JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1675-1680

Analisis Celah Keamanan Aplikasi Website Alumni Universitas Pamulang Dengan Menggunakan *Acunetix Vulnerability Scanner*

Saprudin[1*], Ajies Husna Manais[2], Johan Susuilo[3], Mochammad Rizky[4], Niken Dyah Ayu Puspitarini [5]

[1]Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
Email: [1*]dosen00845@unpam.ac.id, [2]ajiesmanais01@gmail.com, [3]johan.susilo154@gmail.com, [4]mochammadrizky514@gmail.com, [5]ndyahikena14@gmail.com
(* : coressponding author)

Abstrak − Dalam era internet saat ini, keamanan website sangat penting, terutama untuk lembaga akademik seperti Universitas Pamulang. Meskipun website alumni dapat membantu lulusan berinteraksi dan mendapatkan informasi, mereka juga dapat menjadi sasaran serangan siber. Tujuan dari penelitian ini, yang menggunakan perangkat lunak Acunetix untuk melakukan analisis celah keamanan pada situs web alumni Universitas Pamulang, adalah untuk mengumpulkan data melalui pemindaian otomatis menggunakan Acunetix, dan kemudian melakukan analisis mendalam dari temuan yang dihasilkan. Hasil pemindaian menunjukkan beberapa masalah keamanan yang perlu ditangani. Ini termasuk serangan SQL Injection, Cross-Site Scripting (XSS), dan konfigurasi keamanan yang kurang optimal. Selain itu, penelitian ini memberikan saran tentang cara memperbaiki masalah keamanan yang ditemukan dan langkah-langkah pencegahan yang dapat diambil untuk meningkatkan keamanan situs web. Dengan menerapkan saran ini, diharapkan situs web alumni Universitas Pamulang dapat melindungi lebih baik data dan informasi pengguna.

Kata Kunci: Keamanan Web; Celah Keamanan; Acunetix; Vulerability; Web; Universitas Pamulang; Analisis Keamanan

Abstract − In the current internet era, website security is very important, especially for academic institutions like Pamulang University. Although alumni websites can help graduates interact and obtain information, they can also become targets of cyber attacks. The objective of this research, which uses Acunetix software to conduct a security vulnerability analysis on the Pamulang University alumni website, is to collect data through automated scanning using Acunetix, and then perform an in-depth analysis of the generated findings. The scan results show several security issues that need to be addressed. This includes SQL Injection attacks, Cross-Site Scripting (XSS), and suboptimal security configurations. In addition, this research provides recommendations on how to fix the identified security issues and preventive measures that can be taken to enhance the website's security. By implementing these recommendations, it is hoped that the alumni website of Pamulang University can better protect user data and information.

Keywords: Web Security; Security Vulnerabilities; Acunetix; Vulnerability; Web; Pamulang University; Security Analysis

1. PENDAHULUAN

Seiring dengan perkembangan internet, teknologi web memiliki dampak yang signifikan terhadap peradaban. Tatanan hidup masyarakat di seluruh dunia telah diubah oleh internet. Dengan lebih dari 4 miliar orang yang menggunakan internet, diperkirakan akan ada lebih banyak orang yang menyalahgunakan internet untuk tujuan kejahatan [1], dan peretas akan membocorkan data [2]. Aplikasi berbasis web adalah salah satu sistem yang sering menjadi sasaran hacker atau cracker karena penggunaan aplikasi sedang meningkat[3]. Dengan demikian, keamanan sangat penting untuk mencegah serangan seperti Cross Site Scripting (XSS), Cross Site Request Forgeri (CSRF), dan SQL Injection [4].

Kelemahan sistem jaringan komputer, juga dikenal sebagai kelemahan keamanan, adalah kelemahan, kekurangan, atau celah yang dapat dimanfaatkan oleh satu atau lebih penyerang untuk melakukan serangan yang dapat membahayakan ketersediaan, kerahasiaan, atau integritas sistem [5]. Acunetix Vulnerability Scanner adalah salah satu cara untuk melakukan evaluasi keamanan website dengan menggunakan perangkat lunak yang dirancang khusus untuk menemukan kerentanan sistem[6].

