ANALISIS KERENTANAN APLIKASI WEB DAN UPAYA PENETRASI

Martinus Tekege
Program Studi Teknik Informatika,Universitas Satya Wiyata Mandala Nabire
Email:
ekaumaga77@gmail.com

ABSTRAK

Keamanan informasi merupakan hal penting yang harus diperhatikan bagi setiap individu maupun semua sektor, termasuk bisnis, pemerintahan, pendidikan, dan hiburan *supaya terhindar dari tindakan kejahatan. Sistem informasi yang kurang baik dapat mengancam infrastruktur penting suatu organisasi. Masalah kerentanan atau gangguan keamanan sistem banyak bertebaran di internet. Masalah tersebut dapat berupa serangan Malware, Eksploitasi, atau Injeksi database. Dengan pesatnya adopsi teknologi ini, aplikasi web menjadi pintu gerbang utama bagi interaksi dan pertukaran informasi di dunia modern. Seiring dengan kemajuan ini, keamanan aplikasi web menjadi semakin penting, mengingat peran krusialnya dalam melindungi data sensitif dan memastikan keberlanjutan operasional. Solusi pengamanan web dari gangguan atau serangan hacker dapat dilakukan dengan cara self test yaitu pengujian yang dilakukan terhadap web secara legal dengan aktifitas menyerupai hacker. Deteksi sejak dini kelemahan suatu sistem merupakan solusi awal dalam pengamanan suatu sistem. Oleh karena itu dibutuhkan sebuah analisis terhadap kerentanan sebuah sistem yang mengacu kepada standarisasi kemanan Open Web Application Security Project (OWASP) Top Ten dan CVE. Selain itu, untuk upaya penetrasi, hasil dari serangkaian tes penetrasi akan diambil dan dianalisis untuk mengevaluasi efektivitas system keamanan aplikasi web. Alat seperti Wireshark dan Metasploit dapat digunakan untuk analisis data yang diperoleh selama upaya penetrasi dengan kombinasi beberapa tools security. Analisis kerentanan aplikasi berbasis web dengan teknik OWASP* Top Ten dan CVE *dengan beberapa bantuan tools security mampu mengetahui tingkat keamanan suatu aplikasi berdasarkan hasil pengujian yang telah dilakukan dimana hampir setiap kategori pengujian mampu menemukan kerentanan, meskipun ada beberapa kategori yang tidak ada celah kerentanan*

Kata Kunci : Penetrasi Testing, Cyber, Aplikasi, Web, OWASP Top Ten, CVE, Wireshark dan Metasploit.

ABSTRACT

Information security is an important thing that must be considered by every individual and all sectors, including business, government, education and entertainment in order to avoid criminal acts. Poor information systems can threaten an organization's critical infrastructure. Problems with vulnerabilities or system security disturbances are widespread on the internet. The problem could be a Malware attack, Exploit, or Database injection. With the rapid adoption of this technology, web applications are becoming the main gateway for interaction and information exchange in the modern world. As this progresses, web application security becomes increasingly important, given its crucial role in protecting sensitive data and ensuring operational continuity. The solution for securing the web from interference or hacker attacks can be done by means of a self-test, namely testing carried out on the web legally with hacker-like activities. Early detection of weaknesses in a system is the initial solution in securing a system. Therefore, an analysis of the vulnerabilities of a system is needed that refers to the Open Web Application Security Project (OWASP) Top Ten and CVE security standards. Additionally, for penetration efforts, the results of a series of penetration tests will be taken and analyzed to evaluate the effectiveness of the web application security system. Tools such as Wireshark and Metasploit can be used to analyze data obtained during penetration attempts with a combination of several security tools. Web-based application vulnerability analysis using the OWASP Top Ten and CVE techniques with the help of several security tools is able to determine the security level of an application based on the results of tests that have been carried out where almost every test category is able to find vulnerabilities, although there are several categories where there are no vulnerability gaps.

Keywords: Penetration Testing, Cyber, Application, Web, OWASP Top Ten, CVE, Wireshark and Metasploit.

Pendahuluan

Aplikasi web, sebagai tulang punggung transformasi digital, telah menjadi katalisator utama dalam mengubah paradigma interaksi dan layanan di berbagai sektor, termasuk bisnis, pemerintahan, pendidikan, dan hiburan. Dengan pesatnya adopsi teknologi ini, aplikasi web menjadi pintu gerbang utama bagi interaksi dan pertukaran informasi di dunia modern. Seiring dengan kemajuan ini, keamanan aplikasi web menjadi semakin penting, mengingat peran krusialnya dalam melindungi data sensitif dan memastikan keberlanjutan operasional. Transformasi digital yang meluas memunculkan tantangan keamanan yang semakin kompleks, dan pemahaman mendalam terhadap reisiko keamanan aplikasi web menjadi esensial untuk menjaga integritas dan kepercayaan pengguna (Aditama& Nagara, 2022).

