p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Peningkatan Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Jakarta Melalui Klasifikasi Serangan Cyber Dalam Menunjang WFH

Hendra[1*], Eka Budhy
[1]Teknik Informatika, Universitas Muhammadiyah Jakarta, Jalan Cempaka Putih Tengah 27 Jakarta Pusat 10510
**Corresponding Author*: hendra@umj.ac.id

Abstrak

Sistem Informasi Akademik adalah suatu sistem yang dirancang untuk keperluan pengeloaan data-data akademik dengan penerapan teknologi komputer baik hardware maupun software sehingga seluruh proses kegiatan akademik dapat terkelola menjadi informasi yang bermanfaat dalam pengelolaan manajemen perguruan tinggi dan pengambilan keputusan-keputusan bagi pengambil keputusan atau top manajemen di lingkungan Universitas Muhammadiyah Jakarta. Sistem ini bertujuan untuk mendukung penyelenggaraan pendidikan, sehingga Universitas dapat menyediakan layanan informasi yang lebih baik dan efektif kepada civitas akademika, baik didalam maupun diluar Universitas Muhammadiyah Jakarta melalui internet. Berbagai kebutuhan dalam bidang pendidikan maupun peraturan yang melingkupinya sedemikian tinggi, sehingga pengelolaan akademik dalam suatu lembaga pendidikan menjadi pekerjaan yang sangat menguras waktu, tenaga dan pikiran. Masalah yang sering terjadi pada perguruan tinggi pada umumnya adalah keterbatasan pengolahan data yang dimulai dari pengolahan data akademik. Hal tersebut merupakan salah satu proses interaksi antara bagian internal Universitas Muhammadiyah Jakarta yang mengolah data dengan proses serta prosedur-prosedur tertentu, dengan user yang dalam hal ini adalah mahasiswa. Kesulitan yang sering terjadi pada bagian internal perguruan tinggi adalah banyaknya proses pengolahan data yang harus dilakukan dalam waktu yang singkat.

Kata kunci: keamanan, informasi, siakad, serangan

Abstract

Academic Information System is a system designed for the purposes of managing academic data with the application of computer technology, both hardware and software so that all processes of academic activities can be managed into useful information in the management of higher education and decision making for decision makers or top management. at the Muhammadiyah University, Jakarta. This system aims to support the implementation of education, so that the University can provide better and more effective information services to the academic community, both inside and outside the University of Muhammadiyah Jakarta through the internet. Various needs in the field of education as well as the regulations that surround it are so high, so that academic management in an educational institution becomes a very time-consuming job, energy and thought. The problem that often occurs in universities in general is the limitation of data processing starting from processing academic data. This is one of the processes of interaction between the internal part of the University of Muhammadiyah Jakarta which processes data with certain processes and procedures, with users who in this case are students. The difficulty that often occurs in the internal part of higher education is the large number of data processing processes that must be carried out in a short time.

Keywords : security, information, siakad, attack

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

PENDAHULUAN

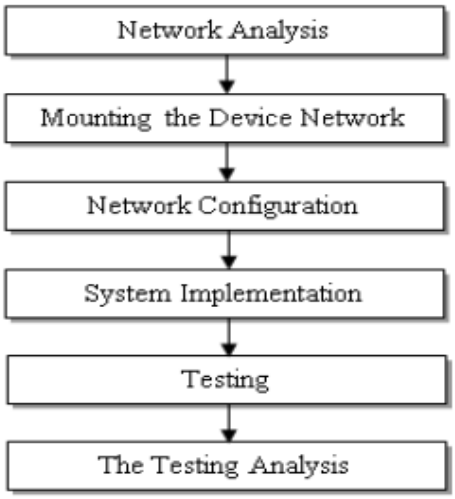
Sistem Informasi Akademik adalah suatu sistem yang dirancang untuk keperluan pengeloaan data-data akademik dengan penerapan teknologi komputer baik hardware maupun software sehingga seluruh proses kegiatan akademik dapat terkelola menjadi informasi yang bermanfaat dalam pengelolaan manajemen perguruan tinggi dan pengambilan keputusan-keputusan bagi pengambil keputusan atau top manajemen di lingkungan Universitas Muhammadiyah Jakarta.

