202010370311139
Irfan Rosyadi
Prodi Informatika

Implementasi dan Evaluasi Sistem Pencegahan Serangan Brute Force pada Web Server Menggunakan Fail2ban

Tugas Akhir

Digunakan Untuk Memenuhi

Persyaratan Guna Meraih Gelar Sarjana

Informatika Universitas Muhammadiyah Malang

Irfan Rosyadi

(202010370311139)

Jaringan Komputer

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MALANG

2026

202010370311139
Irfan Rosyadi
Prodi Informatika

LEMBAR PERSETUJUAN

Implementasi dan Evaluasi Sistem Pencegahan Serangan Brute Force pada Web Server Menggunakan Fail2ban

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

Informatika Universitas Muhammadiyah Malang

Menyetujui,

Malang, *18 April 2026*

Dosen Pembimbing 1	Dosen Pembimbing 2
Ir. Mahar Faiqurahman S.Kom., M.T.	**Bashor Fauzan Muthohirin S.Kom., M.Kom**
NIP. 10808110462PNS.	**NIP. 20230126071994PNS.**

202010370311139
Irfan Rosyadi
Prodi Informatika

LEMBAR PENGESAHAN

Implementasi dan Evaluasi Sistem Pencegahan Serangan Brute Force pada Web Server Menggunakan Fail2ban

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang
Disusun Oleh :

Irfan Rosyadi

202010370311139

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 18 April 2026

Menyetujui,

Dosen Pembimbing 1	Dosen Pembimbing 2
Ir. Mahar Faiqurahman S.Kom., M.T.	**Bashor Fauzan Muthohirin S.Kom., M.Kom**
NIP. 10808110462PNS.	**NIP. 20230126071994PNS.**

Dosen Penguji 1	Dosen Penguji 2
Hardianto Wibowo S.Kom, MT.	**Ir. Wahyu Andhyka Kusuma S.Kom, M.Kom.**
NIP. 10816120592PNS.	**NIP. 10814100543PNS.**

Mengetahui,
Ketua Prodi Informatika

Ir. Agus Eko Minarno S.Kom., M.Kom. IPM.
NIP. 10814100540PNS.

LEMBAR PERNYATAAN

Bertanda tangan di bawah ini:

NAMA : **IRFAN ROSYADI**

NIM : **202010370311139**

FAK/JUR : **TEKNIK/INFORMATIKA**

Menyatakan bahwa Tugas Akhir dengan judul **"Implementasi dan Evaluasi Sistem Pencegahan Serangan Brute Force pada Web Server Menggunakan Fail2ban"** beserta seluruh isinya adalah karya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan seumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran etika terhadap etika keilmuan dalam karya say aini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk risiko/sanksi yang berlaku.

