ANALISIS KEAMANAN SISTEM INFORMASI PADA WEBSITE PT SENTRA VIDYA UTAMA (SEVIMA) MENGGUNAKAN METODE OWASP

INFORMATION SYSTEM SECURITY ANALYSIS ON PT SEVIMA WEBSITE USING THE OWASP METHOD

Nabila Athifah Zahra[1*], Farras Hafish Zidane[1], Nur Racana Kuslaila[1]
*E-mail: nabilazahra1734@gmail.com

[1]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jawa Timur

Abstrak

Keamanan sistem informasi menjadi hal utama yang harus diperhatikan ketika mengembangkan sebuah aplikasi karena memiliki peran krusial untuk proses bisnis perusahaan. Salah satu perusahaan *software house* yang bergerak di bidang pendidikan yaitu PT Sentra Vidya Utama memiliki beberapa produk website untuk mendukung proses bisnis perusahaan, salah satu nya adalah *platform* maukuliah.id. Website ini memudahkan mitra kampus SEVIMA untuk melakukan promosi dan memudahkan calon mahasiswa menemukan kampus atau jurusan yang diinginkan. Terdapat beberapa fitur yang memungkinkan celah kerentanan keamanan pada website seperti fitur pencarian, formulir, dan kontak. Ancaman kerentanan tersebut berpotensi menghambat proses bisnis perusahaan. Oleh karena itu, dalam penelitian ini akan dilakukan pengujian terkait dengan keamanan website secara *black box testing* menggunakan metode *Open Web Application Security Project* (OWASP). Hasil yang diperoleh melalui pengujian menggunakan software OWASP ZAP menunjukkan bahwa tingkat kerentanan celah website maukuliah.id berada di level *medium* hingga *low* dengan skor secara keseluruhan sebesar 5.75 (*medium*). Untuk melakukan pencegahan diperlukan adanya pemasangan *website security* seperti CSP, XSS, dan lain sebagainya.

Kata kunci: *vulnerability testing, OWASP Risk Rating, website*

Abstract

Information system security is the main thing that must be considered when developing an application because it has a crucial role in the company's business processes. One of the software house companies engaged in education, PT Sentra Vidya Utama, has several website products to support the company's business processes, one of their product is maukuliah.id platform. This website makes it easier for SEVIMA campus partners to carry out promotions and prospective students to find the desired campus or major. Several features allow website security vulnerabilities, such as search features, forms, and contacts. The threat of these vulnerabilities could hamper the company's business processes. Therefore, in this study, testing related to website security in black box testing using the Open Web Application Security Project (OWASP) method will be carried out. The results obtained through testing using the OWASP ZAP software show the vulnerability level of the maukuliah.id website gap is medium to low, with an overall score of 5.75 (medium). To prevent it, it is necessary to install website security such as CSP, XSS, etc.

Keywords: *vulnerability testing, OWASP Risk Rating, website*

1. PENDAHULUAN

Keamanan website memiliki peranan penting bagi perusahaan karena mampu memberikan kemudahan bagi perusahaan untuk menjalankan proses bisnisnya dengan aman dan terjaga [1]. Salah satu perusahaan yang telah menerapkan keamanan sistem informasi pada website nya adalah PT Sentra Vidya Utama. PT Sentra Vidya Utama atau SEVIMA merupakan s*oftware house* yang menyediakan produk dan layanan *Learning Management System* (LMS). Salah satu produk dan layanan PT. Sentra Vidya Utama adalah website maukuliah.id. Website tersebut menyediakan lebih dari 3.000 rekomendasi kampus, info jurusan, biaya, prospek karier hingga terdapat layanan untuk *tryout* SNBT, tes minat dan bakat. Dengan banyaknya pengguna website, keamanan menjadi hal yang penting untuk diperhatikan, masalah seperti *defacing, phishing, denial of service, bruteforce attack* menjadi ancaman yang dapat yang dilakukan oleh oknum tidak bertanggung jawab [2]. Bahrun dalam penelitiannya menentukan dampak resiko keamanan website dengan pendekatan OWASP dan terbukti pada terdapat 3 jenis resiko keamanan antara lain Cross Site Scripting, CSRF, dan dan XSS [3]. Oleh karena itu, dalam penelitian ini dilakukan pengujian keamanan sistem informasi pada website maukuliah.id dengan harapan bisa menjadi penilaian objektif bagi perusahaan agar dapat menjadi tinjauan keamanan *website* serta dapat mengetahui daftar prioritas dan mitigasi risiko apa yang perlu di dicegah atau ditangani terlebih dahulu [2]. Salah satu metode untuk menguji keamanan sistem informasi berbasis web tersebut adalah dengan menggunakan metode OWASP (Open Web Application Security Project). OWASP merupakan kerangka kerja yang menyediakan panduan keamanan perangkat lunak khususnya website yang memberikan keamanan sistem melalui proyek open-source bersama dengan *tools* dari OWASP sebagai pendukung dalam pengujian sistem [4]. Pengujian dilakukan dengan menggunakan *software* OWASP ZAP sebagai *screening* awal penilaian risiko. Dengan menggunakan metode tersebut dapat diketahui potensi resiko keamanan website serta rekomendasi cara penanganan dan pencegahan [5]

