

DIAGNOSIS KEAMANAN WEB MENGGUNAKAN METODE UJI PENETRASI WEBSITE SEKOLAH

Web Security Diagnosis Using School Website Penetration Test Method

Mhd. Rozali^{a,1}, Mikha Dayan Sinaga^{b,2}

^{a,b}Universitas Potensi Utama, Jl. Kl. Yos Sudarso Km. 6,5 No. 3-A, Kota Medan, 20241, Indonesia
mohamedrozali19@gmail.com¹, mikhadayan88@gmail.com²

ABSTRAK

Di era Internet dan World Wide Web, keamanan sistem telah menjadi isu penting dalam sistem informasi berbasis web global. Hal ini dapat dilihat dari komitmen yang kuat dari para profesional keamanan sistem, komunitas riset, dan vendor perangkat lunak. Menurut laporan digital yang dibuat oleh We Are Social (Hootsuite), pengguna internet di Indonesia pada awal Januari 2020 sudah mencapai 174 juta pengguna. Indonesia mengalami pertumbuhan pengguna yang mengakses internet sebesar 17 persen atau bertambah sebanyak 25 juta pengguna dalam satu tahun terakhir. SMK Negeri 13 Medan telah memiliki suatu aplikasi website yang dapat memberikan informasi kepada masyarakat tentang sekolah tersebut. Keamanan dari website Sekolah SMK Negeri 13 Medan ini perlu diuji untuk mengetahui bagian-bagian mana saja yang memiliki kelemahan dan rentan akan serangan para hacker. Serangan para hacker ini dapat menyusahkan pihak sekolah karena serangan para hacker ini berpotensi untuk merubah isi dari konten website sekolah tersebut dan memberikan informasi yang salah kepada masyarakat. Permasalahan yang telah dijabarkan tersebut dapat diselesaikan dengan melakukan Penetration testing terhadap website sekolah SMK Negeri 13 Medan. Hasil dari penelitian ini ialah melakukan analisis terhadap keamanan web sekolah SMK Negeri 13 Medan dan memberikan rekomendasi terhadap keamanan web tersebut.

Kata Kunci : Keamanan Web, Penetration Testing, Hacker.

ABSTRACT

In the era of the Internet and the World Wide Web, system security has become an important issue in global web-based information systems. This can be seen from the strong commitment of system security professionals, the research community, and software vendors. According to a digital report made by We Are Social (Hootsuite), internet users in Indonesia at the beginning of January 2020 had reached 174 million users. Indonesia experienced a growth in users accessing the internet by 17 percent or an increase of 25 million users in the past year. SMK Negeri 13 Medan already has a website application that can provide information to the public about the school. The security of the SMK Negeri 13 Medan School website needs to be tested to find out which parts have weaknesses and are vulnerable to attacks by hackers. These hacker attacks can be troublesome for the school because these hacker attacks have the potential to change the contents of the school's website content and provide wrong information to the public. The problems that have been described can be solved by conducting Penetration testing on the SMK Negeri 13 Medan school website. The results of this study are to analyze the security of the school's web at SMK Negeri 13 Medan and provide recommendations for the security of the website.

Keywords : Web Security, Penetration Testing, Hackers.

Disubmit: 10 Oktober 2023

Info Artikel :
Direview: 15 November 2023

Diterima : 12 Desember 2023

Copyright © 2024 - Journal UPU. All rights reserved.

1. PENDAHULUAN

Di era Internet dan *World Wide Web*, keamanan sistem telah menjadi isu penting dalam sistem informasi berbasis *web* global. Hal ini dapat dilihat dari komitmen yang kuat dari para profesional keamanan sistem, komunitas riset, dan vendor perangkat lunak [1]. Menurut laporan digital yang dibuat oleh *We Are Social (Hootsuite)*, pengguna internet di Indonesia pada awal Januari 2020 sudah mencapai 174 juta pengguna. Indonesia mengalami pertumbuhan pengguna yang mengakses internet sebesar 17 persen atau bertambah sebanyak 25 juta pengguna dalam satu tahun terakhir [2].

Website merupakan layanan informasi yang banyak diakses oleh pengguna yang terhubung dalam suatu jaringan internet. Suatu *website* dituntut untuk mampu menangani permintaan pengguna dengan baik, sehingga dalam pembangunannya tidak jarang terdapat celah keamanan yang dapat dimanfaatkan *hacker* untuk merusak sistem didalamnya [3]. Para *hacker* dapat melakukan perusakan atau hanya sekedar untuk mengetes keamanan pada *website* tersebut.

