KOMPUTA : Jurnal Ilmiah Komputer dan Informatika
Vol. 14, No. 1, April 2025, ISSN : 2089-9033, e- ISSN : 2715-7849
DOI: 10.34010/komputa.v14i1.14693

Analisis Keamanan *Website* Kampus UNIPDU Melalui Metode *Vulnerability Assessment* (VA) dengan Menggunakan *Tools Acunetix*

Moh. Rizki Syaifudin[1], Mohamad Ali Murtadho[2],
Moh. Shohibul Wafa[3], Mukhamad Masrur[4]

[1,2,3,4] Program Studi Sistem Informasi, Universitas Pesantren Tinggi Darul Ulum
E-mail: mohrizki.s@unipdu.ac.id

Abstrak

Di tengah pesatnya perkembangan teknologi, kerentanan *website* menjadi ancaman utama, membuka peluang bagi peretas untuk memburu dan mencuri data penting. Aplikasi web menjadi inovasi teknologi yang tidak hanya mempermudah akses informasi di kampus UNIPDU Jombang, tetapi juga berfungsi sebagai penghubung utama dalam sistem informasi, meskipun harus menghadapi tantangan besar dalam menjaga keamanannya. Dengan menggunakan pendekatan *Vulnerability Assessment (VA)* yang memanfaatkan teknologi *Acunetix*, penelitian ini berupaya menilai kelemahan *website* kampus UNIPDU Jombang dan menawarkan saran untuk meningkatkan keamanannya. Domain utama *website* menjadi fokus penelitian, yang menggunakan metodologi pengujian otomatis untuk menemukan kerentanan yang mungkin dapat dieksploitasi. Banyak kerentanan ditemukan oleh hasil pengujian, termasuk penggunaan *reverse proxy detected*, menggunakan layanan *cloud* seperti CloudFlare, dan sertifikat TLS/SSL yang hampir kadaluarsa. Melalui laporan dari pemindaian yang mematuhi pedoman OWASP Top 10 2021 pada *tools Acunetix*, ditemukan 2 kelompok kategori kerentanan yang meliputi: (A05) *security misconfiguration* dan (A06) *Vulnerable and Outdated Components*. Diharapkan bahwa upaya ini akan meningkatkan keamanan data dan menggagalkan berbagai ancaman. Hasil penelitian ini memberikan informasi penting bagi pengembang *website* UNIPDU, termasuk kebutuhan untuk memperbarui sertifikat SSL dan menyarankan pemindaian pada versi internal aplikasi web tanpa WAF aktif. Temuan ini tidak hanya memperkuat keamanan sistem, tetapi juga membantu kampus menjaga kepercayaan pengguna sekaligus menjadi panduan bagi pengembangan sistem informasi yang lebih andal dan aman di masa depan.
Kata kunci: Website, *Vulnerability Assessment* (VA), *Acunetix*, Keamanan, UNIPDU

UNIPDU Campus Website Security Analysis Through Vulnerability Assessment (VA) Method with Acunetix Tools Assistance

Abstract

Amidst the rapid development of technology, website vulnerabilities are a major threat, opening up opportunities for hackers to hunt and steal important data. Web applications are a technological innovation that not only facilitates access to information on the UNIPDU Jombang campus, but also functions as the main link in the information system, even though they have to face major challenges in maintaining its security. By using the Vulnerability Assessment (VA) approach that utilizes Acunetix technology, this study attempts to assess the weaknesses of the UNIPDU Jombang campus website and offers suggestions for improving its security. The main domain of the website is the focus of the study, which uses automated testing methodology to find vulnerabilities that could be exploited. Many vulnerabilities were found by the test results, including the use of reverse proxy detected, using cloud services such as CloudFlare, and TLS/SSL certificates that are almost expired. Through reports from scans that comply with the OWASP Top 10 2021 guidelines on the Acunetix tools, 2 groups of vulnerability categories were found, including: (A05) security misconfiguration and (A06) Vulnerable and Outdated Components. It is expected that this effort will improve data security and thwart various threats. The results of this study provide important information for UNIPDU website developers, including the need to update SSL certificates and suggest

Naskah dikirim: 07-12-2024; direvisi 20-01-2025; diterima: 23-01-2025

scanning on internal versions of web applications without active WAF. These findings not only strengthen system security, but also help campuses maintain user trust while being a guide for the development of more reliable and secure information systems in the future.
Keywords: *Website, Vulnerability Assessment (VA), Acunetix, Security, UNIPDU*

1. Pendahuluan

Peningkatan jumlah kebocoran data akhir-akhir ini telah membuat banyak pihak semakin berhati-hati dalam memberikan data pribadi[1]. Kebocoran tersebut tidak hanya merugikan pengguna, tetapi juga dapat membahayakan kelangsungan organisasi atau perusahaan. *Website* pemerintah/lembaga negara yang cukup sering dijadikan oleh pelaku serangan siber memberikan asumsi pada masyarakat mengenai lemahnya sistem pemerintah kita. Berikut adalah beberapa *website* pemerintah yang mengalami peretasan, baik disengaja oleh *hacker* atau hanya sebagai bahan *penetration testing* yang meliputi: Peretas Bjorka merilis kebocoran 1,3 miliar data registrasi kartu SIM prabayar, yang meliputi informasi seperti NIK, nomor telepon, penyedia layanan telekomunikasi, dan tanggal pendaftaran. Bjorka menjualnya senilai Rp 700 juta pada 2 September 2022, Kelompok peretas Lock Bit mencuri dan mengenkripsi sekitar 1,5 *terabyte* data internal BSI, isinya 15 juta data privat pengguna BSI melalui ransomware. *Lock Bit* akhirnya menyebar data itu ke publik usai permintaan tebusan Rp 309 miliar tidak terpenuhi pada 15 Mei 2023, Server Pusat Data Nasional Sementara (PDNS) yang dikelola Kemkominfo, lumpuh akibat Brain Cipher Ransomware. Imbasnya, 210 instansi pusat dan daerah terdampak. Pelaku minta tebusan Rp 131,2 miliar pada 20 Juni 2024[2].

