ANALISIS PERBANDINGAN *VULNERABILITY ASSESMENT* MENGGUNAKAN OWASP ZAP DAN ACUNETIX PADA WEBSITE SIAKAD STMIK AMIKOM SURAKARTA

Muhammad Firdaus Al-Farizi *[1], Ezar Ramadhan[2], Syakara Akbar [3]
[1234]Prodi Informatika, STMIK Amikom Surakarta
[1234]Sukoharjo Indonesia
Email: [1]muhammad.10411@mhs.amikomsolo.ac.id,
[2]ezar.10387@mhs.amikomsolo.ac.id, [3]syakara.10384@mhs.amikomsolo.ac.id

Abstract

STMIK Amikom Surakarta is a private university that has a web-based information system that supports various needs for lecture activities in the form of an academic information system. In some cases, there are many risks that occur, such as attacks from irresponsible parties if they do not have a good security system. The purpose of the research is to find gaps in the website system by conducting tests as Vulnerability Assessments using two penetration testing tools, namely owasp zap and acunetix. The results obtained from the study showed that there were 13 warnings on the owasp test and 22 warnings on acunetix, each of which had different levels of vulnerability.

Keywords: *Stmik Amikom Surakarta, Academic Information System, Vulnerability Assesment, Owasp Zap and Acunetix*

Abstraksi

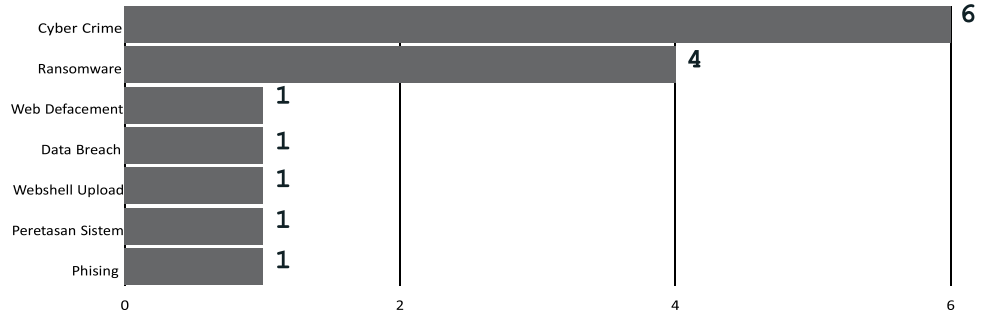
STMIK Amikom Surakarta merupakan perguruan tinggi swasta yang memiliki sistem informasi berbasis web yang menunjang berbagai kebutuhan kegiatan perkuliahan yang berupa sistem informasi akademik.Dalam beberapa hal banyak resiko yang terjadi seperti serangan dari pihak yang tidak bertanggung jawab apabila tidak memliki sistem keamanan yang baik.Tujuan dilakukan penelitian adalah mencari celah sistem website dengan melakukan pengujian sebagai Vulnerability Assesment dengan menggunakan dua alat penetration testing yaitu Owasp Zap dan Acunetix.Hasil yang diperoleh dari penelitian menunjukkan ada 13 peringatan pada pengujian Owasp Zap dan 22 peringatan pada Acunetix yang masing masing memiliki tingkat kerentanan yang berbeda-beda.

Kata Kunci: *STMIK Amikom Surakarta, Sistem Informasi Akademik, Vulnerability Assesment, Owasp Zap dan Acunetix*