SMK Negeri 13 Medan telah memiliki suatu aplikasi *website* yang dapat memberikan informasi kepada masyarakat tentang sekolah tersebut. Aplikasi *website* ini biasanya memuat informasi-informasi terkait sekolah dan kegiatan-kegiatan yang dilakukan oleh siswa-siswi sekolah tersebut. Keamanan dari *website* sekolah SMK Negeri 13 Medan ini perlu diuji untuk mengetahui bagian-bagian mana saja yang memiliki kelemahan dan rentan akan serangan para *hacker*. Serangan para *hacker* ini dapat menyusahkan pihak sekolah karena serangan para *hacker* ini berpotensi untuk merubah isi dari konten *website* sekolah tersebut dan memberikan informasi yang salah kepada masyarakat.

Permasalahan yang telah dijabarkan tersebut dapat diselesaikan dengan melakukan *penetration testing* terhadap *website* sekolah SMK Negeri 13 Medan. *Penetration testing* atau pentesting merupakan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan. penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, untuk menilai apa yang mungkin didapat oleh penyerang setelah eksploitasi sukses [4].

Tujuan dari penelitian ini ialah untuk membantu meningkatkan keamanan dan keandalan situs *web* sekolah SMK Negeri 13 Medan.

2. METODE

A. Penelitian Terdahulu

Berikut adalah beberapa jurnal penelitian terdahulu terkait judul penelitian yang sedang dilakukan:

1. Dalam penelitian pertama ini dengan judul “Metode Penetration testing pada Keamanan Jaringan *Wireless Wardriving* PT. Puma Makmur Aneka Engineering Bekasi” menghasilkan kesimpulan bahwa pengujian keamanan jaringan internal dan publik telah dilakukan dengan menggunakan metode *penetration testing* dan mendapatkan kerentanan seperti *WPA2 Cracking*, *Dos*, *Password Router Wireless Cracking*, dan *AP Isolation Testing* sehingga diketahui kerentanan pada jaringan internal dan publik [5].
2. Dalam penelitian kedua ini dengan judul “Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik *Penetration Testing* dan *Dast (Dynamic Application Security Testing)*” menghasilkan kesimpulan bahwa *penetration testing* pada celah keamanan *Broken Access Control* didapatkan bahwa penyerang dengan mudah dapat menebak id user lain dikarenakan menggunakan angka. Evaluasi yang dilakukan adalah merubah id angka menjadi id yang berisikan karakter acak [6].
3. Dalam penelitian ketiga ini dengan judul “Analisis Keamanan Untuk Mengetahui *Vulnerability* Pada DVWA Lab esting menggunakan *penetration testing Standart OWASP*” menyimpulkan bahwa metode Standart OWASP dapat diterapkan dalam hal *Penetration testing* pemecahan masalah uji keamanan suatu *website* dan mengikuti standarisasi OWASP dalam hal uji keamanan. Pada hasil pengujian, terdapat function dan query MySQL yang tidak di filter maka dalam hal ini

- tidak layak pakai dalam hal website karna penyerang dapat mengambil alih server dan *database* [7].
4. Dalam penelitian keempat ini dengan judul “Evaluasi Keamanan Website Lembaga X Melalui Penetration testing Menggunakan Framework ISSAF” menyimpulkan bahwa Metode penetration testing merupakan pengujian keamanan sistem yang komprehensif untuk menguji basis komputasi yang lengkap. Framework ISSAF merupakan metodologi penetration testing yang dirancang untuk mengevaluasi jaringan, sistem dan kontrol aplikasi. Penetration testing pada website Lembaga X menggunakan Framework ISSAF dilakukan melalui sembilan tahap yang meliputi information gathering, network mapping, vulnerability identification, penetration, gaining access and privilege escalation, enumeration further, compromise remote user/sites, maintaining access, dan covering tracks. Berdasarkan Sembilan tahapan tersebut diperoleh hasil bahwa terdapat celah keamanan yang berbahaya seperti SQL Injection dan XSS pada website Lembaga X [3].
 5. Dalam penelitian kelima ini dengan judul “Penetration testing Untuk Deteksi Vulnerability Sistem Informasi Kampus” menyimpulkan bahwa hasil pengujian dengan melakukan penetration testing terhadap 3 domain yang berbeda, terdapat dua domain yang threat levelnya Medium dan satu domain yang threat levelnya adalah high. Pada pengujian ini juga telah di temukan beberapa celah kelemahan atau kerentanan pada sistem informasi kampus yang bisa saja nantinya digunakan untuk memanipulasi file lokal, mengganggu kinerja dari server itu sendiri dengan teknik DoS, melakukan clickjacking serta melakukan CSRF/Cross-site request forgery. Hasil temuan ini akan peneliti jadikan sebagai bahan masukan kepada pihak pengelola sistem informasi kampus untuk segera melakukan perbaikan terhadap kelemahan (Vulnerability) tersebut [8].