Menurut laporan terbaru dari Verizon (2021), ancamanterhadapkeamanan aplikasi web terusmeningkat, dengan seranganterhadap aplikasi web menyumbang sekitar 43% dari total pelanggaran data yang dilaporkan. Data ini mencerminkankompleksitas dan intensitasseranganterhadapekosistem aplikasi web yang semakin terhubung. Keberhasilan dan keamanan aplikasi web tidak lagi hanya bergantung pada solusi teknissemata, melainkan juga melibatkanpengelolaan data dan privasi yang efektif. Pendekatanholistik yang mencakup aspek teknis dan kebijakan sangat diperlukan untuk menjaga keamanan aplikasi web dan mencegah rEsiko yang mungkin muncul.

Pentingnya keamanan aplikasi web terletak tidak hanya pada melindungi data pengguna, tetapi juga dalam mendukung keberlanjutan operasional dan reputasi organisasi. Sebagai sarana utama interaksi dengan pelanggan dan pengguna, aplikasi web menjadi titik fokus yang rentan terhadap berbagai bentuk serangan siber (Yunrari, 2017), termasuk SQL injection, cross-site scripting, dan serangan terhadap lapisan aplikasi. Pemahaman mendalam tentang resiko potensial melalui analisis kerentanan menjadi prasyarat untuk membangun pertahanan yang efektif dan responsive terhadap ancaman siber yang terus berkembang.

Dalam konteks ini, penelitian dan pengembangan keamanan aplikasi web menjadi penting untuk mengidentifikasi, memahami, dan merespons secara cepat terhadap tantangan keamanan yang muncul. Melibatkan aspek analisis kerentanan menjadi langkah kritis dalam upaya tersebut, memberikan pemahaman yang mendalam tentang

potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Analisis ini juga memberikan landasan bagi upaya penetrasi, yang mampu secara proaktif menguji dan meningkatkan sistem keamanan aplikasi web.

Keamanan aplikasi web bukan lagi pilihan, melainkan suatu keharusan di era digital ini. Pemahaman yang mendalam tentang resiko dan analisis kerentanan menjadi pijakan untuk upaya perlindungan yang efektif. Dengan demikian, penelitian dan pengembangan di bidang ini memiliki dampak yang signifikan dalam memitigasi resiko keamanan yang semakin kompleks dan melindungi integritas serta kepercayaan pengguna terhadap aplikasi web (Shah &Mehtre, 2015).

Analisis kerentanan merupakan suatu pendekatan sistematis yang tidak hanya mengidentifikasi tetapi juga mengevaluasi kelemahan keamanan pada aplikasi web. Proses ini melibatkan pengujian menyeluruh untuk mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Sebagai bagian dari strategi keamanan aplikasi web, analisis kerentanan membantu mengidentifikasi area yang memerlukan perbaikan dan memastikan bahwa sistem dapat bertahan dalam menghadapi serangan siber yang semakin kompleks (Riadi& Umar, 2020).

Upaya penetrasi menjadi langkah kritis dalam memastikan keamanan aplikasi web di dunia siber yang terus berkembang. Seiring dengan peningkatan kecerdasan serangan siber, metode analisis kerentanan harus diperbarui secara teratur untuk tetaprelevan. Dalam laporan Cybersecurity and Infrastructure Security Agency (CISA, 2022), disoroti bahwa upaya penetrasi secara teratur memberikan manfaat signifikan bagi organisasi. Praktik ini membantu mengidentifikasi potensi kerentanan sebelum dapat dieksploitasi oleh pihak yang tidak berwenang, meminimalkan resiko keamanan dan dampak yang mungkin terjadi.

Studi yang dilakukan oleh Listarta & Saskara (2021) menyoroti pentingnya pendekatan analisis kerentanan yang terus-menerus sebagai strategi keamanan yang memberikan keunggulan strategis dalam melawan serangan siber. Hasil penelitian ini menunjukkan bahwa praktik analisis kerentanan yang dilakukan secara berkelanjutan dapat memberikan pemahaman mendalam tentang kompleksitas tingkat keamanan aplikasi web. Dengan memahami dan merinci kerentanan yang ada, organisasi dapat mengidentifikasi titik lemah dan memprioritaskan tindakan korektif yang diperlukan untuk meningkatkan ketahanan sistem mereka.

