PENERAPAN MODSECURITY, FAIL2BAN, IPTABLES, DAN RULE OWASP UNTUK MENINGKATKAN KEAMANAN WEB

TUGAS SKRIPSI

Sebagai salah satu syarat untuk memperoleh gelar Sarjana S-1

Program Studi Informatika

Muhammad Chabib Al Rahman

NIM 20106050064

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2024

HALAMAN PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1462/Un.02/DST/PP.00.9/08/2024

Tugas Akhir dengan judul : PENERAPAN MODSECURITY, FAIL2BAN, IPTABLES, DAN RULE OWASP UNTUK MENINGKATKAN KEAMANAN WEB

yang dipersiapkan dan disusun oleh:

Nama : MUHAMMAD CHABIB AL RAHMAN
Nomor Induk Mahasiswa : 20106050064
Telah diujikan pada : Senin, 05 Agustus 2024
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 66bdb45a627ed

Penguji I

Dr. Ir. Sumarsono, S.T., M.Kom.
SIGNED

Valid ID: 66bda055dac85

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 66bb023541cd3

Yogyakarta, 05 Agustus 2024
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 66c2d944c8a0b

SURAT PERNYATAAN KEASLIAN

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Chabib Al Rahman
NIM : 20106050064
Program Studi : Informatika
Fakultas : Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 24 Juli 2024

Munammad Chabib Al Rahman

NIM. 20106050064

SURAT PERSETUJUAN TUGAS AKHIR

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhammad Chabib Al Rahman
NIM : 20106050064
Judul Skripsi : PENERAPAN MODSECURITY, FAIL2BAN, IPTABLES DAN RULE OWASP UNTUK MENINGKATKAN KEAMANAN WEB

sudah dapat diajukan kembali kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Matematika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 24 Juli 2024

Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM
NIP. 19751024200912100 2

LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga Yogyakarta, diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta.

INTISARI

Era digital telah mempermudah komunikasi dan akses informasi, tetapi juga meningkatkan risiko ancaman siber seperti SQL Injection dan Cross-Site Scripting (XSS). Situs web dan aplikasi online, termasuk yang dikelola oleh pemerintah di Indonesia, sering menjadi target serangan yang dapat mengekspos data sensitif dan merusak sistem.

Penelitian ini bertujuan untuk meningkatkan keamanan web dengan menerapkan ModSecurity, Iptables, Fail2ban, dan aturan OWASP pada server Apache. Tujuannya adalah untuk mendeteksi, memblokir serangan siber, dan mencegah akses tidak sah.

Metodologi penelitian mengikuti metode SDLC (System Development Life Cycle) yang meliputi tahapan Analisis Kebutuhan, Desain, Implementasi, Pengujian, Evaluasi, dan Kesimpulan. Hasilnya menunjukkan bahwa kombinasi alat ini secara signifikan meningkatkan perlindungan, dengan efektivitas deteksi dan pemblokiran serangan yang baik. Evaluasi juga menunjukkan bahwa tanpa firewall terdapat kerentanan, sedangkan setelah penerapan, tidak ada kerentanan yang terdeteksi. Rekomendasi termasuk pembaruan perangkat lunak rutin dan peningkatan kesadaran keamanan.

Kata Kunci: Keamanan web, ModSecurity, SQL Injection, XSS, SDLC

ABSTRACT

The digital era has facilitated communication and access to information but has also increased the risk of cyber threats such as SQL Injection and Cross-Site Scripting (XSS). Websites and online applications, including those managed by the Indonesian government, often become targets of attacks that can expose sensitive data and damage systems.

This research aims to enhance web security by implementing ModSecurity, Iptables, Fail2ban, and OWASP rules on an Apache server. The goal is to detect and block cyber attacks and prevent unauthorized access.

The methodology follows the SDLC (System Development Life Cycle) approach, including the phases of Requirements Analysis, Design, Implementation, Testing, Evaluation, and Conclusion. The results show that this combination of tools significantly improves protection, with effective detection and blocking of attacks. Evaluation also indicates that vulnerabilities existed without the firewall, whereas no vulnerabilities were detected after its implementation. Recommendations include regular software updates and increased security awareness among web administrators.

Keyword: Web security, ModSecurity, SQL Injection, XSS, SDLC

MOTTO

"Tidak ada mimpi yg gagal yg ada hanyalah mimpi yg tertunda, cuma sekiranya kalau teman-teman merasa gagal dalam mencapai mimpi, jangan khawatir mimpi-mimpi lain bisa diciptakan."

Brando Franco Windah

"There Are Two Main Human Sins from Which All the Others Derive: Impatience and Indolence."

