INDEXIA : Informatic and Computational Intelligent Journal
Vol.08, No.01, Mei 2026, hlm. 1-10
P-ISSN: 2657-0424
E-ISSN: 2657-0432

ANALISIS KEAMANAN WEBSITE UNIVERSITAS XYZ MENGGUNAKAN PENDEKATAN PENETRATION TESTING BERDASARKAN OWASP TOP 10

Nur Romadhoni Hidayat[1,], Muhammad Faishol Amrulloh[2,*)]
[1, 2)] Program Studi Teknik Informatika, Universitas Yudharta Pasuruan
Jl. Yudharta No. 07 Sengonagung Purwosari Pasuruan Jawa Timur
e-mail: hidayatramadhani5@gmail.com[1)], faishol@yudharta.ac.id[2)]
*corresponding author

(Naskah masuk : 27 Juli 2025 Diterima untuk diterbitkan : 10 September 2025)

ABSTRAK

Keamanan website pendidikan semakin penting karena meningkatnya ancaman siber yang menargetkan sektor akademik, termasuk serangan SQL Injection, Cross-Site Scripting (XSS), dan misconfiguration. Kondisi ini menimbulkan risiko kebocoran data, gangguan operasional, dan menurunnya kepercayaan pengguna. Website Universitas XYZ belum pernah diuji secara menyeluruh, sehingga terdapat urgensi untuk melakukan evaluasi keamanan guna mengidentifikasi potensi kerentanan. Penelitian ini bertujuan menganalisis tingkat keamanan website Universitas XYZ menggunakan pendekatan penetration testing berbasis OWASP Top 10. Pengujian dilakukan dengan black-box testing melalui tahapan reconnaissance, scanning, vulnerability assessment, exploitation, post-exploitation, dan reporting. Hasil pengujian menunjukkan terdapat tiga kerentanan yang berhasil diidentifikasi, semuanya berada pada tingkat risiko rendah. Salah satu temuan utama adalah tidak adanya header security pada konfigurasi server, yang dapat menyebabkan kerentanan terhadap serangan clickjacking. Selain itu, ditemukan pula dukungan terhadap protokol TLS versi lama dan juga user enumeration. Berdasarkan hasil tersebut, tingkat keamanan website dikategorikan berada pada level rendah risiko dan tergolong aman, namun tetap disarankan untuk melakukan perbaikan pada aspek konfigurasi serta pembaruan komponen sistem. Penelitian ini secara langsung berkontribusi dalam mendokumentasikan kelemahan yang ada dan menghasilkan solusi perbaikan untuk memperkuat keamanan situs web terhadap ancaman siber.

***Kata Kunci**: Blackbox Testing, Keamanan Website, OWASP Top 10, Penetration Testing.*

ABSTRACT

The security of educational websites is increasingly important due to the rise of cyber threats targeting the academic sector, including SQL Injection, Cross-Site Scripting (XSS), and misconfiguration attacks. This situation poses a risk of data leakage, operational disruptions, and decreased user trust. The XYZ University website has never been thoroughly tested, so there is an urgency to conduct a security evaluation to identify potential vulnerabilities. This study aims to analyze the security level of the XYZ University website using an OWASP Top 10-based penetration testing approach. Testing was conducted using a black-box testing through the stages of reconnaissance, scanning, vulnerability assessment, exploitation, post-exploitation, and reporting. The test results showed that three vulnerabilities were identified, all at a low risk level. One of the main findings was the absence of a security header in the server configuration, which could make it vulnerable to clickjacking attacks. Furthermore, support for older versions of the TLS protocol and user enumeration were also found. Based on these results, the website's security level is categorized as low risk and relatively safe, but it is still recommended to make improvements to the configuration aspects and update system components. This research directly contributes to documenting existing vulnerabilities and generating remedial solutions to strengthen website security against cyber threats.

***Keywords**: Blackbox Testing, OWASP Top 10, Penetration Testing, Web Security*

I. PENDAHULUAN

Perkembangan teknologi informasi di era digital telah memberikan dampak yang signifikan pada berbagai sektor, termasuk bidang pendidikan tinggi. Perguruan tinggi semakin bergantung pada layanan

berbasis teknologi informasi, khususnya website, untuk menunjang kegiatan akademik maupun administratif. Website bukan lagi sekadar sarana penyampaian informasi, melainkan juga menjadi portal utama bagi mahasiswa, dosen, dan tenaga kependidikan untuk mengakses layanan akademik, mengelola data, hingga berinteraksi dalam ekosistem pendidikan. Perubahan ini membawa banyak manfaat dari sisi efisiensi dan efektivitas layanan, tetapi sekaligus menimbulkan tantangan baru dalam hal keamanan siber. Namun, meningkatnya kompleksitas teknologi informasi dan ancaman siber membuat keamanan sistem informasi menjadi aspek yang sangat penting [1].

Website Universitas XYZ merupakan salah satu sistem informasi penting yang digunakan untuk menunjang kegiatan akademik dan administrasi. Website ini menyediakan berbagai layanan mulai dari penyampaian informasi perkuliahan, pendaftaran, hingga interaksi dengan sistem akademik internal. Namun, hingga penelitian ini dilakukan, website tersebut belum pernah diuji secara menyeluruh dari sisi keamanan. Kondisi ini menimbulkan potensi kerentanan yang berbahaya apabila tidak segera diidentifikasi dan ditangani. Kerentanan yang tidak terdeteksi dapat dieksploitasi untuk mendapatkan akses ilegal terhadap data sensitif, mengganggu proses akademik, bahkan merusak reputasi universitas. Hilangnya kepercayaan masyarakat akibat insiden kebocoran data tentu akan berdampak langsung pada citra dan keberlangsungan institusi. Jika seorang administrator mengabaikan keamanan sistem atau melakukan kesalahan dalam penulisan kode keamanan, maka akan terbuka celah yang memungkinkan pihak tidak bertanggung jawab mengeksploitasi website untuk kepentingan pribadi [2].