Hasil analisis resiko mengindikasikan bahwa ada beberapa celah keamanan yang perlu diperhatikan dan diperbaiki pada website maukuliah.id. Harapannya melalui hasil analisis resiko ini, pengembang website dapat mengetahui potensi resiko yang ada pada website sehingga bisa melakukan pencegahan atau penguatan terhadap keamanan website.

2. METODOLOGI

Metode penelitian ini menggunakan metode *action research* [6]. Metode ini terdiri dari 5 tahapan yang akan dilakukan yaitu:

1. Diagnosing

Tahap ini merupakan tahap awal dalam penelitian, peneliti akan melakukan identifikasi masalah website yang ada di PT Sentra Vidya Utama (SEVIMA). Pada tahap diagnosing dilakukan studi literatur, perumusan masalah, penentuan ruang lingkup penelitian, serta menentukan tujuan penelitian. Keluaran yang dihasilkan dalam tahap ini berupa rumusan masalah dan rangkuman teori-teori terkait.

2. Information Gathering

Tahap *information gathering* atau pengumpulan informasi dilakukan dengan tujuan untuk mengumpulkan informasi tentang target website melalui *tools* Command Prompt. Selain menggunakan *tools*, pada tahap ini juga dilakukan observasi, wawancara, serta dokumentasi. Hasil dari tahapan ini berupa informasi terkait dengan target website dan informasi baik teknis maupun rekam jejak implementasi keamanan sistem informasi saat ini.

3. Action Planning

Pada tahap ini dilakukan penyusunan rencana penelitian dan pengumpulan data masalah yang tepat untuk menyelesaikan permasalahan pada website PT Sentra Vidya Utama (SEVIMA). Hasil

dari action planning ini berupa rancangan penelitian sesuai dengan framework OWASP untuk menghitung dan menilai risiko terkait aplikasi.

4. Action Taking

Pada tahap ini dilakukan investigasi guna mendapatkan informasi kelemahan sistem dan mengujinya secara langsung dengan menggunakan tipe-tipe ancaman terhadap aplikasi berbasis web yang dibangun PT Sentra Vidya Utama (SEVIMA). Pada tahap ini dilakukan *automating vulnerability scanning* menggunakan *software* OWASP ZAP. Keluaran dari tahapan ini berupa generate report celah keamanan dari OWASP ZAP.

5. Evaluating

Pada tahap ini akan dilakukan evaluasi terhadap hasil dari implementasi sebelumnya berdasarkan tahapan penentuan risk severity framework OWASP diantaranya terdapat Threat Agent Factors, Vulnerability Factors, Technical Impact, dan Business Impact. Dalam tahap ini juga dilakukan perhitungan dan penilaian resiko terkait dengan dua faktor utama yaitu:

1) *Likelihood*, faktor ini untuk menghitung kemungkinan kerentanan di exploitasi.
2) *Impact*, faktor ini untuk mengukur potensi dampak yang ditimbulkan apabila kerentanan di eksploitasi.