Sistem ini bertujuan untuk mendukung penyelenggaraan pendidikan, sehingga Universitas dapat menyediakan layanan informasi yang lebih baik dan efektif kepada civitas akademika, baik didalam maupun diluar Universitas Muhammadiyah Jakarta melalui internet. Berbagai kebutuhan dalam bidang pendidikan maupun peraturan yang melingkupinya sedemikian tinggi, sehingga pengelolaan akademik dalam suatu lembaga pendidikan menjadi pekerjaan yang sangat menguras waktu, tenaga dan pikiran.

Oleh sebab itu, sistem informasi akademik dibangun untuk menjawab secara langsung masalah maupun kebutuhan Universitas terhadap pengelolaan akademik tersebut secara cepat dan tidak melelahkan. Keamanan sistem komputer merupakan mekanisme dan proses kolektif terhadap informasi sensitif dan berharga dan juga layanan yang dilindungi dari publikasi, gangguan atau kehancuran oleh kegiatan yang tidak sah atau individu yang tidak dapat dipercaya dan kejadian-kejadian yang tidak direncanakan masing-masing.

METODE

Dalam melakukan penelitian *pentest* terhadap *web* yang ber-subdomain siakad.umj.ac.id ini terdapat beberapa tahap dalam pengumpulan data. Tahapan yang dilakukan dalam pengumpulan data ini terdapat beberapa sumber antara lain melalui literatur seperti jurnal, buku, paper ilmiah atau dari media digital seperti internet. Selain dari itu informasi juga didapatkan melalui hasil analisis pada infrastruktur jaringan dan sistem UMJ.



Gambar 1. Diagram alur *penetration testing*

HASIL DAN PEMBAHASAN

Alat Kebutuhan Penelitian

Alat yang digunakan dalam melakukan penelitian ini terdiri dari perangkat keras dan perangkat lunak. Perangkat keras yang digunakan adalah laptop sedangkan perangkat lunak yang digunakan adalah Windows 10 yang terinstall juga Java 8+. Contoh spesifikasi laptop yang digunakan seperti pada Tabel 1.

Tabel 1. Spesifikasi Perangkat Penelitian

NO	KOMPONEN	SPESIFIKASI
1.	Processor	Inter(R) Core(TM) i5-8250U
		Processor (1.60Ghz, Cache 6 MB)
		Max Turbo Frequency 1.89 Ghz
2.	RAM	8
3.	Storage Memori	1 TB
4.	VGA	NVIDIA @Radeon 520 2 GB
5.	Sistem Oeprasi	Windows 10
6.	Penetration Tools	OWASZAP
7.	Modem	LC113E
8.	Kartu Provider	By-U Telkomsel
9.	Paket Data	2 Mbps

Tahapan awal dilakukan identifikasi masalah baik dari informasi yang diperoleh dari berbagai sumber atau dengan pihak yang mengelola jaringan UMJ. Identifikasi masalah juga dilakukan berdasarkan berbagai sumber lain yang antara lain yang serupa dengan penelitian ini dan informasi informasi lain yang mendukung.

Tahapan awal dilakukan identifikasi masalah baik dari informasi yang diperoleh dari berbagai sumber atau dengan pihak yang mengelola jaringan UMJ. Identifikasi masalah juga dilakukan berdasarkan berbagai sumber lain

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

yang antara lain yang serupa dengan penelitian ini dan informasi informasi lain yang mendukung.

Tahap selanjutnya setelah mengidentifikasi masalah adalah dengan melakukan studi literatur yang berhubungan dengan konsep keamanan informasi dan uji *pentest* dan jaringan.

