MAPLE Mechatronics Journal in Professional and Entrepreneur
Volume 7 Edisi 1 Bulan Juni Tahun 2025 Politeknik Bosowa P-ISSN : 2685-4868 , E-ISSN : 2963-6175

Evaluasi Keamanan Pada Applikasi SYAM-OK Menggunakan Vulnerability Assesment

Muhammad Adam#, Dewelia Irien Pasa, Dessy Ana Sari, Akhyar Muchtar
Pendidikan Teknik Informatika dan Komputer, Universitas Negeri Makassar
Parangtambung, Kota Makassar, Sulawesi Selatan 90224
adammuhammadunm2003@gmail.com

Abstrak

Aplikasi berbasis web, seperti SYAM-OK, semakin rentan terhadap ancaman keamanan, terutama dalam lingkungan pendidikan yang menangani data sensitif. Penelitian ini bertujuan untuk mengevakuasi keamanan aplikasi SYAM-OK menggunakan metode Vulnerability Assessment. Proses penelitian mencakup identifikasi kerentanan, analisis risiko, dan penyusunan rekomendasi perbaikan berdasarkan hasil pengujian menggunakan alat OWASP. Hasil penelitian menunjukkan adanya beberapa kerentanan tingkat sedang dan rendah, seperti clickjacking dan proteksi XSS yang tidak aktif. Solusi yang direkomendasikan meliputi pengaturan header HTTP yang lebih aman dan peningkatan konfigurasi sistem. Penelitian ini memberikan langkah-langkah perbaikan konkret untuk meningkatkan keamanan aplikasi, sehingga mampu melindungi data pengguna dan mendukung operasional yang lebih aman di masa depan.

Kata kunci : Keamanan Aplikasi, *Vulnerability Assessment*, OWASP, Evaluasi Keamanan, SYAM-OK

Abstract

Image processing and computer vision are rapidly evolving fields with numerous practical applications, including object recognition, medical image analysis, and industrial quality control. This research aims to develop a method for shape detection and classification in images using Chain Code and the Naive Bayes classification algorithm. Chain Code is utilized to digitally represent shape contours, while Naive Bayes is employed to classify shapes based on the probability distribution of features. In its implementation, images are pre-processed using thresholding and edge detection techniques to extract contours, which are then represented using Chain Code. The extracted features serve as input to the Naive Bayes model, trained to recognize various geometric shapes such as circles, pentagons, hexagons, stars, and rectangles. Experimental results demonstrate that this method is effective in detecting and classifying basic shapes with high accuracy. However, it has limitations in detecting more complex shapes or those with irregular edges.Suggestions for future research include utilizing larger and more diverse datasets, testing with other classification algorithms, and developing hybrid algorithms to enhance accuracy and robustness in shape detection.

Keywords : Application Security, *Vulnerability Assessment, AWASP, Security Evaluation, SYAM-OK*

I. PENDAHULUAN

Keamanan informasi merupakan aspek krusial dalam pengembangan aplikasi berbasis web, termasuk dalam dunia pendidikan yang semakin mengandalkan teknologi digital seperti E-Learning. Penggunaan platform pembelajaran daring tidak hanya mempermudah proses belajar mengajar, namun juga meningkatkan risiko keamanan data yang harus dikelola dengan baik. Salah satu platform E-Learning yang banyak digunakan adalah Syam-Ok, yang memfasilitasi proses pembelajaran di berbagai institusi pendidikan. Namun, seperti aplikasi berbasis web lainnya, Syam-Ok berpotensi memiliki kerentanan yang dapat disalahgunakan oleh pihak tidak bertanggung jawab, sehingga keamanan menjadi perhatian utama.

