BINA INSANI ICT JOURNAL
Vol. 13, No. 1, Juni 2026, 51 - 63
ISSN: 2355-3421 (Print) ISSN: 2527-9777 (Online)

Penerapan Metodologi *Penetration Testing Execution Standard* (PTES) dalam Analisis Keamanan Aplikasi *Management Employment System* (MES) Berdasarkan OWASP Top 10

Aryadi Nugroho[1], Ishak Kholil[1], Ani Oktarini Sari[2,*]

[1]Sistem Informasi; Universitas Nusa Mandiri; Jl. Raya Jatiwaringin No.2, RT.8/RW.13, Cipinang Melayu, Kec. Makasar, Jakarta Timur 13620, 02128534471; e-mail: aryadi.nugroho@gmail.com.
[1]Sistem Informasi; Universitas Nusa Mandiri; Jl. Raya Jatiwaringin No.2, RT.8/RW.13, Cipinang Melayu, Kec. Makasar, Jakarta Timur 13620, 02128534471; e-mail: ishak.ihk@nusamandiri.ac.id.
[2]Sains Data; Universitas Nusa Mandiri; Jl. Raya Jatiwaringin No.2, RT.8/RW.13, Cipinang Melayu, Kec. Makasar, Jakarta Timur 13620, 02128534471; e-mail: ani.aos@nusamandiri.ac.id.

* Korespondensi: e-mail: ani.aos@nusamandiri.ac.id.

Diterima: 27 Mei 2026 ; Review: 02 Juni 2026; Disetujui: 29 Juni 2026

Cara sitasi: Nugroho, Aryadi, Kholil, Ishak, Sari, Ani Oktarini. 2026. Penerapan Metodologi Penetration Testing Execution Standard (PTES) dalam Analisis Keamanan Aplikasi Manufacturing Execution System (MES) Berdasarkan OWASP Top 10. Bina Insani ICT Journal. Vol 13(1): 51 - 63.

Abstrak: Pengelolaan data karyawan yang dilakukan melalui aplikasi *Management Employment System* (MES) di PT Mindotama Avia Teknik menuntut penerapan keamanan informasi yang memadai mengingat data yang tersimpan bersifat sensitif dan memiliki nilai strategis bagi perusahaan. Kerentanan pada aplikasi web mudah ditemukan celah oleh pihak diluat perusahaan untuk memperoleh akses ilegal, melakukan pencurian informasi, maupun mengganggu operasional sistem. Oleh karena itu, evaluasi keamanan aplikasi menjadi langkah penting untuk mengidentifikasi potensi risiko yang dapat mengancam kerahasiaan, integritas, dan ketersediaan data. Penelitian ini bertujuan untuk melakukan analisis keamanan terhadap aplikasi MES menggunakan metodologi *Penetration Testing Execution Standard* (PTES) dengan mengacu pada OWASP Top 10 sebagai standar dalam identifikasi kerentanan aplikasi web. Tahapan penelitian meliputi *intelligence gathering, vulnerability analysis, exploitation, dan reporting*. Pada proses pengujian digunakan berbagai perangkat keamanan, seperti *Burp Suite, Nmap, Nuclei, Acunetix, dan FFUF*, untuk mendukung proses identifikasi serta validasi kerentanan yang ditemukan pada sistem. Hasil pengujian menunjukkan bahwa aplikasi MES masih memiliki beberapa kelemahan keamanan yang berpotensi dieksploitasi oleh penyerang. Kerentanan *Cross-Site Scripting* (XSS) memperoleh skor 7,6 dan dikategorikan sebagai risiko tinggi. Selain itu, ditemukan kerentanan *Exposure PhpMyAdmin* dan *Improper Input Validation* yang masing-masing memperoleh skor 5,9 dengan tingkat risiko sedang. Kerentanan lainnya berupa kesalahan konfigurasi security header memperoleh skor 3,5 dan termasuk dalam kategori risiko rendah. Temuan tersebut menunjukkan adanya potensi ancaman berupa kebocoran data, manipulasi informasi, hingga akses tidak sah terhadap sumber daya sistem. Berdasarkan hasil analisis yang dilakukan, direkomendasikan penerapan kontrol keamanan yang lebih komprehensif melalui penguatan mekanisme validasi masukan, optimalisasi konfigurasi security header, pembatasan akses terhadap komponen dan endpoint yang bersifat sensitif, serta peningkatan mekanisme autentikasi. Implementasi rekomendasi tersebut diharapkan mampu meningkatkan tingkat keamanan aplikasi MES dan meminimalkan risiko serangan siber terhadap sistem informasi perusahaan.

Kata kunci: *Penetration Testing*, PTES, OWASP Top 10, Keamanan Aplikasi Web, Management Employment System (MES).

Abstract: *The management of employee data conducted through the Management Employment System (MES) application at PT Mindotama Avia Teknik requires the implementation of adequate information security, considering that the stored data is sensitive and holds strategic value for the company. Vulnerabilities in the web application can be exploited by unauthorized parties to gain illegal access, commit information theft, or disrupt system operations. Therefore, evaluating the security of the application is an important step to identify potential risks that could threaten the confidentiality, integrity, and availability of the data. This study aims to perform a security analysis of the MES application using the Penetration Testing Execution Standard (PTES) methodology, referring to the OWASP Top 10 as a benchmark for identifying web application vulnerabilities. The research phases include intelligence gathering, vulnerability analysis, exploitation, and reporting. During the testing process, various security tools, such as Burp Suite, Nmap, Nuclei, Acunetix, and FFUF, were employed to support the identification and validation of vulnerabilities found within the system. The test results indicate that the MES application still possesses several security weaknesses that could potentially be exploited by attackers. Cross-Site Scripting (XSS) vulnerabilities received a score of 7.6 and are classified as high risk. Additionally, vulnerabilities related to PhpMyAdmin Exposure and Improper Input Validation were identified, each scoring 5.9 with a medium risk level. Another vulnerability, in the form of a security header misconfiguration, received a score of 3.5 and is classified as low risk. This finding indicates potential threats such as data leakage, information manipulation, and unauthorized access to system resources. Based on the conducted analysis, it is recommended to implement more comprehensive security controls by strengthening input validation mechanisms, optimizing security header configurations, restricting access to sensitive components and endpoints, and enhancing authentication mechanisms. Implementing these recommendations is expected to improve the security of the MES application and minimize the risk of cyberattacks on the company's information systems.*