Setiap kali sistem berhasil ditembus, para peretas berusaha mengakses informasi sensitif atau mengganggu operasional dengan tujuan memperoleh manfaat pribadi, baik dalam bentuk finansial maupun informasi berharga. Keberadaan data penting yang berisi informasi suatu organisasi memerlukan perlindungan melalui pendekatan yang menyeluruh dan terencana terhadap resiko yang mungkin muncul. Untuk mengatasi masalah keamanan, diperlukan metode yang mampu menjamin perlindungan data, transaksi, serta komunikasi. Kurangnya keamanan pada sistem dapat mengakibatkan konsekuensi yang merugikan[3]. Pemrograman web, yang merupakan penulisan serangkaian instruksi untuk diikuti komputer guna melakukan aktivitas atau fungsi tertentu, dapat digunakan untuk membuat website. Dengan kata lain, pemrograman web adalah proses pengiriman perintah atau instruksi ke komputer yang terhubung ke internet sehingga tugas atau fungsi lain dapat dibuat. Peramban web seperti Opera, Mozilla, Chrome, dan lainnya kemudian dapat digunakan untuk menjalankan aplikasi daring. Awalnya digunakan terutama untuk keperluan pribadi, *website* saat ini digunakan sebagai media informasi oleh hampir semua perusahaan, lembaga, dan bahkan usaha kuliner.[4].

Sebagai institusi pendidikan, universitas juga memiliki potensi menjadi target serangan siber, yang terkadang *server down* menyebabkan situs tidak dapat diakses oleh pengguna, sehingga menghambat pemenuhan kebutuhan mereka. Gangguan tersebut membatasi akses ke informasi penting seperti jadwal perkuliahan, pengumuman, dan layanan akademik lainnya. Hal ini mengakibatkan terganggunya proses belajar-mengajar dan administrasi, yang berdampak pada ketidaknyamanan bagi mahasiswa, dosen, dan staf. Kegagalan server ini menunjukkan perlu adanya peningkatan infrastruktur TI dan manajemen sistem yang lebih efektif untuk memastikan akses yang stabil dan andal. Karena aplikasi web rentan terhadap serangan seperti injeksi SQL, *Denial of Service*, dan berbagai jenis malware, aplikasi web sering kali menjadi target utama peretas. Banyak aplikasi web dibuat tanpa mempertimbangkan keamanan sejak awal, yang menyebabkan kerentanan ini. Karena aplikasi ini biasanya dibuat oleh pengembang dengan keahlian keamanan web yang kurang, website tersebut memiliki banyak kerentanan yang dapat digunakan untuk menyerang.

Adanya pengujian VAPT yang menjadi suatu kewajiban, karena adanya regulasi dari peraturan bank Indonesia (PBI) dan (OJK) yang mengharuskan perusahaan di Indonesia untuk melakukan pengujian keamanan IT nya[5]. Melalui metode tersebut, diharapkan analisis yang dilakukan dapat memberikan informasi secara detail bagi pengembang untuk memperbaiki atau memperbarui sistem tersebut secara berkala agar terhindar dari serangan siber. Penulis memilih menggunakan metode VA (*Vulnerability Assessment*) dalam pengujian untuk mengidentifikasi kerentanan yang terdapat pada website kampus UNIPDU. Metode ini diterapkan guna mengungkap potensi kelemahan yang dapat dimanfaatkan oleh pihak tidak berwenang, serta memberikan rekomendasi solusi yang tepat untuk memperbaiki dan memperkuat

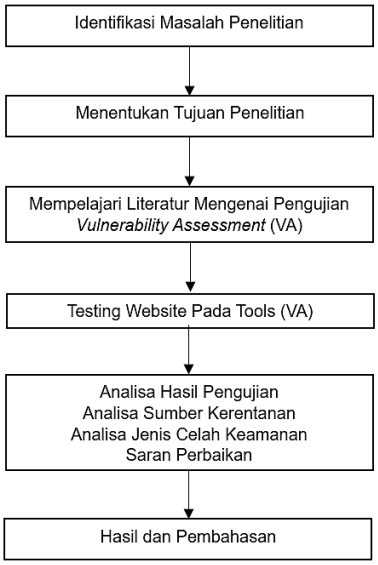
keamanan website tersebut. Dengan pendekatan ini, diharapkan website kampus UNIPDU dapat menjadi lebih aman dan terlindungi dari berbagai ancaman keamanan siber.