Mengetahui
Dosen Pembimbing

Mahar Faiqurahman S.Kom. M.T

Malang, 10 April 2026
Yang Membuat Pernyataan

Irfan Rosyadi

202010370311139
Irfan Rosyadi
Prodi Informatika

ABSTRAK

Web server merupakan komponen penting dalam layanan internet yang berfungsi melayani permintaan pengguna melalui protokol HTTP/HTTPS. Namun, web server juga rentan terhadap berbagai ancaman keamanan, salah satunya adalah serangan brute force pada halaman login web. Serangan ini dilakukan dengan mencoba berbagai kombinasi username dan password secara berulang hingga menemukan kredensial yang benar. Penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi Fail2Ban sebagai sistem pencegahan serangan brute force pada web login WordPress di lingkungan server virtual berbasis Linux. Metode penelitian yang digunakan adalah eksperimen dengan membandingkan kondisi sebelum penerapan Fail2Ban dan sesudah penerapan Fail2Ban, serta menguji variasi parameter maxretry, findtime, dan bantime untuk melihat pengaruhnya terhadap efektivitas pemblokiran dan potensi false positive. Hasil pengujian menunjukkan bahwa pada kondisi baseline tanpa Fail2Ban, serangan brute force dapat terus berjalan tanpa hambatan dengan total 420 percobaan login gagal dalam 10 menit. Setelah Fail2Ban diaktifkan dengan konfigurasi utama maxretry 5, findtime 10 menit, dan bantime 3 menit, alamat IP penyerang berhasil diblokir setelah 5 percobaan gagal dalam waktu 38 detik. Hasil variasi parameter menunjukkan bahwa konfigurasi yang lebih ketat mempercepat pemblokiran, tetapi meningkatkan risiko false positive, sedangkan konfigurasi yang lebih longgar lebih toleran terhadap pengguna normal namun memberi ruang lebih besar bagi penyerang. Dari sisi performa, penerapan Fail2Ban membantu menjaga kestabilan layanan login dengan menekan peningkatan beban server akibat percobaan login berulang. Berdasarkan hasil tersebut, Fail2Ban dinilai efektif sebagai mekanisme pencegahan dasar terhadap serangan brute force pada login WordPress dalam lingkungan uji terkontrol.

Kata kunci: brute force, Fail2Ban, WordPress, web server, keamanan server, virtual machine

202010370311139
Irfan Rosyadi
Prodi Informatika

ABSTRACT

A web server is an essential component of internet services that processes user requests through the HTTP/HTTPS protocol. However, web servers are also vulnerable to various security threats, one of which is brute force attacks targeting web login pages. This type of attack is carried out by repeatedly trying different combinations of usernames and passwords until valid credentials are found. This study aims to implement and evaluate Fail2Ban as a brute force prevention system for the WordPress login page in a Linux-based virtual server environment. The research method used is an experimental approach by comparing conditions before and after the implementation of Fail2Ban, as well as testing variations of the maxretry, findtime, and bantime parameters to examine their effect on blocking effectiveness and the potential for false positives. The test results show that under the baseline condition without Fail2Ban, brute force attacks could continue without interruption, reaching a total of 420 failed login attempts within 10 minutes. After Fail2Ban was activated using the main configuration of maxretry 5, findtime 10 minutes, and bantime 3 minutes, the attacker's IP address was successfully blocked after 5 failed attempts within 38 seconds. The parameter variation results indicate that stricter configurations accelerate blocking but increase the risk of false positives, while more lenient configurations are more tolerant of legitimate users but provide attackers with more opportunity to continue their attempts. In terms of performance, the implementation of Fail2Ban helped maintain login service stability by reducing the increase in server load caused by repeated login attempts. Based on these findings, Fail2Ban is considered effective as a basic prevention mechanism against brute force attacks on WordPress login pages in a controlled testing environment.

Keywords: brute force, Fail2Ban, WordPress, web server, server security, virtual machine

202010370311139
Irfan Rosyadi
Prodi Informatika

LEMBAR PERSEMBAHAN

Puji syukur kepada Allah SWT yang telah memberikan kemudahan serta kemudahan dalam berpikir, sehingga penyusunan skripsi ini dapat terselesaikan dengan baik dan bermanfaat bagi sesame. Skripsi ini saya persembahkan kepada :

1. Allah SWT yang senantiasa memberikan kesehatan dan petunjuk selama proses penyelesaian tugas akhir ini.
2. Orang tua saya yang sangat mendukung semua proses saya yaitu Bapak Sugianto dan Ibu Ismahmudah yang membesarkan saya dengan penuh kasih sayang dan selalu memberikan pendidikan yang terbaik sampai saat ini.
3. Para dosen Universitas Muhammadiyah Malang terutama Bapak Mahar Faiqurahman, S.Kom., M.T dan Bapak Bashor Fauzan Muthohirin, S.Kom., M.Kom yang sangat berjasa dalam membimbing saya dengan tulus dan sabar.
4. Bapak dan Ibu dosen Program Studi Informatika yang telah memberikan ilmu, pengalaman dan pembelajaran berharga selama masa perkuliahan.
5. Teman dan sahabat saya yang selalu memberikan motivasi kepada saya agar selalu bersemangat dalam menjalani kehidupan ini dan juga yang selalu menemani saya dalam menghadapi lika-liku selama masa perkuliahan;
6. Almamater tercinta Informatika Universitas Muhammadiyah Malang yang selalu saya banggakan.

