ANALISIS IMPLEMENTASI *REVERSE PROXY* DAN *MODSECURITY* UNTUK PENCEGAHAN SERANGAN XSS PADA *WEB SERVER* CMS *WORDPRESS*

SKRIPSI

Aldi Satria
2103423001

PROGRAM STUDI D4 BROADBAND MULTIMEDIA
JURUSAN TEKNIK ELEKTRO
POLITEKNIK NEGERI JAKARTA
JANUARI 2023

ANALISIS IMPLEMENTASI *REVERSE PROXY* DAN *MODSECURITY* UNTUK PENCEGAHAN SERANGAN XSS PADA *WEB SERVER* CMS *WORDPRESS*

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Meraih
Gelar Sarjana Terapan

Aldi Satria
2103423001

PROGRAM STUDI D4 BROADBAND MULTIMEDIA
JURUSAN TEKNIK ELEKTRO
POLITEKNIK NEGERI JAKARTA
JANUARI 2023

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar

Nama	**: Aldi Satria**
NIM	**: 2103423001**
Tanda Tangan	**:**

Tanggal	**: 20 Januari 2023**

LEMBAR PENGESAHAN SKRIPSI

Skripsi diajukan oleh:

Nama	: Aldi Satria
NIM	: 2103423001
Program Studi	: Broadband Multimedia
Judul Skripsi	: Analisis Implementasi *Reverse Proxy* dan *ModSecurity* untuk Pencegahan Serangan XSS pada *Web Server* CMS *WordPress*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada 20 Januari 2023 dan dinyatakan **LULUS**.

Pembimbing : Asri Wulandari, S.T., M.T. ( )
NIP. 19750301 199903 2 001

Depok, 20 Januari 2023
Disahkan Oleh
Ketua Jurusan Teknik Elektro

Rika Novita, S.T., M.T.
NIP. 1970 1114 200812 2 001

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena berkat dan rahmat-Nya, penulis dapat menyelesaikan Tugas Akhir ini. Penulisan Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik. Skripsi ini membahas tentang **"Analisis Implementasi *Reverse Proxy* dan *ModSecurity* untuk Pencegahan Serangan XSS pada *Web Server* CMS *WordPress*"**.

Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan Skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan Skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Asri Wulandari, S.T., M.T., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan Skripsi ini;
2. Bapak/Ibu dosen yang telah banyak memberi masukan dan bantuan kepada penulis;
3. Orang tua dan keluarga besar penulis yang telah memberikan bantuan dukungan dalam doa dan material;
4. Serta sahabat yang telah banyak membantu penulis dalam menyelesaikan Skripsi ini.

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Tugas Akhir ini membawa manfaat bagi pengembangan ilmu.

Depok, 20 Januari 2023

Penulis

Aldi Satria

Analisis Implementasi *Reverse Proxy* dan *ModSecurity* untuk Pencegahan Serangan XSS pada *Web Server* CMS *WordPress*

Abstrak

WordPress merupakan salah satu CMS yang paling banyak digunakan di dunia, saat ini 43% website di dunia menggunakan CMS WordPress. Semakin meningkatnya penggunaan WordPress sebagai CMS sebuah web, maka semakin banyak pula isu keamanan yang muncul. Salah satu isu keamanan yang sering ditemui pada website berbasis CMS WordPress adalah serangan Cross-site Scripting (XSS). Implementasi reverse proxy dan ModSecurity bertujuan untuk meningkatkan keamanan CMS WordPress dari kerusakan akibat serangan XSS. Konfigurasi sistem pencegahan serangan XSS pada web server CMS WordPress dimulai dengan mengumpulkan CVE serangan XSS. Pembatasan jumlah HTTP request akan mencegah hacker melakukan brute force untuk menebak payload dari serangan XSS yang PoC CVE-nya tidak dipublikasi. Sementara untuk PoC CVE serangan XSS yang dipublikasi, langkah pengamanannya adalah dengan membuat rule ModSecurity. Pengujian efektivitas reverse proxy menunjukkan bahwa semakin kecil nilai rate limiting yang dimasukkan akan semakin banyak jumlah HTTP request yang ditolak. Begitupun sebaliknya, semakin besar nilai rate limiting yang dimasukkan akan semakin sedikit jumlah HTTP request yang ditolak. Namun jika nilai rate limiting 0 atau tidak menerapkan rate limiting, HTTP request akan selalu diterima oleh server reverse proxy. Selanjutnya pengujian efektivitas ModSecurity menunjukkan bahwa ModSecurity hanya bisa memfilter serangan XSS yang bersumber dari lalu lintas jaringan HTTP. Jika serangan XSS bukan bersumber dari lalu lintas jaringan HTTP, maka ModSecurity tidak bisa memfilternya atau menolaknya.

