ANALISIS KEAMANAN WEBSITE E-LIBRARY KAMPUS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD)

Farah Akmalia Maylani, Muhlis Tahir, Naila Nataswa Juniar, Devita Sari, Widya Ayu Zulaica, Ismael
Pendidikan Informatika, Universitas Trunojoyo
Jalan Raya Telang, Jawa Timur-Indonesia
farahamey1@gmail.com

ABSTRAK

Perkembangan teknologi informasi yang sangat cepat, khususnya dalam bidang e-commerce, telah mendorong inovasi di dalam sistem digital seperti e-library. Sistem ini berperan sebagai pengelola informasi berbasis web, memudahkan akses dan pemanfaatan sumber daya secara efisien. Namun, kemajuan ini juga menghadirkan tantangan besar dalam hal keamanan. Untuk menjaga keamanan sistem, diperlukan pendekatan yang terencana, termasuk penggunaan alat seperti Tenable Nessus Professional untuk mengidentifikasi kerentanan yang ada. Penelitian ini menganalisis keamanan website akademisi kampus menggunakan metode Penetration Testing Execution Standard (PTES) yang melibatkan lima tahap PTES: perencanaan dan pengumpulan informasi, analisis kerentanan, eksploitasi, serta pelaporan. Dalam proses pengujian keamanan, yang meliputi tahapan Perencanaan dan Reconnaissance, Pemindaian, Akses dan Pemeliharaan, serta Analisis dan Konfigurasi WAF, penelitian ini berhasil menemukan beberapa kerentanan yang perlu diperhatikan. Hasil analisis mengungkapkan adanya risiko, seperti direktori yang terbuka untuk publik dan potensi serangan clickjacking, yang masing-masing membutuhkan mitigasi melalui penerapan header keamanan dan pembaruan konfigurasi server. Berdasarkan klasifikasi tingkat kerentanan, ditemukan bahwa 68% kerentanan berada pada kategori low, 18% pada kategori medium, 3% pada kategori high, dan 8% masuk dalam kategori critical. Hasil ini menunjukkan bahwa meskipun sebagian besar kerentanan memiliki risiko rendah, terdapat beberapa celah kritis yang perlu segera diperbaiki untuk meningkatkan keamanan sistem secara menyeluruh.

Kata kunci : *Keamanan Website, E-Library, Penetration Testing, Kerentanan, Serangan Siber*

1. PENDAHULUAN

Selama ini teknologi informasi terus dan semakin berkembang pesat serta mengalami banyak sekali kemajuan. Salah satu bukti kemajuan dari teknologi informasi adalah hadirnya perpustakaan digital pada kampus. Perpustakaan digital atau e-library merupakan suatu sistem yang menyimpan informasi dan sumber daya yang dimiliki dengan memanfaatkan media elektronik seperti website [1].

Sistem informasi e-library berperan penting sebagai pengelola informasi, yang harapannya dapat memaksimalkan potensi dalam diri individu agar lebih giat membaca dengan adanya perpustakaan berbasis digital atau website [2].

Namun, berkembangnya teknologi informasi juga mempengaruhi akan keamanan dari suatu system. Keamanan system informasi ialah cara melakukan pencegahan terhadap penipuan atau mendeteksi akan adanya penipuan didalam system informasi [3].

Saat ini, keamanan menjadi unsur yang penting pada penyusunan jaringan komputer dalam web server [4].

Karena dalam konteks perkembangan teknologi yang pesat membuat serangan-serangan terhadap keamanan suatu sistem juga terus meningkat melalui berbagai bentuk taktik ancaman yang makin canggih. Walaupun begitu terkadang keamanan dari suatu sistem kerapkali disepelekan oleh pihak yang berhubungan. Ancaman keamanan jaringan dalam bidang digital menjadi suatu permasalahan yang bisa berdampak pada system, contohnya bisa terjadi pada sebuah website[5].

Website adalah sebuah media yang menyediakan informasi dengan menawarkan bermacam kemudahan untuk memberikan informasi ke masyarakat luas [6].

Kemudian penggunaan website sebagai media penyebaran informasi sangatlah membantu karena cakupannya yang luas, khususnya pada website e-library kampus. System e-library kampus diciptakan untuk meningkatkan kemudahan civitas akademika dalam mengatur dan menyimpan informasi dengan memanfaatkan system berbasis web. Sehubungan dengan hal tersebut maka melakukan tindakan pengamanan layanan informasi e-library situs web tersebut sangat diperlukan.

Serangan siber terhadap website e-library semakin meningkat dalam beberapa tahun terakhir. Beberapa jenis serangan yang sering terjadi meliputi SQL Injection, Cross-Site Scripting (XSS), dan Distributed Denial of Service (DDoS). Sebuah penelitian menunjukkan bahwa serangan SQL Injection dapat menyebabkan kebocoran data pengguna dan dokumen akademik, yang menjadi ancaman serius bagi institusi Pendidikan [7].

Pada tahun 2022, Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa Indonesia mengalami peningkatan jumlah serangan siber yang signifikan, termasuk serangan terhadap sistem informasi akademik dan perpustakaan digital [8].

