Analisis Kerentanan Keamanan Pada Website PT XYZ Melalui Pengujian Penetrasi Dengan Framework OWASP Top-10

1st Ahmad Hasan Mutawakkil A.
Fakultas Rekayasa Industri
Telkom University
Surabaya, Indonesia
hasanmtwkl@student.telkomuniversity.ac.id

2nd Muhamad Nasrullah
Fakultas Rekayasa Industri
Telkom University
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

3rd Muhammad Ilham Alhari
Fakultas Rekayasa Industri
Telkom University
Surabaya, Indonesia
ilhamalhari@telkomuniversity.ac.id

***Abstrak* — Seiring bertumbuhnya teknologi informasi secara pesat dapat memberikan hal yang positif dalam persebaran informasi. *Website* merupakan salah satu hasil dari perkembangan teknologi informasi sebagai media penyampaian informasi. XYZ sebagai *partner* transformasi pendidikan memiliki *website* yang berisi data-data sensitif seperti data pembelian paket kelas *bootcamp*, namun belum pernah dilakukan penetration testing untuk meningkatkan keamanan sistemnya. Penelitian ini menggunakan *framework* OWASP Top – 10 2021 dengan metode *black box testing* untuk melakukan pengujian penetrasi pada website XYZ. Pengujian dilakukan untuk mengidentifikasi potensi kerentanan keamanan yang mungkin dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Hasil pengujian menemukan beberapa kerentanan signifikan seperti masalah pada *user agent fuzzer*, *improper input validation*, *information disclosure*, kerentanan terkait header keamanan, *plugin* dan tema yang perlu diperbarui, risiko *brute force* dan *user enumeration*, serta *insufficient logging*. Rekomendasi perbaikan yang diberikan meliputi implementasi validasi input, header keamanan yang tepat, mekanisme anti-CSRF, perbaikan konfigurasi *cookie*, pembaruan *plugin* dan tema, implementasi rate limiting dan CAPTCHA, serta peningkatan sistem *logging* dan *monitoring*.**

Kata kunci*— Kali Linux, Kejahatan *Cyber*, *Penetration Testing*, *Website

I. PENDAHULUAN

Pada era teknologi informasi yang berkembang secara pesat, *website* merupakan salah satu contoh hasil perkembangan tersebut[1]. *Website* merupakan perkembangan teknologi yang mengarah pada pertukaran data yang efisien serta mencakup sistem siber-fisik, *internet of things, cloud computing* dan *cognitive computing*[2]. Dengan kemajuan ini, terdapat beberapa keresahan dalam sisi pengguna dan pengembang. Keresahan ini berupa kerentanan keamanan yang mengancam kerugian finansial dan merusak citra nama baik perusahaan[3].

Terdapat beberapa kasus akibat kerentanan keamanan yang menyebabkan adanya celah untuk melakukan peretasan. Pada Kasus pertama adalah bank BSI mengalami kebocoran data sebanyak 15 juta data nasabah, informasi karyawan, dan sekitar 1,5 terabita data *internal[4].* Selanjutnya, 17.000 situs *WordPress* disusupi oleh *malware* yang bernama *ballad injector*, yang akibatnya penyerang dapat mengalihkan pengguna *web* ke halaman penipuan. Dengan contoh beberapa kasus tersebut, sudah seharusnya pihak perusahaan bisa melakukan pengujian penetrasi dalam membantu meningkatkan keamanan. Pengujian penetrasi ini memungkinkan analisis keamanan dalam mendeteksi kerentanan baru[5].

PT XYZ merupakan perusahaan yang bergerak dalam layanan pendidikan seperti penyedia konsultasi, pelatihan, pengembangan kepemimpinan, riset dan pendampingan berkelanjutan. Sebagai *web* penyedia *workshop, course* dan pelatihan, terdapat *billing details* yang berisi data pribadi pengguna layanan, sehingga keamanan *web* mereka menjadi esensial. Selain itu pada *website* XYZ ini sebelumnya belum pernah dilakukan pengujian penetrasi. Maka penting dilakukannya pengujian penetrasi untuk mendeteksi kerentanan agar tingkat keamanan *website* bisa selalu diperbarui[6].

