Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)

Muhlis Tahir[1] , Muhammad Risky[2]
[1,2]Universitas Trunojoyo Madura; Jl. Raya Telang Bangkalan
email : [1]muhlis.tahir@trunojoyo.ac.id , [2]riskyardiansyahh7@gmail.com

Abstrak

Dalam era digitalisasi, keamanan informasi menjadi krusial, terutama di entitas pemerintahan. Penelitian ini berfokus pada identifikasi dan analisis kerentanan keamanan di website Dinas Pemerintahan Yogyakarta, dengan menggunakan metode Penetration Testing Execution and Standard (PTES). Metode penelitian ini bersifat kuantitatif dan deskriptif, digunakan untuk mengevaluasi keamanan website dan memberikan masukan untuk perbaikan. Penelitian melibatkan tool Tenable Nessus Professional yang mengevaluasi kerentanan, seperti Browsable Web Directories dan Web Potentially Clickjacking. Tahapan PTES yang tercakup mencakup Perencanaan, Pengumpulan Data, Pemindaian, Hak Akses, Keamanan, dan konfigurasi Web Application Firewall (WAF). Harapannya, metode ini memberikan pemahaman mendalam tentang potensi ancaman dan kerentanan dalam sistem informasi pemerintahan, serta menyajikan solusi. Hasil penelitian diharapkan memberikan edukasi dan wawasan tentang keamanan website Dinas Pemerintahan Yogyakarta. Ini memungkinkan pihak terkait untuk mengambil langkah-langkah preventif dan korektif, meningkatkan keamanan, serta melindungi integritas dan kerahasiaan data entitas pemerintahan. Sebagai hasilnya, sistem informasi pemerintahan diharapkan lebih aman dan tahan terhadap potensi ancaman siber.

Kata kunci*—Pengujian Penetrasi, Penilaian Kerentanan, Situs Web, Nessus*

Abstract

In the era of digitalization, information security becomes crucial, especially in governmental entities. This research focuses on identifying and analyzing security vulnerabilities on the website of the Yogyakarta Government Office, using the Penetration Testing Execution and Standard (PTES) method. This research method is quantitative and descriptive, employed to evaluate the security of the website and provide input for improvements. The study involves the use of Tenable Nessus Professional tools that assess vulnerabilities such as Browsable Web Directories and Web Potentially Clickjacking. The PTES stages covered in the research include Planning, Data Gathering, Scanning, Access Rights, Security, and Web Application Firewall (WAF) configuration. The hope is that this method provides a profound understanding of potential threats and vulnerabilities in the government information system and presents solutions. The research results are expected to offer education and insights into the security of the Yogyakarta Government Office website. This allows relevant parties to take preventive and corrective measures, enhance security, and protect the integrity and confidentiality of government entity data. As a result, the government information system is anticipated to be more secure and resilient against potential cyber threats.

Keywords*—Penetration Testing, Vulnerability Assessment, Website, Nessus*

1. PENDAHULUAN

Dengan kemajuan yang pesat dalam Teknologi Informasi (TI), kebutuhan akan suatu kerangka dan mekanisme pembelajaran berbasis TI menjadi suatu keharusan yang tidak dapat dihindari. Ini memerlukan keamanan yang solid dalam suatu sistem. Keamanan menjadi elemen kritis dalam pembangunan jaringan komputer di dalam server web[1]. Keamanan sistem informasi menjadi isu krusial dalam evolusi teknologi informasi dan komunikasi saat ini. Penting bagi bisnis untuk menjaga keamanan aset informasi organisasi dengan menerapkan pendekatan yang menyeluruh dan terstruktur, bertujuan memberikan perlindungan terhadap berbagai risiko yang mungkin dihadapi oleh organisasi. Informasi mempunyai bemacam bentuk format dianataranya adalah format teks,

audio, visual, dan video. Berkaitan dengan hal tersebut maka diperlukan tindakan untuk melakukan manajemen pengelolaan informasi yang bertujuan untuk mengamankan aspek penting dari layanan situs web.

Keamanan sistem informasi menjadi sorotan utama dalam evolusi teknologi informasi dan komunikasi. Perlindungan terhadap aset informasi organisasi dianggap krusial untuk kelangsungan bisnis, dan implementasinya memerlukan pendekatan yang terstruktur dan menyeluruh. Pendekatan ini dirancang untuk melindungi organisasi dari berbagai variasi risiko yang mungkin dihadapinya.Dalam menjawab tantangan keamanan ini, diperlukan solusi yang mencakup seluruh aspek sistem informasi. Ini termasuk perlindungan terhadap integritas, kerahasiaan, dan ketersediaan data, serta keamanan transaksi dan komunikasi yang terjadi di lingkungan organisasi. Penerapan metode keamanan yang holistik diperlukan agar tidak hanya mencakup perlindungan terhadap satu aspek saja, tetapi juga melibatkan serangkaian langkah-langkah yang komprehensif dan berlapis-lapis. Pentingnya memahami bahwa ancaman terhadap keamanan sistem informasi terus berkembang seiring dengan kemajuan teknologi. Oleh karena itu, pendekatan yang diterapkan harus dapat menanggapi dinamika ini dan secara proaktif melibatkan strategi keamanan yang mampu mengidentifikasi, mencegah, dan merespons berbagai jenis ancaman yang mungkin muncul. Hanya melalui pendekatan yang holistik dan proaktif ini, organisasi dapat memastikan keamanan yang efektif dan melindungi keberlanjutan operasional serta reputasi mereka[2].