Franz Kafka

HALAMAN PERSEMBAHAN

Tugas akhir ini penulis persembahkan untuk:

1. Kedua orang tua saya Bapak Muhamad Masturi dan Ibu Siti Maimunatun Naqibah yang telah berjuang menjadi orang tua yang memberikan yang terbaik untuk anak anaknya. Terimakasih sudah memberikan dukungan baik materi maupun moral yang tidak bisa saya hitung semua.
2. Kepada kakak saya Ahmad Fadil Irvan dan 2 adik saya Naila Ruhma Aizatin dan Hulwa Amali atas dukungannya sampai hari ini.
3. Kepada Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM. Selaku dosen pembimbinga saya yang telah mencurahkan waktu, tenaga, dan pikirannya sehingga saya menyelesaikan penulisan tugas akhir ini.
4. Bapak dan Ibu dosen Informatika yang telah mendidik serta memberikan ilmu selama saya belajar di UIN Sunan Kalijaga Yogyakarta.
5. Teman teman jurusan Informatika angkatan 2020 UIN Sunan Kalijaga Yogyakarta.
6. Semua Pihak yang tidak dapat di sebutkan satu persatu, yang turut membantu memberikan arahan, serta dukungan dalam menyelesaikan tugas akhir ini.
7. Terakhir kepada diri saya sendiri, terima kasih sudah berkerja keras, tidak menyerah dan sudah bertahan hingga saat ini. Terima kasih sudah menjaga diri dan selalu berusaha memberikan yang terbaik.

KATA PENGANTAR

Penulis mengucapkan puji dan syukur kepada Allah Swt. karena telah melimpahkan berkah dan nikmat yang tidak terhingga, sehingga tugas akhir "Penerapan Modsecurity, Fail2ban, Iptables, dan Rule Owasp untuk Meningkatkan Keamanan Web" dapat diselesaikan. Tugas akhir ini juga dapat diselesaikan atas bantuan berbagai pihak. Untuk itu penulis ingin menyampaikan terima kasih kepada semua pihak yang berjasa berikut ini.

1. Allah SWT, yang selalu memberi rahmat, hidayah, dan kesejahteraan kepada penulis, sehingga mereka dapat menyelesaikan tugas akhir ini sampai selesai.
2. Bapak Prof. Dr. Phil. Al Makin, S.Ag., MA., selaku Rektor Universitas Islam Negri Sunan Kalijaga Yogyakarta.
3. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negri Sunan Kalijaga Yogyakarta.
4. Ibu Maria Ulfah Siregar, S.Kom., MIT., Ph.D. selaku Ketua Program Studi Informatika Fakultas Sains dan Teknologi Universitas Islam Negri Sunan Kalijaga Yogyakarta.
5. Bapak Mandahadi Kusuma, M.Eng., selaku dosen pembimbing akademik yang senantiasa membantu dan mengarahkan penulis selama berada di bangku perkuliahan.
6. Bapak Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., selaku dosen pembimbing skripsi yang selalu bersedia meluangkan waktu untuk memberikan arahan, bimbingan, dan motivasi untuk menyelesaikan dan menyempurnakan penulisan tugas akhir ini.
7. Bapak dan Ibu dosen pada Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta, yang telah memberikan banyak ilmu
8. Kedua orang tua saya Bapak Muhamad Masturi dan Ibu Siti Maimunatun Naqibah yang telah memberikan dukungan sehingga saya dapat menyelesaikan penulisan ini.

9. Kakak saya Ahmad Fadil Irvan dan 2 adik saya Naila Ruhma Aizatin dan Hulwa Amali yang telah memberikan dukungan.
10. Andhika, eko, adi surya, setyo, Khatga, Niksan, dan Uben selaku teman-teman Bolo Kurowo yang telah menemani dan membantu penulis selama masa studi.
11. Petrus selaku kucing teman saya yang telah menemani selama masa studi.
12. Tazki, Yusuf, Cendika, Zuhdi, Azzam, dan ega selaku teman-teman Server Mr. Universe yang telah memberi banyak masukan dan membantu penulis dalam mengerjakan tugas akhir ini.
13. Temen-teman Program studi Informatika angkatan 2020 yang selalu memberikan semangat dan dukungannya untuk penulis.

Akhirnya, besar harapan penulis agar tugas akhir ini dapat memberikan kontribusi positif dalam kajian ilmu informatika. Penulis menyadari banyak kekurangan yang terdapat di dalam tugas akhir ini. Oleh sebab itu, penulis menerima kritik dan saran yang membangun sebagai upaya perbaikan dan pengembangan ke arah yang lebih baik.

