Analisis Kerawanan Pada Aplikasi Website Menggunakan Standar OWASP Top 10 Untuk Penilaian *Risk Rating*

Hermawan Setiawan[1)], Lytio Enggar Erlangga[2)], Syubbanul Siddiq[3)], Yusuf Atha Gunawan[4)]

(1) Rekayasa Perangkat Lunak Kripto, Politeknik Siber dan Sandi Negara, hermawan.setiawan@poltekssn.ac.id

(2) Badan Siber dan Sandi Negara, lytio.enggar@bssn.go.id

(3) Rekayasa Perangkat Lunak Kripto, Politeknik Siber dan Sandi Negara, syubbanul.siddiq@student.poltekssn.ac.id

(4) Rekayasa Perangkat Lunak Kripto, Politeknik Siber dan Sandi Negara, yusuf.atha@student.poltekssn.ac.id

Abstrak

Sejak tahun 2011, SMA N "ABC" menerapkan sistem informasi yang dibangun berbasis web. Sistem informasi tersebut ditujukan sebagai pengantar informasi dan media pembelajaran bagi siswanya. Sistem tersebut tidak pernah mendapatkan audit dan/atau pengujian keamanan sehingga belum diketahui kerawanannya. Dengan pendekatan aplikasi Acunetix untuk menguji keamanan aplikasi SI SMAN "ABC", dilakukan scanning vulnerability dan vulnerability assessment menggunakan Open Web Application Security Project (OWASP) Top 10 Security Risk 2017 dan Open Web Application Security Project (OWASP) Risk Rating Methodology. Proses scanning dilakukan berkali-kali sampai dengan terpenuhinya kriteria OWASP melalui pendekatan metoda tindakan kelas. Dari hasil scanning vulnerability terakhir ditemukan tiga belas kerawanan mulai dari kategori tinggi hingga rendah. Berdasarkan penilaian kerawanan yang terdeteksi, menghasilkan skala 5.72 untuk kemungkinan kerawanan dapat dieksploitasi oleh penyerang dan skala 3.315 untuk dampak terhadap proses bisnis di SMA N "ABC".

Kata kunci: *action research* (1), *scanning vulnerability*(2), *vulnerability assessment* (3)

Abstract

Since 2011, SMA N "ABC" has implemented a web-based information system. The information system is intended as an introduction to information and learning media for students. The system has never been audited and/or tested for security, so the vulnerability is not yet known. With the Acunetix application approach to test the security of the SI SMA N "ABC" application, vulnerability scanning and vulnerability assessment were carried out using the Open Web Application Security Project (OWASP) Top 10 Security Risk 2017 and the Open Web Application Security Project (OWASP) Risk Rating Methodology. The scanning process is carried out many times until the OWASP criteria are met through the class action method approach. From the results of scanning vulnerabilities found thirteen vulnerabilities ranging from high to low categories. From the results of the last vulnerability scanning, it was found thirteen vulnerabilities ranging from high to low categories. Based on the assessment of detected vulnerabilities, resulting in a scale of 5.72 for the possibility of vulnerabilities being exploited by attackers and a scale of 3,315 for the impact on business processes in SMA N "ABC .

Keywords: *action research* (1), *scanning vulnerability* (2), *vulnerability assessment* (3)

1. PENDAHULUAN

Sistem informasi saat ini memiliki peran yang sangat penting bagi keberlangsungan suatu perusahaan atau institusi seperti meningkatkan efisiensi dan efektivitas [1]. Sistem informasi saat ini memiliki peran yang sangat penting bagi keberlangsungan suatu perusahaan atau institusi seperti meningkatkan efisiensi dan efektivitas berkembang menjadi media yang dapat diakses oleh semua pengguna internet. Para pengguna dapat melihat data siswa alumni lengkap dengan alamat dan nomor telepon. Akan tetapi, satu hal yang pasti adalah tidak ada satupun yang aman pada dunia siber [2].

Dengan semakin banyaknya serangan di dunia siber maka instansi selayaknya melakukan uji keamanan terhadap system yang dimilikinya. Namun termasuk pada lokus ini belum ada upaya dari pihak pengelola sistem informasi untuk melakukan uji coba terkait keamanan yang ada di pada sistem informasi tersebut. Pengujian periodik terhadap sistem tentu saja sangat penting.