Faktor - faktor diatas merupakan variabel yang mempengaruhi besarnya Risk, untuk menghitung besarnya risk, digunakan perhitungan sebagai berikut :

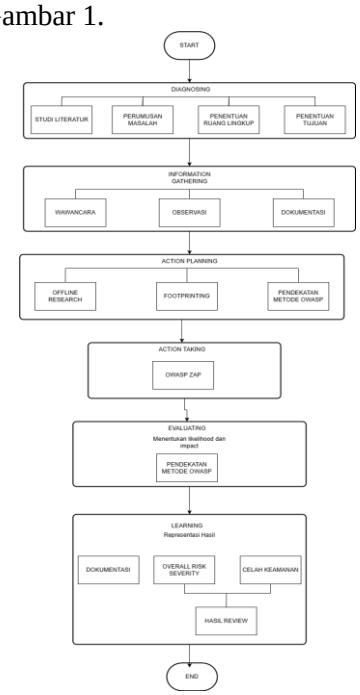
RISK = LIKELIHOOD * IMPACT…….(1)

Tahapan-tahapan untuk menentukan besarnya resiko dalam OWASP Risk Rating Methodology perlu untuk melakukan identifikasi faktor resiko untuk mengestimasikan dampak, menentukan level keparahan resiko, memutuskan apa yang harus diselesaikan, serta kustomisasi model *risk rating* [7].

6. Learning

Pada tahap ini peneliti akan melakukan review terhadap hasil dari tahapan-tahapan yang telah dilalui. Tahap kelima adalah pembelajaran (*Learning*) langkah ini merupakan tahap akhir dari penelitian yaitu melakukan review terhadap hasil dari tahapan-tahapan yang telah dilalui.

Alur penelitian disajikan pada Gambar 1.



Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

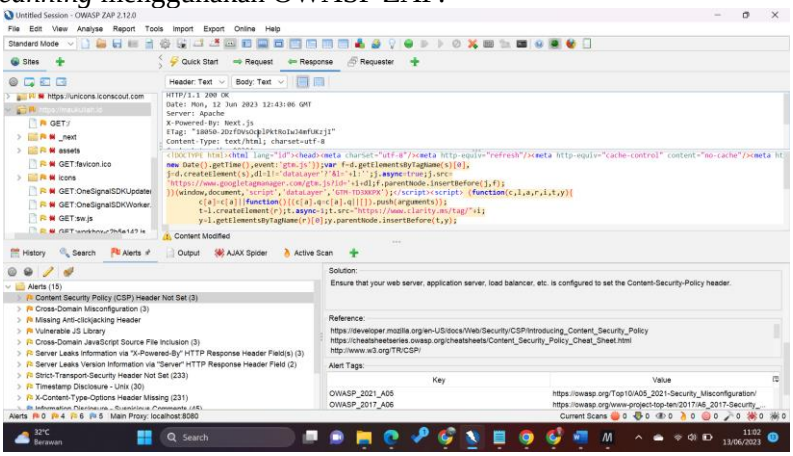
Metode pengujian yang dilakukan pada website target dilakukan menggunakan 2 teknik yaitu *footprinting* dan *vulnerability* scanning.

3.1 Hasil Pengujian *Footprinting*

Teknik *footprinting* merupakan teknik pengumpulan informasi terkait dengan target website, seperti perangkat yang digunakan, tiper, versi OS, *network address*, IP address, dan lain-lain [8]. Tujuan nya untuk menemukan cara menembus ke sebuah web atau sistem tertentu dengan cara memperoleh data keamanan yang ada pada sebuah sistem.

3.2 Hasil Pengujian *Vulnerability Scanning*

Teknik *vulnerability scanning* adalah teknik memperoleh informasi kerentanan dengan memanfaatkan *tools network scanning* dan *vulnerability scanner* [9]. *Tools* yang dipakai pada penelitian ini yakni *software* OWASP ZAP. Berikut pada Gambar 2 merupakan hasil pengujian *vulnerability scanning* menggunakan OWASP ZAP.



Gambar 2. Proses Vulnerability Scanning di OWASP ZAP

Terdapat tiga level yang menggambarkan seberapa besar level risiko yaitu high, medium, dan low. Level *high* berarti terdapat kelemahan yang berpotensi tinggi untuk menjadi ancaman, akan tetapi tingkat pencegahannya tidak memadai. Level *medium* berarti tingkat kelemahan bersifat lokal dan upaya penanganannya bersifat lokal. Sedangkan untuk level *low* memiliki tingkat keamanan yang rendah dan upaya pencegahannya diharapkan cukup memadai [10]. Pada Tabel 1 merupakan sepuluh ancaman celah keamanan hasil vulnerability scanning pada website maukuliah.id menggunakan OWASP ZAP.