Kata kunci: *Keamanan, ModSecurity, Reverse Proxy, WordPress, XSS*

Analysis of Reverse Proxy and ModSecurity Implementation for Prevention of XSS Attacks on the WordPress CMS Web Server

Abstrak

WordPress is one of the most popular Content Management Systems (CMS) in the world; today, 43% of websites utilize the WordPress CMS. The more the adoption of Wordpress as a web CMS, the more security issues occur. Cross-site Scripting (XSS) attacks are one of the most common security issues on WordPress CMS-based websites. The application of reverse proxy and ModSecurity is designed to strengthen the WordPress CMS's security against XSS assaults. Gathering XSS attack CVEs is the first step in configuring an XSS attack protection system on the WordPress CMS web server. Limiting the amount of HTTP requests prevents hackers from brute-forcing the payload of an XSS attack for which the CVE PoC has not been disclosed. For XSS attacks whose CVE PoC has been disclosed, the countermeasure is to set ModSecurity rules. In assessing the efficacy of the reverse proxy, it can be observed that the smaller the rate limiting value input, the bigger the number of refused HTTP requests, and vice versa, the larger the rate limiting value entered, the fewer the number of rejected HTTP requests. If the rate limiting setting is 0 or does not apply rate limiting, the reverse proxy server will always allow HTTP requests. ModSecurity is only capable of filtering XSS attacks that originate via HTTP network traffic, as determined by evaluating its efficiency. ModSecurity is incapable of filtering or denying XSS attacks that do not originate from HTTP network traffic.

Keywords: *ModSecurity, Reverse Proxy, Security, WordPress, XSS*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Content Management System (CMS) adalah sebuah perangkat lunak yang digunakan untuk melakukan pengelolaan *website* seperti menambah, mengubah, dan menghapus konten dalam suatu *website*. CMS menjadi alternatif dalam membuat *website* yang lebih mudah tanpa harus menguasai bahasa pemrograman (Devella, 2021). *WordPress* merupakan salah satu CMS yang paling banyak digunakan di dunia, saat ini 43% *website* di dunia menggunakan *WordPress,* dan *WordPress* telah mendominasi 64% pengguna CMS di seluruh dunia diikuti *Shopify*, *Joomla* dan *Wix* (*Q-Success*, 2022).

Semakin meningkatnya penggunaan *WordPress* sebagai CMS sebuah web, maka semakin banyak pula isu keamanan yang muncul. Salah satu isu keamanan yang sering ditemui pada *website* berbasis *WordPress* adalah serangan *Cross-site Scripting* (XSS). Termuat pada *white paper* yang diterbitkan oleh Patchstack pada tahun 2021, 50% dari total *vulnerability* yang ditemukan pada *website* berbasis CMS *WordPress* adalah serangan XSS (Patchstack, 2021). XSS merupakan sebuah eksploitasi keamanan web dimana penyerang menyisipkan kode berbahaya (biasa HTML dan Javascript) di sisi klien ke suatu halaman web yang memungkinkan peretas atau hacker untuk mencuri data, mengendalikan sesi pengguna, menjalankan kode berbahaya, atau digunakan sebagai bagian dari *phishing scam* (Suroto, 2021).

Salah satu upaya *WordPress* untuk mencegah terjadinya serangan XSS adalah dengan merilis *security update*. Terdapat 2 jenis versi *update* pada CMS *WordPress*, yaitu *update* versi mayor dan *update* versi minor. *Update* versi mayor adalah *update* penambahan fitur dan API yang dilakukan setiap empat bulan sekali, sedangkan *update* versi minor adalah *update* untuk memperbaiki celah keamanan dan memperbaiki *bug* pada CMS *WordPress* yang dilakukan tanpa ketentuan waktu (Rosso, 2015). Dalam hal ini, jika ditemukan celah keamanan serangan XSS baru di CMS *WordPress*, pengguna harus memperbarui versi CMS *WordPress* yang digunakan, agar tidak terkena serangan XSS. Namun untuk

beberapa alasan tertentu, banyak perusahaan yang masih menggunakan CMS *WordPress* versi lama. Tercatat 33% penggunaan CMS *WordPress* di dunia masih menggunakan versi 5 (Q-Success, 2022).

Berkaca dari permasalahan tersebut, dicari solusi agar CMS *WordPress* yang diketahui memiliki celah serangan XSS tetap aman meskipun versinya tidak diperbaharui. Salah satu solusinya adalah memanfaatkan *ModSecurity*. *ModSecurity* adalah sebuah *web application firewall* yang bersifat *open source* yang memfilter HTTP *request* menggunakan *rule* berdasarkan aturan *regular expression* (regex) yang fleksibel (Iskandar, 2020). Selain menggunakan *ModSecurity, reverse proxy* juga dimanfaatkan dalam melakukan pencegahan dari serangan XSS. *Reverse proxy* mengatur agar sebuah server dapat berperan menjadi perantara antara klien dengan server utama (Kautsar, 2021). Sehingga serangan XSS yang diluncurkan *hacker* tidak langsung mengenai *web server* CMS *WordPress* melainkan melewati *reverse proxy* terlebih dahulu.