Ancaman keamanan terhadap layanan berbasis web terus mengalami peningkatan seiring dengan berkembangnya metode serangan. Berbagai teknik seperti SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, hingga Broken Access Control telah banyak dieksploitasi untuk menyerang sistem informasi. Dampak dari serangan tersebut dapat berupa kebocoran data, hilangnya integritas sistem, hingga gangguan operasional yang merugikan institusi. Fenomena ini semakin relevan di Indonesia, di mana pengguna internet terus meningkat setiap tahun. Laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023 mencatat bahwa jumlah pengguna internet di Indonesia telah mencapai lebih dari 215 juta jiwa, atau sekitar 78% dari total populasi [3]. Kondisi ini menunjukkan bahwa layanan berbasis web, termasuk website akademik, menjadi target potensial serangan siber karena tingginya intensitas penggunaan. Sebagai upaya meminimalisir resiko terhadap serangan yang dilakukan oleh hacker yang bisa datang secara tiba-tiba, maka langkah yang dapat dilakukan dengan mengevaluasi keamanan sistem informasi[4].Ancaman keamanan terhadap layanan berbasis web terus mengalami peningkatan seiring dengan berkembangnya metode serangan. Berbagai teknik seperti SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, hingga Broken Access Control telah banyak dieksploitasi untuk menyerang sistem informasi. Dampak dari serangan tersebut dapat berupa kebocoran data, hilangnya integritas sistem, hingga gangguan operasional yang merugikan institusi. Fenomena ini semakin relevan di Indonesia, di mana pengguna internet terus meningkat setiap tahun. Laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023 mencatat bahwa jumlah pengguna internet di Indonesia telah mencapai lebih dari 215 juta jiwa, atau sekitar 78% dari total populasi [3]. Kondisi ini menunjukkan bahwa layanan berbasis web, termasuk website akademik, menjadi target potensial serangan siber karena tingginya intensitas penggunaan. Sebagai upaya meminimalisir resiko terhadap serangan yang dilakukan oleh hacker yang bisa datang secara tiba-tiba, maka langkah yang dapat dilakukan dengan mengevaluasi keamanan sistem informasi[4].

Beberapa penelitian terdahulu telah membahas analisis keamanan website dengan pendekatan penetration testing. Putranto dkk. [5] meneliti keamanan website akademik UPNVJ terhadap serangan SQL Injection dan Sniffing Attack. Hasil penelitian menunjukkan bahwa website tersebut relatif aman karena telah menggunakan Web Application Firewall (WAF) dan Transport Layer Security (TLS). Akil dkk. [6] mengkaji kerentanan terhadap serangan HTML Injection dan menemukan celah yang memungkinkan penyisipan kode berbahaya untuk melakukan defacement atau pencurian data cookie. Gustiyonoo dkk. [7] menganalisis kerentanan Cross-Site Scripting (XSS) dan menemukan potensi serangan berupa pop-up, phishing, serta pencurian data pengguna. Sementara itu, Priyanka dan Smruthi [8] meneliti kerentanan aplikasi web dengan objek DVWA, dan hasilnya menunjukkan bahwa aplikasi tersebut tidak menerapkan praktik keamanan yang baik sehingga rentan terhadap serangan SQL Injection, XSS, dan Cross-Site Request Forgery (CSRF).

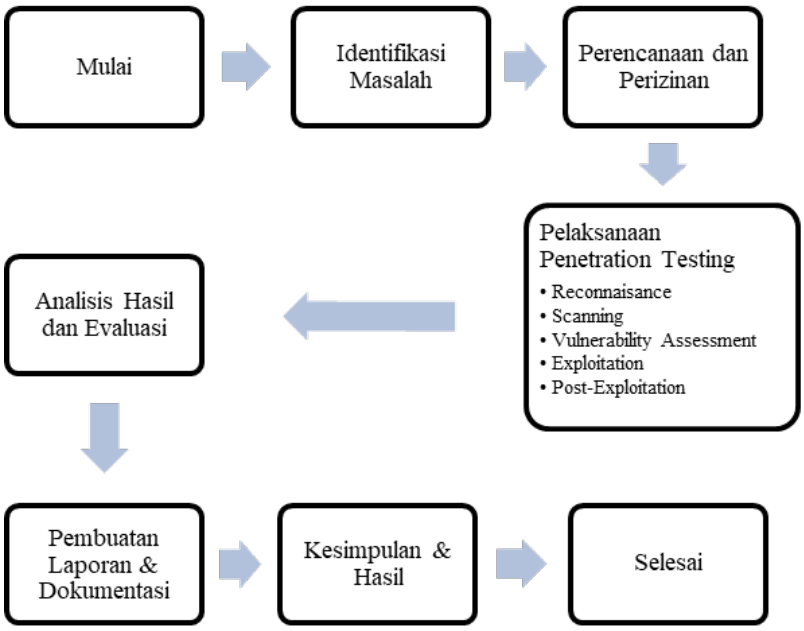
Berdasarkan dari penelitian terdahulu, terlihat bahwa sebagian besar kajian hanya berfokus pada jenis serangan tertentu seperti SQL Injection, Cross-Site Scripting (XSS), HTML Injection, maupun Cross-

Site Request Forgery (CSRF) [5-8]. Pendekatan ini memang memberikan gambaran spesifik, tetapi tidak mencerminkan kondisi kerentanan website secara menyeluruh. Selain itu, terdapat penelitian yang menggunakan aplikasi uji coba seperti DVWA [8], yang kurang merepresentasikan lingkungan riil sebuah website institusi pendidikan. Beberapa penelitian juga hanya menekankan pada proses eksploitasi tanpa membahas langkah mitigasi secara mendalam, sehingga rekomendasi praktis untuk pengelola sistem masih terbatas. Dengan demikian, terdapat perbedaan penelitian berupa ketiadaan analisis komprehensif yang menguji keamanan website institusi pendidikan dengan cakupan penuh menggunakan framework standar internasional serta menghasilkan rekomendasi mitigasi.

