BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Terdapat beberapa penelitian terdahulu atau studi literature yang digunakan untuk mencari referensi dari kumpulan penelitian sebelumnya yang menjadi acuan dalam penelitian tugas akhir ini. Pada penelitian tersebut, terdapat percobaan menggunakan OWASP (Open Web Application Security Project) yang menggunakan Tool ZAP (Zed Attack Proxy) dengan berbagai versi yang mendapatkan beberapa kerentanan dari beberapa website [3]-[10].

Berikut merupakan analisis dari penelitian sebelumnya yang digunakan sebagai penunjang dalam penelitian ini, dapat dilihat pada **Tabel 2.1** berikut:

Tabel 2.1 Penelitian Terdahulu

No	Penulis	Judul	Tahun	Hasil Penelitian
1.	Gregorius Hendita Artha Kusuma	IMPLEMENTASI OWASP ZAP UNTUK PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK	Agustus 2022	Website yang digunakan adalah Sistem Informasi Akademik Universitas Pancasila http://siak.univpancasila.ac.id . Tools yang digunakan adalah OWASP ZAP versi 2.10.0. Hasil scan menemukan adanya kerentanan sedang, rendah, dan informatif , 1.)HTML Form without CSRF protection termasuk dalam kerentanan : Sedang

No	Penulis	Judul	Tahun	Hasil Penelitian
				2.)Clickjacking: X-Frame-Options header missing termasuk dalam kerentanan : Rendah 3.)Password type input with auto-complete enabled termasuk dalam kerentanan : Informatif
2.	1.) Tikaridha Hardiani 2.) Danur Wijayanto 3.) Nurul Latifah	Data Security Analysis with OWASP Framework on Website XYZ	Mei 2022	Analisa keamanan website XYZ menggunakan software OWASP ZAP. Perangkat lunak ini memiliki versi ZAP 2.11.1 yang mendapatkan celah keamanan yaitu: 1.)Celah keamanan data dari website XYZ diperoleh dari hasil pengujian aplikasi OWASP Zed Attack Proxy (ZAP) versi 2.11.1. Hasil pengujian website menghasilkan 11 celah kerentanan yaitu: Directory Browsing, Vulnerable JS Library, X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, Application Error Disclosure, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-control Header Set, Secure Pages Include Mixed Content, Timestamp Disclosure – Unix, X-Content-Type-Options Header Missing, dan Information Disclosure Suspicious Comments. 2.)Nilai atau tingkat resiko kerentanan dari website XYZ diperoleh berdasarkan

No	Penulis	Judul	Tahun	Hasil Penelitian
				pembobotan nilai yang didapatkan dari hasil analisa dan juga panduan Common Weakness Unumeration (CWE) dan Web Application Security Consortium (WASC), pembobotan nilai dikategorikan 2 aspek yakni kemungkinan (likelihood) dan dampak (impact). Nilai yang diperoleh dari hasil pembobotan terdapat 9 celah kerentanan dengan level Medium dan 2 celah kerentanan level Low.
3.	1.) Abdul Fattah Hasibuan, 2.) Tommy 3.) Divi Handoko	Analisis Keretanan Website Dengan Aplikasi Owasp Zap	Mei 2023	Di dapatkan 8 kerentanan yang diantaranya, 3 kerentanan level medium yaitu Absence of Anti-SCRF Tokens, Contect Security Polici (CSP) Header Not Set, Missing Anti-clickjacking Header, dan 5 kerentanan level medium yaitu Cookie No HttpOnly Flag, Cookie without Samesite Attribute, Cross-Domain JavaScript Souce File Inclusion, Timestamp-Type-Option Header Missing, X-Content-Type-Option Header Missing. Dan beberapa kerentanan ini dapat menyebabkan serangan diantaranya, serangan SCRF (Cross-Site Request Forgery)

