INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 8, Tahun 2026, Hal. 847-859, ISSN: 3123-5573 (Online)

Identifikasi Kerentanan Website Universitas Subang Menggunakan Acunetix

Muhammad Arif Amrullah[1], Ardi Ilahi Roby[2], Ramdan Prayitno[3]
[1,2,3]*Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Subang*
e-mail: [1]muhammadarif28392@gmail.com, [2]ardiilahiroby12@gmail.com, [3]Ramdanprayitno8@gmail.com

Article Info

Article history:

Received May 15, 2026
Revised June 11, 2026
Accepted June 13, 2026

Keywords:

Vulnerability, Assessment, Website, Universitas Subang, Acunetix, Clickjacking.

ABSTRACT

The official website of Subang University serves as the digital center for academic, administrative, and institutional information services. Website security is crucial to prevent sensitive data leaks and ensure the best service for the academic community. The method used in this study is Vulnerability Assessment (VA) with a Dynamic Application Security Testing (DAST) approach through a non-destructive Black Box testing scheme. The primary scan using the Acunetix Web Vulnerability Scanner resulted in 6,158 requests with an overall threat level of Low. One security vulnerability was found in the form of Clickjacking: X-Frame-Options header missing and 14 informational findings, with no High or Medium level vulnerabilities. To ensure the validity of the findings, this study conducted cross-tool validation using Helium Scanner, HostedScan Nmap, and OWASP ZAP. The cross-tool validation results confirmed the presence of Cloudflare's Web Application Firewall (WAF) which effectively protects the institution's network infrastructure from fatal exploits. The conclusion of this study shows that the network architecture of Subang University is solid, so the absolute focus of mitigation is directed at patching HTTP Security Headers misconfigurations to minimize the potential for UI Redress and MIME-Sniffing attacks.

Article Info

Article history:

Received May 15, 2026
Revised June 11, 2026
Accepted June 13, 2026

Kata Kunci:

Vulnerability, Assessment, Website, Universitas Subang, *Acunetix, Clickjacking.*

ABSTRAK

Website resmi Universitas Subang digunakan sebagai pusat layanan akademik, administrasi, dan informasi institusi secara digital. Keamanan website tersebut merupakan hal yang sangat krusial untuk mencegah kebocoran data sensitif dan menjamin layanan terbaik bagi civitas akademika. Metode yang digunakan dalam penelitian ini adalah *Vulnerability Assessment* (VA) dengan pendekatan *Dynamic Application Security Testing* (DAST) melalui skema pengujian *Black Box* secara *non-destructive*. Pemindaian utama menggunakan Acunetix Web Vulnerability Scanner menghasilkan 6.158 *request* dengan tingkat ancaman keseluruhan berada pada level *Low*. Ditemukan 1 celah keamanan berupa *Clickjacking: X-Frame-Options header missing* dan 14 temuan bersifat *Informational*, tanpa adanya kerentanan tingkat *High* atau *Medium*. Guna memastikan validitas temuan, penelitian ini melakukan pengujian silang (*cross-tool validation*) menggunakan Helium Scanner, HostedScan Nmap, dan OWASP ZAP. Hasil pengujian silang mengonfirmasi keberadaan *Web Application Firewall* (WAF) Cloudflare yang secara efektif melindungi infrastruktur jaringan institusi dari eksploitasi fatal. Kesimpulan penelitian ini menunjukkan bahwa arsitektur jaringan Universitas Subang sudah solid, sehingga fokus mitigasi mutlak diarahkan pada penambalan miskonfigurasi *HTTP Security Headers*

untuk meminimalisir potensi serangan *UI Redress* dan *MIME-Sniffing*.

Corresponding Author:

Muhammad Arif Amrullah
Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Subang
e-mail: [1]muhammadarif28392@gmail.com

PENDAHULUAN

Website resmi Universitas Subang adalah sebuah portal informasi dan layanan akademik institusi yang dapat diakses secara digital. Tujuannya guna mempermudah mahasiswa, staf, dan masyarakat umum dalam mengakses layanan administrasi, data akademik akademik, serta publikasi hasil penelitian secara online. Saat ini, website tersebut berfungsi sebagai pusat layanan utama institusi dan dapat diakses melalui tautan https://unsub.ac.id.

Di era digitalisasi, bertambahnya ketergantungan pada sistem digital berbanding lurus dengan ancaman keamanan siber. Website universitas menyimpan berbagai data sensitif, yang menuntut jaminan integritas, kerahasiaan, dan ketersediaan sistem informasi (Alwi et al., 2020). Semakin banyak pihak yang menyalahgunakan layanan internet, sehingga kegagalan dalam menjamin keamanan siber dapat berakibat pada pelanggaran regulasi privasi, kebocoran data pribadi, hingga disrupsi layanan akademik. Hal ini seringkali dieksploitasi oleh peretas, yang secara serius dapat merusak reputasi dan kredibilitas institusi (Schneier, n.d.)

Diperlukan adanya analisis keamanan yang bertujuan untuk mengetahui seberapa jauh tingkat kerentanan pada website utama Universitas Subang. Fokus penelitian ini adalah pada evaluasi *vulnerability* menggunakan pendekatan *Dynamic Application Security Testing* (DAST) dengan alat pemindai Acunetix. Rumusan masalah dalam penelitian ini adalah bagaimana mengetahui tingkat risiko keamanan aktual pada website Universitas Subang menggunakan Acunetix Web Vulnerability, dengan tujuan untuk mengukur tingkat risiko, menganalisis kerentanan khusus seperti *Clickjacking*, dan memberikan rekomendasi mitigasi. Metode penelitian yang digunakan adalah *Vulnerability Assessment* guna mendapatkan dokumentasi hasil yang valid dan menjadi kontrol preventif. Penelitian ini menggunakan tools Acunetix, yaitu perangkat lunak yang dikembangkan untuk melakukan pemindaian sistem secara mendalam. Kelebihannya adalah kemampuan yang terbukti dalam menemukan semua kerentanan umum, kelemahan yang diabaikan, hingga kesalahan konfigurasi tingkat rendah pada *server header*.