Dampak dari serangan ini sangat signifikan, mulai dari pencurian data pribadi hingga perubahan

atau penghapusan dokumen akademik yang dapat memengaruhi kredibilitas institusi. Oleh karena itu, analisis keamanan terhadap website e-library diperlukan untuk mengidentifikasi dan menutup celah keamanan guna mengurangi risiko serangan siber. Studi terbaru menunjukkan bahwa layanan open access di perpustakaan perguruan tinggi juga rentan terhadap ancaman siber, sehingga diperlukan langkah mitigasi yang lebih baik [9].

Menjaga asset informasi merupakan salah satu kewajiban untuk keberlangsungan dari website, dan diperlukan pendekatan yang terorganisir secara menyeluruh dalam implementasinya. Melindungi informasi atau data website bisa dengan cara melakukan identifikasi akan kerentanan keamanan dari website menggunakan sebuah alat terpercaya berbasis web yaitu *Tenable Nessus Professional*. Dengan menggunakan web tersebut dapat membantu dalam meningkatkan keamanan website dan mengurangi resiko akan terjadinya serangan pada keamanan. Manajemen keamanan informasi yang berpengaruh juga mencakup dari proses dan praktek secara menyeluruh agar dapat mengolah potensi rentannya keamanan informasi [10].

Salah satu bentuk pengamanan informasi adalah dengan melakukan uji penetrasi yang digunakan untuk mengevaluasi keamanan sistem computer dengan menstimulasikan serangan *cyber*. Metode uji penetrasi yang mudah digunakan dan dapat memberikan deskripsi yang mendetai pada tiap-tiap tahap pengujian adalah PTES. *Penetration Testing Execution Standart (PTES)* memiliki lima bagian utama yang mencakup seluruh aspek pengujian penetrasi diantaranya adalah interaksi dan pengumpulan informasi, pemodelan ancaman, analisis kerentanan, eksploitasi, dan pelaporan [11].

Hasil dari analisis kerentanan dapat membantu pihak pengelola sistem menghindari dan menangani efek resiko pada sistem. Oleh karena itu, pada sistem informasi e-library tersebut memerlukan penilaian keamanan atau *Security Assessment.*

2. TINJAUAN PUSTAKA

2.1. Keamanan Website

Website adalah salah satu teknologi informasi, yang digunakan sebagai media untuk menjangkau konsumen yang tersebar di seluruh dunia dengan syarat terkoneksi jaringan internet [12].

Keamanan website penting untuk melindungi data pengguna. Hal ini ditegaskan oleh Fatkhurozzi, Muhammad bahwa Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaan dan mengantisipasi ketika jaringan dapat ditembus [13].

Keamanan Website adalah tindakan atau praktik yang dilakukan untuk mengamankan situs web dari akses yang tidak sah.

2.2. E-Library Kampus

E-library adalah salah satu bukti perkembangan teknologi era 4.0 yang dimanfaatkan dengan maksimal, seperti halnya di kampus yang memanfaatkan teknologi e-library sehingga kegiatan menjadi lebih efektif [14].

Dari pernyataan diatas e-library dapat dikatakan sebagai alternaltif pemanfaatan perkembangan teknologi. E-library juga memiliki beberapa manfaat terutama bagi mahasiswa, karena e-library ini dapat diakses diaman pun dan kapanpun. Selain meiliki manfaat tentunya e-library ini juga memiliki beberapa kerentanan seperti yang telah dijelaskan oleh Chandra, Joko Christian (2022) dalam jurnalnya bahwa karena sifat kerjanya yang berbasis web, keamanan layanan e-learning rentan terhadap serangan eksternal [15] .

2.3. PTES

PTES (Penetration Testing Execution Standard) merupakan standar atau kerangka kerja yang dirancang untuk memberikan panduan menyeluruh dalam melakukan uji penetrasi (penetration testing) pada sistem, aplikasi, atau pun jaringan. Fase PTES mencakup berbagai tahapan mulai dari perencanaan awal hingga pelaporan hasil uji. Standar ini bertujuan untuk memastikan bahwa pengujian penetrasi dilakukan secara sistematis, terstruktur, dan sesuai dengan kebutuhan keamanan sistem yang diuji [16]. Metode Penetration Testing Execution Standard (PTES) yang merupakan panduan metodologi tentang apa yang diperlukan untuk uji penetrasi yang efektif [17].

Penelitian terdahulu menunjukkan bahwa metode penetration testing digunakan untuk mengidentifikasi kelemahan dalam sistem, jaringan, atau aplikasi web dengan mensimulasikan serangan secara langsung. Hasil pengujian menggunakan Acunetix dalam sebuah penelitian menunjukkan bahwa website min2kotabengkulu.sch.id memiliki kerentanan tingkat rendah dan dianggap cukup aman dari serangan siber [18].

Tanpa adanya keamanan pada sistem, banyak hacker yang akan dengan mudah mengambil alih sistem. Dalam upaya mengatasi permasalahan keamanan, diperlukan suatu metode yang menjamin keamanan. Pada penelitian ini menggunakan metode Penetration Testing dengan menggunakan framework ISSAF. Hasil dari penelitian ini diharapkan dapat mengetahui celah keamanan pada LMS yang digunakan saat ini [19].