Keywords*: Penetration Testing, PTES, OWASP Top 10, Web Application Security, Management Employment System (MES).*

1. Pendahuluan

Perkembangan teknologi informasi saat ini telah membawa banyak perubahan signifikan diperusahaan dalam mengelola informasi dan menjalankan proses bisnis. Salah satu bentuk implementasinya adalah penggunaan sistem berbasis web yang berfungsi untuk mendukung aktivitas operasional serta meningkatkan efektivitas pengelolaan data[1]. Manajemen sumber daya manusia (SDM) merupakan salah satu komponen strategis yang memiliki peran penting dalam keberlangsungan operasional bisnis maupun organisasi. Perkembangan pengelolaan data karyawan memberikan berbagai manfaat signifikan, di antaranya mendukung proses pengambilan keputusan yang lebih efektif, meningkatkan produktivitas kerja, serta mengoptimalkan efisiensi biaya operasional organisasi [2].

Salah satu bentuk penggunaan teknologi dibidang manajemen sumberdaya manusia ut adalah penggunaan aplikasi *Management Employment System* (MES). PT Mindotama Avia Teknik menggunakan aplikasi tersebut untuk mengelola data karyawan, administrasi kepegawaian, serta informasi penting perusahaan secara terintegrasi. Meskipun sistem berbasis web mampu memberikan kemudahan akses informasi dan meningkatkan efisiensi operasional perusahaan, keberadaannya juga membuka peluang munculnya berbagai kerentanan keamanan. Kerentanan tersebut mudah ditemukan oleh pihak yang tidak berwenang untuk mengganggu kerahasiaan, integritas, maupun ketersediaan data yang tersimpan dalam sistem[3].

Kerentanan keamanan pada website mudah ditemukan oleh pihak yang tidak berwenang untuk memperoleh akses secara tidak sah, mengekstraksi informasi yang bersifat sensitif, melakukan manipulasi terhadap data, serta mengganggu ketersediaan layanan sistem. Kondisi tersebut menunjukkan bahwa keberadaan celah keamanan pada aplikasi web dapat menimbulkan risiko yang signifikan terhadap aspek kerahasiaan, integritas, dan ketersediaan informasi [4]. Kerentanan tersebut sering menjadi sasaran berbagai bentuk serangan siber, seperti *SQL Injection, Cross-Site Scripting (XSS), brute force attack, serta Distributed Denial of*

Service (DDoS), yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan sistem [5]. Server aplikasi web yang memiliki tingkat kerentanan tinggi merupakan aplikasi berbasis PHP/MySQL yang dirancang secara khusus untuk tujuan pembelajaran dalam memahami teknik eksploitasi serta metode serangan terhadap server web[6][7].

Metode yang sering digunakan dalam proses evaluasi sistem keamanan berbasis web adalah *Penetration Testing Execution Standard* (PTES)[8]. Metode ini menyediakan tahapan pengujian yang sistematis mulai dari *intelligence gathering, vulnerability analysis, exploitation, hingga reporting*. Metode ini dilakukan melalui simulasi serangan secara terkontrol terhadap sistem dengan tujuan untuk mengidentifikasi kerentanan keamanan yang terdapat pada aplikasi, sekaligus mengevaluasi tingkat ketahanan sistem dalam menghadapi potensi ancaman, baik yang bersumber dari pihak eksternal maupun internal[9]. Penelitian terkait telah dilakukan untuk mengevaluasi keamanan portal web Dinas Sosial Kota Surabaya menggunakan metode penetration testing dengan pendekatan OWASP Top 10 sebagai acuan identifikasi kerentanan. Tahapan pengujian meliputi information gathering, footprinting and scanning, vulnerability assessment, exploitation, serta analyze and report. Berdasarkan hasil pengujian, ditemukan enam jenis kerentanan utama yang berpotensi dimanfaatkan oleh pihak yang tidak berwenang, yaitu *Browsable Web Directories, Web.config File Information Disclosure, Content Security Policy (CSP) Header Not Set, Strict-Transport-Security Header Not Set, Timestamp Disclosure (Unix), dan X-Content-Type-Options Header Missing*. Keberadaan kerentanan tersebut menunjukkan bahwa masih diperlukan peningkatan konfigurasi keamanan dan penerapan kontrol proteksi yang lebih efektif untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi pada website yang diuji[10]. Penelitian terdahulu yang mengkaji keamanan website akademik perguruan tinggi menggunakan metode Penetration Testing Execution Standard (PTES) telah dilakukan melalui tahapan perencanaan dan pengumpulan informasi, analisis kerentanan, eksploitasi, serta pelaporan hasil pengujian. Hasil penelitian menunjukkan adanya beberapa kerentanan keamanan, seperti direktori yang terbuka untuk akses publik dan potensi serangan clickjacking. Untuk mengurangi risiko tersebut, direkomendasikan penerapan security header serta optimalisasi konfigurasi server. Berdasarkan tingkat keparahan kerentanan yang teridentifikasi, sebanyak 68% termasuk kategori low, 18% kategori medium, 3% kategori high, dan 8% kategori critical, sehingga diperlukan upaya mitigasi yang berfokus pada kerentanan dengan tingkat risiko tertinggi[11].

Evaluasi keamanan dalam penelitian ini menggunakan pedoman yang ditetapkan oleh *Open Web Application Security Project* (OWASP) sebagai kerangka acuan dalam mengidentifikasi dan menganalisis kerentanan sistem.[12]. Dengan memanfaatkan dokumen OWASP Top 10 2021 sebagai tolak ukur, proses identifikasi kerentanan difokuskan pada sepuluh kategori ancaman siber paling berisiko. Kerentanan seperti *Cryptographic Failures, Injection, serta Broken Access Control* dianalisis secara mendalam karena berpotensi merusak integritas, melemahkan kerahasiaan, dan mengganggu ketersediaan layanan sistem informasi[13].