Penelitian Kevin Kautsar dalam "Implementasi Serta Analisa *ModSecurity* dan *Reverse Proxy* Untuk Pencegahan DDoS *Attack* Pada *Web Server*" hanya membahas *reverse proxy* dan *ModSecurity* dalam mencegah serangan DDoS, dan penelitian Farid Ridho dalam "Analisis Kinerja *ModSecurity* (Studi Kasus: Pencegahan Terhadap Serangan SQL *Injection*)" hanya membahas *ModSecurity* dalam mencegah serangan SQL *injection*. Pada penelitian ini akan terfokus pada pencegahan serangan XSS pada CMS *WordPress* dengan menggunakan *ModSecurity* sebagai *web application firewall* (WAF), *Apache2* sebagai *web server* , dan *NGINX* sebagai *reverse proxy*.

Berdasarkan latar belakang di atas, maka penulis menyusun skripsi dengan judul "Analisis Implementasi *Reverse Proxy* dan *ModSecurity* untuk Pencegahan Serangan XSS pada *Web Server* CMS *WordPress*".

1.2 Perumusan Masalah

Berdasarkan latar belakang yang diuraikan, permasalahan yang dibahas dalam skripsi ini adalah:

1) Bagaimana cara implementasi infrastruktur reverse proxy dan *ModSecurity* untuk pencegahan XSS pada *web server* CMS *WordPress*?

2) Bagaimana implementasi konfigurasi reverse proxy dan *ModSecurity* untuk pencegahan XSS pada *web server* CMS *WordPress*?
3) Bagaimana analisis efektifitas *reverse proxy* dan *ModSecurity* untuk pencegahan serangan XSS pada *web server* CMS *WordPress*?

1.3 Batasan Masalah

Adapun batasan masalah dalam laporan skripsi ini adalah:

a) *Web server* yang digunakan untuk instalasi CMS *WordPress* adalah *Apache2* dan *web server* yang digunakan untuk instalasi *reverse proxy* adalah *NGINX*.
b) *Content Management System* yang digunakan adalah *WordPress*.
c) *Web application firewall* yang digunakan adalah *ModSecurity*.
d) Celah keamanan yang digunakan sebagai pengujian keamanan web adalah *Cross-Site Scripting* (XSS).

1.4 Tujuan

Adapun tujuan dari penyusunan skripsi ini adalah.

a) Melakukan implementasi infrastruktur reverse proxy dan *ModSecurity* untuk pencegahan XSS pada *web server* CMS *WordPress*
b) Melakukan konfigurasi reverse proxy dan *ModSecurity* untuk pencegahan XSS pada *web server* CMS *WordPress*
c) Menganalisis efektifitas keamanan *reverse proxy* dan *ModSecurity* untuk pencegahan serangan XSS pada *web server* CMS *WordPress*.

1.5 Luaran

Luaran yang ingin dicapai dalam penyusunan skripsi ini adalah:

a) Membantu pengguna dalam mengamankan *web server* CMS *WordPress* mereka dari serangan *Cross-Site Scripting* (XSS).
b) Menghasilkan artikel ilmiah berdasarkan hasil data yang didapatkan dari implementasi *reverse proxy* dan *ModSecurity* untuk pencegahan serangan XSS pada *web server* CMS *WordPress.*

BAB V
KESIMPULAN

Berdasarkan data yang diperoleh dari pembahasan dan pengujian yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut.

1. Realisasi Implementasi *reverse proxy* dan *ModSecurity* untuk pencegahan serangan XSS pada web server CMS *WordPress* berhasil dibuat dengan memanfaatkan server Linux Ubuntu, *reverse proxy Nginx* dan *web server Apache2*.
2. Realisasi implementasi konfigurasi *reverse proxy* dan *ModSecurity* untuk pencegahan XSS pada *web server* CMS *WordPress* berhasil dibuat dengan memanfaatkan fitur *rate limiting reverse proxy* dan *rule* serangan XSS *ModSecurity*.
3. Berdasarkan analisis data hasil pengujian dapat disimpulkan bahwa:
    a. Semakin kecil nilai *rate limiting* yang dimasukkan akan semakin banyak jumlah HTTP *request* yang ditolak, dan begitupun sebaliknya, semakin besar nilai *rate limiting* yang dimasukkan akan semakin sedikit jumlah HTTP *request* yang ditolak. Sedangkan jika nilai *rate limiting* 0 atau tidak menerapkan *rate limiting*, HTTP *request* akan selalu diterima oleh server *reverse proxy.*
    b. M*odSecurity* hanya bisa memfilter serangan XSS yang bersumber dari lalu lintas jaringan HTTP. Jika serangan XSS bukan bersumber dari lalu lintas jaringan HTTP, maka *ModSecurity* tidak bisa memfilternya atau menolaknya.