Berikut beberapa tinjauan pustaka yang peneliti gunakan sebagai acuan dalam penelitian ini: (Syafaat, 2024) dalam penelitiannya melakukan pengujian keamanan sistem informasi secara spesifik pada level fakultas di lingkungan Universitas Subang. Penelitian tersebut memanfaatkan metodologi standar dari OWASP untuk menganalisis celah keamanan, yang menjadi landasan penting mengenai urgensi evaluasi keamanan berkelanjutan di lingkungan institusi kampus. (Al Fajar, 2020) berfokus pada analisis keamanan sistem informasi akademik menggunakan *Acunetix Web Vulnerability*. Hasil penelitiannya menunjukkan bahwa audit keamanan menggunakan tools tersebut merupakan langkah preventif yang krusial, efektif, dan akurat untuk mencegah eksploitasi kerentanan pada aplikasi *web* universitas. (Zirwan, 2022) melakukan studi terkait pengujian dan analisis keamanan

website menggunakan *Acunetix Vulnerability Scanner*. Penelitian tersebut membuktikan efektivitas pemindai Acunetix yang tidak hanya berfokus pada deteksi risiko tinggi, melainkan juga sangat detail dalam menemukan dan mengklasifikasikan kerentanan tingkat rendah (*low-level risk*) hingga tingkat informasional (*informational alerts*). (Wibowo et al., 2019) dalam penelitiannya melakukan evaluasi kerentanan pada *website* akademik, khususnya portal jurnal ilmiah universitas, menggunakan alat pemindai Acunetix WVS. Hasil penelitian tersebut menegaskan bahwa identifikasi celah keamanan secara rutin menggunakan metode *vulnerability assessment* sangat krusial sebagai kontrol preventif untuk mencegah eksploitasi sistem informasi di lingkungan perguruan tinggi. (Kristianto et al., 2022) melakukan penelitian terkait celah keamanan dan miskonfigurasi keamanan website menggunakan metode *vulnerability assessment* berbasis Acunetix. Menurut penelitian tersebut, pemindaian otomatis sangat penting untuk mendeteksi kerentanan yang sering diabaikan pengelola situs, termasuk mitigasi terhadap kerentanan serangan *UI Redress* seperti *Clickjacking* dan tidak adanya proteksi header keamanan yang memadai.

Berdasarkan beberapa tinjauan pustaka di atas, terdapat celah penelitian (*research gap*) yang mendasari urgensi penelitian ini. Meskipun pengujian keamanan menggunakan Acunetix telah terbukti efektif dalam mendeteksi berbagai kerentanan, evaluasi keamanan siber di lingkungan Universitas Subang sejauh ini masih terbatas pada aplikasi spesifik atau tingkat fakultas saja. Belum ada publikasi dan dokumentasi yang secara spesifik, menyeluruh, dan komprehensif mengevaluasi postur keamanan domain utama institusi (https://unsub.ac.id). Oleh karena itu, penelitian ini hadir untuk mengisi celah tersebut dengan memfokuskan pengujian pada domain utama universitas.

Hasil dari penelitian ini diharapkan tidak hanya sekadar memberikan gambaran metrik tingkat kerentanan secara teoritis, tetapi juga dapat menjadi acuan praktis dan rekomendasi mitigasi teknis bagi tim pengelola sistem informasi atau administrator IT di Universitas Subang. Melalui identifikasi celah konfigurasi sejak dini, institusi dapat melakukan langkah penambalan (*patching*) untuk memperkuat keamanan server sebelum celah tersebut dieksploitasi oleh pihak yang tidak bertanggung jawab. Adapun sistematika penulisan pada penelitian ini disusun sebagai berikut: Bagian 2 memaparkan Metodologi Penelitian yang mencakup tahapan pengujian menggunakan Vulnerability Assessment; Bagian 3 menyajikan Hasil dan Pembahasan dari proses pemindaian dan analisis risiko; serta Bagian 4 berisi Kesimpulan yang merangkum hasil temuan keseluruhan beserta saran.

METODE

Penelitian ini menggunakan metode *Vulnerability Assessment* (VA) untuk mengevaluasi postur keamanan informasi pada website resmi Universitas Subang (https://unsub.ac.id). Pendekatan yang diterapkan adalah *Dynamic Application Security Testing* (DAST), di mana pengujian dilakukan pada aplikasi web yang sedang berjalan (runtime) untuk mengidentifikasi celah keamanan yang dapat dieksploitasi dari luar jaringan.

Teknik pengumpulan data dalam penelitian ini menggunakan metode observasi non-partisipan. Peneliti bertindak sebagai pengamat luar yang melakukan interaksi dengan target evaluasi tanpa memiliki akses ke dalam kode sumber (*source code*) maupun struktur basis data server. Oleh karena itu, skema pengujian yang digunakan adalah *Black Box Testing.* Seluruh proses pengujian bersifat *non-destructive penetration testing*, yang berarti pemindaian hanya dilakukan sebatas untuk mengidentifikasi dan memetakan kerentanan tanpa melakukan eksploitasi yang dapat merusak, mengubah data, atau mengganggu operasional layanan akademik universitas.