Keterbaruan dalam penelitian ini terletak pada penerapan pendekatan penetration testing berbasis OWASP Top 10, yang memberikan kerangka kerja sistematis untuk mengidentifikasi kerentanan aplikasi web pada sepuluh kategori utama. Pengujian dilakukan dengan metode black-box testing, di mana peneliti bertindak sebagai pihak luar tanpa akses ke kode sumber maupun konfigurasi sistem, sehingga kondisi pengujian menyerupai skenario serangan nyata. Setiap kerentanan yang ditemukan akan dianalisis tingkat risikonya, kemudian disertai rekomendasi mitigasi yang dapat langsung diimplementasikan oleh pengelola sistem. Dengan cara ini, hasil penelitian tidak hanya memberikan gambaran kerentanan yang ada, tetapi juga solusi praktis untuk meningkatkan perlindungan website Universitas XYZ dari ancaman siber.

Penelitian ini bertujuan untuk menganalisis tingkat keamanan website Universitas XYZ menggunakan OWASP Top 10, mengidentifikasi kerentanan melalui proses penetration testing, dan memberikan rekomendasi mitigasi yang dapat meningkatkan keamanan sistem. Penelitian ini diharapkan dapat memberikan kontribusi praktis bagi Universitas XYZ dalam memperkuat keamanan website akademik serta menjadi referensi bagi penelitian selanjutnya terkait evaluasi keamanan pada institusi pendidikan.

II. METODE PENELITIAN



Gambar 1. Alur Penelitian

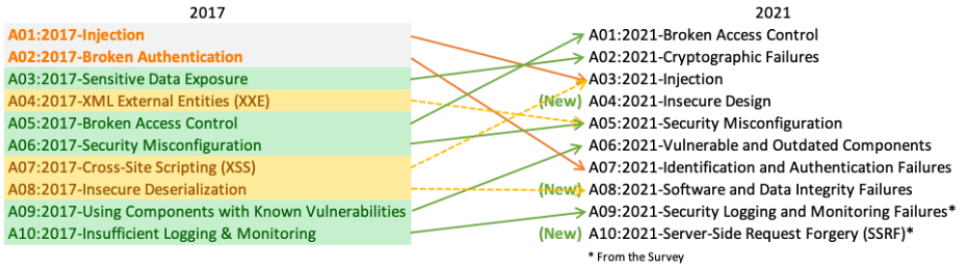
Penetration testing memiliki 3 metode dalam melakukan pengujian diantaranya, black box testing, white box testing dan gray box testing[11]. Penelitian ini menggunakan pendekatan penetration testing berbasis standar OWASP Top 10, dengan metode pengujian black box testing, di mana penguji tidak memiliki akses ke kode sumber website. Fokus pengujian ditujukan untuk mengidentifikasi dan menganalisis potensi kerentanan yang terdapat pada website milik Universitas XYZ, yang berfungsi sebagai portal layanan akademik dan informasi institusional.

A. Objek Penelitian

Objek dari penelitian ini adalah website resmi milik Universitas XYZ yang dibangun menggunakan Content Management System (CMS) WordPress. Seluruh komponen publik dari website diuji, termasuk halaman statis, dinamis, form interaktif, serta plugin yang terpasang secara aktif. Akses ke sisi administrator atau sistem internal tidak dilakukan karena keterbatasan hak akses pengujian.

B. Ruang Lingkup

Pengujian dilakukan terhadap sepuluh kategori ancaman OWASP Top 10, meliputi: Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, serta Server-Side Request Forgery (SSRF) [12].



Gambar 2. OWASP Top 10

C. Tahapan Pengujian

Pengujian dilakukan melalui enam tahapan utama berikut:

1) Reconnaissance

Tahap awal untuk mengumpulkan informasi dasar mengenai sistem target, termasuk alamat IP, domain, CMS yang digunakan, teknologi backend, dan struktur URL. Reconnaissance yang merupakan langkah awal penting dalam pengujian penetrasi[13]. Informasi ini berguna untuk menentukan vektor serangan yang mungkin digunakan.

2) Scanning

Kedua Scanning atau memindai target menggunakan tools yang ada untuk mencari keamanan yang bisa digunakan untuk masuk kedalam sistem objek[14]. Tools seperti Nmap, WPScan, dan Wappalyzer digunakan untuk mendeteksi detail sistem serta plugin atau layanan tambahan yang terpasang.

3) Vulnerability Assessment

Vulnerability Assessment (VA) adalah salah satu cara pengukuran terhadap keamanan sistem[15]. Metode vulnerability assessment dapat membantu mendeteksi kerentanan dalam sebuah aplikasi web[16]. Data dari tahap scanning kemudian dianalisis untuk mengidentifikasi potensi kerentanan yang sesuai dengan kategori OWASP Top 10.

4) Exploitation

Setelah kerentanan teridentifikasi, dilakukan pengujian eksploitasi untuk memastikan apakah celah tersebut benar-benar dapat dimanfaatkan. Uji coba dilakukan terhadap parameter, konfigurasi header, atau layanan tertentu dengan metode yang aman dan tidak merusak.