Penelitian ini dilatarbelakangi oleh pentingnya keamanan aplikasi E-Learning dalam melindungi data pengguna dan memastikan layanan berjalan tanpa gangguan. Berdasarkan studi sebelumnya, aplikasi E-Learning seringkali memiliki celah keamanan yang signifikan, seperti yang ditemukan

di Universitas XYZ, di mana kerentanan kritis memungkinkan eksekusi kode jarak jauh [1]. Penggunaan metode Vulnerability Assessment, yang mencakup deteksi, analisis, prioritas, dan remediasi, memberikan cara sistematis untuk mengidentifikasi dan mengatasi kerentanan dalam aplikasi berbasis web [2]. Evaluasi keamanan ini dapat meminimalkan risiko kehilangan data dan mencegah gangguan operasional yang berakibat pada biaya tambahan atau kerugian reputasi institusi [3].

Urgensi penelitian ini terlihat dari meningkatnya frekuensi serangan siber yang menargetkan aplikasi berbasis web. Aplikasi yang tidak aman dapat mengalami kebocoran data atau gangguan layanan, yang berpotensi merugikan institusi dan pengguna secara signifikan. Selain itu, pentingnya perlindungan data pribadi di era digital membuat evaluasi keamanan aplikasi menjadi semakin mendesak, terutama di sektor pendidikan yang menangani banyak informasi sensitif terkait peserta didik dan staf [3].

Metode Vulnerability Assessment efektif dalam mendeteksi celah keamanan pada aplikasi berbasis web. Beberapa penelitian terdahulu menyimpulkan bahwa pendekatan ini dapat mengidentifikasi aset-aset penting dalam website, menganalisis kerentanan, dan memberikan solusi perbaikan yang tepat sasaran untuk mengurangi risiko keamanan [3]. Selain itu, penilaian berdasarkan Common Vulnerability Scoring System (CVSS) memudahkan pengembang dalam menilai tingkat keparahan kerentanan yang ditemukan, sehingga perbaikan dapat difokuskan pada aspek yang paling berisiko [1].

Dengan demikian, penelitian ini tidak hanya relevan untuk meningkatkan keamanan aplikasi Syam-Ok, tetapi juga memberikan kontribusi yang signifikan dalam pengembangan sistem pembelajaran daring yang lebih aman di masa depan. Hasil penelitian diharapkan dapat memberikan rekomendasi yang konkret dan dapat diimplementasikan, sehingga aplikasi ini dapat berfungsi secara efisien tanpa mengorbankan aspek keamanan.

TINJAUAN PUSTAKA

1. Vulnerability Assessment

Vulnerability Assessment (VA) merupakan proses yang terstruktur untuk mendeteksi, mengevaluasi, dan mengkategorikan kerentanan dalam sistem informasi, jaringan, serta aplikasi. Menurut Budiman et al. (2021), tujuan dari VA adalah untuk menemukan celah keamanan yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab, sehingga tindakan mitigasi dapat dilakukan guna melindungi data dan sistem dari potensi ancaman [4].

2. Katergori Kerentanan

Dalam penelitian terkait keamanan aplikasi web, Setiyani et al. (2023) mengklasifikasikan kerentanan menjadi tiga kategori berdasarkan hasil pemindaian menggunakan alat OWASP:

- Medium: Kerentanan yang dapat menimbulkan risiko sedang.
- Low: Kerentanan dengan risiko rendah.
- Informational: Kerentanan yang bersifat informatif dan tidak langsung membahayakan sistem.

Penelitian tersebut menemukan 15 kerentanan pada aplikasi E-Learning, yang memberikan wawasan penting bagi pengelola dalam upaya meningkatkan keamanan system [6].

3. Implementasi Alat Pemindaian

Penggunaan alat pemindaian seperti Nessus dan Zed Attack Proxy (ZAP) memainkan peran penting dalam proses Vulnerability Assessment (VA). Alat-alat ini memungkinkan deteksi kerentanan secara otomatis serta menyediakan analisis mendalam terkait risiko yang teridentifikasi. Dalam studi yang dilakukan oleh Rissal Efendi et al. (2024), penggunaan Greybone Openvas sebagai alat pemindaian berhasil mendeteksi lima kerentanan dengan berbagai tingkat risiko, menekankan pentingnya memilih alat yang tepat dalam proses penilaian kerentanan [5].