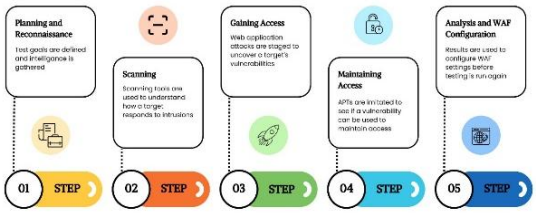
Pengujian menggunakan metode Penetration Testing Execution Standard (PTES) yang merupakan panduan metodologi tentang apa yang diperlukan untuk uji penetrasi yang efektif. Hasil yang didapat setelah uji penetrasi testing yaitu terdapat 14 celah keamanan dimana beberapa celah diantaranya menjadi bahan untuk di ek- sploitasi. Celah keamanan tersebut yaitu Cloud Metadata Potentially Exposed, Absence of Anti-CSRF Tokens, SQL Injection, Missing Anti-clickjacking Header dan Vulnerable JS Library [17].

3. METODE PENELITIAN

Penelitian ini menggunakan metode Penetration Testing Execution Standard (PTES) dengan pendekatan deskriptif untuk menganalisis keamanan website Akademisi Kampus. Fokus penelitian terpusat pada satu Website Akademisi Kampus, dan lokasi penelitian dilakukan secara spesifik di . Gambar 1 menunjukkan bahwa pemeriksaan penetrasi, yang melibatkan sejumlah prosedur, akan menjadi variabel fokus analisis. Planing and Reconnaissance adalah tahap pertama, yang mencakup sublangkah Identifikasi, Konfirmasi, dan Pengumpulan Data [20].

Selanjutnya, pengumpulan informasi akan dilakukan dengan alat seperti whatweb. Pada tahap ketiga, evaluasi risiko akan dilakukan dengan menggunakan Nessus Professional. Tahap keempat eksploitasi akan melibatkan penggunaan Web Directory dan ClickJacking. Terakhir, tahap kelima adalah laporan. Di sini, hasil dari seluruh proses akan dibahas secara menyeluruh. Dengan pendekatan yang terstruktur ini, penelitian ini bertujuan untuk memberikan wawasan mendalam terhadap kerentanan keamanan website Akademisi Kampus.

PTES (Penetration Testing Execution Standard) merupakan standar atau kerangka kerja yang dirancang untuk memberikan panduan menyeluruh dalam melakukan uji penetrasi (penetration testing) pada sistem, aplikasi, atau pun jaringan. Fase PTES mencakup berbagai tahapan mulai dari perencanaan awal hingga pelaporan hasil uji. Standar ini bertujuan untuk memastikan bahwa pengujian penetrasi dilakukan secara sistematis, terstruktur, dan sesuai dengan kebutuhan keamanan sistem yang diuji. Ada 5 langkah dalam melakukan pengujian penetrasi menurut PTES [21].



Gambar 1. Metode *PTES*

Untuk memberikan hasil yang sesuai, maka diperlukan beberapa tahapan. Tahapan yang dibutuhkan untuk metode *PTES* adalah sebagai berikut:

3.1. *Planning and Reconnaissance*

Planning and Reconnaissance adalah tahap awal dalam proses pengujian penetrasi (penetration testing) yang berfokus pada perencanaan dan pengumpulan informasi tentang target [22].

Pada tahap ini, tim keamanan akan menentukan tujuan pengujian, menetapkan ruang lingkup sistem atau jaringan yang akan diuji, serta memilih metode yang paling sesuai untuk melakukan pentesting. Selain itu, para profesional keamanan juga akan mengidentifikasi risiko serta ancaman potensial yang mungkin muncul selama pengujian. Untuk memastikan pengujian berjalan efektif, tim akan melakukan pemetaan menyeluruh terhadap infrastruktur, sistem, dan lingkungan teknis dari target. Dengan memahami struktur sistem secara mendalam sebelum melakukan simulasi serangan, tim dapat meningkatkan efektivitas pengujian serta mengidentifikasi celah keamanan dengan lebih akurat. Pemetaan yang dilakukan dengan cermat tidak hanya membantu dalam menemukan kelemahan sistem, tetapi juga meminimalkan risiko yang tidak diinginkan selama proses pengujian. Dengan pendekatan yang sistematis, tahap ini memungkinkan evaluasi keamanan suatu sistem atau aplikasi secara lebih terarah dan efisien.

3.2. *Scanning*

Scanning adalah tahap penting dalam pengujian penetrasi yang berfokus pada identifikasi dan pemindaian sistem atau jaringan untuk mengungkap celah keamanan yang mungkin ada. Dalam proses ini, berbagai teknik dan alat digunakan untuk menganalisis target, seperti port scanning untuk mendeteksi port terbuka, vulnerability scanning untuk menemukan potensi kerentanan, dan network scanning untuk memahami struktur jaringan secara lebih mendalam [23].

Tujuan utama dari tahap scanning ini adalah memberikan tim pengujian penetrasi wawasan yang lebih jelas mengenai sistem yang diuji, sehingga mereka dapat mengevaluasi tingkat risiko serta kelemahan yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab. Hasil dari pemindaian ini menjadi dasar bagi langkah-langkah selanjutnya dalam proses pengujian penetrasi. Namun, penting untuk memastikan bahwa setiap pemindaian dilakukan dengan izin resmi dan dalam konteks yang sah untuk menghindari dampak negatif terhadap sistem atau jaringan yang diuji. Proses scanning ini merupakan bagian dari langkah sistematis dalam menilai tingkat keamanan suatu sistem atau lingkungan teknologi informasi secara menyeluruh.