Yogyakarta, 01 Agustus 2024

Muhammad Chabib Al Rahman

DAFTAR ISI

HALAMAN PENGESAHAN ii
SURAT PERNYATAAN KEASLIAN iii
SURAT PERSETUJUAN TUGAS AKHIR iv
LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR v
INTISARI vi
ABSTRACT vii
MOTTO viii
HALAMAN PERSEMBAHAN ix
KATA PENGANTAR x
DAFTAR ISI xii
DAFTAR GAMBAR xv
DAFTAR TABEL xvi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah 5
1.4 Tujuan Penelitian 6
1.5 Manfaat Penelitian 6
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI 7
2.1 Tinjauan Pustaka 7
2.2 Landasan Teori 12
2.2.1 Keamanan Siber 12
2.2.2 Proxmox Virtual Environment 13
2.2.3 IP Address 13

2.2.4 Web Server 14
2.2.5 Apache 15
2.2.6 Firewall 15
2.2.7 Fail2Ban 16
2.2.8 IPtables 17
2.2.9 Web Application Firewall 18
2.2.10 ModSecurity 19
2.2.11 OWASP 19
2.2.12 Metode SDLC 20
2.2.13 Penetrasi Testing 20
BAB III METODE PERANCANGAN SISTEM 21
3.1 Jenis Penelitian 21
3.2 Teknik Pengumpulan Data 21
3.3 Studi Literatur 21
3.4 Tempat dan Waktu Penelitian 22
3.5 Alat dan Bahan Penelitian 23
3.5.1 Hardware (Perangkat Keras) 23
3.5.2 Software (Perangkat Lunak) 23
3.6 Alur Penelitian dan Evaluasi 24
3.6.1 Analisis Kebutuhan 25
3.6.2 Desain 26
3.6.3 Implementasi 26
3.6.4 Pengujian 27
3.6.5 Evaluasi 28
BAB IV PERANCANGAN DAN EVALUASI SISTEM 29

4.1 Analisis Kebutuhan 29
4.2 Desain 29
4.3 Implementasi 30
4.4 Pengujian 47
4.5 Evaluasi 50
4.5.1 Sebelum Implementasi 50
4.5.2 Setelah Implementasi 56
BAB V PENUTUP 64
5.1 Kesimpulan 64
5.2 Saran 65
Daftar Pustaka 66
DAFTAR RIWAYAT HIDUP 71

DAFTAR GAMBAR

Gambar 1. Web Server Tanpa Firewall 16
Gambar 2. Web Server Dengan Firewall 16
Gambar 3. Alur Penelitian 25
Gambar 4. Analisis Kebutuhan 29
Gambar 5. Desain 30
Gambar 6. Instalasi Apache 32
Gambar 7. Konfigurasi Phpmyadmin 34
Gambar 8. Aktivasi Modsecurity 36
Gambar 9. Konfigurasi Rule di Apache 37
Gambar 10. Konfigurasi Rule di Apache 37
Gambar 11. Rule SQLI 38
Gambar 12. Rule XSS 40
Gambar 13. Percabaan Pertama Instalasi Framewok 41
Gambar 14. Id yang Aktif Ketika Instalasi Framework 42
Gambar 15. Konfigurasi Rule 43
Gambar 16. Percobaan Instalasi Sesudah Konfigurasi 44
Gambar 17. Konfigurasi Fail2ban untuk Membaca Log Modsecurity 45
Gambar 18. Konfigurasi Fail2ban 46
Gambar 19. Percobaan Akses 48
Gambar 20. Percobaan Akses 49

DAFTAR TABEL

Tabel 1. Studi Literatur 7
Tabel 2. Perbedaan firewall dan WAF 18
Tabel 3. Spesifikasi VM 31
Tabel 4. Status Serangan 50
Tabel 5. Ringkasan OWASP Zap 50
Tabel 6. Status Serangan 55
Tabel 7. Ringkasan Scan OWASP Zap 56
Tabel 8. Status Serangan 61
Tabel 9. Perbandingan Hasil 62

BAB I
PENDAHULUAN

1.1 Latar Belakang

Era digital ini telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan manusia. Perkembangan teknologi dan internet yang pesat mengubah cara manusia berkomunikasi, bekerja, belajar, dan berinteraksi, membuatnya menjadi lebih efisien dan mudah di akses. Misalnya, dibidang pendidikan, platform e-learning berbasis web memungkinkan akases pembelajaran kepada siswa di seluruh dunia. Situs web dan aplikasi online dari pemerintah juga memungkinkan untuk mencari informasi dan mempermudah masyarakat dalam mengurus administrasi.

