JURNAL LENTERA ICT **ISSN 2338-3143**
Volume 8 Nomor 1, Mei 2023 **E-ISSN 2986-9951**

ANALISIS KEAMANAN APLIKASI WEB OAS POLITEKNIK LP3I JAKARTA MENGGUNAKAN ACUNETIX WEB VULNERABILITY

Oleh:
[1]Hariyanto, [2]Marini

[1]Program Studi Manajemen Informatika, Politeknik LP3I Jakarta
Gedung Sentra Kramat Jalan Kramat Raya No. 7-9 Jakarta Pusat 10450

[2]Program Studi Sistem Informasi, Universitas Budi Luhur
Jalan Raya Ciledug Petukangan Utara Pesanggrahan Jakarta Selatan 12260.

Email :harimeku@gmail.com[1], marini@budiluhur.ac.id [2]

ABSTRAK

Keamanan merupakan hal penting yang tidak boleh dilupakan. Kerentanan biasanya terjadi disebabkan kelalaian pengembang dalam mengembangkan aplikasi itu sendiri. Aplikasi web OAS sepenuhnya lewat media internet, ini merupakan keharusan adanya keamanan. *Serangan SQL Injection*, *Cross Site Scripting* dan masih banyak lainnya menjadi sebab perlunya keamanan pada aplikasi web OAS. Perlunya audit terhadap keamanan aplikasi web OAS ini sangat penting bagi tim pengembang aplikasi. Dari hasil penelitian dengan menggunakan tool acunetix di dapatkan banyaknya kerentanan yang ada di aplikasi web OAS. Dengan ditemukannya kerentanan pada aplikasi web OAS, maka bagi tim pengembang aplikasi dapat secepatnya melakukan perbaikan.

Kata kunci: Analisis Keamanan, Audit, Aplikasi Web, *Acunetix Web Vulnerability*

PENDAHULUAN

Aplikasi web merupakan salah satu target dengan metode serangan *cyber* yang paling umum. Menurut penelitian dari tim positive technologies, 17 persen dari semua serangan melibatkan eksploitasi kerentanan dan kelemahan keamanan aplikasi web.

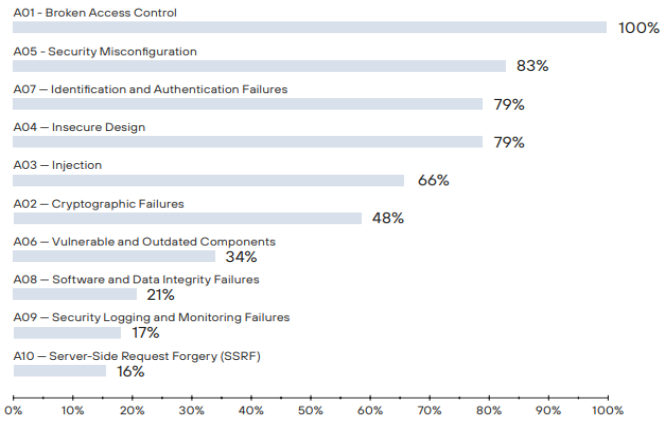
Aplikasi web OAS Politeknik LP3I Jakarta merupakan salah satu aplikasi yang digunakan untuk mengakomodir kebutuhan akan informasi dan data terkait bimbingan mahasiswa tugas akhir, nilai mahasiswa dan semua yang berkaitan dengan akademik di lingkungan Politeknik LP3I Jakarta.

Maksud dibuatkannya aplikasi web OAS ini merupakan salah satu terobosan yang mengedepankan satu pintu untuk semua sistem. Karena selama ini, Politeknik LP3I Jakarta masih menggunakan beberapa aplikasi web lain, sehingga, baik itu mahasiswa, dosen dan karyawan Politeknik LP3I Jakarta, memiliki banyak masalah dalam pemahaman tiap aplikasi.

Dengan tingkat penggunaan aplikasi web ini, dapat memunculkan kerentanan dari teknologi website itu sendiri, dimana serangan para hacker, mencari celah atau kerentanan yang kurang diperhatikan oleh administrator.