Alat Penelitian

Pemindaian kerentanan utama pada penelitian ini diotomatisasi menggunakan perangkat lunak *Acunetix Web Vulnerability Scanner*. Acunetix dipilih karena kemampuannya dalam melakukan proses *crawling* secara mendalam dan mengklasifikasikan tingkat ancaman berdasarkan standar global. Selain itu, guna mencegah *false negative* dan memastikan validitas postur keamanan secara menyeluruh, penelitian ini mengintegrasikan tiga alat bantu tambahan sebagai metode validasi silang (*cross-tool validation*), yaitu:

1. **Helium Scanner:** Digunakan untuk memetakan Attack Surface dan reputasi target infrastruktur.
2. **HostedScan (Nmap):** Digunakan untuk melakukan port scanning guna mengevaluasi lapisan transport dan ketahanan firewall.
3. **OWASP ZAP:** Digunakan sebagai instrumen open-source pendamping DAST untuk memvalidasi kerentanan pada lapisan aplikasi dan HTTP Header.

Tahapan Penelitian

Secara teknis, proses *Vulnerability Assessment* dalam penelitian ini dipecah menjadi tiga tahapan inti yang dilakukan secara berurutan guna memastikan validitas hasil. Berikut adalah uraian tahapan penelitian tersebut:

1. Tahap Persiapan dan Pemindaian (*Vulnerability Scanning)*

Tahap awal ini berfokus pada penentuan target (URL) dan konfigurasi alat pemindai. Acunetix diatur untuk melakukan *crawling* pada seluruh struktur tautan dan direktori publik yang ada pada *website* target. Setelah *crawling* selesai, sistem akan secara otomatis meluncurkan ribuan request (*payload pengujian*) ke server target dan merekam waktu respons (*response time*). Pada tahap ini, *scanner* akan mencari pola-pola yang cocok dengan basis data kerentanan yang dikenal, seperti miskonfigurasi keamanan, kelemahan pada *server header*, hingga kerentanan injeksi. Untuk memastikan validitas data, proses pemindaian dilakukan sebanyak dua kali pengujian.

2. Tahap Analisis Hasil (*Result Analysis*)

Setelah proses pemindaian mencapai 100%, tahap selanjutnya adalah menganalisis data mentah yang dihasilkan oleh Acunetix. Sistem akan secara otomatis mengkategorikan kerentanan yang ditemukan ke dalam empat tingkat keparahan (*Severity Level*), yaitu:

a) *High Risk*, Kerentanan kritis yang dapat memungkinkan pengambilalihan sistem atau pencurian data fatal.
b) *Medium Risk*, Kerentanan yang berpotensi membahayakan sebagian sistem atau membutuhkan manipulasi tambahan oleh penyerang.
c) *Low Risk*, Kerentanan berupa miskonfigurasi ringan yang mengekspos informasi sistem atau membuka celah serangan tingkat rendah seperti *Clickjacking* atau masalah pada lapisan *user interface* (UI).
d) *Informational*, Temuan berupa informasi umum tentang struktur server yang tidak langsung berbahaya, namun dapat membantu proses mitigasi.

Pada tahap ini, peneliti secara khusus melakukan telaah mendalam terhadap kerentanan di level *Low* terkait *X-Frame-Options header missing* untuk memahami mekanisme potensial serangan *UI Redress*.

3. Tahap Pelaporan dan Mitigasi (*Reporting*)

Tahap terakhir dari metode penelitian ini adalah mendokumentasikan seluruh temuan secara komprehensif ke dalam bentuk pelaporan akademik. Laporan ini tidak hanya memaparkan metrik kerentanan dan jumlah *request* yang dilakukan oleh *scanner*, tetapi juga merumuskan rekomendasi perbaikan (*patching*). Peneliti menyusun panduan mitigasi teknis yang spesifik dan *actionable* khususnya terkait implementasi kontrol kebijakan keamanan konten (*Content-Security-Policy*) pada server yang nantinya dapat direkomendasikan kepada pihak administrator IT Universitas Subang.

Gambar 1. Diagram Alur Pengujian

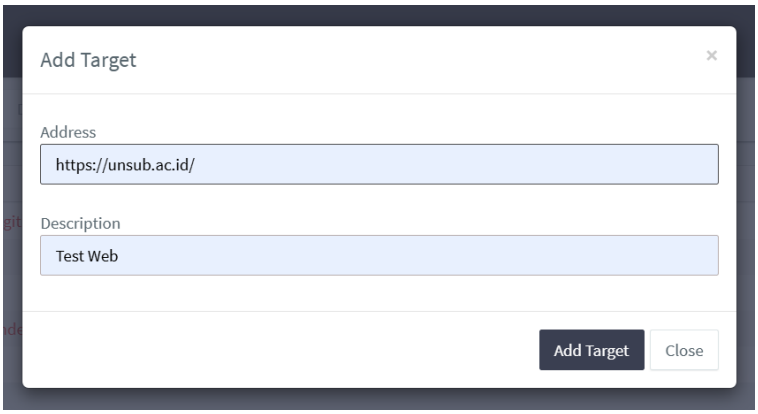
HASIL DAN PEMBAHASAN

Kerentanan website dianalisis menggunakan software Acunetix web Vulnerability dengan tahapan sebagai berikut:

A. Implementasi Pemindaian

1) *Add Target*

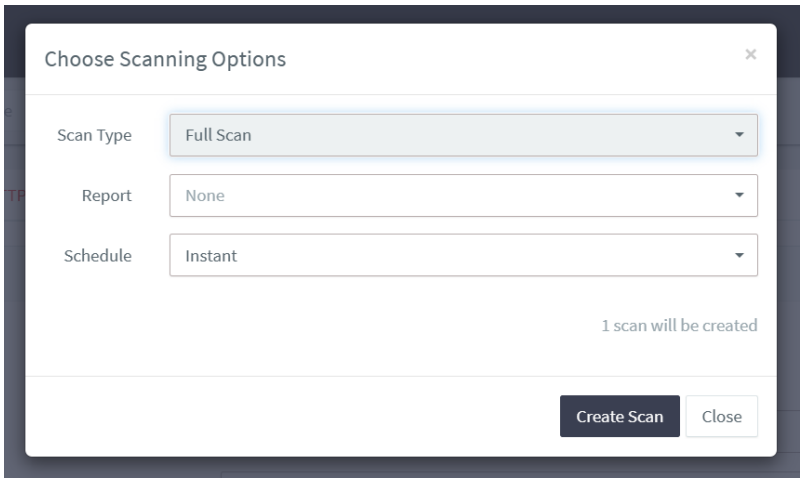
Proses *add target* merupakan langkah awal dengan menginput URL target address dan deskripsi. Pengujian ini difokuskan pada domain utama dengan memasukkan alamat https://unsub.ac.id seperti yang terlihat pada Gambar 2.



