Jurnal Sistem Informasi dan Sistem Komputer, Vol. 7, No. 1, Januari 2022
ISSN: 2715-906X (Online)
10.51717/simkom.v7i1.63

ANALISIS KERENTANAN WEBSITE SMA NEGERI 2 AMLAPURA MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

I Made Edy Listartha[1], I Made Ardha Premana Mitha[2], Made Wahyu Aditya Arta[3] I Km. Wahyu Yuda Arimika[4]
[1]listartha@undiksha.ac.id, [2]ardha.premana@undiksha.ac.id, [3]wahyu.aditya.arta@undiksha.ac.id, [4]km.wahyu@undiksha.ac.id
[1234]Universitas Pendidikan Ganesha

Abstrak

Sekolah memiliki websiste sebagai media yang menampilkan informasi sekolah, dan media interaksi. Terjadinya transisi komunikasi secara tradisional ke dalam lingkup aplikasi berbasis website bisa saja dimanfaatkan oleh beberapa pelaku kejahatan dunia maya dengan tujuan mencuri informasi rahasia siswa-siswi dengan tujuan tertentu, maka mendeteksi kerentanan keamanan website adalah hal yang sangat penting untuk mengetahui tingkat resiko dengan menggunakan metode Open Web Application Security Project (OWASP) Risk Rating untuk mendeteksi kerentanan keamanan pada aplikasi berbasis website. Penelitian ini menghasilkan 2 faktor untuk memperkirakan Likelihood dan Impact, dari masing-masing faktor terdapat 3 resiko yang ditemukan yaitu risk severity High, risk severity Medium dan risk severity Low. Hasil penilaian resiko ini dapat membantu para pengelola dan pengembang sistem untuk menyadari resiko yang mungkin terjadi sehingga dapat mengambil tindakan untuk mencegah dan mengatasi resiko tersebut.

Kata kunci: Vulnerability, OWASP, Risk Rating.

Abstract

The school has a website as a medium that interactively displays information, and interaction media. The transition of traditional communication into the scope of website-based applications can be used by some cybercriminals with the aim of stealing students' confidential information with a specific purpose, so detecting website security vulnerabilities is very important to determine the level of risk by using the Open method. Web Application Security Project (OWASP) Risk Rating to detect security vulnerabilities in web-based applications. This study resulted in 2 factors to estimate Likelihood and Impact, from each factor there were 3 risks found, namely risk severity High, risk severity Medium and risk severity Low. The results of this risk assessment can help system managers and developers to be aware of the risks that may occur so that they can take action to prevent and overcome these risks.

Keywords: *Vulnerability, OWASP, Risk Rating*.

1. Pendahuluan

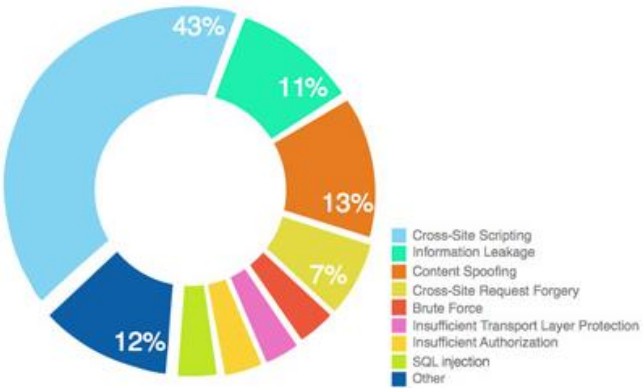
Pengujian sistem keamanan aplikasi berbasis website adalah hal yang penting di era perkembangan aplikasi berbasis web yang melaju dengan pesat. Semakin berkembangnya aplikasi berbasis web juga diiringi dengan tingginya serangan keamanan dari berbabagai teknik ancaman. Seringkali masalah keamanan berada di urutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting [1]. Oleh karena itu organisasi perlu melakukan asesmen pada aplikasi berbasis website agar oraganisasi mampu mendeteksi kerentanan dan memahami resiko yang dihadapi.

Jurnal Sistem Informasi dan Sistem Komputer, Vol. 7, No. 1, Januari 2022
ISSN: 2715-906X (Online)
10.51717/simkom.v7i1.63

Salah satu bentuk penilaian tingkat resiko kerentanan keamanan aplikasi berbasis website adalah OWASP Risk Rating Methodology. Langkah besar dalam mengukur tingkat resiko adalah menentukan dampak buruk yang dihasilkan dari analisa kerentanan [2].