OWASP Top 10 2021 Vulnerability (web application) menunjukkan beberapa kerentanan paling umum, seperti yang terlihat pada gambar 1.

ISSN 2338-3143
E-ISSN 2986-9951



Gambar 1. OWASP Top 10 2021 Vulnerability

Keamanan ini bisa dikatakan merupakan bagian dari *cyber security*. Menurut ISO (*International Organization for Standardization*) ISO/IEC 27032 bahwa *cyber security* merupakan preservasi dari kerahasiaan, integritas dan ketersedian informasi di *cyberspace*.

Pentingnya pengamanan dari sebuah sistem merupakan suatu keharusan yang harus dipenuhi oleh setiap organisasi yang menggunakan aplikasi tersebut.

Berdasarkan permasalahan tersebut, perlu adanya penerapan analisis keamanan aplikasi web OAS. Ini akan meminimalisir dari gangguan dan kerentanan yang disebabkan oleh sistem yang dibangun. Adapun tujuan penelitian ini untuk menemukan kerentanan dan menguji aplikasi web OAS sehingga dapat menjadi masukan kepada pemilik aplikasi web agar dapat melakukan perbaikan dan meningkatkan keamanan dari aplikasi web OAS itu sendiri.

TINJAUAN PUSTAKA

Website

Teknologi dimana media penyampaian informasi dapat berupa video dan lagu yang disebut website. Website ini mudah diakses dari manapun asal memiliki koneksi internet. Dalam penggunaannya, pengguna hanya perlu menggunakan perangkat komputer atau smartphone yang terhubung dengan internet.

Pengujian Penetrasi

Pengujian penetrasi merupakan metode pengujian dari kelemahan keamanan sistem, program aplikasi web ataupun jaringan komputer. Dimana hasil pengujian ini bisa menjadi masukan dalam perbaikan kelemahan sistem yang terdeteksi. Ada 3 metode dalam pengujian penetrasi, yaitu *black box testing*, *white box testing* dan *grey box testing*.

1. *Black Box Testing*
   Pada metode ini, *tester* melakukan serangan dengan mengabaikan infrastruktur target. *Tester* mencari semua kerentanan pada keamanan sistem berdasarkan kemampuan serta pengetahuan mereka. Metode ini mengaudit keamanan sistem melalui serangan eksternal untuk menemukan celah kerentanan aplikasi sistem itu sendiri.
2. *White Box Testing*

Pada metode ini, *tester* memiliki semua informasi terkait infrastruktur keamanan yang diberikan dari internal. Serangan ini dimaksudkan sebagai simulasi jika terjadi hal yang berbahaya dan dalam pelaksanaannya hanya dilakukan di lingkungan internal saja.

3. *Gray Box Testing*
   Pada metode ini, merupakan gabungan dari 2 metode sebelumnya dimana *tester* diberikan informasi infrastruktur keamanan sistem tapi *tester* juga harus mencari informasi sendiri dimana *tester* menemukan celah kerentanan sistem.

Acunetix

***Acunetix web vulnerability* merupakan alat layanan aplikasi web pengujian keamanan yang secara otomatis dapat mengaudit aplikasi web dengan mengecek *vulnerability – Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Features, Server – Side Request Forgery*.**

Komponen kunci dari hasil scanning yaitu daftar vulnerability yang ditemukan pada target selama berlangsungnya scanning. Daftar scanning biasanya berupa web alerts atau network alerts dimana mereka dikategorikan menjadi 4 tingkat severity :

High Risk Alert Level 3 – Kerentanan ini paling bahaya, dimana target memiliki resiko maksimum dalam peretaasan dan pencurian data.