DAFTAR PUSTAKA

Devella, Siska. 2021. Pelatihan Pembuatan *Website* Sekolah Menggunakan *Wordpress* Untuk Guru TIK SMA Negeri 17 Palembang. *Palembang: TMIK Global Informatika MDP*, Palembang.

H., Pareklya (2022). *Using Seclist for Penetration Testing*. https://www.varutra.com/using-seclists-for-penetration-testing/

Iskandar, Riska., Alamsyah, Hendri Alamsyah (2020). Penerapan Sistem Keamanan *WEB* Menggunakan Metode *WEB Application Firewall*. *Universitas Dehasen Bengkulu*, Bengkulu.

Jannah, Yasmin Izzatul (2022). Apa Itu WordPress? Pengertian, Kelebihan, dan Kekurangan. izza

Kautsar, Kevin (2021). Implementasi Serta Analisa Modsecurity Dan Reverse Proxy Untuk Pencegahan Ddos Attack Pada Web Server. *Depok: Jurusan Teknik Informatika dan Komputer*, Politeknik Negeri Jakarta

Kettle, James (2021). *Alert() is dead, long live print()*. https://portswigger.net/research/alert-is-dead-long-live-print

Kettle, James (2021). *Turbo Intruder: Embracing the billion-request attack*. https://portswigger.net/research/turbo-intruder-embracing-the-billion-request-attack

MITRE (2021). Researcher Reservation Guidelines. https://cve.mitre.org/cve/researcher_reservation_guidelines

Muliantara, Agus (2009). Penerapan *Regular Expression* Dalam Melindungi Alamat *Email* Dari *Spam* Robot Pada Konten *WordPress. Bali: Jurusan Ilmu Komputer. Fakultas Matematika dan Ilmu Pengetahuan Alam*. Universitas Udayana

NGINX, 2023. nginx-about. https://nginx.org/en/

Owasp (2021). *Top 10 Web Application Security Risks*. https://owasp.org/www-project-top-ten/

Patchstack (2022). *State of Wordpress Security in 2021*. https://patchstack.com/whitepaper/the-state-of-wordpress-security-in-2021/?utm_medium=banner&utm_source=database&utm_campaign=whitepaper

PortSwigger (2021). *What is Burp Proxy?*. https://portswigger.net/burp/documentation/desktop/tools/proxy

Q-Success. (2021). *Usage statistics and market share of WordPress*. https://w3techs.com/technologies/details/cm-wordpress

Rahmad, Ade (2019). Forensik Serangan *Brute Force* pada *Cloud Public* Menggunakan Logika Fuzzy. *Palembang: Jurusan Sistem. Komputer Fakultas Ilmu Komputer*. Universitas Negeri Sriwijaya

Rawdat, Amir (2017). *Rate Limiting with NGINX and NGINX Plus*. https://www.nginx.com/blog/rate-limiting-nginx/

Red Hat (2021). *What is a CVE?*. https://www.redhat.com/en/topics/security/what-is-cve

Rosso, Sara (2015). *Wordpress Security.* https://wordpress.org/about/security/

Subari, Arkhan., dkk (2022). Pemanfaatan Metode Wavs (*Web Application Security Scanners*) Menggunakan Burp Suite *Tools* Dalam Audit Teknis Keamanan Sistem Informasi Surat Tugas Sekolah Vokasi Undip. *Semarang:*

Program Studi Str. Teknik Listrik Industri. Sekolah Vokasi. Universitas Diponegoro

Suroto, Asman (2021). Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-site Scripting (XSS) Dan Metode Pencegahannya. *Batam: Teknik Sistem Informasi. Fakultas Teknik*. Universitas Batam

Tao, Y. & Chen, G., 2016. An Extensible Universal Reverse Proxy Architecture. International Conference on Network and Information Systems for Computers

DAFTAR RIWAYAT HIDUP

Aldi Satria

Lulus dari SDN 63 Surabayo Lubuk Basung pada tahun 2008, SMPN 3 Lubuk Basung pada tahun 2011 dan SMAN 2 Lubuk Basung pada tahun 2014. Gelar Diploma Tiga (DIII) diperoleh pada tahun 2017 dari Jurusan Teknik Elektro, Program Studi Teknik Telekomunikasi, Politeknik Negeri Padang., dan Gelar Diploma Empat (DIV) atau Sarjana Terapan pada tahun 2023 dari Jurusan Teknik Elektro, Program Studi Broadband Multimedia, Politeknik Negeri Jakarta.