Pentingnya pengujian keamanan sistem aplikasi berbasis web menjadi semakin mencolok dalam era perkembangan pesat aplikasi berbasis web. Dalam konteks pertumbuhan yang cepat ini, serangan keamanan terus meningkat melalui berbagai teknik ancaman yang semakin canggih. Meskipun demikian, seringkali isu keamanan ditempatkan pada prioritas yang lebih rendah, mungkin terpinggirkan dan berada di peringkat kedua atau bahkan terakhir dalam daftar prioritas suatu organisasi. Oleh karena itu, menjadi suatu keharusan bagi organisasi untuk secara aktif melakukan penilaian terhadap keamanan aplikasi berbasis web mereka guna mendeteksi potensi kerentanan dan memahami risiko yang mungkin timbul[3]. Salah satu metode yang sangat efektif dalam menilai tingkat risiko kerentanan keamanan pada aplikasi berbasis web adalah menggunakan *Tenable Nessus Professional*, sebuah alat yang terpercaya untuk mengidentifikasi dan mengatasi kerentanan keamanan. Implementasi metode ini dapat membantu organisasi meningkatkan tingkat keamanan aplikasi berbasis web mereka dan mengurangi potensi risiko terkait serangan keamanan.

Banyak situs web telah diresmikan sebagai platform akun resmi di berbagai instansi pemerintahan, termasuk situs-situs pemerintahan yang berada di wilayah Jogjakarta. Pemanfaatan website sebagai sarana komunikasi, pengaduan, dan layanan telah menjadi praktik umum di banyak instansi pemerintahan di Yogyakarta. Pengoperasian situs web ini di instansi pemerintahan di Yogyakarta dimulai pada tahun 2008, dan pertama kali diterapkan di Layanan Lembaga Pemerintahan Jogjakarta. Pada awal tahun 2008, sistem ini secara bertahap disosialisasikan ke seluruh instansi sesuai dengan jadwal yang telah ditetapkan. Setelah penyelesaian seluruh kegiatan sosialisasi, website tersebut dapat diakses oleh seluruh pegawai yang terlibat dalam program pelayanan, serta masyarakat yang telah mendaftar dalam program tersebut. Ini mencerminkan evolusi penerapan teknologi dalam upaya pemerintah di Jogjakarta untuk meningkatkan aksesibilitas, efisiensi, dan transparansi dalam penyediaan layanan kepada masyarakat.

Manajemen keamanan informasi mencakup peraturan, prosedur, pedoman prinsip, bersama dengan aset dan langkah-langkah yang dijalankan oleh organisasi untuk melindungi informasinya. Sistem ini merupakan metodologi yang terorganisir dengan baik untuk konstruksi, penerapan, operasionalisasi, pemeriksaan, evaluasi, pemeliharaan, dan peningkatan keamanan informasi organisasi, dengan tujuan mencapai sasaran yang telah ditetapkan[4]. Uji penetrasi adalah simulasi serangan siber resmi pada sistem komputer untuk mengevaluasi keamanannya. *Penetration Testing Execution Standard (PTES)* memiliki 5 bagian utama yang mencakup seluruh aspek pengujian penetrasi, dimulai dari Interaksi dan Pengumpulan Intelijen, Pemodelan Ancaman, Analisis Kerentanan, Eksploitasi, hingga Pelaporan[5].