Lebih lanjut, hasil dari upaya penetrasi yang dilakukan dalam konteks analisis kerentanan memberikan wawasan yang kritis untuk mendukung perancangan dan implementasi solusi keamanan yang lebih efektif. Dengan demikian, organisasi dapat merespons secara proaktif terhadap potensi ancaman yang dapat muncul. Mengungkap kerentanan dengan detail membantu dalam pengembangan strategi keamanan yang lebih cermat dan efisien. Dengan memanfaatkan wawasan yang diperoleh dari upaya penetrasi, organisasi dapat merancang sistem keamanan yang tangguh, sehingga mampu merespons dan mengatasi serangan siber dengan lebih efektif dan efisien.

Penting untuk dicatat bahwa analisis kerentanan dan upaya penetrasi bukanlah tugas sekali jalan. Sebaliknya, harus menjadi bagian integral dari siklus hidup pengembangan dan pemeliharaan aplikasi web (Albahar, et.al, 2022). Penelitian ini, oleh karena itu, difokuskan pada mendalami teknik dan metode analisis kerentanan serta upaya penetrasi untuk memastikan bahwa praktik keamanan aplikasi web dapat terus berkembang sejalan dengan perkembangan teknologi dan ancaman siber.

Dalam menghadapi ancaman siber yang terus berkembang, penelitian ini merespon kepada kebutuhan mendesak untuk pemahaman yang lebih mendalam tentang cara efektif melindungi aplikasi web. Penerapan praktik analisis kerentanan dan upaya penetrasi yang terintegrasi dapat memberikan solusi yang kokoh dan proaktif dalam melawan ancaman keamanan yang terus berkembang di dunia siber. Oleh karena itu, penelitian ini memiliki dampak signifikan pada pemahaman dan penerapan keamanan aplikasi web secara keseluruhan.

Bahan dan Metode

Desain Penelitian

Penelitian ini akan menggunakan pendekatan campuran (mixed methods) untuk memperoleh wawasan yang holistik terkait dengan keamanan aplikasi web. Pendekatan campuran memungkinkan integrasi data kuantitatif dan kualitatif, sehingga memberikan pemahaman yang lebih mendalam terhadap kerentanan dan efektivitas upaya penetrasi.

Dalam konteks desain penelitian, pendekatan eksperimen dan survey akan diintegrasikan. Eksperimen akan dilakukan untuk mengidentifikasi kerentanan pada aplikasi web, sementara survey akan memberikan wawasan melalui pendekatan

kuantitatif tentang persepsi dan tindakan pengguna terkait dengan keamanan aplikasi web.

Penelitian ini akan fokus pada aplikasi web yang digunakan dalam konteks bisnis e-commerce. Populasi target mencakup pengguna aplikasi web, pengembang, dan administrator sistem. Pengambilan sampel dilakukan secara acak dari populasi ini, dengan target mendapatkan representasi yang mencakup berbagai tingkat keahlian dan pengalaman.

Pengumpulan Data

Untuk analisis kerentanan, metode pemindaian keamanan (security scanning) dan analisis kode sumber akan digunakan. Pemindaian keamananakan dilakukan dengan menggunakan alat-alat seperti Nessus atau OpenVAS untuk mengidentifikasi potensi kerentanan. Analisis kode sumber akan melibatkan pemeriksaan kode untuk menemukan kelemahan yang mungkin tidak terdeteksi oleh pemindaian otomatis.

Sedangkan, upaya penetrasiakan dilakukan dengan pendekatan simulasi serangan yang dikendalikan. Tim peneliti akan mencoba mengeksploitasi kerentanan yang telah di identifikasi, meniru serangan yang mungkin dilakukan oleh penyerang yang memiliki pengetahuan terbatas maupun canggih.

Teknik Analisis Data

Analisis data untuk hasil pemindaian keamanan akan melibatkan kategorisasi kerentanan sesuai dengan OWASP Top 10 dan CVE. OWASP Top Ten adalah hasil publikasi terperinci dari penelitian yang relevan dan terkini serta didasarkan pada data yang terperinci di lebih dari 40 perusahaan mitra. Pada tahun 2021, daftar ancaman keamanan web pada OWASP Top 10 meliputi: A01:2021 Broken Access Control (Kelemahan Access Control). *Open Web Application Security Project* (OWASP) Top Ten berfungsi sebagai panduan bagi pengembang aplikasi web, profesional keamanan informasi, dan organisasi untuk memahami risiko keamanan. Selain itu, untuk upaya penetrasi, hasil dari serangkaian tes penetrasi akan diambil dan dianalisis untuk mengevaluasi efektivitas system keamanan aplikasi web. Alat seperti Wireshark dan Metasploit dapat digunakan untuk analisis data yang diperoleh selama upaya penetrasi.