3.3. *Gaining Access*

Gaining Access adalah tahap dalam pengujian penetrasi yang bertujuan untuk memperoleh akses ke sistem atau jaringan target dengan mengeksploitasi kelemahan yang telah ditemukan pada tahap sebelumnya. Akses ini memungkinkan tim pengujian untuk menilai sejauh mana suatu sistem rentan terhadap serangan yang mungkin dilakukan oleh pihak yang tidak berwenang [5].

Pada tahap ini, penguji mencoba membuktikan dan mengeksploitasi celah keamanan dengan berbagai teknik, seperti memasukkan input yang tidak terduga, mengeksekusi kode berbahaya, atau menggunakan metode eksploitasi lainnya. Tujuan utamanya adalah menguji aspek kerahasiaan dalam sistem. Jika eksploitasi berhasil, penguji bisa mendapatkan akses

ke akun penting seperti administrator atau memperoleh data sensitif, termasuk informasi perusahaan atau pengguna. Dalam konteks pengujian penetrasi, gaining access mencerminkan situasi di mana penguji berhasil masuk ke dalam sistem tanpa izin, meniru cara yang mungkin dilakukan oleh peretas berbahaya. Proses ini membantu mengidentifikasi potensi risiko keamanan dan memberikan wawasan tentang langkah-langkah yang perlu diambil untuk memperkuat sistem dari ancaman nyata.

3.4. *Maintaining Access*

Maintaining Access atau mempertahankan akses adalah tahap dalam uji penetrasi di mana penguji berusaha tetap berada di dalam sistem yang sudah berhasil mereka masuki. Setelah menemukan celah keamanan dan mendapatkan akses, langkah selanjutnya adalah memastikan bahwa akses tersebut tidak terputus dan tetap bisa digunakan tanpa terdeteksi [5].

Dalam tahap ini, penguji biasanya menggunakan berbagai cara untuk mempertahankan akses, misalnya dengan memasang backdoor, membuat akun pengguna baru dengan hak istimewa, atau mengeksploitasi kelemahan dalam sistem keamanan. Tujuan utamanya adalah untuk melihat apakah sistem memiliki mekanisme pertahanan yang cukup kuat untuk mendeteksi dan menghapus akses yang tidak sah. Simulasi ini penting karena dalam serangan nyata, peretas tidak hanya ingin masuk sebentar, tetapi juga mencari cara agar tetap bisa mengontrol sistem dalam jangka waktu lama tanpa ketahuan. Dengan melakukan tahap ini dalam pengujian penetrasi, tim keamanan bisa memahami bagaimana seorang peretas bisa bertahan dalam sistem mereka dan memperbaiki celah-celah yang memungkinkan hal itu terjadi. Namun, perlu diingat bahwa semua ini dilakukan dalam pengujian yang sah dengan izin dari pemilik sistem. Tujuannya bukan untuk benar-benar merusak sistem, melainkan untuk mengidentifikasi titik lemah dan membantu meningkatkan keamanannya sebelum diserang oleh pihak yang tidak bertanggung jawab

3.5. *Analysis and WAF Configuration*

Analysis and WAF Configuration atau tahap evaluasi dan peningkatan keamanan setelah tim pengujian berhasil masuk ke dalam sistem dan mengidentifikasi berbagai kelemahan keamanan, langkah berikutnya adalah Analisis dan Konfigurasi WAF (Web Application Firewall). Tahap ini berfokus pada evaluasi hasil pengujian serta penerapan langkah-langkah perbaikan untuk menutup celah keamanan yang ditemukan sebelumnya [5].

Pada tahap ini, tim penguji akan menyusun laporan yang berisi ringkasan temuan mereka, termasuk titik-titik lemah dalam sistem, risiko yang bisa muncul, serta rekomendasi perbaikan yang harus segera dilakukan. Laporan ini kemudian diberikan kepada pemilik sistem atau tim keamanan untuk ditindaklanjuti. Selain itu, konfigurasi ulang WAF (Web Application Firewall) juga menjadi bagian penting dalam tahap ini.

WAF digunakan untuk memantau dan mencegah serangan yang menargetkan aplikasi web, seperti SQL Injection, Cross-Site Scripting (XSS), dan serangan DDoS. Tim keamanan akan memastikan bahwa WAF diatur dengan benar agar dapat mendeteksi dan memblokir upaya peretasan sebelum mencapai sistem utama. Langkah ini sangat penting karena tidak hanya mengidentifikasi kelemahan yang ada, tetapi juga memastikan bahwa sistem telah diperbaiki dan lebih tahan terhadap serangan di masa mendatang. Dengan melakukan evaluasi ulang setelah perbaikan, organisasi dapat memastikan bahwa langkah-langkah yang diambil benar-benar efektif dalam meningkatkan keamanan sistem mereka.