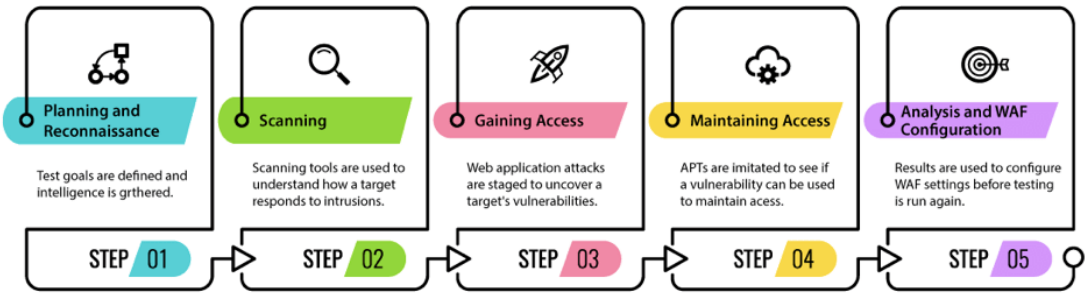
Dari kerentanan yang ditemukan, dapat menjadi sangat serius jika dimanfaatkan oleh pihak yang berkepentingan untuk merusak sistem, mengakibatkan kerugian pada instansi atau perusahaan terkait. Selanjutnya, individu ini dapat membuat ancaman terhadap sistem yang mengharuskan instansi atau perusahaan membayar sejumlah uang agar dapat mengakses kembali data penting mereka[6]. Vulnerability assessment secara rutin dilakukan untuk menjaga keamanan website. Untuk meningkatkan dan memelihara keamanan, perlu dilakukan evaluasi kerentanan, baik melalui metode manual maupun otomatis. Hasil dari evaluasi kerentanan dapat memberikan informasi yang berharga

kepada suatu organisasi, termasuk kondisi keamanan infrastruktur dan identifikasi potensi ancaman keamanan, seperti serangan terhadap aset perusahaan yang mungkin dimanfaatkan oleh pihak lain[6].

Langkah signifikan dalam mengevaluasi tingkat risiko adalah menentukan dampak negatif yang muncul dari analisis kerentanan. Hasil analisis kerentanan dapat membantu manajer dan pengembang sistem untuk mencegah serta mengatasi dampak risiko yang teridentifikasi pada sistem. Saat ini, belum dilakukan penilaian keamanan pada sistem informasi. Proses pembangunan sistem tersebut saat ini bergantung pada penggunaan *library* untuk meningkatkan keamanan. Meskipun penerapan library bertujuan untuk meningkatkan keamanan sistem, namun belum ada pengujian langsung dari internal perusahaan, sehingga masih kurang pemahaman terhadap celah keamanan yang mungkin ada pada sistem yang telah dibangun. Oleh karena itu, diperlukan Penilaian Keamanan (*Security Assessment*) pada sistem tersebut[7].

2. METODE PENELITIAN

Penetration *Testing Execution Standard (PTES)* bukan sekadar penyedia layanan keamanan, tetapi lebih merupakan sebuah standar yang mengadopsi bahasa umum dan mencakup area yang luas dalam pengujian penetrasi. Gambar 1 memvisualisasikan 5 langkah kunci yang ditempuh dalam melaksanakan pengujian penetrasi menurut *PTES*.



Gambar 1. Tahapan *Penetration Testing*

a. **Planning and Reconnaissance** salah satu tahapan dalam pengujian penetrasi (penetration testing) yang merupakan langkah awal dalam menjalankan penetration testing adalah fase perencanaan. Pada tahap ini, para profesional keamanan akan menetapkan tujuan pen testing, mencakup ruang lingkup sistem atau jaringan yang akan diuji, dan menentukan metode *pentesting* yang akan digunakan. Selain itu, para ahli keamanan juga akan melakukan identifikasi terhadap risiko dan potensi ancaman yang mungkin timbul selama proses *pentesting*. Setelah itu pemahaman mendalam terhadap infrastruktur, sistem, dan lingkungan teknis adalah tujuan dari kegiatan pemetaan sebelum melakukan serangan simulasi. Pemetaan yang dilakukan secara hati-hati dan mendalam memungkinkan tim penetration testing untuk memiliki pemahaman yang menyeluruh terhadap target sebelum melaksanakan serangan simulasi. Proses ini dapat meningkatkan efektivitas penetrasi dan membantu dalam mengidentifikasi kelemahan serta potensi risiko yang mungkin dihadapi oleh target yang sedang diuji. Lebih lanjut, pemetaan yang baik juga berperan dalam mencegah dampak negatif yang tidak diinginkan pada infrastruktur dan sistem yang sedang diuji, kegiatan sistematis untuk mengevaluasi keamanan suatu sistem atau aplikasi.
b. **Scanning** yaitu pada fase uji penetrasi, *scanning* menjadi kegiatan utama yang mencakup identifikasi dan pemindaian terhadap sistem atau jaringan untuk mengungkap potensi kelemahan atau celah keamanan. Proses ini melibatkan pemanfaatan berbagai alat dan teknik, seperti port scanning untuk mengidentifikasi port yang terbuka, *vulnerability scanning* untuk menemukan kelemahan potensial, dan *network scanning* untuk mengeksplorasi struktur jaringan. Tujuan utama dari kegiatan scanning ini adalah memberikan pemahaman mendalam kepada tim uji penetrasi mengenai target yang sedang diuji. Hasil dari pemindaian berperan penting dalam mengevaluasi tingkat kerentanan dan risiko yang mungkin dihadapi oleh target, serta menyediakan dasar untuk langkah-langkah berikutnya dalam uji penetrasi. Penting untuk ditekankan bahwa setiap kegiatan scanning harus dilaksanakan dengan izin dan dalam konteks yang sah untuk mencegah potensi dampak negatif pada sistem atau jaringan yang sedang diuji. Pemindaian ini menjadi bagian dari serangkaian tindakan yang dijalankan guna menilai tingkat keamanan suatu sistem atau lingkungan teknologi informasi.