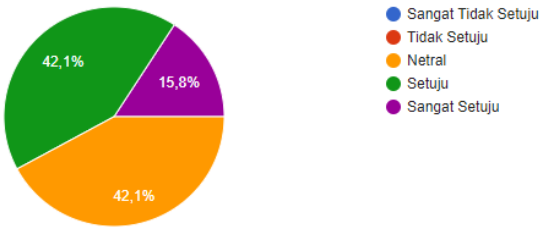
Selanjutnya adalah tahap menentukan metode pengujian. Hasil dari pengujian akan didapatkan data dan *log* yang digunakan untuk analisis guna menemukan hasil akhir serta solusi yang tepat. Terakhir adalah pembuatan laporan akhir yang berisi semua tahapan-tahapan penelitian.

Hasil Pengolahan Kepuasan Pengguaan

Pengolahan pengukuran kepuasan penggunaan Sistem Informasi Akademik menggunakan aplikasi excel dengan menampilakn Pie Chart sebagai gambaran tingkat kepuasan pengguna. Hasil pengolahan memperlihatkan 42,1 % pengguna Setuju, sedangkan 42,1 % Netral dan 15,8 % Sangat Setuju atas kepuasan pelayanan Sistem Informasi Akademik Universitas Muhammadiyah Jakarta.

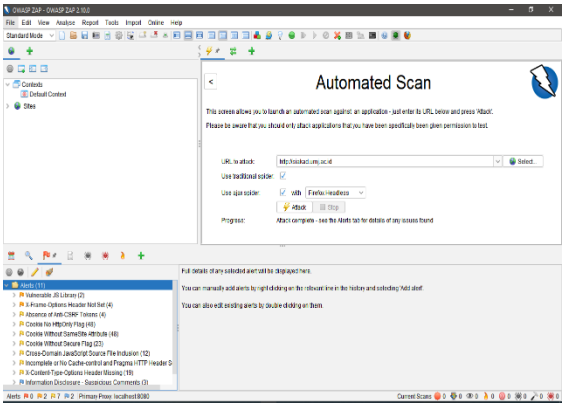
Tabel 2. Kuisioner Kepuasan Penggunaan Siakad UMJ

NO	STATUS	JUMLAH
1	Mahasiswa	5
2	Dosen	5
3	Karyawan	5
Jumlah		15



Gambar 2. Hasil pengolahan kuisioner

Dari proses *scanning* yang telah dilakukan didapat hasil kemungkinan terdapat celah keamanan pada 10 *web* target yang berdomain siakad.umj.ac.id diantara seperti pada Gambar 3.



Gambar 3. Hasil Scannng Website Siakad UMJ menggunakan OWASP-ZAP

Pengujian celah keamanan menggunakan aplikasi ZAP yang dikembangkan oleh OWASP (*Open Web Application Security Project*). Dengan menggunakan *tools* ini, dapat memindai sejumlah keamanan yang rentan terkena serangan *online* di situs web. Selain itu, ZAP juga dapat memperlihatkan hal-hal lainnya, seperti injeksi SQL dan XSS, *private IP disclosure, application error disclosure*, dan lain-lain. Pada penggujian dengan menggunakan Tools tersebut terdapat terlihat 13 (Tiga Belas) celah keamanan.

Pengujian dilakukan mulai antara tanggal 31 Juli sampai dengan 6 Agustus 2021 mulai jam 20.00 sampai dengan 21.00, hal ini dilakukan agar pengujian lebih stabil dan valid serta tidak banyak yang mengakses wesbite tersebut. Akses Internet yang di gunakan dalam penggujian menggunakan Kartu by. U produk dari Telkomsel dengan Bandwith 2 Mbps.

Adapun rincian jenis celah keamanan dapat dilihat pada Tabel 3. berikut di bawah ini.