No	Penulis	Judul	Tahun	Hasil Penelitian
4.	1.) Anggi Elanda 2.) Robby Lintang Buana	ANALISIS KEAMANAN SISTEM INFORMASI BERBASIS WEBSITE DENGAN METODE OPEN WEB APPLICATIO N SECURITY PROJECT (OWASP) VERSI 4 SYSTEMATI C REVIEW	Juli 2020	Pada Literatur [2] yang menguji sebuah Aplikasi Ujian Online Berdasarkan Hasil Pengujian OWASP versi 4 dari tabel I sampai tabel III terlihat bahwa pada proses otentifikasi terdapat kerentanan yaitu pada pengujian OTG-AUTHN-001, OTG-AUTHN-003, OTG-AUTHN-004, OTG-AUTHN-005, OTGAUTHN-006 sehingga proses ini perlu mendapat perbaikan. Pada proses pengujian otorisasi terdapat kerentanan pada OTG-AUTHZ-002, OTG-AUTHZ-004, namun setelah dilakukan pengecekan diatas hasilnya adalah false alarm sehingga proses otorisasi sudah berjalan dengan baik, sedangkan pada manajemen sesi terdapat kerentanan pada OTG-SESS001, OTG-SESS-005, OTG-SESS-007, OTG-SESS008.
5.	1.) Haeruddin 2.) Hermanto	Peningkatan Sistem Keamanan Website Menggunakan	April 2022	Dalam melakukan pengujian sistem keamanan web menggunakan metode OWASP pada 43.255.184.109 berdasarkan

No	Penulis	Judul	Tahun	Hasil Penelitian
		Metode OWASP		dari seluruh kegiatan yang dilakukan diatas maka penulis memberikan kesimpulan bahwa dari hasil penelitiannya kita bisa mengetahui bahwa website UIB memiliki tingkat risiko yang rendah namun demikian, tetap harus melakukan perbaikan terhadap ancaman yang muncul untuk mencegah datangnya serangan serangan yang lebih membahayakan website.

2.2 Kerentanan Website

Website SIMPKN Informatika Universitas Muhammadiyah Malang pada beberapa waktu yang lalu mengalami website missing yang dimana website tidak dapat diakses. Membuat mahasiswa Informatika Universitas Muhammadiyah Malang kesulitan dalam mendaftarkan PKN (Program Kerja Nyata) dan MBKM (Merdeka Belajar Kampus Merdeka) yang berdampak dalam pencatatan laporan harian yang berfungsi sebagai pencatatan kegiatan mahasiswa Informatika dalam melaksanakan kegiatan PKN (Program Kerja Nyata) dan MBKM (Merdeka Belajar Kampus Merdeka). Tidak hanya dalam segi pencatatan kegiatan tetapi juga Mahasiswa yang telah menyelesaikan kegiatan PKN (Program Kerja Nyata) dan MBKM (Merdeka Belajar Kampus Merdeka) juga kesulitan dalam pengecekan nilai akhir dan penilaian mata kuliah konversi.

2.3 Website SIMPKN Informatika

Website SIMPKN Informatika Universitas Muhammadiyah Malang merupakan website yang digunakan untuk memberikan kemudahan pendaftaran mahasiswa informatika dalam mengikuti kegiatan PKN (Program Kerja Nyata) dan MBKM (Merdeka Belajar Kampus Merdeka) yang dimana kedua kegiatan tersebut merupakan kegiatan yang dapat meningkatkan keahlian pada mahasiswa Informatika Universitas Muhammadiyah Malang. Tidak hanya pendaftaran saja pada Website SIMPKN Informatika juga terdapat beberapa fitur seperti pencatatan laporan harian, penilaian dosen pembimbing, penilaian dosen pendamping lapang, tabel mata kuliah konversi bagi mahasiswa yang mengikuti MBKM (Merdeka Belajar Kampus Medeka) dan pencetakan sertifikat PKN (Program Kerja Nyata).