Hasil dari analisa kerentanan dapat membantu pengelola dan pengembang sistem untuk mencegah dan mengatasi dampak resiko yang ditemukan pada sistem. Belum adanya Security Assessment pada sistem informasi yang dibangun oleh pihak DisnakerTrans. Saat ini dalam membangun sistem tersebut dengan mengandalkan library untuk mengamankan sistem. Namun dengan menerapkan library belum diiringi dengan pengujian sistem secara langsung dari internal perusahaan, sehingga belum mengetahui secara pasti celah keamanan sistem yang sudah dibangun. Oleh karena itu perlu adanya Security Assessment (penilaian keamanan) pada sistem tersebut. Ada beberapa faktor yang menyebabkan kurangnya tingkat keamanan pada aplikasi website, diantaranya adalah kesalahan penulisan kode program dan misconfiguration [3].

Kesalahan pada penulisan kode program dalam pembuatan aplikasi berbasis website sering dimanfaatkan oleh penyerang, dalam hal ini serangan yang sering dimanfaatkan oleh penyerang diantaranya adalah SQL Injection, Authentication dan XSS [4]. Seperti pada diagram statistik yang dirilis oleh webappsec.org (diperbaharui pada januari 2010) pada Gambar 1 menunjukan bahwa XSS (43%) dan SQL Injection (6%) merupakan jenis serangan yang sering digunakan [5].



Gambar 1. Persentase kerentanan website.

2. Metode

Metode penilaian resiko OWASP adalah suatu cara sederhana untuk menghitung dan menilai kerentanan resiko yang terdapat pada website. Dimana dengan metode tersebut dapat diputuskan apa saja yang harus dilakukan terhadap resiko-resiko tersebut [6]. Dengan mengetahui resiko yang akan terjadi maka banyak manfaat yang akan diperoleh diantaranya, menghemat waktu dan mengurangi terjadinya resiko yang lebih serius.

2.1 Scaning Website

Pada proses scaning website sekolah yang dituju kita copy terlebih dahulu url website sekolah tersebut, lalu kita buka software OWASP versi 2.11.0/versi yang terbaru, setelah memasuki halaman utama dari OWASP, kita pilih menu “Automated Scan”, dan paste url website sekolah tadi yang sudah kita copy pada bagian “URL to attack”, jika sudah, langsung saja klik “Attack”. Kita diharuskan untuk menunggu proses Scaning Website sampai selesai 100%, biasanya bisa sampai memakan waktu 1 – 3 jam. Apabila proses scaning sudah selesai, proses selanjutnya adalah membuat report, berikut langkah-langkahnya, pertama pilih menu “Report” di bagian atas, kedua klik “Generate Report”, ketiga membuat

Jurnal Sistem Informasi dan Sistem Komputer, Vol. 7, No. 1, Januari 2022
ISSN: 2715-906X (Online)
10.51717/simkom.v7i1.63

Report Title, dan keempat klik “Generate Report”, maka output dari file tersebut berupa file .html, dan disana terdapat informasi tentang resiko kerentanan dari website terebut. Seperti pada Gambar 2.

Alert type	Risk	Count
Cross Site Scripting (Reflected)	High	2 (0.2%)
SQL Injection	High	7 (0.6%)
Absence of Anti-CSRF Tokens	Low	179 (16.2%)
Cookie No HttpOnly Flag	Low	2 (0.2%)
Cookie without SameSite Attribute	Low	2 (0.2%)
Incomplete or No Cache-control Header Set	Low	52 (4.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	354 (32.0%)
Timestamp Disclosure - Unix	Low	157 (14.2%)
X-Content-Type-Options Header Missing	Low	223 (20.2%)
Information Disclosure - Suspicious Comments	Informational	127 (11.5%)

Gambar 2. File Report OWASP

3. Hasil dan Pembahasan

Mendeteksi kerentanan pada penelitian ini menggunakan aplikasi OWASP untuk mengetahui celah keamanan yang ada di aplikasi berbasis website. Dimana pengembangan aplikasi website yang sudah dibangun menggunakan PHP Native dan Framework CI (CodeIgniter) sebagai platform web application development. Faktor vulnerability bertujuan untuk memperkirakan kemungkinan vulnerability tertentu yang terlibat ditemukan dan dieksploitasi. Asumsikan dengan threat agent yang sudah dipilih. Berikut kriteria untuk memperkirakan Likelihood kelompok vulnerability factors antara lain. Ease of discovery seberapa mudah bagi kelompok threat agent untuk menemukan kerentanan ini? cara Praktis tidak mungkin (1), sulit (3), mudah (7), alat otomatis tersedia (9). Ease of exploit Seberapa mudah bagi kelompok threat agent untuk benar-benar memanfaatkan kerentanan ini? Alat bantu otomatis teoritis (1), sulit (3), mudah (5), tersedia (9). Awareness Seberapa terkenal kerentanan ini terhadap kelompok threat agent? Tidak diketahui (1), tersembunyi (4), jelas (6), pengetahuan umum (9). Intrusion detection Seberapa besar kemungkinan exploit untuk dideteksi? Deteksi aktif dalam aplikasi (1), login dan ditinjau (3), login tanpa review (8), tidak login (9).

