E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55

ANALISIS KEAMANAN *WEB SERVER OPEN JOURNAL SYSTEM* (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING)

Guntoro[1)], Loneli Costaner[2)], dan Musfawati[3)]
[1, 2)] Teknik Informatika, Fakultas Ilmu Komputer, Universitas Lancang Kuning
[3)] Sistem Informasi, Fakultas Ilmu Komputer, Universitas Lancang Kuning
Jalan Yos Sudarso No.KM. 8, Rumbai, Pekanbaru, Riau
e-mail: guntoro@unilak.ac.id[1)], lonelicostaner@gmail.com[2)], musfawati16@yahoo.com [3)]

ABSTRAK

Perkembangan teknologi informasi yang begitu pesat memberikan dampak positif dalam berbagai bidang, salah satunya adalah teknologi internet. Website menjadi alternatif bagi institusi dalam mempromosikan kepada masyarakat umum. Website juga mudah diakses oleh banyak orang, yang tidak kenal tempat maupun waktu. Dengan adanya kemudahan tersebut, banyak instansi membangun web server tanpa memperhatikan apakah web server yang dibangun sesuai dengan standar keamanan atau tidak, apakah sistem yang dibangun sudah aman atau ada gangguan. Universitas Lancang Kuning mempunyai web server yang berisi banyak sistem informasi dan dokumen yang dipublikasi bagi pengguna. Salah satu sistem yang paling krusial adalah sistem Open Journal System (OJS). Menurut informasi dari PDPT Universitas Lancang Kuning, bahwa sistem Open Journal System (OJS) sudah dua kali terjadi cracking. Kerusakan terhadap OJS ini mengakibatkan data yang terdapat pada sistem OJS hilang, bahkan author sering komlain kepada pengelola jurnal. Pengujian terhadap web server sangatlah penting dilakukan, pengujian ini bertujuan untuk menguji apakah web server sudah aman atau belum dari tindak kejahatan para hacker. Dalam pengujian penetrasi ada beberapa metode yang sering dipakai seperti Information Systems Security Assessment Framework (ISSAF), OWASP. Pada penelitian ini digunakan metode ISSAF dan OWASP versi 4. Metode penelitian yang digunakan pada penelitian ini diantaranya adalah studi literatur, pengumpulan data, pengujian penetrasi menggunakan metode ISSAF dan OWASP, dan analisa dan laporan. Adapun tujuan penelitian ini adalah bagaimana menganalisis keamanan sistem Open Journal System (OJS) menggunakan metode ISSAF dan OWASP pada Universitas Lancang Kuning. Berdasarkan pengujian yang telah dilakukan menggunakan metode ISSAF dan OWASP, sistem OJS Universitas Lancang tergolong aman, karena tidak mampu untuk ditembus. Walaupun OJS Universitas Lancang Kuning tergolong aman, serangan bisa saja terjadi dari dalam institusi.

***Kata Kunci**: Keamanan Sistem, Open Journal System, ISSAF, OWASP*

ABSTRACT

The rapid development of information technology has had a positive impact in various fields, one of which is internet technology. Website is an alternative to the general public for companies to support. A lot of people, who don't know the place or time, can easily access the website. With the ease, many agencies are building a web server regardless of whether the web server is designed according to security standards or not, whether the built infrastructure is secure, or intrusion. Universitas Lancang Kuning has a web server which contains many user-published information systems and documents. Open Journal System (OJS) is among the most crucial systems. The Open Journal System (OJS) system was cracked twice according to information from PDPT Universitas Lancang Kuning. Damage to this OJS results in loss of the data contained in the OJS system and even the author often complains to the organizers of journals. Testing the web server is very relevant, this check aims at checking whether or not the web server is secure from hacker activity. There are several methods that are often used in penetration testing such as the Framework for Security Assessment of Information Systems (ISSAF), OWASP. This work utilizes version 4 of ISSAF and OWASP. The research methods used in this research include literature review, data collection, ISSAF- and OWASP-based penetration testing, and analysis and reports. This study aims to examine the security of the Open Journal Framework (OJS) using the Universitas Lancang Kuning ISSAF and OWASP methods. The Universitas Lancang Kuning OJS program, based on tests performed using ISSAF and OWASP methods, is considered secure because it can not be penetrated. While Universitas Lancang Kuning of OJS is relatively secure, attacks can occur from inside the institution.

***Keywords**: System Security, Open Journal System, ISSAF, OWASP*

I. PENDAHULUAN

Pesatnya perkembangan TI memiliki dampak positif di berbagai bidang, salah satunya adalah bidang teknologi web. Website menjadi alternatif bagi institusi dalam mempromosikan kepada masyarakat umum. Website juga mudah diakses oleh banyak orang, yang tidak kenal tempat maupun waktu [1]. Dengan adanya kemudahan tersebut, banyak instansi membangun web server tanpa memperhatikan apakah web server yang

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55

dibangun sesuai dengan standar keamanan atau tidak, apakah sistem yang dibangun sudah aman atau ada gangguan.