Gambar 2. *Add Target* (httpss://unsub.ac.id)

2) *Vulnerability Scanning*

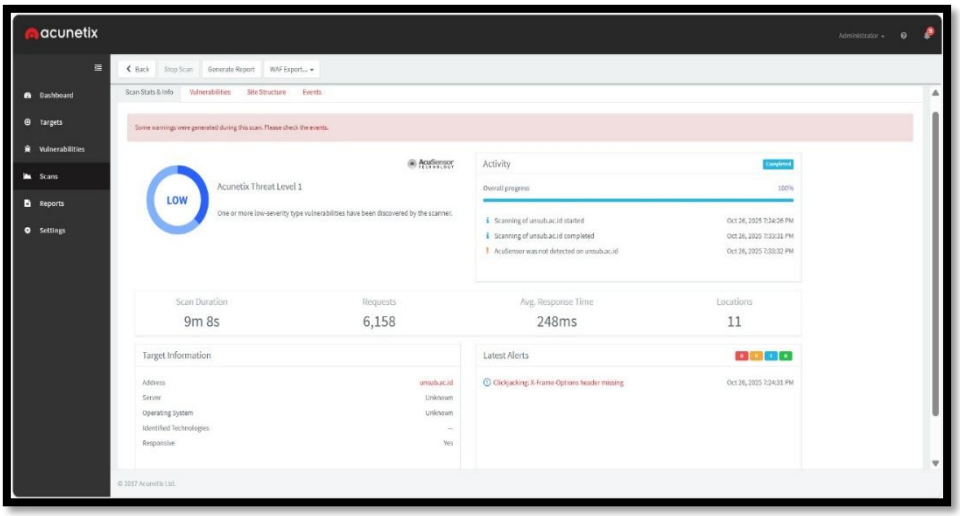
Terdapat 6 tipe scanning pada Acunetix yaitu *full scan, high risk vulnerabilities, Cross-Site Scripting vulnerability, sql injection vulnerability, weak password, dan crawl only.* Penelitian ini menggunakan tipe *full scan* agar bisa mendapatkan hasil kerentanan website secara keseluruhan.



Gambar 3. *Vulnerability Scanning*

B. Hasil Pemindaian

Berdasarkan pemindaian kerentanan website https://unsub.ac.id menggunakan Acunetix Web Vulnerability Scanner, maka didapatkan hasil sebagai berikut:



Gambar 4. Hasil Pemindaian Kerentanan Website Universitas Subang (Sumber: Acunetix, 2025)

C. Data Kuantitatif Pemindaian

Pengujian menggunakan *Web Vulnerability Scanner* (WVS) Acunetix yang dilakukan secara non-destruktif. Data kuantitatif proses pemindaian dicatat untuk memvalidasi intensitas dan cakupan hasil pengujian.

Tabel 1. Data Kuantitatif Statistik Pemindaian Acunetix

Parameter	Data Hasil Pemindaian	Keterangan
URL Target	https://unsub.ac.id	Target utama pengujian.
Profil Pemindaian	Full Scan	Cakupan pemindaian maksimal.
Total Permintaan *(Request)*	6.158	Volume interaksi yang dikirim oleh scanner.
Total Waktu Pemindaian	9 menit 8 detik	Durasi yang relative cepat utuk pemindaian full scan.
Average Response Time	248 ms	Kecepatan rata-rata respons server.
Status Pemindaian	100% Completed	Proses pemindaian selesai dengan sempurna

Berdasarkan Tabel 1, *scanner* berhasil meluncurkan 6.158 *request* dalam durasi 9 menit 8 detik. Volume *request* yang masif ini merepresentasikan proses *crawling* yang mendalam terhadap seluruh struktur tautan dan direktori publik, dengan *average response time* sebesar 248 ms yang mengindikasikan stabilitas server selama pengujian berlangsung.

D. Ringkasan Tingkat Risiko

Berdasarkan hasil pemindaian yang diselesaikan 100%, website Universitas Subang menunjukan profil risiko kerentanan yang secara keseluruhan rendah. Tabel 2 menyajikan klasifikasi temuan berdasarkan Acunetix *Threat Level*.

Tabel 2. Ringkasan Tingkat Risiko Kerentanan

Tingkat Risiko	Klasifikasi Acunetix	Jumlah Temuan
High	Critical/High	0
Medium	Medium	0
Low	Low	1
Informational	Informational	14
Total		15

Hasil pemindaian Acunetix membagi temuannya menjadi beberapa kategori, bukan hanya kerentanan yang dapat dieksploitasi. Berikut adalah 2 tingkat kerentanan:

a) Kerentanan Keamanan (*Vulnerabilities*), Tidak ditemukan adanya celah kritis, dengan perincian tingkat HIGH (0 temuan) dan MEDIUM (0 temuan). Hal ini menjadi indikator positif bahwa sistem telah terhindar dari kerentanan umum yang fatal seperti *SQL Injection* atau *Cross-Site Scripting* (XSS). Terdapat 1 kerentanan di tingkat LOW berupa *Clickjacking: X-Frame-Options header missing*.
b) Temuan informasi (*Infortmational*), Terdapat 14 temuan pada kategori ini. Temuan ini umumnya berupa identifikasi versi *web server*, *file path* yang terekspos, serta *header* pendukung yang hilang. Meski tidak berstatus kritis, dalam kerangka keamanan siber (fase *reconnaissance*), informasi arsitektur server yang terekspos dapat dimanfaatkan oleh pihak luar untuk menyusun vektor serangan yang lebih terarah.