1. PENDAHULUAN

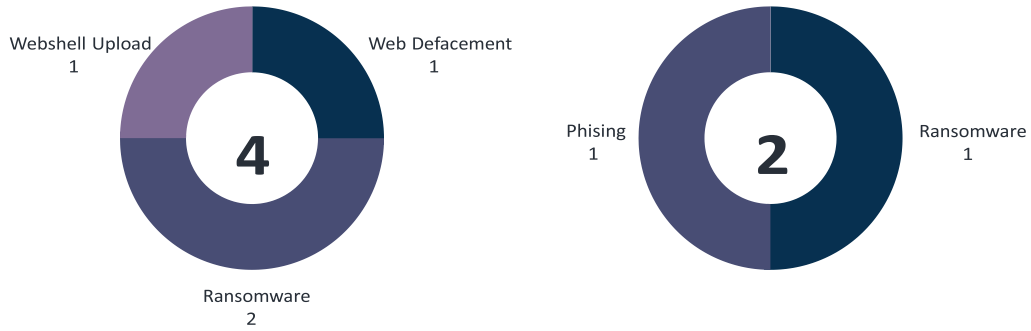
Di era kemajuan teknologi sistem informasi dan keamanan jaringan komputer merupakan aspek penunjang dalam kehidupan masa kini.Jaringan komputer sebagai sarana untuk berkomunikasi pertukaran data dan informasi serta pengelola sumber daya yang efektif,akan tetapi seiring kemajuan kompleksitas jaringan.Berbagai serangan muncul dari segi keamanannya.Serangan tersebut dapat berupa,malware,ancaman siber,penyalahgunaan kerentanan jaringan.

Menurut laporan direktorat operasi keamanan cyber pada november 2022 menerima berbagai aduan tentang cyber crime yang berjumlah 6 aduan,serta diikuti aduan mengenai ransomware berjumlah 4 aduan,aduan tersebut berupa web defacement,phising,data breach,webshell,dan peretasan sistem yang masing masing memiliki jumlah 1 aduan.Sementara itu dari segi pembagian sektor yang terpengaruh,aduan siber paling banyak berjumlah 7 aduan yang berasal dari sektor yang lain [1].



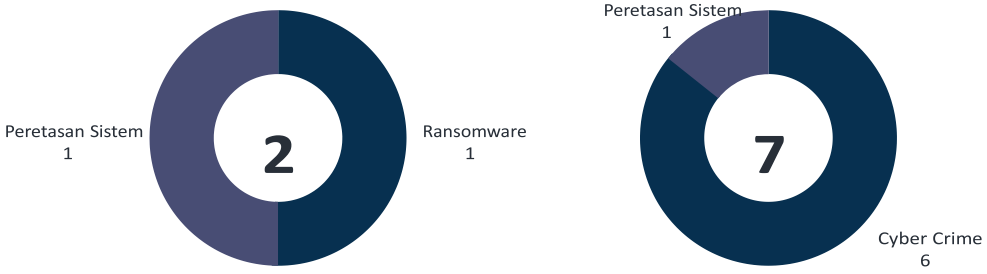
Sumber : BSSN (2022)

Gambar 1. Statistik Laporan



Sumber : BSSN (2022)

Gambar 2. Statistik Laporan



Sumber : BSSN (2022)

Gambar 3. Statistik Laporan

c

Menurut (G.J.Simons, 2018) [2] keamanan Sistem Informasi merupakan bagaimana kita dapat mendeteksi atau lebih tepatnya mencegah perilaku tidak jujur dalam sebuah sistem yang didasarkan pada sistem informasi tetapi informasinya sendiri tidak memiliki arti fisik. (Perrin, 2008) [3] memberikan penjelasan bahwasanya dalam sistem informasi terdapat CIA (confidentiality,Integrity,Availibility) yang merupakan model terkenal untuk mengembangkan kebijakan keamanan informasi.Model ini digunakan untuk mengidentifikasi masalah dan solusi yang dibutuhkan untuk keamanan Sistem Informasi. Sistem informasi digital seperti website merupakan salah satu contoh target utama dari serangan siber.Beberapa contoh serangan diantaranya serangan ddos (distributed denial of service),serangan brute force,serangan cross-site (xss),serangan sql injection, serangan malware dan lain sebagainya.Untuk mengamankan web server dari pihak yang tidak bertanggung jawab,sistem harus dievaluasi dengan baik dengan menjalankan self-test pada web server dengan menggunakan *penetration testing* [4].*Penetration testing*,sering dikenal sebagai uji penetrasi,adalah metode yang efektif untuk mendeteksi kerentanan sistem.Dengan demikian,penetration testing adalah metode yang digunakan untuk mendapatkan akses ke sistem tanpa perlu mengetahui nama pengguna,kata sandi,atau detail data pribadi yang lain [5].