Pernyataan ini merujuk pada beberapa proyek penelitian sebelumnya yang menggunakan metodologi yang sama, namun dengan memanfaatkan beberapa tools yang berbeda. Beberapa penelitian sebelumya diantaranya "Penerapan Metode *Vulnerability Assessment* untuk Identifikasi Keamanan *Website* berdasarkan OWASP ID Tahun 2021" menggunakan *tools* OWASP ID 2021 dan menerapkan teknik mitigasi [6]. Penelitian kedua dengan judul "*Vulnerability Assessment And Penetration Testing* Menggunakan Metode *Zero Entry Hacking* (Zeh) Terhadap *Website*" studi kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan dengan menggunakan Kali Linux dalam pengujiannya, *Whois*, The Harvester, Whatweb, CXSecurity, Google Hacking Database + Google Dorking, Terminal, Nmap, dan OWASP ZAP[7]. Penelitian ketiga dengan judul "*Vulnerability Assessment* Untuk Meningkatkan Kualitas Keamanan *Web* pada aplikasi berbasis web" mengalami permasalahan dalam penelitiannya adalah aplikasi web sangat rentan terhadap serangan seperti penolakan layanan, injeksi SQL, dan berbagai jenis *malware*, yang merupakan perangkat lunak berbahaya, program berbahaya yang dapat mengganggu atau merusak komputer, data, atau jaringan kita.[8]. Target dalam penelitian ini diidentifikasi sebagai proxy terbuka HTTP, menurut temuan pengujian VA menggunakan nmap. Setelah itu, tidak ada bukti adanya skrip lintas situs pada target yang diuji. Lebih jauh, *host* target tidak menunjukkan tanda-tanda Injeksi SQL[9]. Penelitian keempat dengan judul "Analisis Metode *Open Web Application Security Project* (OWASP) Menggunakan *Penetration Testing* pada Keamanan *Website* Absensi pada aplikasi web absensi sub.domain.com" masalah dalam penelitian ini yaitu di internet, sering terjadi masalah atau celah keamanan sistem. Adanya serangan *Malware*, Eksploitasi dan Injeksi database[10]. Penelitian kelima dengan judul "Analisis *Security Mitigation* dengan Metode *Vulnerability Assessment and Penetration Testing* (VAPT) (Kasus Website Kerja Praktek dan Pengabdian Masyarakat)" Pengujian keamanan lebih lanjut diperlukan untuk mengidentifikasi kerentanan yang lebih dalam dan rekomendasi mitigasi untuk mengamankan data pengguna dan menurunkan resiko serangan yang mengancam sistem website karena masalah ini melibatkan kerentanan yang ditemukan selama pengujian sebelumnya dan tidak ada mitigasi lanjutan yang diterapkan[11].

Penulis memilih menggunakan metode VA (*Vulnerability Assessment*) dalam pengujian untuk mengidentifikasi kerentanan yang terdapat pada website kampus Unipdu. Metode ini diterapkan guna mengungkap potensi kelemahan yang dapat dimanfaatkan oleh pihak tidak berwenang, serta memberikan rekomendasi solusi yang tepat untuk memperbaiki dan memperkuat keamanan website tersebut. Dengan pendekatan ini, diharapkan *website* kampus Unipdu dapat menjadi lebih aman dan terlindungi dari berbagai ancaman keamanan siber.

2. Metodologi

Penulis menggunakan metode *Vulnerability Assessment* (VA) dalam prosedur pengujian dan analisis ini untuk menemukan kelemahan keamanan dalam sistem. Pengujian *Vulnerability Assessment* (VA) menggunakan alat *Acunetix Web Vulnerability Scanner* adalah proses identifikasi dan analisis kerentanan pada aplikasi berbasis web. *Acunetix* adalah program populer untuk mengidentifikasi kelemahan web, termasuk kelemahan pengkodean dan kesalahan konfigurasi, dan mengklasifikasikan temuan menurut tingkat resiko. Aplikasi ini memungkinkan pemindaian otomatis dan analisis menyeluruh pada *website* untuk memastikan tidak ada kelemahan potensial yang dapat dimanfaatkan oleh orang yang tidak berwenang. Kerangka kerja penelitian ini dijelaskan melalui alur yang ditampilkan pada gambar 1, sebagai berikut.



Gambar 1. Kerangka kerja penelitian

2.1 Identifikasi Masalah Penelitian

Penelitian ini dilakukan untuk mengidentifikasi dan memahami kelemahan keamanan yang ada pada *website* UNIPDU Jombang. Masalah utamanya adalah menghindari potensi celah keamanan yang dapat dieksploitasi oleh orang-orang yang tidak bertanggung jawab untuk meretas atau mendapatkan akses ke data sensitif. Oleh karena itu, diperlukan metode pengujian keamanan seperti VA (V*ulnerability Assessment*) untuk mengidentifikasi kerentanan dan memberikan solusi yang tepat dalam meningkatkan keamanan *website*.

2.2 Menentukan Tujuan Penelitian

Menetapkan tujuan utama penelitian merupakan langkah awal yang penting dalam setiap upaya penelitian karena memberikan instruksi yang tepat tentang apa yang harus dilakukan. Tujuan penelitian harus dirumuskan secara spesifik dan relevan dengan permasalahan yang diangkat, sehingga mampu memberikan solusi atau kontribusi yang nyata. Tujuan penelitian juga menjadi acuan bagi peneliti dalam menentukan metode, teknik analisis, dan langkah-langkah yang diperlukan selama proses penelitian. Selain itu, tujuan yang jelas membantu memfokuskan penelitian agar tidak menyimpang dari topik utama, serta memberikan gambaran mengenai manfaat yang diharapkan dari hasil penelitian tersebut.

2.3 Mempelajari Literatur Mengenai Pengujian *Vulnerability Assessment (VA)*

Mempelajari literatur tentang pengujian *Vulnerability Assessment* membantu memahami cara mengidentifikasi dan mengatasi kerentanan keamanan pada suatu sistem. Dengan mempelajari literatur ini, kita bisa mengetahui langkah-langkah yang tepat untuk mendeteksi dan memperbaiki celah keamanan sebelum disalahgunakan oleh orang yang tidak bertanggung jawab mengeksploitasinya. Pengetahuan ini sangat penting untuk memastikan bahwa sistem informasi lebih aman dari potensi serangan siber.
Berikut merupakan metodologi umum dalam melakukan VA:

a. **Perencanaan dan Persiapan:** menentukan sistem dan komponen yang akan diuji serta tujuan dan parameter evaluasi.
b. **Pemindaian:** Untuk menemukan kerentanan yang diketahui, sistem dan jaringan dipindai menggunakan teknologi otomatis.
c. **Analisis Kerentanan:** Menentukan tingkat keparahan kerentanan dengan memeriksa hasil pemindaian.
d. **Pelaporan:** Menulis laporan yang mencantumkan kerentanan yang ditemukan, peringkat resiko yang sesuai, dan saran perbaikan.
e. **Perbaikan:** Menangani kerentanan yang telah ditemukan dan memastikan bahwa tindakan perbaikan dilakukan dengan sukses.

