KAINAN: Jurnal Pengabdian Teknik Informatika
Vol. xx No. xx, xxxxxx xxx (xxx-xxx) https://doi.org/10.23960/kainan

ANALISIS CELAH KEAMANAN APLIKASI WEB SEBAGAI DASAR REKOMENDASI PENGUATAN SISTEM (STUDI KASUS: PAP.BAPENDA.LAMPUNGPROV.GO.ID)

Web Application Security Vulnerability Analysis as a Basis for System Strengthening Recommendations (Case Study: pap.bapenda.lampungprov.go.id)

Dean Kresna Ananda[1*], Mahendra Pratama[1], Hendrawansyah[2]

[1]*Program Studi Teknik Informatika, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Lampung, Jl. Prof. Dr. Ir. Sumantri Brojonegoro No.1, Bandar Lampung, Indonesia 35145*
[2] *Badan Pendapatan Daerah Provinsi Lampung, Jl. Hasanuddin No. 45, Teluk Betung, Bandar Lampung, Indonesia 35211*

**** Email Korespondensi:***

dian.tresna2015@gmail.com

Abstrak: Apikasi web instansi pemerintah memiliki peran krusial dalam pelayanan publik dan penyebaran informasi, namun hal ini juga diiringi dengan tingginya kerentanan terhadap ancaman siber. Penelitian ini bertujuan untuk mengevaluasi postur keamanan aplikasi web pap.bapenda.lampungprov.go.id milik Badan Pendapatan Daerah (BAPENDA) Provinsi Lampung secara proaktif guna mencegah insiden peretasan. Metode yang digunakan adalah *Penetration Testing* dengan pendekatan *Black-box testing*, di mana pengujian dilakukan secara komprehensif dari perspektif eksternal tanpa memiliki akses ke kode sumber, arsitektur internal, maupun akses *root* ke *server*. Hasil pengujian mengungkap sejumlah kerentanan dengan tingkat risiko kritis dan tinggi. Temuan utama meliputi paparan panel administrasi layanan yaitu phpMyAdmin, Zimbra, MikroTik ke internet publik, aktifnya fitur *Directory Listing* pada direktori sensitif /esalam/ yang mengekspos *file* konfigurasi, ketiadaan mekanisme proteksi serangan *brute-force* pada halaman otentikasi, serta penggunaan versi perangkat lunak yang telah usang PHP 5.5.12 dengan celah keamanan *Locale::parseLocale Memory Corruption*. Sebagai tindak lanjut mitigasi risiko, direkomendasikan penguatan sistem melalui penonaktifan *directory listing* menggunakan konfigurasi .htaccess, pembatasan akses panel administrasi melalui *firewall*, penerapan *rate limiting* pada halaman *login*, dan pembaruan komponen perangkat lunak ke versi stabil terbaru.

Kata kunci: black-box testing, celah keamanan, kerentanan web, *penetration testing,* sistem informasi.

Abstract: *Government web applications play a crucial role in public services and information dissemination, but this is also accompanied by a high vulnerability to cyber threats. This study aims to proactively evaluate the security posture of the web application pap.bapenda.lampungprov.go.id owned by the Regional Revenue Agency (BAPENDA) of Lampung Province to prevent hacking incidents. The method used is Penetration Testing with a Black-box testing approach, where comprehensive testing is carried out from an external perspective without access to source code, internal architecture, or root access to the server. The test results revealed a number of vulnerabilities with critical and high-risk levels. Key findings include the exposure of service administration panels phpMyAdmin, Zimbra, MikroTik to the public internet, active Directory Listing feature in a sensitive directory /esalam/ exposing configuration files, the absence of brute-force attack protection mechanisms on authentication pages, and the use of outdated software versions PHP 5.5.12 vulnerable to Locale::parseLocale Memory Corruption. As a risk mitigation follow-up, system strengthening is recommended through disabling directory listing using .htaccess configuration, restricting administration panel access via firewall, applying rate limiting on login pages, and updating software components to the latest stable versions.*

Keywords: *black-box testing, penetration testing, security vulnerability, information system, web vulnerability.*

1. PENDAHULUAN

Di era digitalisasi yang terus berkembang pesat, instansi pemerintah di berbagai tingkatan semakin mengandalkan aplikasi berbasis web sebagai sarana vital untuk menyediakan layanan mandiri, mengelola data administratif, dan menyebarkan informasi publik secara *real-time.* Ketergantungan terhadap ekosistem digital ini, meskipun membawa dampak positif berupa efisiensi dan transparansi birokrasi, juga membuka celah terhadap berbagai ancaman siber yang terus bermutasi dan berkembang

secara canggih [1]. Keamanan sistem informasi kini menjadi prioritas krusial yang tidak dapat dikompromikan untuk melindungi kerahasiaan, integritas, dan ketersediaan data, sekaligus menjaga kepercayaan masyarakat terhadap institusi negara.