Tabel 1. Hasil vulnerability scanning dengan OWASP ZAP

No	Alert	Deskripsi	Risk Level
1	Content Security Policy (CSP) Header Not Set	Sistem keamanan untuk melindungi web dari serangan XSS, ClickJacking, dan injection.	Medium
2	Cross-Domain Misconfiguration	Kesalahan konfigurasi lintas domain yang tidak diterapkan dengan benar	Medium
3	Missing Anti-Clickjacking Header	Header yang mengatur perlindungan terhadap serangan Clickjacking tidak diatur dengan benar.	Medium
4	Vulnerable JS Library	Kerentanan library javascript	Medium
5	Cross-Domain JavaScript Source File Inclusion	Mengakses file javascript dari domain yang berbeda secara lintas domain (cross-domain)	Low
6	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Pengungkapan informasi sensitif tentang komponen yang digunakan web melalui header respons http x-powered-by	Low

7	Server Leaks Version Information via "Server" HTTP Response Header Field	Pengungkapan rincian perangkat lunak yang sedang dijalankan, informasi tersebut dapat digunakan penyerang untuk eksploitasi	Low
8	Strict-Transport-Security Header Not Set	HTTP Strict Transport Security (HSTS) adalah mekanisme kebijakan keamanan web di mana server web hanya menerima komunikasi melalui HTTPS.	Low
9	Timestamp Disclosure - Unix	Aplikasi/ webserver membocorkan/memperlihatkan informasi timestamp.	Low
10	X-Content-Type-Options Header Missing	Header Anti-MIME-Sniffing X-Content-Type-Options tidak diatur ke 'nosniff'. Hal ini membuat search engine versi lama dapat melakukan MIME-Sniffing pada isi respons, sehingga berpotensi isi respons di interpretasi dan ditampilkan sebagai jenis konten.	Low

Dari pengujian tersebut diketahui bahwa celah keamanan yang terdapat pada *website* maukuliah.id berkisar pada risk level medium dan low. Tidak ditemukan celah keamanan dengan resiko tinggi.

3.3 Pengukuran Resiko

Merujuk pada metodologi OWASP Risk Rating, setelah melakukan vulnerability scanning langkah selanjutnya adalah menentukan seberapa besar resiko berdasarkan *Threat Agent factors, Vulnerability Factors, Technical Impact, dan Business Impact.* Pengukuran resiko menggunakan *tools* OWASP Risk Rating Calculator, pengukuran ini memiliki skala 1-9 dengan patokan atau acuan dari masing-masing indikator. Pada pengukuran resiko apabila hasilnya 0-3 termasuk dalam kategori low, >3-6 maka termasuk medium, dan >6-9 termasuk high.

3.3.1 Threat Agent Factors

Threat agent factors bertujuan untuk memperkirakan kemungkinan-kemungkinan serangan yang berhasil yang disebabkan oleh kelompok threat agents [11].

Table 2. Hasil Risk Rating pada *Threat Agent Factors*

No	Alert	Skill Level	Motive	Opportunity	Size	Threat Agents Factors Score
1	Content Security Policy (CSP) Header Not Set Prompt	6	4	4	8	5.5
2	Cross-Domain Misconfiguration	5	9	4	9	5.75
3	Missing Anti-clickjacking Header	6	4	7	6	5.75
4	Vulnerable JavaScript Library	3	4	4	9	5
5	Cross-Domain JavaScript Source File Inclusion	6	4	8	7	6.25
6	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	3	1	7	9	5
7	Server Leaks Version Information via "Server" HTTP Response Header Field	5	1	7	9	5.5
8	Strict-Transport-Security Header Not Set	9	1	7	4	5.25
9	Timestamp Disclosure - Unix	6	3	4	9	5.5
10	X-Content-Type-Options Header Missing	4	5	4	3	4

Pada hasil *Threat Agent Factors* diatas, diperoleh hasil 1 kerentanan dengan level *Threat Agent Factors* high, dan sisanya merupakan kerentanan dengan level *Threat Agent Factors* medium.