Kejahatan dunia maya sudah sangat marak dikalangan masyarakat terutama pendidikan [3]. Bahkan siswa yang masih berstatus sebagai pelajar di sekolah menengah pertama dapat melakukan sebuah serangan yang nantinya dapat merugikan suatu perusahaan maupun instansi.

OWASP Top 10 adalah standar industri dari risiko keamanan aplikasi yang paling kritis. Metrik OWASP didasarkan pada beberapa faktor seperti prevalensi kelemahan, deteksi, eksploitasi, dan faktor dampak teknis [4].

Sistem informasi SMA N "ABC" merupakan aplikasi berbasis web yang dibuat tanpa adanya audit dan/atau pengujian. Sehingga belum diketahui kerawanan yang ada pada aplikasi tersebut [5]. Oleh karena itu, dibutuhkan suatu pengujian terhadap

keamanan pada sistem informasi SMA N "ABC" . Untuk melakukan pengujian keamanan, akan dilakukan *vulnerability scanning* menggunakan *tools* Acunetix [6]. Dari 6 *tools* yang dibandingkan data yang diperoleh dari skenario yang diterapkan dan program uji bahwa Acunetix menepati urutan ke 2 dari 6 *tools* yang dibandingkan [7]. Sejalan dengan hal itu, [8] menunjukkan banyaknya penelitian yang mengevaluasi *tools* tersebut.

Dengan bantuan metodologi tindakan kelas yang banyak digunakan dalam dunia pendidikan, pengujian keamanan dengan Acunetix dilakukan. Berbeda dengan [9], [10] penelitian ini menggunakan pendekatan tindakan kelas untuk dapat memenuhi kriteria OWASP melalui *tool* Acunetix [11]. Metodologi tersebut untuk mendeteksi pemenuhan kriteria yang dilakukan secara berulang sesuai dengan pendekatan tindakan kelas.

Pendekatan *assesment* itulah yang dilakukan terhadap keamanan yang terdapat pada sistem informasi SMA N "ABC" menggunakan standar *Open Web Application Security Project* (OWASP) *Top 10 Security Risks*.

2. LANDASAN TEORI

2.1. OWASP Top 10 Security Risks

OWASP (*Open Web Application Security Project*) merupakan organisasi internasional yang bergerak dalam mengembangkan, memperoleh, mengoperasikan dan memelihara suatu aplikasi agar dapat terjaga keamanannya. OWASP menyediakan berbagai *tools*, dokumen dan forum diskusi yang dapat diakses secara bebas untuk meningkatkan keamanan suatu aplikasi [12].

OWASP memiliki standar (*touchpoint*) untuk meningkatkan keamanan aplikasi. OWASP Top 10 merupakan standar (*touchpoint*) keamanan aplikasi web yang paling umum digunakan, dengan tujuan untuk mendidik pengembang, perancang, manajer dan organisasi tentang dampak dari kerawanan keamanan pada aplikasi web. Top 10 menyediakan panduan mengenai teknik dasar dalam mengamankan suatu aplikasi dan memberikan panduan mengenai cara untuk mengatasi kerawanan yang beresiko tinggi pada suatu aplikasi [13].

2.2. *Penetration Testing*

Penetration test akan menunjukkan kerentanan dan mendokumentasikan bagaimana kelemahan tersebut dapat dieksploitasi. Selain itu, juga dapat menunjukkan cara penyerang dapat mengeksploitasi beberapa kerentanan kecil untuk membocorkan informasi dengan komputer atau jaringan. *Penetration test* mengekspos kesenjangan dalam model keamanan suatu organisasi dan membantu organisasi mencapai keseimbangan antara kecakapan teknis dan fungsionalitas bisnis dari perspektif potensi pelanggaran keamanan. Informasi dari hasil *Penetration test* berguna selama pemulihan bencana dan perencanaan kesinambungan bisnis [14].

Penetration test mensimulasikan metode yang digunakan oleh penyusup untuk mendapatkan akses tidak sah ke jaringan organisasi. *Penetration test* melibatkan teknik manual untuk melakukan yang ditargetkan pengujian pada sistem spesifik untuk memastikan bahwa tidak ada celah keamanan yang mungkin tidak terdeteksi sebelumnya.

Terdapat tiga tipe *Penetration test* yaitu *Black box testing* (*zero-knowledge testing*), *White box testing* (*complete-knowledge testing*), dan *Gray box testing* [15].