2.4 OWASP (Open Web Application Security)

OWASP (Open Web Application Security) adalah serangkaian panduan, alat, dan sumber daya untuk membantu mengidentifikasi dan mengatasi masalah keamanan pada website [11]. OWASP (Open Web Application Security) mencakup berbagai topik, termasuk kerentanan umum, metode serangan, dan pengembangan pembuatan website yang aman. Tujuan adanya OWASP (Open Web Application Security) adalah mempromosikan kesadaran terhadap keamanan dan meningkatkan kualitas website yang sedang dibangun.

2.5 OWASP ZAP (Zed Attack Proxy)

OWASP ZAP (Zed Attack Proxy) adalah salah satu alat keamanan yang dapat membantu menemukan kerentanan keamanan dalam website. ZAP (Zed Attack Proxy) dapat memindai melalui website dan mendeteksi masalah yang berkaitan dengan SQL Injection, Broken Authentication, Exposure of Sensitive Data, Broken Access Control, Security Configuration Error, Cross-site Scripting (XSS), Unsafe Deserialization, Component With Known Vulnerabilities, dan lainnya. ZAP (Zed Attack Proxy) menghasilkan laporan pemindaian dalam bentuk peringatan yang ditandai dengan bendera berkode warna. Bendera tersebut terbagi menjadi 4, Bendera Merah (Kerentanan Tinggi), Bendera Oranye (Kerentanan Sedang), Bendera Kuning (Kerentanan Rendah), dan Bendera Biru (Kerentanan Tidak Berdampak Hanya Informasi) [12].

2.6 OWASP Risk Rating Kalkulator

OWASP Risk Rating Kalkulator adalah proses yang ada pada OWASP (Open Web Application Security) yang menyediakan penilaian dan mengategorikan resiko yang terkait dengan website [14]. Metode Risk Rating dirancang untuk membantu memprioritaskan dan mengatasi risikiko keamanan secara efektif. OWASP Risk Rating dihitung berdasarkan dua faktor utama yaitu Kemungkinan Eksploitasi (Likelihood Factors), dan Dampak Resiko (Impact factors). Pada bagian Likelihood Factors terdapat kriteria penilaian sebagai berikut:

Tabel 2.6.1 Penilaian Threat Agent Factors

NO	Threat Agent Factors	Kriteria Penilaian
1.	Tingkat Keterampilan	Tidak Berlaku (0) Tidak Ada Keterampilan Teknis (1) Beberapa Keterampilan Teknis (3) Pengguna komputer Tingkat Lanjut (5) Keterampilan Jaringan Dan Pemograman (6) Keterampilan Penetrasi Keamanan (9)
2.	Motif	Tidak Berlaku (0) Tidak Ada Hadiah (1) Kemungkinan Hadiah (4) Hadiah Tinggi (9)
3.	Peluang	Akses Penuh Atau Sumber Daya Yang Mahal (0)

NO	Threat Agent Factors	Kriteria Penilaian
		Akses Atau Sumber Daya Yang Khusus (4) Beberapa Akses Atau Sumber Daya Yang Diperlukan (7) Tidak Diperlukan akses sumber daya (9)
4.	Ukuran Populasi	Tidak Berlaku (0) Sistem Administrator (2) Pengguna Intranet (4) Mitra (5) Pengguna Yang Terotentikasi (6) Pengguna Internet Anonim (9)

Tabel 2.6.2 Penilaian Vulnerability Factors

NO	Vulnerability Factors	Kriteria Penilaian
1.	Kemudahan Penemuan	Tidak Berlaku (0) Cara Praktis Yang Tidak Mungkin (1) Sulit (3) Mudah (7) Tersedia Alat Otomatis (9)
2.	Kemudahan Eksploitasi	Tidak Berlaku (0)