Kerentanan dengan *Threat Agent Factors* High diperoleh dari kerentanan Cross-Domain JavaScript Source File Inclusion.

3.3.2 *Vulnerability Factors*

Vulnerability Factors bertujuan untuk memperkirakan kemungkinan vulnerability yang dapat dieksploitasi oleh calon penyerang [11].

Table 3. Hasil Risk Rating pada *Vulnerability Factors*

No	Alert	Ease of Discovery	Ease of Exploit	Awareness	Intrusion	Vulnerability Factors Score
1	Content Security Policy (CSP) Header Not Set	3	5	4	8	5
2	Cross-Domain Misconfiguration	7	6	4	7	6
3	Missing Anti-clickjacking Header	6	4	7	6	5.75
4	Vulnerable JS Library	3	4	4	9	5
5	Cross-Domain JavaScript Source File Inclusion	6	4	4	9	5.75
6	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	3	1	7	9	5.5
7	Server Leaks Version Information via "Server" HTTP Response Header Field	5	1	7	9	5.5
8	Strict-Transport-Security Header Not Set	9	1	7	4	5.25
9	Timestamp Disclosure - Unix	5	4	9	9	6.75
10	X-Content-Type-Options Header Missing	6	4	7	9	6.5

Pada hasil *Vulnerability Factors Score* yang disajikan pada Tabel 2 diatas, diperoleh 2 kerentanan dengan level *Vulnerability Factors* High, dan sisanya merupakan kerentanan dengan likelihood medium. Kerentanan dengan *Vulnerability Factors* High diperoleh dari kerentanan Cross-Domain Misconfiguration, Timestamp Disclosure - Unix, dan X-Content-Type-Options Header Missing.

3.3.3 Hasil Likelihood

Likelihood adalah kemungkinan sebuah kerentanan dieksploitasi dan merupakan salah satu variabel yang berpengaruh terhadap besarnya risk, untuk menghitung keseluruhan likelihood sebuah kerentanan, digunakan rumus:

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

Table 4. Hasil Risk Rating pada *Technical Impact*

No	Alert	Threat Agents Factors Score	Vulnerability Factors Score	Likelihood
1	Content Security Policy (CSP) Header Not Set Prompt	5.5	5	5.25
2	Cross-Domain Misconfiguration	5.75	6	5.87
3	Missing Anti-clickjacking Header	5.75	5.75	5.75
4	Vulnerable JavaScript Library	5	5	5
5	Cross-Domain JavaScript Source File Inclusion	6.25	5.75	6
6	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	5	5.5	5.25
7	Server Leaks Version Information via "Server" HTTP Response Header Field	5.5	5.5	5.5
8	Strict-Transport-Security Header Not Set	5.25	5.25	5.25
9	Timestamp Disclosure - Unix	5.5	6.75	6.12
10	X-Content-Type-Options Header	4	6.5	5.25

Pada hasil *likelihood* pada Tabel 3 diatas, diperoleh hasil 2 kerentanan dengan likelihood High, dan sisanya merupakan kerentanan dengan likelihood medium. Kerentanan dengan likelihood High diperoleh dari kerentanan Timestamp Disclosure - Unix dan Cross-Domain JavaScript Source File Inclusion, sehingga berdasarkan hasil likelihood diatas, kedua kerentanan ini yang paling mungkin diserang oleh penyerang.

3.3.4 Technical Impact

Technical impact bertujuan untuk mengidentifikasi dan mengukur konsekuensi yang terjadi akibat adanya celah keamanan atau serangan terhadap aplikasi web [11].

Table 5. Hasil Risk Rating pada *Technical Impact*

No	Alert	Lost of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability	Technical Impact Score
1	Content Security Polic (CSP) Header Not Set Prompt	7	5	4	7	5.75
2	Cross-Domain Misconfiguration	4	5	5	7	5.25
3	Missing Anti-clickjacking Header	6	5	6	6	5.75
4	Vulnerable JS Library	7	4	7	4	5.5
5	Cross-Domain JavaScript Source File Inclusion	5	7	5	6	5.75
6	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	7	6	5	5	5.75
7	Server Leaks Version Information via "Server" HTTP Response Header Field	6	3	5	6	5
8	Strict-Transport-Security Header Not Set	7	5	5	4	5.25
9	Timestamp Disclosure - Unix	3	2	1	3	2.25
10	X-Content-Type-Options Header Missing	3	4	5	4	4

Pada hasil *Technical Impact Score* pada Tabel 5 diatas, diperoleh hasil bahwa semua kerentanan memiliki level *Technical Impact* Medium, dengan skor *Technical Impact* tertinggi didapat dari kerentanan Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Cross-Domain JavaScript Source File Inclusion, Missing Anti-clickjacking Header, dan Content Security Policy (CSP) Header Not Set Prompt.