PEMBAHASAN

1. Analisis Kerentanan Spesifik: *Clickjacking*

Dari total 15 temuan, fokus celah keamanan yang menjadi temuan utama adalah *Clickjacking: X-Frame-Options Header Missing* (Tingkat LOW). Secara teknis, hal ini terjadi

karena server tidak mengirimkan HTTP *security header* X-Frame-Options pada respons halaman, baik di halaman utama maupun beberapa halaman publik lainnya.

Absennya header ini membuka celah terhadap skenario serangan *UI Redress*. Dalam skenario ini, penyerang dapat memuat halaman portal universitas ke dalam elemen iframe pada domain pihak ketiga (situs berbahaya) yang dikendalikan oleh penyerang. Pengguna yang tertipu dapat melakukan klik pada elemen transparan yang ditempatkan di atas halaman asli universitas, sehingga secara tidak sadar mereka melakukan interaksi (seperti pengiriman formulir atau navigasi) tanpa otorisasi yang disengaja.

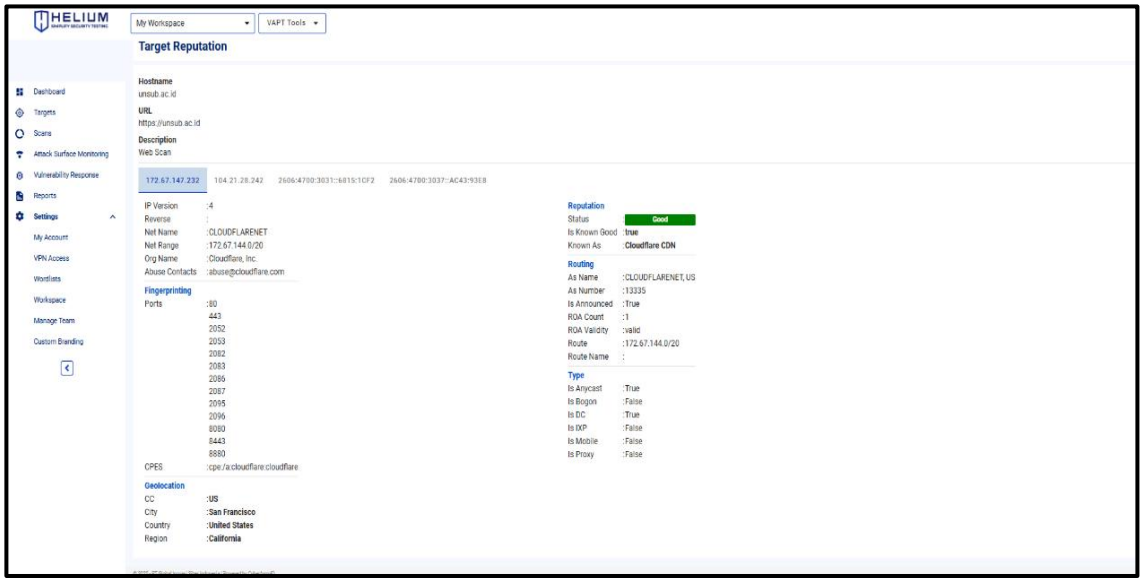
2. Interpretasi Hasil dan Tujuan Penelitian

Hasil penelitian ini membuktikan bahwa tujuan evaluasi risiko keamanan telah tercapai, dengan postur keamanan saat ini berada pada tingkat LOW. Ketiadaan kerentanan HIGH atau MEDIUM menunjukkan bahwa sistem institusi telah menerapkan validasi input dasar yang cukup kuat. Namun, kelemahan pada konfigurasi *server header* (*Missing Anti-Clickjacking Header*) secara langsung melanggar prinsip Integritas (*Integrity*) di dalam CIA Triad, karena penyerang berpotensi memanipulasi tindakan akhir dari pengguna.

Jika ditinjau dari implikasi praktis, risiko terbesar tidak terletak pada kebocoran basis data (*data breach*), melainkan pada risiko reputasi. Pihak yang tidak bertanggung jawab dapat menyalahgunakan citra antarmuka institusi untuk mengelabui mahasiswa atau staf akademik.

3. Validasi Infrastruktur Eksternal Menggunakan Helium Scanner

Guna memperkuat validitas temuan pada kategori Informational yang dihasilkan oleh Acunetix, penelitian ini melakukan pengujian tandingan (*cross-tool validation*) menggunakan *platform* keamanan berbasis *cloud*, Helium. Fokus pemindaian pada Helium diarahkan pada pemetaan reputasi target (*Target Reputation*) dan *port fingerprinting* untuk menganalisis perimeter eksternal jaringan Universitas Subang.



Gambar 5. Hasil Analisis Infrastruktur dan Reputasi Target Menggunakan Helium

Data hasil pemindaian infrastruktur dari Helium menyajikan informasi teknis mendalam yang merangkum postur jaringan domain utama universitas. Rangkuman hasil deteksi dapat dilihat pada Tabel 3.

