

**OTOMASI REMEDIASI INSECURE DESIGN PADA WEB
SERVER APACHE2 BERBASIS FAIL2BAN**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

AZHAR SURYA PRATAMA

20.83.0550

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2024

**OTOMASI REMEDIASI INSECURE DESIGN PADA WEB
SERVER APACHE2 BERBASIS FAIL2BAN**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh
AZHAR SURYA PRATAMA
20.83.0550

Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2024

**HALAMAN PERSETUJUAN
SKRIPSI**

**OTOMASI REMEDIASI INSECURE DESIGN PADA WEB SERVER
APACHE2 BERBASIS FAIL2BAN**

yang disusun dan diajukan oleh

Azhar Surya Pratama

20.83.0550

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 13 Agustus 2024

Dosen Pembimbing,



Muhammad Kopravi, S.Kom., M.Eng

NIK. 190302454

HALAMAN PENGESAHAN
SKRIPSI
OTOMASI REMEDIASI INSECURE DESIGN PADA WEB SERVER
APACHE2 BERBASIS FAIL2BAN

yang disusun dan diajukan oleh

Azhar Surya Pratama

20.83.0550

Telah dipertahankan di depan Dewan Penguji
pada tanggal 13 Agustus 2024

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Anggit Ferdita Nugraha, S.T., M.Eng
NIK. 190302480

Harvoko, S. Kom. M. Cs.
NIK. 190302286

Muhammad Kopravi, S.Kom., M.Eng
NIK. 190302454

Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 13 Agustus 2024

DEKAN FAKULTAS ILMU KOMPUTER



Hunif Al Fatta, S.Kom., M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Azhar Surya Pratama
NIM : 20.83.0550

Menyatakan bahwa Skripsi dengan judul berikut:

OTOMASI REMEDIASI INSECURE DESIGN PADA WEB SERVER APACHE2 BERBASIS FAIL2BAN

Dosen Pembimbing : Muhammad Kopravi, S.Kom., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 13 Agustus 2024

Yang Menyatakan,



Azhar Surya Pratama

HALAMAN PERSEMBAHAN

Puji syukur peneliti panjatkan kehadiran Allah SWT, yang telah memberikan rahmat dan hidayah-Nya sehingga peneliti dapat menyelesaikan skripsi ini dengan baik. Skripsi ini saya persembahkan untuk :

1. Kedua orang tua saya, Bapak Slamet Bagiyono dan Ibu Siti Asiyah yang selalu memberikan doa restu, dukungan, dan memenuhi keperluan selama perkuliahan hingga proses penyelesaian skripsi.
2. Bapak Muhammad Kopravi, S.Kom., M.Eng selaku dosen pembimbing yang telah bersedia meluangkan waktu untuk mengkurasi dan memberikan masukan agar skripsi ini menjadi lebih baik.
3. Joko Dwi Santoso, M.Kom. selaku bapak saya di kampus yang telah memberikan kesempatan belajar dibawah bimbingan beliau dan diberikan alat serta tempat untuk mengembangkan minat hingga dapat menjadi seperti sekarang.
4. Kepada teman saya R. Ahmad Hidayat yang telah memberikan gagasan dan masukan dalam proses penelitian skripsi ini.
5. Terakhir untuk teman teman angkatan 22 seperti Grisha, Rachmat, Rian, Naufal Azhar, Lingga, dan teman teman lain di kontrakan yang hadir dalam suka duka ketika melakukan penelitian ini hingga menjadi skripsi.

KATA PENGANTAR

Segala puji dan syukur penulis haturkan kepada Allah SWT atas izin, rahmat, dan hidayah-Nya penulisan skripsi dengan judul “Otomasi Remediasi Insecure Design pada Web Server Apache2 berbasis Fail2Ban” dapat selesai dengan baik. Penulis berharap hasil penelitian ini dapat memberikan manfaat bagi banyak pihak.