Universitas Lancang Kuning mempunyai web server yang berisi banyak sistem informasi dan dokumen yang dipublikasi bagi pengguna. Salah satu sistem yang paling krusial adalah sistem Open Journal System (OJS). Menurut informasi dari PDPT Universitas Lancang Kuning, bahwa sistem Open Journal System (OJS) sudah dua kali terjadi cracking. Kerusakan terhadap OJS ini mengakibatkan data yang terdapat pada sistem OJS hilang, bahkan author sering komlain kepada pengelola jurnal. Pengujian terhadap web server sangatlah penting dilakukan, pengujian ini bertujuan untuk menguji apakah web server sudah aman atau belum dari tindak kejahatan para hacker. Pada pengujian penetrasi ada beberapa metode yaitu metode Informastion Systems Security Assessment Framework (ISSAF), Open Web Application Security Project (OWASP) dan Open Source Security Testing Methodology Manual (OSSTMM). Pada penelitian ini digunakan dua metode yaitu metode ISSAF dan OWASP.

Menurut [1] dalam penelitiannya melakukan pengujian keamanan pada sebuah situs web perusahaan. Adapun pengujian ini menggunakan metode OWASP versi 4 dengan modul Testing for Information Gathering. Berdasarkan pengujian yang dilakukan sistem web memiliki kerentanan terkait dengan GET, POST maupun sistematika URL. Menurut [2] dalam penelitian Analisis Deteksi Vulnerability Pada Webserver Open Journal System Menggunakan OWASP Scanner, hasil pengujian penelitian ini adalah untuk mencari vulnerability pada webserver Open Jurnal Sistem (OJS). Penelitian bertujuan untuk mengamankan dari serangan SQL Injection maupun Cross Site Scripting XSS dengan menggunakan tool OWASP. Menurut [3] dalam penelitiannya Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp untu Penilaian Risk Rating, hasil dari penelitian ini adalah membantu bagi para pengelola dan pengembang sistem untuk menyadari terhadap tindakan kejahatan pada website. Penelitian ini menghasilkan 2 faktor untuk memperkirakan Likelihood dan Impact dengan 3 faktor resiko yaitu risk severity High, risk severity Medium dan risk severity Low. Berdasarkan permasalahan diatas maka, bahwa penelitian ini bertujuan bagaimana menganalisis keamanan sistem Open Journal System (OJS) menggunakan metode ISSAF dan OWASP pada Universitas Lancang Kuning

II. LANDASAN TEORI

A. *Website*

Website adalah serangkaian halaman data berbasis web yang dapat diakses orang lain di seluruh dunia tanpa harus dibatasi oleh lokasi dan waktu [3]. *Website* ini terdiri dari teks, gambar, audio, video, animasi dan menjadi media untuk membaca atau mengunjungi informasi. [4].

B. Open Journal System (OJS)

Open Journal System (OJS) adalah jurnal online dan sistem manajemen penerbitan artikel [5]. *Open Journal System* (OJS) adalah perangkat lunak sumber terbuka yang tersedia secara bebas untuk jurnal di seluruh dunia. OJS menjadi salah satu pilihan yang tepat untuk pengelolaan jurnal, sehingga dapat meningkatkan publikasi bagi institusi pendidikan, serta dapat meningkatkan pembaca sebuah jurnal. OJS bersifat GNU *Public Licence* yang berarti seluruh salinan bebas digunakan oleh orang lain dengan tetap mempertahankan lisensi yang sama [2].

C. Keamanan Informasi

Hal yang menjadi masalah utama dari keamanan sistem informasi disimpulkan pada 2 hal yaitu [6]:

a. *Threats*

Ancaman datang dari tiga masalah utama, yaitu bahaya alam (gempa bumi, banjir, tanah longsor, kebakaran), manusia (perusak, peretas, virus, dan lingkungan) (polusi, efek kimia, pengurangan tegangan listrik) [1].

b. *Vulnerability*

CIA atau yang biasa dikenal dengan Confidentiality (kerahasiaan), Integrity (intergritas) dan Aviability (ketersediaan) merupakan salah satu parameter yang sering digunakan dalam menganalisis celah keamanan dan menjadi acuan dalam keamanan sebuah website. Parameter tersebut digunakan sebagai standar dan acuan dalam menilai baik atau buruknya sebuah keamanan pada suatu jaringan [7].

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55

D. Open Web Application Security Project (OWASP)

Open Web Application Security Project (OWASP) adalah sebuah framework yang bersifat open source yang berfokus dalam memperbaiki keamanan *software* aplikasi [8]. OWASP merupakan organisasi yang dibangun untuk menemukan celah keamanan dari sebuah aplikasi website [9].

Berdasarkan standar yang dikeluarkan oleh OWASP terdapat sebelas langkah yang dapat dilakukan untuk menilai dan menguji keamanan pada sebuah website, berupa: *Information Gathering*, *Configuration Management*, *Secure Transmission*, *Authentication*, *Session Management*, *Authorization*, *Cryptography*, *Data Validation*, *Denial of Service*, *Error Handling.* Pada tabel 1 adalah perbandingan antara OWASP versi 10 tahun 2013 dan OWASP 10 2017.