Di balik kemajuan pesat dari perkembangan teknologi ini juga di barengi dengan ancaman siber yang semakin banyak. Hal tersebut menjadi fokus utama karena aktivitas semakin bergantung pada teknologi dan internet. Ancaman siber dapat mencakup serangan yang berpotensi merusak sistem, malware yang dapat mencuri data, dan ancaman lainnya. Ancaman siber merupakan tantangan nyata, dan upaya untuk melindungi jaringan dan sistem digital menjadi sangat penting untuk memastikan keberlanjutan dan keamanan dalam dunia digital yang terus berkembang [1].

Ada banyak kerugian yang dialami dari serangan siber yang mengancam keamanan web ini. Diantaranya adalah ancaman keamanan data pribadi dapat berupa kerusakan, kehilangan data, pencurian, atau bahkan penyalahgunaan. Resiko yang diakibatkan dari ancaman ini juga mengakibatkatkan gangguan operasional, yang berdampak ke kerugian finansial bagi organisasi, instansi bahkan sampai pengguna. Selain itu, organisasi atau instansi akan kehilangan reputasi dan kehilangan kepercayaan yang berdampak jangka panjang [2], [3], [4].

Di Indonesia sendiri telah terjadi banyak serangan serangan siber. Menurut laman zone-h [5]., lebih dari 10.000 laman web dengan domain go.id telah terserang serangan defacement web, yaitu serangan terhadap situs web yang merubah

tampilan visual halman web. Serangan defacement mengeksploitasi kelemahan situs web atau server untuk mengubah konten halaman web, biasanya untuk alasan pribadi atau politik. Dampak dari serangan ini dapat menyebabkan kerugian finansial dan reputasi, serta menimbulkan masalah politik dan ekonomi[6]. Pada tahun 2019, persentase insiden siber yang dilaporkan oleh Gov-CSIRT Indonesia kerentanan menjadi kategori insiden siber dengan persentase tertinggi, yaitu 63% dengan 66 insiden di Pemerintah Pusat dan 37% dengan 38 insiden di Pemerintah Daerah Wilayah I. Insiden web defacement dilaporkan pada 14% kasus di Pemerintah Pusat dengan 15 insiden dan 33% di Pemerintah Daerah Wilayah I dengan 34 insiden. Insiden malware terjadi pada 9% kasus di Pemerintah Pusat dengan 10 insiden dan 13% di Pemerintah Daerah Wilayah I dengan 13 insiden. Kategori phishing dilaporkan pada 5% insiden di Pemerintah Pusat dengan 5 insiden, sedangkan kategori lain-lain mencakup 9% insiden dengan 9 kasus di Pemerintah Pusat [7].

Ada banyak cara untuk melindungi aplikasi web dari serangan serangan siber, seperti penggunaan Web application Firewall (WAF) untuk melindungi web server dari serangan atau akses yang tidak diizinkan [8]. SSL Encryption yang memastikan mengenkripsi data yang dikirim antara server master dan server slave, sehingga mencegah penyadapan oleh pihak ketiga [9]. Selain itu, memperbaharui perangkat lunak secara rutin juga merupakan langkah untuk menutup celah yang bisa di exploitasi oleh penyerang. Implementasi sistem deteksi dan pencegahan intrusi (IDS/IPS) juga membantu dalam menjaga keamanan jaringan dengan mendeteksi dan mencegah serangan sebelum aplikasi web mengalami kerusakan [10]. Melakukan backup berkala adalah tindakan penting untuk memastikan data bisa dipulihkan jika terjadi kehilangan. Penggunaan CAPTCHA untuk mencegah akses otomatis yang digunakan dalam serangan seperti DDOS dan pencurian data [11]. Konfigurasi keamanan server web yang tepat dan pemindaian keamanan berkala memastikan bahwa semua potensi kerentanan diidentifikasi dan diperbaiki. Penggunaan Honeypot juga berfungsi sebagai umpan untuk mendeteksi dan melindungi server yang sebenarnya [12].

Dari berbagai metode tersebut, penggunaan Web Application Firewall (WAF) menjadi salah satu yang sangat efektif dikarenakan firewall merupakan garis pertahanan pertama dalam mencegah serangan [13]. Web Application Firewall (WAF) adalah bagian dari strategi keamanan yang lebih luas yang mencakup IDS/IPS, SSL, dan CAPTCHA, dimana masing-masing menangani aspek keamanan yang berbeda. IDS/IPS mendeteksi dan mencegah intrusi, SSL mengamankan transmisi data, dan CAPTCHA membedakan manusia dari bot. Web Application Firewall (WAF) adalah metode keamanan yang di rancang untuk melindungi aplikasi web dan mencegah serangan siber. Implementasi WAF ini dapat di lakukan tanpa merubah konfigurasi pada server web, sehingga tidak memerlukan perubahan pada script aplikasi yang sudah berjalan. Hal ini sangat menguntungkan integrasi antara WAF dan server web lebih mudah. Manfaat dari penggunaan WAF ini adalah menciptakan keamanan yang dapat mendeteksi dan mencegah serangan terhadap aplikasi web [14]. WAF berkerja dengan memfilter lalulintas data yang masuk dan keluar dari web server bedasarkan aturan keamanan yang di tetapkan [8].

