INTISARI

OTOMASI REMEDIASI *BROKEN ACCESS CONTROL* PADA *WEB SERVER APACHE* BERBASIS *FAIL2BAN*

Ridho Ahmad Hidayat
20/464278/SV/18597

Aplikasi *web* telah menjadi komponen penting dalam operasi bisnis. Meningkatnya ketergantungan pada aplikasi *web* juga meningkatkan risiko kerentanan keamanan siber. *Broken Access Control* (*BAC*) telah menjadi masalah serius dalam layanan *web*. Pada tahun 2021, *OWASP* menempatkan *BAC* sebagai urutan pertama di antara sepuluh risiko aplikasi *web* teratas, dengan tingkat kejadian terbanyak. Mengamankan aplikasi *web* sebuah bisnis semestinya menjadi perhatian utama untuk melindungi bisnis dari akses tidak sah, namun demikian, belum banyak ditemukan penelitian yang membahas mitigasi atau remediasi kerentanan terlebih yang membahas terkait *BAC* maupun yang dirancang dalam bentuk otomasi. Penelitian ini bertujuan untuk merancang sistem sederhana yang dapat digunakan oleh pengembang *web* dengan keterbatasan biaya, waktu, sumber daya, dan keahlian terkait keamanan siber, untuk melakukan otomasi remediasi terhadap kerentanan *BAC* yang paling umum ditemukan dan kerap dieksploitasi pada *web server Apache*. Penelitian ini menerapkan gabungan dari metode *Code-Level Security Hardening* pada konfigurasi *web server Apache* dan *Design-Level Security Hardening* dengan menambahkan aplikasi *Fail2ban* pada desain sistem layanan *web*, ke dalam sebuah sistem otomasi. Pada penelitian ini, dibuat sebuah solusi berupa sistem otomasi yang dapat melakukan remediasi terhadap kerentanan *BAC* pada *web server Apache*, seperti kerentanan aktifnya indeks opsi, adanya berkas pada konfigurasi dengan izin akses yang tidak semestinya, akses menebak *URL* yang berulang, dan percobaan eksekusi perintah pada isi dari *http request*, yang dapat membuat pengamanan kerentanan *BAC* pada *web server Apache* tersebut menjadi lebih cepat dengan menurunkan kebutuhan waktu remediasi sebesar 42,8% dibandingkan dengan remediasi secara manual dan dengan rasio keberhasilan atau *success rate* sebesar 100%.

Kata kunci : Otomasi, *Broken Access Control*, *Apache2*, *Python*, *Fail2ban*

ABSTRACT

AUTOMATION OF BROKEN ACCESS CONTROL REMEDIATION IN APACHE WEB SERVER BASED ON FAIL2BAN

Ridho Ahmad Hidayat
20/464278/SV/18597

Web applications have become an essential component of business operations. The increasing reliance on web applications also increases the risk of cybersecurity vulnerabilities. Broken Access Control (BAC) has become a serious problem in web services. In 2021, OWASP ranked BAC as number one among top ten web application risks, with the highest occurrence rate. Securing a business web application should be a major concern to protect the business from unauthorized access, however, there has not been much research that discusses vulnerability mitigation or remediation, especially those related to BAC or those designed in the form of automation. This research aims to design a simple system that can be used by web developers with limited costs, time, resources, and expertise in cybersecurity, to automate remediation of the most common BAC vulnerabilities found and often exploited on Apache web servers. This research combines Code-Level Security Hardening on Apache web server configuration and Design-Level Security Hardening by adding Fail2ban to the web service design, into an automation system. In this research, a solution is made in the form of an automation system that can remediate BAC vulnerabilities on the Apache web server, such as vulnerability of active index options, the existence of configuration files with improper access permissions, repeated URL guessing access, and command execution attempts inside the contents of http requests, which can make securing BAC vulnerabilities on the Apache web server faster by reducing the remediation time required by 42,8% compared to manual remediation and with 100% success rate.

Keywords : Automation, Broken Access Control, Apache2, Python, Fail2ban