Pada penelitian ini dilakukan pengujian penetrasi apakah protokol keamanan telah diterapkan dengan baik, serta mencari celah kerentanan pada *website* XYZ. Dalam melakukan pengujian penetrasi, peneliti mengacu pada *framework* OWASP Top – 10 2021. OWASP Top – 10 ini berisi daftar 10 teratas kerentanan *web* yang perlu diperhatikan dan untuk menghindari adanya percobaan eksploitasi atas kerentanan tersebut[7].

II. KAJIAN TEORI

A. OWASP (*Open Worldwide Application Security Project)*

Open Worldwide Application Security Project (OWASP) adalah yayasan nirlaba yang berfokus pada mempelajari keamanan aplikasi *website,* dan menyediakan informasi terkait kerentanan yang terbaru dan populer pada aplikasi *web*[8].

B. OWASP Top – 10

OWASP Top – 10 merupakan sebuah daftar teratas kerentanan keamanan yang dapat mengancam keamanan suatu *website*, daftar tersebut bisa dijadikan menjadi acuan

bagi pengembang aplikasi *web* dan tim keamanan untuk mendeteksi celah-celah kelemahan dari aplikasi *web*[9].

C. *Penetration Testing*

Penetration testing atau pengujian penetrasi merupakan sebuah pengujian dengan melakukan eksploitasi ke dalam sistem yang bertujuan untuk mengetahui kemungkinan adanya eksploitasi pada sistem[10]. Hasil dari pengujian ini berupa rekomendasi perbaikan atas kelemahan sistem yang terdeteksi, sehingga dapat meningkatkan keamanan serta meminimalisir risiko serangan siber[11].

D. *Black Box Testing*

Black box testing merupakan sebuah metode dalam melakukan pengujian penetrasi, dalam pengujian penetrasi metode ini, tidak diperlukan informasi apapun tentang sistem, struktur *web*, hingga kode sumber[12]. Metode ini digunakan untuk audit keamanan sistem dengan melakukan penyerangan dari eksternal dan juga menemukan celah kerentanan[13].

E. Kali Linux

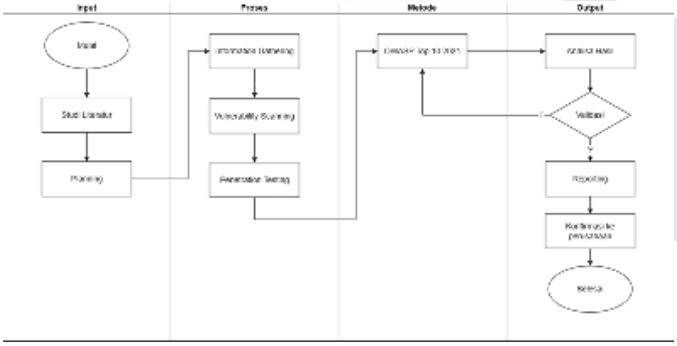
Kali Linux merupakan sistem operasi distribusi Linux berbasis Debian, yang dirancang untuk memudahkan dalam pengujian penetrasi dan keamanan siber. Kali Linux ini menyediakan berbagai alat yang tiap fungsinya dapat membantu dalam pengujian keamanan, seperti misal OWASP ZAP yang merupakan *security scanner*[14].

III. METODE

Peneliti menggunakan *framework* OWASP Top – 10 2021 pada pengujian penetrasi ini, sebagai pedoman utama untuk mengidentifikasi dan mengevaluasi kerentanan keamanan pada sistem, guna memastikan pengujian dilakukan sesuai dengan standar terbaik yang relevan dengan konteks penelitian.

A. Alur Penelitian

Berikut merupakan alur penelitian yang digunakan.



GAMBAR 1
Alur penelitian

Pada tahap input, literatur relevan dikumpulkan sebagai referensi, kemudian dilanjutkan dengan perencanaan melalui analisis fitur website, penentuan alat yang akan digunakan, dan wawancara dengan perwakilan perusahaan untuk mengumpulkan informasi terkait. Selanjutnya, pada tahap proses, dilakukan pengumpulan data seperti domain ID, nama domain, dan alamat IP, dilanjutkan dengan pemindaian kerentanan dan pengujian penetrasi yang mengacu pada standar OWASP Top 10 2021. Tahap akhir, yaitu output, meliputi analisis hasil pengujian, validasi oleh seorang validator untuk memastikan kesesuaian temuan dengan standar tersebut, serta pelaporan hasil pengujian dan konfirmasi kepada perusahaan.