TABEL 1
PERBANDINGAN OWASP TOP 10-2013 DENGAN OWASP TOP 10-2017

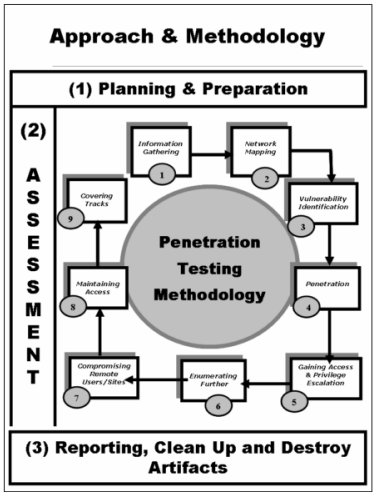
OWASP TOP 10 – 2013	**OWASP TOP 10 – 2017**
A1 – Injeksi	A1 – Injeksi
A2 – Otentikasi dan manajemen sesi yang buruk	A2 – Otentikasi yang buruk
A3 – Cross-Site Scripting (XSS)	A3 – Data sensitif yang terekspos
A4 – Referensi obyek langsung yang tidak aman	A4 – XML External Entities (XXE)
A5 – Kesalahan konfigurasi keamanan	A5 – Akses kontrol yang buruk
A6 – Data sensitif yang terekspos	A6 – Kesalahan konfigurasi keamanan
A7 – Kehilangan fungsi kontrol tingkatan akses	A7 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Deserialisasi yang tidak aman
A9 – Menggunakan komponen rentan yang diketahui	A9 – Menggunakan komponen rentan yang diketahui
A10 – Redireksi dan Forward yang tidak tervalidasi	A10 – Pencatatan dan pemantauan yang tidak cukup

E. OWASP ZAP

OWASP ZAP (*Zed Attack Proxy*) merupakan sebuah aplikasi yang digunakan untuk *penetration testing* dalam menemukan vulnerabilities/celah keamanan pada suatu aplikasi website. ZAP menyediakan scanner secara automatis [10].

F. Information System Security Assessment Framework (ISSAF)

Information System Security Assessment Framework (ISSAF) merupakan sebuah metodologi yang digunakan untuk mengevaluasi sebuah jaringan, sistem dan aplikasi [11]. Framework ISSAF terdiri dari 3 fase pendekatan dan sembilan langkah penilaian. Adapun arsitektur framework ISSAF terlihat pada gambar 1.



Gambar 1 Metodologi ISSAF [11]

1. Fase-I: *Planning and Preparation*

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55

Ini adalah tahap di mana pemeriksa yang melakukan penetrasi dan pihak-pihak yang ditembus diperkenalkan dan diadaptasi. Fase ini mempunyai beberapa langkah yaitu bertukar informasi, merencanakan dan mempersiapkan pengujian. Sebelum menguji, perjanjian penilaian formal harus ditandatangi oleh kedua belah pihak. Dengan perjanjian tersebut akan memberikan perlindungan hukum bagi kedua belah pihak. Dalam tahapan ini juga melibatkan tim dalam pengujian, perencanaan waktu, tanggal serta ketentuan lainnya [11].

2. Fase-II: *Assessment*.
   Fase ini merupakan fase pelaksanaan uji penetrasi. Adapun tahapan disetiap layer pada fase ini adalah *Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access & Privilege Escalation, Enumerating Further, Compromise Remote Users/Sites, Maintaning Access and Covering Tracks* [11].

3. Fase-III: *Reporting, Clean Up and Destroy Artefats*.
   Fase ini merupakan tahapan akhir dari pengujian. Pengujian ini adalah membuat laporan hasil pengujian penetrasi. Setelah penetrasi dilakukan, maka log harus segera dihapus, karena dapat membahayakan sistem, yang nanti bisa dimanfaatkan oleh orang lain [11].

G. *Penetration Testing*

Penetration Testing adalah metode yang digunakan untuk menguji kelemahan sistem komputer, jaringan atau aplikasi web. Tiga strategi pengujian vulnerability assessment berdasarkan lingkup dan jenis audit . Tiga strategi tersebut adalah sebagai berikut [6]:

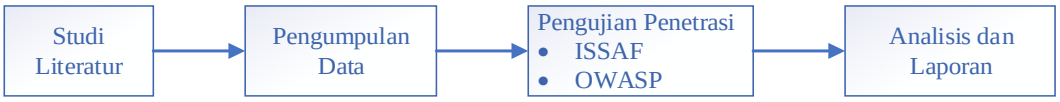
1. *Black Box Testing*
   Pada pendekatan ini penguji tidak memiliki pengetahuan tentang target yang akan diuji. Penguji hanya mencari tahu semua celah keamanan sistem berdasarkan dengan pengalaman maupun keahlian [12]. Tujuan penguji pada dasarnya bertujuan untuk mengaudit keamanan dari eksternal dengan cara mensimulasikan sebagai attacker.

2. *White Box Testing*
   Pada pendekatan ini, seorang penguji diberikan semua informasi secara lengkap seperti konfigurasi jaringan, konfigurasi sistem dan penguji melakukan audit terhadap sistem keamanan dari internal. Penguji mensimulasikan tindakan tersebut seperti bahaya karyawan yang hadir dalam batas target maupun kebijakan. Pengujian ini memerlukan keahlian yang mendalam agar mendapatkan hasil yang lebih baik [13].

3. *Gray Box Testing*
   Pada pendekatan ini adalah menggabungkan antara dua pendekatan *Black Box Testing* dengan White Box Testing. Pada pendekatan ini, seorang penguji harus memiliki pengetahuan tentang pengujian sebuah jaringan atau sistem [14].

III. METODE PENELITIAN

Adapun tahapan penelitian ini diantaranya adalah studi literatur, pengumpulan data, pengujian penetrasi menggunakan ISSAF dan OWASP dan serta analisis dan laporan. Adapun Metode penelitian yang dilakukan adalah seperti terlihat pada Gambar 1.