4. HASIL DAN PEMBAHASAN

4.1. *Planning and Reconnaissance*

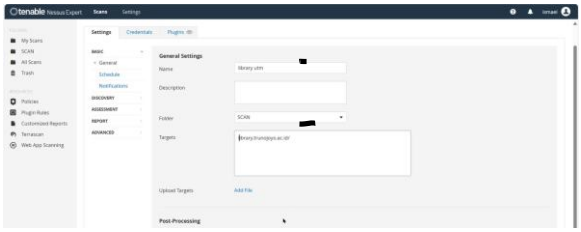
Planing and Reconnaissance digunakan untuk menjelaskan informasi mencakup beberapa elemen penting, seperti alamat IP, sistem operasi, target yang ingin dicapai dan layanan yang digunakan pada situs web. Perintah whatweb diterapkan pada URL situs web yang sedang diuji guna mencapai tujuan dari Planning Reconnaissance. Pada tahap ini teknik yang digunakan akan dijelaskan secara rinci dengan setiap hasil yang ditemukan akan dijaga kerahasiaannya. Hasil dari tahapan ini akan dijelaskan dan diberikan pemahaman yang baik tentang temuan yang telah terjadi dengan tujuan untuk memberi gambaran kepada pihak terkait sehingga pihak terkait dapat mengembangkan keamanan sistem dan layanan.

4.2. *Scanning*

Tahap pengujian selanjutnya adalah Scanning yang merupakan tahapan penting untuk mendeteksi kelemahan informasi yang ada pada sistem, jaringan, atau aplikasi. Langkah pertama yang dilakukan pada tahapan ini adalah pengumpulan informasi penting, identifikasi dan verifikasi data dengan tujuan supaya mendapatkan pemahaman menyeluruh tentang kelemahan keamanan yang bisa dimanfaatkan oleh kelompok atau individu. Hasil dari Scanning adalah mencatat secara detail mengenai kerentanan yang ada sehingga pengujian dapat membangun landasan informasi yang kuat. Dari hasil ini dapat mengatasi resiko keamanan, perbaikan sistem, dan membantu mengidentifikasi potensi ancaman.

a. Pembuatan Pemindaian (*Scan Creation*)

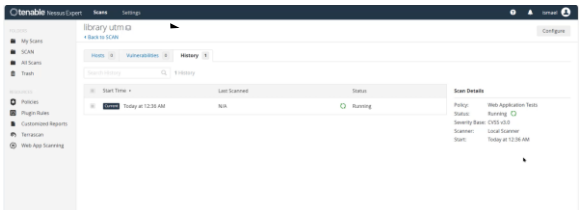
Pada tahap ini penguji menentukan target peninjauan bisa berupa IP address, domain, atau jaringan. Penguji memilih jenis target peninjauan Web Application Tests dan mulai mengisi Genneral Setting sebagai berikut :



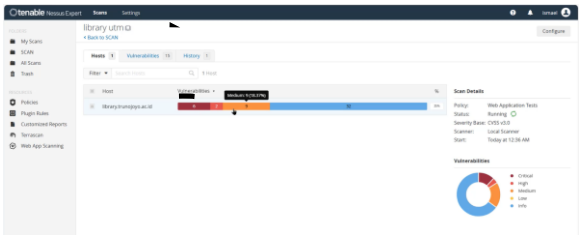
Gambar 2. Menentukan target website

b. Menjalankan Pemindaian (*Executing the Scan*)

Pada tahap ini Nessus akan memindai target, mengidentifikasi layanan, port yang terbuka, dan kemungkinan kerentanan. Proses ini bisa berlangsung dalam hitungan menit hingga jam tergantung pada ukuran target.



Gambar 3. Proses mencari kerentanan



Gambar 4. Presentase kerentanan website

c. Analisis Hasil Pemindaian (*Scan Result Analysis*)

Hasil dari proses ini dapat memberikan gambaran terkait potensi kerentanan berdasarkan tingkatanya dengan Tingkat keberhasilan eksploitasi 80%. Sedangkan untuk klasifikasi tingkat kerentananpada website ditemukan bahwa 68% kerentanan berada pada kategori low, 18% pada kategori medium, 3% pada kategori high, dan 8% masuk dalam kategori critical.

Table 1. Hasil proses identifikasi

No.	Kerentanan	Tingkat
1.	*Browsable Web Directories*	*Medium*
2.	*Web Application Pontially Vulnerable to Click Jacking*	*Medium*
3.	*Web Server (Multiple Issues)*	*Mixed*

Browsable Web Directories, ditemukannya direktori yang dapat diakses langsung pada server web merupakan risiko keamanan yang dapat dimanfaatkan oleh penyerang untuk mengakses informasi sensitif atau menemukan celah eksploitasi lebih lanjut. Dengan menerapkan solusi yang disarankan seperti menonaktifkan directory indexing, membatasi akses, serta menggunakan firewall, maka potensi risiko ini dapat diminimalisir dan sistem menjadi lebih aman dari ancaman keamanan siber. Dengan langkah-langkah perbaikan yang telah dilakukan, diharapkan server web dapat lebih terlindungi dari potensi kebocoran data dan serangan siber di masa mendatang.