2. TINJAUAN PUSTAKA

Beberapa penelitian yang sudah dilakukan yang berkenan dengan Pengujian keamanan website menggunakan Berbagai *Tools* Memperoleh Kelebihan dan Kekurangannya.Tinjauan pustaka dibuat untuk memberikan gambaran pada perkembangan dari pengujian terdahulu.

Penelitian ini menggunakan 2 alat penetration testing yaitu *Owasp Zap dan Acunetix* yang digunakan untuk mengidentifikasi serta menyelidiki celah dari keamanan sistem pada website.*Owasp* adalah sebuah kerangka kerja yang digunakan oleh para pengembang dan ahli teknologi untuk mengamankan situs web.*Owasp* menyediakan tempat bagi para pengembang untuk meningkatkan keamanan sistem melalui proyek sumber terbuka dan *tools Owasp* sebagai sarana pengujian sistem [6].Sedangkan *Acunetix Web Vulnerability* merupakan alat keamanan aplikasi web yang secara otomatis menilai sebuah aplikasi dengan mencari kerentanan seperti SQL Injection,Cross-Site Scripting,dan berbagai kerentanan yang yang lain.*Acunetix* adalah alat otomatis yang dapat memindai aplikasi web pada sebuah perusahaan untuk mengidentifikasi dan mendapati celah pada aplikasi [7].

Dari penelitian sebelumnya menggunakan jenis website yang berbeda dalam melakukan pengujian serta masih menggunakan *tools* yang sama tetapi memperoleh hasil kerentanan yang berbeda Penelitian ini akan dilakukan analisis perbandingan untuk menentukan jumlah peringatan,tingkat peringatan,serta dilakukan *Vulnerability Assesment* yang berguna untuk pencarian data baru sebagai penentuan rekomendasi

dalam pengujian.Berdasarkan permasalahan yang ada,objek penelitian ini adalah website sistem Informasi akademik Stmik Amikom Surakarta.

3. METODE PENELITIAN

Metode *Vulnerability Assesment* digunakan dengan melakukan beberapa tahapan proses untuk mengindentifikasi resiko serta dikelompokkan berdasarkan tingkat kerentanan pada suatu sistem menggunakan *Tools Owasp Zap* yang akan dikomparasikan dengan *Tools Acunetix*.pada penelitian ini dilakukan dengan tahapan tahapan yang sesuai dengan gambar flowchart yang tertera.

3.1. Studi Literatur

Tahapan pertama adalah studi literatur dengan tujuan memberikan penjelasan terkait kajian pustaka berlandaskan teori teori yang dapat menjadi bahan penelitian.Studi literatur didapat dari membaca berbagai jurnal,artikel,maupun buku yang ada diinternet [8].

3.2. Indentifikasi Website

Tahapan kedua adalah mengidentifikasi website sistem akademik informasi Stmik Amikom Surakarta yang didalamnya terdapat yang memuat informasi seputar kampus yang digunakan untuk berbagai kebutuhan seperti kurikulum,program studi,jadwal kuliah,pengajuan krs,dan masih banyak lagi yang dapat diakses oleh mahasiswa melalui situs web resmi http://siakad.amikom.solo.ac.id/ [9].

3.3. Pengujian pemindaian dengan *OWASP Zap* dan *Acunetix*

Tahapan ketiga adalah melakukan pengujian pemindaian dari data yang sudah didapatkan dengan menggunakan *Owasp Zap* dan *Acunetix* untuk melakukan *Vulnerability Assesment* yang nantinya dapat digunakan untuk mencari data baru dari berbagai celah yang ada pada website.