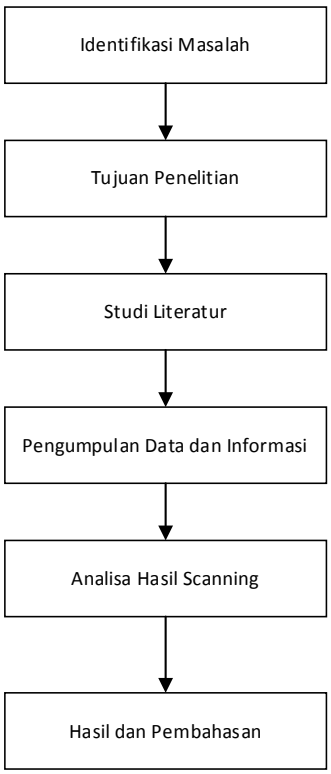
Medium Risk Alert Level 2 – Kerentanan ini disebabkan oleh kesalahan konfigurasi server dan kelemahan pengkodean situs, dimana ini memberikan fasilitas kepada peretas untuk melakukan gangguan dan intrusi server.

Low Risk Alert Level 1 – Kerentanan ini berasal dari kurangnya enkripsi data traffic atau terbukanya jalur direktori / path.

Information Alert – Kerentanan ini merupakan pengungkapan alamat IP internal atau alamat email, pencocokan pencarian yang dapat ditemukan di Google Hacking Database.

METODE PENELITIAN

Untuk mempermudah serta membantu dalam penelitian, peneliti menyusun kerangka kerja yang merupakan tahapan kegaitan yang dilakukan selama penelitian, yang dapat dilihat pada gambar 2.



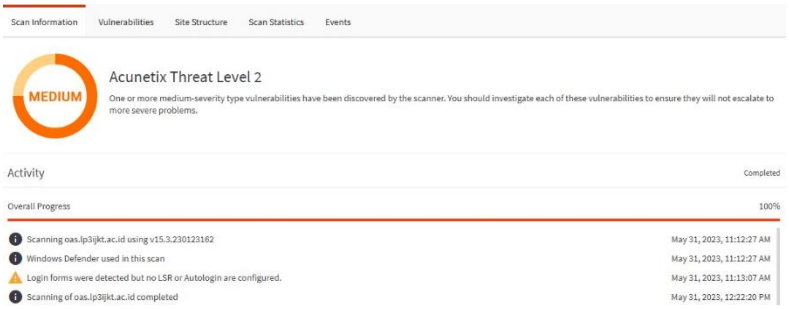
Gambar 2. Kerangka Kerja Penelitian

1. **Identifikasi Masalah**, merupakan penemuan masalah yang harus dikerjakan sebelum aplikasi web OAS itu di release yaitu vulnerability assesment yang merupakan bagian dari pengujian. Metode yang akan digunakan mengacu pada metode *Black Box Testing*.
2. **Tujuan Penelitian,** menemukan *vulnerability* dari aplikasi web OAS yang dapat dijadikan sasaran oleh penyerang. Dapat memberikan penjelasan kepada administrator agar dapat melakukan perbaikan dari *vulnerability* yang ada.
3. **Studi Literatur,** dengan mempelajari literatur yang berkaitan dengan *cyber security*, *vulnerability* yang dapat menunjang dari penelitian ini. Sumber literatur berasal dari artikel, jurnal ilmiah maupun referensi yang berhubungan dengan penelitian.
4. **Pengumpulan Data dan Informasi,** kegiatan dari scanning aplikasi web OAS dengan menggunakan tools *Acunetix web vulnerability scanner*. Data dan informasi yang di dapat di klasifikasikan agar mudah untuk di analisa.
5. **Analisa Hasil Scanning,** tahap ini merupakan penganalisaan dari data dan informasi yang sudah di dapat. Dimana analisa yang dijelaskan meliputi jenis celah keamanan, sumber celah, solusi perbaikan dari celah keamanan tersebut
6. **Hasil dan Pembahasan,** penjelasan secara komprehensif terhadap semua kegiatan yang sudah dilakukan sebelumnya.

