Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode *Vulnerability Assessment*

Erick Irawadi Alwi[*], Lutfi Budi Ilmawan[**]
[*]Program Studi Sistem Informasi, Fakultas Ilmu Komputer Universitas Muslim Indonesia
[**]Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Muslim Indonesia
[*]erick.alwi@umi.ac.id, [**]lutfibudi.ilmawan@umi.ac.id

ABSTRACT

The use of academic information systems (siakad) has become mandatory for universities in providing user convenience in online academic administrative activities. However, sometimes college siakad has security holes that irresponsible people can take advantage of by hacking. This study aims to identify security vulnerabilities at XYZ Siakad University.

The method used in this study is a vulnerability assessment method. A university syakad will conduct an initial vulnerability assessment by doing footprinting to get information related to XYZ syakad after that a vulnerability scan is carried out using vulnerability assessment tools to identify vulnerabilities and the level of risk found.

Based on the vulnerability of the XYZ university's vulnerabilities, it is quite good, with a high risk level of 1, a medium risk level of 6 and a low risk level of 14. Researchers provide recommendations for improvements related to the findings of security holes in XYZ university Siakad from XSS (Cross Site Scripting) attacks, Clickjacking, Brute Force, Cross-site Request Forgery (CSRF) and Sniffing.

Keyword: Siakad, Security, Vulnerbaility Assessment, risk level

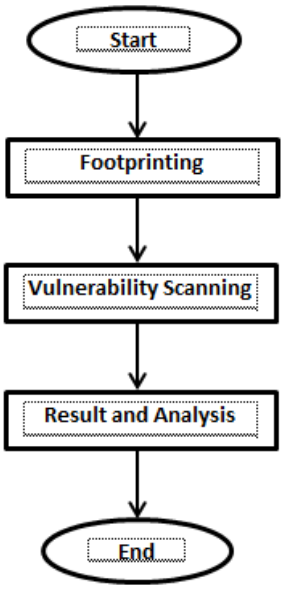
1. Introduction

Sistem Informasi Akademik (SIAKAD) merupakan sistem yang mengolah data dan melakukan proses kegiatan akademik yang melibatkan antara mahasiswa, dosen, dan administrasi akademik. Sistem informasi Akademik melakukan kegiatan proses administrasi mahasiswa dalam melakukan kegiatan administrasi akademik, melakukan proses pada transaksi belajar-mengajar antara dosen dan mahasiswa, melakukan proses administrasi akademik baik yang menyangkut kelengkapan dokumen dan biaya yang muncul pada kegiatan registrasi administrasi akademik[1]. Sistem Informasi Akademik (SIAKAD) selain merupakan sumber daya informasi di kampus, juga dapat digunakan sebagai sarana media komunikasi antara dosen dan mahasiswa, mahasiswa dengan mahasiswa dosen dengan pejabat kampus terkait dan siapa saja yang ada di lingkungan kampus tersebut. Namun terkadang siakad pada perguruan tinggi memiliki celah keamanan yang dapat dimanfaatkan orang yang tidak bertanggung jawab dengan melakukan peretasan. Penelitian ini bertujuan untuk mengidentifikasi celah kerentanan keamanan pada siakad universitas XYZ.

Vulnerability Assessment adalah proses mendefinisikan, mengidentifikasi, mengklasifikasikan, dan memprioritaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan dan memberikan organisasi melakukan penilaian dengan pengetahuan, kesadaran, dan latar belakang risiko yang diperlukan untuk memahami ancaman terhadap lingkungannya dan bereaksi dengan tepat. Proses *vulnerability assessment* yang dimaksudkan untuk mengidentifikasi ancaman dan risiko yang ditimbulkannya biasanya melibatkan penggunaan alat pengujian otomatis, seperti pemindai keamanan jaringan, yang hasilnya terdaftar dalam laporan *vulnerability assessment* [2].

2. Research Method

Metode yang digunakan pada penelitian ini adalah metode *Vulnerability Assessment*. *Vulnerability assessment* adalah sebuah metode mencari celah kerentanan dari *website* target (SIAKAD Universitas XYZ) yang dapat diakses secara online dengan menggunakan *tools vulnerability scanning* [3]. Adapun tahapan penelitian dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

1. *Footprinting* adalah tahapan menemukan struktur rancang bangun dari keamanan jaringan pada target sasaran yang dituju sebagai barometer metodologi [4].
2. *Vulnerability Scanning* adalah tahapan dilakukannya *vulnerability scanning* dengan mengggunakan berbagai *tools vulnerability scanning* (Acunetix, OWASP ZAP, dan Nikto). tujuan yang ingin dicapai yaitu mencari celah keamanan yang terdapat pada target mencakup beberapa seperti *SQL Injection, Cross Site Scripting* (XSS), *Remote OS Command, Path Transversal, Private IP Disclosure* pada suatu sistem operasi atau aplikasi [5].
3. *Result and Analysis*, Tahapan ini akan memberikan hasil analisis terkait celah keamanan yang ditemukan dan memberikan rekomendasi perbaikan celah keamanan tersebut.