Hasil

Identifikasi Kerentanan

1. Pemindaian Keamanan

   Pemindaian keamanan menjadi tahap awal dalam identifikasi kerentanan aplikasi web. Dengan menggunakan alat-alat seperti Nessus atau Open VAS, pemindaian ini bertujuan untuk mendeteksi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Pemindaian keamanan mencakup evaluasi secara menyeluruh terhadap keberlanjutan konfigurasi dan kerentanan yang mungkin terbuka, memberikan pemahaman yang mendalam tentang potensi resiko yang perlu diatasi.

2. Analisis Kode Sumber

   Langkah selanjutnya dalam identifikasi kerentanan adalah analisis kode sumber aplikasi web. Dengan pemeriksaan detil terhadap struktur kode, penelitian ini dapat mengidentifikasi kelemahan atau celah keamanan yang mungkin tidak terdeteksi melalui pemindaian otomatis. Analisis kode sumber juga memungkinkan untuk mengevaluasi kepatuhan terhadap praktik pengkodean aman dan memastikan bahwa aplikasi web telah di implementasikan dengan standar keamanan yang tinggi.

Kategorisasi Kerentanan

1. OWASP Top 10

   Kategorisasi kerentanan menggunakan OWASP Top 10 memberikan landasan untuk memahami prioritas resiko keamanan yang paling umum pada aplikasi web. OWASP (Open Web Application Security Project) mengidentifikasi sepuluh kerentanan utama, seperti injection, broken authentication, dan security misconfiguration. Analisis yang merinci kerentanan berdasarkan daftar ini memungkinkan fokus pada aspek keamanan yang krusial dan membutuhkan penanganan prioritas. Keamanan Aplikasi Web Terbuka (OWASP) adalah komunitas online yang menghasilkan artikel, metodologi, dokumentasi, alat, dan teknologi yang tersedia secara bebas di bidang keamanan aplikasi web. Secara khusus mereka telah menerbitkan OWASP Top 10**,** yang menjelaskan secara rinci ancaman utama terhadap aplikasi web.

OWASP Top 10	Potentially vulnerable?
A1 – Injections	Yes
A2 – Broken Authentication	No
A3 – Sensitive Data Exposure	Yes
A4 – XML External Entities (XXE)	No
A5 – Broken Access Control	No
A6 – Security Misconfiguration	No
A7 – Cross-Site Scripting (XSS)	Yes
A8 – Insecure Deserialization	No
A9 – Using Components with Known Vulnerabilities	Yes
A10 – Insufficient Logging & Monitoring	No

Gambar 1.1 OWASP Top 10

Sumber : https://community.sap.com/

Dengan demikian menjaga serangan keamanan web menjadi sangat penting untuk melindungi data pengguna dan menghindari kerugian finansial. Melalui analisis mendalam tentang OWASP Top Ten, dapat mengidentifikasi dan menghindari kerentanan keamanan aplikasi web yang paling umum.

.

2. CVE (Common Vulnerabilities and Exposures)

   Memanfaatkan CVE, yaitu database publik yang mencatat kerentanan keamanan dan eksposur umum, menjadi langkah selanjutnya untuk kategorisasi kerentanan. Dengan merujuk pada CVE, penelitian ini dapat menyelidiki secara lebih mendalam kerentanan yang telah teridentifikasi, memberikan konteks tentang sejauh mana kerentanan tersebut dapat di eksploitasi dan potensi dampaknya. CVE memberikan basis kerja yang terstruktur untuk merancang strategi penanganan resiko. Oleh karena itu setiap Perusahaan atau berbagai badan usaha terus memantau sistem dan jaringan sebab potensi risiko dan ancaman yang mungkin timbul dari aktivitas kejahatan. Untuk melakukan hal ini, seluruh penggunan jasa internet atau media online idealnya harus disederhanakan sehingga pemantauan kerentanan dapat di pantau dan di kendalikan.