Acunetix menguji keamanan aplikasi web secara otomatis dan mengaudit aplikasi web dengan memeriksa kerentanan. *Tool* tersebut lebih memperinci bagian mana yang perlu diperiksa lebih lanjut. Penyajian laporan Acunetix lebih jauh dapat mengerti permasalahan yang dihadapi pada suatu aplikasi [16].

3. METODE PENELITIAN

Metodologi penilaian risiko OWASP adalah pendekatan sederhana untuk menghitung dan menilai risiko yang terkait dengan aplikasi. Dengan metode tersebut dapat diputuskan apa saja yang harus dilakukan terhadap risiko-risiko yang ada. Dengan mengetahui risiko yang akan terjadi, maka banyak manfaat yang akan diperoleh, diantaranya menghemat waktu dan mengurangi terjadinya risiko yang lebih serius. Perkiraan risiko dimulai dengan model:

*Risk = Likelihood * Impact*

Keterangan:

Likelihood: Kemungkinan kerentanan untuk dieksploitasi oleh penyerang

Impact: Dampak dari serangan yang berhasil sukses

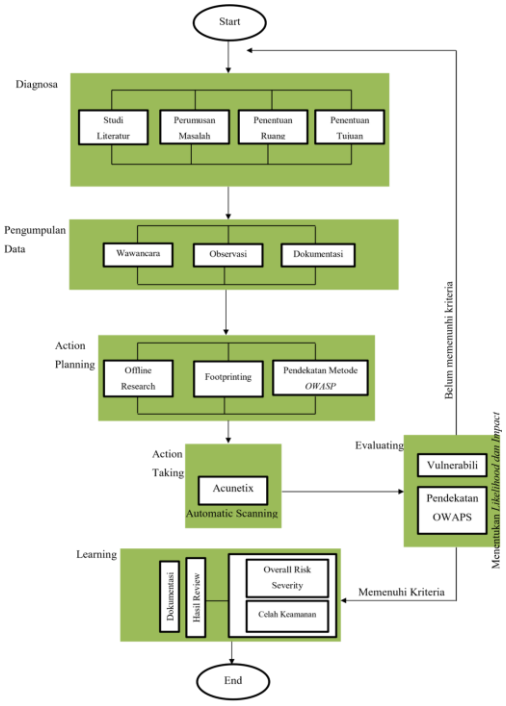
Risk: Kemungkinan risiko yang terkait dengan faktor ancaman, kerentanan, dampak teknis dan bisnis.

3.1. Penelitian Tindakan

Metodologi penelitian yang digunakan adalah metodologi penelitian tindakan kelas atau *action research*. Dalam metode *action research*, terdapat lima tahap penelitian yang harus dilakukan. Tahap pertama adalah diagnosa. Tahap kedua adalah membuat rencana tindakan *(action planning)*. Tahap ketiga adalah melakukan tindakan *(action taking)*. Tahap keempat adalah evaluasi *(evaluating)*. Tahap kelima adalah pembelajaran *(learning)*[17].

3.2. Alur Penelitian

Alur penelitian merupakan tahap yang harus dilakukan dalam penelitian, hingga mencapai suatu kesimpulan. Adapun alur penelitian yang penulis gunakan seperti terlihat pada Gambar 1.



Gambar 1. Diagram Alur Penelitian

4. HASIL DAN PEMBAHASAN

Berdasarkan OWASP *Risk Rating*, terdapat beberapa tahapan untuk menentukan dan mengkombinasikan besarnya resiko yang ditimbulkan, tahapan tersebut diantaranya *threat agent factor*, *vulnerability factors*, dan *business impact* [18]. Pada Tabel 1 ditunjukkan daftar celah keamanan yang ada di sistem informasi SMA N "ABC".