Gambar 2 Metode Penelitian

A. Studi Literatur

Pada tahapan ini akan dilakukan studi literatur. Studi literatur bertujuan untuk menjelaskan kajian pustaka berdasarkan teori-teori penunjang yang digunakan sebagai bahan penelitian. Adapun studi literatur ini didapatkan dari membaca buku, jurnal, artikel maupun dari internet [15].

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55

B. Pengumpulan Data

Pada tahapan ini dilakukan pengumpulan data dengan cara mengumpulkan data target yang akan dilakukan pengujian dengan menggunakan alat yang sudah disiapkan. Adapun pengumpulan data dilakukan dengan mengidentifikasi web server OJS Universitas Lancang Kuning dengan menggunakan aplikasi OWASP ZAP. Adapun alat kebutuhan yang digunakan untuk pengumpulan data adalah:

a. Analisa kebutuhan sistem

Adapun analisis kebutuhan sistem meliputi:

a) Perangkat Keras

Untuk pengumpulan data dibutuhkan perangkat keras, berikut perangkat keras yang digunakan:

- Laptop Lenovo T430 Processor i5
- Ram 8 GB
- Hardisk 160 SSD
- Modem eksternal

b) Perangkat Lunak

Untuk memenuhi kebutuhan perangkat lunak pendukung dalam pembuatan aplikasi rancang bangun portal seminar nasional berbasis web ini, yaitu:

- Sistem Operasi Windows 10
- OWASP ZAP

C. Pengujian Penetrasi dengan ISSAF dan OWASP

Pada tahapan ini akan dilakukan pengujian terhadap data yang telah ditemukan dengan menggunakan metode ISSAF dan OWASP versi 4 serta metode black-box. Adapun tahapan pengujian dengan metode ISSAF seperti terlihat pada tabel 2.

TABEL 2
FRAMEWORK ISSAF

Tahapan	Source	Tools
Information Gathering	Domain Info	Whois, SSL Scan OK
	SSL (Secure Socket Layer)	SSL Scan
Network Mapping	Network Info	Zen Map
Vulnerability Identification	Web Scanner Vulnerability	Acunetix
Penetration	DoS Attack	Low Orbit Ion Canon
	SQL Injection	SQLmap

Tabel 2 adalah framework metode ISSAF yang digunakan dalam pengujian sistem OJS di Universitas Lancang Kuning. Adapun tahapan yang dilakukan diantaranya *Information Gathering, Network Mapping, Vulnerability Identificattion* dan *Penetration.*

TABEL 3
STANDAR KONTROL OWASP VERSI 4 (MEUCCI, N.D.)

ID Kontrol	Standar Kontrol
Information Gathering	
OTG-INFO-001	*Conduct Search Engine Discovery and Reconnaissance for Information Leakage*
OTG-INFO-002	*Fingerprint Web Server*
OTG-INFO-003	*Review Webserver Metafiles for Information Leakage*
OTG-INFO-004	*Enumerate Applications on Webserver*
OTG-INFO-005	*Review Webpage Comments and Metadata for Information Leakage*
OTG-INFO-006	*Identify application entry points*
OTG-INFO-007	*Map execution paths through application*
OTG-INFO-008	*Fingerprint Web Application Framework*
OTG-INFO-009	*Fingerprint Web Application*
OTG-INFO-010	*Map Application Architecture*
Configuration and Deploy Management Testing	
OTG-CONFIG-001	*Test Network/Infrastructure Configuration*
OTG-CONFIG-002	*Test Application Platform Configuration*
OTG-CONFIG-003	*Test File Extensions Handling for Sensitive Information*
OTG-CONFIG-004	*Backup and Unreferenced Files for Sensitive Information*
OTG-CONFIG-005	*Enumerate Infrastructure and Application Admin Interfaces*
OTG-CONFIG-006	*Test HTTP Methods*
OTG-CONFIG-007	*Test HTTP Strict Transport Security*
OTG-CONFIG-008	*Test RIA cross domain policy*
Identity Management Testing	
OTG-IDENT-001	*Test Role Definitions*
OTG-IDENT-002	*Test User Registration Process*
OTG-IDENT-003	*Test Account Provisioning Process*