c. Gaining Access langkah berikutnya dalam menjalankan penetration testing adalah memperoleh akses. Akses yang dimaksud dalam tahap ini merujuk pada kemampuan untuk masuk ke dalam sistem atau jaringan yang sedang diuji. Dalam tahap ini, akses tersebut diperoleh melalui kelemahan atau kerentanan yang teridentifikasi pada tahap sebelumnya. Tujuan utama dari tahap ini adalah untuk menilai tingkat kerentanan sistem atau jaringan terhadap potensi serangan yang dapat dilakukan oleh penyerang atau *hacker*. Proses ini melibatkan identifikasi kerentanan dalam sistem dan aplikasi, kemudian mencoba untuk memvalidasinya dengan memengaruhi aspek-aspek keamanan informasi seperti Kerahasiaan, Integritas, dan Ketersediaan. Setelah kerentanan potensial ditemukan, eksploitasi dapat dilakukan melalui berbagai metode, mulai dari memberikan input yang tidak terduga, *pentester* ataupun hacker akan melakukan eksploitasi untuk mengakses dan mengambil data yang dapat diambil. Contohnya termasuk perolehan akses ke akun administrator, data-data pribadi perusahaan, dan hal-hal sejenisnya. Dalam konteks pengujian penetrasi, fase "*gaining access*" merujuk pada proses di mana peneliti penetrasi berhasil mendapatkan akses tanpa izin ke dalam suatu sistem, jaringan, atau aplikasi. Pada tahap ini, peneliti melakukan eksplorasi dan memanfaatkan kerentanan atau celah keamanan yang telah teridentifikasi selama tahap pemindaian dan analisis. Selama fase ini, peneliti berusaha untuk melakukan penetrasi ke dalam sistem menggunakan metode-metode yang mungkin juga digunakan oleh penyerang yang tidak memiliki izin.

d. **Maintaining Access** dalam fase uji penetrasi mengacu pada kemampuan mempertahankan akses ke dalam sistem atau jaringan yang telah berhasil diakses oleh pentester. Setelah sukses mengeksploitasi kerentanan dan memperoleh akses, langkah berikutnya adalah mempertahankan kemampuan untuk tetap masuk ke dalam sistem tersebut tanpa terdeteksi. Pada tahap ini, pentester akan berupaya memanfaatkan berbagai teknik dan alat guna menjaga aksesnya untuk periode yang lebih lama. Tujuan utamanya adalah mensimulasikan situasi di mana seorang penyerang atau peretas berhasil meretas sistem dan mampu mempertahankan akses tanpa segera terdeteksi oleh sistem keamanan. Perlu ditekankan bahwa maintaining access dilaksanakan dalam konteks uji penetrasi yang sah dan dengan izin dari pemilik sistem atau jaringan yang diuji. Tindakan ini membantu organisasi untuk mengevaluasi sejauh mana sistem mereka rentan terhadap upaya mempertahankan akses yang tidak sah, sehingga dapat diambil tindakan perbaikan yang diperlukan untuk meningkatkan keamanan sistem. Dan di mana peneliti penetrasi berhasil mempertahankan akses yang telah berhasil diperoleh ke dalam suatu sistem, jaringan, atau aplikasi setelah berhasil mengeksploitasi kerentanan atau celah keamanan. Setelah berhasil mendapatkan akses awal, tujuan peneliti adalah memastikan bahwa mereka mampu menjaga akses tersebut dalam jangka waktu yang lebih panjang, serupa dengan tindakan yang dapat dilakukan oleh penyerang sebenarnya.

e. **Analysis and WAF Configuration** Tahap ini dimulai setelah laporan hasil penetralan disusun dan diserahkan kepada pemilik atau pengelola sistem. Fokus utamanya adalah memastikan bahwa implementasi hasil uji keamanan dilakukan secara efektif, dan langkah-langkah perbaikan telah diambil untuk menangani kelemahan yang terdeteksi. Selama tahap ini, pemilik sistem akan melakukan analisis mendalam terhadap laporan penetralan yang diterima. Dalam evaluasi ini, pemilik sistem dapat berkomunikasi dengan tim *penetration testing* untuk memperoleh penjelasan lebih lanjut mengenai temuan dan rekomendasi yang terdapat dalam laporan. Setelah evaluasi selesai, pemilik atau pengelola sistem diharapkan mengimplementasikan tindakan perbaikan untuk mengatasi kelemahan dan kerentanan yang telah diidentifikasi oleh tim penetration testing. Perbaikan ini melibatkan langkah-langkah teknis, seperti pembaruan perangkat lunak, rekonfigurasi sistem, atau peningkatan konfigurasi jaringan. Evaluasi dan implementasi perbaikan menjadi tahap yang sangat kritis dalam siklus penetration testing karena memastikan bahwa hasil uji keamanan tidak hanya berhenti pada tingkat laporan, tetapi benar-benar dijalankan untuk meningkatkan keamanan dan melindungi sistem dari potensi serangan siber di masa mendatang.