Sholawat serta salam semoga tetap tercurahkan kepada junjungan kita Nabi Muhammad SAW yang senantiasa kita harapkan syafa'atnya di hari akhir. Penyusunan skripsi ini merupakan salah satu syarat untuk memperoleh gelar Strata I dalam program studi teknik komputer Universitas Amikom Yogyakarta. Dalam penyusunan skripsi ini berbagai pihak telah memberikan dorongan, bantuan, serta masukan sehingga dalam kesempatan ini penulis menyampaikan terima kasih yang sebesar-besarnya kepada :

1. Ayah, ibu, dan adik penulis yang senantiasa memberikan dukungan, do'a, dan motivasi untuk penulis dalam menyelesaikan pendidikan di Universitas Amikom Yogyakarta
2. Bapak Prof. Dr. M. Suyanto, M.M, selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Hanif Al-Fatta, M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Bapak Dony Ariyus, M.Kom selaku Kepala Prodi Teknik Komputer
5. Bapak Muhammad Kopravi, S.Kom., M.Eng selaku dosen pembimbing yang dengan sabar dan ikhlas telah meluangkan waktu dan memberikan ilmunya kepada penulis dalam memberikan petunjuk dan bimbingan sehingga penulis dapat menyelesaikan skripsi ini.
6. Ridho Ahmad H selaku teman penulis yang telah memberikan bantuan supervisi, inspirasi, serta masukan dalam menyelesaikan penelitian ini.

Penulis menyadari sepenuhnya bahwa dalam penulisan penelitian ini masih terdapat banyak kekurangan dan jauh dari kata sempurna. Penulis juga mengharapkan masukan berupa kritik dan saran yang membangun sebagai bahan pertimbangan dalam memperbaiki kekurangan yang ada sehingga kedepannya dapat menjadi semakin baik. Terakhir, penulis berharap semoga penelitian ini dapat memberikan manfaat bagi pembaca serta pada diri penulis sendiri.