Pengujian keamanan terhadap aplikasi MES di PT Mindotama Avia Teknik menjadi penting karena sistem tersebut menyimpan data sensitif karyawan dan informasi internal perusahaan. Pengujian sistem dilakukan pada beberapa fitur utama untuk memastikan aspek fungsionalitas dan keamanan aplikasi berjalan dengan baik. Pengujian form login difokuskan ketahanan terhadap serangan seperti *SQL Injection, Cross-Site Scripting* (XSS), dan *brute force*. Pada form izin kantor, pengujian mencakup validasi input, serta keamanan terhadap SQL Injection dan XSS. Selanjutnya, pengujian menu Approval dilakukan untuk memastikan keamanan data terhadap *SQL Injection, XSS, dan CSRF,* serta keamanan komunikasi data. Pengujian menu Configuration berfokus pada validasi input, pengaturan hak akses, dan keamanan endpoint dari potensi eksploitasi. Sementara itu, pengujian menu Website Product bertujuan mengidentifikasi potensi ancaman pada fitur CRUD dengan memastikan validasi input dan keamanan unggahan data dari serangan *SQL Injection* maupun XSS.

Penggunaan metodologi PTES dengan standar OWASP Top 10 akan memastikan bahwa proses pengujian keamanan ini tidak hanya mengidentifikasi kerentanan, tetapi juga memberikan panduan spesifik untuk perbaikan yang dibutuhkan. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan tingkat keamanan sistem melalui identifikasi, analisis, dan rekomendasi mitigasi terhadap kerentanan yang ditemukan[14] pada aplikasi MES di PT Mindotama Avia Tehnik.

2. Metode Penelitian

Metodologi yang digunakan dalam penelitian ini adalah *Penetration Testing Execution Standard* (PTES), yang menyediakan panduan langkah-langkah pengujian keamanan mulai dari perencanaan, pengujian, hingga pelaporan. PTES memberikan pendekatan yang terstruktur dan menyeluruh untuk melakukan evaluasi keamanan aplikasi, yang akan memungkinkan identifikasi kerentanan dengan tingkat ketelitian yang tinggi. Dalam pengujian ini, pendekatan OWASP Top 10 [15] digunakan sebagai standar untuk mendeteksi dan memitigasi risiko keamanan yang paling umum pada aplikasi web.
PTES terdiri dari tujuh tahapan utama yang mencakup seluruh proses uji penetrasi dari perencanaan hingga pelaporan hasil dapat dilihat pada gambar 1.

Sumber:Hasil Penelitian (2025)

Gambar 1: Tahapan PTES

Penjelasan Tahapan PTES pada gambar 1 adalah sebagai berikut :

a. ***Pre-Engagement Interactions*** : Langkah ini merupakan gambaran komunikasi antara peneliti sebagai tim penetration testing dan PT Mindotama Avia Teknik sebagai klien untuk memahami hasil uji, jangkauan, batasan, dan ekspektasi hasil.
b. ***Information Gathering*** dilakukan untuk mengumpulkan informasi tentang target sistem guna memahami struktur, konfigurasi, dan potensi kelemahan. Metode pasif seperti WHOIS, DNS enumeration, OSINT, dan Shodan digunakan untuk memperoleh data tanpa interaksi langsung, sementara metode aktif seperti port scanning, service versioning, OS fingerprinting, banner grabbing, dan vulnerability scanning menggunakan alat seperti Nmap dan Nessus.
c. ***Threat Modeling*** dilakukan untuk menganalisis ancaman yang mungkin dihadapi oleh sistem target dengan mengevaluasi kerentanan dan menentukan prioritas pengujian. Proses ini mencakup identifikasi aset bernilai tinggi seperti data sensitif atau server kritis, analisis ancaman dari penyerang eksternal, orang dalam, atau malware, serta evaluasi kerentanan yang ditemukan menggunakan framework seperti CVSS.
d. ***Vulnerability Analysis*** merupakan proses identifikasi, analisis, dan prioritisasi kerentanan dalam sistem target. Pengujian dilakukan dengan pemindaian kerentanan menggunakan alat seperti Nessus, OpenVAS, dan QualysGuard, serta analisis manual terhadap konfigurasi keamanan dan validasi input aplikasi web.
e. ***Exploitation*** adalah tahap di mana penguji memanfaatkan kerentanan yang telah diidentifikasi untuk mendapatkan akses tidak sah atau menyebabkan dampak tertentu seperti pengungkapan data, eskalasi hak akses, atau gangguan layanan. Proses ini dimulai dengan perencanaan eksploitasi untuk memilih teknik atau alat yang tepat, diikuti dengan pelaksanaan metode serangan seperti SQL Injection, Buffer Overflow, Privilege Escalation, Cross-Site Scripting (XSS), atau Remote Code Execution (RCE).
f. ***Post-Exploitation*** berfokus pada evaluasi dampak eksploitasi dan potensi penyalahgunaan akses yang telah diperoleh. Penguji menilai sejauh mana akses tersebut dapat memengaruhi operasi, data, dan keamanan organisasi, serta mengeksplorasi risiko lanjutan seperti mempertahankan akses jangka panjang, mencuri data, atau menyerang sistem lain yang terhubung.
g. ***Reporting*** merupakan langkah terakhir dalam PTES, di mana penguji menyusun laporan komprehensif yang merangkum temuan, eksploitasi, dan rekomendasi mitigasi berdasarkan hasil pengujian [16].

Untuk mencapai tujuan penelitian, pelaksanaan penetration testing dilakukan melalui serangkaian tahapan yang sistematis sesuai dengan metodologi yang telah ditentukan.