3.4. Pengumpulan Data dan Dokumentasi

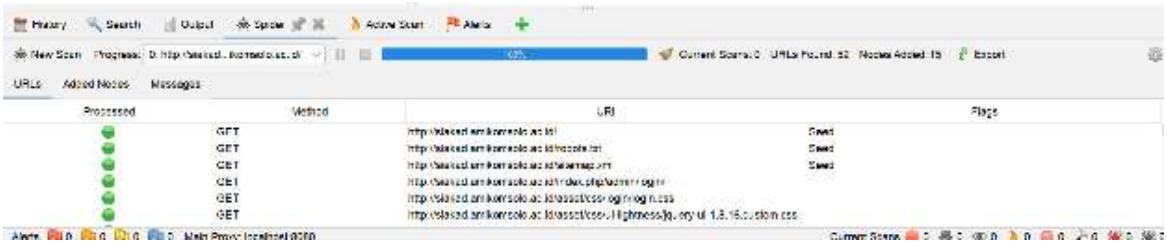
Tahapan keempat adalah pengumpulan data serta dokumentasi yang akan digunakan untuk mengkategorikan jenis celah keamanan,Dengan cara tersebut maka analisis menjadi lebih mudah dan efisien.Data tersebut akan dilakukan penilaian kerentanan pada proses penetration testing dari kedua alat yang nantinya dapat digunakan untuk Saran Perbaikan Serta Rekomendasi yang cocok bagi pengembang website [10].

4. HASIL DAN PEMBAHASAN

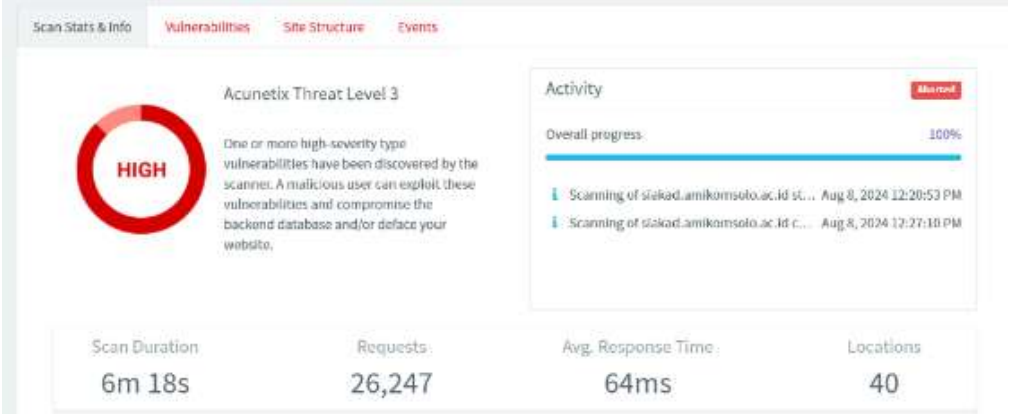
Setelah dilakukan penetrasi menggunakan *Owasp Zap dan Acunetix*,hasil dan pembahasan *Vulnerability Assesment* dari *Penetration Testing* meliputi proses scanning,hasil peringatan scanning,rekomendasi perbaikan.

4.1. Proses Pemindaian

Proses Pemindaian (scanning) adalah suatu proses dimana dari suatu sistem akan dilakukan pengujian untuk mengetahui tingkat keamanan website serta untuk mencari kerentanan dari sistem website yang dapat digunakan sebagai bahan evaluasi pengembang untuk memperkuat dan memperbaiki sistem tersebut.Berikut Proses dari pemindaian pada website sistem informasi akademik Stmik Amikom Surakarta menggunakan *Owasp Zap* dan *Acunetix* terdapat pada gambar 4 dan gambar 5**.**