Yogyakarta, 13 Agustus 2024

Azhar Surya Pratama

20.83.0550

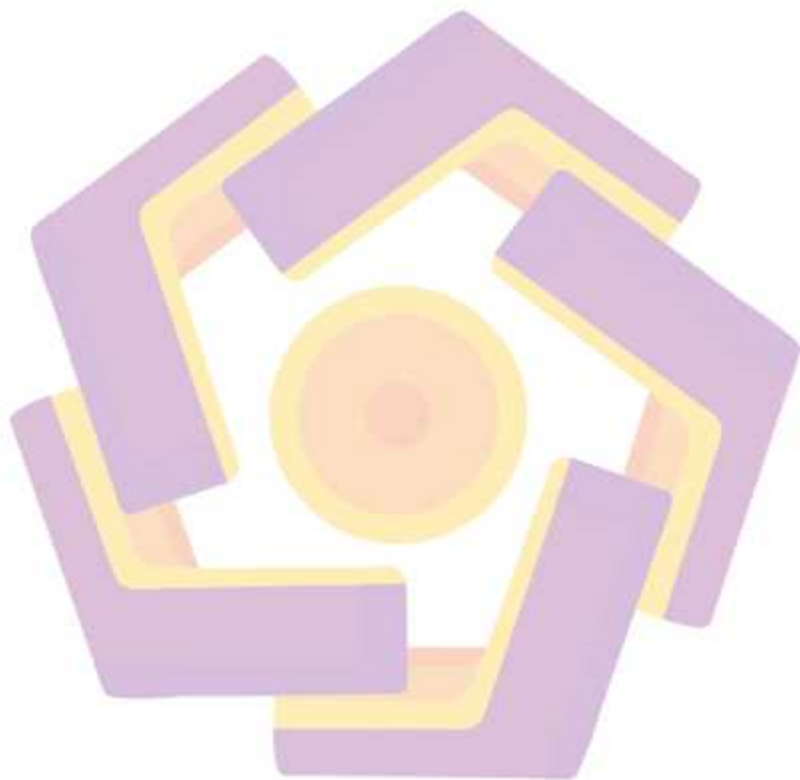


DAFTAR ISI

| | |
|--|----------|
| HALAMAN JUDUL | i |
| HALAMAN PERSETUJUAN | ii |
| HALAMAN PENGESAHAN | iii |
| HALAMAN PERNYATAAN KEASLIAN SKRIPSI..... | iv |
| HALAMAN PERSEMBAHAN | v |
| KATA PENGANTAR..... | vi |
| DAFTAR ISI..... | viii |
| DAFTAR TABEL | xi |
| DAFTAR GAMBAR..... | xii |
| INTISARI | xv |
| <i>ABSTRACT</i> | xvi |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 3 |
| 1.3 Batasan Masalah | 3 |
| 1.4 Tujuan Penelitian | 5 |
| 1.5 Manfaat Penelitian | 5 |
| 1.6 Sistematika Penulisan | 5 |
| BAB II TINJAUAN PUSTAKA | 8 |
| 2.1 Studi Literatur | 8 |
| 2.2 Dasar Teori | 18 |
| 2.2.1 Otomasl | 18 |
| 2.2.2 Remediasl | 19 |
| 2.2.3 <i>Security Hardening</i> | 20 |

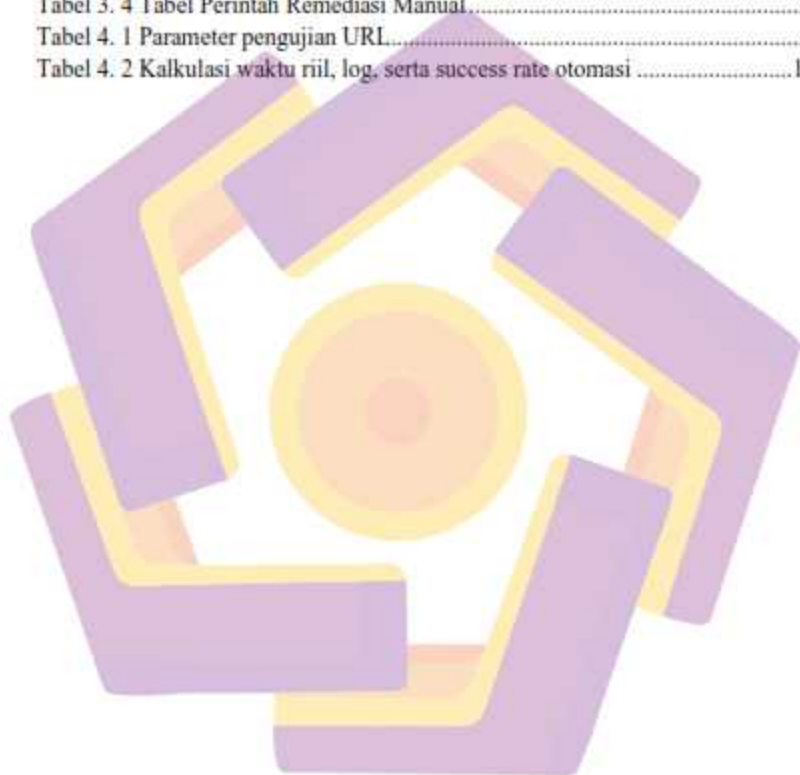
| | | |
|--|---|-----------|
| 2.2.4 | <i>Insecure Design</i> | 22 |
| 2.2.5 | <i>Debian</i> | 24 |
| 2.2.6 | <i>Web Server</i> | 25 |
| 2.2.7 | <i>Web Server Apache</i> | 27 |
| 2.2.8 | <i>Fail2Ban</i> | 28 |
| 2.2.9 | <i>IPTables</i> | 30 |
| 2.2.10 | <i>Python</i> | 31 |