Gambaran umum tahapan penelitian yang digunakan dalam penelitian ini dapat dilihat pada Gambar 2 :

Sumber:Hasil Penelitian (2025)

Gambar 2. Tahapan Penelitian

Penjelasan dari gambar 2 terkait roadmap tahapan penelitian dapat dilihat pada tabel 1

Tabel 1. Roadmap Penelitian

No	Tahapan	Aktivitas	Tools	Tujuan
1	*Pre-Engagement Interactions*	Penentuan lingkup (Scope)	Wawancara, zoom metting	Pastikan semua pihak memahami tujuan dan ruang lingkup pengujian.
2	*Reconnaissance*	Crawling Direktori	*Dirsearch, Ffuf*	Mengidentifikasi direktori maupun berkas yang bersifat tersembunyi atau sensitif pada server web yang berpotensi tidak dapat diakses maupun diketahui oleh pengguna umum.
3	*Scanning*	Melakukan pemindaian kerentanan secara otomatis dan analisis parameter aplikasi web untuk mengidentifikasi potensi celah keamanan pada sistem	*Acunetix, Nuclei*	Mengevaluasi parameter aplikasi melalui teknik pemindaian kerentanan guna menemukan kelemahan keamanan yang berpotensi mengancam integritas dan kerahasiaan sistem.
4	*Enumeration*	Mengidentifikasi endpoint sensitif serta menganalisis struktur URL dan parameter yang digunakan oleh aplikasi.	*Ffuf, Nmap*	Melakukan identifikasi terhadap endpoint sensitif serta menganalisis struktur URL dan parameter yang digunakan oleh aplikasi guna memahami alur komunikasi dan potensi risiko keamanan pada sistem.
5	*Exploitation*	Sql Injection, pengujian CrossSite Scripting XSS	*Burpsuite*	Melakukan pengujian terhadap kerentanan seperti SQL Injection dan Cross-Site Scripting (XSS) untuk memverifikasi

				keberadaan celah keamanan pada aplikasi.
6	*Post Exploitation*	Mengevaluasi akses yang diperoleh, mengekstraksi data sensitif.	*BurpSuite Manual Testing, SQL Map*	Melakukan evaluasi terhadap tingkat akses yang berhasil diperoleh serta mengidentifikasi informasi sensitif yang dapat diakses dari sistem.
7	*Reporting*	Menyusun laporan kerentanan secara komprehensif serta memberikan rekomendasi mitigasi untuk mengurangi risiko keamanan yang teridentifikasi.	*Manual*	Membuat laporan yang terstruktur dan menyeluruh mengenai hasil pengujian, termasuk usulan langkah-langkah mitigasi terhadap kerentanan yang ditemukan pada sistem..

Sumber:Hasil Penelitian (2025)

3. Hasil dan Pembahasan

Pengujian keamanan terhadap Aplikasi *Management Employment System* (MES) dilakukan dengan tujuan mampu mengidentifikasi potensi celah keamanan yang terdapat pada sistem. Proses pengujian tersebut dilaksanakan berdasarkan tahapan-tahapan yang telah ditetapkan sesuai dengan metodologi yang digunakan. Penjelasan tiap tahapan sebagai berikut :

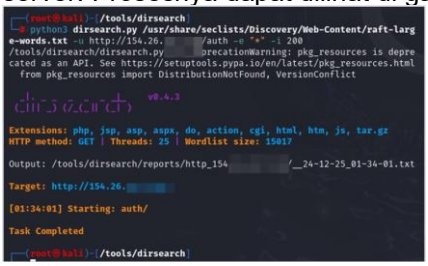
a. Pre-Engagement Interaction

Pada tahap ini dilakukan batasan ruang lingkup yang aka dilakukan pengujian terhadap aplikasi MES pada PT PT Mindotama Avia Teknik. Ruang lingkupnya adalah sebagai berikut : Pengujian form login difokuskan ketahanan terhadap serangan seperti *SQL Injection, Cross-Site Scripting* (XSS), dan *brute force*. Pada form izin kantor, pengujian mencakup validasi input, serta keamanan terhadap SQL Injection dan XSS. Selanjutnya, pengujian menu Approval dilakukan untuk memastikan keamanan data terhadap *SQL Injection, XSS, dan CSRF,* serta keamanan komunikasi data. Pengujian menu Configuration berfokus pada validasi input, pengaturan hak akses, dan keamanan endpoint dari potensi eksploitasi. Sementara itu, pengujian menu Website Product bertujuan mengidentifikasi potensi ancaman pada fitur CRUD dengan memastikan validasi input dan keamanan unggahan data dari serangan *SQL Injection* maupun XSS.

b. ***Pengintaian (Reconnaissance)*** Dalam tahapan ini penguji menggunakan dua tools ***Dirsearch*** dan ***Ffuf*** melakukan pengumpulan data sebanyak mungkin dan menggali informasi yang digunakan pada struktur aplikasi MES

1) ***Dirsearch*** peneliti mencoba mencari informasi direktori atau file yang dapat diakses berdasarkan wordlist pada domain http://154.26.xxx.xxx/auth.
*python3 dirsearch.py -u http://154.26.x.x/auth -e * -i 200 -w /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt*

Pengujian dilakukan dengan memanfaatkan wordlist raft-large-words.txt dari SecLists dan hanya menampilkan respons HTTP 200 (OK). Tujuan pengujian ini adalah mengidentifikasi direktori maupun file yang dapat diakses secara langsung sehingga dapat digunakan untuk memetakan struktur aplikasi web dan menemukan potensi paparan informasi pada server. Prosesnya dapat dilihat di gambar 3.



Sumber:Hasil Penelitian (2025)

Gambar 3. Pengujian Pencarian Direktori

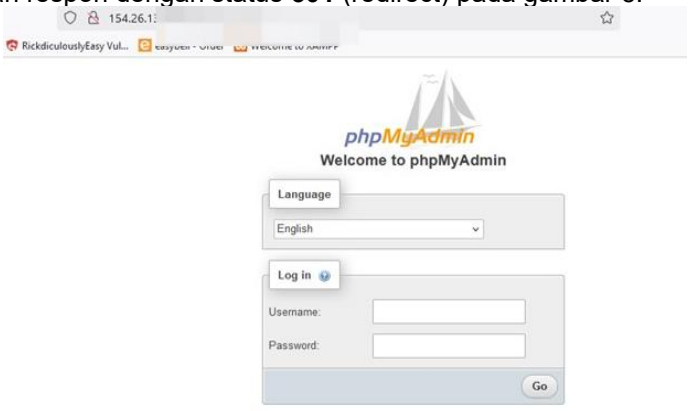
Hasil pengujian pada gambar 3 ***:*** menunjukkan bahwa target dapat diakses dan telah dilakukan pemetaan direktori file menggunakan wordlist meskipun tidak mendapatkan file direktori yang terbuka.