Tabel 1. Daftar celah keamanan yang ditemukan

No	Kerawanan
1	*Cross site scripting*
2	*Directory Listing*
3	*Clickjacking*
4	*PHP allow_url_fopen_enabled*
5	*Possible sensitive directories*
6	*PHPinfo page found*
7	*Possible relative path overwrite*
8	*Possible relative path overwrite*
9	*Possible sensitive files*
10	*Content Security Policy (CSP) not implemented*
11	*Email address found*
12	*Possible internal IP address disclosure*
13	*Possible server path disclosure (Unix)*
14	*Possible username or password disclosure*

4.1. *Threat Agent Factor*

Tahap ini bertujuan untuk memperkirakan serangan yang berhasil oleh kelompok *threat agent* [19]. Terdapat kriteria untuk memperkirakan *likelihood* kelompok *threat agent factors*, diantaranya:

a. *Skill level* adalah keterampilan penetrasi yang dimiliki threat agent, dibagi menjadi lima skala nilai yaitu penetration testing bernilai sembilan, keterampilan jaringan dan pemrograman bernilai enam, pengguna komputer tingkat lanjut bernilai 5, beberapa keterampilan teknis bernilai 3, tidak ada keterampilan teknis bernilai satu
b. *Motive* adalah motivasi untuk melakukan sebuah serangan, dibagi menjadi 3 skala nilai yaitu mendapat reward yang tinggi bernilai 9, memungkinkan mendapat reward bernilai 4, tidak mendapatkan reward bernilai 1.
c. *Opportunity* adalah sumber daya yang dibutuhkan untuk menemukan kerentanan, dibagi menjadi empat skala nilai yaitu tidak ada akses atau sumber daya yang diperlukan bernilai sembilan, beberapa akses atau sumber daya yang dibutuhkan bernilai 7, akses khusus atau sumber daya yang dibutuhkan bernilai 4, akses penuh atau membutuhkan sumber daya yang mahal bernilai 0.
d. *Size* adalah seberapa besar kelompok threat agent, dibagi menjadi enam skala nilai yaitu pengembang bernilai 2, administrator sistem bernilai 2, pengguna internet bernilai 4, mitra bernilai 6, pengguna terotentikasi bernilai 6, pengguna internet anonim bernilai sembilan.

Rumus yang digunakan untuk mendapatkan hasil *threat agent* secara keseluruhan menggunakan persamaaan:

$$Threat\ Agent = \frac{Skill + level + Motive + Opportunity + Size}{4}$$

Hasil pilihan *threat agent factor* yang sudah disediakan oleh OWASP *risk rating*, tercantum pada Tabel 2.

Tabel 2. Skor *Threat Agent Factor*

Jenis Ancaman	*Skill Level*	*Motive*	*Opportunity*	*Size*
Clickjacking	9	9	4	9
PHP allow_url_fopen_enabled	9	9	4	9
Content Security Policy (CSP) not implemented	9	4	7	9
Email address found	6	4	9	9
Possible relative path overwrite	5	4	9	9
Possible sensitive files	5	4	9	9
Possible internal IP address disclosure	5	4	9	9
Possible server path disclosure (Unix)	5	4	9	9
Possbile username or password disclosure	5	4	9	9
Cross site scripting	9	1	4	9
Possible sensitive directories	9	1	4	9
Directory Listing	6	3	4	9
PHPinfo page found	6	4	9	2

Dari Tabel 2 diperoleh nilai *skill level* sebesar 6,77 yang termasuk keterampilan penetrasi yang dimiliki *threat agent* adalah keterampilan jaringan dan pemrograman, *motive* bernilai 4,2 yakni motivasi

untuk melakukan sebuah serangan memungkinkan mendapat *reward*, *opportunity* bernilai 6,9 yang berarti beberapa akses atau sumber daya yang dibutuhkan untuk menemukan kerentanan dan *size* bernilai 8,4 berarti kelompok *threat agent* merupakan pengguna internet anonim [20].

4.2. *Vulnerability factors*

Faktor kedua terkait dengan kerawanan yang ada. Dengan tujuan untuk memperkirakan kemungkinan kerawanan tertentu yang ditemukan dan dieksploitasi. Asumsikan dengan threat agent yang sudah dipilih. Berikut kriteria untuk memperkirakan *likelihood* kelompok *vulnerability factors*:

a. *Ease of discovery* adalah tingkat kesulitan bagi kelompok *threat agent* untuk menemukan kerawanan yang ada. Terbagi menjadi empat dengan skala penilaian yang berbeda. Tidak mungkin bernilai 1, sulit bernilai 3, mudah bernilai 7, alat otomatis tersedia bernilai 9.
b. *Ease to exploit* adalah tingkat kesulitan bagi kelompok *threat agent* untuk benar-benar memanfaatkan kerentanan yang ada. Terbagi menjadi empat dengan skala penilaian yang berbeda. Alat bantu otomatis teoritis bernilai 1, sulit bernilai 3, mudah bernilai 5, tersedia bernilai 9.
c. *Awareness* adalah tingkat kerawanan terhadap kelompok *threat agent*. Terbagi menjadi empat dengan skala penilaian yang berbeda. Tidak diketahui bernilai 1, tersembunyi bernilai 4, jelas bernilai 6, pengetahuan umum bernilai 9.
d. *Intrusion detection* adalah kemungkinan *exploit* untuk dideteksi. Terdapat empat kriteria dengan skala penilaian yang berbeda. Deteksi aktif dalam aplikasi bernilai 1, *login* dan ditinjau bernilai 3, *login* tanpa *review* bernilai 8, tidak *login* bernilai 9.

Rumus yang dapat digunakan untuk mendapatkan hasil *vulnerability factors* secara keseluruhan mengikuti OWASP *risk rating* menggunakan persamaan:

$$Vulnerability\ factors = \frac{Ease\ to\ discovery + Ease\ to\ exploit + Awareness + Instrusion\ Detection}{4}$$

Hasil skala nilai *vulnerability factor* yang sudah disediakan oleh OWASP *risk rating*, tercantum pada Tabel 3. Dari Tabel 3 diperoleh nilai *Ease to discovery* sebesar 9 yang berarti alat otomatis tersedia bagi kelompok *threat agent* untuk menemukan kerawanan yang ada, dan *Ease of exploit* bernilai 3,1 yakni sulit bagi kelompok *threat agent* untuk benar-benar memanfaatkan kerentanan yang ada. *Awareness* bernilai 4,77 yang berarti bahwa kerawanan terhadap kelompok *threat agent* tersembunyi, dan *Intrusion Detection* bernilai 1 yakni kemungkinan *exploit* untuk dideteksi *login* dan ditinjau [20].

Tabel 3. Skor *Vulnerability Factor*

Jenis Ancaman	*Ease to discovery*	*Ease of exploit*	*Awareness*	*Intrusion Detection*
PHP info page found	9	3	9	1
Content Security Policy (CSP) not implemented	9	3	9	1
Clickjacking	9	5	4	1
Cross site scripting	9	3	4	1
Directory Listing	9	3	4	1
PHP allow_url_fopen_ enabled	9	3	4	1
Possible sensitive directories	9	3	4	1
Possible relative path overwrite	9	3	4	1
Possible sensitive files	9	3	4	1
Email address found	9	3	4	1
Possible internal IP address disclosure	9	3	4	1
Possible server path disclosure (Unix)	9	3	4	1
Possbile sername or password disclosure	9	3	4	1

4.3. *Technical Impact*

Tujuan utama dari dampak teknis adalah menghitung besarnya dampak jika kerentanan dieksploitasi dari aplikasi. Faktor dampak teknis lebih jauh dibagi menjadi empat kelas, yaitu kerahasiaan integritas, ketersediaan, dan akuntabilitas [21]. Tujuan keamanan sistem informasi adalah melindungi keempat hal tersebut. Terdapat empat kriteria dalam *technical impact*, yaitu:

a. *Loss of confidentiality* adalah tingkat kerahasiaan data yang dapat diungkap dan seberapa sensitif data tersebut. Dibagi menjadi lima dengan nilai skala yang berbeda. Data yang diungkap minimum dan tidak sensitif bernilai 2, minimal data kritis yang diungkap bernilai 6, data non-sensitif ekstensif yang diungkapkan bernilai 6, data kritis dan ekstensif diungkapkan bernilai 7, semua data yang diungkapkan bernilai 9.
b. *Loss of integrity* adalah tingkat integritas data yang rusak dan seberapa besar kerusakannya. Terbagi menjadi empat dengan skala nilai yang berbeda. Data korup yang minimal sedikit bernilai 1, data korup minimal yang serius bernilai 3, data yang agak korup bernilai 7, semua data korup bernilai 9.
c. *Loss of availability* adalah tingkat layanan yang hilang dan seberapa vital layanan tersebut. Terbagi menjadi lima dengan skala nilai yang berbeda. Layanan sekunder minimal terputus

bernilai 1, layanan primer minimal terputus bernilai 5, layanan sekunder yang luas terganggu bernilai 5, layanan utama yang luas terganggu bernilai 7, semua layanan hilang bernilai 9.

d. *Loss of accountability* adalah tingkat akuntabilitas tindakan dari *threat agent* dapat dilacak. Terbagi menjadi tiga dengan nilai skala yang berbeda. Sepenuhnya dapat dilacak bernilai 1, mungkin dapat dilacak bernilai 7, anonim bernilai 9.