Gambar 4. Proses Pemindaian Owasp Zap



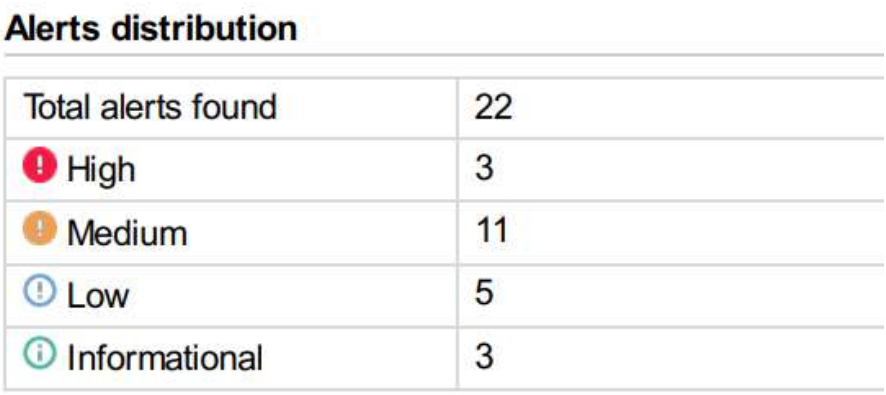
Gambar 5. Proses Pemindaian Acunetix

4.1.1. Hasil Peringatan Pemindaian

Setelah proses pemindaian selesai Tahapan selanjutnya adalah hasil peringatan akan muncul pada alat Owasp Zap dan Acunetix.Hasil menunjukkan ada 13 jenis peringatan pada Owasp Zap dimana terdapat kerentanan dengan status 0 high,4 medium,5 low,dan informational 4 yang menandakan sedangkan Acunetix berjumlah 22 peringatan dengan status high 3,medium 11,low 5,dan informational 4 dan disertakan tabel dari hasil pemindaian.Hasil pemindaian dan daftar peringatannya tertera gambar 6, gambar 7 dan Tabel.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (7.7%)	2 (15.4%)	1 (7.7%)	4 (30.8%)
	Low	0 (0.0%)	1 (7.7%)	4 (30.8%)	0 (0.0%)	5 (38.5%)
	Informational	0 (0.0%)	2 (15.4%)	0 (0.0%)	2 (15.4%)	4 (30.8%)
	Total	0 (0.0%)	4 (30.8%)	6 (46.2%)	3 (23.1%)	13 (100%)

Gambar 6. Hasil Scanning Owasp Zap



Alerts distribution

Total alerts found	22
High	3
Medium	11
Low	5
Informational	3

Gambar 7. Hasil Scanning Acunetix

Tabel 1. Daftar Kerentanan owasp zap dan acunetix

No	Owasp Zap	Acunetix
1	Absence of Anti-CSRF Tokens	Sql Injection
2	Content Security Policy (CSP) Header Not Set	Sql Injection
3	Missing Ant-clickjacking Header	Sql Injection
4	Vulnerable Js Library	Application Error Message
5	Cookie No HttpOnly Flag	Application Error Message
6	Cookie without sameSite Attribute	Application Error Message
7	Server Leaks Information via "X-Powered-By" HTTP Response Header Field (s)	Application Error Message
8	Server Leaks Information via "Server" HTTP Response Header Field	HTML form without CSRF protection
9	X-Content-Type-Options Header Missing	PHP versions 5.5.1.2 and 5.4.28
10	Authentication Request Identified	Slow HTTP Denial of Service Attack
11	Information Disclosure - Suspicious Comments	User Credential are sent in clear text
12	Session Management Response Identified	User Credential are sent in clear text
13	User Controllable HTML Element Attribute (Potensial XSS)	Vulnerable Javascript library
14		Vulnerable Javascript library
15		Clickjacking: X-Frame-Options header missing
16		Login Page password-guessing attack
17		Possible sensitive directories
18		Possible sensitive directories
19		Possible sensitive directories

No	**Owasp Zap**	**Acunetix**
20		Error page web server version disclosure
21		Password type input with auto-complete enabled
22		Password type input with auto-complete enabled
Total	13	22