3.3.5 Business Impact

Tujuan dari penilaian resiko ini adalah untuk meninjau dampak potensial secara ekonomi yang mungkin terjadi jika kerentanan tersebut berhasil ditembus [11].

Table 6. Hasil Risk Rating pada *Business Impact*

No	Alert	Financial Damage	Reputatiion Damage	Non-compliance	Privacy Violation	Business Impact Score
1	Content Security Policy (CSP) Header Not Setd Prompt	4	5	6	5	5.5
2	Cross-Domain Misconfiguration	6	5	4	7	5.5
3	Missing Anti-clickjacking Header	5	4	5	7	5.25
4	Vulnerable JS Library	7	6	6	5	6
5	Cross-Domain JavaScript Source File Inclusion	6	5	2	5	4.5
6	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	6	4	3	4	4.25
7	Server Leaks Version Information via "Server" HTTP Response Header Field	3	6	3	3	3.75
8	Strict-Transport-Security Header Not Set	5	4	3	5	4.25
9	Timestamp Disclosure - Unix	6	4	4	4	4.5
10	X-Content-Type-Options Header Missing	5	3	3	5	4

Pada hasil *Business Impact Score* diatas, diperoleh hasil 1 kerentanan dengan level *Business Impact* high, dan sisanya merupakan kerentanan dengan level *Business Impact* medium. Kerentanan dengan *Business Impact* High diperoleh dari kerentanan Vulnerable JS Library.

3.3.6 Hasil Impact

Impact adalah salah satu variabel yang mempengaruhi besaran risk dari sebuah kerentanan, untuk mengukur keseluruhan Impact dari sebuah kerentanan, digunakan rumus :

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

Table 6. Hasil Risk Rating pada *Impact*

No	Alert	Technical Impact Score	Business Impact Score	Impact Score
1	Content Security Policy (CSP) Header Not Set Prompt	5.75	5.5	5.62
2	Cross-Domain Misconfiguration	5.25	5.5	5.37
3	Missing Anti-clickjacking Header	5.75	5.25	5.5
4	Vulnerable JavaScript Library	5.5	6	5.75
5	Cross-Domain JavaScript Source File Inclusion	5.75	4.5	5.12

6	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	5.75	4.25	5
7	Server Leaks Version Information via "Server" HTTP Response Header Field	5	3.75	4.37
8	Strict-Transport-Security Header Not Set	5.25	4.25	4.75
9	Timestamp Disclosure - Unix	2.25	4.5	3.37
10	X-Content-Type-Options Header Missing	4	4	4

Pada hasil *Impact* diatas, diperoleh hasil bahwa semua kerentanan memiliki impact dengan level medium, skor impact tertinggi diperoleh dari kerentanan Vulnerable JavaScript Library.

3.4 Rekomendasi Solusi

Berdasarkan hasil dari analisis, diketahui website tersebut memiliki empat resiko tertinggi dengan level medium, yaitu Content Security Policy (CSP), Cross Domain Misconfiguration, Missing Anti-Clickjacking, Vulnerable JS Library. Solusi dari resiko CSP adalah dengan mengkonfigurasi server website ke CSP HTTP header agar dapat mencegah terjadinya serangan seperti data injection dan Cross-Site Scripting (XSS) [9]. Selanjutnya, Cross Domain Misconfiguration atau miskonfigurasi lintas domain dapat dicegah dengan memastikan bahwa data sensitif tidak tersedia dan konfigurasikan 'Access-Control-Allow-Origin' pada HTTP header untuk mengatur domain dan mengimplementasikan kebijakan CORS yang sesuai [12]. Kemudian ancaman selanjutnya adalah Missing Anti-Clickjacking yang tidak diatur dengan benar. Solusi dalam mengatasi missing anti-clickjacking, SEVIMA dapat mengaktifkan anti-clickjacking di konfigurasi server, atau menggunakan Content Security Policy (CSP) [14]. Kemudian yang terakhir yaitu Vulnerable JS Library merupakan kerentanan ancaman pada library javascript. Hal yang perlu dilakukan untuk mengatasi kerentanan ini adalah dengan memperbarui versi library, evaluasi alternatif library, dan lain-lain.