Rumus yang dapat digunakan untuk mendapatkan hasil *technical impact* secara keseluruhan mengikuti OWASP *Risk Rating* menggunakan persamaan:

$$Technical\ Impact\ = \frac{Confidentiality + Integrity + \ Avaibility\ + Accountability}{4}$$

Berikut adalah hasil dari penilaian *technical impact* yang sudah disediakan oleh OWASP *risk rating*, seperti pada Tabel 4.

Tabel 4. Skor *Technical Impact*

Jenis Ancaman	*(a)*	***(b)***	©	*(d)*
Cross site scripting	7	3	1	9
Directory Listing	2	1	1	1
Clickjacking	2	1	1	9
PHP allow_url_fopen_ena bled	6	3	1	7
Possible sensitive directories	2	1	1	7
PHPinfo page found	2	1	1	1
Possible relative path overwrite	2	1	1	7
Possible sensitive files	2	1	1	7
Content Security Policy (CSP) not implemented	6	3	1	9
Email address found	2	1	1	1
Possible internal IP address disclosure	2	1	1	7
Possible server path disclosure (Unix)	2	1	1	7
Possbile username or password disclosure	2	1	1	7

Keterangan:
(a) = *Loss of Confidentiality*
(b) = *Loss of Integrity*
(c) = *Loss of Avaibility*
(d) = *Loss of Accountability*

Dari Tabel 4 diperoleh nilai *Loss of Confidentiality* sebesar 3 berarti banyak data yang dapat diungkap minimum dan tidak sensitif, *Loss of Integrity* bernilai 1,46 yakni data korup yang minimal sedikit, *Loss of Avaibility* bernilai 1 artinya layanan sekunder minimal terputus, dan *Loss of Accountability* bernilai 6 adalah tindakan dari *threat agent* mungkin dapat dilacak [20].

4.4. *Business impact*

Tujuan akhir dari penilaian risiko adalah untuk mengukur dampak bisnis. Pada umumnya, suatu organisasi harus mengarahkan risiko organisasi dengan dampak bisnis ke depannya [21]. Berikut merupakan faktor untuk memperkirakan *business impact*:

a. *Financial Damage* adalah tingkat kerusakan finansial yang diakibatkan oleh eksploitasi. Terbagi menjadi empat dengan nilai skala yang berbeda, yaitu: kurang biaya untuk memperbaiki kerentanan bernilai 1, pengaruh kecil terhadap laba tahunan bernilai 3, berpengaruh signifikan terhadap laba tahunan bernilai 7, kebangkrutan bernilai 9.
b. *Reputation Damage* adalah tingkat kerusakan reputasi yang akan merugikan bisnis berdasarkan hasil eksploitasi yang dilakukan. Terbagi menjadi empat dengan skala nilai yang berbeda, yaitu: kerusakan minimal bernilai 1, kehilangan akun utama bernilai 4, kehilangan niat baik bernilai 5, kehilangan merek bernilai 9.
c. *Non-Compliance* adalah tingkat keterpaparan yang tidak dikenali. Terbagi menjadi tiga dengan skala nilai yang berbeda, yaitu: pelanggaran ringan bernilai 2, pelanggaran yang jelas bernilai 5, pelanggaran profil tinggi bernilai 7.
d. *Privacy Violation* adalah tingkat pelanggaran informasi pribadi yang dapat diungkap akibat eksploitasi. Terbagi menjadi empat dengan nilai skala yang berbeda, antara lain: satu orang bernilai 3, ratusan orang bernilai 5, ribuan orang bernilai 7, jutaan orang bernilai 9.

Rumus yang dapat digunakan untuk mendapatkan hasil *technical impact* secara keseluruhan mengikuti OWASP *Risk Rating* menggunakan persamaan:

$$Technical\ Impact\ = \frac{Confidentiality + Integrity + \ Avaibility\ + Accountability}{4}$$

Hasil dari penilaian business impact yang sudah disediakan oleh OWASP *risk rating*, seperti pada Tabel 5.

