CVSS2	Base Score: 0.0 (None) Access Vector: Network_accessible Access Complexity: Low	
CWE	CWE-16	
Error page web server version disclosure		**Solusi**

Affected item	WebServer	Hapus informasi versi dari pesan error. Gunakan Web Application Firewall (WAF) yang dapat mendeteksi dan mencegah serangan yang berhubungan dengan pengungkapan versi server web.
CVSS2	Base Score: 5.0 (medium) Access Vector: Network_accessible Access Complexity: Low Confidentiality Impact: Partial	
CVSS3	Base Score: 0.0 (none) Attack Vector: Network Attack Complexity: Low Scope: Unchanged	
CWE	CWE-200	
Password type input with auto-complete enabled		**Solusi**
Affected item	WebServer	Menonaktifkan fitur "auto-complete" pada browser mereka secara manual
CVSS2	Base Score: 0.0 (none) Access Vector: Network_accessible Access Complexity: Low	
CVSS3	Base Score: 7.5 (High) Attack Vector: Network Attack Complexity: Low Scope: Unchanged Confidentiality Impact: High	
CWE	CWE-200	
Parameter	login_form	

5. Simpulan

Berdasarkan pengujian penetrasi testing pada website mail server dapat di simpulkan pengujian menggunakan OWASP ZAP menunjukkan bahwa website server local yang berdomain mail.umkt.sch.id memiliki 9 kerentanan yaitu, Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, Cookie No HttpOnly Flag, Cookie without SameSite Attribute, Server Leaks Version Information via "Server" HTTP Response Header Field, X-Content-Type-Options Header Missing, GET for POST, Modern Web Application, User Agent Fuzzer dengan dan berdasarkan pengujian penetrasi dengan menggunakan tools Acunetix dengan ketentuan OWASP TOP 10 2017 terdeteksi 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. Berdasarkan kesimpulan di atas maka saran dari penelitian ini adalah perlu dilakukan penelitian dengan menggunakan metode Information System Security Assessment Framework (ISSAF) agar dapat diketahui kerentanan apa saja secara mendalam pada web server.

Daftar Referensi

[1] Bagus Ramadhan, “Data Internet di Indonesia dan Perilakunya,” *TEKNOIA—Inspirasimu untuk Berinovasi*, 2020. https://teknoia.com/data-internet-di-indonesia-dan-perilakunya-880c7bc7cd19

[2] A. Dharmawan, Y. Prihati, and H. Listijo, “Penetration Testing Menggunakan Owasp Top 10 Pada Domain Xyz. Ac. Id,” *Electro Luceat*, vol. 8, no. 1, 2022, [Online]. Available: https://jurnal.poltekstpaul.ac.id/index.php/jelekn/article/view/455%0Ahttps://jurnal.poltekstpaul.ac.id/index.php/jelekn/article/download/455/328

[3] D. Sumarto and R. Yuliani, “Rancang Bangun Mail Server Berbasis Squirrelmail Menggunakan Mta (Mail Transfer Agent) Pada Pt. Teras Inti Media,” *J. Prosisko*, vol. 4, no. 2, pp. 55–59, 2017, [Online]. Available: https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/392

[4] G. Hendita, A. Kusuma, P. T. Informatika, F. Teknik, U. Pancasila, and J. Selatan, “IMPLEMENTASI OWASP ZAP UNTUK PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK,” vol. 16, no. 2, pp. 178–186, 2022.

[5] B. Ghozali, M. Teknik, I. Universitas, and A. Yogyakarta, “Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating,” pp. 264–275, 2018.

[6] M. T. Hidayat, F. M. Sn, and N. I. Kurniati, “Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Gratis Terhadap Serangan Packet Sniffing,” vol. 1, no. 2, pp. 112–119, 2018.

[7] N. Rumaf, K. Anwar, and D. S. Utsalina, “Analisis Keamanan Web Server Terhadap Website Pt. Victory Internasional Futures Malang Dengan Teknik Sql Injection,” *Din. Dotcom J.* …, vol. 13, pp. 73–83, 2022, [Online]. Available: http://ejurnal.stimata.ac.id/index.php?journal=DINAMIKA&page=article&op=view&path%5B%5D=437

[8] F. Fachri, A. Fadlil, and I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.

[9] B. Basorudin, “Implementasi Mail Server Berbasis Squirrelmail Dengan Exchange Server Menggunakan Teknologi Virtualisasi di SMK Negeri 1 Pendalian IV Koto,” *J. Media Infotama*, vol. 14, no. 2, pp. 51–57, 2018, doi: 10.37676/jmi.v14i2.651.

[10] T. Farida, “Pengembangan Media Pembelajaran Virtual Box Untuk Mengukur Kelayakan Modul Pada Mata Pelajaran Komputer Dan Jaringan Dasar Di Smkn 7 Surabaya,” *J. It-Edu*, vol. 4, no. 01, pp. 68–75, 2019.

[11] L. Johnson, “System and network assessments,” *Secur. Control. Eval. Testing, Assess. Handb.*, pp. 447–469, 2020, doi: 10.1016/b978-0-12-818427-1.00010-0.

[12] G. Guntoro, L. Costaner, and M. Musfawati, “Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning),” *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.

[13] A. Zirwan, “Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner,” *J. Inf. dan Teknol.*, vol. 4, no. 1, pp. 70–75, 2022, doi: 10.37034/jidt.v4i1.190.

[14] M. Walkowski, J. Oko, and S. Sujecki, “Article vulnerability management models using a common vulnerability scoring system,” *Appl. Sci.*, vol. 11, no. 18, 2021, doi: 10.3390/app11188735.

[15] Y. Wu, Y. Yesha, and I. Bojanova, “They know your weaknesses - Do you?: Reintroducing Common Weakness Enumeration,” *CrossTalk*, vol. 29, no. 3, pp. 19–24, 2016.

[16] H. A. Juhad, R. R. Isnanto, E. D. Widianto, J. S. Komputer, F. Teknik, and U. Diponegoro, “Analisis Keamanan pada Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro,” vol. 4, no. 3, pp. 479–484, 2016, doi: 10.14710/jtsiskom.4.3.2016.479-484.

UMKT
UNIVERSITAS MUHAMMADIYAH
Kalimantan Timur

Kampus 1 : Jl. Ir. H. Juanda, No.15, Samarinda
Kampus 2 : Jl. Pelita, Pesona Mahakam, Samarinda
Telp. 0541-748511 Fax.0541-766832

بسم الله الرحمن الرحيم

SURAT KETERANGAN ARTIKEL PUBLIKASI

Assalamu'alaikum Warahmatullahi wabarakatuh

Saya yang bertanda tangan dibawah ini:

Nama	:	Faldi, S.Kom., M.Ti
NIDN	:	1121079101
Nama	:	Ali Zainal Abidin
NIM	:	1911102441087
Fakultas	:	Sains dan Teknologi
Progam Studi	:	S1 Teknik Informatika

Manyatakan bahwa artikel ilmiah yang berjudui "*Penetration Testing* Pada Wesite Mail Server Dengan Menggunakan Metode Owasp" telah di submit pada Jurnal Teknik Informatika dan Sistem Informasi STIMIK Banjarbaru.
http://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/user

Demikian surat keterangan ini dibuat untuk dapat dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Warahmatullahi wabarakatuh

Samarinda, Selasa 25 Juli 2023

Mahasiswa	Dosen Pembimbing
Ali Zainal Abidin	Faldi, S.Kom.,M.TI
NIM. 1911102441087	NIDN. 1121079101