ISSN: 2715-906X (Online)
10.51717/simkom.v7i1.63

4. Kesimpulan dan Saran

Hasil penilaian resiko ini dapat membantu para pengelola dan pengembang sistem untuk menyadari resiko yang mungkin terjadi sehingga dapat mengambil tindakan untuk mencegah dan mengatasi resiko tersebut. Hasil dari analisa kerentanan dapat membantu pengelola dan pengembang sistem untuk mencegah dan mengatasi dampak resiko yang ditemukan pada sistem. Metode penilaian resiko OWASP adalah suatu cara sederhana untuk menghitung dan menilai kerentanan resiko yang terdapat pada website.

Berdasarkan kesimpulan ada beberapa saran untuk dilakukan penelitian diantaranya menggunakan metode yang lain untuk melengkapi OWASP atau menggabungkan dua metode antara OWASP dan Cobit, untuk melakukan Security Assessment sebaiknya juga dilakukan proses uji penetrasi sistem secara manual. Penetrasi manual membutuhkan proses dan waktu yang lama karena harus melakukan uji coba untuk menemukan dan membuktikan celah keamanan yang ada pada sistem. Serta aplikasi berbasis web yang dibangun dan akan dilakukan Security Assessment ada baiknya membandingkan antara Framework Codeigniter dan Laravel.

Daftar Pustaka

[1] Web Application Security Consortium, http://www.webappsec.org/ Shanley, A., Johnstone, M. N., 2015, Selection of penetration testing methodologies: A comparison and evaluation, Australian Information Security Management Conference. Western Australia.

[2] Hutagalung, R. H., Nugroho, L. E., Hidayat, R., 2017, Menentukan Dampak Resiko Keamanan Berbasis Pendekatan Owasp, Prosiding SNATI F Ke-4 Tahun 2017, Kudus, Indonesia.

[3] Rao, R. M., Durgesh, P., 2010, Security risk assessment of Geospatial Weather Information System (GWIS): An OWASP based approach, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 5, Hal 24 – 32. [4] M. H. Botutihe, "Model Neural Network Berbasis Forward Selection," *Ilk. J. Ilm.*, vol. 9, pp. 239–243, 2017.

[4] uliharta, I. G. P. K., 2012, Business Impact Analysis Sistem dan Jaringan Komputer Menggunakan Metode Network Security Assessment, EKSPLORA INFORMATIKA, Vol. 2, No. 1, Hal 89 – 100.

[5] Kesuma, M. C., Shiddiqi, A. M., Pratomo, B. A., 2013, Pencari Celah Keamanan pada Aplikasi Web, Tugas Akhir, Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember.

[6] Rafiq, A., Touseef, P., Ashraf, M. A., Analysis of Risks against Web Applications in MVC. NFC IEFR Journal of Engineering and Scientific Research, Vol. 5, No. 1, hal. 1- 6.

[7] Fernando, Y. I., Abdillah, R., 2016, Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM), Jurnal CoreIT, Vol. 2, No.1, Hal 33 – 40.

[8] M. Mujib, A. Khafid, and S. Sumarlinda, "EasyChair Preprint Expert System Detecting Symptoms Of Game Addiction With The Forward Chaining Method And Certainty Factor," 2nd Int. Confrence Heal. Sci. Technol., 2021.

[9] P. Engrebeston, The Basics of Hacking and Penetration Testing, Waltham, Massachusetts: Elsevier Inc., 2011.

[10] Symantec, "Symantec Internet Security Threat Report," 2015. [Online]. Available: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GAinternet-security-threat-report-volume-20-2015-social_v2.pdf

[11] O. Foundation, "OWASP Top 10 - 2013 Release Candidate," 2013. [Online]. Available: https://code.google.com/p/owasptop10/.

[12] P. Engrebeston, The Basics of Hacking and Penetration Testing, Waltham, Massachusetts: Elsevier Inc., 2011.

[13] Rao, R. M., Durgesh, P., 2010, Security risk assessment of Geospatial Weather Information System (GWIS): An OWASP based approach, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 5, Hal 24 – 32.

ISSN: 2715-906X (Online)
10.51717/simkom.v7i1.63

[14] Shanley, A., Johnstone, M. N., 2015, Selection of penetration testing methodologies: A comparison and evaluation, Australian Information Security Management Conference. Western Australia. 30 November – 2 Desember 2015.

[15] Kesuma, M. C., Shiddiqi, A. M., Pratomo, B. A., 2013, Pencari Celah Keamanan pada Aplikasi Web, Tugas Akhir, Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember.

[16] Fernando, Y. I., Abdillah, R., 2016, Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM), Jurnal CoreIT, Vol. 2, No.1, Hal 33 – 40.

[17] Hutagalung, R. H., Nugroho, L. E., Hidayat, R., 2017, Menentukan Dampak Resiko Keamanan Berbasis Pendekatan Owasp, Prosiding SNATI F Ke-4 Tahun 2017, Kudus, Indonesia.