Tabel 5. Skor *Business Impact*

Jenis Ancaman	(1)	(2)	(3)	(4)
Cross site scripting	1	1	2	3
Directory Listing	1	1	2	3
Clickjacking	1	1	2	3
PHP allow_url_fopen_ena bled	1	1	2	3
Possible sensitive directories	1	1	2	3
PHPinfo page found	1	1	2	3
Possible relative path overwrite	1	1	2	3
Possible sensitive files	1	1	2	3
Content Security Policy (CSP) not implemented	1	1	2	3
Email address found	1	1	2	3
Possible internal IP address disclosure	1	1	2	3
Possible server path disclosure (Unix)	1	1	2	3
Possbile username or password disclosure	1	1	2	3

Keterangan
(1) = *Financial Damage*
(2) = *Repitation Damage*

(3) = *Non compliance*
(4) = *Privacy Violation*

Dari Tabel 5 diperoleh *Financial Damage* sebesar 1 yang menunjukkan kerusakan finansial yang diakibatkan oleh eksploitasi kurang biaya untuk memperbaiki kerentanan, *Repitation Damage* bernilai 1 yakni kerusakan reputasi yang akan merugikan bisnis berdasarkan hasil eksploitasi yang dilakukan minimal, *Non compliance* bernilai 2 yaitu keterpaparan yang tidak dikenali ringan dan *Privacy Violation* bernilai 3 artinya satu orang informasi pribadi yang dapat diungkap akibat eksploitasi[20].

4.5. Hasil

Hasil tingkat risiko keamanan akan dihitung dan diakumulasikan sebagai hasil akhir penilaian tingkat risiko. Perhitungan dilakukan dengan menggunakan persamaan:

$$Likelihood = \frac{Threat\ Agent\ Factor + Vulnerability\ Factors}{2}$$

$$Impact = \frac{Technical\ Impact + Business\ Impact}{2}$$

Skor secara keseluruhan *likelihood* dan *impact* dari sistem informasi SMA N "ABC" adalah 5.72 termasuk pada resiko medium dan 3.315 termasuk pada dampak yang rendah. Nilai skor keseluruhan factor tercantum pada Tabel 6.

Tabel 6. Skor keseluruhan faktor

	Faktor 1	*Faktor 2*	*Faktor 3*	*Faktor 4*	*Total*	*Risk*
Threat Agent Factors	*4.65*	*4*	*10.6*	*8.73*	*27.98*	*5.72*
Vulnerability Factors	9	2.85	4.96	1	17.81	
	Faktor 1	*Faktor 2*	*Faktor 3*	*Faktor 4*	*Total*	*Impact*
Technical Impact	1.69	0.92	1	6.15	9.76	3.315
Business Impact	1	1	2	3	7	

5. KESIMPULAN

Berdasarkan hasil *security assessment* dengan menggunakan OWASP *Risk Rating* terhadap aplikasi berbasis website yang dimiliki SMA N "ABC" dapat disimpulkan:

1. Perlu adanya penilaian risiko kerentanan keamanan terhadap aplikasi berbasis website agar terlihat potensi risiko keamanan untuk mencegah dan mengatasi risiko keamanan.
2. Terdapat 13 kerawanan pada website SMA N "ABC". Dengan rincian: 1 risiko memiliki *risk severity high*, 10 memiliki *risk severity medium*, dan 2 memiliki *risk severity low*.
3. Skala kemungkinan serangan yang dapat dieksploitasi oleh penyerang (*likelihood*) sebesar 5.72. Sedangkan *impact* yang diperoleh sebesar 3.315.

Hasil penelitian dengan pemeringkatan kerentanan menunjukkan, bahwa keamanan harus mendapat perhatian serius karena website sekolah ada peluang untuk disalahgunakan. Penelitian selanjutnya bisa mengembangkan dengan pendekatan metode lain agar hasil lebih detail.

REFERENSI

[1] R. Tores, "PERANAN SISTEM INFORMASI DALAM MENINGKATKAN EFISIENSI DAN EFEKTIVITAS PENYIARAN DI RADIO DANGDUT INDONESIA (RDI) SEKAYU," um-palembang, 2017.