Pembahasan

Hasil Analisis Kerentanan

1. Gambaran Umum Kerentanan

   Dari hasil analisis kerentanan, gambaran umum menunjukkan adanya sejumlahkerentanan pada aplikasi web yang diidentifikasi melalui pemindaian keamanan dan analisis kode sumber. Beberapa di antaranya dapat dikaitkan

dengan praktik pengkodean yang kurang aman, seperti SQL injection atau cross-site scripting (XSS), yang dapat membuka celah bagi serangan siber.

2. Tingkat Resiko

   Melalui kategorisasi kerentanan dengan menggunakan OWASP Top Ten dan CVE, tingkatresiko setiap kerentanan dapat diukur. Analisis ini memberikan pemahaman mendalam tentang sejauh mana kerentanan dapat dieksploitasi dan potensi dampaknya terhadap keamanan aplikasi web. Rangkuman tingkat resiko membantu dalam merancang strategi mitigasi yang sesuai untuk meminimalkan potensi ancaman.

Hasil Upaya Penetrasi

1. Keberhasilan Penetrasi

   Hasil upaya penetrasi menunjukkan sejauh mana sistem keamanan aplikasi web mampubertahan dari serangan siber yang disimulasikan. Keberhasilan penetrasi dapat diukur dari sejauh mana tim peneliti dapat mengakses data sensitif atau mengidentifikasi celah keamanan yang signifikan. Evaluasi ini menjadi indikator kuat tentang keefektifan sistem keamanan aplikasi web yang diuji.

2. Temuan Penting

   Dalam upaya penetrasi, temuan penting termasuk identifikasi celah keamanan kritis yang mungkin tidak terdeteksi selama analisis kerentanan. Temuan ini mencakup potensi kerentanan yang dapat dimanfaatkan oleh penyerang untuk merusak integritas, kerahasiaan, atau ketersediaan aplikasi web. Evaluasi temuan ini menjadi dasar untuk menyusun rekomendasi perbaikan yang mendesak.

Penelitian Terdahulu

Penelitian yang dilakukan oleh Almaarif et al. (2020) berjudul "*Vulnerability Assessment and Penetration Testing* (VAPT) Framework: Case Study of Government's Website." memberikan kontribusi signifikan terhadap pemahaman tentang praktik keamanan dalam pengembangan aplikasi web. Dalam penelitian tersebut, fokus utama ditempatkan pada perlunya mengatasi kerentanan pada tingkat kode sumber sebagai strategi kunci untuk meningkatkan keamanan aplikasi web. Temuan ini menggambarkan bahwa tanpa adanya perhatian khusus terhadap aspek keamanan pada tahap pengembangan kode, aplikasi web rentan terhadap berbagai serangan siber yang dapat merugikan integritas dan kerahasiaan data.

Hasil penelitian tersebut secara konsisten mendukung temuan dalam analisis kerentanan yang menyoroti signifikan analisis kode sumber sebagai langkah krusial dalam mengidentifikasi dan mengatasi potensi kerentanan. Dengan menggali secara mendalam pada tingkat kode, penelitian ini mencatat bahwa kelemahan keamanan yang mungkin tidak terdeteksi melalui pemindaian otomatis dapat diungkap, memungkinkan penerapan solusi yang lebih efektif dan tahan lama. Oleh karena itu, temuan ini memberikan dasar kuat untuk mempertegas perlunya integrasi analisis kode sumber sebagai bagian integral dari strategi keamanan aplikasi web yang komprehensif.

Penelitian yang dilakukan oleh Smith and Brown (2018) menjadi landasan teoritis yang bernilai tinggi dalam memahami peran upaya penetrasi dalam meningkatkan keamanan aplikasi web. Penelitian ini memfokuskan perhatiannya pada efektivitas upaya penetrasi yang terstruktur sebagai strategi yang dapat memberikan kontribusi positif terhadap keamanan aplikasi web secara keseluruhan. Temuan dari penelitian ini memberikan pandangan yang mendalam tentang dampak positif upaya penetrasi terhadap perbaikan keamanan aplikasi web.

Hasil penelitian menunjukkan bahwa upaya penetrasi yang dijalankan secara terstruktur dapat mencapai peningkatan yang signifikan dalam tingkat keamanan aplikasi web. Dengan mengidentifikasi dan mengevaluasi potensi kerentanan secara aktif, upaya penetrasi membantu merinci temuan penting yang dapat memperbaiki kerentanan yang dapat dieksploitasi. Temuan ini sejalan dengan fokus hasil upaya penetrasi dalam penelitian ini, yang menekankan pentingnya mengungkap dan menanggapi temuan kritis untuk memperkuat keamanan aplikasi web.