2.4 *Testing Website* pada *Tools* VA

Testing website dengan menggunakan *tools Vulnerability Assessment* (VA) adalah proses pengujian untuk mencari dan menganalisis kelemahan atau celah keamanan pada sebuah *website*. Proses ini dilakukan secara otomatis menggunakan alat-alat yang sudah tersedia untuk memindai seluruh bagian *website*, mulai dari tampilan antarmuka hingga struktur kode di dalamnya. *Tools* VA membantu menemukan kelemahan keamanan yang mungkin dieksploitasi oleh peretas, seperti injeksi SQL, skrip lintas situs (XSS), atau kesalahan konfigurasi[12].

Setelah dilakukan pemindaian, *tools* VA akan menghasilkan laporan tentang area-area beresiko, lengkap dengan rincian potensi ancaman yang mungkin terjadi, tingkat keparahan dari masing-masing kerentanan, dan saran perbaikan yang dapat dilakukan untuk mengamankan situs tersebut. Dengan adanya hasil dari proses ini, pengembang atau tim keamanan bisa langsung mengambil langkah pencegahan atau perbaikan agar situs menjadi lebih aman.

2.5 Analisa

a. Analisa Hasil Pengujian

Hasil *scanning* menunjukkan ada beberapa kelemahan di *website* yang diuji. Ini termasuk kelemahan yang berpotensi membahayakan data pengguna, seperti SQL *Injection* dan *Cross-Site Scripting* (XSS). Setiap masalah tersebut diberi penilaian berdasarkan tingkat resikonya, mulai dari yang rendah hingga yang serius. Hasil analisis ini menunjukkan bahwa masih ada bagian dari *website* yang perlu segera diperbaiki agar lebih aman dan tidak mudah diserang oleh peretas yang memiliki kemampuan pemrograman untuk menembus atau melewati sistem keamanan komputer atau jaringan untuk tujuan tertentu di masa depan[13].

b. Analisa Sumber Kerentanan

Sumber kerentanan pada sebuah sistem sering kali muncul dari berbagai faktor. Salah satunya adalah kesalahan dalam konfigurasi atau pengaturan sistem yang tidak optimal. Selain itu, penggunaan perangkat lunak yang sudah lama dan tidak diperbarui secara rutin juga menjadi celah yang bisa dimanfaatkan oleh peretas. Kerentanan juga bisa muncul dari kode program yang memiliki *bug* atau tidak dirancang dengan mempertimbangkan aspek keamanan. Bahkan, faktor manusia seperti ketidaktahuan atau kelalaian dalam menerapkan protokol keamanan yang benar juga bisa menjadi penyebab. Untuk itu, penting dilakukan analisis menyeluruh agar kita bisa mengetahui sumber kerentanan tersebut dan segera mengambil langkah pencegahan yang tepat.

c. Analisa Jenis Celah Keamanan

Analisis celah keamanan bertujuan untuk menemukan titik lemah dalam sistem yang bisa dimanfaatkan oleh peretas. Jenis-jenis celah ini bisa terjadi karena kesalahan dalam kode, pengaturan yang kurang tepat, atau kurangnya perlindungan akses. Contohnya, serangan seperti SQL *Injection*, *Cross-Site Scripting* (XSS), dan *Denial of Service* (DoS) memanfaatkan sejumlah perangkat komputer untuk menyerang sistem target, yang menyebabkan sistem atau layanan tidak dapat diakses oleh pengguna untuk sementara waktu, atau bahkan bisa berlangsung tanpa batas waktu jika sistem tersebut tidak dilindungi dengan baik[14]. Dengan melakukan analisis ini, kita bisa mengetahui di mana letak kerentanannya dan mengambil langkah untuk memperbaikinya agar sistem lebih aman dari serangan.

d. Saran Perbaikan

Saran perbaikan yang dapat diusulkan meliputi peningkatan keamanan dan pengelolaan resiko pada sistem. Langkah ini dapat dilakukan melalui audit berkala untuk memastikan tidak ada celah keamanan baru yang muncul seiring perkembangan teknologi. Selain itu, memperkuat proses autentikasi dan menerapkan kebijakan enkripsi pada data sensitif akan menambah perlindungan sistem. Peningkatan keterampilan bagi tim IT juga diperlukan agar mereka bisa lebih responsif dalam menangani ancaman keamanan.

2.6 Hasil dan Pembahasan

Penulis memaparkan data atau temuan yang diperoleh selama penelitian. Setelah hasil dipaparkan, penulis menjelaskan makna dari data yang ditemukan, menghubungkannya dengan teori atau penelitian sebelumnya. Bagian ini juga menguraikan alasan di balik hasil yang didapat, termasuk menjelaskan faktor yang mungkin mempengaruhi hasil penelitian dan kemungkinan adanya keterbatasan.

3. Hasil dan Pembahasan

Berdasarkan kerangka kerja penelitian yang terdapat pada metode penelitian, terdapat 6 tahapan yang terdiri dari identifikasi masalah penelitian, menentukan tujuan penelitian, mempelajari literatur mengenai pengujian *vulnerability assessment* (VA), *testing website* pada tools (VA), analisa (analisa hasil pengujian, analisa sumber kerentanan, analisa jenis celah keamanan, saran perbaikan), hasil dan pembahasan. Untuk mempermudah dalam melakukan analisa maka penulis membuat bagan alir analisa, guna mempermudah pemahaman seperti pada gambar 2 berikut ini.