Adapun tools yang digunakan pada pengujian *vulnerability assessment* penelitian ini dapat diliat pada Tabel 1.

Tabel 1. *Tools Footprinting* dan *Vulnerability Scanning*

No	Tools	Fungsi
1	Zenmap (Nmap)	Aplikasi *open source* untuk explorasi *network* dan audit keamanan
2	Dnsdumpster	Aplikasi mengumpulkan data dan mapping suatu domain dan subdomain
3	Acunetix	Aplikasi mendeteksi dan memberitahukan berbagai macam kerentanan dalam aplikasi yang dibangun pada berbagai platform seperti *WordPress, PHP, ASP.NET, Java Frameworks, Ruby on Rails* dan lain-lain.
4	Owasp Zap	aplikasi pentest untuk menemukan *vulnerabilities* dalam suatu web applications
5	Nikto	alat scanning aplikasi web yang mencari kesalahan konfigurasi, direktori web diakses secara terbuka dan sejumlah kerentanan aplikasi web.

3. Result and Analysis

3.1. Hasil pengujian *Footprinting* dan *Vulnerability Assessment*

Footprinting adalah kegiatan mengumpulkan informasi sebanyak-banyaknya yang terkait dengan target, seperti perangkat yang digunakan, merek, tipe, nomor versi OS, topologi fisik *network*, perangkat *security, network address, subnetting*, dan lain-lain [6]. Adapun *tools footprinting* yang digunakan pada penelitian ini yaitu aplikasi Zenmap, dan dnsdumpster

3.1.1 Hasil *footprinting* dengan Zenmap dan dnsdumpster

Tabel 2. Hasil pengujian *Footprinting* pada *website* siakad universitas XYZ

No	*Tools Footprinting*	Informasi yang ditemukan target
1	Zenmap	*Operating system (OS) version*
		Port-port yang terbuka
		Traceroute
		Topologi jaringan
		Service pada server dan *version*
2	dnsdumpster	Nama domain
		Alamat IP
		Lokasi server
		Server software
		Reverse IP

Dari hasil pengujian pada Tabel 2. terlihat hasil pengujian *Footprinting* pada *website* target dengan menggunakan *tools Footprinting* (Zenmap dan dnsdumpster) ditemukan beberapa informasi terkait target sebagai sub domain dari xxxxxx.xx.id antara lain IP Server, *Operating system (OS) version server*, *port-port* yang terbuka, topologi jaringan, *service* pada server dan *version* dan lokasi server. peneliti memberikan rekomendasi kepada admin pengelola *website* siakad universitas XYZ untuk memprotect informasi-informasi data sensitif dari *website (whois protect)* agar pihak yang tidak berkepentingan (*hacker*) tidak dapat mengakses dan tidak dapat mengekploitasi lebih lanjut informasi tersebut.

3.2. Hasil pengujian dengan teknik *vulnerability scanning*

Vulnerability scanning adalah proses memperoleh informasi *vulnerability network* dengan memanfaatkan berbagai *tools vulnerability scanning*, seperti *port* yang terbuka, *bugs* aplikasi server dan lain-lain [6]. adapun *tools vulnerability scanning* yang digunakan pada penelitian ini yaitu Acunetix, OWASP ZAP dan Nikto.

Tabel 3. Hasil pengujian *Vulnerability Scanning* pada *website* siakad universitas XYZ

No	*Vulnerability Scanning*	*Alert*	*Risk Assessment*	Rekomendasi
1	Acunetix	- Multiple vulnerabilities fixed in PHP versions 5.5.12 and 5.4.28	- High	- Upgrade versi PHP terbaru
		- Clickjacking: X-Frame-Options header missing	- Medium	- Konfigurasi web server pada X-Frame Option dan header CSP
		- Cookie(s) without Secure flag set	- Medium	- cookie disetting dengan menggunakan Secure Flag Set
		- Login page password-guessing attack	- Medium	- konfigurasi host virtual dan periksa apakah host virtual ini harus dapat diakses publik.
		- Cookie(s) without HttpOnly flag set	- Low	- Mengkonfigurasi session cookie dengan HttpOnly Flag Set.
		- Possible virtual host found	- Medium	- Memisahkan aplikasi dalam server yang berbeda
		- Error page web server version disclosure	- Low	- Konfigurasi web server dengan baik untuk tidak mengungkap informasi sensitif
		- Password type input with auto-complete enabled	- Low	- Mematikan *services autocomplete* pada form input password pada sistem
2	OWASP ZAP	- X-Frame-Options Header Not Set	- Medium	- Mengatur header X-Frame-Options: DENY

