ABSTRACT

Modern web applications are generally developed using PHP frameworks such as Laravel and Codeigniter, which implement the principles of Service-Oriented Architecture (SOA) through endpoint-based services. The implementation of CRUD endpoints in RESTful APIs is a concrete form of SOA implementation. RESTful APIs connect various services through the HTTP protocol. Although this approach offers advantages in terms of flexibility, speed, and ease of integration, it also opens up potential vulnerabilities that can be exploited by irresponsible parties. Various API-related security incidents, such as Broken Object Level Authorization and Broken Authentication, highlight the importance of early detection of potential vulnerabilities. This study aims to identify vulnerabilities using the Vulnerability Assessment and Penetration Testing method, which combines automated and manual testing. The default security of each framework and ModSecurity as a Web Application Firewall are implemented. Based on the final test results using Burp Suite, the Laravel framework is still detected to have Cross-Domain Misconfiguration vulnerabilities, where by default all origins are allowed to access resources. This vulnerability was identified in the GET All, POST, and GET By Data methods. The Cross-Domain Misconfiguration vulnerability was calculated using CVSS with a score of 5.3, which falls into the medium category, while Codeigniter did not show a similar vulnerability. Therefore, it can be concluded that when the default security of both frameworks and the implementation of ModSecurity WAF are applied, the Codeigniter framework is better in terms of security.

Keywords: *Laravel, Codeigniter, Restful API, Service-Oriented Architecture (SOA), VAPT.*

ABSTRAK

Aplikasi web modern umumnya dikembangkan menggunakan framework PHP seperti *Laravel* dan *Codeigniter* yang menerapkan prinsip *Service-Oriented Architecture (SOA)* melalui layanan berbasis *endpoint*. Implementasi *CRUD endpoint* dalam *RESTful API* menjadi bentuk konkret penerapan SOA. *Restful API* menghubungkan berbagai layanan melalui protokol HTTP. Meskipun pendekatan ini memberikan keunggulan dalam fleksibilitas, kecepatan, dan kemudahan integrasi, hal tersebut juga membuka celah potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Berbagai insiden keamanan terkait *API* seperti *Broken Object Level Authorization* dan *Broken Authentication* menjadikan pentingnya deteksi dini terhadap potensi kerentanan. Penelitian ini bertujuan untuk mengidentifikasi kerentanan dengan menggunakan metode *Vulnerability Assessment and Penetration Testing* yang menggabungkan pengujian otomatis dan manual. Keamanan *default* masing-masing framework dan *ModSecurity* sebagai *Web Application Firewall* diterapkan. Berdasarkan hasil pengujian akhir menggunakan Burp Suite, framework *Laravel* masih terdeteksi memiliki kerentanan *Cross-Domain Misconfiguration*, di mana secara default seluruh *origin* diizinkan untuk mengakses sumber daya. Kerentanan tersebut teridentifikasi pada *method GET All, POST,* dan *GET By Data.* Kerentanan *Cross-Domain Misconfiguration* dihitung menggunakan *CVSS* dengan skor 5.3 masuk kedalam kategori medium*,* sedangkan *Codeigniter* tidak menunjukan kerentanan serupa. Sehingga dapat disimpulkan ketika keamanan *default* kedua framework dan penerapan WAF *modsecurity* diterapkan, framework *Codeigniter* lebih baik dalam segi keamanan.

Kata kunci: *Laravel, Codeigniter, Restful API, Service-Oriented Architecture (SOA), VAPT.*