ModSecurity, Iptables, fail2ban, dan penerapan rule OWASP adalah beberapa solusi firewall yang dapat di kombinasikan untuk perlindungan aplikasi web. Keunggulan memakai ModSecurity adalah kemampuannya yang kuat dalam merespons berbagai peristiwa atau kejadian yang terjadi selama pemantauan dan perlindungan aplikasi web. Hal ini memungkinkan ModSecurity untuk memberikan perlindungan yang efektif dari berbagai serangan terhadap aplikasi web. Fungsi ModSecurity tidak hanya sebatas memantau lalu lintas HTTP, tetapi juga mencakup kemampuan logging dan analisis data secara real-time [15]. Kelebihan lain dari ModSecurity adalah fleksibilitas dalam implementasinya. ModSecurity dapat diimplementasikan dengan berbagai aturan sesuai kebutuhan seperti mengimplementasikan rule OWASP. Dengan demikian, serangan-sreangan, termasuk serangan SQL injection dan XSS tidak lagi menjadi ancaman.

Selain itu, mengkonfigurasi fail2ban dan Iptables untuk mengatur mengendalikan lalulintas jaringan yang masuk. Fail2ban dan Iptables adalah solusi

untuk melindungi server web dari upaya akses tidak sah. Penggunaan fail2ban dapat untuk memblokir alamat ip mencurigakan setelah mendeteksi aktivitas yang tidak biasa [2]. Fail2ban juga memungkinkan untuk membaca special log seperti log dari modsecurity. Sedangkan Iptables mengatur lalu lintas masuk dan keluar bedasarkan aturan yang di tentukan. Keduanya saling melengkapi, fail2ban menggunakan iptables untuk menerapkan aturan blokir terhadap IP yang melakukan serangan [16].

Kemudian mengimplementasikan rule yang disediakan oleh OWASP (Open Web Application Security Project) sebagai panduan keamanan aplikasi web. Sebagai komunitas yang bersekala international, OWASP berfokus pada keamanan aplikasi web yang menyediakan pedoman yang di perlukan untuk mengidentifikasi kerentanan sistem [17]. OWASP menyediakan aturan yang telah teruji dan terbukti dalam melindungi aplikasi web dari serangan yang umum terjadi, seperti SQL Injection dan Cross-Site Scripting (XSS). Aturan-aturan ini akan terapkan dengan cermat dan mengintegrasikannya dengan infrastruktur web.

Dengan mengimplementasikan ModSecurity, Iptables, Fail2ban, dan aturan OWASP, diharapkan penelitian ini dapat menghasilkan web yang lebih aman dari serangan siber. Tujuan utamanya adalah untuk meningkatkan keamanan web dalam mencegah serangan umum seperti SQL Injection dan Cross-Site Scripting (XSS).

1.2 **Rumusan Masalah**

Berdasarkan latar belakang yang telah dijelaskan, ditemukan bahwa web server sering kali memiliki kelemahan dalam mendeteksi dan merespons berbagai serangan siber, termasuk serangan SQL injection dan Cross-Site Scripting (XSS). Maka dari itu, peneliti menetapkan rumusan masalah sebagai berikut:

1. Bagaimana cara mencegah serangan SQL injection dan XSS untuk meningkatkan keamanan web dengan menggunakan ModSecurity, Fail2ban, dan Iptables dan rule owasp?

2. Bagaimana konfigurasi ModSecurity dengan aturan OWASP dapat dilakukan pada aplikasi berbasis framework untuk meningkatkan keamanan web secara keseluruhan?

Penelitian ini bertujuan untuk menjawab kedua pertanyaan tersebut guna memperkuat keamanan web server dari berbagai ancaman siber.