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55

ID Kontrol	Standar Kontrol
OTG-IDENT-004	*Testing for Account Enumeration and Guessable User Account*
OTG-IDENT-005	*Testing for Weak or unenforced username policy*
OTG-IDENT-006	*Test Permissions of Guest/Training Accounts*
OTG-IDENT-007	*Test Account Suspension/Resumption Process*
Authentication Testing	
OTG-AUTHN-001	*Testing for Credentials Transported over an Encrypted Channel*
OTG-AUTHN-002	*Testing for default credentials*
OTG-AUTHN-003	*Testing for Weak lock out mechanism*
OTG-AUTHN-004	*Testing for bypassing authentication schema*
OTG-AUTHN-005	*Test remember password functionality*
OTG-AUTHN-006	*Testing for Browser cache weakness*
OTG-AUTHN-007	*Testing for Weak password policy*
OTG-AUTHN-008	*Testing for Weak security question/answer*
OTG-AUTHN-009	*Testing for weak password change or reset functionalities*
OTG-AUTHN-010	*Testing for Weaker authentication in alternative channel*
Authorization Testing	
OTG-AUTHZ-001	*Testing Directory traversal/file include*
OTG-AUTHZ-002	*Testing for bypassing authorization schema*
OTG-AUTHZ-003	*Testing for Privilege Escalation*
OTG-AUTHZ-004	*Testing for Insecure Direct Object References*
Session Management Testing	
OTG-SESS-001	*Testing for Bypassing Session Management Schema*
OTG-SESS-002	*Testing for Cookies attributes*
OTG-SESS-003	*Testing for Session Fixation*
OTG-SESS-004	*Testing for Exposed Session Variables*
OTG-SESS-005	*Testing for Cross Site Request Forgery*
OTG-SESS-006	*Testing for logout functionality*
OTG-SESS-007	*Test Session Timeout*
OTG-SESS-008	*Testing for Session puzzling*
Input Validation Testing	
OTG-INPVAL-001	*Testing for Reflected Cross Site Scripting*
OTG-INPVAL-002	*Testing for Stored Cross Site Scripting*
OTG-INPVAL-003	*Testing for HTTP Verb Tampering*
OTG-INPVAL-004	*Testing for HTTP Parameter pollution*
OTG-INPVAL-006	*Testing for SQL Injection*
	Oracle Testing
	SQL Server Testing
	Testing PostgreSQL
	MS Access Testing
OTG-INPVAL-007	*Testing for LDAP Injection*
OTG-INPVAL-008	*Testing for ORM Injection*
OTG-INPVAL-009	*Testing for XML Injection*
OTG-INPVAL-010	*Testing for SSI Injection*
OTG-INPVAL-011	*Testing for XPath Injection*
OTG-INPVAL-012	*IMAP/SMTP Injection*
OTG-INPVAL-013	*Testing for Code Injection*
	Testing for Local File Inclusion
	Testing for Remote File Inclusion
OTG-INPVAL-014	*Testing for Command Injection*
OTG-INPVAL-015	*Testing for Buffer overflow*
	Testing for Heap overflow
	Testing for Stack overflow
	Testing for Format string
OTG-INPVAL-016	*Testing for incubated vulnerabilities*
OTG-INPVAL-017	*Testing for HTTP Splitting/Smuggling*
Error Handling	
OTG-ERR-001	*Analysis of Error Codes*
OTG-ERR-002	*Analysis of Stack Traces*
Cryptography	
OTG-CRYPST-001	*Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection*
OTG-CRYPST-002	*Testing for Padding Oracle*
OTG-CRYPST-003	*Testing for Sensitive information sent via unencrypted channels*
Business Logic Testing	
OTG-BUSLOGIC-001	*Test Business Logic Data Validation*
OTG-BUSLOGIC-002	*Test Ability to Forge Requests*
OTG-BUSLOGIC-003	*Test Integrity Checks*
OTG-BUSLOGIC-004	*Test for Process Timing*
OTG-BUSLOGIC-005	*Test Number of Times a Function Can be Used Limits*
OTG-BUSLOGIC-006	*Testing for the Circumvention of Work Flows*
OTG-BUSLOGIC-007	*Test Defenses Against Application Mis-use*
OTG-BUSLOGIC-008	*Test Upload of Unexpected File Types*
OTG-BUSLOGIC-009	*Test Upload of Malicious Files*
Client Side Testing	
OTG-CLIENT-001	*Testing for DOM based Cross Site Scripting*

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55

ID Kontrol	Standar Kontrol
OTG-CLIENT-002	*Testing for JavaScript Execution*
OTG-CLIENT-003	*Testing for HTML Injection*
OTG-CLIENT-004	*Testing for Client Side URL Redirect*
OTG-CLIENT-005	*Testing for CSS Injection*
OTG-CLIENT-006	*Testing for Client Side Resource Manipulation*
OTG-CLIENT-007	*Test Cross Origin Resource Sharing*
OTG-CLIENT-008	*Testing for Cross Site Flashing*
OTG-CLIENT-009	*Testing for Clickjacking*
OTG-CLIENT-010	*Testing WebSockets*
OTG-CLIENT-011	*Test Web Messaging*
OTG-CLIENT-012	*Test Local Storage*

Pada tabel 3 diatas adalah standar kontrol OWASP versi 4. Metode ini juga digunakan dalam proses pengujian sistem OJS Universitas Lancang Kuning.

D. Analisis dan Laporan

Tahapan ini akan dilakukan dengan pembuatan laporan hasil pengujian penetrasi menggunakan metode ISSAF dan OWASP versi 4.

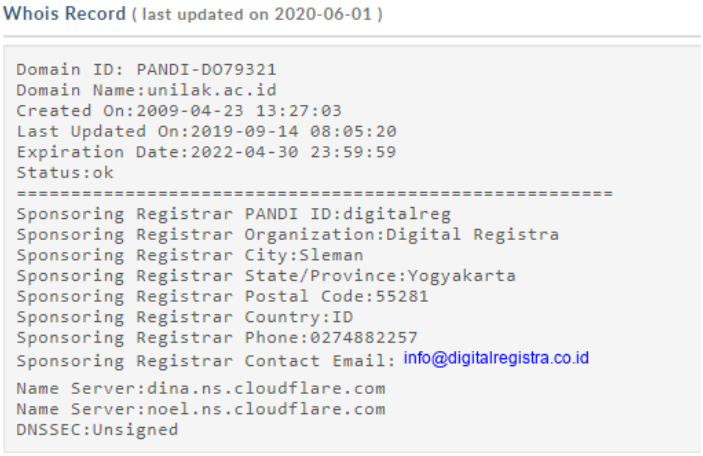
IV. HASIL DAN PEMBAHASAN

A. Pengujian ISSAF

Pada tahapan ini dilakukan pengujian menggunakan metode ISSAF. Adapun hasil pengujiannya adalah sebagai berikut.