Konteks keamanan siber di Indonesia sendiri masih menjadi tantangan yang masif. Data dan tren terkini menunjukkan bahwa Indonesia merupakan salah satu negara dengan jumlah kasus kejahatan siber yang tinggi, di mana situs-situs berdomain pemerintah (*.go.id*) seringkali menjadi target utama serangan, baik oleh peretas yang dimotivasi oleh faktor ekonomi, politik, maupun sekadar mencari pengakuan [2][3]. Secara spesifik, kekhawatiran mengenai ketahanan keamanan siber ini juga dirasakan secara nyata oleh Badan Pendapatan Daerah (BAPENDA) Provinsi Lampung. BAPENDA merupakan institusi yang mengelola data esensial terkait Pendapatan Asli Daerah (PAD) dan informasi wajib pajak.

Sebelum pelaksanaan penelitian ini, telah tercatat sebuah insiden keamanan berupa serangan peretasan perubahan tampilan halaman pada salah satu sub-bagian dari domain situs pap.bapenda.lampungprov.go.id. Terdapat probabilitas tinggi mengenai adanya celah keamanan lain yang tersembunyi, belum teridentifikasi, dan berpotensi dieksploitasi di kemudian hari dengan dampak yang jauh lebih merusak. Oleh karena itu, BAPENDA memandang perlunya langkah evaluasi keamanan yang proaktif, preventif, dan terstruktur untuk mencegah terulangnya insiden pelanggaran keamanan siber melalui manajemen risiko teknologi informasi yang tepat [4].

Menjawab urgensi dan kebutuhan tersebut, metode *Penetration Testing* diusulkan dan diimplementasikan sebagai solusi utama [5]. *Penetration Testing* adalah sebuah praktik metodologis untuk mengevaluasi keamanan sistem komputer atau jaringan secara menyeluruh dengan cara melakukan simulasi serangan yang terkendali dan dan etis [6]. Tujuan utamanya adalah untuk mengidentifikasi titik-titik lemah sistem dari sudut pandang penyerang sungguhan, sehingga celah tersebut dapat ditambal dan diperbaiki sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab [7].

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis celah keamanan teknis yang terdapat pada infrastruktur aplikasi web pap.bapenda.lampungprov.go.id secara mendalam. Selain itu, penelitian ini bertujuan mendemonstrasikan dampak nyata dari setiap kerentanan yang ditemukan guna memberikan pemetaan risiko yang akurat kepada pemangku kepentingan. Hasil akhir dari penelitian ini adalah sebuah luaran berupa analisis kerentanan komprehensif yang disertai dengan rekomendasi perbaikan teknis yang bersifat *actionable* guna memperkuat arsitektur keamanan BAPENDA Provinsi Lampung. Ruang lingkup dibatasi pada pengujian *black-box testing*, di mana pengujian berfokus pada kerentanan teknis tanpa menyertakan pengujian berbasis *Denial of Service* (DoS) yang berisiko mengganggu stabilitas pelayan publik.

2. BAHAN DAN METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental terapan di bidang keamanan siber dengan mengadopsi metodologi uji penetrasi standar industri. Pendekatan yang digunakan adalah *Black-box testing*, sebuah metode pengujian di mana evaluator tidak dibekali dengan informasi internal apapun mengenai sistem target [1].

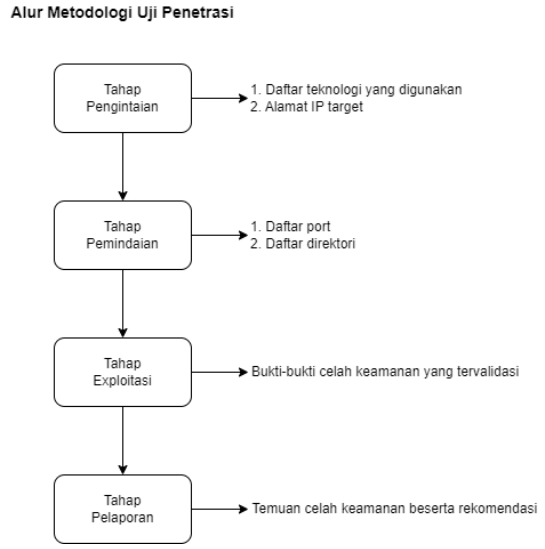
2.1. Perangkat Lunak Pengujian

Dalam pelaksanaan uji penetrasi, serangkaian perangkat lunak keamanan khusus digunakan untuk memfasilitasi setiap tahapan [8]. Perangkat yang digunakan meliputi:

1. WhatWeb yaitu perangkat pengintai generasi mutakhir yang dirancang untuk mengekstrasi informasi profil dari sebuah situs web, termasuk jenis *web server*, kerangka kerja, hingga bahasa pemrograman spesifik beserta versinya.
2. Nmap yaitu utilitasi pemindai jaringan andalan yang digunakan untuk menemukan *host* yang aktif, memetakan *port* yang terbuka, serta mengidentifikasi layanan dan sistem operasi yang berjalan di belakang port tersebut dengan menganalisis respons paket jaringan.
3. Dirb yaitu pemindai konten berbasis kamus yang berfungsi menemukan objek web tersembunyi. Alat ini mencari direktori dan *file* yang tidak memiliki tautan publik namun dapat diakses jika URL diketahui.
4. Hydra yaitu perangkat otentikasi jaringan paralel yang sangat cepat dan fleksibel, dimanfaatkan secara khusus untuk menyimulasikan serangan *brute-force* secara daring guna menguji ketahanan halaman otentikasi target.
5. Exploit-DB yaitu basis data arsip publik terbesar yang mendokumentasikan ribuan program exploitasi dan informasi kerentanan perangkat lunak. Basis data ini digunakan sebagai refrensi untuk memvalidasi apakah versi perangkat lunak yang ditemukan pada target memiliki cacat keamanan yang telah terekspos.