1.3 **Batasan Masalah**

Penelitian ini menambahkan beberapa batasan masalah agar fokus penelitian tidak bergeser dan tetap terarah. Beberapa batasan masalah yang ditambahkan adalah sebagai berikut:

1. Aplikasi web server yang digunakan adalah Apache.
2. Pengujian dilakukan menggunakan lingkungan virtual machine yang dibangun dalam server Proxmox.
3. Hasil yang diharapkan dari penelitian ini adalah peningkatan keamanan web dengan menggunakan ModSecurity, Iptables, Fail2ban, dan aturan OWASP.
4. Serangan yang diuji menggunakan konsep penetration testing berupa serangan SQL Injection dan Cross-Site Scripting (XSS).
5. Penelitian ini hanya menggunakan ModSecurity, Iptables, dan Fail2ban sebagai alat keamanan utama.
6. Implementasi aturan keamanan mengikuti panduan dari OWASP (Open Web Application Security Project).
7. Pengujian dilakukan dalam lingkungan tertutup dan terkontrol, tidak mencakup pengujian serangan fisik atau non-siber.
8. Integrasi hanya dilakukan dengan teknologi firewall dari Linux, tidak mencakup integrasi dengan sistem operasi atau perangkat keras lainnya.
9. Pengujian dilakukan dengan akses terbatas hanya pada lingkungan laboratorium di UIN Sunan Kalijaga.
10. Firewall bawaan dari Proxmox VE masih dalam keadaan aktif untuk semua host dan VM yang digunakan dalam penelitian ini.

11. Penggunaan Fail2ban dengan mekanisme pemblokiran IP dapat menyebabkan pemblokiran massal pada semua pengguna yang berbagi jaringan WiFi dengan satu alamat IP publik yang sama.

1.4 **Tujuan Penelitian**

Tujuan dari penelitian ini adalah untuk mengimplementasikan dan mengevaluasi sistem keamanan web server menggunakan ModSecurity, Iptables, Fail2ban, dan aturan OWASP. Dengan penelitian ini, diharapkan dapat:

1. Meningkatkan perlindungan keamana web yang lebih kuat dengan mencegah serangan siber, termasuk SQL injection dan XSS.
2. Dapat memberikan pengetahuan tentang cara mengkonfigurasi modsecurity dengan rule owasp di aplikasi framework

1.5 **Manfaat Penelitian**

Perancangan ini diharapkan memberikan manfaat dan membantu mengetahui tentang Keamanan web serta konfigurasinya, juga dapat memiliki dampak positif dalam hal keamanan dan memberikan panduan praktis yang dapat diimplementasikan untuk meningkatkan keamanan informasi dalam lingkungan digital yang semakin kompleks dan rentan terhadap serangan siber.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan dan pengujian yang telah dilakukan dalam penelitian dengan judul "Meningkatkan Keamanan Web dengan Penerapan ModSecurity, Fail2ban, Iptables, dan Rule OWASP," dapat disimpulkan sebagai berikut:

- Penerapan ModSecurity dengan aturan OWASP berhasil mendeteksi dan mencegah serangan SQL Injection (SQLi) dan Cross Site Scripting (XSS). Analisis perbandingan antara kedua hasil pengujian tersebut menunjukkan bahwa penggunaan firewall secara signifikan meningkatkan keamanan sistem. Tanpa firewall, beberapa kerentanan ditemukan yang dapat dieksploitasi oleh penyerang, terutama melalui SQL Injection dan manipulasi User Agent. Namun, setelah pemasangan firewall, tidak ada kerentanan yang terdeteksi, menunjukkan bahwa firewall efektif dalam mencegah serangan tersebut. Durasi pengujian yang lebih lama dan jumlah permintaan yang lebih sedikit pada sistem yang menggunakan firewall menunjukkan bahwa firewall tidak hanya melindungi tetapi juga mengelola lalu lintas jaringan dengan baik. Oleh karena itu, penggunaan firewall dan aturan OWASP sangat direkomendasikan untuk mencegah ancaman siber.
- ModSecurity dengan aturan OWASP berhasil diterapkan dan diuji pada aplikasi web dengan framework. Konfigurasi ini memberikan lapisan keamanan yang kuat terhadap berbagai jenis serangan yang sering terjadi, seperti yang ada dalam pemindaian OWASP ZAP. Tidak ada kerentanan yang terdeteksi setelah konfigurasi ini diterapkan. Penelitian ini juga menjawab bagaimana cara konfigurasi ModSecurity agar mengabaikan aturan-aturan tertentu untuk URI yang sesuai. Hal ini penting untuk mencegah munculnya kesalahan 403 (Forbidden) ketika framework web diinstal, sehingga framework dapat berfungsi dengan baik tanpa dikompromikan oleh aturan keamanan yang ketat.