| 2.2.11 | Bahasa Pemrograman C..... | 32 |
| 2.2.12 | <i>GNU Compiler Collection (GCC)</i> | 33 |
| BAB III METODE PENELITIAN | | 34 |
| 3.1 | Alur Penelitian..... | 34 |
| 3.2 | Alat dan Bahan..... | 37 |
| 3.2.1 | Peralatan..... | 37 |
| 3.2.2 | Bahan..... | 38 |
| 3.3 | Rancangan Penelitian..... | 40 |
| 3.4 | Instalasi dan Konfigurasi pada Sistem..... | 41 |
| 3.4.1 | Instalasi dan Konfigurasi Media Pengujian..... | 41 |
| 3.4.2 | Pembuatan Skrip Otomasi..... | 47 |
| 3.5 | Pengujian Sistem..... | 60 |
| 3.5.1 | Pengujian Sistem Otomasi..... | 62 |
| 3.5.2 | Pengujian Keamanan Pasca Remediasi..... | 64 |
| 3.5.3 | Pengujian Kecepatan Remediasi Manual..... | 68 |
| 3.5.4 | Pengujian Konsistensi Kecepatan Sistem Otomasi..... | 69 |
| BAB IV HASIL DAN PEMBAHASAN | | 71 |
| 4.1 | Hasil Pengujian Sistem Otomasi..... | 71 |
| 4.2 | Hasil Pengujian Keamanan Pasca Remediasi..... | 78 |
| 4.3 | Hasil Pengujian Kecepatan Remediasi Manual..... | 90 |
| 4.4 | Hasil Pengujian Konsistensi Kecepatan Sistem Otomasi..... | 95 |
| 4.5 | Perbandingan Kecepatan Remediasi Manual dan Otomasi..... | 103 |