2.2 Tahapan Pelaksanaan Uji Penetrasi

Metodologi pengujian dijalankan secara terstruktur melalui empat fase berurutan yang mengadaptasi best practice keamanan:



Gambar 1. Alur Metodologi Uji Penetrasi

Berdasarkan alur di atas, rincian tahapan pengujian adalah sebagai berikut:

1. Tahap Pengintaian yaitu tahap pengumpulan intelijen pasif dan aktif. Pada fase ini, WhatWeb dikerahkan untuk melakukan *profiling* terhadap domain pap.bapenda. lampungprov.go.id, mengumpulkan metadata, mengidentifikasi stack teknologi, dan mendapatkan resolusi alamat IP server.
2. Tahap Pemindaian yaitu tahap pemetaan permukaan serangan. Informasi dari tahapan pertama digunakan sebagai basis sasaran Nmap. Nmap memindai seluruh *port* TCP/UDP untuk mencari celah administratif yang terbuka. Secara bersamaan, Dirb melakukan pemindaian *brute-force* pada struktur URL untuk mencari rute ke direktur sensitif.
3. Tahap Eksploitasi yaitu tahap pembuktian konsep. Kerentanan potensial yang dipetakan pada tahap sebelumnya diuji coba. Proses ini meliputi verifikasi manual akses terhadap URL administratif, pencocokan kerentanan versi perangkat lunak dengan Exploit-DB, dan meluncurkan serangan simulasi menggunakan Hydra pada formulir otentikasi yang terekspos.
4. Tahap Pelaporan yaitu tahap akhir berupa dokumentasi komprehensif atas temuan dan rumusan mitigasi teknis [5].

3. HASIL DAN PEMBAHASAN

Proses uji penetrasi terhadap sistem BAPENDA Provinsi Lampung menghasilkan sejumlah temuan teknis yang signifikan. Pengujian difokuskan pada alamat IP *server* utama, yakni 103.145.47.66. Berikut ini adalah pemaparan mendetail mengenai proses identifikasi dan analisis kerentanan yang telah tervalidasi.

Tabel 1. Matriks Temuan Celah Keamanan

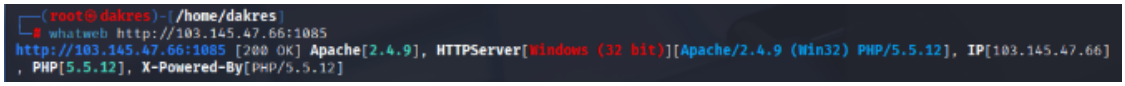
Nama Kerentanan	Port	Tingkat Risiko	Dampak Potensial
Directory Listing Aktif	6066	Kritis	Pengungkapan struktur *file* sistem dan *file* konfigurasi sensitif.
Paparan Panel Administrasi	7071, 8443, dan 8081	Tinggi	Memberikan jalur masuk bagi penyerang untuk mencoba mengambil alih *router*, email, dan basis data secara penuh.
Kerentanan *Brute-Force*	/administrator/loginapp	Tinggi	Penyerang dapat menggunakan bot untuk menebak *password* secara massal tanpa diblokir oleh sistem.
Perangkat Lunak Usang	PHP versi 5.5.12 (Port 1085)	Sedang	Rentan terhadap eksekusi kode jarak jauh (*Remote Code Execution*) akibat cacat pengelolaan memori.

3.1 Identifikasi Teknologi dan Versi Perangkat Lunak

Langkah inisial dimulai dengan menggunakan *tool* WhatWeb. Hasil pemindaian awal (HTTP respons kode 200 OK) memperlihatkan bahwa *server* utama beroperasi di atas peladen web Apache, dengan *frontend* yang dibangun memanfaatkan kerangka kerja Bootstrap dan JQuery.

Gambar 2. Hasil Identifikasi Teknologi dengan WhatWeb

Pemindaian mendalam lebih lanjut dilakukan pada layanan yang berjalan di *port* spesifik, yaitu *port* 1085. Pada *port* ini, WhatWeb berhasil mengekstrak informasi yang sangat krusial terkait versi bahasa pemrograman sisi *server*, yaitu PHP 5.5.12.



Gambar 3. Hasil Identifikasi Teknologi WhatWeb Lanjut

Tabel 1 menyajikan rangkuman profil infrastruktur teknologi yang menopang web tersebut.