Gambar 2. Bagan alir analisis dan hasil

Pada bagan alir di atas, akan dibahas dalam poin pembahasan berikut ini.

3.1 Data

Informasi yang digunakan dalam bagian ini berasal dari pemindaian otomatis atau penilaian kerentanan website UNIPDU Jombang yang dilakukan penulis. Penulis menggunakan alat *Acunetix* untuk memperoleh data ini. Dalam bentuk data celah keamanan di *website*, data alat tersebut merupakan laporan dari prosedur pemindaian yang mematuhi pedoman OWASP Top 10 2021. *Acunetix* merupakan komponen penting dalam pengumpulan data dan dapat berfungsi sebagai standar untuk mengevaluasi hasil studi penilaian kerentanan. Gambar 3 dibawah ini merupakan dasbor utama *website* unipdu jombang.

Gambar 3. Halaman Utama Website Unipdu Jombang

Pemindaian keamanan difokuskan pada domain utama website kampus UNIPDU Jombang, yang berfungsi sebagai pintu gerbang utama bagi siswa untuk mengakses informasi dan layanan kampus secara online. Fokus ini memungkinkan analisis lebih mendalam untuk menemukan ancaman keamanan yang spesifik pada layanan utama kampus. Dengan memfokuskan pemindaian pada domain utama situs web, penulis memastikan bahwa bagian yang paling penting terjamin keamanannya. Hal ini memungkinkan untuk melindungi informasi pengguna dan meningkatkan kepercayaan masyarakat terhadap sistem informasi kampus.

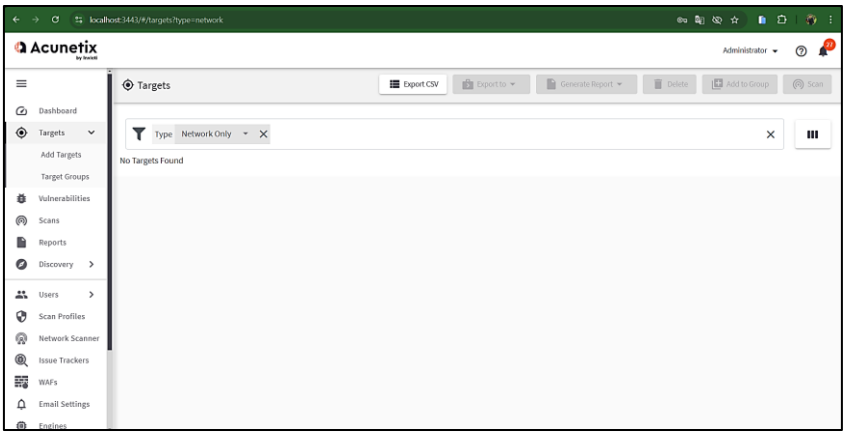
3.2 Acunetix Web Vulnerability

Salah satu metode untuk mengevaluasi keamanan *website* adalah dengan Menggunakan perangkat lunak seperti *Acunetix Vulnerability Scanner*, yang dibuat khusus untuk menemukan kelemahan di *website*,

adalah salah satu cara untuk menilai keamanan *website*. Dalam hal mengidentifikasi kelemahan keamanan seperti injeksi SQL dan XSS, Acunetix adalah salah satu program terbaik yang tersedia [13]. Dalam penyelidikan ini, penulis menggunakan Acunetix versi 14x. *Acunetix* mengkategorikan kerentanan dalam laporan VA menjadi empat tingkat: Peringatan *High Risk Level 3* (resiko sangat tinggi), Peringatan *Medium Risk Level 2* (disebabkan oleh kesalahan konfigurasi server dan kelemahan pengkodean situs), Peringatan *Low Risk Level 1* (biasanya terkait dengan keamanan direktori atau lalu lintas data yang tidak dienkripsi), dan Peringatan Informasional (data yang mungkin merupakan kerentanan, seperti alamat IP atau alamat email).[15]. Data diambil dengan menggunakan *Acunetix Web Vulnerability* melalui tahapan-tahapan berikut:

a. Masukkan Target

Dengan cara Klik button *Targets* ➔ *Add Targets* ➔ *Address*: masukkan *link website* ➔ *Save* ➔ *Scan* ➔ *Create Scan* ➔ Proses.



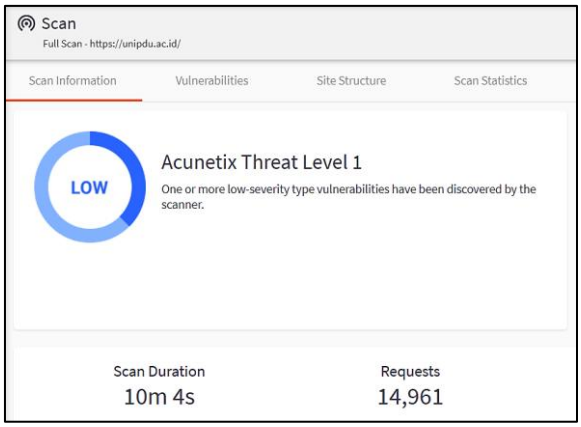
Gambar 4. Menu target

Pada menu target ini, penulis melakukan pengujian melalui link *website* kampus UNIPDU untuk mendeteksi apabila ada celah kerentanan yang memerlukan perbaikan.

b. Tingkat Kerentanan

Pada informasi *scan* ditemukan kerentanan pada *level 1 (Low)* dengan durasi waktu scan otomatis selama 10 menit 4 detik. Meskipun terdapat kelemahan, dampaknya kecil terhadap sistem secara keseluruhan dan tidak memberikan ancaman signifikan terhadap keamanan. Biasanya, level Resiko ini dapat diatasi dengan langkah pencegahan yang cukup sederhana dan tidak memerlukan tindakan perbaikan yang mendesak. Meski begitu, tetap penting untuk mengatasi kerentanan level rendah dan berguna untuk menjaga keamanan sistem secara menyeluruh

.