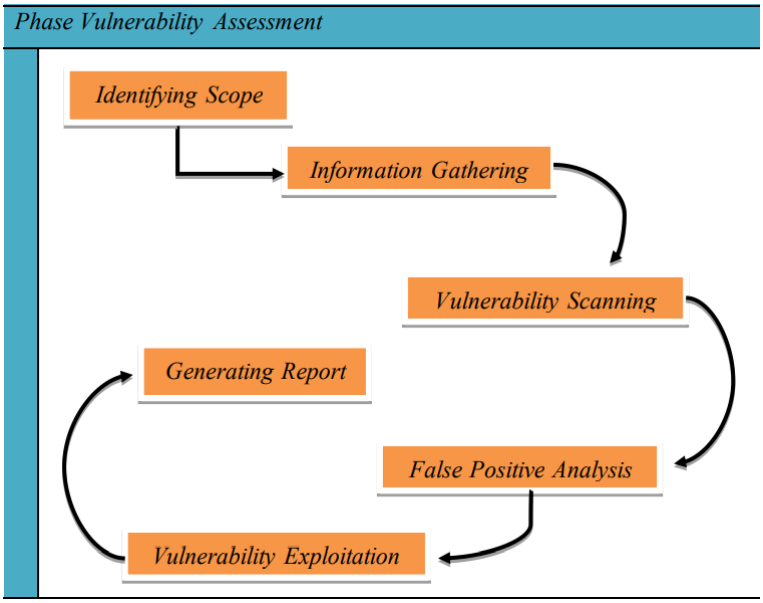
JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1675-1680

Pengujian kelemahan adalah pengukuran atau evaluasi yang mutlak dilakukan untuk mendapatkan peningkatan kualitas, dan salah satu caranya adalah dengan mengukur keamanan sistem. Hasil pengukuran atau evaluasi ini akan membantu pengembang mengambil tindakan pencegahan dan mengetahui bagaimana serangan atau pencuri beroperasi[7].

Penelitian ini bertujuan untuk mengevaluasi keamanan situs web alumni Universitas Pamulang melalui pemindaian otomatis menggunakan perangkat lunak Acunetix. Dengan mengidentifikasi celah keamanan yang mungkin ada, penelitian ini diharapkan dapat memberikan gambaran yang jelas mengenai kondisi keamanan situs web serta rekomendasi untuk perbaikan. Hasil dari penelitian ini tidak hanya bermanfaat bagi Universitas Pamulang, tetapi juga dapat dijadikan referensi bagi lembaga pendidikan lainnya dalam upaya meningkatkan keamanan digital mereka.

2. METODE

Metode penelitian yang digunakan adalah Vulnerability Assesment dan Penetration Testing Life Cycle. Tahapan pada VAPT Life Cycle, dapat dilihat pada gambar 1.



Gambar 1. Tahap Penelitian

Penjelasan dari tahapan-tahapan VAPT Life Cycle:

1. *Identifying Scope*

   Tahap pertama adalah menentukan jenis penelitian yang akan dilakukan. Untuk penelitian ini, peneliti akan menggunakan situs web alumni Universitas Pamulang sebagai subjek penelitian.

2. *Information Gathering*

   Tahap kedua adalah tahap perencanaan untuk mengidentifikasi kerentanan.

3. *Vulnerability Scanning*

   Tahap ketiga merupakan tahap *Vulnerability Scanning* yang dimana tahap ini mengidentifikasi potensi kerentanan dalam sistem atau aplikasi yang diuji menggunakan tools scanning acunetix

4. *False Positive Analysis*

   Pada tahap keempat, daftar kerentanan yang diperoleh dari hasil pemindaian tahap ketiga dikumpulkan. Tugas utama yang harus dilakukan di sini adalah membedakan daftar kerentanan yang diperoleh dari kerentanan yang salah.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1675-1680

5. *Vulnerability Explotation*

   Tahap kelima adalah untuk menembus sistem target melalui eksploitasi kerentanan yang telah diidentifikasi atau eksploitasi kerentanan yang terkenal yang tersedia secara publik dan dapat dimanfaatkan.