IV. HASIL DAN PEMBAHASAN

A. *Planning*

Pada tahapan *planning* ini merupakan langkah awal untuk memastikan bahwa tujuan pengujian telah sesuai, adapun *website* yang diuji beralamat di abc.id. *Website* ini merupakan *platform* yang digunakan oleh XYZ untuk mendukung layanan konsultasi pendidikan. Pengujian penetrasi dilakukan pada situs ini untuk mengidentifikasi celah kerentanan keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pada tahapan ini juga dilakukan wawancara untuk mendapatkan informasi yang mendalam terkait tujuan, fungsi, dan layanan yang ditawarkan pada *website* objek.

B. *Information Gathering*

Pada tahap *information gathering* ini dilakukan pengumpulan informasi untuk memahami target secara mendalam untuk meningkatkan efisiensi dalam pengujian[15].

TABEL 1
Hasil *Information Gathering*

Tools	**Hasil**
Whois	Domain ID: xxxxx-xxxxxxxx, Nama Domain: xxxxxx.xx, Nama Server, alamat registrar, dan informasi lainnya yang terkait dengan web.
Nslookup	IP Address: 104.xx.xx.xxx, Mail Exchanger, Informasi SOA (Start of Authority) record.
Dig	IP Address: 104.xx.xx.xxx dan 172.xx.xxx.xxx)
Nmap	Port 80/HTTP, Port 443/SSL HTTP, Port 8080/HTTP, Port 8443/SSL HTTP.

C. *Vulnerability Scanning*

Pada tahapan *vulnerability Scanning* ini dilakukan pemindaian kerentanan untuk mengevaluasi keamanan web dengan alat yang dapat mendeteksi kerentanan serta saran mitigasi[16]. Dari hasil OWASP ZAP, ditemukan 1 kerentanan dengan tingkat *high*, 4 kerentanan dengan tingkat *medium*, 6 kerentanan dengan tingkat *low*, dan 7 kerentanan dengan tingkat *informational*.

D. *Penetration Testing*

Pada tahapan *penetration testing* ini peneliti melakukan serangkaian uji penetrasi dengan berbagai skenario untuk menemukan celah keamanan yang sesuai dengan OWASP Top – 10 2021.

TABEL 2
Hasil *Penetration Testing*

ID	**Temuan**
A01:2021 – *Broken Access Control*	Ditemukan kerentanan *user agent fuzzer* dan *improper input validation*.
A02:2021 – *Cryptographic Failures*	Tidak ditemukan adanya indikasi kerentanan.
A03:2021 – *Injection*	Tidak ditemukan adanya indikasi kerentanan.
A04:2021 – *Insecure Design*	Ditemukan kerentanan desain yang tidak aman, pesan error yang menyatakan informasi validitas *username*.

ID	Temuan
A05:2021 – *Security Misconfiguration*	Ditemukan adanya kerentanan tidak ada beberapa *header* keamanan, tidak ditemukan mekanisme CSRF *token* pada formulir, dan konfigurasi *cookies* yang tidak diatur dengan baik.
A06:2021 – *Vulnerable and Outdated Components*	Ditemukan kerentanan komponen yang digunakan oleh *website* sudah cukup usang.
A07:2021 – *Identification and Authentication*	Ditemukan kerentanan pesan error menyatakan validitas *username* yang membantu penyerang dalam *username enumerating,* dan tidak ditemukan adanya mekanisme yang mencegah pengujian *brute force*.
A08:2021 – *Software and Data Integrity Failures*	Tidak ditemukan adanya indikasi kerentanan
A09:2021 – *Security Logging and Monitoring*	Ditemukan kerentanan mekanisme *logging* dan *monitoring* yang tidak diterapkan dengan baik pada percobaan login dengan kredensial yang tidak sah secara berulang kali.
A10:2021 – *Server-Side Request Forgery*	Tidak ditemukan adanya indikasi kerentanan.

E. *Reporting*

Pada tahapan *reporting* ini dilakukan penyusunan daftar temuan hasil pengujian dan pemberian rekomendasi perbaikan.