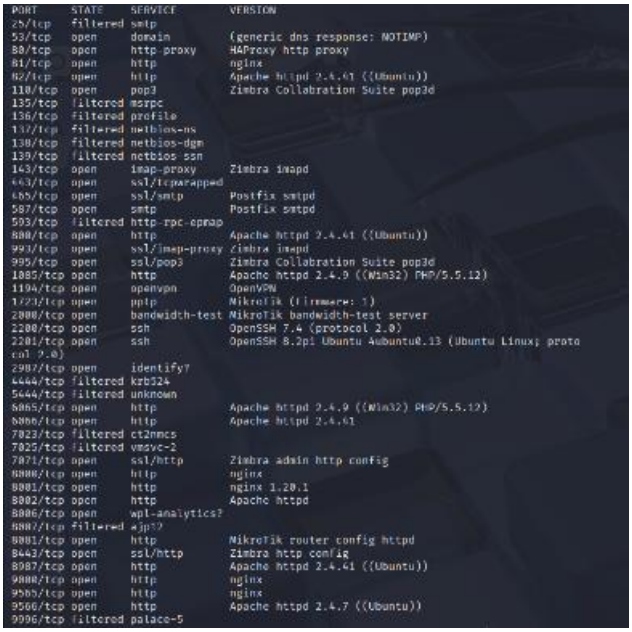
Tabel 2. Ringkasan Hasil Identifikasi Teknologi

Atribut	Keterangan
Alamat IP	103.145.47.66
Web Server	Apache
Bahasa Pemrograman	PHP/5.5.12
Framework	Bootstrap, Jquery
Sistem Operasi	Linux

Penemuan versi PHP 5.5.12 ini menjadi catatan merah pertama yang masif. Mengingat versi ini telah mencapai status *End of Life* sejak tahun 2016, sistem dipastikan tidak lagi menerima patch pembaruan keamanan esensial.

3.2 Pemindaian Port, Layanan

Pemetaan permukaan serangan dengan Nmap mengungkap arsitektur jaringan *server* yang cukup longgar. Pemindaian pada IP 103.145.47.66 menunjukkan puluhan *port* TCP terbuka, menjalankan berbagai layanan internal maupun eksternal.

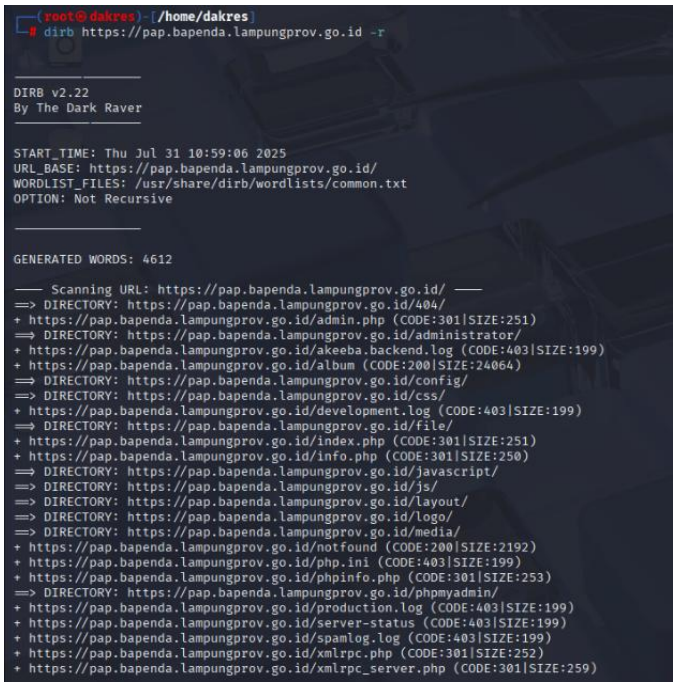


Gambar 4. Hasil Pemindaian Port dan Layanan dengan Nmap

Di antara daftar panjang layanan yang berjalan, ditemukan sejumlah layanan yang merepresentasikan risiko keamanan tinggi karena seharusnya bersifat internal dan tidak boleh terekspos ke ruang publik internet. Layanan tersebut meliputi:

1. Port 8071 & 8443: Mengidentifikasi layanan Zimbra Admin Console.
2. Port 8081: Mengidentifikasi layanan konfigurasi jaringan *router* Mikrotik.
3. Port 6066 & 1085: Menjalankan layanan HTTPD Apache versi lawas yaitu 2.4.9.

Secara bersamaan, pemindaian konten dengan menggunakan Dirb melengkapi temuan ini dengan mengidentifikasi eksistensi direktori-direktori vital. Dirb menavigasi struktur aplikasi web secara agresif dan mendapati beberapa *paths* sensitif yang menuntun ke *backend* sistem [8].