6. *Generating Report*

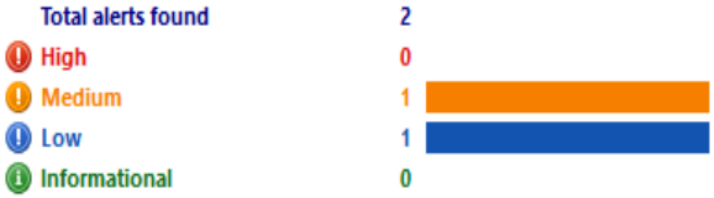
   Tahap keenam, yang merupakan tahap akhir, melibatkan pembuatan laporan yang menunjukkan kerentanan pada alamat IP 202.137.16.89 dan saran tentang cara memperbaiki kerentanan pada target uji.

3. HASIL DAN PEMBAHASAN

Pada bagian ini berisi hasil dari kegiatan penelitian yang sudah dilakukan

3.1 *Vulnerability Scanning (Executing Scan)*

Untuk mencapai tujuan ini, alat digunakan untuk melakukan pemindaian kerentanan pada situs web Alumni Universitas Pamulang. Hasil pemindaian dapat dilihat pada Gambar 2.



Gambar 2. Hasil Vulnerability Assement

Gambar di atas menunjukkan hasil scanning Vulnerability Assesment terhadap Web Alumni Universitas Pamulang. Tabel 1 berikut menunjukkan rincian kerentakan.

Tabel 1. Daftar Kerentanan

NO	Nama Kerentanan	Base Score	Tingkat Kerentanan
1	Clickjacking: X-Frame-Options header missing		
	CVSS3	4,3	Low
2	HTTPS connection with weak key length.		
	CVSS3	5,9	Medium

Hasil pindaian kerentanan menunjukkan beberapa kerentanan pada website alumni Universitas Pamulang. Diantaranya, Clickjacking: X-Frame-Options header missing, HTTPS connection with weak key length. Masing-masing kerentanan memiliki dampak dan tingkat kerentanan berbeda. Adapun penjelasan tiap-tiap kerentanan pada tabel diatas, sebagai berikut:

1. ***Clicjacking: X-Frame-Options header missing*** adalah teknik serangan yang memungkinkan penyerang untuk menipu pengguna agar mengklik sesuatu yang berbeda dari yang mereka pikirkan, yang bisa menyebabkan pengguna mengungkapkan informasi sensitif atau memberikan kontrol kepada penyerang atas perangkat mereka. Serangan ini terjadi ketika elemen interaktif pada sebuah situs web disembunyikan dalam iframe di halaman yang tampaknya aman, dan pengguna tanpa sadar mengklik elemen tersembunyi tersebut. Kerentanan ini terjadi pada port HTTP/HTTPS standar (port 80/tcp atau 443/tcp) dan dapat ditemukan ketika server tidak mengirimkan header X-Frame-Options, yang berfungsi untuk membatasi apakah sebuah halaman dapat disematkan dalam iframe di halaman lain. Tanpa header ini, situs web rentan terhadap serangan clickjacking, karena halaman web tersebut dapat

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1675-1680

disematkan di situs lain yang dimiliki penyerang. Kerentanannya memiliki base score CVSS 3.0 sebesar 4.3, yang menunjukkan tingkat keparahan low. Ini berarti meskipun kerentanannya ada, potensi dampak dari eksploitasi relatif rendah, tergantung pada elemen apa yang ada di dalam halaman tersebut. Kerentanan ini lebih berisiko jika halaman berisi elemen-elemen sensitif seperti tombol atau formulir yang bisa disalahgunakan oleh penyerang.