4.1.2. Rekomendasi Perbaikan

Tahapan terakhir penelitian adalah Rekomendasi perbaikan.Rekomendasi Perbaikan adalah dokumentasi penilaian kerentanan yang digunakan untuk saran perbaikan bagi pengembang agar sistem yang dijalankan terlindungi dan terhindar dari serangan dari pihak yang tidak bertanggung jawab.Pengembange sistem dapat mengikuti Rekomendasi perbaikan untuk memperbaiki peringatan kerentanan.

a. Owasp Zap

1. **Absence of Anti-CSRF Tokens**
   Lakukan Implementasi token CSRF pada setiap formulir serta permintaan yang dapat melakukan modifikasi untuk memproteksi Serangan CSRF.
2. **CSP Header Not Set**
   Lakukan Konfigurasi header CSP pada server untuk mengatur sumber daya yang boleh disematkan oleh aplikasi web agar dapat mengurangi resiko Serangan XSS.
3. **Missing Anti-clickingjacking Header**
   Penambahan header X-Frame-Options atau Content-Security-Policy: frame-ancestors pada server untuk mencegah Apikasi disematkan iframe oleh situs lain.
4. **Vulnerable JS Library**
   Perbaruan Javascript ke versi yang baru dari kerentanan keamanan.
5. **Cookie without SameSite Atribute**
   Penyetelan atribut cookie yang ada pada SameSite untuk memproteksi serangan CSRF dengan cara memastikan kebijakan pengiriman cookie (Contoh : Samesite : Strict atau Samesite : Lax).
6. **Server Leaks Information via " X-Powered -By"HTTP Response Header Field**
   Modifikasikan atau hapus header X-Powered-By untuk menghindari pembongkaran informasi teknoloigi yang dipakai server.
7. **Server Leaks Information via " Server -By"HTTP Response Header Field**
   Sembunyikan atau Hapus Header Server dari tanggapan HTTP untuk mencegah Pembongkaran informasi server.
8. **X-Content-Type-Options Header Missing**
   Berikan Penambahan header X-.

9. **Content-Type-Options**
   nosniff untuk mencegah laman browser memprediksi tipe konten dan mengurangi resiko terjadinya serangan MIME Sniffing.
10. **Authetication Request Identified**
    Pastikan permintaan otentikasi melalui saluran dilakukan secara aman (contoh : HTTPS) sebagai pertimbangan mekanisme otentikasi yang kokoh.
11. **Information Discloure-Suspicious Comments**
    Hapus informasi sensitif dan komentar yang tidak menyakinkan yang terdapat pada kode sumber yang dapat menyebabkan kebocoran informasi yang berkaitan dengan aplikasi dan infrastruktur.
12. **Session management Response Identified**
    Peninjauan serta perbaikan Manajemen Sesi sebagai jaminan pada sesi yang dikelola berstatus aman,termasuk memverifikasikan token sesi serta mengatur waktu yang telah kadaluwarsa.
13. **User controllable HTML Element Attribute (Potensial XSS)**
    verifikasi serta pembersihan masukkan pengguna sebagai langkah pencegahan Penambahan skrip berbahaya pada elemen HTML.Gunakan panduan atau fungsi untuk mengelola HTML dinamis secara aman.

b. Acunetix

1. **Sql Injection**
   Gunakan kueri parameter saat melakukan penanganan kueri SQL yang berisi masukkan pengguna. Kueri yang diparameterisasi memungkinkan memahami bagian database mana dari kueri SQL yang harus dianggap sebagai input pengguna, sehingga dapat menyelesaikan injeksi SQL.
2. **Application Error Message**
   Verifikasi halaman menampilkan pesan kesalahan atau peringatan dan konfigurasikan aplikasi dengan benar untuk mencatat kesalahan kedalam file yang alih-alih yang dapat menampilkan kesalahan kepada pengguna.
3. **HTML form without CSRF protection**
   Verifikasi apakah formulir memerlukan perlindungan anti-CSRF dan lakukan penerapan pencegahan CSRF jika perlu.
4. **Multiple vulnerabilities fixed in PHP version 5.5.12 and 5.4.28**
   Tingkatkan Php ke versi yang baru.
5. **Slow HTTP Denial of Service Attack**
   pelajari referensi Web untuk informasi tentang cara melindungi server web dari serangan jenis ini.lu.
6. **User credentials are sent in clear text**
   dikarenakan kredensial pengguna dianggap sebagai informasi sensitif, maka harus selalu ditransfer ke server melalui koneksi terenkripsi (HTTPS).