		- X-Content-Type-Options Header Missing - Cookie Without SameSite Attribute - Absence of Anti-CSRF Tokens - Cookie No HttpOnly Flag - Cross-Domain JavaScript Source File Inclusion - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) - Information Disclosure - Suspicious Comments - Timestamp Disclosure – Unix	- Low - Low - Low - Low - Low - Low - Low - Low	- Mengatur header X-Content-Type-Option Nosniff - Gunakan atribut SameSite sehingga browser dapat memberitahu kapan dan bagaimana mengaktifkan cookie - Gunakan Anti-CSRF pada form login - Sertakan HttpOnly ke dalam HTTP Header Response, sehingga cookie tidakdapat diakses melalui skrip klien. - Pastikan web server, application server, load balancer dikonfigurasi untuk disembunyikan dari header - Menghapus semua komentar yang mengembalikan informasi - Mengkonfirmasi secara manual bahwa data stampel waktu tidak sensitif dan data tidak dapat dikumpulkan untuk mengungkap pola yang dapat dieksploitasi
	Nikto	- The anti-clickjacking X-Frame-Options header is not present - The X-XSS-Protection header is not defined - The X-Content-Type-Options header is not set - Cookie PHPSESSID created without the httponly flag	- Medium - Low - Low - Low	- Mengaktifkan Header X-Frame-Options - Gunakan X-XSS-Protection: 1; mode=block untuk melindungi website dari serangan XXS. - Tambahkan header X-Content-Type-Options dengan nilai "nosniff". X-Content-Type-Options: nosniff agar terhindar dari serangan sniffing. - Melakukan konfigurasi fungsi PHP pada session cookie flag httponly

Dari hasil pengujian pada Tabel 3. terlihat pengujian *Vulnerability Scanning* pada *website* universitas XYZ dengan menggunakan *tools vulnerability scanning* Acunetix ditemukan 1 *vulnerability risk high*, 4 *vulnerability risk medium*, 3 *vulnerability risk low*, tool OWAPS ZAP ditemukan 1 *vulnerability risk medium*, 8 *vulnerability risk low*, dan *tool* Nikto ditemukan 1 *vulnerability risk medium*, 4 *vulnerability risk low*.

4. Conclusion

Beberapa hal yang dapat disimpulkan dari hasil penelitian ini, antara lain:

1.Ditemukan beberapa celah kerentanan keamanan pada *website* universitas XYZ dengan menggunakan *tools vulnerability assessment* (Acunetix, OWAPS, dan Nikto) diantaranya 1 *risk level high* yaitu *Multiple vulnerabilities fixed in PHP versions* 5.5.12 *and* 5.4.28 , 6 *risk level medium* yaitu *Clickjacking: X-Frame-Options header missing, Cookie(s) without Secure flag set, Login page password-guessing attack, Possible virtual hpost found, X-Frame-Options Header Not Set*, dan *The anti-clickjacking X-Frame-Options* dan 14 *risk level low yaitu Cookie(s) without HttpOnly flag set, Error page web server version disclosure, Password type input with auto-complete enabled, Cookie Without SameSite Attribute, Absence of Anti-CSRF Tokens, Cookie No HttpOnly Flag, Cross-Domain JavaScript Source File Inclusion, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Information Disclosure - Suspicious Comments, Timestamp Disclosure – Unix, The X-XSS-Protection header is not defined, The X-Content-Type-Options header is not set, Cookie PHPSESSID created without the httponly flag, Cookie CRC created without the httponly flag.*

2.Berdasarkan hasil analisa celah kerentanan pada siakad universitas XYZ cukup baik, dengan celah kerentanan *risk level high* 1, *risk level medium* 6 dan *risk level low* 14. Peneliti memberikan rekomendasi perbaikan terkait temuan celah keamanan pada siakad universitas XYZ dari serangan XSS (*Cross Site Scripting*), *Clickjacking, Brute Force, Cross-site Request Forgery* (CSRF) dan *Sniffing.*

Acknowledgements

Alhamdulillah puji syukur kepada Allah swt, karena kehendak dan ridha-Nya peneliti dapat menyelesaikan penelitian ini serta ucapan terima kasih kepada YW Universitas Muslim Indonesia untuk dana penelitian dosen pemula LP2S UMI.

References

[1] Harleni, "SISTEM INFORMASI AKADEMIK (SIAKAD) STIKES PERINTIS PADANG)", Jurnal Teknologi Informasi dan Pendidikan Vol. 11, No. 2, September 2018

[2] Dewi, Laksmiati, "Vulnerability Assessment pada Situs WWW.HATSEHAT.COM Menggunakan OPENVAS", Jurnal AKRAB JUARA Vol 5 No. 3 Agustus 2020

[3] Bita parga, Analisis Security Assessment Menggunakan Metode Penetration Testing Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara, Jurnal Teknologi Penginderaan Vol. 2 No. 1 Tahun 2020

[4] Riadi, Imam "*Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment*", Jurnal Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), Vol. 7, No. 4, Agustus 2020, hlm. 853-860

[5] Kurniawan. Riadi." *Security Level Analysis of Academic Information System Based on Standart Iso27002: 2013 Using Sse-Cmm*.", Internasional Journal of Computer Science and Information Security (IJCSIS) 2017

[6] Yunus, "*Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Projectberdasarkan Framework OWASP VERSI 4*", Jurnal Ilmiah Informatika Komputer Vol. 24, No. 1: April 2019