2. **HTTPS *connection with weak lenght*** adalah kerentanan yang terjadi ketika panjang kunci enkripsi untuk koneksi HTTPS lebih rendah dari rekomendasi standar yang aman, yaitu kurang dari 128 bit. HTTPS (HyperText Transfer Protocol Secure) digunakan untuk memastikan keamanan komunikasi antara server dan klien, dengan mengenkripsi data yang ditransmisikan. Panjang kunci yang lebih pendek dari standar yang disarankan dapat membuat koneksi lebih rentan terhadap serangan brute-force atau teknik lainnya yang dapat digunakan oleh pihak ketiga untuk memecahkan enkripsi. Kerentanan ini terjadi pada port 443/tcp, yang digunakan oleh koneksi HTTPS, yang seharusnya memastikan komunikasi yang aman melalui enkripsi yang kuat. Dalam kasus ini, panjang kunci yang lebih pendek dari yang seharusnya membuat data lebih mudah diintersepsi dan didekripsi oleh pihak yang tidak berwenang. Kerentanan ini memiliki base score CVSS 3.0 sebesar 5.9, yang menunjukkan tingkat kerentanannya medium. Hal ini berarti, meskipun serangan terhadap koneksi ini mungkin tidak langsung mengancam, potensi risiko untuk mengekspos data atau memecahkan enkripsi tetap ada, terutama jika informasi yang ditransmisikan sangat sensitif.

3.2 *Vulnerability Port Service*

Berikut ini merupakan port service yang dimiliki vulnerability pada web alumni universitas pamulang, dapat dilihat pada tabel 2.

Tabel 2. *Scanning Web Server*

Service Port	Threat Level
80/tcp	Low
443/tcp	Low
9200/tcp	Medium

Pada tabel 2 menjelaskan ada tiga port yang terbuka pada web alumni universitas pamulang. Berdasarkan hasil pemindaian, port 80/tcp(HTTP) dan 443/tcp(HTTPS) yang digunakan oleh web server, menunjukkan level ancaman yang rendah. Namun, ada juga port 9200/tcp(Elasticsearch) yang terdeteksi terbuka dengan level ancaman medium. Port ini figunakan oleh Elasticsearch, yang digunakan untuk pencarian dan analisis data besar. Jika tidak dikonfigurasi dengan benar, port ini bisa rentan terhadap serangan yang dapat mengekspos data sensitif atau memberikan akses yang tidak sah ke basis data.

Disarankan agar pengelola Web Alumni Universitas Pamulang secara terus-menerus memperbarui dan memantau web server serta semua port yang terbuka. Pembaruan keamanan harus dilakukan secara berkala untuk memastikan bahwa aplikasi tetap terlindungi dari potensi ancaman yang bisa membahayakan integritas dan keamanan data.

3.3 *Generating Report*

Generating report merupakan laporan tahap akhir dari kegiatan vulnerability scanning pada aplikasi web Web Alumni Universitas Pamulang. Laporan ini memberikan gambaran rinci tentang kerentanan yang telah diidentifikasi selama penilaian, beserta rekomendasi untuk mengatasinya. Web Alumni Universitas Pamulang diidentifikasi dengan tingkat kerentanan kritis, tinggi, medium, dan rendah. Tentu saja, setiap kerentanan memiliki dampak yang berbeda. Oleh karena itu, kami akan mencatat setiap masalah yang ditemukan dan membuat laporan tentang masalah tersebut pada tahap pembuatan laporan ini, seperti yang ditunjukkan oleh Tabel 3.

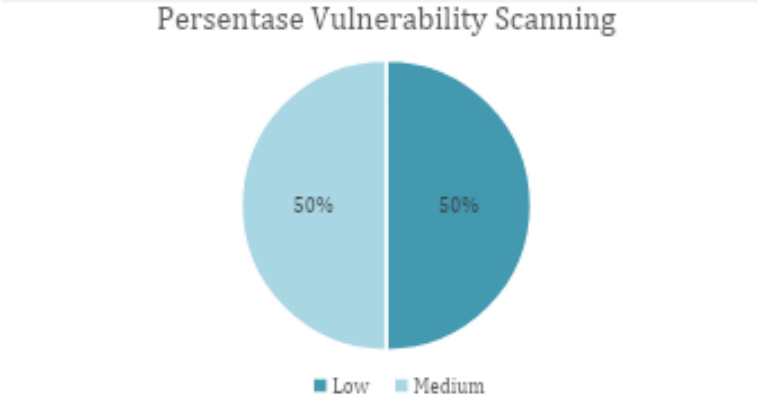
JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1675-1680