Tabel 3. Data Intelijen Jaringan *(Helium Scanner)*

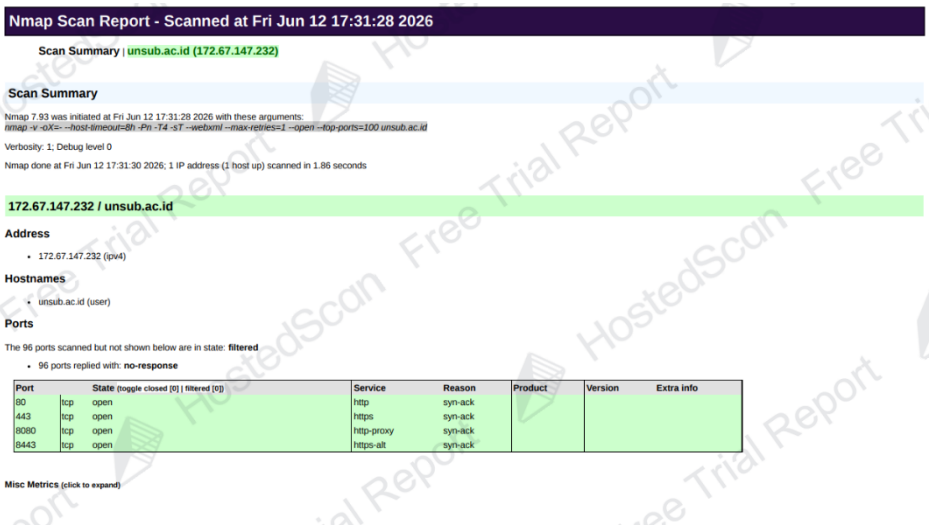
Parameter Deteksi	Hasil Keluaran (Output)	Keterangan
IP Addres Utama	172.67.147.232	IP yang terekspos ke publik (*Anycast*).
Network Name (ASN)	CLOUDFLARENET (AS13335)	Jaringan dikelola oleh infrastruktur pihak ketiga.
Status Reputasi	*Good* (Dikenal sebagai Cloudflare CDN)	Domain memiliki reputasi bersih dan tidak masuk dalam daftar hitam (*blacklist*).
Geolocation	San Francisco, California, US	Lokasi perutean server proksi (*node* Anycast).
Port Fingerprinting	80, 443, 2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8080, 8443, 8880	*Port* HTTP/HTTPS standar dan proksi panel kontrol yang terbuka secara eksternal.

Berdasarkan hasil analisis silang tersebut, terungkap beberapa temuan krusial terkait arsitektur pertahanan sistem:

a) *Implementasi Content Delivery Network* (CDN) dan WAF: Helium secara definitif mendeteksi bahwa lalu lintas menuju https://unsub.ac.id diarahkan melalui CLOUDFLARENET. Penggunaan layanan proksi terbalik (*reverse proxy*) dari Cloudflare ini bertindak ganda sebagai CDN dan *Web Application Firewall* (WAF). Keberadaan lapisan WAF ini menjadi justifikasi teknis mengapa pemindaian intensif (6.158 *request*) oleh Acunetix sebelumnya tidak menyebabkan server down, dan mengapa tidak ditemukan kerentanan injeksi tingkat *HIGH* atau *MEDIUM*. Sistem pertahanan tepi (*edge defense*) *Cloudflare* telah menyaring muatan berbahaya (*malicious payloads*) sebelum mencapai server asal (*origin server*).
b) Pemetaan Lapisan Permukaan (*Attack Surface*): Hasil Port *Fingerprinting* menunjukkan adanya 13 port terbuka yang identik dengan port proksi standar Cloudflare (mendukung trafik web dan akses panel kontrol seperti cPanel/WHM yang disamarkan). Meski terbuka, port ini dirutekan secara aman (status Reputation: Good), sehingga mempersempit vektor serangan berbasis jaringan (*network-based attacks*).
c) Sintesis Temuan: Pengujian dengan Helium mengonfirmasi bahwa institusi telah memiliki lapisan pertahanan infrastruktur (perimeter) yang solid. Fakta ini semakin memperkuat urgensi mitigasi pada temuan utama Acunetix, yaitu *Clickjacking*. Mengingat firewall infrastruktur sudah dikonfigurasi dengan baik, penyerang akan mengalihkan fokus pada manipulasi antarmuka klien (*UI Redress*) yang mengeksploitasi header *HTTP* yang hilang, karena serangan jenis ini kerap lolos dari penyaringan WAF konvensional.

4. Validasi Lapisan Transport dan Perimeter Jaringan Menggunakan HostedScan (Nmap)

Sebagai tahap akhir dari validasi silang (*cross-tool validation*), penelitian ini melakukan pemindaian jaringan pada lapisan transport (*Transport Layer*) menggunakan mesin pemindai Nmap yang terintegrasi di dalam platform HostedScan. Pengujian ini menggunakan parameter pemindaian cepat pada 100 *port* paling umum (--top-ports=100) dengan metode *TCP Connect Scan* (-sT). Tujuannya adalah untuk mengukur seberapa responsif perimeter firewall institusi terhadap pemindaian jaringan (*port scanning*) dari luar.



Gambar 6. Laporan Pemindaian Port Jaringan menggunakan HostedScan (Nmap)

Hasil pemindaian yang diselesaikan dalam waktu sangat singkat (1,86 detik) tersebut memberikan gambaran yang sangat jelas mengenai konfigurasi kontrol akses jaringan (Access Control List/ACL) pada target pengujian. Rincian status port dapat dilihat pada Tabel 4.