5.2 **Saran**

Berdasarkan penelitian dan perancangan ini masih memiliki banyak kekurangan dan masih diperlukan pengembangan yang lebih baik lagi. Ada beberapa saran yang penulis usulkan sebagai mana dibawah

- Pengujian dengan jenis serangan lainnya seperti Distributed Denial of Service (DDoS), Command Injection, dan serangan brute force yang lebih canggih. Pengujian ini akan memberikan gambaran yang lebih komprehensif tentang kekuatan dan kelemahan sistem keamanan yang telah diterapkan. Penggunan alat-alat lain selain OWASP ZAP, seperti Burp Suite atau Nessus, juga dapat membantu dalam mengidentifikasi celah keamanan yang mungkin terlewatkan oleh OWASP ZAP.
- Disarankan untuk melakukan evaluasi terhadap potensi beban yang ditimbulkan oleh ModSecurity, Iptables, dan Fail2ban pada server. Meskipun alat-alat ini memberikan perlindungan yang signifikan, penting untuk memastikan bahwa mereka tidak mengurangi kinerja aplikasi web secara keseluruhan. Pengujian kinerja dan pemantauan penggunaan sumber daya sistem harus dilakukan untuk memastikan bahwa server dapat menangani beban tambahan yang diakibatkan oleh penerapan alat-alat keamanan ini.

Daftar Pustaka

[1] I. Farid, A. H. Reksoprodjo, and S. Suhirwan, "PEMANFAATAN ARTIFICIAL INTELLIGENCE DALAM PERTAHANAN SIBER," *NUSANTARA : Jurnal Ilmu Pengetahuan Sosial*, vol. 10, no. 2, Art. no. 2, Apr. 2023, doi: 10.31604/jips.v10i2.2023.779-788.

[2] A. D. Batistuta, A. H. Hendrawan, and Ritzkal, "ANALISIS KEAMANAN JARINGAN SERVER TERHADAP SERANGAN DICTIONARY MENGGUNAKAN TOOLS FAIL2BAN DENGAN NOTIFIKASI TELEGRAM," *INFOTECH journal*, vol. 10, no. 1, Art. no. 1, Feb. 2024, doi: 10.31949/infotech.v10i1.8730.

[3] A. Nurain, R. A. Gultom, and R. E. Indrajit, "Manajemen Ketahanan Risiko Siber pada Internet of Things dan Cyber Physical System," *Journal on Education*, vol. 6, no. 2, pp. 13271–13281, 2024.

[4] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "Manajemen Keamanan Cyber di Era Digital," *Journal of Business And Entrepreneurship*, vol. 11, no. 1, pp. 23–33, 2023.

[5] "Zone-H.org - Unrestricted information | Special Defacements archive." Accessed: Jun. 21, 2024. [Online]. Available: https://www.zone-h.org/archive

[6] M. Albalawi, R. Alouf, N. Alamrani, N. Albalawi, A. Aljaedi, and A. R. Alharbi, "Website Defacement Detection and Monitoring Methods: A Review," Nov. 2022, Accessed: Jun. 22, 2024. [Online]. Available: https://doi.org/10.3390/electronics11213573

[7] Badan Siber dan Sandi Negara, "LAPORAN TAHUNAN GOV-CSIRT BSSN 2019." Accessed: Jun. 22, 2024. [Online]. Available: https://www.bssn.go.id/laporan-tahunan-gov-csirt-bssn-2019/

[8] G. H. A. Kusuma, “Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19,” *Journal of Informatics and Advanced Computing (JIAC)*, vol. 2, no. 2, pp. 1–4, 2021.

[9] H. Yuliansyah, “Perancangan replikasi basis data mysql dengan mekanisme pengamanan menggunakan ssl encryption,” *Jurnal Informatika*, vol. 8, no. 1, pp. 826–836, 2014.

[10] M. I. Iqbal and H. Harfani, “IMPLEMENTASI PFSENSE-SNORT PADA SISTEM PENCEGAHAN INTRUSI JARINGAN KOMPUTER PADA PT LINTAS TEKNOLOGI INDONESIA,” *Jurnal Informatika Software dan Network (JISN)*, vol. 4, no. 2, 2023.

[11] J. Hansen and T. Sutabri, “Mendesain Cyber Security Untuk Mencegah Serangan DDoS Pada Website Menggunakan Metode Captcha,” *Digital Transformation Technology*, vol. 3, no. 1, pp. 289–298, 2023.

[12] Z. Fuada, “Penerapan keamanan jaringan menggunakan sistem snort dan honeypot sebagai pendeteksi dan pencegah malware,” 2024.

[13] P. Marcillo, D. Maldonado-Ruiz, S. Arrais, L. I. B. López, and A. L. V. Caraguay, “Trends on computer security: cryptography, user authentication, denial of service and intrusion detection,” *Latin-American Journal of Computing*, vol. 6, no. 1, pp. 39–50, 2019.

[14] R. Riska and H. Alamsyah, “Penerapan Sistem Keamanan Web Menggunakan Metode Web Aplication Firewall,” *j. amp. : j. ilm. bid. tek. elect. and comp.*, vol. 11, no. 1, Art. no. 1, Jul. 2021, doi: 10.33369/jamplifier.v11i1.16683.