5) Post-Exploitation

Post Exploitation bertujuan untuk menilai pentingnya sistem yang berhasil dieksploitasi sekaligus memastikan kendali atas sistem tersebut tetap terjaga[17]. Meskipun tidak dilakukan akses atau perubahan data secara langsung, analisis dilakukan untuk memahami potensi ancaman yang dapat terjadi apabila kerentanan tersebut dimanfaatkan oleh pihak berbahaya.

6) Reporting

Seluruh hasil pengujian dicatat dan dianalisis dalam bentuk laporan akhir. Laporan mencakup jenis kerentanan, tingkat risiko, serta rekomendasi teknis untuk mitigasi yang dapat diterapkan oleh pihak pengelola sistem.

III. HASIL DAN PEMBAHASAN

Website milik Universitas XYZ yang menjadi objek penelitian merupakan sistem berbasis WordPress

dan difungsikan sebagai portal akademik untuk kebutuhan informasi dan layanan kampus. Pengujian dilakukan dengan pendekatan black-box tanpa akses ke sisi server atau administratif.

A. Pengujian

Sebagai langkah utama dalam penelitian ini, dilakukan evaluasi terhadap keamanan website berdasarkan sepuluh kategori kerentanan yang tercantum dalam standar OWASP Top 10. Setiap kategori dianalisis secara terpisah melalui proses pengujian menyeluruh terhadap struktur dan fungsionalitas website. Hasil dari proses ini diklasifikasikan ke dalam dua kondisi: kategori yang ditemukan mengandung kerentanan, dan kategori yang telah diuji namun tidak ditemukan celah keamanan yang dapat dieksploitasi.

1) A01 - Broken Access Control

Pengujian terhadap kategori Broken Access Control dilakukan menggunakan metode manual dan tools otomatis seperti WPScan, untuk mengevaluasi apakah terdapat kontrol akses yang tidak efektif pada website. Fokus utama pengujian adalah untuk mengidentifikasi kemungkinan akses terhadap sumber daya yang seharusnya dibatasi.

Salah satu kelemahan yang ditemukan adalah adanya kerentanan user enumeration melalui endpoint wp-json, yang merupakan bagian dari REST API WordPress. Endpoint ini secara default memberikan informasi tentang akun pengguna yang telah terdaftar, seperti username dan ID pengguna.

Kerentanan ini berpotensi dimanfaatkan oleh penyerang untuk mengumpulkan daftar akun pengguna yang valid. Meskipun tidak langsung memberikan akses administratif, informasi yang diekspos dapat digunakan dalam serangan brute-force terhadap halaman login atau digunakan dalam teknik rekayasa sosial.

Temuan ini menunjukkan bahwa sistem belum menerapkan pembatasan akses yang memadai terhadap API publik, yang seharusnya hanya dapat diakses oleh pengguna dengan hak tertentu.

2) A02 - Cryptographic Failures

Pengujian pada kategori Cryptographic Failures difokuskan untuk mengevaluasi kekuatan dan konfigurasi sistem enkripsi yang digunakan oleh website. Salah satu aspek penting dalam pengujian ini adalah dukungan terhadap protokol Transport Layer Security (TLS), yang digunakan untuk mengenkripsi komunikasi antara klien dan server.

Berdasarkan hasil pemindaian menggunakan tools seperti SSL Labs, ditemukan bahwa server masih mendukung protokol TLS versi 1.0 dan 1.1, yang saat ini telah dianggap usang dan tidak aman oleh banyak standar industri, termasuk oleh Internet Engineering Task Force (IETF), National Security Agency (NSA) dan browser modern[18][19]. Kedua versi TLS ini memiliki kelemahan kriptografi yang telah diketahui secara publik dan berpotensi dieksploitasi, meskipun eksploitasi langsung tidak berhasil dilakukan selama pengujian. Temuan ini mengindikasikan bahwa website belum mengikuti praktik terbaik dalam hal keamanan kriptografi.

3) A03 – Injection

Pada kategori Injection, fokus pengujian adalah untuk mengetahui apakah sistem web rentan terhadap serangan injeksi, seperti SQL Injection (SQLi), Command Injection, HTML Injection, dan lainnya. Jenis kerentanan ini umumnya terjadi ketika input dari pengguna tidak divalidasi atau disanitasi dengan baik sebelum digunakan dalam query atau perintah ke sistem backend.

Pengujian dilakukan baik secara manual maupun menggunakan tools otomatis seperti SQLmap, dan Burp Suite. Seluruh form input, dan parameter URL diuji dengan berbagai payload injeksi.

Namun, berdasarkan hasil pengujian menyeluruh, tidak ditemukan adanya respons dari sistem yang mengindikasikan keberadaan kerentanan SQL Injection atau bentuk injeksi lainnya. Seluruh input tampak telah difilter dengan baik, dan sistem tidak memberikan error yang mengungkapkan struktur query internal atau informasi sensitif lainnya.

4) A04 - Insecure Design

Pada kategori Insecure Design, fokus pengujian adalah untuk mengevaluasi apakah sistem memiliki kelemahan pada desain arsitektur atau logika aplikasi yang memungkinkan eksploitasi, meskipun implementasi teknisnya berjalan dengan benar. Kerentanan dalam kategori ini biasanya muncul karena tidak adanya kontrol keamanan sejak tahap perancangan sistem.

Pengujian dilakukan dengan menganalisis bagaimana alur pengguna, autentikasi, dan akses ke fitur-fitur dalam website dikendalikan. Termasuk di dalamnya adalah upaya untuk mengakses fungsi-fungsi

yang seharusnya dibatasi, mencoba mengakses halaman tertentu langsung melalui URL, serta mengevaluasi desain pengelolaan sesi pengguna.