Tabel 3. Celah keamanan pada Siakad UMJ

No	Jenis Ancaman	Jumlah	Tingkat Ancaman
1.	Vulnerable JS Library	2	Medium
2.	X-Frame-Options Header Not Set	4	Medium
3.	Absence of Anti-CSRF Tokens	4	Low
4.	Cookie NoHttpOnly Flag	40	Low
5.	Cookie Without Secure Flaq	19	Low
6.	Cookie with SameSite Attribute None	19	Low
7.	Cookie with SameSite Attribute	21	Low
8.	Cross-Domain JavaScript Source File Inclusion	12	Low
9.	X-Content-Type-Options Header Missing	17	Low
10.	Information Disclosure – Suspicious Comment	2	Low
11.	Time Stam Dislosure – Unix	9	Low

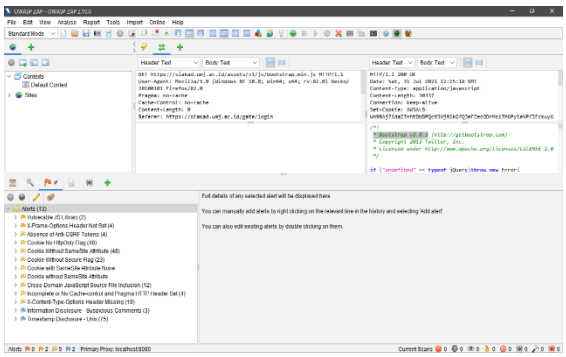
p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Gambar 3. menunjukan hasil *scanning* menggunakan aplikasi otomatisasi OWASP yang menujukan jumlah kemungkinan celah keamanan yang ada pada *web* target menurut level tingkat ancaman di sini terbagi menjadi 11 kategorikan berdasarkan efek yang ditimbulkan dari celah keamanan tersebut yaitu *High*, *Medium*, dan *Low*. Untuk detail ancaman yang terdapat pada tiap target dapat dilihat pada Tabel 4. 2. Selanjutnya hasil dari proses *scanning* menggunakan *tools* WPScan seperti yang ditunjukan pada Gambar 4. 2. Pada Gambar 4. 2 ini menjelaskan jumlah jenis kemungkinan celah keamanan yang terdapat dalam tiap *web*, pada grafik di bawah *web* siakad.umj.ac.id tidak menunjukan hasil dikarena *web* bukan bertipe Wordpress seperti *web* lainya. Untuk melihat detail kemungkinan celah keamanan yang terdapat dalam *web* target dapat dilihat pada Tabel 4. 2 di bawah.

Hasil selanjutnya yang ditemukan dalam proses *scanning web* berdomain siakad.umj.ac.id ini juga ditemukan beberapa *user login* pada beberapa *web* target yang diduga merupakan *user login* dari target. *User login* yang ditemukan pada proses *scanning* diantaranya dapat dilihat pada Tabel 3.

Aplikasi otomatisasi OWASP ZAP

Hasil *report* yang dikeluarkan aplikasi dalam format .html akan berupa tabel. Tabel paling atas berisikan risk level celah keamanan, jumlah celah yang dapat di deteksi dan tabel ke 2 berisikan level risk celah, kategori atau nama celah, lokasi celah berada, method, parameter dan juga yang terakhir solusi untuk menghadapi celah keamanan tersebut seperti yang ditunjukan pada Gambar 4. 3 dan Gambar 4.



Gambar 4. Hasil Pengecekan Spider Progress Siakad UMJ

Uji kemungkinan celah

Pada tahap ini dilakukan pengujian terhadap kemungkinan celah kemanan yang telah ditemukan pada tahap sebelumnya.

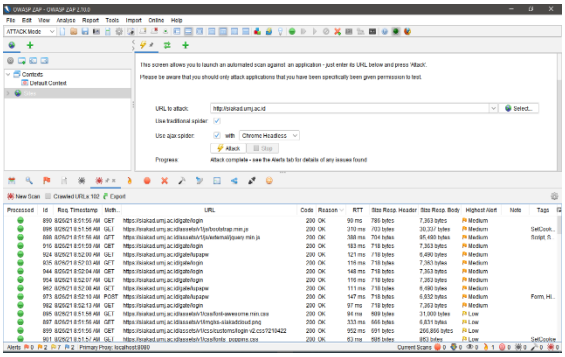
a. Fase Hacking

Fase Hacking identik dengan metoda attack yang digunakan *attacker* untuk melakukan serangan. Mulai dari tahap pencarian informasi hingga penghapusan jejak. Fase Hacking umumnya terkait dengan network scanning yang mencakup dialers, port scanner, network mappers, sweepers, vulnerability scanner.

b. Denial of Service (DoS)

Inti dari DoS adalah melumpuhkan *service* tertentu yang disediakan oleh target. Misalnya web service, email service, dan lain-lain. Sehingga *service* menjadi tidak tersedia. Dampak yang ditimbulkan bisa sangat serius, khususnya jika *service* tersebut terkait dengan hajat hidup orang banyak.

