Evaluasi Web Application Vulnerability Scanner untuk Aplikasi Web Modern = Evaluation of Web Application Vulnerability Scanner for Modern Web Application

Azwar Al Anhar, author

Abstrak

Perkembangan zaman dan teknologi meningkatkan penggunaan aplikasi berbasis digital. Salah satunya adalah aplikasi berbasis web yang mudah untuk diakses dan digunakan oleh masyarakat sekarang. Seiring dengan perkembangan tersebut, tidak jarang terdapat celah keamanan yang terdapat pada web aplikasi yang tanpa disadari oleh pemiliknya sehingga menimbulkan risiko kebocoran data ataupun hancurnya reputasi organisasi yang memiliki aplikasi tersebut. Banyaknya web aplikasi yang dimiliki oleh suatu organisasi atau perusahaan juga memiliki tantangan sendiri untuk dapat menemukan celah keamanan yang terdapat pada aplikasi tersebut. Hal ini karena terdapat batasan waktu dan sumber daya untuk melakukan assessment secara manual. Oleh sebab itu, adanya kebutuhan penggunaan pemindai celah keamanan web aplikasi, yang melakukan pencarian celah secara otomatis, untuk dapat membantu dan mempersingkat pencarian dari celah keamanan. Terdapat banyak jenis pemindai celah keamanan web aplikasi yang dapat digunakan secara gratis maupun komersial. Pada penelitian ini Penulis mengevaluasi kemampuan alat pemindai celah keamanan yang opensource seperti OWASP ZAP, Wapiti, Arachni dan Burp Suite Professional dengan target benchmark berbasiskan NodeJS yaitu Damn Vulnerable NodeJS Application (DVNA) dan NodeGoat. Dari hasil eksperimen didapatkan bahwa keempat WAVS (Web Application Vulnerability Scanner) memiliki rata-rata nilai f-measured antara 0,4-0,6. Burp Suite Professional memiliki nilai True Positive (TP) dan Recall paling baik dan Arachni untuk nilai Precision sempurna untuk kedua target benchmark.
.....Current needs and developments encourage the increasing use of digital-based applications. One of them is a web-based application that is easy to access and used by today's society. Along with these developments, it is common for vulnerabilities to exist in web applications that the owners are unaware of. It creates the risk of data leakage or damage to the organization's reputation as the application owner. In addition, the number of web applications owned by an organization or company leads to challenges in finding vulnerabilities in these applications. This happened due to time and resource constraints for conducting manual assessments. Therefore, there is necessary to use a web application vulnerability scanner, which performs vulnerability scanning automatically, to be able to help and streamline the search for vulnerabilities. There are many types of web application vulnerability scanners that can be used for free or commercially. This study evaluated the capabilities of WAVS (Web Application Vulnerability Scanners) tools such as OWASP ZAP, Wapiti, Arachni, and Burp Suite Professional with NodeJS-based benchmark targets, namely Damn Vulnerable NodeJS Application (DVNA) and NodeGoat. This study found that the four WAVS have an average f-measured value between 0.4-0.6. Burp Suite Professional had the best True Positive (TP) and Recall values, while Arachni for perfect Precision valued for both benchmark targets.