7. **Vulnerable Java library**
   Tingkatkan java ke versi yang baru.
8. **Clickjacking: X-Frame-Options header missing**
   Konfigurasikan server web untuk menyertakan header X-Frame-Options. Lihat referensi Web untuk informasi lanjutan tentang nilai yang boleh jadi untuk header.
9. **Login Page Password-guessing attack**
   Disarankan untuk menerapkan beberapa jenis penguncian akun setelah beberapa kali apabila setelah melakukan percobaan kata sandi yang salah.
10. **Possible sensitive directories**
    Berikan Batasan akses ke direktori ini atau hapus dari situs web.
11. **Error page web server version discloure**
    Konfigurasikan server web dengan benar agar tidak mengungkapkan informasi tentang cara kerja internal aplikasi kepada pengguna. Lihat pada bagian referensi web untuk informasi lebih lanjut.
12. **Password type input with auto-completed enabled**
    Pelengkapan otomatis kata sandi harus dinonaktifkan pada aplikasi yang sensitif.Untuk menonaktifkan pelengkapan otomatis,dapat dengan menggunakan kode yang mirip dengan:
    (<INPUT TYPE = "password" AUTOCOMPLETE = "off">)

5. KESIMPULAN

Kesimpulan yang didapatkan dari penelitian ini adalah setelah dilakukan Pengujian pada Alat Owasp Zap dan Acunetix pada website sistem informasi akademik stmik amikom surakarta berhasil mendeteksi kerentanan pada berjumlah

- 13 peringatan untuk *Owasp Zap* yang memiliki level
  1. medium 4
  2. low 5
  3. informational 4
- sedangkan *Acunetix* berjumlah 22 Peringatan dengan level
  1. high 3
  2. medium 11
  3. low 5
  4. informational 3

Setelah pemindaian dan pemrosesan data, selanjutnya data data tersebut dikumpulkan yang nantinya dapat dikaji ulang serta dilakukan pembuatan rekomendasi sebagai bahan pertimbangan perbaikan bagi pengembang sistem.

DAFTAR PUSTAKA

[1] BSSN, "Laporan Bulanan Publik," no. 70, pp. 01–20, 2023, [Online]. Available: www.idsirtii.or.id

[2] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)," *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022, doi: 10.31933/jemsi.v3i5.992.

[3] B. Harahap, "Penerapan Keamanan Owasp Terhadap Aplikasi GTFW Pada Website Universitas Battuta," *J. Inform. dan Teknol. Pendidik.*, vol. 1, no. 2, pp. 80–86, 2021, doi: 10.25008/jitp.v1i2.15.

[4] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[5] H. Sofyan, M. Sugiarto, and B. M. Akbar, "Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN 'Veteran' Yogyakarta," *Telematika*, vol. 20, no. 2, p. 153, 2023, doi: 10.31315/telematika.v20i2.7757.

[6] 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

[7] 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: 10.32832/inova-tif.v3i2.4127.

[8] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.

[9] 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.

[10] Riyan Farismana and Dian Pramadhana, "Perbandingan Vulnerability Assesment Menggunakan Owasp Zap dan Acunetix Pada Sistem Informasi Repositori Politeknik Negeri Indramayu," *J. Tek. Inform. dan Teknol. Inf.*, vol. 3, no. 2, pp. 26–32, 2023, doi: 10.55606/jutiti.v3i2.2853.