B. Landasan Teori

Landasan teori berisi teori-teori yang dapat mendukung penelitian yang sedang dilakukan. Adapun landasan teori dalam penelitian ini adalah sebagai berikut:

1. Keamanan Informasi

Informasi merupakan salah satu aset penting pada sistem informasi sebuah organisasi. Ini dikarenakan informasi merupakan sumber daya strategis dalam meningkatkan nilai usaha. Penting untuk melindungi informasi, sehingga terbebas dari ancaman dan bahaya dari pihak luar. Keamanan pada sistem informasi perlu untuk diperhatikan, hal ini bertujuan untuk mencegah ancaman terhadap sistem dan mendeteksi segala kerusakan sistem. Keamanan informasi memiliki beberapa aspek yang harus dipahami dan dilindungi. Aspek keamanan sistem informasi antara lain confidentiality (kerahasiaan) yaitu informasi haruslah dapat diakses hanya oleh mereka yang memiliki wewenang untuk memperolehnya serta menjamin kerahasiaan data, integrity (integritas) yaitu keakurasian informasi yang dilindungi melalui beberapa metodologi pengolahan yang baik, dan availability (ketersediaan) yaitu memastikan bahwa informasi dapat diakses sesuai dengan kebutuhan [3].

Pada keamanan informasi, dikenal istilah CIA yakni *Confidentiality*, *Integrity*, dan *Availability* sebagai jantung dari keamanan informasi. Berdasarkan ISO27000, *Confidentiality* atau kerahasiaan dalam hal ini adalah informasi yang kita miliki pada sistem atau database kita yang sifatnya rahasia sehingga pengguna atau orang yang tidak berkepentingan tidak dapat melihat/mengaksesnya. *Integrity* adalah menjamin konsistensi data terhadap semua konstrain yang diberlakukan terhadap data tersebut, sehingga memberikan jaminan keabsahan data itu sendiri. Sedangkan *Availability* adalah memastikan sumber daya yang ada siap diakses kapanpun oleh user, application atau sistem yang membutuhkannya [4].

2. Penetration Testing

Penetration testing, atau pentesting merupakan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan [4]. Penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, untuk menilai apa yang mungkin didapat oleh penyerang setelah eksploitasi sukses [8].

Penetration testing adalah metode untuk mengevaluasi keamanan suatu sistem komputer atau jaringan dengan mensimulasikan peretasan [9]. Pengujian penetrasi merupakan langkah penting dalam pengembangan sistem pertahanan berbasis komputer server yang aman yang terhubung dalam suatu jaringan dalam hal apapun karena tidak hanya menekankan operasi, tetapi implementasi dan desain sistem. Ini adalah tindakan resmi dan dijadwalkan yang memisahkan tester penetrasi dari penyerang dan telah banyak diadopsi oleh organisasi dan Lembaga [10].

Pentesting dimulai dengan fase *Pre-engagement*, yang melibatkan klien tentang tujuan mereka untuk pentest, memetakan lingkup (tingkat dan parameter tes), dan seterusnya. Ketika pentester dan klien menyetujui ruang lingkup, format pelaporan, dan topik lainnya, pengujian yang sebenarnya dimulai.

Dalam fase *Gathering-Information*, pentester mencari informasi yang tersedia secara umum tentang klien dan mengidentifikasi cara-cara potensial untuk terhubung ke sistemnya. Dalam fase *Threat-Modeling*, pengujian menggunakan informasi ini untuk menentukan nilai setiap temuan dan dampaknya bagi klien jika temuan tersebut memungkinkan penyerang untuk membobol sistem. Evaluasi ini memungkinkan pentester untuk mengembangkan rencana aksi dan metode serangan [9].

Sebelum pentester dapat mulai menyerang sistem, dia melakukan *Vulnerability Analysis*. Pada fase ini, pentester berupaya menemukan kerentanan dalam sistem yang dapat dimanfaatkan dalam fase exploitation. Eksploitasi yang berhasil dapat menyebabkan fase *Post-Exploitation*, di mana hasil eksploitasi dimanfaatkan untuk menemukan informasi tambahan, data sensitif, akses ke sistem lain, dan sebagainya. Akhirnya, dalam fase *Reporting*, pentester merangkum temuan untuk para eksekutif dan praktisi teknis.

Penelitian Penelitian ini menggunakan metode penelitian deskriptif kualitatif. Pada umumnya metode ini dipergunakan untuk penyelidikan kebenaran yang bersifat relatif, teoretis dan menggunakan hermenetika sebagai langkah untuk mencari makna dan interpretasi. Pilihan pada pendekatan ini lebih banyak menggunakan analisis teoretik yang berwujud *state of arts* di dalam pembahasannya dan usaha penulis membangun konstruksi konseptual bagi topik penelitiannya. Titik akhir yang ingin dicapai adalah konstruk atau kesimpulan teoritis yang dibangun peneliti dari teori-teori yang terlibat di dalam pembahasan. Paparan dari metode kuantitatif ini dilakukan secara deskriptif. Penelitian eksploratori biasanya menjadi sub bagian dari metode kualitatif [11].