| | |
|-----------------------------|------------|
| BAB V PENUTUP..... | 105 |
| 5.1 Kesimpulan | 105 |
| 5.2 Saran..... | 105 |
| REFERENSI..... | 107 |



DAFTAR TABEL

| | |
|---|-----|
| Tabel 2. 1 Keaslian Penelitian | 12 |
| Tabel 3. 1 Spesifikasi Laptop..... | 38 |
| Tabel 3. 2 Spesifikasi VPS..... | 38 |
| Tabel 3. 3 Spesifikasi Bahan..... | 40 |
| Tabel 3. 4 Tabel Perintah Remediasi Manual..... | 69 |
| Tabel 4. 1 Parameter pengujian URL..... | 80 |
| Tabel 4. 2 Kalkulasi waktu riil, log, serta success rate otomatis | 102 |



DAFTAR GAMBAR

| | |
|--|----|
| Gambar 2. 1 Perbedaan kinerja mesin dan manusia | 19 |
| Gambar 2. 2 Logo Linux Debian | 24 |
| Gambar 2. 4 Cara kerja <i>web server</i> | 26 |
| Gambar 2. 5 Logo <i>web server Apache</i> | 27 |
| Gambar 2. 6 Logo aplikasi <i>Fail2ban</i> | 28 |
| Gambar 2. 7 Logo <i>firewall IPTables</i> | 30 |
| Gambar 2. 8 Logo bahasa pemrograman <i>Python</i> | 31 |
| Gambar 2. 9 Logo bahasa pemrograman <i>C</i> | 32 |
| Gambar 3. 1 Diagram alir dari tahapan Penelitian | 37 |
| Gambar 3. 2 Desain rancangan sistem | 40 |
| Gambar 3. 3 Status layanan <i>apache2</i> yang aktif | 42 |
| Gambar 3. 4 Status layanan <i>apache2</i> yang tidak aktif | 42 |
| Gambar 3. 5 Modifikasi konfigurasi situs bawaan <i>Apache2</i> | 43 |
| Gambar 3. 6 Rekayasa konfigurasi kustom <i>Apache2</i> | 44 |
| Gambar 3. 7 Penambahan isi aset situs <i>web</i> | 44 |
| Gambar 3. 8 Penambahan berkas kosong pada konfigurasi <i>Apache2</i> | 45 |
| Gambar 3. 9 Akses ke halaman bawaan <i>Apache2</i> | 45 |
| Gambar 3. 10 Akses ke aset situs dengan indeks opsi <i>Apache2</i> | 46 |
| Gambar 3. 11 Riwayat akses tidak valid yang berulang | 47 |
| Gambar 3. 12 Kode sumber berkas konfigurasi filter <i>Fail2ban</i> | 48 |
| Gambar 3. 13 Kode sumber berkas konfigurasi <i>jail Fail2ban</i> | 49 |
| Gambar 3. 14 Kode sumber berkas <i>C</i> | 50 |
| Gambar 3. 15 Kode sumber definisi fungsi pemeriksaan indeks opsi | 51 |
| Gambar 3. 16 Kode sumber tindakan untuk skenario indeks opsi pertama | 52 |
| Gambar 3. 17 Kode sumber tindakan untuk skenario indeks opsi kedua | 52 |
| Gambar 3. 18 Kode sumber untuk kerentanan indeks opsi yang tidak ditemukan | 53 |
| Gambar 3. 19 Kode sumber deklarasi fungsi remediasi izin akses | 54 |
| Gambar 3. 21 Kode sumber eksekusi pembenahan izin akses | 55 |
| Gambar 3. 22 Kode sumber fungsi memuat ulang layanan <i>Apache2</i> dan <i>Fail2ban</i> | 55 |
| Gambar 3. 23 Kode sumber fungsi utama pemindaian dan pembenahan <i>Apache2</i> | 56 |
| Gambar 3. 24 Kode sumber deklarasi waktu, <i>log</i> , dan direktori basis | 57 |
| Gambar 3. 25 Kode sumber fungsi pemeriksaan eksistensi <i>Apache2</i> | 57 |
| Gambar 3. 26 Kode sumber fungsi pemeriksaan eksistensi <i>Fail2ban</i> | 57 |
| Gambar 3. 27 Kode sumber fungsi instalasi <i>Fail2ban</i> | 57 |
| Gambar 3. 28 Kode sumber fungsi konfigurasi <i>Fail2ban</i> | 58 |

