Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 7, No. 7, Juli 2023, hlm. 3431-3433 http://j-ptiik.ub.ac.id

Pengujian Efektivitas OWASP ZAP dalam Menemukan Kerentanan dari Metasploitable

Muhammad Gibran Abraham Danialdo[1], Fariz Andri Bakhtiar[2], Mahendra Data[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]gibranabraham@student.ub.ac.id, [2]fariz@ub.ac.id, [3]mahendra.data@ub.ac.id

Abstrak

Penggunaan Aplikasi Web semakin tinggi. Dengan maraknya Aplikasi Web tersebut, tentu saja keamanan menjadi salah satu hal yang menjadi perhatian karena tidak menentunya sebuah keamanan dari aplikasi web. Aplikasi Web sangat rentan terhadap serangan. Vulnerability Assessment merupakan sebuah langkah dalam menemukan celah kerentanan pada sebuah Aplikasi Web. Vulnerability Scanning adalah salah satu langkah yang dilakukan pada Vulnerability Assessment. Vulnerability Scanning dapat dilakukan dengan menggunakan Vulnerability Scanner. Vulnerability Scanner merupakan alat yang dapat membantu menemukan kerentanan pada Aplikasi Web secara otomatis. OWASP ZAP merupakan sebuah aplikasi scanner yang cukup banyak digunakan. Pengujian dilakukan untuk mengetahui efektivitas OWASP ZAP dalam menemukan kerentanan. Pengujian ini dilakukan dengan menggunakan Vulnerable Machine yang sengaja dibuat memiliki banyak kerentanan yang sudah didokumentasikan yang menjadi parameter ukur dalam menemukan efektivitas sebuah scanner. Metasploitable merupakan Vulnerable Machine yang kelemahannya sudah didokumentasikan yang dapat digunakan dalam pengujian. Pengujian dilakukan dengan memanfaatkan Aplikasi Web penuh kerentanan yang dimiliki oleh Vulnerable Machine. Alamat dari Aplikasi Web tersebut dimasukkan kedalam scanner yang secara otomatis melakukan scan dan memberikan hasil berupa daftar kelemahan yang ada pada Aplikasi Web tersebut. Dari pengujian yang telah dilakukan, bisa didapatkan akurasi OWASP ZAP dalam menemukan kerentanan. Akurasi OWASP ZAP dalam menemukan kerentanan yang didapatkan adalah 61% untuk Metasploitable 2, 70% untuk Metasploitable 3 Ubuntu dan 30% untuk Metasploitable 3 Windows.

Kata kunci: *Aplikasi Web, Vulnerability Assessment, Vulnerability Scanner, OWASP ZAP, Vulnerable Machine, Metasploitable*

Abstract

The use of Web Applications is increasing. With the rise of these Web Applications, of course security is one of the concerns because of the uncertainty of the security of web applications. Web applications are very vulnerable to attacks. Vulnerability Assessment is a step in finding vulnerabilities in a Web Application. Vulnerability Scanning is one of the steps taken in Vulnerability Assessment. Vulnerability Scanning can be done using a Vulnerability Scanner. Vulnerability Scanner is a tool that can help find vulnerabilities in Web Applications automatically. OWASP ZAP is a scanner application that is quite widely used. Testing is done to determine the effectiveness of OWASP ZAP in finding vulnerabilities. This test was carried out using a Vulnerable Machine which was deliberately made to have many documented vulnerabilities which became a measuring parameter in finding the effectiveness of a scanner. Metasploitable is a Vulnerable Machine whose weaknesses have been documented which can be used in testing. Testing is done by utilizing the full Web Application vulnerabilities owned by the Vulnerable Machine. The address of the Web Application is entered into a scanner that automatically scans and provides results in the form of a list of weaknesses that exist in the Web Application. From the tests that have been carried out, the accuracy of OWASP ZAP in finding vulnerabilities can be obtained. The accuracy of OWASP ZAP in finding vulnerabilities obtained is 61% for Metasploitable 2, 70% for Metasploitable 3 Ubuntu and 30% for Metasploitable 3 Windows.