2) ***Fuzz Faster U Fool (Ffuf)*** untuk mencari informasi struktur aplikasi yang tidak ditampilkan secara langsung kepada pengguna, namun masih dapat diakses melalui permintaan HTTP pada domain http://154.26.xxx.xxx/auth
ffuf -u http://154.26.xxx.xxx/FUZZ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt 200,301,302.
Pada konfigurasi tersebut, parameter -u digunakan untuk menentukan alamat target yang akan diuji. Kata kunci **FUZZ** berfungsi sebagai penanda lokasi yang akan digantikan secara otomatis oleh setiap entri yang terdapat dalam *wordlist*. Dengan demikian, FFUF akan mengirimkan sejumlah permintaan HTTP ke berbagai kemungkinan direktori atau file berdasarkan daftar kata yang tersedia pada *wordlist*.
Parameter -w digunakan untuk menentukan *wordlist* yang dipakai dalam proses pengujian, yaitu raft-medium-words.txt yang berasal dari koleksi SecLists. *Wordlist* tersebut berisi berbagai nama direktori dan file yang umum ditemukan pada aplikasi web sehingga dapat meningkatkan efektivitas proses enumerasi. Selanjutnya, parameter -mc 200,301,302 (*match code*) digunakan untuk menampilkan hanya respons HTTP dengan kode status 200 (*OK*), 301 (*Moved Permanently*), dan 302 (*Found/Redirect*). Kode-kode tersebut dipilih karena umumnya menunjukkan bahwa sumber daya yang diuji benar-benar ada atau mengarahkan pengguna ke lokasi lain yang valid. Prosesnya dapat dilihat pada gambar 4.

Sumber:Hasil Penelitian (2025)

Gambar 4. Pencarian Direktori Dengan FFUF

Hasil Pengujian pada gambar 4 ***:*** menemukan kerentanan ***Exposure PhpMyadmin.*** Berdasarkan hasil pengujian menggunakan tool **ffuf** untuk melakukan enumerasi direktori, peneliti menemukan adanya endpoint **/phpmyadmin** yang aktif dan memberikan respon dengan status **301** (redirect) pada gambar 5.



Sumber:Hasil Penelitian (2025)

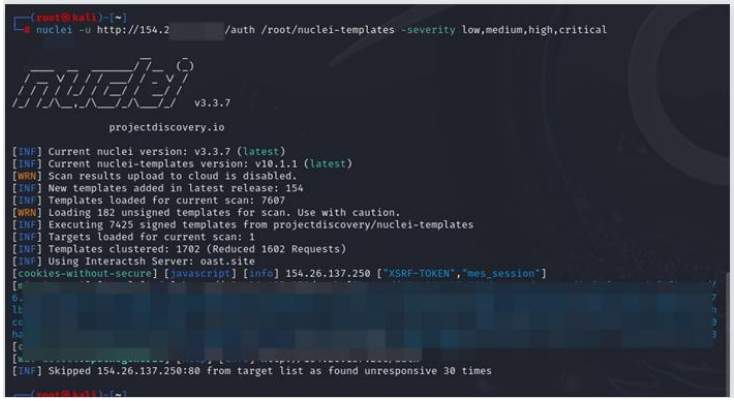
Gambar 5. Temuan Exposure PhpMyAdmin

c. *Scanning*

Nuclei untuk melakukan proses scanning dengan tujuan mencari dan mengidentifikasi informasi yang relevan.

nuclei -u http://154.26.xxx.xxx/auth /root/nuclei-templates -severity low,medium,high,critical

Pada perintah tersebut, parameter -u digunakan untuk menentukan target pemindaian, yaitu aplikasi web yang berada pada alamat http://154.26.xxx.xxx/auth. Selanjutnya, parameter -t digunakan untuk menentukan lokasi direktori *template* Nuclei yang akan digunakan selama proses pemindaian. Direktori nuclei-templates berisi kumpulan aturan pengujian yang telah disusun berdasarkan berbagai jenis kerentanan, konfigurasi sistem, teknologi web, hingga kelemahan yang telah diketahui sebelumnya (*known vulnerabilities*). Parameter -severity low,medium,high,critical digunakan untuk membatasi hasil pemindaian berdasarkan tingkat keparahan kerentanan. Tingkat keparahan tersebut mengacu pada klasifikasi risiko yang umum digunakan dalam pengujian keamanan informasi, yaitu **Low**, **Medium**, **High**, dan **Critical**. Kerentanan dengan tingkat *Low* umumnya memiliki dampak yang relatif kecil terhadap sistem, sedangkan kategori *Critical* menunjukkan kelemahan yang berpotensi memberikan dampak serius terhadap kerahasiaan, integritas, maupun ketersediaan sistem apabila berhasil dieksploitasi. Prosesnya dapat dilihat pada gambar 6.