Penelitian ini menggunakan pendekatan deskriptif dengan metode kuantitatif untuk menganalisis keamanan website Pemerintahan di Yogyakarta. Fokus penelitian terpusat pada satu Website Pemerintahan, dan lokasi penelitian dilakukan secara spesifik di Yogyakarta. Variabel yang akan menjadi fokus analisis, sebagaimana tergambarkan pada Gambar 1, adalah *Penetration Testing* yang melibatkan serangkaian langkah-langkah. Tahap pertama mencakup *Planning and Reconnaissance* dengan sub-langkah Identifikasi, Konfirmasi, dan Pengumpulan Data. Selanjutnya, *Intelligence Gathering* akan dilakukan menggunakan alat seperti *whatweb*. Pada tahap ketiga, *Vulnerability Analysis* akan dilakukan melalui pemindaian menggunakan *Nessus Professional*. *Exploitation*, tahap keempat,

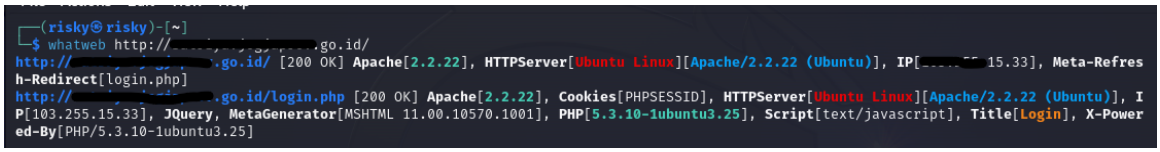
akan melibatkan penggunaan *Web Directories* dan *ClickJacking*. Terakhir, tahap kelima adalah Pelaporan, di mana hasil-hasil dari seluruh proses akan disampaikan secara rinci. Dengan pendekatan yang terstruktur ini, penelitian ini bertujuan untuk memberikan wawasan mendalam terhadap kerentanan keamanan website Pemerintahan di Yogyakarta.

3. HASIL DAN PEMBAHASAN

Dalam tahapan ini, pengujian dan analisis dilakukan untuk mengidentifikasi potensi kerentanan atau kelemahan dalam sistem melalui beberapa langkah berikut ini :

a. **Planning and Reconnaissance**

Tahap ini ditujukan untuk merinci dan menjelaskan rencana informasi yang mencakup sejumlah elemen kunci, seperti sasaran target, alamat IP, server, sistem operasi, dan layanan yang digunakan oleh situs web. Untuk mencapai tujuan ini, digunakan perintah *whatweb* pada URL situs web yang tengah diuji. Selama tahap ini, teknik-teknik yang akan diterapkan selama uji penetrasi akan dijelaskan secara rinci kepada pihak yang terlibat dalam proses ini. Dengan menjaga kerahasiaan sebagai prioritas utama, uji penetrasi ini dijalankan tanpa pemberitahuan sebelumnya, dan semua temuan yang diidentifikasi dan dieksekusi harus dijaga kerahasiaannya. Izin untuk melaksanakan uji penetrasi menjadi aspek krusial yang harus diakui dan dimiliki. Dokumen izin untuk penelitian ini telah diperoleh melalui Dinas Komunikasi dan Informatika Yogyakarta serta telah disahkan oleh mitra kerjasama yang relevan. Izin ini mencerminkan komitmen untuk melibatkan pihak berwenang dan memastikan kegiatan ini dilaksanakan dengan pertanggungjawaban yang tinggi. Sebagai langkah selanjutnya, hasil dari tahap penguji akan dijelaskan dan dipresentasikan, memberikan pemahaman yang mendalam terkait temuan yang muncul selama tahap ini. Hal ini bertujuan untuk memberikan gambaran yang komprehensif kepada pihak terkait dan menjadi dasar untuk langkah-langkah lanjutan dalam pengembangan keamanan sistem dan layanan.