Berdasarkan pengujian yang dilakukan, tidak ditemukan kerentanan yang terkait dengan Insecure Design. Tidak ada fitur atau jalur interaksi pengguna yang memberikan akses atau informasi lebih dari yang seharusnya. Proses login, navigasi, dan pembatasan fitur tampak telah dirancang secara sederhana namun fungsional, tanpa celah akses yang tidak sah.

Namun, karena pengujian dilakukan dalam kondisi black-box dan tidak memiliki akses terhadap dokumentasi desain internal atau kode sumber aplikasi, maka penilaian terhadap Insecure Design hanya dapat dilakukan berdasarkan observasi eksternal.

5) A05 - Security Misconfiguration

Pengujian pada kategori Security Misconfiguration menunjukkan bahwa konfigurasi server website Universitas XYZ belum optimal dalam menerapkan standar keamanan. Berdasarkan hasil inspeksi menggunakan Burp Suite dan analisis manual, ditemukan bahwa server tidak menerapkan beberapa header keamanan penting.

Header X-Frame-Options tidak ditemukan dalam respons server, sehingga halaman web dapat dimuat dalam elemen <iframe> oleh domain lain. Hal ini berpotensi memungkinkan terjadinya clickjacking, yaitu serangan yang memanipulasi tampilan antarmuka website untuk menipu pengguna melakukan tindakan tanpa disadari. Kategori ini mencakup kesalahan atau kelalaian dalam pengaturan keamanan yang seharusnya melindungi situs dari berbagai serangan, seperti clickjacking, downgrade attack, dan MIME-type sniffing[20]

Selain itu, header Strict-Transport-Security (HSTS) juga tidak ditemukan dalam response header. Namun, pengalihan dari HTTP ke HTTPS tetap terjadi secara konsisten, yang mengindikasikan bahwa pengalihan tersebut dikelola oleh lapisan proteksi eksternal seperti WAF, bukan berasal dari konfigurasi server internal. Meskipun efeknya sebanding dengan penggunaan HSTS, ketergantungan terhadap proteksi eksternal dapat menjadi titik lemah apabila arsitektur berubah atau layanan pihak ketiga tidak aktif.

6) A06 - Vulnerable and Outdated Components

Dalam kategori Vulnerable and Outdated Components, pengujian difokuskan pada identifikasi komponen perangkat lunak atau library yang digunakan oleh website yang telah usang atau memiliki kerentanan keamanan yang diketahui (CVE). Proses ini dilakukan menggunakan pendekatan manual dan dukungan tools seperti WPScan, dan Wappalyzer untuk mendeteksi versi CMS, plugin, serta teknologi yang digunakan.

Hasil pengujian menunjukkan bahwa website menggunakan WordPress sebagai CMS, namun versi pastinya tidak berhasil diidentifikasi secara eksplisit karena server tidak mengungkapkan informasi tersebut melalui metadata atau halaman login. Beberapa plugin dan tema juga tidak menampilkan versi secara terbuka, yang membatasi proses verifikasi langsung terhadap daftar kerentanan umum (CVE).

Hasil dari pengujian menunjukkan bahwa semua komponen yang digunakan oleh website telah diperbarui ke versi terbaru dan tidak ditemukan kerentanan yang diketahui berdasarkan referensi Common Vulnerabilities and Exposures (CVE) yang tersedia. Baik CMS WordPress, maupun plugin tidak menunjukkan adanya penggunaan versi yang rentan.

7) A07 - Identification and Authentication Failures

Pengujian terhadap kategori Identification and Authentication Failures difokuskan untuk menilai seberapa aman mekanisme identifikasi dan autentikasi yang digunakan oleh website, termasuk perlindungan terhadap brute force, keamanan penyimpanan kredensial, pengelolaan sesi, dan kontrol autentikasi lainnya.

Selama pengujian, berbagai teknik digunakan untuk mengevaluasi kelemahan sistem, baik secara manual maupun dengan bantuan tools otomatis. Hasil dari pengujian menunjukkan bahwa tidak ditemukan kerentanan pada mekanisme autentikasi.

Dengan demikian, dapat disimpulkan bahwa pada kategori ini, website telah mengimplementasikan kontrol autentikasi yang cukup baik dan tidak ditemukan celah yang dapat dieksploitasi oleh penyerang. Meski demikian, evaluasi rutin tetap disarankan untuk memastikan bahwa tidak muncul kerentanan baru seiring dengan pembaruan sistem atau plugin.

8) A08 - Software and Data Integrity Failures

Kategori Software and Data Integrity Failures berkaitan dengan penggunaan komponen atau plugin pihak ketiga yang tidak terpercaya, serta kurangnya validasi integritas pada proses pembaruan perangkat lunak dan data penting dalam sistem. Serangan pada kategori ini biasanya terjadi ketika penyerang mampu menyisipkan atau mengganti komponen dalam rantai distribusi (supply chain attack), atau ketika tidak ada mekanisme verifikasi integritas saat pembaruan dilakukan.

Pada proses pengujian, analisis dilakukan terhadap versi plugin, tema, dan komponen lain yang digunakan dalam website. Namun, karena pengujian dilakukan dalam kondisi black-box, informasi mengenai validasi integritas secara internal atau mekanisme verifikasi pembaruan tidak dapat diakses secara langsung. Pengujian tidak menemukan adanya tanda-tanda komponen mencurigakan atau bukti adanya manipulasi terhadap data atau perangkat lunak yang digunakan oleh sistem.