NO	Vulnerability Factors	Kriteria Penilaian
		Teoritis (1) Sulit (3) Mudah (5) Tersedia Alat otomatis (9)
3.	Kesadaran	Tidak Berlaku (0) Tidak Diketahui (1) Tersembunyi (4) Jelas (6) Pengetahuan Publik (9)
4.	Deteksi Intrusi	Tidak Berlaku (0) Deteksi Aktif Dalam Aplikasi (1) Dicatat Dan Ditinjau (3) Dicatat Tanpa Ditinjau (8) Tidak Dicatat (9)

Tidak hanya perhitungan pada kemungkinan eksploitasi (Likelihood Factors) saja melainkan pada faktor dampak (Impact Factors) juga terdapat kriteria penilaian untuk menganalisa apakah website mengalami dampak yang berbahaya apabila telah terjadi penyerangan. Pada bagian Impact Factors terdapat penilaian sebagai berikut:

Tabel 2.6.3 Penilaian Technical Impact Factors

NO	Technical Impact Factors	Kriteria Penilaian
1.	Kehilangan Kerahasiaan	Tidak Berlaku (0) Data Yang Diungkapkan Minimum Dan Tidak Sensitif (2) Data Tidak Sensitif Ekstensif Yang Diungkapkan (6) Data Penting Dan Ekstensif Diungkapkan (7) Semua Data Yang Diungkapkan (9)
2.	Kehilangan Integritas	Tidak Berlaku (0) Data Yang Korup Minimal Sedikit (1) Data Korup Parah Yang Mnimal Sedikit (3) Data Ekstensif Yang Sedikit Korup (5) Data Ekstensif Yang Sangat Korup (7) Semua Data Benar-Benar Korup (9)
3.	Kehilangan Ketersediaan	Tidak Berlaku (0) Minimal Layanan Sekunder Terputus (1) Minimal Layanan Primer Terputus (5)

NO	Technical Impact Factors	Kriteria Penilaian
		Layanan Primer Ekstensif Terputus (7) Semua Layanan Benar-Benar Hilang Total (9)
4.	Kehilangan Akuntabilitas	Tidak Berlaku (0) Dapar dilacak sepenuhnya (1) Kemungkinan dapat dilacak (7) Sepenuhnya Anonim (9)

Tabel 2.6.4 Penilaian Business Impact Factors

NO	Business Impact Factors	Kriteria Penilaian
1.	Kerusakan Finansial	Tidak Berlaku (0) Kurang Dari Biaya Untuk Memperbaiki Kerentanan (1) Pengaruh Kecil Terhadap Laba Tahunan (3) Berpengaruh Signifikan Terhadap Laba Tahunan (7) Kebangkrutan (9)
2.	Kerusakan Reputasi	Tidak Berlaku (0) Kerusakan Minimal (1) Kehilangan Akun Utama (4) Kehilangan Niat Baik (5) Kerusakan Merek (9)

NO	Business Impact Factors	Kriteria Penilaian
3.	Ketidakpatuhan	Tidak Berlaku (0) Pelanggaran Kecil (2) Pelanggaran Jelas (5) Pelanggaran Profit Tinggi (7)
4.	Pelanggaran Privasi	Tidak Berlaku (0) Satu Orang (3) Ratusan Orang (5) Ribuan Orang (7)

2.7 Mitigation

Mitigasi adalah upaya mengurangi risiko dan dampak potensial dari kerentanan keamanan. Melalui mitigasi risiko eksploitasi kerentanan dapat dikurangi atau dihilangkan. Tindakan mitigasi membantu mencegah serangan yang mungkin dieksploitasi melalui kerentanan yang ditemukan. Perlindungan seperti firewall dan lapisan perlindungan aplikasi dapat memblokir serangan sebelum mencapai website. Dengan mengurangi kemungkinan eksploitasi kerentanan, mitigasi membantu melindungi data yang disimpan dan diolah oleh website. Pada penelitian ini memberikan upaya mengurangi risiko berdasarkan tingkat kerentanan nya seperti Kerentanan Sedang, Kerentanan Rendah, dan Kerentanan Tidak Berdampak (Informatif).