Gambar 2. Informasi Website

b. **Scanning**

Proses pemindaian dalam uji penetrasi tidak hanya sekadar langkah rutin, melainkan menjadi serangkaian tindakan kritis yang sangat penting dalam rangka mengenali informasi dan kerentanan yang mungkin terdapat dalam suatu sistem, jaringan, atau aplikasi. Sebagai tahap awal yang terintegrasi dalam keseluruhan proses uji penetrasi, pemindaian ini memiliki fokus khusus pada pengumpulan informasi esensial, seperti identifikasi dan validasi data. Tujuannya adalah untuk memahami secara menyeluruh lanskap keamanan yang melibatkan identifikasi potensi titik lemah yang mungkin dapat dieksploitasi oleh pihak yang tidak sah. Hasil dari tahap pemindaian ini tidak hanya memberikan gambaran awal terkait potensi kerentanan, melainkan juga secara rinci didokumentasikan, seringkali dalam bentuk Tabel 1. Informasi yang terperinci ini menciptakan landasan yang kokoh untuk tahap uji penetrasi berikutnya. Pemahaman awal yang diperoleh dari pemindaian ini menjadi kunci dalam menangani risiko keamanan yang mungkin timbul. Selain itu, hasil pemindaian menjadi dasar penting untuk langkah-langkah evaluasi lebih lanjut dan perbaikan sistem, membantu mengidentifikasi dan mengatasi potensi ancaman yang mungkin terjadi di masa mendatang. Dengan demikian, tahap pemindaian bukan hanya merupakan langkah permulaan, tetapi juga langkah yang krusial dalam memastikan keamanan dan ketangguhan suatu sistem terhadap potensi serangan.

Tabel 1. Daftar Kerentanan dari Website

No.	Kerentanan	Tingkat
1.	*Browsable Web Directories*	Sedang
2.	*Web Application Potentially Vulnerable to Click Jacking*	Sedang
3.	*Web Server (Multiple Issues)*	Gabungan

c. **Gaining Access**

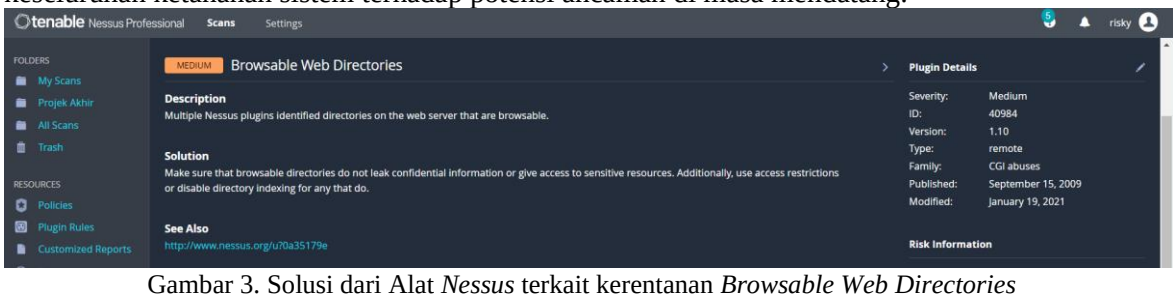
Tahap ini merupakan fase di mana peneliti penetrasi berusaha mendapatkan akses yang tidak sah

ke dalam sistem, jaringan, atau aplikasi yang telah dipindai. Upaya dilakukan untuk mencapai hak akses atau akses ilegal berdasarkan hasil penelitian. Tujuan utama tahap ini adalah mengevaluasi sejauh mana sistem keamanan dapat ditembus dan menunjukkan potensi risiko keamanan jika penyerang tidak sah berhasil memperoleh akses ke server tersebut. Kegiatan ini melibatkan penerapan teknik eksploitasi atau hacking untuk memanfaatkan kerentanan atau celah keamanan yang terdeteksi pada tahap pemindaian atau analisis sebelumnya. Hasil eksploitasi dari website ini tercatat dalam laporan penelitian berikut.

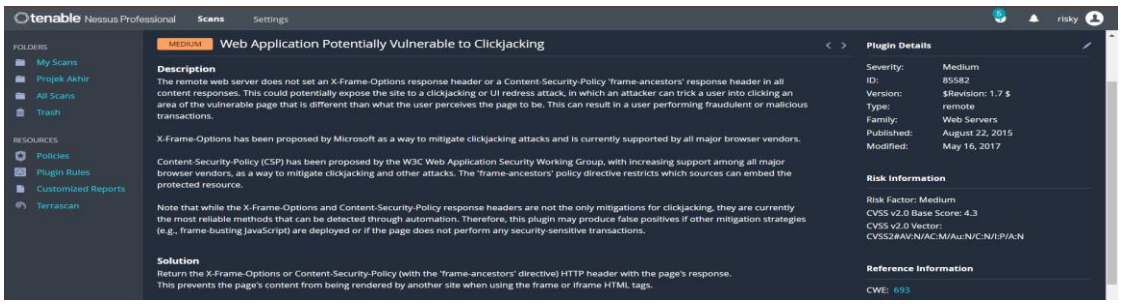
Yang dimana pada temuan pertama yakni kerentanan *Browsable Web Directories* atau juga disebut Akses Direktori Web yang dapat dijelajahi memungkinkan pengguna melihat daftar file dan folder yang ada di server web. Isi dari file dan folder tersebut dapat mencakup berbagai konten situs web, file media, dokumen, atau data lainnya. Pengguna memiliki kemampuan untuk menemukan dan mengakses direktori ini melalui peramban web, serta dapat mengunduh atau melihat file sesuai kebutuhan mereka. Untuk temuan kerentanan kedua yakni *Web Application Potentially Vulnerable to ClickJacking* dapat diartikan sebagai Clickjacking atau yang juga dikenal sebagai user interface (UI) *redirect* dalam istilah formal industri, adalah istilah yang laman cenderung tidak resmi. Bagi para profesional di dalam industri ini, istilah *UI redirect* sebenarnya lebih deskriptif karena teknik *clickjacking* saat ini tidak benar-benar "mengambil alih" kursor atau elemen halaman web pengguna dengan cara apapun. Sebaliknya, *clickjacking* hanya menempatkan sesuatu yang tidak terlihat di atas area layar yang kemungkinan besar akan di-klik oleh pengguna, dengan sesuatu yang tidak terlihat dan seharusnya tidak di-klik. Temuan kerentanan terakhir yaitu *Web Server* (*Multiple Issues)* yaitu pada temuan ini tidak bisa dipungkiri bahwasannya pada pemeliharaan terkait pada server yang dimana pada masalah ini diwajibkan untuk mengupgrade versi dari *Apache Web Server*.