1. *Information Gathering*

Pada tahap ini dilakukan pencarian informasi terhadap website yang akan diteliti yaitu OJS Universitas Lancang Kuning. Berikut adalah hasil pencarian menggunakan aplikasi Whois Domain terlihat pada gambar 3.



Gambar 3 Domain OJS journal.unilak.ac.id

Pada tabel 4 adalah hasil pencarian OJS journal.unilak.ac.id menggunakan tool Whois Domain. Dalam pencarian domain, bahwa domain jurnal UNILAK terdaftar oleh PANDI, domain name unilak.ac.id, didaftarkan pada tahun 2009, berakhir pada tahun 2022 dan bersatus OK.

TABEL 4
HASIL PENCARIAN DOMAIN OJS UNILAK

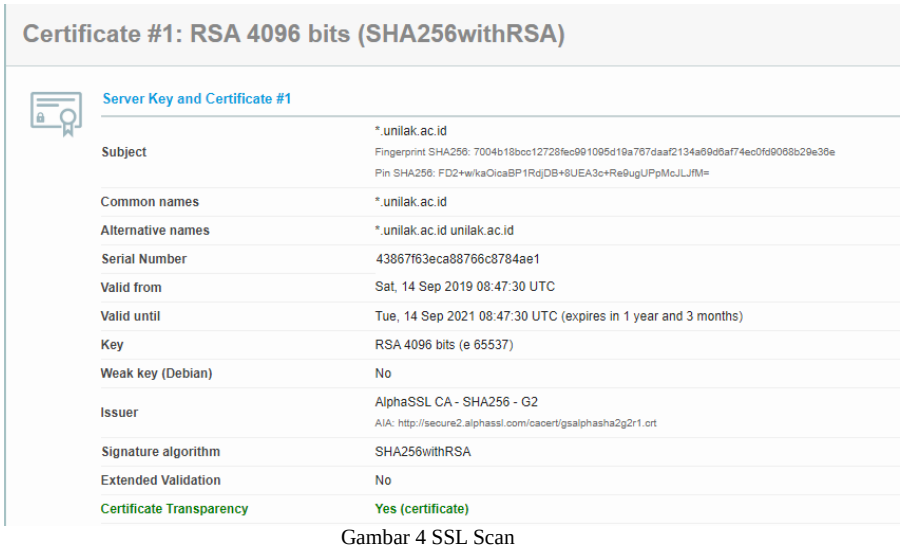
Domain OJS journal.unilak.ac.id	
Domain ID	PANDI-DO79321
Domain Name	unilak.ac.id
Create On	23 April 2009
Expiration Date	30 April 2022
Status	Ok

2. SSL Scan

SSL scan digunakan untuk mengetahui apakah domain sudah menggunakan keamanan SSL. Adapun tool yang digunakan adalah https://www.ssllabs.com/. Berdasarkan hasil scanning yang telah dilakukan bahwa domain journal.unilak.ac.id, telah menggunakan SSL, seperti yang terlihat pada gambar 4.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55



Gambar 4 SSL Scan

3. *Network Mapping*

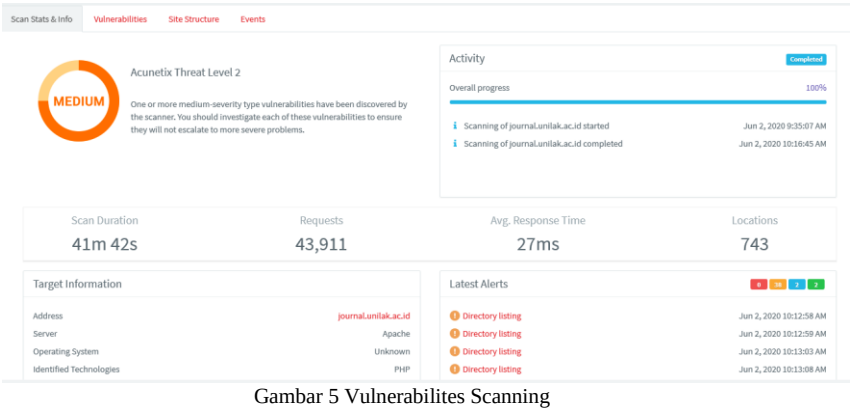
Network mapping dilakukan dengan menggunakan tool Zenmap. Berdasarkan scanning yang dilakukan bahwa domain jurnal Universitas Lancang Kuning, port 80 dan port 443 bersatus open, seperti yang terlihat pada tabel 5.

TABEL 5
HASIL SCANNING PORT

Domain journal.unilak.ac.id		
Port	80	443
Status	Open	Open
Services	HTTP	HTTP

4. *Vulnerability*

Pada tahap ini dilakukan scanning terhadap domain jurnal unilak, proses scanning menggunakan aplikasi Acunetix. Pengujian ini bertujuan untuk mengetahui tingkat kerentanan dari sebuah sistem. Adapun tipe yang dilakukan scanning adalah *Crawl Only, Weak Passwords, High Risk Vulnerabilites, Cross-site Scripting Vulnerabilities* dan *SQL Injection Vulnerabilites*. Berdasarkan hasil pengujian yang telah dilakukan, domain journal.unilak.ac.id masuk ke level 2 Medium seperti terlihat pada gambar 5.