TABEL 3
Hasil *Reporting*

ID	Temuan	Rekomendasi Perbaikan
A01	*User Agent Fuzzer*	Memastikan *server* melakukan pemantauan terhadap *user agent* yang mencurigakan.
	Improper Input Validation	Menerapkan batas nilai maksimal pada *input box* serta melakukan validasi pada tiap *input*.
A02	-	-
A03	-	-
A04	*Information Disclosure*	Menerapkan desain pesan error yang bersifat umum, dan tidak memberikan informasi yang berlebihan.
A05	*Content Security Policy Header Not Set*	Menambahkan *header* "Content-Security-Policy".
	Absence of Anti-CSRF Tokens	Implementasi *token* Anti-CSRF pada tiap formulir.
	Missing Anti-Clickjacking Header	Menambahkan *header* "X-Frame-Options".
	Cookie No HttpOnly Flag	Menambahkan *flag* "HttpOnly" pada semua *cookie*.
	Cookie without SameSite Attribute	Menambahkan atribut "SameSite" pada semua *cookie.*
	Server Leaks Information	Hapus atau sembunyikan informasi sensitif pada *header*.
	Strict-Transport-Security Header Not Set	Menambahkan *header* "Strict-Transport-Security"
	Timestamp Disclosure – Unix	Hapus atau sembunyikan *timestamp*.
	Information Disclosure – Suspicious Comments	Menghapus komentar-komentar yang berisi informasi sensitif.
	Re-examine Cache-control Directives	Menambahkan *header* "Cache-Control"
	Retrieved from Cache	Menambahkan *header* "Cache-Control".
	Cookie without Secure Flag	Atur secure flag pada cookie serta menggunakan atribut "SameSite".
	Referrer Leakage	Menambahkan *header* "Referrer-Policy".
	Cross-Domain Policy	Menambahkan *header* "CORS".
A06	*Outdated Plugins and Themes*	Memperbarui *plugin* dan tema ke versi yang terbaru, serta melakukan pemeriksaan berkala untuk mengetahui pembaruan.
A07	*User Enumeration*	Menggunakan pesan error yang menyatakan secara general seperti "username atau password salah".
	Brute Force Attack	Implementasi pembatasan percobaan *login* pada satu alamat IP dengan periode waktu tertentu (*rate limiting*). Menggunakan CAPTCHA untuk memastikan permintaan dilakukan oleh manusia dan bukan bot.
A08	-	-
A09	*Insufficient logging*	*Monitoring real-time* untuk aktivitas yang mencurigakan, terapkan pembatasan (*rate limiting*).
A10	-	-

V. KESIMPULAN

Berdasarkan hasil pengujian penetrasi pada *website* Abc.id dengan *framework* OWASP Top 10 2021, teridentifikasi sejumlah kerentanan kritis yang memerlukan perhatian segera. Kerentanan tersebut meliputi masalah *input validation* (A01:2021), kebocoran informasi (A04:2021), konfigurasi header keamanan yang lemah (A05:2021), penggunaan plugin/tema usang (A06:2021), risiko *brute force* (A07:2021), hingga *logging* yang tidak memadai (A09:2021). Untuk memitigasi risiko ini, rekomendasi perbaikan difokuskan pada validasi *input*, implementasi *header* keamanan (CSP, X-Frame-Options, HSTS), pencegahan CSRF, pembaruan konfigurasi *cookie* (HttpOnly, SameSite), serta pembaruan *plugin*/tema ke versi terbaru. Di sisi lain, pencegahan *brute force* memerlukan penerapan *rate limiting* dan CAPTCHA, sementara kebocoran informasi dapat diminimalkan dengan perbaikan penanganan error. Selain itu, peningkatan sistem *logging* dan *monitoring* diperlukan untuk mendeteksi ancaman secara proaktif. Dengan mengimplementasikan rekomendasi ini, keamanan website Abc.id diharapkan dapat ditingkatkan secara signifikan, mengurangi risiko eksploitasi, dan memastikan perlindungan data yang lebih optimal.

REFERENSI

[1] A. Bastian, H. Sujadi, and L. Abror, "Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing Dan SQL Injection," *INFOTECH journal* , vol. 6, no. 2, pp. 65–70, Dec. 2020.