4. Pentingnya Remediasi

Setelah kerentanan teridentifikasi, langkah remediasi menjadi sangat penting untuk memperbaiki dan mengurangi risiko. Proses ini mencakup penerapan patch, penyesuaian ulang konfigurasi sistem, serta peningkatan kesadaran pengguna terhadap potensi ancaman. Penelitian menunjukkan bahwa tindakan remediasi yang efektif dapat secara signifikan meningkatkan tingkat keamanan system [5].

II. METODE PENELITIAN

Metode penelitian atau tahapan-tahapan yang digunakan adalah Vulnerability Assessment, yang merupakan proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi kerentanan dalam sistem informasi serta mengevaluasi keamanannya dengan simulasi serangan [7].

Penelitian ini akan mengikuti enam tahapan utama dalam VAPT Life Cycle untuk mengevaluasi

keamanan aplikasi SYAM-OK. Penjelasan dari masing-masing tahapan adalah sebagai berikut :

Identifying Scope

Tahap pertama adalah menentukan ruang lingkup penelitian. Pada penelitian ini, lingkupnya adalah aplikasi SYAM-OK yang digunakan oleh Universitas Negeri Makassar. Lingkup ini mencakup area yang relevan dengan potensi kerentanan, termasuk autentikasi pengguna, manajemen data, dan transfer informasi.

Information Gathering

Tahap ini melibatkan pengumpulan informasi tentang aplikasi SYAM-OK untuk memahami lebih lanjut tentang infrastruktur, teknologi, dan konfigurasi sistem yang digunakan. Beberapa tools yang digunakan dalam tahap ini antara lain:

- WHOIS: untuk mendapatkan informasi tentang domain aplikasi.
- DIG dan NSLOOKUP: untuk melakukan pemeriksaan DNS dan mendapatkan informasi tambahan terkait server.
- NMAP: untuk memetakan port yang terbuka dan layanan yang berjalan pada aplikasi SYAM-OK.

Vulnerability Scanning

Pada tahap ini, penelitian akan melakukan pemindaian kerentanan pada aplikasi SYAM-OK untuk mengidentifikasi potensi celah keamanan. Tools dari OWASP (seperti OWASP ZAP) akan digunakan untuk memeriksa kerentanan, dengan fokus pada hal-hal berikut:

- Identifikasi potensi kerentanan terkait konfigurasi yang tidak aman.
- Pemeriksaan pada port yang terbuka, layanan yang berjalan, dan potensi celah keamanan lainnya.

False Positive Analysis

Setelah pemindaian selesai, hasilnya akan diperiksa secara mendalam untuk memastikan bahwa semua kerentanan yang ditemukan adalah valid. Pada tahap ini, akan dilakukan:

- Analisis hasil scanning untuk memastikan tidak ada false positives (temuan yang keliru).
- Hasil yang valid akan dicatat untuk kemudian dievaluasi pada tahap selanjutnya.

Vulnerability Exploitation

Tahap ini bertujuan untuk mengeksploitasi kerentanan yang telah teridentifikasi pada aplikasi SYAM-OK untuk melihat sejauh mana dampaknya terhadap sistem. Eksploitasi dilakukan hanya pada kerentanan yang dipastikan aman untuk diuji. Aktivitas yang dilakukan di tahap ini meliputi:

- Menjalankan exploit pada kerentanan yang ditemukan menggunakan alat atau teknik yang sesuai.
- Melakukan eksploitasi hanya pada lingkungan uji untuk menghindari gangguan pada sistem produksi.