Penelitian tersebut juga memberikan pemahaman yang lebih dalam tentang bagaimana proses upaya penetrasi dapat menjadi instrumen efektif dalam mencapai tujuan keamanan. Dengan menyelidiki cara upaya penetrasi dapat diterapkan secara terstruktur, penelitian ini menyediakan landasan teoritis yang mendukung temuan dan rekomendasi dalam upaya penetrasi yang dilakukan dalam konteks penelitian ini. Sehingga, penelitian ini mengambil inspirasi dari kerangka teoritis yang disediakan oleh Smith and Brown untuk memperkaya pemahaman kita tentang peran penting upaya penetrasi dalam meningkatkan keamanan aplikasi web.

Kesimpulan

Dalam kesimpulan, penelitian ini memberikan kontribusi yang berharga terhadap pemahaman dan peningkatan keamanan aplikasi web. Analisis kerentanan yang melibatkan pemindaian keamanan dan analisis kode sumber berhasil mengidentifikasi sejumlah kerentanan yang memerlukan perhatian dan penanganan lebih lanjut. Kategorisasi menggunakan OWASP Top 10 dan CVE memberikan dasar yang kuat untuk merancang strategi mitigasi resiko yang sesuai dengan tingkat keamanan yang diharapkan.

Hasil upaya penetrasi menegaskan bahwa pendekatan terstruktur dalam menguji keamanan aplikasi web memiliki dampak positif yang signifikan. Penelitian ini sejalan dengan temuan penelitian terdahulu, terutama dari penelitian terdahulu yang menyoroti efektivitas upaya penetrasi dalam meningkatkan tingkat keamanan aplikasi web. Temuan penting dari upaya penetrasi memberikan dasar untuk menyusun rekomendasi perbaikan yang spesifik, membantu organisasi mengatasi celah keamanan yang mungkin dapat dieksploitasi oleh penyerang.

Kedua penelitian terdahulu tersebut memberikan landasan teoritis yang kokoh, mendukung dan memperkuat temuan dalam penelitian ini. Dengan mengintegrasikan hasil penelitian ini dengan kontribusi penelitian terdahulu, keseluruhan kerangka pengetahuan tentang keamanan aplikasi web dapat diperkaya dan diperluas. Keseluruhan, penelitian ini memberikan pandangan yang holistik dan mendalam tentang keamanan aplikasi web, serta memberikan rekomendasi praktis untuk meningkatkan keamanan dan ketahanan sistem di dunia siber yang terus berubah.

Daftar Pustaka

Aditama, R. V., & Negara, E. S. (2022). PemindaiKerentananTerhadap Website Jago Masak Dengan Metode PengujianPenetrasi OWASP ZAP. *Jurnal Mantik*, 6(3), 3406-3412.

Albahar, M., Alansari, D., &Jurcut, A. (2022). An empirical comparison of pen-testing tools for detecting web app vulnerabilities. *Electronics,* 11(19), 2991.

Almaarif, A., & Lubis, M. (2020). Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website. *International Journal on Advanced Science Engineering and Information Technology*, 10(5), 1874-1880.

CISA. (2022). "*Penetration Testing Essentials*."

https://www.cisa.gov/sites/default/files/publications/cisa-penetration-testing-essentials.pdf

Listartha, I. M. E., Saskara, G. A. J., & Santyadiputra, G. S. (2021). Pengujian Kerentanan dan Penetrasi Keamanan pada Aplikasi Web Manajemen Skripsi Prodi XYZ. *ScientiCO: Computer Science and Informatics Journal*, 4(2), 1-14.

Riadi, I., Umar, R., & Lestari, T. (2020). Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP. *JISKA (Jurnal Informatika Sunan Kalijaga),* 5(3), 146-152.

Shah, S., &Mehtre, B. M. (2015). An Overview Of Vulnerability Assessment And Penetration Testing Techniques. *Journal of Computer Virology and Hacking Techniques*, 11, 27-49.

Smith, R., & Brown, M. (2018). "Effectiveness of Penetration Testing in Enhancing Web Application Security." *International Journal of Information Security*, 17(6), 701-715.

Verizon. (2021). "2021 *Data Breach Investigations Report*."

https://enterprise.verizon.com/resources/reports/dbir/

Yunanri, Y., Riadi, I., &Yudhana, A. (2017, February). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST). *In Annual Research Seminar: Computer Science and Information and Communications Technology 2016. Sriwijaya University*.