Keywords: *Web Application, Vulnerability Assessment, Vulnerability Scanner, OWASP ZAP, Vulnerable Machine, Metasploitable*

1. PENDAHULUAN

Penggunaan Aplikasi Web yang semakin tinggi meningkatkan perhatian pada keamanan Aplikasi Web (D. Yadav et al., 2018). Aplikasi Web sangat rentan terhadap serangan (S. Kumar et al., 2017).

Vulnerability Assessment adalah langkah yang dapat dilakukan dalam menemukan kerentanan sebuah sistem termasuk Aplikasi Web. *Vulnerability Assessment* dapat dilakukan menggunakan sebuah alat berupa *Vulnerability Scanner* (E. I. Alwi & F. Umar, 2020).

OWASP ZAP merupakan sebuah *Vulnerability Scanner*. Penggunaan sebuah *scanner* dalam melakukan *Vulnerability Assessment* tidak memiliki akurasi 100%. Oleh karena itu, pengujian efektivitas sebuah *Vulnerability Scanner* harus dilakukan.

Pengujian efektivitas sebuah *Vulnerability Scanner* dapat dilakukan dengan mengukur akurasi *scanner* tersebut dalam menemukan kerentanan dalam sebuah Aplikasi Web. Pengujian dapat dilakukan dengan memanfaatkan *Vulnerable Machine*. *Vulnerable Machine* adalah sebuah sistem yang sengaja dirancang secara untuk memiliki kerentanan. Kerentanan yang dimiliki sebuah *Vulnerable Machine* sudah didokumentasikan. Didalam *Vulnerable Machine* terdapat Aplikasi Web yang dapat diakses melalui browser dengan mengidentifikasi alamat IP dari sebuah *Vulnerable Machine*.

Metasploitable merupakan salah satu *Vulnerable Machine*. Metasploitable memiliki 3 versi sampai saat ini. Versi pertama dan kedua dari Metasploitable berjalan pada Sistem Operasi Linux, sedangkan versi ketiga memiliki 2 pilihan dimana salah satunya berjalan pada Sistem Operasi Windows dan satu lagi pada Sistem Operasi Linux.

Pengujian efektivitas sebuah *Vulnerability Scanner* dilakukan dengan cara mengidentifikasi alamat IP sebuah *Vulnerability Machine.* Alamat IP tersebut jika dimasukkan kedalam browser maka akan muncul Aplikasi Web. Alamat IP ini dapat digunakan pada OWASP ZAP yang dapat melakukan *scanning* pada alamat IP tersebut dan mengembalikan hasil berupa kerentanan yang ada pada Aplikasi Web

2. TINJAUAN PUSTAKA

2.1 *Vulnerability Scanning*

Vulnerability scanning adalah proses memperoleh informasi *vulnerability network* dengan memanfaatkan berbagai *tools network scanning* dan *vulnerability scanner*, seperti *port* yang terbuka, *bugs* aplikasi *server* dan lain-lain (I. Sofana & R. Primartha, 2019).

Vulnerability scanning dapat dilakukan secara otomatis menggunakan aplikasi seperti OWASP ZAP. Pengguna dapat memasukkan target seperti Aplikasi Web yang ingin dicari kelemahannya, lalu OWASP ZAP akan melakukan *scanning* pada Aplikasi Web tersebut (https://www.zaproxy.org/getting-started/).

2.2 OWASP ZAP

OWASP ZAP merupakan sebuah aplikasi yang digunakan dalam menemukan kerentanan pada suatu Aplikasi Web. OWASP ZAP menyediakan *scanner* secara otomatis (A. Saputra et al., 2017).

Dalam penggunaan OWASP ZAP, *scanner* dapat digunakan untuk menguji server, jaringan, perangkat dan endpoints. Saat melakukan *scanning*, tahap-tahap yang dilakukan adalah *Explore*, *Attack* dan *Report* (www.zaproxy.org/getting-started/).