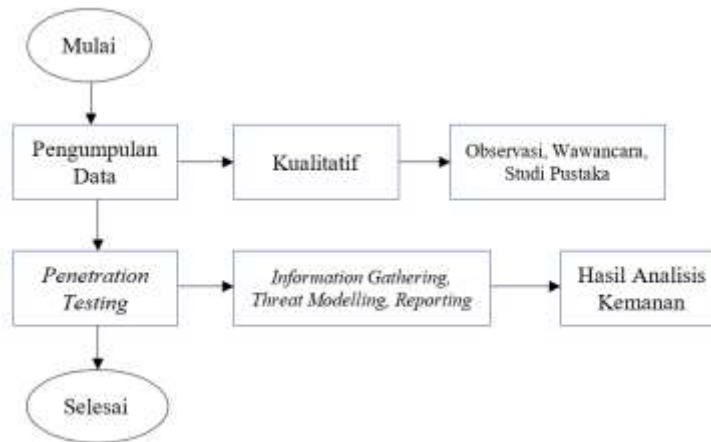
Metode analisis deskriptif kualitatif adalah metode yang berisi proses analisis, penggambaran serta ringkasan atas berbagai kondisi yang diambil dari kumpulan informasi yang berasal dari hasil wawancara ataupun pengamatan langsung di lapangan terhadap masalah yang sedang diteliti [12]. Metode deskriptif kualitatif, yaitu teknik yang menggambarkan, memaparkan dan menginterpretasikan objek yang diteliti dengan sistematis sehingga peneliti dapat mengetahui bagaimana aktivitas komunikasi pemasaran melalui observasi dan wawancara mendalam terhadap informan [13].

Penelitian deskriptif kualitatif ditujukan untuk mendeskripsikan dan menggambarkan fenomena-fenomena yang ada, baik bersifat alamiah maupun rekayasa manusia, yang lebih memperhatikan mengenai karakteristik, kualitas, keterkaitan antar kegiatan. Selain itu, Penelitian deskriptif tidak memberikan perlakuan, manipulasi atau perubahan pada variabel-variabel yang diteliti, melainkan menggambarkan suatu kondisi yang apa adanya. Satu-satunya perlakuan yang diberikan hanyalah penelitian itu sendiri, yang dilakukan melalui observasi, wawancara, dan dokumentasi. Berdasarkan keterangan dari beberapa ahli di atas, dapat ditarik kesimpulan bahwa penelitian deskriptif kualitatif yaitu rangkaian kegiatan untuk memperoleh data yang bersifat apa adanya tanpa ada dalam kondisi tertentu yang hasilnya lebih menekankan makna.

Disini, peneliti menggunakan metode penelitian deskriptif kualitatif karena penelitian ini mengeksplor tingkat keamanan dari web sekolah SMK Negeri 13 Medan. Penelitian ini akan bersifat memberikan rekomendasi kepada pihak sekolah terkait keamanan dari web sekolah. Dalam proses

A. Prosedur Penelitian

Prosedur penelitian merupakan langkah-langkah yang harus dilakukan dalam penelitian hingga mencapai suatu kesimpulan. Adapun alur penelitian yang penulis gunakan terlihat pada gambar berikut ini:



Gambar 1. Prosedur Penelitian

1) Pengumpulan Data (*Observation*)

Berikut adalah beberapa metode pengumpulan data yang peneliti gunakan dalam melakukan penelitian.

1) Observasi

Observasi yang dilakukan peneliti yaitu melakukan pengamatan langsung ditempat penelitian yaitu di SMK Negeri 13 Medan dan pengamatan yang dilakukan yaitu mengamati secara langsung bagaimana operasional *website* yang ada ditempat penelitian.

2) Wawancara

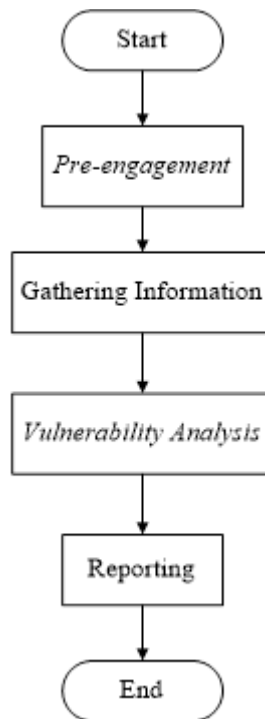
Penliti melakukan pengumpulan data dengan cara berkomunikasi langsung dengan operator *website* di SMK Negeri 13 Medan yaitu Bapak Muhammad Abdul Rozak, S.TP untuk menanyakan beberapa hal yang menyangkut *website* sekolah tersebut.

3) Studi Pustaka

Pengumpulan data dengan melihat referensi dari berbagai sumber berupa skripsi, buku dan jurnal mengenai keamanan *website*, kualitatif dan data pendukung lainnya.