Sumber:Hasil Penelitian (2025)

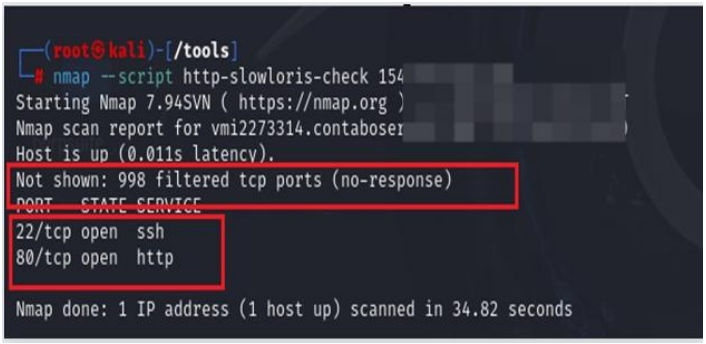
Gambar 6. Scanning Tools Nuclei

Hasil pengujian pada gambar 6 : pada pegujian ini tidak menemukan tingkat severity dari (low,medium,high,critical) hanya terdeteksi severity info

d. *Enumeration*

Network Mapper (Nmap) untuk melakukan proses enumeration dengan skrip **http-slowloris-check** untuk mengidentifikasi potensi kerentanan terhadap serangan **Slowloris** pada server yang menjadi objek penelitian. Slowloris merupakan salah satu jenis serangan **Denial of Service (DoS)** yang menargetkan layanan web dengan cara mempertahankan sejumlah besar koneksi HTTP dalam keadaan terbuka selama mungkin. Akibatnya, sumber daya server dapat habis digunakan untuk melayani koneksi tersebut sehingga pengguna yang sah mengalami kesulitan atau bahkan tidak dapat mengakses layanan yang tersedia. Prosesnya dapat dilihat pada gambar 7.

nmap --script http-slowloris-check 154.26.xxx.xxx



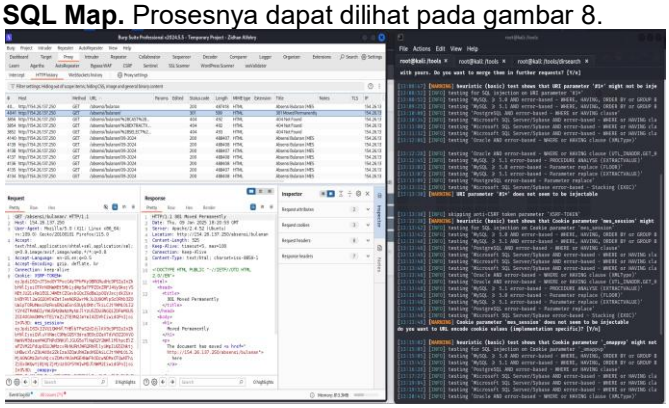
Sumber:Hasil Penelitian (2025)

Gambar 7. SlowLoris

Hasil Pengujian pada gambar 7 : Menunjukkan bahwa server memiliki dua port terbuka, yaitu port 22/tcp untuk layanan SSH dan port 80/tcp untuk layanan HTTP, sementara 998 port lainnya dalam status "filtered" (tidak merespons). Skrip Slowloris Nmap memindai layanan HTTP pada port 80, namun tidak memberikan indikasi eksplisit mengenai kerentanan terhadap serangan Slowloris. Proses pengujian selesai dalam waktu 34,82 detik, Pengujian ini hanya mengidentifikasi layanan yang berjalan pada server (HTTP dan SSH), tetapi tidak menunjukkan apakah server benar-benar rentan terhadap serangan Slowloris.

e. Post Exploitation

1) Pengujian Pada tahap ini, peneliti memanfaatkan kerentanan yang telah ditemukan selama proses pengujian manual menggunakan **Burp Suite** dan pengujian otomatis menggunakan **SQL Map.** Prosesnya dapat dilihat pada gambar 8.

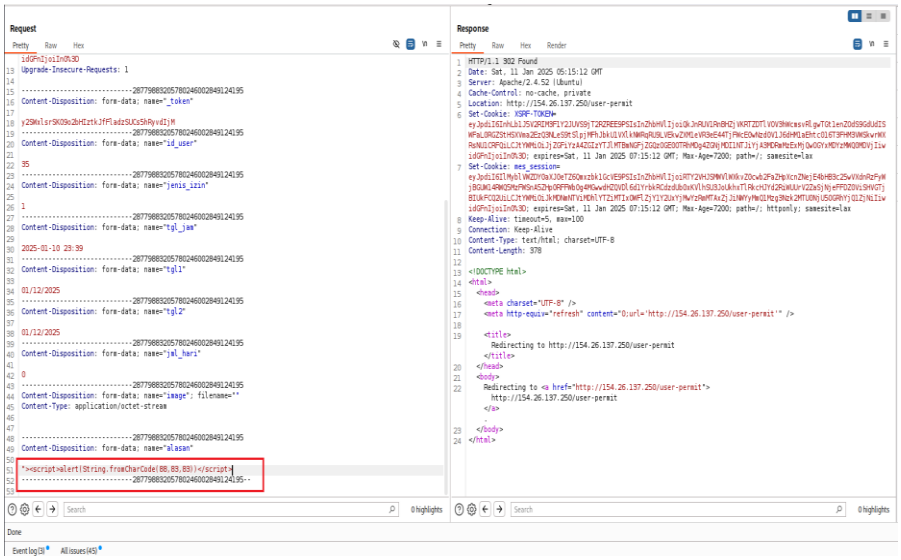


Sumber:Hasil Penelitian (2025)

Gambar 8. Pengujian dengan sqlmap

Hasil pada gambar 8 menunjukkan bahwa sistem telah mempunyai validasi input yang cukup baik, meskipun tetap disarankan untuk memperkuat keamanan melalui sanitasi parameter dan perlindungan tambahan terhadap manipulasi header atau cookie.

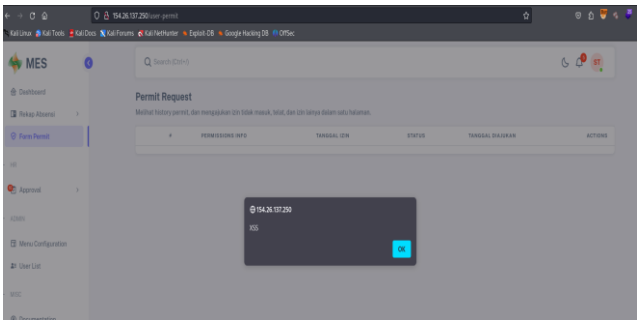
2) Pengujian Form Permit : menggunakan Burp Suite untuk menganalisis parameter input yang dikirim saat pengguna mengisi formulir. Dengan fitur proxy, request HTTP diintersepsi untuk mengidentifikasi parameter seperti periode izin, alasan, dan jenis izin dapat dilihat di gambar 9.