Gambar 5. Hasil Enumerasi Direktori dengan Dirb

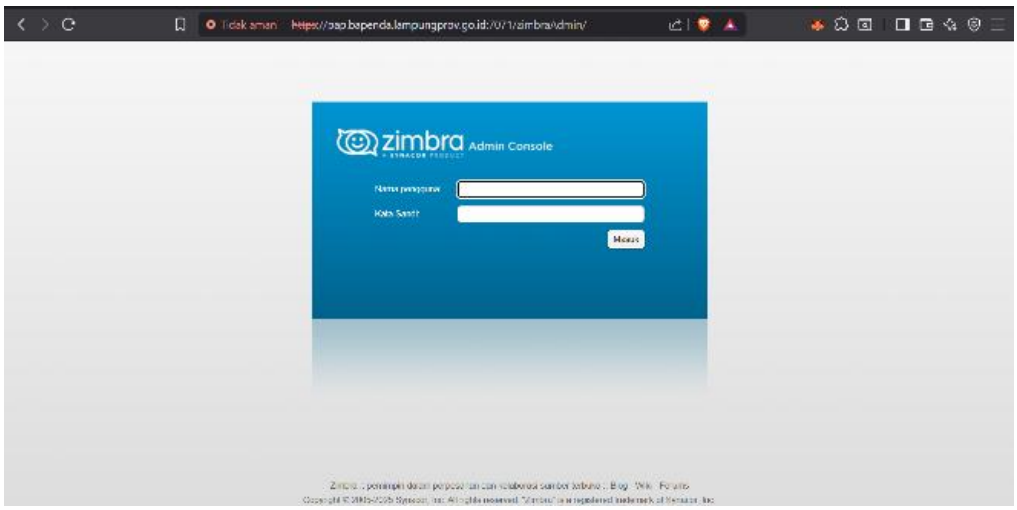
3.3 Analisis Celah Keamanan Kritis dan Beresiko Tinggi

Berdasarkan agregasi data dari pemindaian pasif dan aktif, verifikasi eksploitasi tahap selanjutnya memastikan keparahan dari celah-celah tersebut.

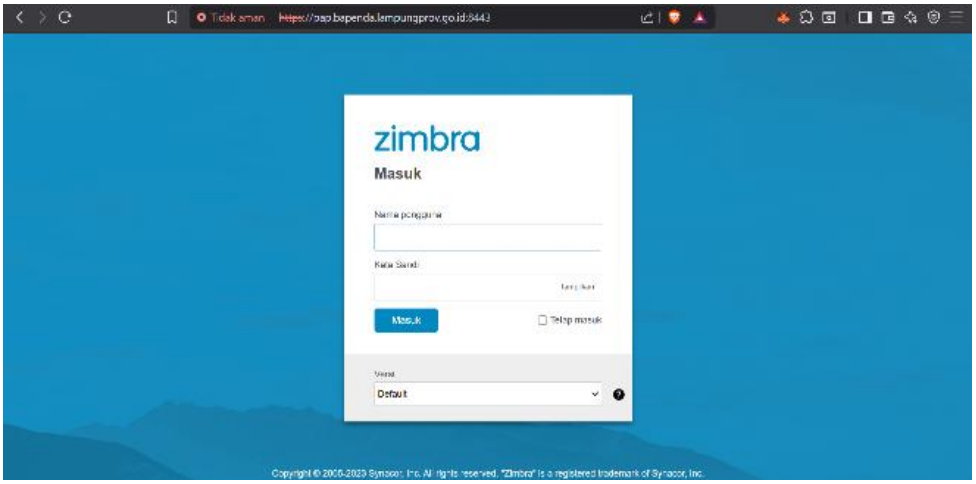
3.3.1 Paparan Panel Administrasi Multilayanan

Dari hasil identifikasi Nmap dan Dirb, dilakukan pengujian akses secara manual menggunakan peramban web. Verifikasi ini membuktikan skenario terburuk: panel kontrol untuk infrastruktur krusial sepenuhnya terbuka bebas ke publik tanpa pembatasan akses geografis atau IP jaringan [8].