Pada Gambar 5. serangan ditunjukan kepada *web* siakad.umj.ac.id namun dari serangan DoS *website* siakad.umj.ac.id tidak terpengaruhi sama sekali terhadap serangan besar kemungkinan *web* siakad.umj.ac.id sudah menggunakan load balancing.



Gambar 5. Analisis serangan DoS dengan OWASP

c. SQL Injection

Pada proses sebelumnya terdeteksi bahwa beberapa *web* target memiliki kemungkinan celah keaman SQL Injection. Dari proses *scanning* tahap sebelumnya menggunakan tools otomatisasi OWASPZap dan Sucury ditemukan kemungkinan celah keamana serangan SQL Injection pada *web* siakad.umj.ac.id. Dari kemungkinan ini

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

dilakukan pembuktian dengan pengujian secara manual menggunakan browser. Selanjutnya pengujian dilakukan secara manual dengan memasukan query tertentu dalam URL target dan hasilnya seperti ditunjukan pada Gambar 4.8 dimana query yang dimasukan langsung terdeteksi oleh *firewall* yang dimiliki dan langsung dicegah oleh *firewall.*

d. **Cross-Site Scripting (XSS)**

XSS adalah salah satu jenis serangan injeksi code *(code injection attack)*. XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau *client script code* lainnya ke suatu situs. Kemungkinan celah keamanan ini juga ditemukan hampir pada semua *web* target sehingga perlu dilakukan pengujian. Disini penguji melakukan serangan XSS secara manual dengan browser dan memasukan *code injeksi* ke dalam *web* target. Akan tetapi serangan yang dilakukan penguji terdeteksi oleh *firewall* sehingga langsung dicegah oleh *firewall.*

e. **Directory Browsing**

Directory Browsing adalah celah keamanan dimana orang yang tidak memiliki hak akses terhadap suatu *website* dapat mengakses halaman yang berupa informasi informasi sensitif pada suatu *website* tertentu. Pada kasus ini kemungkinan celah keamanan ini terdeteksi pada proses *scanning* dan hampir terdeteksi pada seluruh *web* target sehingga perlu dilakukan pengujiaan lagi dengan mencoba melakukan akses terhadap Directory. Dari Gambar 4.10. didapatkan informasi mengenai file apa saja yang terdapat dalam *web* siakad.umj.ac.id dan informasi tanggal terakhir admin melakukan perubahaan pada file tersebut. Dari proses pengujian ini didapatkan hasil seperti pada Gambar 4.10 grafik yang menunjukan jumlah *Directory Browsing* yang dapat diakses pada setiap *web* target.

f. **Sensitive Data Exposure**

Pada proses *scanning* ditemukan beberapa userlogin pada *web* target sehingga perlu dilakukan pengujian. Pengujian terhadap kemungkinan user login yang ditemukan pada tahap sebelumnya dengan metode *brute force* yang berjenis *dictionary attack.* Serangan dilakukan terhadap halaman form login *web* target disini penulis melakukan pengujian terhadap siakad.umj.ac.id.

Hasil serangan *brute force* menggunakan aplikasi OWASP-ZAP dinyatakan tidak berhasil dikarenakan langsung terjadi notification *server eror* yang kemungkinan besar serangan yang dilakukan langsung dicegah oleh *firewall* yang di miliki oleh *web* target.

Kemungkinan serangan dicegah oleh *firewall* yang dimiliki oleh *web* target dikuatkan dengan yang mencoba melakukan akses menggunakan browser ke halaman login *web* target dan terdapat peringatan.