Sumber:Hasil Penelitian (2025)

Gambar 9. Proses Request

3) Selanjutnya, request dianalisis untuk mendeteksi potensi kerentanan, seperti SQL Injection atau XSS, dengan memanipulasi input menggunakan script *<script>alert(String.fromCharCode(88,83,83))</script>*



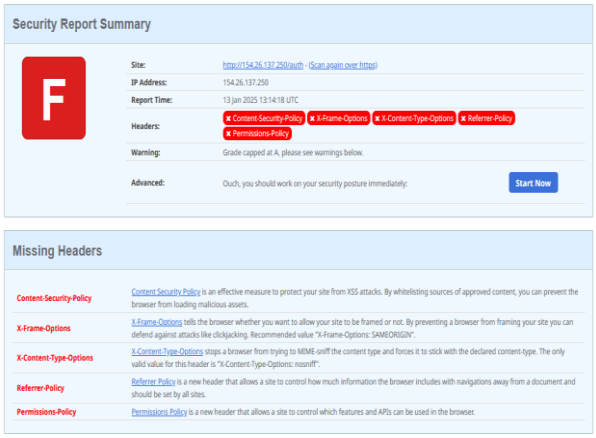
Sumber:Hasil Penelitian (2025)

Gambar 10. *Cross Site Scripting* (XSS)

Hasil Pengujian pada gambar 10: Berhasil menemukan kerentanan ***Cross-Site Scripting* (XSS)** melalui field "Alasan". Peneliti memasukkan payload berisi kode JavaScript.

f. Pengujian *Security Header*

Dilakukan untuk mengevaluasi penerapan header keamanan pada server web yang berfungsi melindungi aplikasi dari berbagai ancaman, seperti XSS (*Cross-Site Scripting*), *click jacking*.



Sumber:Hasil Penelitian (2025)

Gambar 11. *Miss Config Security Header*

Hasil Pengujian pada gambar 11 **:** Menunjukkan bahwa aplikasi tidak memiliki beberapa header keamanan yang penting, *seperti Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, dan Permissions-Policy.* Hal ini mengindikasikan bahwa server tidak memberikan perlindungan memadai terhadap ancaman keamanan tertentu.

g. Reporting

Bertujuan untuk menyusun dokumentasi hasil pengujian penetrasi secara menyeluruh dan jelas, sehingga dapat dipahami oleh tim teknis maupun non-teknis. Proses ini mencakup penyusunan laporan teknis yang memuat detail temuan kerentanan, bukti eksploitasi, dan dampaknya, serta rekomendasi mitigasi. Berikut ringkasan hasil pengujian analisa keamanan pada aplikasi MES. Bentuk Laporan yang dibuat dapat di lihat pada tabel 2 dan contoh detail dari hasil ringkasan dapat dilihat pada tabel 3.

Tabel 2. Ringkasan Temuan

No.	Nama Temuan	Object	Severity	Status
1	Cross-Site Scripting (XSS)	http://154.26.137.250/user-permit	High	Open
2	Exposure PhpMyadmin	http://154.26.137.250/phpmyadmin/	Medium	Open
3	Improper Input Validation	http://154.26.137.250/menu http://154.26.137.250/new-jabatan	Medium	Open
4	Miss Config Security Header	http://154.26.137.250/	Low	Open

Sumber:Hasil Penelitian (2025)

Tabel 3. *Miss Config Security Header*

Miss Config Security Header	
Severity	Low
CVSS Score 3.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N 
Deskripsi	*Header* keamanan yang salah dikonfigurasi pada aplikasi *web* dapat menyebabkan berbagai masalah keamanan. Header ini digunakan oleh aplikasi *web* untuk memberi instruksi kepada *browser* tentang bagaimana mengelola konten yang dikirimkannya. Konfigurasi yang salah atau ketiadaan *header* keamanan yang penting dapat meninggalkan aplikasi rentan terhadap serangan.
Affected URL	http://154.26.137.250/
Dampak	Beberapa masalah dengan kurangnya header keamanan adalah sebagai berikut: 1. Kurangnya content-security-policy header respons meningkatkan risiko serangan injeksi konten. 2. Kurangnya x-frame-options header respons bisa berpotensi memungkinkan serangan clickjacking. 3. Kurangnya x-content-type-options header respons mengurangi perlindungan terhadap serangan unduhan. 4. Kurangnya strict-transport-security header respons bisa meningkatkan risiko serangan jaringan tertentu, misalnya downgrade.attacks, cookie hijacking. 5. Kurangnya x-permitted-cross-domain-policies response header meningkatkan risiko penyalahgunaan sumber daya infrastruktur misalnya penggunaan bandwidth.
Rekomendasi Mitigasi	Mengonfigurasi header dengan menerapkan perlindungan meliputi: 1. Content-Security-Policy: script-src 'self' js.example.com 2. X-Frame-Options: SAMEORIGIN 3. X-Content-Type-Options: nosniff35 4. Strict-Transport-Security: max age=16070400;includeDomains 5. X-Permitted-Cross-Domain-Policies: none 6. Referrer-Policy: no-referrer 7. Permissions-Policy: geolocation=()
Referensi	https://owasp.org/Top10/A05_2021 Security_Misconfiguration/

Sumber:Hasil Penelitian (2025)

4. Kesimpulan

Berdasarkan hasil penelitian keamanan terhadap aplikasi *Management Employment System* (MES) di PT Mindotama Avia Teknik menggunakan metodologi PTES dan pendekatan OWASP Top 10, ditemukan beberapa kerentanan keamanan yang berpotensi membahayakan integritas, ketersediaan, dan kerahasiaan data karyawan. Proses pengujian dilakukan melalui berbagai tahapan, termasuk reconnaissance, scanning, enumeration, exploitasi, dan post-exploitation. Beberapa kerentanan utama yang ditemukan meliputi *Cross-Site Scripting* (XSS), Exposure PhpMyAdmin, *Improper Input Validation*, dan *Miss Config Security Header*. Dampak dari kerentanan ini mencakup potensi eksploitasi terhadap sistem autentikasi, risiko kebocoran data sensitif, kemungkinan manipulasi tampilan atau konten, serta ancaman terhadap stabilitas layanan akibat serangan *denial-of-service* (DoS). Meskipun beberapa parameter telah diuji menggunakan teknik seperti SQL Injection dan brute-force, masih ditemukan celah keamanan yang perlu diperbaiki untuk meningkatkan sistem keamanan web terhadap serangan siber.