202010370311139
Irfan Rosyadi
Prodi Informatika

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas segala rahmat, karunia, dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul **"Implementasi dan Evaluasi Sistem Pencegahan Serangan Brute Force pada Web Server Menggunakan Fail2Ban"** dengan baik. Tugas Akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Malang. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT yang telah memberikan kesehatan, kekuatan, dan kemudahan dalam setiap proses penyusunan Tugas Akhir ini.
2. Kedua orang tua dan keluarga tercinta yang selalu memberikan doa, kasih sayang, dukungan, dan semangat tanpa henti.
3. Bapak Mahar Faiqurahman, S.Kom., M.T**.** selaku Dosen Pembimbing I yang telah memberikan arahan, masukan, dan bimbingan selama proses penyusunan Tugas Akhir.
4. Bapak Bashor Fauzan Muthohirin, S.Kom., M.Kom**.** selaku Dosen Pembimbing II yang telah memberikan saran, kritik, dan dukungan dalam penyelesaian Tugas Akhir ini.
5. Seluruh Bapak dan Ibu dosen Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Malang, yang telah memberikan ilmu dan pengalaman selama masa perkuliahan.

Penulis menyadari bahwa Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun demi perbaikan pada masa yang akan datang. Penulis berharap semoga Tugas Akhir ini dapat memberikan manfaat bagi penulis sendiri, pembaca, serta pihak-pihak yang membutuhkan, khususnya dalam bidang keamanan jaringan.

202010370311139
Irfan Rosyadi
Prodi Informatika

DAFTAR ISI

202010370311139
Irfan Rosyadi
Prodi Informatika

DAFTAR GAMBAR

202010370311139
Irfan Rosyadi
Prodi Informatika

DAFTAR TABEL

DAFTAR PUSTAKA

[1] Y. Ramadhani and M. Sholeh, "Penerapan Tools Fail2Ban Untuk Mencegah Serangan Brute Force Pada Web Server Online Learning Uhamka (OLU)," J. Tek. Inform. dan Komput., vol. 1, no. 2, pp. 41–45, Nov. 2022, doi: 10.22236/JUTIKOM.V1I2.10447.

[2] F. Dawamsyach, I. Ruslianto, U. Ristian, P. Studi Rekayasa Sistem Komputer, and F. H. Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura Jalan Hadari Nawawi Pontianak, "Implementation of IPS (Intrusion Prevention System) Fail2ban on Server for DDoS and Brute Force Attacks," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 8, no. 1, pp. 149–161, Jan. 2023, doi: 10.24114/CESS.V8I1.40259.

[3] A. Rustianto, A. Fadillah, and J. Kasih, "Pencegahan dan Visualisasi Serangan Brute Force Menggunakan Fail2Ban, Prometheus, dan Grafana Studi Kasus di Sekolah Tinggi Teknologi Terpadu Nurul Fikri," *J. Publ. Tek. Inform.*, vol. 4, no. 2, pp. 195–209, May 2025, doi: 10.55606/JUPTI.V4I2.5144.

[4] N. D. Aji, N. D. Aji, T. T. Sujaka, Husain, O. Asroni, and K. A. Latif, "Analisis Dan Implementasi Algoritma Bcrypt Dengan Affine Cipher Untuk Pengamanan Password Pada Aplikasi Web: Analysis And Implementation Of Bcrypt Algorithm With Affine Cipher For Password Security In Web Applications," *Cyber Secur. dan Forensik Digit.*, vol. 8, no. 1, pp. 1–9, Jun. 2025, doi: 10.14421/csecurity.2025.8.1.5076.