d. **Maintaining Access**

Tahap yang dikenal sebagai "*Maintaining Access*" adalah fase krusial dalam uji penetrasi, di mana peneliti penetrasi atau penguji berkomitmen untuk mempertahankan dan memberikan solusi terhadap akses yang berhasil diperoleh ke dalam sistem, jaringan, atau aplikasi setelah berhasil mengeksploitasi kerentanan atau celah keamanan. Fokus utama tahap ini adalah mengevaluasi sejauh mana tingkat kerentanan sistem terhadap serangan berkelanjutan dan seberapa sulit bagi penyerang untuk mempertahankan akses yang tidak sah. Dalam konteks temuan kerentanan, seperti yang diidentifikasi pada "*Browsable Web Directories*" dan "*Web Application Potentially Vulnerable to Clickjacking*", penguji menarik kesimpulan bahwa melalui bantuan alat Nessus Professional, sistem memberikan peringatan dan solusi terperinci terhadap kerentanan tersebut. Alat ini tidak hanya mengidentifikasi kerentanan, tetapi juga menyajikan panduan yang komprehensif bagi Penetration Tester. Informasi yang terperinci ini membantu peneliti untuk memahami secara mendalam sifat dan tingkat keparahan kerentanan, memungkinkan mereka untuk mengambil langkah-langkah mitigasi yang tepat. Proses menjaga dan memberikan solusi terhadap akses yang berhasil diperoleh ini menciptakan peluang untuk menguji respons sistem terhadap upaya pemeliharaan akses yang dilakukan oleh peneliti. Selain itu, memberikan solusi terhadap kerentanan yang ditemukan juga berperan dalam meningkatkan pemahaman dan tindakan preventif terhadap risiko keamanan yang ada, membantu mengasah kebijakan keamanan, dan meningkatkan keseluruhan ketahanan sistem terhadap potensi ancaman di masa mendatang.



Gambar 3. Solusi dari Alat *Nessus* terkait kerentanan *Browsable Web Directories*



Gambar 4. Solusi dari Alat *Nessus* terkait kerentanan *Clickjacking*

e. **Analysis and WAF Configuration**

Fase uji penetrasi, yang terwujud dalam tahap intensif ini, mencirikan periode di mana peneliti penetrasi menunjukkan dedikasi tinggi untuk mendapatkan akses yang tidak sah ke dalam suatu sistem, jaringan, atau aplikasi yang telah melalui tahap pemindaian sebelumnya. Fokus utama tahap ini adalah mencapai hak akses atau akses ilegal berdasarkan temuan hasil penelitian sebelumnya. Misi utama yang diemban adalah mengidentifikasi dan mengevaluasi sejauh mana sistem keamanan dapat ditembus, sambil secara khusus menyoroti potensi risiko keamanan yang dapat muncul jika seorang penyerang berhasil memperoleh akses yang tidak sah ke server. Kegiatan yang terlibat dalam tahapan ini mencakup penerapan teknik eksploitasi atau peretasan yang bertujuan memanfaatkan kerentanan atau celah keamanan yang telah terdeteksi pada tahap pemindaian atau analisis sebelumnya. Hasil dari eksploitasi ini memberikan wawasan lebih mendalam tentang ketidakamanan sistem, menyoroti titik lemah yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Seluruh proses ini menjadi bagian integral dari penelitian keamanan yang bertujuan meningkatkan ketahanan sistem melalui identifikasi dan penanganan potensi ancaman. Selanjutnya, hasil eksploitasi dari situs web tersebut akan menjadi fokus penelitian, di mana mereka akan dicermati dan dianalisis secara rinci. Tujuan utamanya adalah menyajikan pemahaman yang lebih komprehensif tentang tingkat keamanan sistem yang telah diuji. Dengan melakukan analisis ini, penelitian keamanan dapat memberikan pandangan yang lebih mendalam tentang kelemahan dan area potensial yang memerlukan perbaikan, serta memberikan dasar untuk rekomendasi keamanan yang lebih efektif.