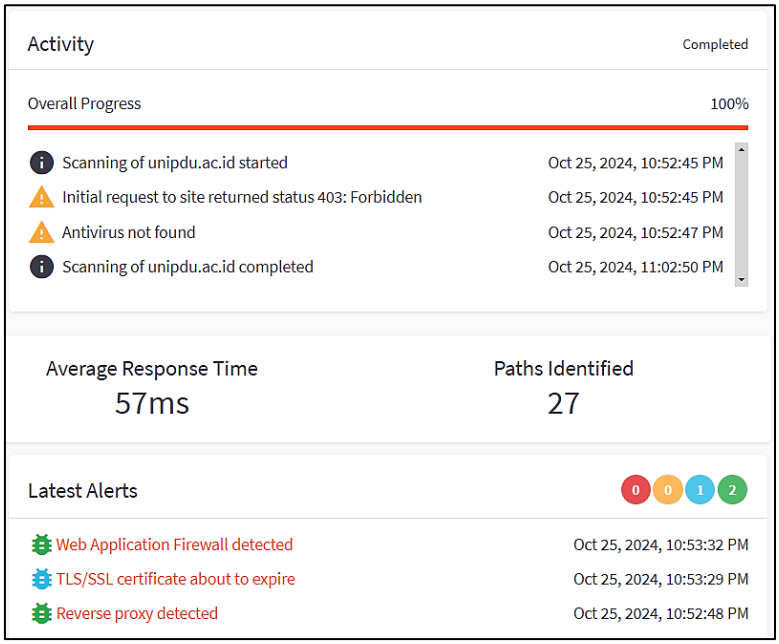


Gambar 5. Tingkat kerentanan

Informasi Target
Menginformasikan target yang didapat dari hasil *scan* meliputi:
1) Address : https://unipdu.ac.id/
2) Server : CloudFlare
3) Operating System : Unknown
4) Teknologi terdeteksi : *Responsive*

Gambar 6. Informasi target

c. Aktivitas *Scan*
Pada gambar 7 dapat dilihat mengenai aktivitas *scanning* dimulai pada tahap ➔ ditemukan pada permintaan awal status 403: dilarang ➔ sistem antivirus tidak ditemukan ➔ *scanning* selesai. Dengan peringatan yang ditemukan 1 berwarna biru yang artinya *low* dan 2 berwarna hijau sebagai informational.



Gambar 7. Aktivitas dan peringatan

Hasil *Acunetix Web Vulnerability*
Hasil dari *acunetix* menggunakan standar *report* OWASP Top 10 2021 sebagai berikut dalam tabel hasil *scanning* kerentanan yang terdeteksi.

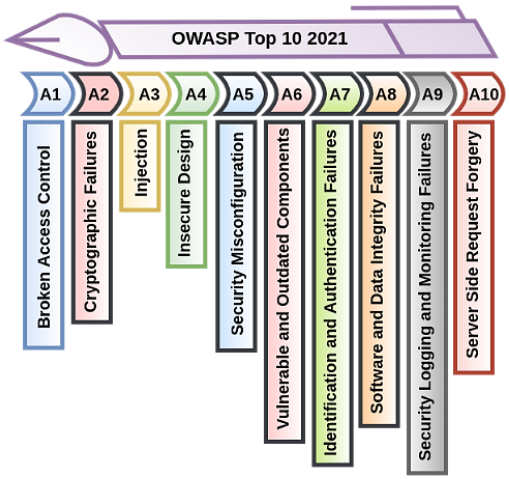
Tabel 1. Hasil *scanning website* UNIPDU

Alerts	***Risk***	**OWASP ID**
TLS/SSL certificate about to expire	*Low*	A05:2021
Reverse proxy detected	*Informasional*	A05:2021
Web Application Firewall detected	*Informasional*	A05:2021
TLS/SSL certificate about to expire	*Low*	A06:2021
Reverse proxy detected	*Informasional*	A06:2021
Web Application Firewall detected	*Informasional*	A06:2021

Berdasarkan informasi dalam tabel 1, enam kerentanan ini dapat diklasifikasikan menurut standar OWASP ID, yang terbagi dalam dua kategori kerentanan yang perlu segera ditangani. Pertama, kerentanan pada (A05) *security misconfiguration*. Artinya kesalahan pengaturan sistem atau aplikasi yang membuka celah keamanan, seperti penggunaan pengaturan default, izin akses yang terlalu longgar, atau kurangnya pembaruan, yang dapat dimanfaatkan oleh penyerang dan kedua, kerentanan pada (A06) *vulnerable and outdated components.* Artinya penggunaan komponen perangkat lunak, seperti *library*, *framework*, atau modul, yang memiliki kelemahan keamanan atau sudah kadaluarsa, sehingga rentan dieksploitasi oleh penyerang[16].

Setelah melakukan *scanning* berulang kali untuk memastikan bahwa peringatan yang ditemukan benar, ditemukan tingkat kerentanan pada *website* UNIPDU yang termasuk dalam dua kategori kerentanan OWASP: A5: *Security Misconfiguration* dan A6: *Vulnerable and Outdated Components*. Pada gambar 8 dibawah ini menunjukkan bahwa situs web tersebut menghadapi masalah berikut:

1. A5: *Security Misconfiguration*
   Terjadi karena pengaturan keamanan yang tidak optimal, seperti konfigurasi server atau aplikasi yang tidak aman, pengaturan default yang tidak diubah, atau kegagalan dalam menerapkan langkah-langkah keamanan yang tepat.
2. A6: *Vulnerable and Outdated Components*
   Mengacu pada penggunaan perangkat lunak, pustaka, atau komponen lain yang sudah ketinggalan zaman atau memiliki kerentanan yang diketahui, namun belum diperbarui atau diperbaiki.