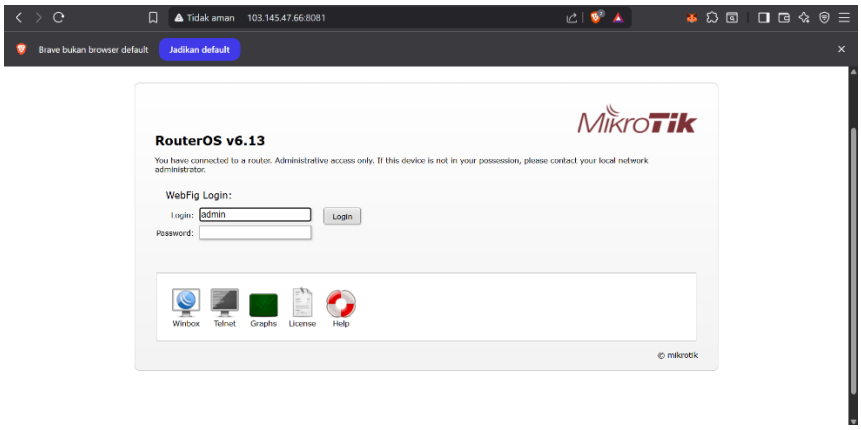
Gambar 6. Halaman Login phpMyAdmin



Gambar 7. Halaman Login Zimbra Admin



Gambar 8. Halaman Login Zimbra

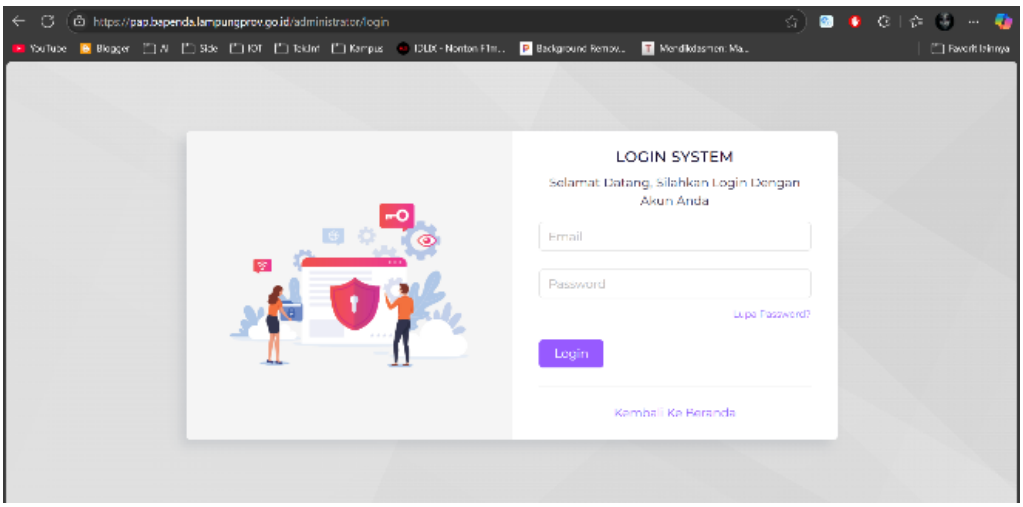


Gambar 9. Halaman Login Mikrotik

Keterbukaan akses ke phpMyAdmin, antarmuka administrasi Zimbra, dan pintu konfigurasi MikroTik memberikan penyerang sebuah bidang interaksi yang luas. Ketersediaan panel *login* ini berarti penyerang hanya perlu menebak kredensial yang tepat untuk meretas jaringan instansi hingga ke akarnya.

3.3.2 Kerentanan Brute-Force pada Panel Otentikasi

Selain panel infrastruktur, ditemukan pula direktori /administrator/loginapp yang memuat antarmuka otentikasi kustom milik sistem informasi aplikasi BAPENDA.

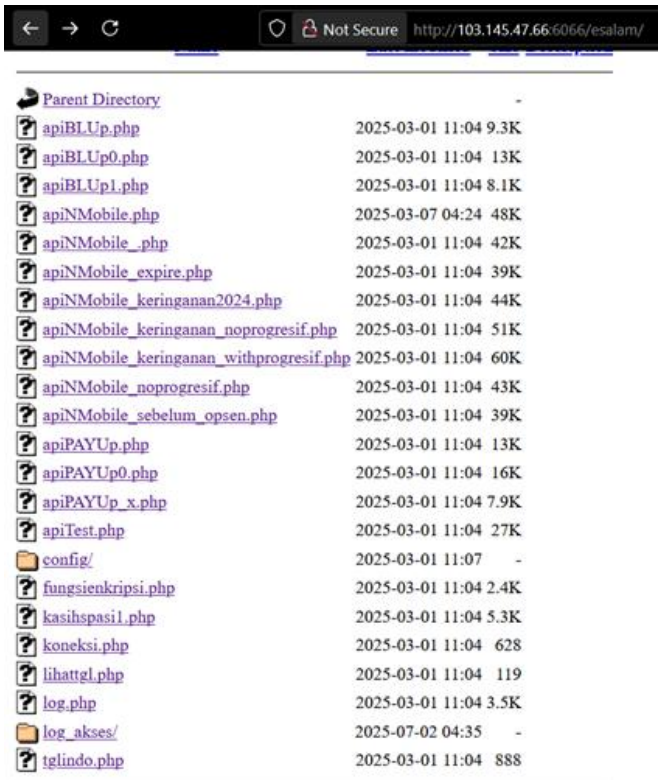


Gambar 10. Halaman Login Administrator

Sebagai bagian dari prosedur uji penetrasi, sebuah serangan *dictionary-based brute-force* diujicobakan secara terkontrol menggunakan perangkat lunak Hydra. Walaupun percobaan simulasi dalam jendela waktu penelitian tidak berhasil memecahkan kata sandi, pengujian ini mengonfirmasi satu kelemahan fatal: ketidakhadiran implementasi mekanisme *Rate Limiting* dan absennya sistem CAPTCHA. Kondisi ini berarti penyerang dengan ketersediaan *wordlist* besar dan sumber daya komputasi tinggi dapat membombardir halaman otentikasi dengan ribuan kombinasi *username/password* tanpa terblokir oleh *server*, meningkatkan ekspektasi keberhasilan serangan secara drastis [1].

3.3.3 Kerentanan Directory Listing Aktif

Penjelajahan manual pada *port* 6066 menuntun pada penemuan kerentanan berstatus kritis, yakni terekspos nya struktur berkas akibat aktifnya modul *Directory Listing* pada direktori /esalam/ [9].