Generating Report

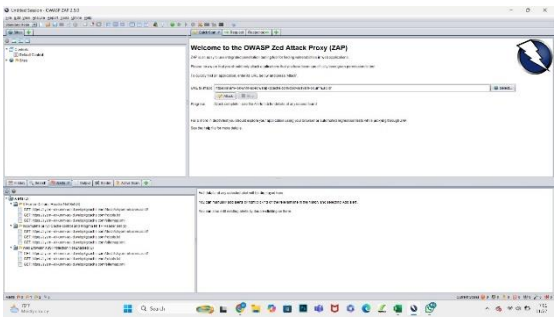
Tahap akhir adalah menyusun laporan hasil evaluasi keamanan aplikasi SYAM-OK. Laporan ini akan mencakup:

- Daftar kerentanan yang ditemukan beserta tingkat keparahannya.
- Potensi dampak yang mungkin terjadi jika kerentanan tidak segera ditangani.
- Rekomendasi perbaikan untuk mengatasi kerentanan yang ditemukan.

Laporan ini akan menjadi bahan evaluasi bagi pengembang aplikasi SYAM-OK untuk meningkatkan tingkat keamanan aplikasi tersebut.

III. HASIL DAN PEMBAHASAN

Hasil pemindaian mengidentifikasi beberapa kerentanan, yang dapat dilihat pada gambar 1. di bawah ini.



Gambar 1. Hasil Analisis Kerentanan

Dari gambar 1 diatas, hasil diklasifikasikan berdasarkan tingkat risikonya. Berikut adalah analisis lebih rinci dari setiap temuan :

1. **Kerentanan Tingkat Sedang: X-Frame-Options Header Tidak Disetel.**

Kerentanan ini ditemukan karena website yang tidak menyertakan header X-Frame-Options dalam respons HTTP. Akibatnya, website rentan terhadap serangan clickjacking. Serangan ini dapat menyebabkan pengguna mengklik elemen tanpa sadar di halaman yang dimanipulasi.

- Potensi dampak : Pengguna dapat diarahkan ke tindakan yang tidak disengaja, seperti mengungkapkan informasi sensitif.

- Solusi yang Disarankan : Menyertakan header X-Frame-Options dengan nilai SAMEORIGIN atau DENY untuk mencegah pemuatan halaman pada frame di domain yang tidak diizinkan.

2. Kerentanan Tingkat Rendah: Cache-control dan Pragma HTTP Header Tidak Lengkap

Header HTTP cache-control dan pragma tidak dikonfigurasi dengan benar.

Hal ini dapat memungkinkan browser atau proxy menyimpan cache konten yang seharusnya tidak boleh di-cache, meningkatkan risiko akses informasi sensitif oleh pihak yang tidak sah.

- Potensi dampak : Informasi sensitif dapat diakses dari cache yang tidak terproteksi.
- Solusi yang Disarankan : Mengatur nilai ni-cache, no-store, must-relivalidate pada header cache-control dan no-cache pada header pragma.

3. Kerentanan Tingkat Rendah: Proteksi XSS Tidak Diaktifkan

Header HTTP x-xss-Protection tidak diaktifkan. Hal ini meningkatkan risiko serangan Cross-Site Scripting (XSS), di mana penyerang dapat menyisipkan skrip berbahaya untuk mencuri data pengguna atau mengubah tampilan halaman.

- Potensi dampak : Skrip berbahaya dapat dieksekusi di browser pengguna tanpa sepengetahuan mereka.
- Solusi yang Disarankan : Menyertakan header X-XSS-Protection dengan nilai 1; mode=block untuk mengaktifkan proteksi XSS.

Kerentanan yang di temukan mayoritas tergolong tingkat risiko rendah hingga sedang. Namun, meskipun tidak ada kerentanan tingkat tinggi, kerentanan tingkat sedang seperti clickjacking tidak dapat menimbulkan ancaman serius jika tidak segera diperbaiki. Hal ini penting untuk mencegah eksploitasi oleh pihak yang tidak bertanggung jawab.