Selama proses *brute force* dijalankan semua akses ke halaman login *web* taget yang menggunakan *gateway* yang sama tidak dapat dilakukan dan akan otomatis muncul peringatan seperti Gambar 4.14 di atas. Setelah proses *brute force* dihentikan dan menunggu kurang lebih 5 menit halaman login dapat diakses secara normal kembali. Proses ini juga dilakukan terhadap semua kemungkinan userlogin yang ditemukan pada tahap sebelumnya.

SIMPULAN DAN SARAN

Kesimpulan

Hasil dari penelitian ini dapat disimpulkan bahwa analisis kerentanan aplikasi Sistem Informasi Akademik berbasis web dengan teknik OWASP-ZAP mampu mengetahui keamanan suatu aplikasi. Metode OWASP-ZAP dapat dijadikan sebagai standar penilaian keamanan aplikasi berbasis web berdasarkan hasil pengujian kerentanan pada website yang beralamat di siakad.umj.ac.id dari beberapa tahapan kategori yaitu pada tahap Authentication Testing Authorization, Session Management Testing, Input Validation Testing, dan Error Handling.

Saran

Setelah melakukan proses *penetration testing* terhadap *web* yang berdomain siakad.umj.ac.id dan melakukan analisa lebih dalam terhadap hasil uji, maka memiliki beberapa rekomendasi:

1. Melakukan evaluasi untuk analisa log-log dan melakukan monitoring secara berkala pada aplikasi web dan juga sistem.
2. Perlu dilakukan encryption terhadap data yang penting untuk mengurangi resiko terjadinya kebocoran informasi yang sensitif.
3. Programmer perlu mendapatkan pelatihan bagaimana membuat kode-kode yang aman untuk mencegah *cross-site scripting,*

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

misalkan *encoding data* dan *input validation.*

4. Melakuka update secara berkala terhadap sistem yang digunakan untuk mencegah celah keamanan baru yang muncul seperti pada *plugin* yang digunakan.
5. Melakukan konfigurasi kembali pada DNS server agar mengijinkan IP addres yang sudah ditentukan saja yang dapat melaukan permintaan zone transfer.
6. Melakukan disable directori browsing melalui CPanel atau dapat melakukan pemblokiran menggunakan file .htacces.
7. Melakukan *Static application security testing* (SAST) untuk menemukan issue dengan cara menganalisis *dependencies* dan *configuration.*
8. Perlu dilakukan penelitian lebih lanjut dengan metode ISSAF (Information System Security Assessment Framework) agar dapat diketahui kerentanan dari sisi web server.

DAFTAR PUSTAKA

Budi Rahadjo. Keamanan Sistem Informasi. PT Insan Infonesia, 2017.

Guntoro, Loneli Costaner, dan Musfawati. Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan OWASP-ZAP (Studi Kasus Ojs Universitas Lancang Kuning) (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika). JIPI. Volume 05, Nomor 01, Juni 2020 : 45 – 55.

Indra Irawan. Pengembangan Sistem Informasi Akademik Universitas Pahlawan Tuanku Tambusai Riau. Jurnal Teknologi dan Open Source Issn Online: 2622-1659. Vol. 1 No. 2, Desember 2018 Hal. 55-56.

Iwan Sofana & Rifkie Primartha. Network Security dan Cyber Security, Teori dan Praktek Cisco CCNA, Linux, Windows, Amazon AWS, Android. Informatika. 2019.

Jogiyanto.2009.Analisis dan Desain Sistem Informasi.Yogyakarta: Andi.

Joseph Migga Rizza. Computer Network Security. University of Tennessee-Chattanooga. Chattanooga, TN, U. S.A.

Johan Ericka Wahyu Prakasa. Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi. Jurnal Ilmiah Teknologi Informasi Asia. Vol.14, No.2, Tahun 2020. ISSN: 2580-8397 (O); 0852-730X (P).

Ladjamudin, bin Al – Bahra. 2005. Analisis dan Desain Sistem Informasi. Yogyakarta: Graha Ilmu.

Rifkie Primartha. Security Jaringan Komputer Berbasis CEH. Informatika. 2017.