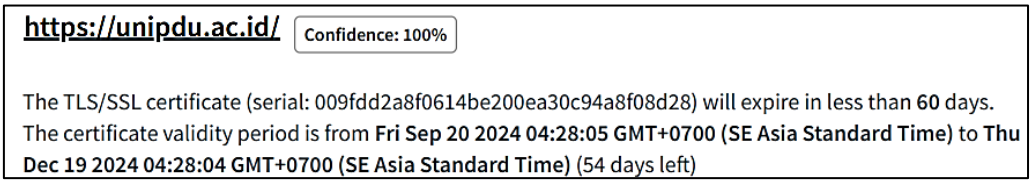
Gambar 8. Kategori Tingkat Kerentanan

Berikut adalah penjelasan mengenai masalah keamanan yang ditemukan pada website UNIPDU. Kerentanan ini dapat mencakup berbagai macam ancaman yang dapat dimanfaatkan oleh pihak tidak berwenang.

1) TLS/SSL *certificate about to expire*

Sertifikat TLS/SSL server akan segera kadaluarsa. Sebagian besar *browser* akan memberitahu pengguna tentang masalah keamanan saat sertifikat kadaluarsa, meminta mereka untuk mengkonfirmasi keabsahan rantai secara manual. Perangkat lunak atau sistem otomatis dapat tiba-tiba berhenti terhubung ke server. Sertifikat perantara juga dapat menjadi sumber peringatan ini, bukan sertifikat server utama (leaf). Untuk

mengetahui sertifikat yang terpengaruh, Anda dapat memeriksa nomor seri sertifikat pada rincian peringatan. Pada gambar 8 merupakan sertifikat TLS/SSL serial.



Gambar 9. Sertifikat number TLS/SSL

Sertifikat SSL yang kadaluarsa dapat memberikan dampak signifikan pada operasional aplikasi web. Jika server aplikasi tetap memproses data tanpa menyadari masalah ini, maka komunikasi yang terjadi berisiko tidak terenkripsi secara aman, membuka peluang bagi peretas untuk melakukan serangan man-in-the-middle atau mencuri data sensitif. Sebaliknya, sistem juga dapat tiba-tiba menghentikan koneksi jika mendeteksi sertifikat yang sudah tidak valid, yang dapat mengganggu layanan kepada pengguna. Untuk mencegah masalah ini, disarankan agar administrator segera menghubungi Otoritas Sertifikat (*Certificate Authority*) guna memperbarui sertifikat SSL, memastikan keamanan komunikasi tetap terjamin dan layanan berjalan dengan lancar.

2) Reverse proxy detected

Reverse proxy detected adalah sebuah server yang berfungsi sebagai perantara di depan *server web*, yang bertugas meneruskan permintaan dari klien (seperti browser) ke server web utama. *Reverse proxy* bertindak sebagai penghubung di depan server asal, memastikan bahwa klien tidak langsung berinteraksi atau berkomunikasi langsung dengan server asal tersebut. Server ini menggunakan *reverse proxy*, penyeimbang beban atau CDN (*Content Delivery Network*) atau di *hosting* pada penyedia *cloud*. *Acunetix* mendeteksi hal ini dengan mengirimkan berbagai muatan dan mendeteksi perubahan pada header dan tubuh.

Pada tahap pengujian ini, mengidentifikasi adanya sistem pelindung pada website agar pengguna tidak berinteraksi secara langsung dengan website. Hal ini mengindikasikan bahwa area yang diuji telah memiliki tingkat perlindungan yang memadai. Namun, langkah pengawasan dan peningkatan sistem secara berkelanjutan tetap diperlukan untuk mengantisipasi ancaman yang mungkin muncul di masa mendatang.

3) Web Application Firewall detected

Firewall aplikasi web ditemukan. Sistem seperti *Intrusion Prevention System* (IPS), *Intrusion Detection System* (IDS), atau *firewall* aplikasi web (WAF) telah diterapkan untuk melindungi server ini. Dengan mengirimkan berbagai ancaman dan melacak modifikasi pada kode response, header, dan isi, *Acunetix* dapat mengidentifikasi hal ini.

Pemindaian server yang dilindungi oleh sistem keamanan seperti *Intrusion Prevention System* (IPS), *Intrusion Detection System* (IDS), atau *Web Application Firewall* (WAF) memiliki risiko menghasilkan hasil yang tidak akurat atau tidak lengkap. Hal ini terjadi karena mekanisme perlindungan tersebut dapat menghalangi akses pemindai ke bagian tertentu dari server atau memfilter aktivitas yang dianggap mencurigakan. Selain itu, jika WAF mendeteksi aktivitas pemindaian sebagai ancaman, alamat IP pemindai dapat diblokir setelah beberapa percobaan, sehingga menghambat proses analisis lebih lanjut. Kondisi ini dapat mengurangi efektivitas pemindaian dalam mengidentifikasi kerentanan yang ada pada sistem.

Selanjutnya pada host *https://unipdu.ac.id/* Terdeteksi *CloudFlare* WAF dari *header*. Dengan memuat permintaan HTTP sebagai berikut.

```
GET /9338521 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: unipdu.ac.id
Connection: Keep-alive
```

Gambar 10. Request HTTP

Disarankan untuk melakukan pemindaian pada versi internal (*development*) aplikasi web, di mana Web *Application Firewall* (WAF) tidak aktif. Hal ini memungkinkan pengujian berjalan lebih efektif tanpa adanya interferensi dari lapisan perlindungan WAF, sehingga kerentanan yang sebenarnya dapat terdeteksi dengan lebih akurat sebelum aplikasi diimplementasikan ke lingkungan produksi.