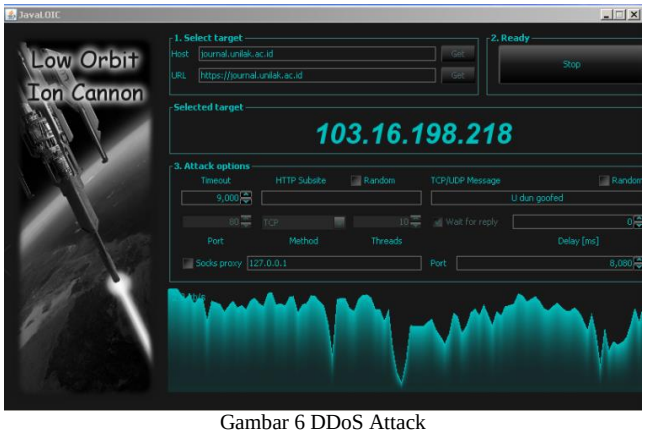
Gambar 5 Vulnerabilites Scanning

5. *Penetration*

Penetration merupakan salah satu tahapan pada Information System Security Assesment Framework (ISSAF) dimana pada tahapan ini penguji akan melakukan penetrasi terhadap website yang diuji. Dalam tahap ini penguji akan menguji apakah website ini terdapat kerentanan kepada DDOS Attck dengan menggunakan tool Low Orbit Ion Canon dan SQL Injection dengan menggunakan tool yaitu SQLmap. Berikut merupakan screenshot hasil dari pengujian menggunakan Low Orbit Ion Canon dan SQLmap terlihat pada gambar 6 dan 7.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55



Gambar 6 DDoS Attack

Report

Gambar 7 SQLmap Scanning

Berdasarkan hasil scanning yang telah dilakukan, bahwa jurnal journal.unilak.ac.id rentan terhadap serangan DoS. Tetapi tidak memiliki kerentanan terhadap SQL Injection. Adapun hasil dari pengujian menggunakan metode ISSAF bahwa dalam tahap Information Gathering menunjukkan status OK, tahap Network Mapping menunjukkan status OK, tahap Vulnerability Identification

B. Hasil Pengujian OWASP versi 4

Pada tahapan ini adalah melakukan pengujian menggunakan metode OWASP versi 4 terhadap domain journal.unilak.ac.id. Adapun hasil pengujiannya seperti terlihat pada tabel 6.

TABEL 6
HASIL PENGUJIAN OWASP

Tahapan	Tools	Hasil
Authentication Testing		
Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)	Browser Google Chrome	Menerapkan HTTPS
Testing for default credentials (OTG-AUTHN-002)	Brutus	Lolos
Testing for Weak lock out mechanism (OTG-AUTHN-003)	Browser Google Chrome	Tidak Lolos
Testing for bypassing authentication schema (OTG-AUTHN-004)	WebScarab	Lolos
Test remember password functionality (OTG-AUTHN-005)	WebScarab	Lolos
Testing for Browser cache weakness (OTG-AUTHN-006)	Browser Google Chrome	Lolos
Testing for Weak password policy (OTG-AUTHN-007)	Brutus	Lolos
Testing for Weak security question/answer (OTG-AUTHN-008)	-	Lolos
Testing for weak password change or reset functionalities (OTG-AUTHN-009)	-	Lolos
Testing for Weaker authentication in alternative channel (OTG-AUTHN-010)	-	Lolos
Authorization Testing		
Testing Directory traversal/file include (OTG-AUTHZ-001)	WFuzz	Lolos
Testing for bypassing authorization schema (OTG-AUTHZ-002)	Dirb	Lolos
Testing for Privilege Escalation (OTG-AUTHZ-003)	WebScarab	Lolos
Testing for Insecure Direct Object References (OTG-AUTHZ-004)	Browser Google Chrome	Lolos

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 05, Nomor 01, Juni 2020 : 45 – 55

Session Management Testing		
Testing for Bypassing Session Management Schema (OTG-SESS-001)	Dirb	Lolos
Testing for Cookies attributes (OTG-SESS-002)	Zed Attack Proxy	Lolos
Testing for Session Fixation (OTG-SESS-003)	Zed Attack Proxy	Lolos
Testing for Exposed Session Variables (OTG-SESS-004)	Zed Attack Proxy	Lolos
Testing for Cross Site Request Forgery (OTG-SESS-005)	OWASP CSRF Tester	Lolos
Testing for logout functionality (OTG-SESS-006)	Browser Mozilla Firefox	Lolos
Test Session Timeout (OTG-SESS-007)	Browser Mozilla Firefox	Lolos
Testing for Session puzzling (OTG-SESS-008)	Zed Attack Proxy	Lolos