[2] D. Hendarsyah, "E-Commerce Di Era Industri 4.0 Dan Society 5.0," *IQTISHADUNA : Jurnal Ilmiah Ekonomi Kita*, vol. 8, no. 2, pp. 171–184, 2019.

[3] D. M. Al Vriano, "Pengujian Keamanan Web Juice Shop Dengan Metode Pentesting Berbasis OWASP Top 10," *Kohesi: Jurnal Sains dan Teknologi*, vol. 1, no. 6, pp. 91–100, Oct. 2023.

[4] D. D. Paramitha, "15 Juta Data Nasabah BSI Diduga Bocor, Pakar Siber: Hati-hati Serangan Phising ke Pemilik Rekening," tempo.co. Accessed: Nov. 20, 2023. [Online]. Available: https://bisnis.tempo.co/read/1726521/15-juta-data-nasabah-bsi-diduga-bocor-pakar-siber-hati-hati-serangan-phising-ke-pemilik-rekening

[5] R. M. S. Zeebare, K. Jacksi, and R. , R. Zebari, "Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 1, pp. 505–512, Jul. 2020.

[6] E. Irawadi Alwi, Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *Informatics Journal*, vol. 5, no. 2, pp. 43–48, 2020, doi: https://doi.org/10.19184/isj.v5i2.18941.

[7] R. Febriana, "Blackbox Testing Sistem Informasi Absensi Pegawai Karawang Dengan Metode Top 10 Owasp Attack," *Jurnal Ilmiah Wahana Pendidikan*, vol. 2022, no. 12, pp. 327–334, 2022, doi: 10.5281/zenodo.6945632.

[8] K. Patel, "A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication," *3rd International Conference on Trends in Electronics and Informatics (ICOEI),* pp. 320–325, 2019, doi: https://doi.org/10.1109/ICOEI.2019.8862767.

[9] N. Sulisnawati and Subektiningsih, "Implementation of Open Web Application Security Project for Penetration Testing on Educational Institution Websites," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)*, vol. 9, no. 2, pp. 250–267, 2023, doi: 10.26555/jiteki.v9i2.25987.

[10] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *Jurnal Ilmiah Merpati*, vol. 8, no. 2, pp. 113–124, Aug. 2020, doi: https://doi.org/10.24843/JIM.2020.v08.i02.p05.

[11] S. E. Prasetyo and N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF," *JIF: Jurnal Ilmiah Informatika*, vol. 9, no. 2, pp. 83–86, 2021, doi: https://doi.org/10.33884/jif.v9i02.3758.

[12] A. Bimandaru, A. Alamsyah, and A. Nugroho, "Analisis Pengujian Penetrasi Pada Layanan Hosting Menggunakan Metode Black Box (Studi kasus : Blogspot, Wordpress dan Shared Hosting)," *Jurnal Foristek*, vol. 14, no. 1, Jun. 2023, doi: 10.54757/fs.v14i1.238.

[13] Guntoro, L. Costaner, and Musfawati, "Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)," *JIPI : Jurnal Ilmiah Penelitian dan Pembelajaran Informatika*, vol. 5, no. 1, pp. 45–55, 2020, doi: https://doi.org/10.29100/jipi.v5i1.

[14] A. Andria, "Website Security Gap Analysis Using WEBPWN3R Tools at Kali Linux," *Generation Journal*, vol. 4, no. 2, pp. 69–76, Aug. 2020, doi: 10.29407/gj.v4i2.14532.

[15] A. Kothia, B. Swar, and F. Jaafar, "Knowledge Extraction and Integration for Information Gathering in Penetration Testing," in *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, IEEE, Jul. 2019, pp. 330–335. doi: 10.1109/QRS-C.2019.00068.

[16] M. Ahsan, D. A. Rochmah, and D. Redaksi, "Analisa Kerentanan Sistem Dengan Menerapkan Open Vulnerability Assessment System Menggunakan Greenbone Vulnerability Management (GVM) INFORMASI ARTIKEL ABSTRACT," *INFORMATIKA DAN TEKNOLOGI (INTECH)* , vol. 3, no. 2, pp. 23–29, 2022.