Penelitian berikutnya juga dapat memanfaatkan metodologi pengujian keamanan yang lebih komprehensif dengan mengombinasikan PTES, OWASP *Web Security Testing Guide* (WSTG), dan standar keamanan lainnya guna memperoleh hasil analisis yang lebih mendalam. Selain itu, pengujian keamanan dapat dilakukan secara berkelanjutan melalui pendekatan *automated security testing* dan *continuous security assessment* untuk mengevaluasi efektivitas perbaikan yang telah diterapkan. Dengan demikian, penelitian selanjutnya diharapkan mampu

memberikan gambaran yang lebih menyeluruh mengenai tingkat keamanan sistem serta menghasilkan rekomendasi yang lebih optimal dalam mendukung penguatan keamanan informasi di lingkungan organisasi.

Referensi

[1] S. Azzahra and R. Septiyanti, "Perancangan Sistem Inventory Berbasis Web Untuk Efisiensi Operasional Di PT.KAI Palembang," *J. Surya Inform.*, vol. 16, no. 1, pp. 43–49, 2026.

[2] D. Prayogi *et al.*, "Pengembangan Aplikasi Smarthr Manajemen Data Karyawan Berbasis Hr Schema Oracle," *J. Ris. dan Apl. Mhs. Inform.*, vol. 06, no. 01, pp. 188–195, 2025.

[3] T. T. A. Risky and Armansyah, "Penerapan Metode Rapid Application Development Untuk Pengembangan Sistem Pengelolaan Data Kepegawaian," *J. Komput. dan Teknol.*, vol. 5, no. 1, pp. 14–26, 2026.

[4] Y. Y. Yuwono, D. Ferdiansyah, and M. F. Muttaqin, "Analisis Keamanan Website Universitas Pasundan Menggunakan Metode Penetration Testing Berbasis Kerangka Kerja PTES," *Pasinformatik*, vol. 5, no. 1, 2026.

[5] M. F. A. Ramadhan and A. S. Ilmananda, "Analisis Ancaman Keamanan Pada Sistem Informasi Akademik Kampus Menggunakan Metode OWASP ZAP," *J. Mhs. Tek. Inform.*, vol. 8, no. 4, pp. 7985–7991, 2024.

[6] T. Wilhelm, *Professional Penetration Testing: Creating and Learning in a Hacking Lab*. Elsevier, 2025.

[7] D. A. Andhika, Slamet, and N. Ningsih, "Pengujian Penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES)," *J. Technol. Informatics*, vol. 3, no. 2, pp. 55–61, 2022, doi: 10.37802/joti.v3i2.222.

[8] R. M. Fauzi, R. Hermawan, D. R. Adhy, and S. Maesaroh, "Analisis Kerentanan Keamanan Web Menggunakan Metode OWASP Dan PTES di Web Pemerintahan Desa XYZ," *Power Elektron. J. Orang Elektro*, vol. 13, no. 2, 2024.

[9] R. A. R. B. Firdaus and T. I. Widyawan, "Pengujian Kerentanan Website Menggunakan Metode Penetration Testing Dengan OWASP (Studi Kasus : Pemerintah Kabupaten Semarang) Website Vulnerability Testing Using the Penetration Testing Method with OWASP (Case Study : Semarang Regency Government)," *CyberSecurity dan Forensik Digit.*, vol. 8, no. 2, pp. 106–115, 2025.

[10] B. A. Bagaskara, M. Idhom, and H. E. Wahanani, "Pengujian Website Dinas Sosial Surabaya Menggunakan Metode Penetration Testing Dan OWASP TOP 10," *J. Inform. Rekayasa Elektron.*, vol. 8, no. 1, pp. 40–50, 2025.

[11] F. A. Maylani, M. Tahir, N. N. Juniar, D. Sari, W. A. Zulaica, and Ismael, "Analisis Keamanan Website E-Library Kampus Dengan Metode PTES (Penetration Testing Execution Standard)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 4, pp. 5643–5650, 2025.

[12] E. W. Darwis, Junaedy, and I. A. Musdar, "Analisis Kerentanan Website Renovaction Menggunakan Rangkaian Security Tools Project Berdasarkan Framework OWASP," *J. Kharisma Tech*, vol. 17, no. 01, pp. 1–15, 2022.

[13] M. Y. Firnanda, H. E. Wahanani, and A. Junaidi, "ERP Website Security Testing Using PTES Method and OWASP Top 10 Approach," *Bit-Tech (Binary Digit. - Technol.*, vol. 8, no. 1, 2025, doi: 10.32877/bt.v8i1.2564.

[14] I. Sutanto and M. F. Reza, "Penerapan Pentesting pada EasyCart untuk Menghadapi Ancaman Keamanan Siber," *Appl. Inf. Technol. Comput. Sci. (AICOMS)*, vol. 4, no. 2, pp. 37–45, 2025.

[15] R. R. Yusuf and T. N. Suharsono, "Pengujian Keamanan Dengan Metode OWASP Top 10 Pada Website Eform Helpdesk," in *Prosiding Seminar Sosial Politik, Bisnis, Akuntansi dan Teknik (SoBAT) ke-5*, 2023, pp. 402–413.

[16] A. Wirasto and D. Mustofa, "Analisis Keamanan Aplikasi Berbasis Web Di Universitas Harapan Bangsa Menggunakan Ptes," *J. Inf. Interaktif*, vol. 8, no. 3, pp. 89–94, 2023.