| | |
|---|----|
| Gambar 3. 29 Kode sumber fungsi utama sistem otomasi..... | 59 |
| Gambar 3. 30 Kode sumber fungsi pembuatan laporan sederhana..... | 60 |
| Gambar 3. 31 Alur kerja sistem otomasi..... | 60 |
| Gambar 4. 1 Hasil klon sistem otomasi dari repositori <i>github</i> | 71 |
| Gambar 4. 2 Hasil pemeriksaan isi direktori sistem otomasi sebelum eksekusi.... | 71 |
| Gambar 4. 3 Hasil eksekusi berkas utama dari sistem otomasi | 72 |
| Gambar 4. 4 Hasil pemeriksaan isi direktori sistem otomasi sesudah eksekusi | 72 |
| Gambar 4. 5 Hasil pemeriksaan isi direktori <i>log</i> dan laporan sistem otomasi..... | 73 |
| Gambar 4. 6 Hasil peninjauan isi laporan sistem otomasi | 74 |
| Gambar 4. 7 Hasil peninjauan isi <i>log</i> sistem otomasi..... | 75 |
| Gambar 4. 8 Hasil peninjauan isi konfigurasi sistus <i>web Apache2</i> pasca remediasi | 75 |
| Gambar 4. 9 Hasil peninjauan izin akses pasca remediasi..... | 76 |
| Gambar 4. 10 Hasil eksekusi sistem otomasi pada skenario tanpa kerentanan | 77 |
| Gambar 4. 11 Hasil tinjauan isi laporan sistem otomasi pada skenario tanpa kerentanan | 77 |
| Gambar 4. 12 Hasil tinjauan isi <i>log</i> sistem otomasi pada skenario tanpa kerentanan | 78 |
| Gambar 4. 13 Hasil pemeriksaan status <i>jail</i> aktif <i>Fail2ban</i> | 79 |
| Gambar 4. 14 Hasil peninjauan <i>jail apache-exploit-attempts</i> | 79 |
| Gambar 4. 15 Hasil peninjauan <i>log</i> dan <i>jail</i> pertama..... | 79 |
| Gambar 4. 16 Akses laman disertai " <i>!?=exec_file</i> "..... | 80 |
| Gambar 4. 17 Hasil peninjauan <i>log</i> dan <i>jail</i> kedua..... | 81 |
| Gambar 4. 18 Navigasi ke laman " <i>/wp-admin</i> " | 81 |
| Gambar 4. 19 Hasil peninjauan <i>log</i> dan <i>jail</i> ketiga..... | 82 |
| Gambar 4. 20 Akses ke aset situs <i>web</i> " <i>/asset</i> "..... | 82 |
| Gambar 4. 22 Navigasi ke " <i>/wp-admin/?=cmd_file</i> "..... | 83 |
| Gambar 4. 23 Akses ke " <i>/asset/?=wget_url</i> "..... | 84 |
| Gambar 4. 24 Hasil peninjauan <i>log</i> dan <i>jail</i> kelima..... | 84 |
| Gambar 4. 25 Akses laman <i>default</i> setelah pemlokiran..... | 85 |
| Gambar 4. 26 Pemuatan ulang layanan <i>Fail2ban</i> | 86 |
| Gambar 4. 27 Hasil peninjauan <i>log</i> dan <i>jail</i> keenam..... | 86 |
| Gambar 4. 28 Akses disertai " <i>!?=wget+https://github.com/XzByte/script-dev.git</i> " | 86 |
| Gambar 4. 29 Akses disertai " <i>!?=curl%20https://github.com/XzByte/script-dev.git</i> " | 87 |
| Gambar 4. 30 Akses disertai " <i>!?=shell+/root/aio-script/main.py</i> " | 87 |
| Gambar 4. 31 Akses disertai " <i>!?=cmd%20root/aio-script/main.py</i> " | 88 |
| Gambar 4. 32 Akses disertai " <i>!?=exec+/root/aio-script/main.py</i> " | 88 |
| Gambar 4. 33 Hasil peninjauan <i>log</i> dan <i>jail</i> ketujuh..... | 89 |

| | |
|--|-----|
| Gambar 4. 34 Hasil peninjauan <i>log</i> dan <i>jail</i> kedelapan | 90 |
| Gambar 4. 35 Hasil waktu pemeriksaan status layanan <i>Apache2</i> dan <i>Fail2ban</i> manual..... | 91 |
| Gambar 4. 36 Hasil waktu instalasi <i>Fail2ban</i> manual..... | 92 |
| Gambar 4. 37 Hasil waktu konfigurasi <i>jail</i> dan filter <i>Fail2ban</i> manual..... | 93 |
| Gambar 4. 38 Hasil waktu pembenahan konfigurasi situs <i>web Apache2</i> manual..... | 93 |
| Gambar 4. 39 Hasil waktu pembenahan izin akses manual..... | 94 |
| Gambar 4. 40 Hasil waktu pemuatan ulang layanan <i>Apache2</i> dan <i>Fail2ban</i> manual..... | 94 |
| Gambar 4. 41 Hasil waktu otomasi pertama..... | 95 |
| Gambar 4. 42 Hasil waktu otomasi kedua..... | 96 |
| Gambar 4. 43 Hasil waktu otomasi ketiga..... | 97 |
| Gambar 4. 44 Hasil waktu otomasi keempat..... | 98 |
| Gambar 4. 45 Hasil waktu otomasi kelima..... | 98 |
| Gambar 4. 46 Hasil waktu otomasi keenam..... | 99 |
| Gambar 4. 47 Hasil waktu otomasi ketujuh..... | 100 |
| Gambar 4. 48 Hasil waktu otomasi kedelapan..... | 100 |
| Gambar 4. 49 Hasil waktu otomasi kesembilan..... | 101 |
| Gambar 4. 50 Hasil waktu otomasi kesepuluh..... | 101 |
| Gambar 4. 51 Visualisasi perbandingan waktu dengan diagram batang..... | 103 |