Tabel 3. Laporan *Vulnerability Assesment*

Nama Kerentanan	Dampak Kerentanan	**Solusi**
Clickjacking: X-Frame-Options header missing	Pengguna dapat terjebak dalam serangan clickjacking, yang bisa mengungkapkan informasi sensitif atau mengakibatkan tindakan yang tidak sah.	Menambahkan header X-Frame-Options dengan nilai DENY atau SAMEORIGIN pada server untuk mencegah halaman disematkan dalam iframe.
HTTPS connection with weak key length.	Sambungan dapat disadap dan mungkin didekripsi oleh pihak ketiga.	Panjang kunci harus minimal 128 bit untuk memastikan enkripsi yang cukup aman.

3.4 Presentase Vulnerability Scanning

Persentase ini didapatkan dari jumlah kerentanan yang ditemukan selama proses Vulnerability Scanning untuk mengetahui tingkat kerentanannya dari sisi keamanan pada Web Alumni Universitas Pamulang. Dengan persentase ini, kita dapat memahami distribusi kerentanannya berdasarkan tingkat keparahan, seperti Low dan Medium, dan menentukan langkah selanjutnya untuk meningkatkan keamanan aplikasi web.



Gambar 3. Web Alumni Universitas Pamulang

Pada Gambar 3 di bawah ini, menunjukkan persentase vulnerability scanning yang didapatkan dari jumlah kerentanan yang ditemukan. Total kerentanan yang ditemukan adalah 2, yang terdiri dari 1 kerentanan dengan level Low dan 1 kerentanan dengan level Medium. Dengan persentase ini, dapat dilihat bahwa Web Alumni Universitas Pamulang memiliki kerentanannya yang tersebar antara dua tingkat keparahan, yaitu Low dan Medium. Hal ini memberikan gambaran bahwa aplikasi web perlu melakukan beberapa perbaikan untuk mengatasi potensi ancaman yang ada, meskipun tingkat kerentanannya relatif moderat.

4. KESIMPULAN

Hasil pemindaian kerentanan adanya beberapa kerentanan yang perlu segera ditangani untuk menjaga keamanan situs Web Alumni Universitas Pamulang. Pemindaian kerentanan situs mengidentifikasi beberapa masalah keamanan, termasuk risiko clickjacking akibat header X-Frame-Options yang hilang, penggunaan HTTPS dengan kunci enkripsi lemah, dan akses terbuka pada port 9200/tcp (Elasticsearch). Untuk mengatasi hal ini, disarankan untuk menambahkan header X-Frame-Options, memperbarui kunci enkripsi HTTPS dengan minimal 128-bit, serta membatasi akses port Elasticsearch dengan firewall. Langkah-langkah ini akan meningkatkan keamanan situs dan melindungi data pengguna.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 9 Februari Tahun 2025
ISSN 3025-0919 (media online)
Hal 1675-1680

REFERENCES

[1] Number of Internet Users (2016) - Internet Live Stats. (2020, February 2).
[2] Juardi, D. (2017, November 28). Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. Syntax: Jurnal Informatika.
[3] F. Al Fajar, "Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web Vulnerability," Inova-Tif, vol. 3, no. 2, p. 110, 2020, doi: https://doi.org/10.32832/inova-tif.v3i2.4127
[4] I. Riadi, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," JTIIK, vol. vol 7 No 4, 2020.
[5] B. W. Retna Mulya and A. Tarigan, "Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan Cvss Dan Fmea," Ilk. J. Ilm., vol. 10, no. 2, pp. 190-200, 2018, doi :https://doi.org/10.33096/ilkom.v10i2.311.190-200
[6] R. Mayasari, A. A. Ridha, D. Juardi, and K. A. Baihaqi, "Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability," 2020. doi : https://doi.org/10.35706/sys.v2i1.3450
[7] M. Orisa and M. Ardita, "VULNERABILITY ASSESMENT UNTUK MENINGKATKAN KUALITAS KEAMANAN WEB," 2021. doi : https://doi.org/10.36040/mnemonic.v4i1.3213