9) A09 - Security Logging and Monitoring Failures

Kategori Security Logging and Monitoring Failures berfokus pada kemampuan sistem dalam mencatat aktivitas penting serta mendeteksi dan merespons insiden keamanan secara efektif. Ketiadaan atau kelemahan pada sistem pencatatan (logging), pemantauan (monitoring), serta respons insiden dapat menyebabkan keterlambatan dalam mendeteksi serangan dan menyulitkan proses investigasi forensik apabila terjadi pelanggaran keamanan.

Dalam pengujian yang dilakukan, tidak terdapat akses langsung terhadap sistem backend atau file log karena keterbatasan pengujian black-box. Oleh karena itu, evaluasi terhadap sistem logging dan monitoring hanya dapat dilakukan berdasarkan perilaku aplikasi di sisi pengguna (frontend). Berdasarkan observasi dan karakteristik platform WordPress yang digunakan, diketahui bahwa sistem secara default hanya mencatat aktivitas dasar seperti login dan logout pengguna.

10) A10 - Server-Side Request Forgery

Kategori Server-Side Request Forgery (SSRF) mengacu pada kerentanan yang memungkinkan penyerang untuk membuat server mengirimkan permintaan HTTP ke domain internal atau eksternal yang ditentukan oleh penyerang. Jika tidak dibatasi, kerentanan ini dapat dimanfaatkan untuk mengakses layanan internal, metadata cloud, atau melakukan scanning terhadap sistem lain dari sisi server, yang seharusnya tidak dapat diakses oleh pihak eksternal.

Dalam pengujian yang dilakukan terhadap website Universitas XYZ, tidak ditemukan fitur yang mengizinkan pengguna menginput URL atau endpoint yang kemudian diproses oleh server. Fitur seperti URL fetcher, integrasi API pihak ketiga, atau pengambilan konten dari URL eksternal juga tidak ditemukan selama fase reconnaissance maupun eksploitasi. Dengan demikian, tidak terdapat vektor serangan yang dapat dimanfaatkan untuk melakukan SSRF.

Selain itu, tidak ditemukan parameter tersembunyi atau endpoint backend yang dapat diindikasikan memproses input URL dari pengguna. Pengujian juga dilakukan dengan mencoba memanipulasi parameter pada endpoint yang tersedia, namun server tidak menunjukkan respon yang relevan dengan SSRF. Berdasarkan hasil pengujian tersebut, dapat disimpulkan bahwa kategori ini tidak menunjukkan adanya kerentanan pada sistem saat penelitian dilakukan.

B. Ringkasan Analisis Hasil dan Perbandingan

Sebelum penelitian ini dilakukan, website Universitas XYZ memang pernah diuji, namun pengujian tersebut tidak dilakukan secara menyeluruh dan laporan hasilnya tidak tersedia. Oleh karena itu, kondisi awal seluruh kategori OWASP Top 10 dianggap belum teruji secara menyeluruh.

Penelitian ini menggunakan pendekatan black-box testing untuk menggambarkan kondisi aktual keamanan website dari perspektif penyerang eksternal. Perbandingan kondisi sebelum dan sesudah pengujian ditunjukkan pada Tabel 1.

Dari Tabel 1 terlihat bahwa dari sepuluh kategori OWASP Top 10 yang diuji, ditemukan tiga kategori dengan kerentanan seluruhnya berada pada tingkat risiko rendah, sementara tujuh kategori lainnya tidak menunjukkan adanya celah keamanan. Ketiga kerentanan tersebut adalah User Enumeration pada A01 – Broken Access Control, dukungan terhadap versi TLS lama pada A02 – Cryptographic Failures, dan tidak adanya security headers pada A05 – Security Misconfiguration.

Temuan ini menunjukkan bahwa meskipun website Universitas XYZ memiliki kerentanan, tingkat risikonya relatif rendah dan tidak secara langsung mengancam keberlangsungan sistem. Namun, apabila

tidak segera diperbaiki, kelemahan tersebut tetap berpotensi dieksploitasi oleh penyerang untuk tahap awal serangan.

Hasil ini menegaskan bahwa website Universitas XYZ secara umum berada dalam kondisi yang cukup aman, meskipun masih terdapat kelemahan kecil pada aspek kontrol akses, konfigurasi kriptografi, dan pengaturan keamanan dasar. Oleh karena itu, pengujian keamanan tetap perlu dilakukan secara berkala untuk memastikan tidak muncul kerentanan baru dan agar kelemahan dengan tingkat risiko rendah dapat segera diatasi sebelum berkembang menjadi ancaman yang lebih serius.

Tabel 1. Perbandingan Kondisi Sebelum dan Sesudah Pengujian

Kategori OWASP Top 10 (2021)	Sebelum Pengujian	Sesudah Pengujian
A01 – Broken Access Control	Belum teruji	User Enumeration (tingkat risiko rendah)
A02 – Cryptographic Failures	Belum teruji	Dukungan terhadap Versi TLS Lama (tingkat risiko rendah)
A03 - Injection	Belum teruji	Tidak ditemukan kerentanan
A04 - Insecure Design	Belum teruji	Tidak ditemukan kerentanan
A05 – Security Misconfiguration	Belum teruji	Tidak Adanya Security Headers (tingkat risiko rendah)
A06 - Vulnerable and Outdated Components	Belum teruji	Tidak ditemukan kerentanan
A07 - Identification and Authentication Failures	Belum teruji	Tidak ditemukan kerentanan
A08 - Software and Data Integrity Failures	Belum teruji	Tidak ditemukan kerentanan
A09 - Security Logging and Monitoring Failures	Belum teruji	Tidak ditemukan kerentanan
A10 - Server-Side Request Forgery	Belum teruji	Tidak ditemukan kerentanan

C. Rekomendasi Perbaikan

Berdasarkan hasil pengujian terhadap website Universitas XYZ, beberapa kelemahan telah ditemukan dan dikategorikan dalam OWASP Top 10. Setiap kerentanan yang teridentifikasi diberikan rekomendasi perbaikan yang spesifik agar sistem dapat ditingkatkan dari sisi keamanan.