2.3 Metasploitable 2

Metasploitable 2 adalah salah satu mesin virtual yang digunakan dalam penelitian ini. Metasploitable adalah sistem operasi berbasis Linux yang sengaja dibuat memiliki kelemahan yang dapat digunakan untuk penelitian keamanan sebuah sistem.

Setelah diunduh dan dijalankan melalui Virtual Box, pengguna memasukkan input berupa username dan password yaitu ‘msfadmin’. Dari sini, pengguna dapat mengeksplorasi Metasploitable 2 tentang kelemahan apa saja yang bisa diuji menggunakan mesin virtual ini (M. Singh & S. Kumar, 2020).

2.4 Metasploitable 3

Metasploitable 3 adalah salah satu mesin virtual yang digunakan dalam penelitian ini. Metasploitable adalah sistem operasi berbasis Linux dan Windows yang sengaja dibuat memiliki kelemahan yang dapat digunakan untuk penelitian keamanan sebuah sistem.

Metasploitable 3 berbasis Windows Server 2008 R2 dan Ubuntu 14.0.4 yang dapat digunakan setelah diunduh dengan bantuin Vagrant serta Packer (H. Sharma, 2020). Kedua mesin dapat dijalankan setelah pengguna

memasukkan input berupa username dan password yaitu ‘vagrant’. Setelah itu, pengguna dapat mengeskplorasi apa saja kelemahan yang dapat diuji.

3. PENGUJIAN

Pengujian dilakukan dengan tujuan mengetahui efektivitas OWASP ZAP dalam mengetahui kerentanan Aplikasi Web pada Metasploitable 2 dan Metasploitable 3. Pengujian menggunakan *scanner* otomatis pada OWASP ZAP dengan memasukkan alamat IP Metasploitable 2 maupun Metasploitable 3 yang sudah diidentifikasi.

Hasil *scan* dari OWASP ZAP dapat dibandingkan dengan kerentanan yang sudah didokumentasikan oleh Metasploitable. Berdasarkan hasil *scan* yang telah dilakukan, akurasi OWASP ZAP dalam menemukan kerentanan dari Metasploitable 2 adalah 61%, 70% untuk Metasploitable 3 Ubuntu dan 30% untuk Metasploitable 3 Windows.

4. KESIMPULAN

Berikut merupakan kesimpulan dari hasil pengujian efektivitas OWASP ZAP dalam menemukan kerentanan pada Metasploitable :

- OWASP ZAP menemukan kerentanan pada Metasploitable 2 dan Metasploitable 3 dengan melakukan *scanning* pada Alamat IP yang terhubung dengan Aplikasi Web dari Metasploitable 2 dan Metasploitable 3.
- OWASP ZAP memiliki akurasi sebesar 61% dalam menemukan kerentanan Metasploitable 2, 70% pada Metasploitable 3 Ubuntu dan 30% pada Metasploitable 3 Windows.

5. DAFTAR REFERENSI

D. Yadav, D. Gupta & D. Singh (2018). Vulnerabilities and Security of Web Applications.

S. Kumar, et al. (2017). A Study on Web Application Security and Detecting Security Vulnerabilities

E. Irawadi Alwi & F. Umar (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning.

I. Sofana & R. Primartha (2019). Network Security dan Cyber Security; Teori dan Praktek Cisco CCNA, Linux, Windows, Amazon AWS Android

Zaproxy.org. ZAP Getting Started. Diakses pada 14 Juni 2023, dari https://www.zaproxy.org/getting-started/#introducing-zap

A. Saputra, Nelmiawati & M. A. R. Sitorus (2017). Penilaian Ancaman pada Website Transkrip Aktifitas Mahasiswa Politeknik Negeri Batam Menggunakan Metode DREAD

M. Singh, S. Kumar, T. Garg & N. Pandey (2020). Penetration Testing on Metasploitable 2

H. Sharma (2020). Exploiting Vulnerabilities of Metasploitable 3 (WINDOWS) Using Metasploit Framework