ISSN 2338-3143
E-ISSN 2986-9951

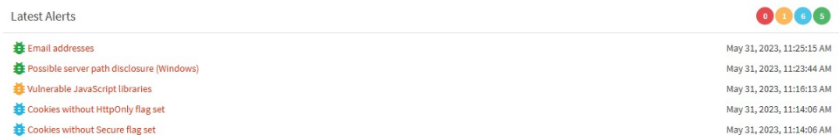
HASIL DAN PEMBAHASAN

Berdasarkan hasil scanning Acunetix web vulnerability di dapatkan beberapa permasalahan dengan keamanan aplikasi web OAS, diantaranya :



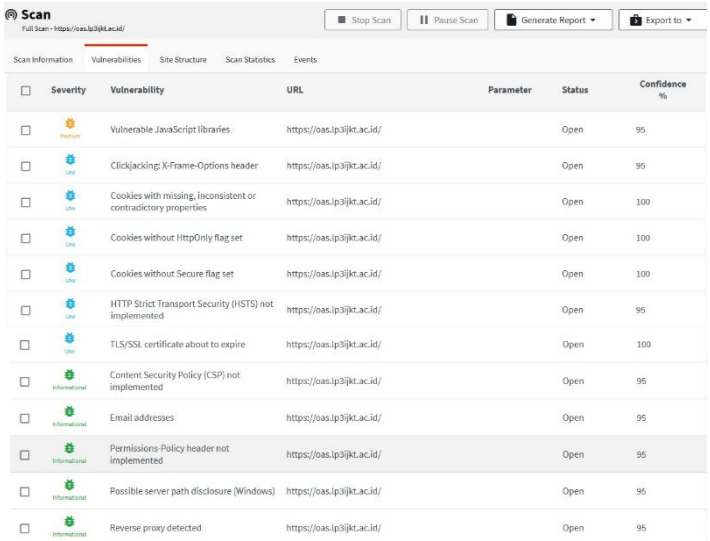
Gambar 3. Scan Information Acunetix

Pada gambar 3 di dapatkan bahwa aplikasi web OAS ini masuk ke dalam *Threat Level* 2, dimana pada level ini kerentanan dapat disebabkan oleh *server misconfiguration* dan *sitecoding* yang lemah, ini merupakan bagian dari gangguan dan intrusi server.



Gambar 4. Scan Information Alert Acunetix

Pada gambar 4 menunjukkan peringatan yang diberikan Acunetix di beberapa bagian yang merupakan krusial di dalam aplikasi web OAS. Diantaranya seperti *Email address*, *Possible server path disclosure (Windows)*, *Vulnerable JavaScript libraries*, *Cookies without HttpOnly flag set* dan *Cookies without Secure flag set*.



Gambar 5. Vulnerabilites Acunetix

Yang menjadi perhatian utama pada gambar 5 adalah *Vulnerable JavaScript libraries* karena dari tingkat keparahan keamanan ini menduduki tingkat ke 2.

ISSN 2338-3143
E-ISSN 2986-9951

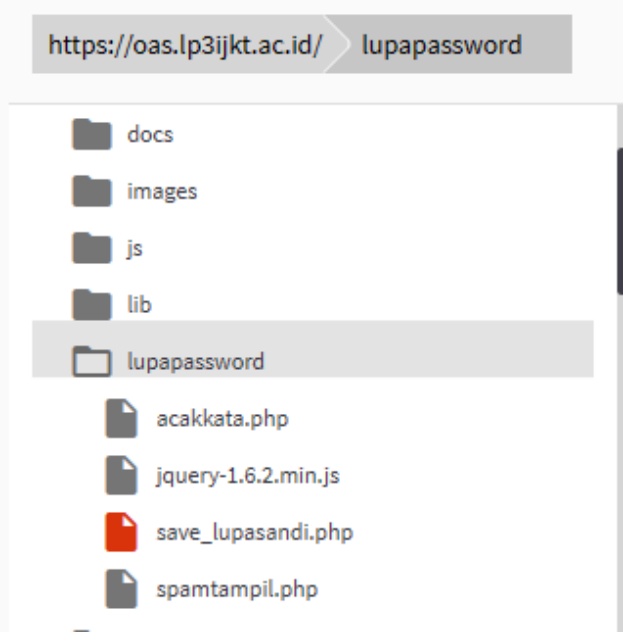
Dimana terlihat bahwa semuanya berstatus open, sehingga ini bisa jadi kemungkinan peretasan.