1) A01 - Broken Access Control

Dalam kategori ini, ditemukan adanya celah pada endpoint wp-json yang memungkinkan siapa pun melakukan enumerasi pengguna. Endpoint ini merupakan bagian dari REST API WordPress yang secara default menampilkan informasi akun pengguna, termasuk username, meskipun pengguna tersebut tidak sedang login.

Adapun rekomendasi perbaikan yang bisa dapat dilakukan yakni dengan Membatasi akses ke endpoint REST API tersebut hanya untuk pengguna yang sudah terotentikasi. Terdapat beberapa plugin dari wordpress yang bisa digunakan untuk membatasi akses tersebut seperti : Disable Wp Rest API https://wordpress.org/plugins/disable-wp-rest-api/#installation

2) A02 - Cryptographic Failures

Pada kategori ini, ditemukan bahwa server masih mendukung protokol TLS versi 1.0 dan 1.1 yang telah dinyatakan usang. Meskipun saat ini serangan belum berhasil dieksploitasi, keberadaan protokol ini tetap menjadi risiko karena tidak sesuai dengan standar keamanan industri saat ini.

Adapun rekomendasi perbaikan yang bisa dapat dilakukan yakni dengan menonaktifkan TLS 1.0 dan TLS 1.1 di konfigurasi server dan pastikan hanya TLS 1.2 dan TLS 1.3 yang diperbolehkan. Berikut rekomendasi konfigurasi pada tiap servernya:

1. NGINX

   Ubah isi file /etc/nginx/nginx.conf agar hanya menggunakan TLSv1.2 dan TLSv1.3 pada ssl_protocols seperti dibawah ini:

   ssl_protocols TLSv1.2 TLSv1.3;

2. Apache

   Ubah isi file /etc/apache2/sites-available/default-ssl.conf agar hanya menggunakan TLSv1.2 dan TLSv1.3 pada SSLProtocol seperti dibawah ini

   SSLProtocol -all +TLSv1.2 +TLSv1.3

3. Cloudflare
   a. Masuk ke dashboard Cloudflare
   b. Buka tab SSL/TLS > Edge Certificates
   c. Scroll ke bagian “Minimum TLS Version” Atur ke TLS 1.2

3) A05 - Security Misconfiguration

Kerentanan ini muncul karena tidak adanya konfigurasi header keamanan seperti X-Frame-Options dan Strict-Transport-Security (HSTS) dalam respon server. Ketiadaan header tersebut memungkinkan serangan clickjacking, di mana penyerang dapat memanipulasi tampilan halaman untuk menipu pengguna melakukan tindakan berbahaya.

Adapun rekomendasi perbaikan yang bisa dapat dilakukan yakni dengan Menggunakan set security headers yang sudah disediakan oleh cloudflare:
https://developers.cloudflare.com/workers/examples/security-headers/

IV. KESIMPULAN

Penelitian ini telah berhasil melakukan analisis keamanan pada website milik Universitas XYZ menggunakan pendekatan penetration testing berbasis OWASP Top 10. Dengan skenario black-box, pengujian dilakukan secara sistematis melalui tahapan reconnaissance, scanning, vulnerability assessment, exploitation, post-exploitation, hingga reporting.

Berdasarkan hasil pengujian, ditemukan tiga kerentanan pada tingkat risiko rendah, yaitu: tidak diterapkannya beberapa header keamanan penting (seperti X-Frame-Options), dukungan terhadap protokol TLS versi lama, serta kemampuan user enumeration pada CMS WordPress. Meskipun tidak ditemukan eksploitasi tingkat lanjut, temuan tersebut menunjukkan bahwa sistem masih memiliki celah yang dapat dimanfaatkan apabila tidak segera diperbaiki.

Meskipun tidak ditemukan eksploitasi terhadap kerentanan dengan dampak tinggi, sistem tetap memerlukan penguatan pada aspek konfigurasi dan pembaruan komponen untuk mencegah risiko keamanan yang mungkin muncul di masa mendatang. Namun secara keseluruhan, tingkat keamanan website tergolong aman.

Dengan demikian, tujuan penelitian tercapai, yaitu mengidentifikasi tingkat keamanan, mendokumentasikan kerentanan, serta memberikan rekomendasi mitigasi untuk meningkatkan ketahanan website terhadap ancaman siber.

DAFTAR PUSTAKA

[1] F. Tinambunan, A. Junaidi, and A. Mustika Rizki, “PENGUJIAN SISTEM INFORMASI AKADEMIK UNIVERSITAS X MELALUI PENDEKATAN PENETRATION TESTING BERDASARKAN OWASP TOP 10,” JATI (Jurnal Mahasiswa Teknik Informatika), vol. 8, no. 1, pp. 1062–1069, Mar. 2024, doi: 10.36040/jati.v8i1.8920.