Web Application Pontially Vulnerable to Click Jacking, Clickjacking adalah serangan keamanan yang memanfaatkan teknik manipulasi antarmuka untuk menipu pengguna agar melakukan tindakan tanpa sadar, seperti mengklik tombol berbahaya atau memberikan akses ke informasi sensitif. Kerentanan ini terjadi ketika situs web tidak memiliki perlindungan terhadap penyematan dalam iframe oleh domain lain. Untuk mencegah clickjacking, penting untuk menerapkan header keamanan seperti X-Frame-Options dan Content Security Policy (CSP), serta menggunakan teknik frame-busting dengan JavaScript. Selain itu, pengujian keamanan secara berkala menggunakan alat seperti Nessus, OWASP ZAP, atau Burp Suite sangat disarankan untuk mendeteksi dan mengatasi potensi ancaman ini. Dengan mengadopsi langkah-langkah mitigasi yang tepat, organisasi dapat mengurangi risiko eksploitasi clickjacking dan meningkatkan keamanan serta kepercayaan pengguna terhadap aplikasi web mereka.

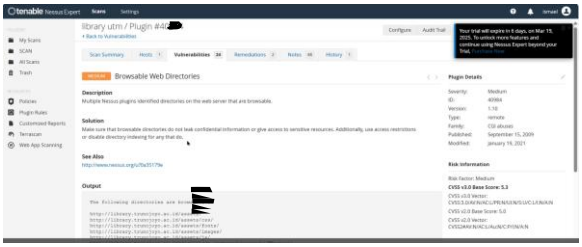
Temuan penelitian selanjutnya ialah, terdapat jenis permasalahan Clickjacking X-Frame-Options dan Clickjacking CSP Frame-Ancestors Missing. Keduanya memiliki tingkat kerentanan LOW. X-Frame-Options header dapat diatasi dengan membatasi cara halaman web dapat dimuat dalam bingkai. Sedangkan Frame-Ancestors adalah direktif dalam CSP yang membatasi halaman mana yang boleh memuat halaman dalam bingkai. Dari permasalahan dan solusi tersebut, peneliti melakukan scanning menggunakan Accunetix dan menghasilkan website hanya memiliki kerentanan di level low sehingga website cukup aman dan hanya perlu dilakukan beberapa penyesuaian agar keamanan website lebih meningkat [5].

Adapun Vulnerability scanning adalah kegiatan proses memperoleh informasi vulnerability network dengan memanfaatkan berbagai tools network scanning dan vulnerability scanner, seperti port yang terbuka, bugs aplikasi dan mengetahui serangan - serangan yang akan terjadi terhadap kerentaan website yang ada, yang akan berdampak cukup buruk apabila terjadi [13].

Web Server (Multiple Issues), Berdasarkan hasil pemindaian keamanan menggunakan Nessus, ditemukan berbagai kerentanan pada server web, yang dikategorikan sebagai "Web Server (Multiple Issues)." Kerentanan ini mencakup konfigurasi server yang tidak aman, penggunaan perangkat lunak yang sudah usang, kebocoran informasi, direktori yang dapat diakses secara publik, serta kelemahan dalam enkripsi dan teknologi web yang digunakan. Untuk mengatasi permasalahan ini, organisasi harus mengambil langkah-langkah mitigasi seperti memperbarui perangkat lunak, mengamankan konfigurasi server, membatasi akses ke direktori sensitif, menerapkan

enkripsi yang kuat, dan melakukan uji keamanan secara berkala. Penggunaan alat seperti Nessus, OWASP ZAP, dan Nmap dapat membantu dalam mengidentifikasi serta memperbaiki celah keamanan sebelum dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Dengan menerapkan praktik keamanan yang baik, organisasi dapat mengurangi risiko serangan siber, melindungi data sensitif, dan memastikan keandalan serta integritas sistem web mereka.

Pada tahap ini ditemukan permasalahan "*Multiple Nessus plungins identified directories on the web server that are browsable*", yang berarti terdapat folder atau direktori di server web yang bisa diakses secara langsung oleh pengguna melalui browser. Jika tidak dikonfigurasi dengan benar, akan menyebabkan kebocoran informasi sensitif atau membuka celah keamanan.



Gambar 5. Kerentanan website

Nessus juga memberikan solusi "*Make sure that browsable directories do not leak confidental information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do*" atau memastikan direktori yang dapat diakses tidak mengandung informasi rahasia atau memberikan akses ke sumber daya sensitif. Jika Nessus menemukan direktori server yang bisa diakses secara publik bisa meningkatkan risiko kebocoran informasi. Untuk mengatasinya hal tersebut dapat menonaktifkan directory indexing, atur izin akses, dan pindahkan file sensitif ke lokasi yang lebih aman.

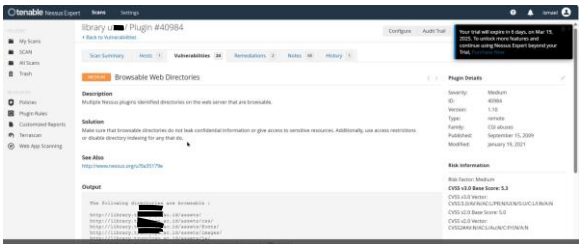
4.3. *Gaining Access*

Pada bagian Gaining Access, akan terhubung ke jaringan untuk melakukan serangan dan mendapatkan informasi yang lebih akurat ke dalam sistem website yang dituju [24].

Tujuan utama tahap ini adalah mengevaluasi seberapa mudah sistem keamanan dapat ditembus dan menunjukkan bahaya keamanan yang mungkin terjadi jika penyerang tidak sah berhasil mengakses server.