Tabel 4. Hasil Pemindaian 100 Port Teratas (Nmap HostedScan)

Port/Protokol	Status	Layanan (Service)	Alasan (Reason)
80/tcp	Open	HTTP	syn-ack
443/tcp	Open	HTTPS	syn-ack
8080/tcp	Open	HTTP-Proxy	syn-ack
8443/tcp	Open	HTTPS-Alt	syn-ack
96 port lainnya	Filtered	Berbagai layanan	no-response (Paket diabaikan)
80/tcp	Open	HTTP	syn-ack

Analisis mendalam terhadap output Nmap tersebut menghasilkan beberapa kesimpulan teknis yang sangat penting dalam menyusun postur keamanan menyeluruh:

a) Pembatasan Akses Berbasis Layanan Web (Lapis 7): Dari 100 port utama yang dipindai, hanya 4 port yang berstatus terbuka (open), yaitu port 80, 443, 8080, dan 8443. Keempat port ini didedikasikan secara eksklusif untuk lalu lintas web (HTTP/HTTPS) dan proksi web. Hal ini mengonfirmasi temuan sebelumnya bahwa seluruh lalu lintas jaringan yang masuk memang difilter ketat dan hanya diizinkan untuk layanan antarmuka web melalui infrastruktur proksi WAF (Cloudflare).
b) Konfigurasi Firewall Drop/Filtered yang Solid: Sebanyak 96 port lainnya (seperti port SSH, FTP, Telnet, atau database) berstatus filtered dengan keterangan no-response. Ini membuktikan bahwa firewall jaringan kampus dikonfigurasi dengan aturan Drop (bukan Reject). Saat ada permintaan ke port yang tidak diizinkan, server secara diam-diam membuang (drop) paket tersebut tanpa memberikan respons penolakan. Teknik ini sangat efektif untuk memperlambat upaya reconnaissance dari peretas dan mencegah serangan langsung ke infrastruktur lapisan bawah.
c) Konklusi Akhir Postur Keamanan: Berdasarkan validasi menggunakan Acunetix, Helium, dan HostedScan (Nmap), dapat disimpulkan bahwa arsitektur jaringan lapisan bawah (infrastruktur) Universitas Subang sudah sangat aman dan terlindungi oleh WAF pihak ketiga. Oleh karena itu, satu-satunya vektor ancaman (threat vector) yang tersisa

dan paling memungkinkan untuk dieksploitasi adalah pada lapisan aplikasi, khususnya miskonfigurasi sisi klien (client-side) seperti absennya X-Frame-Options yang memicu kerentanan Clickjacking (temuan utama Acunetix).

5. Validasi Lapisan Aplikasi Menggunakan OWASP ZAP

Sebagai langkah verifikasi komprehensif terhadap hasil pemindaian Dynamic Application Security Testing (DAST) dari Acunetix, penelitian ini menambahkan lapis validasi menggunakan instrumen open-source standar industri, yaitu OWASP ZAP versi 2.17.0. Pengujian ini diotomatisasi melalui platform HostedScan dengan menargetkan domain utama https://unsub.ac.id. Tujuan utama dari komparasi ini adalah untuk memastikan tidak ada celah aplikasi tingkat kritis yang terlewatkan (false negative) oleh alat pemindai tunggal.

Secara garis besar, hasil pemindaian OWASP ZAP selaras dengan temuan Acunetix, yakni tidak ditemukannya celah berisiko tinggi (High Risk). Temuan OWASP ZAP berfokus pada peringatan tingkat Menengah (Medium) dan Rendah (Low) yang bersumber dari miskonfigurasi keamanan pada HTTP Response Header. Rincian temuan tersebut disajikan pada Tabel 5.

Tabel 5. Rincian Kerentanan Lapis Aplikasi (OWASP ZAP HostedScan)

Nama Kerentanan	Tingkat Risiko	Deskripsi Singkat
Content Security Policy (CSP) Header Not Set	Medium	Server tidak menerapkan kebijakan keamanan konten. Ketiadaan header ini mengurangi lapisan perlindungan tambahan yang berfungsi mendeteksi dan memitigasi serangan Cross Site Scripting (XSS) dan injeksi data.
Strict-Transport-Security Header Not Set	Low/Medium	Server tidak mendeklarasikan kebijakan *HTTP Strict Transport Security* (HSTS). Mekanisme ini krusial untuk memaksa agen pengguna (*browser*) agar berinteraksi secara eksklusif menggunakan koneksi HTTPS yang aman, serta mencegah serangan *downgrade* protokol.
X-Content-Type-Options Header Missing	Low	*Header* anti-*MIME-Sniffing* tidak diatur ke nosniff. Hal ini memungkinkan versi *browser* tertentu untuk menebak tipe konten (*MIME-sniffing*) pada respons *server*, yang berpotensi menyebabkan konten dieksekusi di luar tipe yang dideklarasikan secara resmi.

Analisis silang antara temuan OWASP ZAP dan Acunetix menghasilkan sintesis yang memperkuat postur pertahanan lapisan aplikasi institusi:

a) Konsistensi Akar Masalah (*Root Cause*): OWASP ZAP memvalidasi bahwa titik terlemah dari website Universitas Subang tidak terletak pada kelemahan struktural basis kode (seperti kerentanan injeksi SQL atau Broken Access Control), melainkan secara spesifik pada miskonfigurasi lapisan presentasi dan Security Headers.
b) Korelasi dengan Mitigasi *Clickjacking*: Temuan OWASP ZAP terkait Content Security Policy (CSP) Header Not Set berkorelasi langsung dengan temuan Clickjacking: X-Frame-Options Header Missing dari pemindaian Acunetix sebelumnya. Dalam arsitektur keamanan web modern, implementasi CSP (khususnya direktif frame-

ancestors) merupakan protokol pengamanan tingkat lanjut yang berfungsi ganda untuk memitigasi XSS sekaligus menambal kerentanan UI Redress (Clickjacking).

c) Penyempurnaan Rekomendasi: Kemunculan temuan Strict-Transport-Security dan X-Content-Type-Options dari OWASP ZAP menunjukkan perlunya pendekatan mitigasi yang holistik. Administrator sistem tidak cukup hanya menambal satu header saja.

Berdasarkan keseluruhan uji komparatif menggunakan Acunetix, Helium (WAF & Infrastruktur), HostedScan Nmap, dan OWASP ZAP, didapatkan kesimpulan akhir bahwa perimeter sistem dan basis data institusi telah terlindungi dengan baik oleh filter lapisan jaringan (Cloudflare). Oleh karena itu, fokus mitigasi mutlak diarahkan pada penguatan (hardening) konfigurasi Web Server dengan merancang dan menerapkan sekumpulan kebijakan HTTP Security Headers yang komprehensif.