INTISARI

Keamanan *web server* menjadi perhatian penting bagi UMKM, namun seringkali terkendala oleh anggaran untuk melakukan audit keamanan secara rutin. Penelitian ini memperkenalkan sebuah aplikasi yang dapat melakukan otomatisasi remediasi terhadap desain *web server* Apache yang tidak aman, dengan memanfaatkan fail2ban sebagai mekanisme deteksi dan mitigasi serangan. Aplikasi ini ditujukan untuk memudahkan UMKM dalam mengamankan web server mereka tanpa membutuhkan keahlian khusus atau anggaran besar. Aplikasi ini dapat dijalankan hanya dengan sekali eksekusi dan memiliki *footprint* yang sangat ringan, sehingga tidak memberatkan sumber daya yang ada pada infrastruktur UMKM. Dengan demikian, aplikasi ini dapat menjadi solusi praktis bagi UMKM untuk meningkatkan keamanan *web server* mereka tanpa perlu mengeluarkan biaya tambahan. Melalui analisis mendalam terhadap desain keamanan *web server* Apache yang rentan, aplikasi ini mampu mendeteksi *misconfiguration* dan celah keamanan sederhana yang umum ditemukan. Aplikasi ini kemudian melakukan perbaikan otomatis terhadap konfigurasi *web server*, seperti mengaktifkan *firewall*, mengatur pembatasan akses, hingga mengoptimalkan *logging* dan *monitoring*. Dengan kemampuan ini, aplikasi terbukti efektif dalam mengidentifikasi dan memitigasi ancaman keamanan yang sering menyerang *web server* UMKM. Penelitian ini berkontribusi dalam menyediakan solusi praktis dan terjangkau bagi UMKM untuk meningkatkan keamanan *web server* mereka. Aplikasi ini dapat menjadi alat bantu yang berharga bagi UMKM yang memiliki keterbatasan sumber daya, namun tetap membutuhkan perlindungan yang memadai terhadap kerentanan siber. Aplikasi ini mampu meningkatkan kecepatan dalam melakukan remediasi *Insecure Design (Misconfiguration)* dengan tingkat penurunan waktu yang dibutuhkan sebesar 43,98% dibandingkan dengan remediasi secara manual. Selain itu, *tools* ini dapat melakukan remediasi kerentanan yang ditargetkan dengan rasio keberhasilan atau *success rate* sebesar 100%

Kata kunci: Otomasi, Web, Keamanan Jaringan, fail2ban, Apache2

ABSTRACT

Web server security is an important concern for UMKM, but is often constrained by the budget to conduct regular security audits. This research introduces an application that can automate remediation of insecure Apache web server designs, by utilizing fail2ban as an attack detection and mitigation mechanism. This application is intended to make it easier for UMKM to secure their web servers without requiring special skills or a large budget. This application can be run with just one execution and has a very light footprint, so it does not burden existing resources in the MSME infrastructure. Thus, this application can be a practical solution for MSMEs to improve the security of their web servers without the need to spend additional costs. Through in-depth analysis of the security design of vulnerable Apache web servers, the application is able to detect simple misconfigurations and security holes that are commonly found. The app then performs automatic fixes to the web server configuration, such as enabling firewalls, setting access restrictions, and optimizing logging and monitoring. With these capabilities, the application proves effective in identifying and mitigating security threats that often attack UMKM web servers. This research contributes to providing practical and affordable solutions for UMKM to improve their web server security. This application can be a valuable tool for UMKM that have limited resources, but still need adequate protection against cyber security vulnerabilities. This application is able to increase the speed in remediating Insecure Design (Misconfiguration) with a decrease in the time required by 43.98% compared to manual remediation. In addition, this tool can remediate targeted vulnerabilities with a success rate of 100%.

Keyword: Automation, Web, Network Security, fail2ban, Apache2