Analisis dan Evaluasi Keamanan pada Domain Website Organisasi Riset Menggunakan Open Source Intelligence (OSINT) = Security Analysis and Evaluation of Research Organization Website Domains Using Open Source Intelligence (OSINT)

Taufik Akbar, author

Abstrak

Berdasarkan Lanskap Keamanan Siber Indonesia 2022, BSSN melaporkan terdapat 4.421.992 aktivitas APT dan 2.348 kasus defacement web di Indonesia pada tahun itu. Serangan yang ditujukan pada aplikasi web berfokus pada kelemahan aplikasi, yang disebut kelemahan atau celah keamanan. Akibatnya, penting untuk melakukan analisis dan evaluasi domain website organisasi riset tersebut. Metode yang digunakan adalah analisa deskriptif, yaitu data yang diperoleh disajikan dalam bentuk kalimat yang dideskripsikan. Sehingga memberikan kejelasan dari hasil analisis yang dilakukan. Indeks Keamanan Informasi (KAMI) sebagai alat untuk menilai kesiapan implementasi keamanan data. Serangkaian pertanyaan yang berkaitan dengan berbagai aspek digunakan untuk melakukan evaluasi. Kemudian OWASP ZAP sebagai tools vulnerability scanning, digunakan untuk mengidentifikasi tingkat kemungkinan kerentanan pada aplikasi berbasis web. Pada penelitian ini melakukan analisis dan evaluasi terhadap domain dan subdomain xyz.go.id yang terdapat di organisasi riset. Langkah pertama pengumpulan data target, selanjutnya dilakukan pengukuran dan pengujian tools dengan menggunakan Indeks KAMI pada kategori Sistem Eletronik. Langkah berikutnya dengan aplikasi OWASP ZAP digunakan untuk pengujian vulnerability scanning pada domain target. Data hasil DNSDumpster digunakan, dimana beberapa domain website xyz.go.id dijadikan sasaran penelitian untuk vulnerability scanning. Hasil penilaian Indeks KAMI menunjukkan bahwa 4 subdomain dianggap tergolong tinggi. Kemudian berdasarkan pengujian vulnerability scanning terhadap domain website xyz.go.id memiliki kerentanan dengan kategori low terdapat 15 peringatan, medium terdapat 32 peringatan, high terdapat 4 peringatan dan informational terdapat 20 peringatan. Dari hasil pengujian dapat dibuktikan pendeteksian dengan vulnerability scanning pada OWASP ZAP sangat efektif, meskipun ini tool open source sehingga tidak perlu menggunakan tool berbayar.

.....Based on the Indonesian Cybersecurity Landscape 2022, BSSN reported 4,421,992 APT activities and 2,348 web defacement cases in Indonesia that year. Attacks aimed at web applications focus on application weaknesses, called security flaws or gaps. As a result, it is important to conduct an analysis and evaluation of the research organization's website domain. The method used is descriptive analysis, in which the data obtained is presented in the form of sentences that are described. Information Security Index (KAMI Index) as a tool to assess the readiness of data security implementation A series of questions relating to various aspects are used to conduct the evaluation. Then OWASP ZAP as a vulnerability scanning tool, was used to identify the level of possible vulnerabilities in web-based applications. In this study, the analysis and evaluation of xyz.go.id domains and subdomains found in research organizations. The first step is collecting target data, then measuring and testing tools using the KAMI Index in the Electronic Systems category. The next step with the OWASP ZAP application is vulnerability scanning testing on the target domain. DNSDumpster result data is used, and several xyz.go.id website domains are used as research material for vulnerability scanning. The results of the KAMI Index assessment show that 4 subdomains are considered

high. Then based on vulnerability scanning testing of the xyz.go.id website domain, it has a vulnerability with a low category of 15 warnings, a medium category of 32 warnings, a high category of 4 warnings, and an informational category of 20 warnings. From the test results, it can be proven that detection with vulnerability scanning on OWASP ZAP is very effective, even though this is an open source tool, so there is no need to use paid tools.