6. Pelaporan (*Reporting*) dan Rekomendasi Mitigasi Teknis

Mengingat kerentanan ini disebabkan secara eksklusif oleh ketiadaan header, mitigasi dapat dilakukan secara efisien tanpa harus merombak *source code* aplikasi. Sangat direkomendasikan bagi pengelola server untuk segera mengimplementasikan konfigurasi *header* berikut pada lapisan *Web Server* (misalnya Apache atau Nginx):

a) X-Frame-Options: SAMEORIGIN, Mekanisme ini akan menginstruksikan peramban (browser) agar hanya mengizinkan pemuatan halaman di dalam frame jika frame tersebut berasal dari domain yang identik (https://unsub.ac.id).
b) Content-Security-Policy: frame-ancestors ‘self’, Ini merupakan kebijakan (policy) yang lebih modern, fleksibel, dan didukung oleh sebagian besar peramban terkini untuk mencapai pengamanan berlapis terhadap serangan antarmuka.
c) Strict-Transport-Security: max-age=31536000; includeSubDomains, Implementasi header HSTS ini direkomendasikan untuk memaksa seluruh interaksi agen pengguna (browser) agar selalu menggunakan koneksi terenkripsi HTTPS secara ketat, serta memitigasi risiko serangan downgrade protokol.
d) X-Content-Type-Options: nosniff, Penambahan header ini krusial untuk mencegah kerentanan MIME-Sniffing, memastikan browser selalu mengeksekusi tipe konten sesuai dengan yang dideklarasikan oleh server.

KESIMPULAN

Penelitian ini berhasil mengevaluasi postur dan tingkat risiko keamanan siber aktual pada website resmi Universitas Subang (https://unsub.ac.id) menggunakan pendekatan *Dynamic Application Security Testing* (DAST). Berdasarkan hasil pemindaian *Black Box* menggunakan Acunetix yang diselesaikan secara sempurna (100%), diperoleh kesimpulan bahwa tingkat ancaman keamanan pada website target secara keseluruhan berada pada kategori rendah (*LOW*). Dari total 15 temuan yang dilaporkan, sistem terbukti bersih dari kerentanan kritis di tingkat *HIGH* maupun *MEDIUM*, yang mengindikasikan bahwa mekanisme validasi *input* dasar pada aplikasi web institusi telah diimplementasikan dengan cukup baik.

Fokus utama risiko dalam postur keamanan saat ini tertuju pada satu temuan tingkat rendah (*LOW*), yaitu celah keamanan *Clickjacking: X-Frame-Options Header Missing*. Sementara itu, 14 temuan lainnya berada pada level *Informational* yang mencerminkan keterbukaan informasi arsitektur *server*.

Lebih lanjut, pengujian silang (*cross-tool validation*) menggunakan Helium Scanner, HostedScan (Nmap), dan OWASP ZAP berhasil mengonfirmasi postur keamanan secara lebih menyeluruh. Hasil pemindaian infrastruktur membuktikan bahwa jaringan institusi telah

terlindungi secara solid oleh lapisan *Web Application Firewall* (WAF) Cloudflare yang secara efektif menyaring lalu lintas berbahaya dan mengunci *port* yang tidak berizin. Namun, validasi pada lapisan aplikasi (OWASP ZAP) mempertegas absennya perlindungan pada *HTTP Security Headers* lainnya, seperti *Content Security Policy* (CSP), *Strict-Transport-Security* (HSTS), dan *X-Content-Type-Options*. Ketiadaan *header* keamanan ini berpotensi mengekspos risiko reputasi jika disalahgunakan oleh pihak ketiga untuk serangan *UI Redress* maupun *MIME-Sniffing*.

Penelitian ini memberikan kontribusi ganda, baik secara teoretis maupun praktis. Secara teoretis, penelitian ini menyajikan dokumentasi empiris dan verifikasi keamanan aktual mengenai domain utama Universitas Subang yang selama ini belum terpublikasi secara komprehensif. Secara praktis, validasi berlapis ini menghasilkan rumusan mitigasi teknis (*hardening*) yang sangat konkret. Mengingat lapisan infrastruktur (*back-end*) telah aman, tim IT institusi kini dapat memfokuskan upaya mitigasi secara efisien pada implementasi sekumpulan kebijakan *HTTP Security Headers* yang komprehensif untuk memperkuat ketahanan *server* di masa mendatang.

DAFTAR PUSTAKA

Al Fajar, F. (2020). *Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web*. *2*, 110–120.

Kristianto, F., Rahman, S., & Bahri, S. (2022). *Analisis Kerentanan Pada Website Servio*. *9*(1), 46–55.

Alwi, M., et al. (2020). Keamanan Sistem Informasi dan Privasi Data di Era Digital. *Jurnal Keamanan Siber*, 5(2), 45-55.

OWASP Foundation. (2021). OWASP Top Ten - 2021. Diakses dari https://owasp.org/www-project-top-ten/

Schneier, B. (n.d.). *The Hidden Battles to Collect Your Data and Control Your World*. https://c3jemx2ube5v5zpg.onion.

Syafaat, A. (2024). Identifikasi Kerentanan Keamanan Pada Website Fakultas Ilmu Komputer Universitas Subang Menggunakan Metodologi Owasp. *Http://Ejournal.Unsub.Ac.Id/Index.Php/Fasilkom*, *11*(1), 84–99.

Wibowo, F., Harjono, & Wicaksono, A. P. (2019). *Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS*. *6*(2), 212–217.

Zirwan, A. (2022). *Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner*. *4*(1), 1–3. https://doi.org/10.37034/jidt.v4i1.190