4. KESIMPULAN

Tahapan uji penetrasi merupakan proses yang terintegrasi dan kritis dalam penelitian keamanan sistem, di mana peneliti penetrasi secara tekun melakukan serangkaian langkah untuk mengidentifikasi informasi, mengenali kerentanan, dan mengevaluasi tingkat keamanan suatu sistem, jaringan, atau aplikasi. Fase pemindaian menjadi langkah awal, fokus pada pengumpulan informasi esensial dan pemahaman mendalam terkait lanskap keamanan. Proses ini menciptakan dasar yang kokoh untuk tahap berikutnya, yaitu fase uji penetrasi yang intensif, di mana peneliti berusaha memperoleh akses tidak sah dan mengeksploitasi kerentanan yang telah terdeteksi sebelumnya. Selama tahap uji penetrasi, penerapan teknik eksploitasi atau hacking dilakukan untuk menguji sejauh mana sistem dapat ditembus, dengan tujuan utama mencapai hak akses ilegal. Aktivitas ini berjalan bersamaan dengan penyorotan potensi risiko keamanan yang mungkin muncul jika suatu server berhasil diakses secara tidak sah. Keseluruhan proses ini memiliki peran krusial dalam penelitian keamanan, yang bertujuan meningkatkan ketahanan sistem melalui identifikasi dan penanganan potensi ancaman. Hasil eksploitasi dari tahap uji penetrasi selanjutnya dianalisis secara mendalam untuk menyajikan gambaran komprehensif tentang keamanan sistem yang diuji. Kesimpulan yang diambil dari penelitian ini memberikan landasan bagi rekomendasi keamanan yang lebih efektif dan membantu organisasi meningkatkan tingkat ketahanan mereka terhadap potensi serangan di masa mendatang. Dengan demikian, tahapan uji penetrasi bukan hanya merupakan langkah dalam proses, melainkan fondasi yang sangat penting dalam memastikan keamanan yang optimal bagi sistem informasi dan jaringan.

Hasil audit pengujian dengan mengikuti tahapan *Penetration Testing Execution Standard* pada website Dinas Pemerintahan Yogyakarta, menggunakan alat *Tenable Nessus Professional*, mengungkap bahwa tingkat kerentanan keamanan situs tersebut berada pada Level 2, yang dikategorikan sebagai tingkat Medium. Meskipun demikian, peringatan lain diidentifikasi sebagai kurang rentan terhadap akses ilegal, sebab hasil pengujian yang menunjukkan kerentanannya mungkin dapat diakses secara tidak sah oleh pihak yang tidak berwenang. Oleh karena itu, potensi dampak serangan terhadap situs tersebut dinilai tidak terlalu signifikan. Penting untuk dicatat bahwa upaya eksploitasi melalui *SQL*

Injection tidak berhasil, dikarenakan tingkat keamanan website yang telah ditingkatkan dengan implementasi *SSL (Secure Socket Layer).* Selain itu, kemungkinan besar protokol yang digunakan masih berupa http. Dengan temuan-temuan ini, diperoleh pemahaman yang lebih mendalam mengenai tingkat keamanan dan potensi risiko yang mungkin dihadapi oleh website Dinas Pemerintahan Yogyakarta.

DAFTAR PUSTAKA

[1] Andhika, D. A., Slamet, & Ningsih, N. (2022). Pengujian Penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES). *Journal of Technology and Informatics (JoTI)*, *3*(2), 55–61. https://doi.org/10.37802/joti.v3i2.222

[2] Aryanti, D., Nurholis, & Utamajaya, J. N. (2021). *ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA* (Vol. 1, Issue 3).

[3] Fauzan, F. Y., & Syukhri. (2021). Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang. *Jurnal Vocational Teknik Elektronika Dan Informatika*, *9*(2), 105–111. http://ejournal.unp.ac.id/index.php/voteknika/

[4] Fronita, M. (2023). Analisis Celah Keamanan Website Sitasi Menggunakan Vulnerability Assessment. *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi*, *9*(1), 1–7. https://doi.org/10.24014/rmsi.v9i1.21823

[5] Syarifuddin Syahab, A. (2023). Analisis Audit Keamanan Informasi Website Dari Drown Attack Menggunakan Network Mapper Dan Qualys Ssl. *Jurnal Manajemen Informatika & Sistem Informasi (MISI)*, *6*(1), 39–47.