Solusi yang disarankan untuk setiap kerentanan telah disusun berdasarkan dokumentasi OWASP dan pedoman dalam pengamanan aplikasi web. Implementasi solusi tersebut dapat meningkatkan keamanan website SYAM-OK secara signifikan dan mengurangi risiko serangan siber.

IV. KESIMPULAN

Kesimpulan

Penelitian ini berhasil mengidentifikasi beberapa kerentanan keamanan pada aplikasi SYAM-OK menggunakan metode vulnerability assessment. Temuan utama mencakup kerentanan tingkat sedanag, seperti clickjacking, dan tingkat rendah, seperti proteksi XSS yang tidak aktif dan konfigurasi cache-control yang tidak memadai. Meskipun tidak ditemukan kerentanan tingkat tinggi, setiap celah keamanan yang teridentifikasi berpotensi membahayakan jika tidak segara diperbaiki. Solusi yang disarankan berbasis pada panduan OWASP, dengan penerapan langkah-langkah seperti pengaturan header HTTP yang tepat dan peningkatan konfigurasi keamanan lainnya. Implementasi rekomendasi ini akan meningkatkan keamanan aplikasi SYAM-OK secara signifikan.

Saran

1. Peningkatan Konfigurasi Keamanan: Penerapan header HTTP seperti X-Frame-Opyions, X-XSS-Protection, dan cache-control harus segera dilakukan untuk mengurangi risiko kerentanan
2. Peningkatan Kesadaran Pengguna: Pelatihan dan edukasi bagi pengguna aplikasi SYAM-OK tentang pentingnya keamanan data dan cara mencegah risiko serangan dapat membantu mengurangi potensi ancaman.
3. Pengujian Keamanan Berkala: Evaluasi keamanan harus dilakukan secara berkala untuk memastikan bahwa pembaruan sistem atau perubahan konfigurasi tidak membuka celah baru.
4. Peningkatan Infrastruktur Keamanan: Menambahkan fitur keamanan tambahan, seperti autentikasi multifaktor, dapat memperkuat perlindungan aplikasi dari serangan yang lebih kompleks.

REFERENSI

[1] Aziz, M. A. (2023). "Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas Xyz". Journal of Engineering, Computer Science and Information Technology (JECSIT), 2(1). https://doi.org/10.33365/jecsit.v1i1.13

[2] Efendi, R., Wahyono, T., & Widiasari, I. R. (2024). "Uji kerentanan keamanan pada web Sistem Informasi Akademik Satya Wacana menggunakan metode Vulnerability Assessment". Aiti, 21(1), 44–57. https://doi.org/10.24246/aiti.v21i1.44-57

[3] Tania, A. M., Setiyadi, D., Khasanah, F. N., Kunci, K., Cvss, Linux, K., & Website, K. (2018). "Keamanan Website Menggunakan Vulnerability Assessment. Informatics For Educators and Professionals", 2(2), 171–180

[4] Darmawan, C., Naibaho, J. P. P., & Kweldju, A. De. (2024). "Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021".

Edumatic : Jurnal Pendidikan Informatika, 8(1), 272–281. https://doi.org/10.29408/edumatic.v8i1.25834

[5] Armando, R., Melyantara, I. G. A. K. A., Elfariani, R., Latuconsina, D. F. A., & Nasrullah, M. (2022). "*IT Support Website Security Evaluation Using Vulnerability Assessment Tools*." Journal of Information Systems and Informatics, 4(4), 949–957. https://doi.org/10.51519/journalisi.v4i4.330

[6] Rohim, A., & Setiyani, L. (2023). "Analisis Celah Keamanan E-LearningPerguruan Tinggi Menggunakan Vulnerability Assessment". Jipakif, 1(1), 1–10

[7] Chandrakant, B. A., & Prakash, J. P. (2019). "*Vulnerability Assessment and Penetration Testing As Cyber Defence"*. International Journal of Engineering Applied Sciences and Technology, 4(2), 72–76. https://doi.org/10.33564/ijeast.2019.v04i02.012