INTISARI

ANALISIS KINERJA MODSECURITY DAN NAXSI TERHADAP SERANGAN *SLOW HTTP DENIAL OF SERVICE*

Ardy Nugroho
21/479068/SV/19428

Serangan *Denial of Service* (DoS) merupakan ancaman serius terhadap aplikasi berbasis web. Serangan ini menyebabkan layanan tidak dapat diakses oleh pengguna yang sah. Cloudflare, sebuah penyedia layanan *cloud* untuk perlindungan situs web menyebutkan bahwa tren serangan DDoS terus meningkat dari waktu ke waktu. Serangan DoS tidak hanya mengeksploitasi lapisan jaringan atau transport, namun juga berkembang dan mengeksploitasi lapisan aplikasi yang menggunakan protokol HTTP. Salah satu bentuk perlindungan pada aplikasi berbasis web adalah penggunaan *Web Application Firewall*(WAF).

Penelitian ini menguji dua jenis WAF, yaitu ModSecurity dan NAXSI dalam menghadapi serangan jenis *Slow HTTP DoS.* Terdapat tiga jenis serangan yang diujikan, yaitu Slow Headers, Slow Body, dan Slow Read. Pengujian dilakukan dengan variasi jumlah koneksi dan durasi yang beragam. Hasil pengujian serangan Slow Headers menujukkan bahwa NAXSI memiliki efektifitas 87.96%, lebih baik daripada ModSecurity dengan efektifitas 83.7%. Pada serangan Slow Body, ModSecurity memiliki efektifitas 73.1%, lebih baik daripada NAXSI dengan efektifitas 60%. Pada serangan Slow Read, ModSecurity memiliki efektifitas 81.8%, lebih baik daripada NAXSI dengan efektifitas 77.92%.

Kata Kunci: *Denial of Service, Web Application Firewall*, ModSecurity, NAXSI, Slow Headers, Slow Body, Slow Read

ABSTRACT

PERFORMANCE ANALYSIS OF MODSECURITY AND NAXSI AGAINST SLOW HTTP DENIAL OF SERVICE ATTACKS

Ardy Nugroho
21/479068/SV/19428

Denial of Service attacks Denial of Service (DoS) attacks are a serious threat to web-based applications. This attack makes the service inaccessible to legitimate users. Cloudflare, a cloud service provider for website protection mentioned that the trend of DDoS attacks continues to increase over time. DoS attacks not only exploit the network or transport layer, but also develop and exploit the application layer that uses the HTTP protocol. One form of protection in web-based applications is the use of Web Application Firewall (WAF).

This research tests two types of WAF, namely ModSecurity and NAXSI in dealing with Slow HTTP DoS type attacks. There are three types of attacks tested, namely Slow Headers, Slow Body, and Slow Read. Tests were conducted with a variety of connection counts and durations. The test results of the Slow Headers attack show that NAXSI has an effectiveness of 87.96%, better than ModSecurity with an effectiveness of 83.7%. In the Slow Body attack, ModSecurity has 73.1% effectiveness, better than NAXSI with 60% effectiveness. In the Slow Read attack, ModSecurity has an effectiveness of 81.8%, better than NAXSI with an effectiveness of 77.92%.

Keywords: Denial of Service, Web Application Firewall, ModSecurity, NAXSI, Slow Headers, Slow Body, Slow Read