4.4. *Maintaining Access*

Mintanning Acces adalah tahapan penting yang bertujuan untuk mempertahankan kemanan dan menawarkan solusi terkait akses yang telah berhasil didapatkann ke dalam sistem setelah berhasil mendapatkan celah keamanannya. Tujuan dari Maintanning Access untuk memungkinkan sistem yang ditargetkan untuk memperoleh informasi yang dianggap berharga dan kemudian berhasil mengekstraknya dari sistem [25].



Gambar 6. Solusi kerentanan website

Informasi detail ini memungkinkan peneliti untuk lebih memahami karakteristik kerentanan dan dapat menerapkan langkah pengurangan resiko yang sesuai. Hasil dari proses ini dapat memberikan kesempatan untuk menjaga, memberikan solusi dan mengevaluasi respon sistem pemeliharaan akses. Pada proses ini juga dapat menangani kerentanan yang teridentifikasi serta berkontribusi pada peningkatan pemahaman pencegahan terkait potensi resiko keamanan yang ada dan memperkuat ketahanan sistem terhadap ancaman yang mungkin akan muncul.

4.5. *Analysis and WAF Configuration*

Pada tahap Analysis and WAF Configuration ini menunjukkan penelitih untuk memperoleh akses ilegal ke dalam suatu sistem jaringan dengan tujuan untuk mendapatkan hak akses ilegal berdasarkan temuan dari penelitihan sebelumnya. Proses ini dapat mengidentifikasi dan menilai seberapa jauh sistem keamanan dapat ditembus dan mencegah resiko keamanan yang mungkin muncul jika seseorang berhasil mendapatkan akses yang tidak sah ke server. Pada kegiatan ini meliputi penggunaan strategi peretasan yang ditujukan untuk memanfaatkan kelemahan yang telah ditemukan untuk dianalisis.

Hasil dari proses ini memberikan pemahaman mengenai ketidaknyamanan sistem dan memberikan penjelasan tentang kerentanan yang dapat dimanfaatkan oleh pihak yang tidak berhak. Proses ini sangat penting untuk tujuan meningkatkan daya tahan sistem melalui identifikasi dan pencegahan potensi ancaman. Hasil dari proses ini akan dianalisis secara rinci dengan tujuan utama untuk menyajikan pemahaman yang lebih menyeluruh mengenai sejauh mana keamanan sistem yang telah diuji. Dengan melakukan analisis ini, penelitihan keamanan dapat memberikan informasi yang lebih jelas mengenai titik lemah dan potensi yang mungkin membutuhkan peningkatan dan memberikan rekomendasi keamanan yang lebih efisien.

5. KESIMPULAN DAN SARAN

Dalam penelitian ini, dilakukan pengujian keamanan terhadap website E-Library menggunakan metode Penetration Testing Execution Standard (PTES). Pengujian dilakukan melalui beberapa

tahapan, yaitu Planning and Reconnaissance, Scanning, Gaining Access, Maintaining Access, serta Analysis and WAF Configuration. Hasil pengujian menunjukkan bahwa sistem memiliki berbagai tingkat kerentanan, dengan rincian sebagai berikut: 68% kerentanan ditemukan berada pada kategori rendah (low), 18% dalam kategori sedang (medium), 3% dalam kategori tinggi (high), dan 8% dalam kategori kritis (critical). Pada tahap Scanning, ditemukan beberapa celah keamanan yang dapat dieksploitasi untuk memperoleh akses tidak sah ke dalam sistem. Pengujian Gaining Access berhasil mendapatkan akses dengan tingkat keberhasilan tertentu, sementara pada tahap Maintaining Access ditemukan potensi bagi penyerang untuk mempertahankan akses tanpa terdeteksi. Implementasi Web Application Firewall (WAF) yang diterapkan dalam tahap Analysis and WAF Configuration terbukti mampu meningkatkan keamanan sistem dengan mengurangi kemungkinan eksploitasi lebih lanjut.

Berdasarkan hasil penelitian ini, terdapat beberapa saran yang dapat diterapkan untuk meningkatkan keamanan sistem. Pertama, perlu dilakukan peningkatan pengamanan terhadap kerentanan yang ditemukan, terutama pada kategori high dan critical, dengan menerapkan patch keamanan serta konfigurasi sistem yang lebih ketat. Kedua, monitoring sistem secara berkala harus dilakukan untuk mendeteksi dan menangani ancaman sebelum menjadi eksploitasi serius. Ketiga, pengembangan kebijakan keamanan yang lebih baik, seperti penggunaan autentikasi ganda (2FA) dan pembatasan akses berbasis peran (RBAC), dapat membantu mengurangi risiko serangan. Ke depannya, penelitian lebih lanjut dapat dilakukan dengan menguji efektivitas berbagai sistem keamanan tambahan, seperti intrusion detection systems (IDS) dan keamanan berbasis AI, untuk meningkatkan ketahanan sistem terhadap ancaman siber yang lebih kompleks.

DAFTAR PUSTAKA

[1] A. Purnamayanti and N. Oktaria, "Kesiapan perpustakaan SMA Muhammdiyah 2 Bandar Lampung dalam pengembangan website E-Perpustakaan," *Informatio: Journal of Library and Information Science*, vol. 2, no. 1, pp. 19–28, 2022.