[5] A. Tely, A. Aryanti, and S. Soim, "Sharing SSH Threat Intelligence across Multiple Servers using WebSocket and Fail2Ban," *ITEJ (Information Technol. Eng. Journals)*, vol. 10, no. 2, pp. 221–229, Jul. 2025, doi: 10.24235/ITEJ.V10I2.270.

[6] R. P. Aji, Y. Prayudi, and A. Luthfi, "ANALYSIS OF BRUTE FORCE ATTACK LOGS TOWARD NGINX WEB SERVER ON DASHBOARD IMPROVED LOG LOGGING SYSTEM USING FORENSIC INVESTIGATION METHOD," *J. Tek. Inform.*, vol. 4, no. 1, pp. 39–48, Feb. 2023, doi: 10.52436/1.JUTIF.2023.4.1.644.

[7] E. setiawan, E. setiawan, and fahmi fachri, "Pengujian dan Mitigasi Kerentanan Website Sistem Informasi Akademik Universitas Ma'arif Nahdlatul Ulama Kebumen dengan OWASP ZAP: Testing and Mitigation of Website Vulnerabilities in the Academic Information System of Universitas Ma'arif Nahdlatul Ulama …," *Cyber Secur. dan Forensik Digit.*, vol. 8, no. 1, pp. 25–33, Jun. 2025, doi: 10.14421/csecurity.2025.8.1.5190.

[8] A. D. Batistuta, A. Hendrawan, and Ritzkal, "ANALISIS KEAMANAN JARINGAN SERVER TERHADAP SERANGAN DICTIONARY

MENGGUNAKAN TOOLS FAIL2BAN DENGAN NOTIFIKASI TELEGRAM," *Infotech J.*, vol. 10, no. 1, pp. 64–73, Feb. 2024, doi: 10.31949/INFOTECH.V10I1.8730.

[9] R. William, I. Ruslianto, U. Ristian, J. Prof, H. Hadari, and N. Pontianak, "Implementation of Intrusion Prevention System (IPS) as a Website-Based Server Security System and Mobile Application," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 8, no. 1, pp. 123–137, Jan. 2023, doi: 10.24114/CESS.V8I1.40258.

[10] L. Benova, L. Hudec, L. Benova, and L. Hudec, "Comprehensive Analysis and Evaluation of Anomalous User Activity in Web Server Logs," *Sensors 2024, Vol. 24,* vol. 24, no. 3, Jan. 2024, doi: 10.3390/S24030746.

202010370311139
Irfan Rosyadi
Prodi Informatika

UNIVERSITAS MUHAMMADIYAH MALANG

FAKULTAS TEKNIK

INFORMATIKA
informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **Irfan Rosyadi**

NIM : **202010370311139**

Judul TA : **Implementasi dan Evaluasi Sistem Pencegahan Serangan Brute Force pada Web Server Menggunakan Fail2Ban**

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	1%
2.	Bab 2 – Daftar Pustaka	25 %	2%
3.	Bab 3 – Analisis dan Perancangan	25 %	2%
4.	Bab 4 – Implementasi dan Pengujian	15 %	2%
5.	Bab 5 – Kesimpulan dan Saran	5 %	4%
6.	Makalah Tugas Akhir	20%	5%

) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

***) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)**

Mengetahui,

Pemeriksa (Staff TU)

(.....)

Kampus I
Jl. Bandung 1 Malang, Jawa Timur
P: +62 341 551 253 (Hunting)
F: +62 341 460 435

Kampus II
Jl. Bendungan Sutami No.188 Malang, Jawa Timur
P: +62 341 551 149 (Hunting)
F: +62 341 582 060

Kampus III
Jl. Raya Tlogomas No.246 Malang, Jawa Timur
P: +62 341 464 318 (Hunting)
F: +62 341 460 435
E: webmaster@umm.ac.id