Untuk menangani kerentanan dari *Vulnerable JavaScript libraries* ini dapat dilakukan dengan mengupdate *library* JavaScript yang terbaru, sehingga di dapatkan hasil keamanan yang maksimal.

Baik itu Clickjacking: X-Frame-Options header, Cookies with missing, inconsistent or contradictory properties, Cookies without HttpOnly flag set, Cookies without Secure flag set, HTTP Strict Transport Security (HSTS) not implemented, TLS / SSL certificate about to expire semua masuk pada low risk level 1.

Pada level 1 ini, kerentanan diperoleh dari banyaknya data yang tidak terenkripsi serta terbukanya jalur / *path* direktori yang ada. Untuk menanganinya diperlukan sebuah enkripsi terhadap *path*, *file* dan perlu adanya SSL certificate.

Jika dilihat pada *site structure* aplikasi web OAS ini, peneliti melihat ada kefatalan yang disebabkan oleh script aplikasi web OAS ini, yaitu pada direktori lupapassword > save_lupasandi.php, seperti yang terlihat pada gambar 6.



Gambar 6. Site Structure Aplikasi Web OAS

Kerentanan ini masuk pada *Clickjacking: X-Frame-Options header*, dimana path tersebut tidak memiliki keamanan XFO header. Untuk menanganinya diperlukan konfigurasi web server dengan menyertakan *header X-Frame-Options* dan *header CSP* yang *directive* ke *frame-ancestors*.

PENUTUP

Kesimpulan dan Saran

Berdasarkan banyaknya temuan kerentanan / celah keamanan dari aplikasi web OAS ini, sudah sepantasnya pihak yang berkepentingan memberikan perhatian khusus jika nantinya aplikasi web OAS ini akan mengakomodir seluruh kegiatan administrasi Politeknik LP3I Jakarta. Perlunya penguatan keamanan aplikasi menjadi suatu keharusan dan ini merupakan pekerjaan rumah yang sangat komplek.

Saran yang dapat diberikan untuk pengembangan aplikasi web OAS ini diperlukannya sebuah SSL yang baik serta pengkodean situs yang lebih aman lagi.

DAFTAR PUSTAKA

Acunetix. (2023). Reviewing Scan Results. Diakses pada 1 Mei 2023, dari https://www.acunetix.com/support/docs/wvs/analyzing-scan-results/

Budi dkk. (2021). *Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan di Era Society 5.0. Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia Volume 3*, hlm. 223-234.

Fachri, F dkk. (2021). *Analisis Keamanan Webserver Menggunakan Penetration Test. JURNAL INFORMATIKA, Vol. 8 No.2*, Halaman 183-190. ISSN : 2355 – 6579.

Fajar., A., F. (2020*). Analisis Keamanan Aplikasi Web Prodi Teknik Informatika UIKA Menggunakan Acunetix Web Vulnerability, Jurnal INOVA-TIF Vol: 3 No.2*.

Fatkhurozzi, M (2021). *Analisa Keamanan Website Menggunakan Metode Footprinting dan Vulnerability Scanning pada Website Kampus, Seminar Nasional Informatika Bela Negara (SANTIKA) Volume 2*. ISSN : 2747 – 0563.

Positive Technologies. (2023). *Threats and vulnerabilities in web applications 2020 – 2021*. Diakses pada 1 Mei 2023, dari https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020-2021/

Prasetyo, E.S & Hassanah, N (2021). *Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF. Jurnal Ilmiah Informatika (JIF) Vol.09 No. 2*. ISSN : 2337 – 8379.

Riadi dkk. (2020). *Analisis Keamanan Webiste Open Journal System Menggunakan Metode Vulnerability Assessment, Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) Vol.7 No.4*, hlm. 853 – 860. ISSN : 2355 – 7699.

Zirwan., A. (2022). *Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner, Jurnal Informasi dan Teknologi Vol.4 No.1*, Hal : 70-75. e-ISSN: 2714 – 9730.