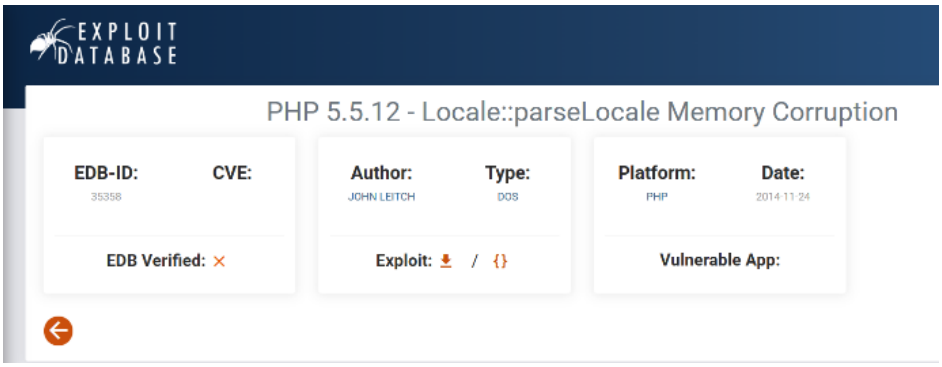
Gambar 11. Directory Listing Aktif pada Direktori /esalam/

Kerentanan arsitektural ini secara harafiah mengizinkan publik melihat daftar inventaris berkas internal peladen. Terpampang nyata keberadaan *file* berisiko sangat tinggi seperti

kumpulan API pembayaran, catatan aktivitas *server* (log_akses), serta yang paling fatal, koneksi.php beserta sub-direktori config/ [9]. Meskipun skrip berakhiran .php akan dieksekusi di *backend* sehingga isinya tidak langsung tercetak, keterbukaan nama *file* ini memberikan *blueprint* struktur aplikasi. Dengan informasi ini, peretas selangkah lebih maju dalam mengeksploitasi cacat *Local File Inclusion* untuk mengunduh kode sumber dan mencuri parameter kredensial basis data.

3.4 Analisis Celah Keamanan Berisiko Sedang

Penggunaan PHP versi 5.5.12 bukan sekadar soal usia rilis, melainkan penumpukan utang teknis keamanan. Konsultasi data pada Exploit-DB mencocokkan profil rilis ini dengan eksploitasi publik tervalidasi dengan identitas *EDB-ID: 35358* berbasis kerentanan *Locale::parseLocale Memory Corruption*.



Gambar 12. Pencarian Versi PHP di Exploit Database

Memory corruption ini tidak boleh dipandang sebelah mata. Jika diinjeksi dengan muatan eksploitasi yang tepat melalui parameter input aplikasi, cacat ini sanggup memicu berhentinya layanan secara sistemik *Denial of Service* dan memberikan ruang eskalasi yang mengizinkan eksekusi program ilegal jarak jauh tanpa perlu kredensial sah

3.5 Rekomendasi Penguatan Sistem Secara Praktis.

Untuk mengeliminasi vektor-vektor ancaman yang telah dijabarkan, rekomendasi perbaikan berbasis mitigasi teknis mutlak diimplementasikan [2] [3]. Perbaikan ini diurutkan berdasarkan urgensi:

3.5.1 Penonaktifan Segera Modul Direcotry Listing

Risiko pengungkapan informasi hierarki harus langsung dimatikan dari level manajemen berkas *web server* Apache. Solusi teringan yang tidak memerlukan prosedur *restart* layanan peladen utama adalah memodifikasi konfigurasi *hypertext access*.

1. Buat sebuah *file* murni berbasis teks bernama .htaccess.
2. Tanamkan direktif keamanan berikut di dalamnya: Options -Indexes
3. Letakkan konfigurasi ini pada *root folder* proyek /var/www/html/ atau setara. *Server* secara independen akan langsung merevisi perilaku aksesnya, dan pengguna tak sah akan terhadang oleh respons *"HTTP 403 Forbidden"*.

3.5.2 Pembatasan Ketat Akses ke Seluruh Panes Administrasi

Layanan infrastruktur Zimbra, MikroTik, phpMyAdmin dilarang berhadapan dengan koneksi *inbound* internet secara polos. Rekomendasi terbaik adalah menerapkan blokir *Deny All*, lalu meracik daftar putih alamat IP intranet/kantor yang diizinkan melintas. Sebagai ilustrasi teknis, pengamanan untuk MikroTik port 8081 dapat diinisiasi via terminal dengan aturan pemfilteran berbasis *firewall*.

3.5.3 Peningkatan Mekanisme Ketahanan Halaman Login

Modifikasi kode wajib dicanangkan pada antarmuka *login* agar tangguh menahan gempuran tebakan robot otomatis. Implementasi teknik *Rate Limiting* berbasis memori atau basis data dapat dibangun berdasarkan pendekatan *pseudo-code* mitigasi.

Untuk pertahanan berlapis, integrasi layanan CAPTCHA v2/v3 secara signifikan dapat menggagalkan sebagian besar perangkat lunak *brute-forcing* modern seperti Hydra.