[2] I. Muttaqin, "E-Library Berbasis Website Menggunakan Metode Algoritma Apriori Dan Sequential Search," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 9, no. 2, pp. 1223–1232, 2022.

[3] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)," *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 3, no. 5, pp. 564–573, 2022.

[4] H. Herman, I. Riadi, Y. Kurniawan, and I. A. Rafiq, "Analisis Keamanan Website Menggunakan Information System Security Asessment Framework(ISSAF)," *Jurnal Teknologi Informatika dan Komputer*, vol. 9, no. 1, pp. 126–136, Mar. 2023, doi: 10.37012/jtik.v9i1.1439.

[5] M. Tahir and M. R. Ardiansyah, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)," *Jurnal Teknik Informatika UNIKA Santo Thomas*, pp. 118–125, 2024.

[6] M. Arafat, Y. Trimarsiah, and H. Susantho, "Rancang Bangun Sistem Informasi Pemesanan Online Percetakan Sriwijaya Multi Grafika Berbasis Website," *INTECH (Informatika dan Teknologi)*, vol. 3, no. 2, pp. 58–63, 2022.

[7] N. S. S. Yomo, A. Z. Mardiansyah, and I. W. A. Arimbawa, "Deteksi Serangan SQL Injection Menggunakan Security Information and Event Management (SIEM) Wazuh (Sudi Kasus: Sistem Informasi Akademik Universitas Mataram)," 2023.

[8] B. Siber and S. Negara, "Lanskap Keamanan Siber Indonesia Tahun 2022," 2023.

[9] Y. Bahgie and A. Masruri, "Keamanan Informasi pada Layanan Open Access di Perpustakaan Perguruan Tinggi," *Indonesian Journal of Library and Information Science*, vol. 4, no. 2, pp. 40–46, 2023.

[10] R. Vansuri *et al.*, "Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi," *Jurnal Ilmu Multidisplin*, vol. 2, no. 1, pp. 106–113, 2023.

[11] S. U. Sunaringtyas and D. S. Prayoga, "Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On," *Edu Komputika Journal*, vol. 8, no. 1, pp. 48–56, 2021.

[12] S. Soedewi, A. Mustikawan, and W. Swasty, "Penerapan metode design thinking pada perancangan website umkm kirihuci," 2022.

[13] M. Fatkhurozzi, "Analisa Keamanan Website Menggunakan Metode Footprinting Dan Vulnerability Scanning Pada Website Kampus," *Prosiding Seminar Nasional Informatika Bela Negara*, vol. 2, pp. 144–148, 2021, doi: 10.33005/santika.v2i0.74.

[14] F. Y. Nagifea, "OPTIMALISASI LAYANAN E-LIBRARY BERBASIS SLiM UNTUK MENINGKATKAN LITERASI SISWA PADA PERPUSTAKAAN SMKN 6 JEMBER," *Jurnal Technopreneur (JTech)*, vol. 11, no. 2, pp. 76–84, 2023, doi: 10.30869/jtech.v11i2.1250.

[15] J. C. Chandra, "Analisis Keamanan Layanan E-Learning Terhadap Serangan Dos Dan Implementasi Mitigasi Pada Universitas Budi Luhur," *Jurnal TICOM: Technology of*

Information and Communication, vol. 10, no. 3, p. 2022, 2022.

[16] M. Tahir and M. Risky, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)," vol. 09, pp. 118–125, 2024.

[17] L. F. Burhani and D. Priyawati, "Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (Ptes)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 1, pp. 307–319, 2024, doi: 10.29100/jipi.v9i1.4455.

[18] Muhammad Risky Ardiansyah *et al.*, "Analisis Kerentanan Keamanan Website Menggunakan Metode PTES (Penetration Testing Execution And Standart)," *Nuansa Informatika*, vol. 18, no. 2, pp. 145–153, 2024, doi: 10.25134/ilkom.v18i2.119.

[19] R. Umar, I. Riadi, and S. A. Wicaksono, "Security Analysis of Learning Management System Using Penetration Testing with ISSAF Framework," *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, vol. 12, no. 1, pp. 59–68, 2024, doi: 10.33558/piksel.v12i1.8331.

[20] S. T. M. I. K. LIKMI, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," *pdfs. semanticscholar. org*.

[21] S. G. Saputra and B. P. Zen, "Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES)," *Jurnal Sistem Informasi Galuh*, vol. 1, no. 2, pp. 43–51, 2023.

[22] J. A. Ginting and I. G. G. N. Suryantara, "Pengujian Kerentanan Sistem Dengan Menggunakan Metode Penetration Testing Di Universitas Xyz," *Infotech: Journal of Technology Information*, vol. 7, no. 1, pp. 41–46, 2021.

[23] M. D. Khoiroh *et al.*, "PENETRATION TESTING UNTUK MENGUJI KERENTANAN SISTEM INFORMASI PEMERINTAH DAERAH," *Jurnal Sistem dan Teknologi Informasi (JSTI)*, vol. 6, no. 3, 2024.

[24] F. Fachri, A. Fadlil, I. Riadi, A. Dahlan, Y. Jln Soepomo, and I. Artikel, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform*, vol. 8, no. 2, pp. 183–190, 2021.

[25] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *Jurnal Informatika*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854