[15] M. R.-175410054 Siregar, “MEMBANGUN WEB APPLICATION FIREWALL DENGAN FILTER MODSECURITY SEBAGAI UPAYA PENGAMANAN WEBSITE,” skripsi, STMIK AKAKOM YOGYAKARTA, 2018. Accessed: Nov. 21, 2023. [Online]. Available: https://eprints.utdi.ac.id/8085/

[16] R. Ramadhan, J. Latuny, and S. J. Litiloly, "PERANCANGAN PENGAMANAN SERVER APACHE MENGGUNAKAN FIREWALL IPTABLES DAN FAIL2BAN," *Jurnal ISOMETRI*, vol. 1, no. 1, Art. no. 1, May 2022, doi: 10.30598/isometri.2022.1.1.9-15.

[17] E. Nurelasari and D. G. A. Farabi, "ANALISIS KEAMANAN SISTEM WEBSITE MENGGUNAKAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA SIMANTEP.ID," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, Art. no. 3, May 2024, doi: 10.36040/jati.v8i3.9314.

[18] N. R. P. Chairisda, "Optimalisasi Satgas Cyber Patrol Polres Banyumas dalam Menghadapi Pemilu 2019," *Police Studies Review*, vol. 4, no. 1, Art. no. 1, Jan. 2020.

[19] H. Ardiyanti, "Cyber-security dan tantangan pengembangannya di indonesia," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, vol. 5, no. 1, 2016.

[20] Proxmox, "Proxmox Virtual Environment," Proxmox. Accessed: Feb. 17, 2024. [Online]. Available: https://www.proxmox.com/en/

[21] R. Kumar and P. R. Shinde, "Computer Network-IP Address & Subnetting," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 5, no. 4, pp. 242–246, 2016.

[22] V. F. Aura, S. Ananda, R. Aulia, R. Safitri, and D. P. Sari, "Teknik Maksimalisasi Keamanan Jaringan Hotspot Link dengan Metode Filtering IP Address dan MAC Address Pada SMA 1 Stabat," *JURNAL INFORMATIKA DAN PERANCANGAN SISTEM (JIPS)*, vol. 5, no. 1, pp. 37–44, 2023.

[23] E. Nurmiati, "Analisis dan perancangan web server pada handphone," *Studia Informatika: Jurnal Sistem Informasi*, vol. 5, no. 2, 2012.

[24] "The Apache HTTP Server Project." Accessed: Dec. 12, 2023. [Online]. Available: https://httpd.apache.org/

[25] “Usage Statistics and Market Share of Apache, December 2023.” Accessed: Dec. 12, 2023. [Online]. Available: https://w3techs.com/technologies/details/ws-apache

[26] *fail2ban/fail2ban*. (Dec. 03, 2023). Python. Fail2Ban. Accessed: Dec. 03, 2023. [Online]. Available: https://github.com/fail2ban/fail2ban

[27] L. Bies, “A near perfect iptables firewall configuration,” Lammert Bies. Accessed: Nov. 21, 2023. [Online]. Available: https://www.lammertbies.nl/comm/info/iptables

[28] L. Ceragioli, P. Degano, and L. Galletta, “Can my firewall system enforce this policy?,” *Computers & Security*, vol. 117, p. 102683, Jun. 2022, doi: 10.1016/j.cose.2022.102683.

[29] “Quick HOWTO : Ch14 : Linux Firewalls Using iptables - Linux Home Networking.” Accessed: Nov. 21, 2023. [Online]. Available: http://iwanarif.lecturer.pens.ac.id/NetSecure/

[30] I. M. Suartana, H. E. Wahanani, and A. N. Sandy, “SISTEM PENGAMANAN WEB SERVER DENGAN WEB APPLICATION FIREWALL (WAF,” *Scan : Jurnal Teknologi Informasi dan Komunikasi*, vol. 10, no. 1, Art. no. 1, Jan. 2015, doi: 10.33005/scan.v10i1.598.

[31] M. Mischel, *ModSecurity 2.5*. Packt Publishing Ltd, 2009.

[32] OWASP Foundation, “OWASP Foundation, the Open Source Foundation for Application Security.” Accessed: Feb. 17, 2024. [Online]. Available: https://owasp.org/

[33] “Cross Site Scripting Prevention - OWASP Cheat Sheet Series.” Accessed: Nov. 21, 2023. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

[34] K. E. Kendall and J. E. Kendall, *Systems analysis and design*. Pearson, 2014.

[35] M. E. Suryani, "Penetration Testing: Actual Exploit," *Penetration Testing: Actual Exploit*.