4. Kesimpulan

Penelitian ini bertujuan untuk mengevaluasi keamanan pada *website* utama kampus UNIPDU Jombang dengan domain *https://unipdu.ac.id/*. Evaluasi dilakukan menggunakan metode *Vulnerability Assessment* (VA) dengan memanfaatkan *tools* otomatis *Acunetix versi 14x*. risiko, mulai dari Informational, *Low Risk Level 1*, *Medium Risk Level 2*, hingga *High* Dalam pengujian ini, berbagai kelemahan keamanan berhasil diidentifikasi dan dikelompokkan berdasarkan tingkat *Risk Level* 3. Temuan utama meliputi potensi masalah serius seperti hampir kadaluarsanya sertifikat TLS/SSL, keberadaan *reverse proxy* yang menggunakan layanan cloud seperti *CloudFlare*, serta implementasi *Web Application Firewall* (WAF) sebagai sistem perlindungan *website*. Penanganan prioritas diberikan pada sertifikat TLS/SSL yang hampir kadaluarsa dengan memberikan rekomendasi kepada administrator untuk menghubungi Otoritas Sertifikat guna melakukan pembaruan. Setelah dilakukan perbaikan, masalah tersebut berhasil diatasi. Dua temuan lainnya, meskipun hanya bersifat informational, tetap memberikan kontribusi penting dalam proses evaluasi. Secara keseluruhan, langkah pemindaian dan rekomendasi yang diberikan berhasil meningkatkan keamanan *website* dan memberikan kenyamanan lebih bagi pengguna.
\

Daftar Pustaka

[1] A. Zaini dan R. Wijanarko, "Jurnal Informatika dan Rekayasa Perangkat Lunak Analisis Keamanan Website Menggunakan Standar Keamanan Open Web Application Security Project (OWASP) Studi Kasus Website Penerimaan Mahasiswa Baru Universitas Wahid Hasyim Semarang," vol. 5, no. 2, 2023.

[2] najwashihab, "Indonesia (Terlalu) Sering Diretas. Sederet Kasus Peretasan Terhadap Kementerian/Lembaga Negara," https://www.instagram.com/najwashihab?utm_source=ig_web_button_share_sheet&igsh=ZDNlZDc0MzIxNw%3D%3D. Diakses: 27 November 2024. [Daring]. Tersedia pada: https://www.instagram.com/p/C8vujPnyf6s/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA%3D%3D

[3] I. Riadi, A. Yudhana, dan Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, hal. 853–860, 2020, doi: 10.25126/jtiik.2020701928.

[4] M. S. Ummah, Belajar Pemrograman Web Dasar HTML, CSS & Skrip Java Untuk Pemula, vol. 11, no. 1. 2019.. Tersedia pada: http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI

[5] PT Widya Adijaya Nusantara, "B2B Sangat Membutuhkan Penetration Testing," widyasecurity.com. Diakses: 27 November 2024. [Daring]. Tersedia pada: https://widyasecurity.com/tag/penetration-testing/page/12/

[6] C. Darmawan, J. Panda, P. Naibaho, dan A. De Kweldju, "Edumatic: Jurnal Pendidikan Informatika Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021," vol. 8, no. 1, hal. 272–281, 2024, doi: 10.29408/edumatic.v8i1.25834.

[7] M. Yaqi, *Vulnerability Assessment dan Penetration Testing (Vapt) Menggunakan Metode Zero Entry Hacking (Zeh) Terhadap Website Studi Kasus: Dinas Penanaman Modal …*. 2023. Tersedia pada: https://repository.uinjkt.ac.id/dspace/handle/123456789/73422%0Ahttps://repository.uinjkt.ac.id/dspace/bitstream/123456789/73422/1/MUHAMMAD YAQI-FST.pdf

[8] N. Hayaty, "Buku Ajar: Sistem Keamanan," hal. 1–99, 2020.

[9] Mira Orisa dan M. Ardita, "Vulnerability Assessment Untuk Meningkatkan Kualitas Keamanan Web," *J. Mnemon.*, vol. 4, no. 1, hal. 16–19, 2021, doi: 10.36040/mnemonic.v4i1.3213.
[10] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, hal. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.
[11] M. I. Fadillah, U. Yunan, K. S. Yanto, dan M. Fathinuddin, "Analisis Security Mitigation dengan Metode Vulnerability Assessment and Penetration Testing (VAPT) (Kasus Website Kerja Praktek dan Pengabdian Masyarakat)," *J. Sains Komput. Inform. (J-SAKTI*, vol. 7, no. 2, hal. 753–764, 2023.
[12] A. Zirwan, "Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner," *J. Inf. dan Teknol.*, vol. 4, no. 1, hal. 70–75, 2022, doi: 10.37034/jidt.v4i1.190.
[13] J. T. Santoso, *Hacker dengan Linux*. 2022.
[14] F. C. B. Wicaksono dan I. M. Suartana, "Deteksi Serangan Denial Of Service (DoS) pada Cloud Menggunakan Security Onion," *JINACS (Journal Informatics Comput. Sci.*, vol. 5, no. 1, hal. 111–118, 2023.
[15] F. Al Fajar, "Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web Vulnerability," *Inova-Tif*, vol. 3, no. 2, hal. 110, 2020, doi: 10.32832/inova-tif.v3i2.4127.
[16] owasp.org, "OWASP Top 10:2021," https://owasp.org/. Diakses: 27 November 2024. [Daring]. Tersedia pada: https://owasp.org/Top10/id/