[2] H. P. Siagian, "ULNERABILITY ASSESSMENT PADA WEB SERVER WWW.BINADARMA.AC.ID," Jurnal Mahasiswa Teknik Informatika., 2014, Accessed: Oct. 28, 2022. [Online]. Available: http://eprints.binadarma.ac.id/id/eprint/2018

[3] N. Qomariah, "Sekolah Online di Inggris Berhenti Gara-Gara Serangan Siber," Republika, Mar. 05, 2021.

[4] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," Creative Information Technology Journal, vol. 4, no. 4, p. 264, Jan. 2019, doi: 10.24076/citec.2017v4i4.119.

[5] R. Aditya Pratama Wijaya, A. Rahman Hakim, S. Tinggi Sandi Negara, and P. Korespondensi, "PERANCANGAN PERANGKAT AUDIT INTERNAL UNTUK SISTEM KEAMANAN INFORMASI PADA ORGANISASI XYZ," vol. 7, no. 3, pp. 435–442, 2020, doi: 10.25126/jtiik.202071940.

[6] A. Elanda and R. Lintang Buana, "ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10," vol. 6, no. 2, pp. 2502–714, 2021.

[7] M. Ula, "Evaluasi Kinerja Software Web Penetration Testing," TECHSI - Jurnal Teknik Informatika, vol. 11, no. 3, p. 336, Oct. 2019, doi: 10.29103/techsi.v11i3.1996.

[8] S. Alazmi and D. C. de Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," IEEE Access, vol. 10. Institute of Electrical and Electronics Engineers Inc., pp. 33200–33219, 2022. doi: 10.1109/ACCESS.2022.3161522.

[9] A. Santos-Olmo, L. E. Sánchez, D. G. Rosado, E. Fernández-Medina, and M. Piattini, "Applying the action-research method to

develop a methodology to reduce the installation and maintenance times of Information Security Management Systems," Future Internet, vol. 8, no. 3, Sep. 2016, doi: 10.3390/fi8030036.

[10] I. Lopes and P. Oliveira, "Applying action research in the formulation of information security policies," in Advances in Intelligent Systems and Computing, 2015, vol. 353, pp. 513–522. doi: 10.1007/978-3-319-16486-1_50.

[11] A. Elanda and R. Lintang Buana, "ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10," 2021.

[12] "OWASP Top 10-2017," 2003. [Online]. Available: https://github.com/OWASP/Top10/issues

[13] I. M. Edy Listartha, I. M. A. Premana Mitha, M. W. Aditya Arta, and I. Km. W. Yuda Arimika, "Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project)," SIMKOM, vol. 7, no. 1, pp. 23–27, Jan. 2022, doi: 10.51717/simkom.v7i1.63.

[14] F. Fachri, A. Fadlil, I. Riadi, A. Dahlan, Y. Jln Soepomo, and I. Artikel, "Analisis Keamanan Webserver Menggunakan Penetration Test," JURNAL INFORMATIKA, vol. 8, no. 2, 2021, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/ji

[15] M. E. Khan and F. Khan, "A Comparative Study of White Box, Black Box and Grey Box Testing Techniques," 2012. [Online]. Available: www.ijacsa.thesai.org

[16] R. Pangalila, A. Noertjahyana, and J. Andjarwirawan, "Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra".

[17] A. Zakiah, A. Ekawijana, and E. A. Laksana, "IMPLEMENTASI METODE ACTION RESEARCH UNTUK PENINGKATAN DAYA SAING UMKM MELALUI E-COMMERCE IMPLEMENTATION OF ACTION RESEARCH FOR IMPROVING THE COMPETITIVENESS OF SMES WITH E-COMMERCE."

[18] I. M. E. Listartha, "ANALISIS KERENTANAN WEBSITE SMA NEGERI 2 AMLAPURA MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT)," Prosiding Seminar Nasional Teknologi dan Informatika, 2017.

[19] T. Casey, P. Koeberl, and C. Vishik, "Threat agents: A necessary component of threat analysis," in ACM International Conference Proceeding Series, 2010. doi: 10.1145/1852666.1852728.

[20] M. M. Naier, A. Hamidi, and R. Momand, "Analysis of Web Application Security Vulnerabilities: A Case Study of Web Applications in Afghanistan," 2020. [Online]. Available: http://ijses.com/

[21] B. Ghozali, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating Detect Web Application Security Flaws Using the Owasp (Open Web Application Security Project) Method for Risk Assessment," Dikirim: 09 Februari, 2018.

[22]