Berdasarkan hasil pengujian yang dilakukan, bahwa sistem OJS Universitas Lacang Kuning tergolong aman. Tetapi terdapat beberapa kelemahan yaitu sistem tidak bisa memblokir ketika user melakukan berkali-kali kesalahan dalam proses login. Berdasarkan pengujian menggunakan OWASP Zap tergolong ke dalam level medium. Dikarenakan sistem yang digunakan adalah menggunakan Open Source OJS. Tetapi walaupun tergolong aman, serangan bisa saja terjadi dari berbagai pihak, baik dari dalam kampus sendiri atau serangan dari virus. Adapun rekomendasi framework ISSAF dan OWASP Versi 4 adalah sebagai berikut:

1. Menerapkan sistem IDS (*Intrusion Detection System*), sehingga dapat memonitoring serangan, baik dari dalam maupun dari luar sistem.
2. Melakukan backup data secara berkala. Agar ketika sistem *crash*, maka masih dapat mengambalikan data.
3. Selalu melakukan update terhadap sistem OJS (*Open Journal System*), karena memang OJS yang digunakan oleh Universitas Lancang Kuning adalah OJS versi 3 dan OJS harus selalu dilakukan update berkala.
4. Jika memungkinan dapat menerapkan pemblokiran terhadap login yang tidak valid, sesuai pada tahapan *Testing for Weak lock out mechanism* (OTG-AUTHN-003), hal ini bertujuan untuk mencegah serangan-serangan yang ada.

V. KESIMPULAN

Dalam penelitian ini dilakukan pengujian penetrasi menggunakan metode ISSAF dan OWASP versi 4 yang bertujuan untuk menguji tingkat keamanan sistem OJS journal.unilak.ac.id. Berdasarkan pengujian yang telah dilakukan, dapat diambil kesimpulan sebagai berikut:

1. Berdasarkan pengujian menggunakan metode ISSAF dan OWASP, sistem OJS Universitas Lancang tergolong aman, karena tidak mampu untuk ditembus.
2. Walaupun OJS Universitas Lancang Kuning tergolong aman, serangan bisa saja terjadi dari dalam institusi.
3. Perlunya menerapkan sistem monitoring, untuk melindungi server yang ada, misalnya menerapkan Firewall maupun *Intrusion Detection System* (IDS)

UCAPAN TERIMA KASIH

Ucapan terima kasih diberikan kepada Fakultas Ilmu Komputer Universitas Lancang yang telah membantu dalam dukungan finansial.

DAFTAR PUSTAKA

[1] I. P. Agus and E. Pratama, "Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study : X Company)," *Int. J. Comput. Netw. Inf. Secur.*, no. July, pp. 8–12, 2019.
[2] Y. W, I. Riadi, and A. Yudhana, "Analisis Deteksi Vulnerability Pada Webserver Open Journal System Menggunakan OWASP Scanner," *JURTI*, vol. 2, no. 1, pp. 1–8, 2018.
[3] B. Ghozali, Kusrini, and Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating," *Citec J.*, vol. 4, no. 4, pp. 264–275, 2017.
[4] M. Z. Maharani, H. R. Andrian, and S. J. I. Ismail, "ANALISIS KEAMANAN WEBSITE MENGGUNAKAN METODE SCANNING DAN PERHITUNGAN SECURITY METRIKS," *e-Proceeding Appl. Sci.*, vol. 3, no. 3, pp. 1775–1782, 2017.
[5] P. Pendidikan and D. A. N. Pelatihan, "PENGENALAN OPEN JOURNAL SYSTEM MADIKA PUSAT PENDIDIKAN DAN PELATIHAN," *MADIKA Media Inf. dan Komun. Diklat Kepustakawanan*, vol. 5, no. 1, pp. 95–106, 2019.
[6] M. Yunus, "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4," *J. Ilm. Inform. Komput.*, vol. 24, no. 1, pp. 37–48, 2019.
[7] K. Vijayalakshmi and D. A. A. Leema, "Extenuating Web Vulnerability with a Detection and Protection Mechanism for a Secure Web Access," *Int. Conf. Signal Process. Commun. Netw. (ICSCN -2017)*, pp. 16–19, 2017.
[8] Matteo Meucci, *OWASP TESTING GUIDE*. OWASP Foundation, 2008.
[9] T. Syarif Revolino and D. Jatmiko Andri, "Analisis Perbandingan Metode Web Security Ptes , Issaf Dan Owasp Di Dinas Komunikasi Dan Informasi Kota Bandung," p. 8, 2018.
[10] A. Saputra, Nelmiawati, and M. A. R. Sitorus, "Penilaian Ancaman pada Website Transkrip Aktivitas Kemahasiswaan Politeknik Negeri Batam Menggunakan Metode DREAD," *J. Integr.*, vol. 9, no. 1, pp. 53–66, 2017.

[11] B. Rathore, *Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B*. Open Information Systems Security Group, 2006.
[12] R. H. Hutagalung, L. E. Nugroho, and R. Hidayat, "Analisis Uji Penetrasi Menggunakan ISSAF," *Hacking Digit. Forensics Expo.*, pp. 32–40, 2017.
[13] B. Rusmarasy, B. Priyambadha, and F. Pradana, "Pengembangan Chat Bot pada CoMa untuk memberikan motivasi kepada pengguna menggunakan AIML," vol. 3, no. 5, pp. 4484–4490, 2019.
[14] M. Meucci, *OWASP Testing Guide 4.0*. .
[15] G. Guntoro and M. Fikri, "Perancangan Aplikasi Single Sign-On Menggunakan Autentikasi Gambar," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 9, no. 1, pp. 12–21, 2018.