4. KESIMPULAN DAN SARAN

Dari penelitian yang telah dilakukan dapat disimpulkan bahwa keamanan sistem informasi pada website PT Sentra Vidya Utama (SEVIMA) menggunakan metode OWASP (Open Web Application Security Project) terdapat beberapa kerentanan yang perlu ditangani. Ditemukan ada empat resiko yang tergolong pada tingkat medium dengan skor secara keseluruhan sebesar 5.75. Oleh karena itu, diperlukan langkah-langkah penanganan yang sesuai untuk mengurangi potensi eksploitasi dan dampak negatif terhadap keamanan sistem. Berdasarkan analisis terhadap risiko kerentanan di website maukuliah.id, terdapat beberapa rekomendasi solusi untuk menangani keamanan website tersebut, sebagian besar dari solusi tersebut adalah dengan melakukan konfigurasi ulang server pada bagian-bagian yang masih rentan. Dengan menerapkan rekomendasi solusi ini, diharapkan dapat mengurangi risiko kerentanan keamanan pada website maukuliah.id dan meningkatkan keamanannya.

Saran untuk penelitian selanjutnya yaitu melakukan penelitian terkait persepsi dan kekhawatiran pengguna terhadap keamanan data mereka. Dengan melakukan penelitian-penelitian tersebut, akan memberikan kontribusi dalam meningkatkan pemahaman dan langkah-langkah yang diperlukan untuk meningkatkan keamanan sistem informasi pada website maukuliah.id, serta melindungi informasi yang disimpan di dalamnya.

5. DAFTAR RUJUKAN

[1] Sanjaya G. Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, p. 113, 2020, doi: 10.24843/jim.2020.v08.i02.p05.
[2] A. W. Kuncoro and F. Rahma, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," *Automata*, vol. 3, no. 1, pp. 1–5, 2021, [Online]. Available: https://www.sciencedirect.com
[3] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," *Creat. Inf. Technol. J.*, vol. 4, no. 4, p. 264, 2019, doi: 10.24076/citec.2017v4i4.119.
[4] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.
[5] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *J. Komtika (Komputasi dan Inform.*, vol. 5, no. 1, pp. 35–42, 2021, doi: 10.31603/komtika.v5i1.5134.
[6] D. Priyawati, S. Rokhmah, and I. C. Utomo, "Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP," *Int. J. Comput. Inf. Syst. Peer Rev. J.*, vol. 03, no. 03, pp. 2745–9659, 2022, [Online]. Available: https://ijcis.net/index.php/ijcis/index
[7] E. I. Alwi, H. Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *INFORMAL Informatics J.*, vol. 5, no. 2, p. 43, 2020, doi: 10.19184/isj.v5i2.18941.
[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, pp. 33200–33219, 2022, doi: 10.1109/ACCESS.2022.3161522.
[9] A. Zirwan, "Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner," *J. Inf. dan Teknol.*, vol. 4, no. 1, pp. 70–75, 2022, doi: 10.37034/jidt.v4i1.190.
[10] J. William, "No Title." https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (accessed Jun. 01, 2023).
[11] V. F. Dr. Vladimir, "OWASP Web Security Testing guide v4-2," *Gastron. ecuatoriana y Tur. local.*, vol. 1, no. 69, pp. 5–24, 1967.
[12] I. P. H. Putri, "Ragam Bahasa Ngalam dalam Media Sosial Instagram: Kajian Sosiolinguistik," *Diskurs. J. Pendidik. Bhs. Indones.*, vol. 5, no. 2, p. 171, 2022, doi: 10.30998/diskursus.v5i2.13530.
[13] R. Ashar, "Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF," *J. Inf. dan Teknol.*, vol. 4, no. 4, pp. 187–194, 2022, doi: 10.37034/jsisfotek.v4i4.233.