3.5.4 Siklus Pembaruan Modul dan Perangkat Lunak Secara Menyeluruh

Meningkatkan dan menambal versi mesin PHP dari 5.5.12 ke yang lebih baru serta Apache merupakan prosedur preventif puncak.

Administratif peladen harus melakukan rutinitas migrasi versi melalui manajer paket distribusi, misalnya: sudo apt-get update && sudo apt-get upgrade untuk lingkungan berbasis Ubuntu/Debian. Modul kuno yang tak lagi bertuan harus *uninstalled* demi mereduksi luasan area potensi serangan.

4. KESIMPULAN

Uji penetrasi proaktif pada aplikasi web BAPENDA Provinsi Lampung (pap.bapenda.lampungprov.go.id) berhasil menemukan celah krusial yang harus segera diatasi. Secara garis besar, profil keamanan saat ini dipengaruhi secara signifikan oleh kelemahan di ranah manajemen miskonfigurasi layanan peladen dan absennya kedisiplinan pembaruan siklus hidup aplikasi. Terekspos nya pintu otentikasi esensial seperti *router* dan *database*, serta kerentanan *Directory Listing* yang menyebarkan peta konfigurasi berkas, membuka akses langsung awal bagi kejahatan siber untuk merusak ekosistem. Dengan adanya temuan sistematis ini, BAPENDA diimbau untuk menyegerakan transisi ke standar *secure-coding* yang mapan, menerapkan strategi proteksi pemfilteran alamat IP, dan merutinkan kalender audit keamanan sebagai siklus wajar dalam transformasi dan pemerintahan digital

.

UCAPAN TERIMA KASIH

Rasa terima kasih yang mendalam penulis tujukan kepada Kepala Badan Pendapatan Daerah (BAPENDA) Provinsi Lampung beserta jajaran manajemen atas keterbukaan izin dalam menyelenggarakan program riset akademis dan kerja praktik ini. Penghargaan istimewa turut diberikan kepada Staf dan Pembimbing Lapangan di Sub Bidang Pengembangan Informasi Pendapatan yang telah menyediakan pengawasan penuh serta asistensi teknis yang memadai di lapangan selama proses analisis berlangsung. Terima kasih pula kami haturkan kepada para pendidik, secara khusus Dosen Pembimbing Praktik, atas limpahan telaah, sumbangan pikiran, serta pengarahan akademis dalam memperkokoh kerangka keilmuan penyusunan analisis temuan kerentanan siber ini

DAFTAR PUSTAKA

[1] A. Alquwayzani, R. Aldossri, and M. Frikha, “Mitigating Security Risks in Firewalls and Web Applications using Vulnerability Assessment and Penetration Testing (VAPT),” *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 15, no. 5, 2024, [Online]. Available: www.ijacsa.thesai.org

[2] A. Almaarif and M. Lubis, “Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government’s Website,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 5, pp. 1874–1880, Oct. 2020, doi: 10.18517/ijaseit.10.5.8862.

[3] M. Dian Khoiroh *et al.*, “Penetration Testing untuk Menguji Kerentanan Sistem Informasi Pemerintah Daerah,” *Jurnal Sistem dan Teknologi Informasi (JSTI)*, vol. 6, Aug. 2024, [Online]. Available: https://journalversa.com/s/index.php/jsti

[4] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. Sri Arsa, “Information Technology Risk Management Using ISO 31000 Based on ISSAF Framework Penetration Testing (Case Study: Election Commission of X City),” *International Journal of Computer Network and Information Security*, vol. 12, no. 4, pp. 30–40, Aug. 2020, doi: 10.5815/ijcnis.2020.04.03.

[5] W. G. J. Halfond, S. R. Choudhary, and A. Orso, “Improving penetration testing through static and dynamic analysis,” *Software Testing, Verification and Reliability*, vol. 21, no. 3, pp. 195–214, Sep. 2011, doi: 10.1002/stvr.450.

[6] M. Mirjalili, A. Nowroozi, and M. Alidoosti, “A survey on web penetration test,” *ACSIJ Advances in Computer Science: an International Journal*, no. 6, Nov. 2014, [Online]. Available: www.ACSIJ.org

[7] D. Dalalana Bertoglio and A. F. Zorzo, “Overview and open issues on penetration test,” *Journal of the Brazilian Computer Society*, vol. 23, no. 1, Dec. 2017, doi: 10.1186/s13173-017-0051-1.

[8] M. F. Rifqi, O. Krianto Sulaiman, and A. Ichsan, “Pemindaian Kerentanan Aplikasi Web Dinas Kearsipan dan Perpustakaan Daerah Kabupaten Semarang menggunakan Information System Security Assessment Framework (ISSAF),” vol. 2, Jul. 2025, [Online]. Available: https://journal.hasbaedukasi.co.id/index.php/jurmieHalaman:777-792

[9] M. Tahir and M. Risky, “Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard),” *Jurnal Teknik Informatika Unika ST. Thomas (JTIUST)*, pp. 2657–1501, Jun. 2024.