[2] S. Febriani, A. Muni, B. Rianto, M. Jalil, and Chrismondari, “Analisis Kerentanan Keamanan Sistem Informasi Akademik,” Jurnal Sistem Informasi(TEKNOFILE), vol. 2(6), pp. 409–420, Jun. 2024, Accessed: Mar. 17, 2025. [Online]. Available: https://jurnal.nawansa.com/index.php/teknofile/article/view/251

[3] R. Yati, “Survei APJII: Pengguna Internet di Indonesia Tembus 215 Juta Orang,” Bisnis Tekno, Mar. 08, 2023. Accessed: Sep. 02, 2025. [Online]. Available: https://teknologi.bisnis.com/read/20230308/101/1635219/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang

[4] G. Suprianto, “Penetration Testing Pada Sistem Informasi Jabatan Universitas Hayam Wuruk Perbanas,” InComTech : Jurnal Telekomunikasi dan Komputer, vol. 12, no. 2, p. 129, Aug. 2022, doi: 10.22441/incomtech.v12i2.15093.
[5] D. Perdana Putranto, B. Hananto, F. Ilmu Komputer, U. Pembangunan Nasional Veteran Jakarta, J. R. Fatmawati Raya, and P. Labu, “Analisis Keamanan Website Leads UPNVJ Terhadap Serangan SQL Injection & Sniffing Attack,” JURNAL INFORMATIK, vol. 8(1), pp. 230–238, Dec. 2022, Accessed: Mar. 17, 2025. [Online]. Available: https://doi.org/10.36040/jati.v8i1.8700
[6] M. Akil, E. I. Alwi, and S. M. Abdullah, “Analisa Keamanan Website Terhadap Serangan Html Injection Menggunakan Metode Penetrasion Testing,” VARIABLE RESEARCH JOURNAL, vol. 1(01), pp. 42–45, Apr. 2024, Accessed: Mar. 17, 2025. [Online]. Available: https://variablejournal.my.id/index.php/VRJ/article/view/9
[7] Ade Gustiyonoo, E. Irawadi Alwi, and S. Mubarak Abdullah, “Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing,” Cyber Security dan Forensik Digital, vol. 7, no. 1, pp. 25–33, Nov. 2024, doi: 10.14421/csecurity.2024.7.1.4432.
[8] A. K. Priyanka and S. Sai Smruthi, “Web Application Vulnerabilities: Exploitation and Prevention,” 2020 International Conference on Electrotechnical Complexes and Systems (ICOECS), pp. 1–5, Oct. 2020, doi: 10.1109/ICOECS50468.2020.9278437.
[9] A. Elanda and R. Lintang Buana, “ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10,” 2021. Accessed: Jul. 26, 2025. [Online]. Available: https://poltekstpaul.ac.id/jurnal/index.php/jelekn/article/view/455
[10] H. Sofyan, M. Sugiarto, and B. M. Akbar, “Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN ‘Veteran’ Yogyakarta,” Jurnal Informatika dan Teknologi Informasi, vol. 20, no. 2, pp. 153–162, 2023, doi: 10.31515/telematika.v20i2.7757153.
[11] Widi Linggih Jaelani, Y. Yanto, and F. Khoirunnisa, “PENETRATION TESTING WEBSITE DENGAN METODE BLACK BOX TESTING UNTUK MENINGKATKAN KEAMANAN WEBSITE PADA INSTANSI (REDACTED),” Naratif : Jurnal Nasional Riset, Aplikasi dan Teknik Informatika, vol. 5, no. 1, pp. 1–8, Jun. 2023, doi: 10.53580/naratif.v5i1.180.
[12] Open Web Application Security Project, “OWASP Top 10:2021.” Accessed: Aug. 06, 2025. [Online]. Available: https://owasp.org/www-project-top-ten/
[13] Muhamad Givari Ramadan and Mardi Hardjianto, “Pembuatan GH3RTZ Framework untuk Proses Reconnaissance dan Deteksi Celah Keamanan,” Jurnal Ticom: Technology of Information and Communication, vol. 13, no. 2, pp. 92–97, Jan. 2025, doi: 10.70309/ticom.v13i2.146.
[14] J. A. Ginting and I. G. G. Ngurah Suryantara, “PENGUJIAN KERENTANAN SISTEM DENGAN MENGGUNAKAN METODE PENETRATION TESTING DI UNIVERSITAS XYZ,” Infotech: Journal of Technology Information, vol. 7, no. 1, pp. 41–46, Jun. 2021, doi: 10.37365/jti.v7i1.105.
[15] I. G. P. K. Juliharta, N. L. P. N. S. Puja Astawa, and K. T. Werthi, “VULNERABILITY ASSESSMENT SISTEM MANAJEMEN KEAMANAN INFORMASI e-GOVERNMENT PEMERINTAH KOTA DENPASAR,” Jurnal Teknologi Informasi dan Komputer, vol. 8, no. 2, Jan. 2022, doi: 10.36002/jutik.v8i2.1589.
[16] G. A. Saputra, E. I. Alwi, A. Widya, and M. Gaffar, “Analisis Keamanan Website SIAKAD menggunakan Pentest Tools,” Literatur Informatika & Komputer, vol. 4, no. 4, pp. 379–388, 2024, doi: 10.33096/linier.v1i4.2537.
[17] F. Widianto, E. S. Wijaya, H. Harjono, and A. P. Wicaksono, “Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES,” Jurnal Pendidikan dan Teknologi Indonesia, vol. 5, no. 1, pp. 155–166, Jan. 2025, doi: 10.52436/1.jpti.609.
[18] K. M. Dell and E. S. Farrell, “RFC 8996 Deprecating TLS 1.0 and TLS 1.1,” Mar. 2021. [Online]. Available: https://www.rfc-editor.org/info/rfc8996
[19] National Security Agency, “Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations,” Jan. 2021. Accessed: Aug. 07, 2025. [Online]. Available: https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF
[20] F. Septian, H. Arfian, J. Sunupurwa Asri, and B. Tjahjono, “Pengujian Keamanan Website dengan Metode Penetration Testing (Studi Kasus: Universitas Esa Unggul),” Innovative: Journal Of Social Science Research, Sep. 2024, doi: 10.31004/innovative.v4i5.15197.