2. Penetration Testing

Tahapan *penetration testing* yang dilakukan dapat dilihat pada *flowchart* berikut:



Gambar 2. *Flowchart Penetration Testing*

1) *Pre-engagement*

Sebelum pentest dimulai, pentester melakukan interaksi *Pre-engagement* dengan klien untuk memastikan semua orang berada di halaman yang sama tentang pengujian penetrasi. Miskomunikasi antara pentester dan klien yang mengharapkan pemindaian kerentanan sederhana dapat menyebabkan situasi yang sulit karena tes penetrasi jauh lebih mengganggu. Klien dalam kasus ini ialah Sekolah SMK Negeri 13 Medan.

2) *Information Gathering*

Dalam tahap ini, penulis melakukan pengumpulan data yang biasa dikategorikan sebagai *passive penetration testing*, karena pada tahap ini, penulis pengumpulan data secara manual melalui dokumentasi dari pihak yang terkait ataupun informasi yang bersifat terbuka pada pihak terkait dengan sistem yang akan diuji. Pada tahap ini akan digunakan *tools* Whois yang dapat memberikan informasi terkait *website* sekolah SMK Negeri 13 Medan.

3) *Vulnerability Analysis*

Selanjutnya, pentester mulai aktif menemukan kerentanan untuk menentukan seberapa sukses strategi mengeksploitasi mereka. Kegagalan yang gagal dapat merusak layanan, memicu peringatan deteksi gangguan, dan sebaliknya merusak peluang Anda untuk mengeksploitasi yang sukses. Seringkali selama fase ini, pentester menjalankan pemindai kerentanan, yang menggunakan *database* kerentanan dan serangkaian pemeriksaan aktif untuk membuat perkiraan terbaik tentang kerentanan yang ada pada sistem klien. Tetapi meskipun pemindai kerentanan adalah alat yang kuat, mereka tidak dapat sepenuhnya mengganti pemikiran kritis, jadi Pentester juga melakukan analisis manual dan memverifikasi hasil sendiri dalam fase ini juga. Pada tahap ini digunakan *tools* Nmap dan OWASP ZAP yang dapat menemukan celah keamanan dari *website* Sekolah SMK Negeri 13 Medan.

4) *Reporting*

Dalam tahap ini penulis menyimpulkan hasil dari tahap sebelumnya kerentanan yang teridentifikasi selama pengujian, dan memberikan rekomendasi terkait langkah untuk mengurangi

kerentanan yang ditemukan dan peningkatan keamanan sistem. Pada tahap ini akan digunakan *tool* OWASP Top 10-2021 yang dapat memberikan laporan terkait 10 keamanan *website*.

3. HASIL DAN PEMBAHASAN

Penelitian ini menggunakan data dan informasi yang diperoleh dari beberapa sumber yang berkaitan dengan penetration testing seperti jurnal, karya ilmiah, buku, tugas akhir atau melalui media internet. Parameter yang digunakan dalam pengujian kerentanan *website* SMK Negeri 13 Medan adalah OWASP Top 10-2021. Berikut adalah 10 daftar kerentanan yang terdapat di dalam OWASP Top 10 2021:

1. *Broken Access Control* naik dari posisi kelima; 94% dari aplikasi yang telah diuji dengan *broken access control* dalam beberapa bentuk. 34 CWE yang dipetakan ke *Broken Access Control* memiliki lebih banyak kemunculan dalam aplikasi daripada kategori lainnya.
2. *Cryptographic Failures* menggeser satu posisi menjadi #2, sebelumnya dikenal sebagai Pengungkapan Data Sensitif, yang merupakan gejala luas dan bukan penyebab utama. Fokus baru di sini adalah pada kegagalan yang terkait dengan Kriptografi yang sering mengarah pada Pengungkapan Data Sensitif atau sistem yang telah terinfeksi oleh *hacker*.
3. *Injection* turun ke posisi ketiga. 94% aplikasi diuji untuk beberapa bentuk injeksi, dan 33 CWE yang dipetakan ke dalam kategori ini memiliki kejadian terbanyak kedua dalam aplikasi. *Skrip cross-site* sekarang menjadi bagian dari kategori ini dalam edisi ini.
4. *Insecure Design* adalah kategori baru untuk tahun 2021, dengan fokus pada resiko yang terkait dengan kekurangan desain. Jika kita ingin benar-benar bergerak sebagai industri, itu membutuhkan lebih banyak penggunaan pemodelan ancaman, pola dan desain yang aman, dan arsitektur referensi.
5. *Security Misconfiguration* naik dari #6 di edisi sebelumnya; 90% aplikasi diuji untuk beberapa bentuk kesalahan konfigurasi. Dengan lebih banyak perubahan ke *software* dengan konfigurasi yang banyak, tidak mengherankan melihat kategori ini naik. Kategori sebelumnya untuk *XML External Entities (XXE)* sekarang menjadi bagian dari kategori ini.
6. *Vulnerable and Outdated Components* sebelumnya berjudul *Using Components with Known Vulnerabilities* dan #2 dalam survei industri, tapi juga memiliki cukup data untuk masuk TOP 10 melalui analisis data. Kategori ini naik dari #9 di tahun 2017 dan merupakan masalah umum yang kami perjuangkan untuk menguji dan menilai resiko. Ini adalah satu-satunya kategori yang tidak memiliki CVE yang dipetakan ke CWE yang disertakan, jadi eksploitasi *default* dan bobot dampak 5.0 diperhitungkan dalam skornya.
7. *Identification and Authentication Failures* sebelumnya adalah *Broken Authentication* dan turun dari posisi kedua, dan sekarang termasuk CWE yang lebih terkait dengan kegagalan identifikasi. Kategori ini masih merupakan bagian integral dari Top 10, tetapi peningkatan ketersediaan *framework* yang telah distandarisasi tampaknya membantu.
8. *Software and Data Integrity Failures* adalah kategori baru untuk tahun 2021, yang berfokus pada pembuatan asumsi terkait pembaruan perangkat lunak, data penting, dan *pipeline* CI/CD tanpa memverifikasi integritas. Salah satu dampak tertinggi dari CVE/CVSS yang dipetakan ke 10 CWE dalam kategori ini. *Insecure Deserialization* dari tahun 2017 sekarang menjadi bagian dari kategori yang lebih besar ini.
9. *Security Logging and Monitoring Failures* sebelumnya Logging dan Monitoring tidak memadai dan ditambahkan dari survei industri (#3), naik dari #10 sebelumnya. Kategori ini diperluas untuk mencakup lebih banyak jenis kegagalan, suatu tantangan untuk diuji, dan tidak terwakili dengan baik dalam data CVE/CVSS. Namun, kegagalan dalam kategori ini dapat secara langsung mempengaruhi visibilitas, *alert* pada insiden, dan forensik.
10. *Server-Side Request Forgery* ditambahkan dari survei industri (#1). Data menunjukkan tingkat insiden yang relatif rendah dengan cakupan pengujian di atas rata-rata, bersama dengan peringkat di atas rata-rata untuk potensi eksploitasi dan dampak. Kategori ini mewakili skenario di mana para

profesional industri memberi tahu kami bahwa ini penting, meskipun tidak diilustrasikan dalam data saat ini.

B. Penerapan Metode Penetration Testing

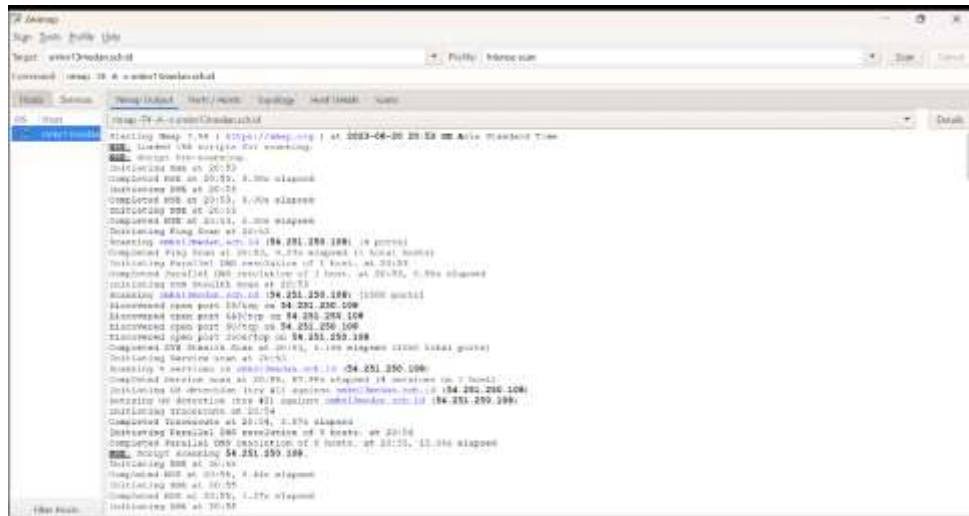
Metode yang digunakan dalam penelitian ini ialah *penetration testing*. Adapun proses dari *penetration testing* untuk mengukur tingkat keamanan *website* Sekolah SMK Negeri 13 Medan adalah sebagai berikut:

1. Analisis *domain web* dengan aplikasi Whois. Berdasarkan hasil analisis menggunakan aplikasi Whois diketahui bahwa domain id atas nama Pandi, *website* dibuat pada tanggal 8 bulan 11 tahun 2021, *website* di registrasi pada Perusahaan Digital Registra. Adapun hasil Analisa dari aplikasi Whois terhadap <https://www.smkn13medan.sch.id/> adalah sebagai berikut:

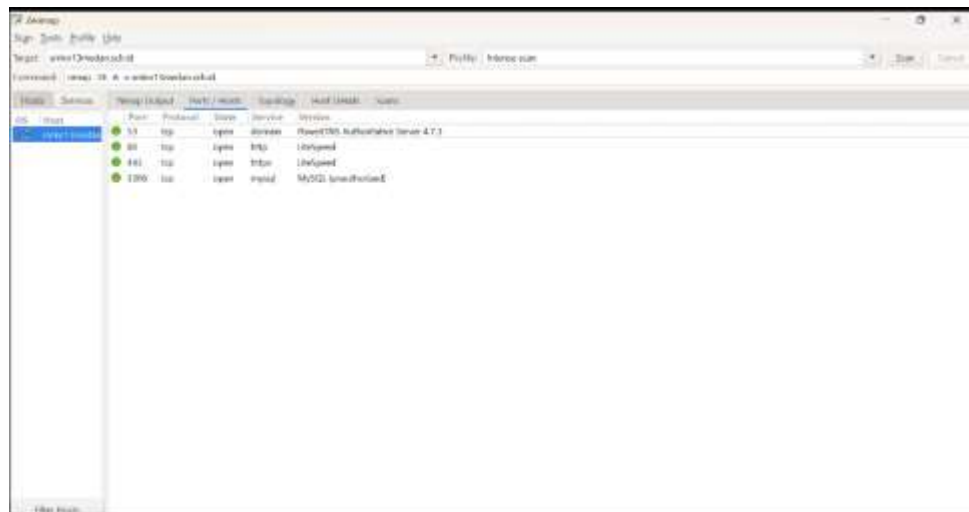


Gambar 2. Hasil Analisis Menggunakan Aplikasi WhoIs

2. Analisis terhadap keamanan jaringan menggunakan aplikasi Nmap. Berdasarkan hasil analisis dengan aplikasi Nmap diperoleh ada 4 port yang terbuka, IP Address IPv4: 54.251.250.108. Adapun hasil dari analisis aplikasi Nmap terhadap *website* [smkn13medan.sch.id](https://www.smkn13medan.sch.id/) adalah sebagai berikut:

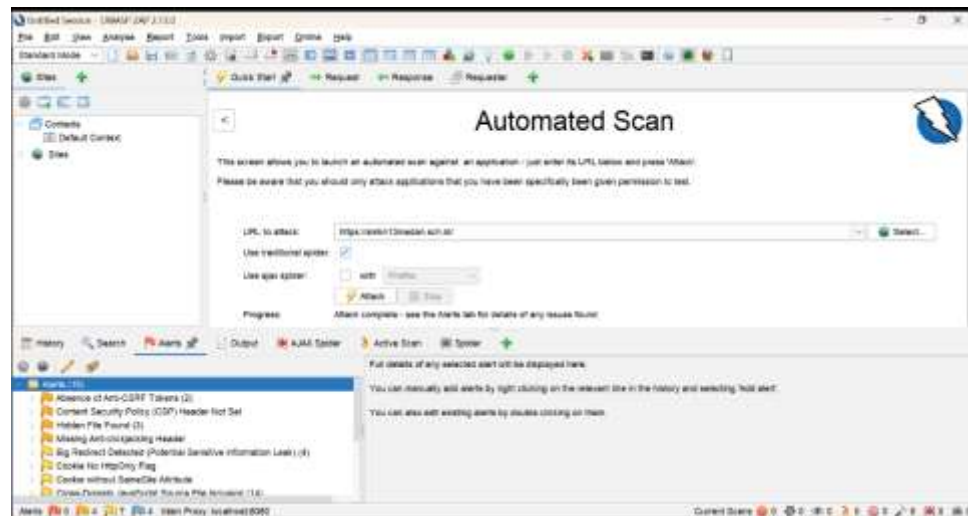


Gambar 3. Hasil Analisis dengan Aplikasi Nmap



Gambar 4. Port yang terbuka

- Analisis Keamanan website dengan aplikasi OWASP ZAP. Berdasarkan asil analisis dengan menggunakan OWASP ZAP, terdapat 11 alerts keamanan. Adapun hasil analisis dapat dilihat pada gambar berikut:



Gambar 5. Analisis dengan OWASP ZAP

C. Hasil

Tahapan inti terdiri *penetration testing* yaitu melakukan penyerangan. Penyerangan dilakukan terhadap kerentanan yang telah ditemukan pada tahap sebelumnya. Adapun hasil dari penyerangan dapat dilihat pada tabel berikut:

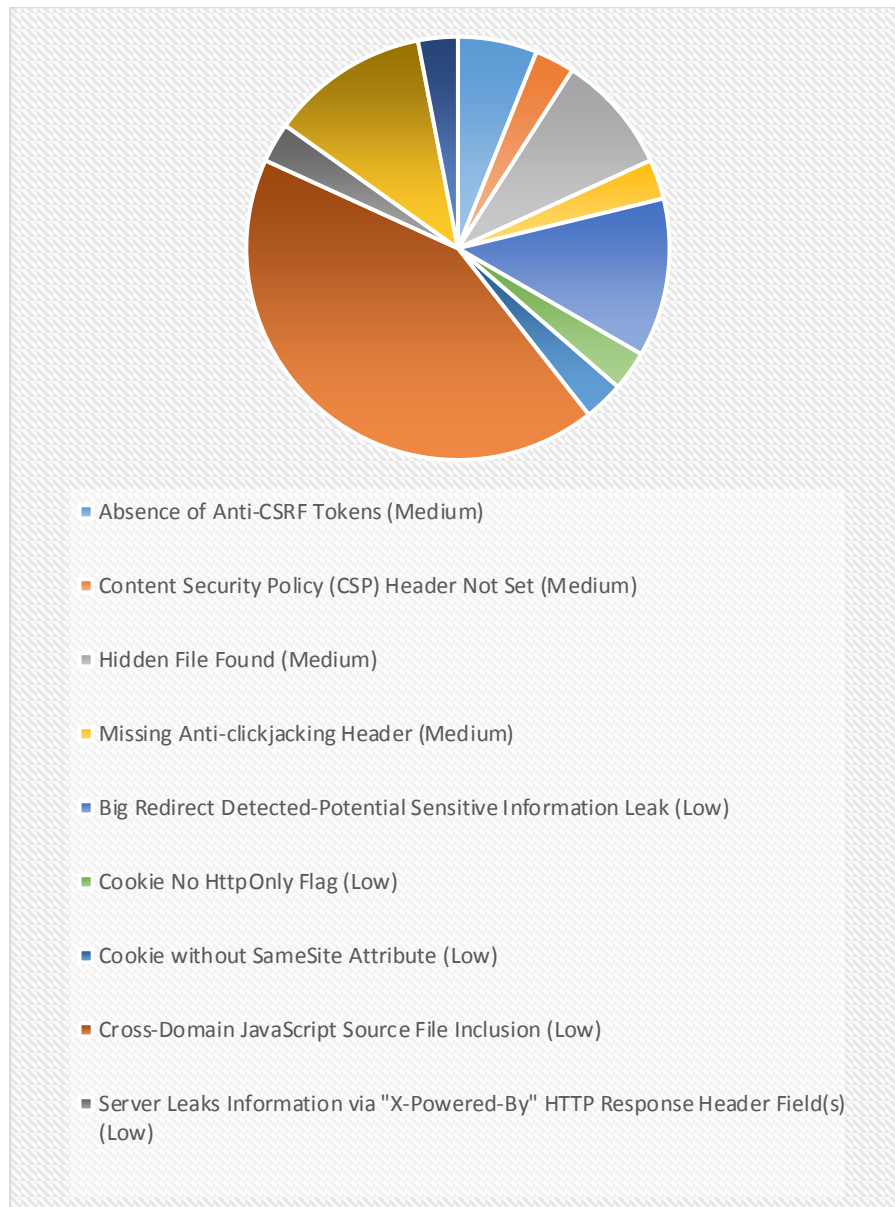
No.	Jenis Ancaman	Jumlah Ancaman	Resiko	Rekomendasi
1.	Absence of Anti-CSRF Tokens	2	Medium	Fase: Arsitektur dan Desain Gunakan pustaka atau kerangka kerja terverifikasi yang tidak memungkinkan kelemahan ini terjadi atau menyediakan konstruksi yang membuat kelemahan ini lebih mudah dihindari. Misalnya, gunakan paket anti-CSRF seperti OWASP CSRFGuard.
2.	Content Security Policy (CSP) Header Not Set	1	Medium	Pastikan bahwa server web Anda, server aplikasi, penyeimbang muatan, dll dikonfigurasi untuk menyetel header Kebijakan-Kelompokan-Konten.
3.	Hidden File Found	3	Medium	Pertimbangkan apakah komponen benar-benar diperlukan dalam produksi atau tidak, jika tidak maka nonaktifkan. Jika kemudian memastikan akses ke sana memerlukan otentikasi dan otorisasi yang sesuai, atau membatasi paparan ke sistem internal atau IP sumber tertentu, dll.

4.	Missing Anti-clickjacking Header	1	Medium	Browser Web modern mendukung header HTTP Content-Security-Policy dan X-Frame-Options. Pastikan salah satunya disetel di semua halaman web yang dikembalikan oleh situs/aplikasi Anda. Jika Anda mengharapkan halaman dibingkai hanya oleh halaman di server Anda (misalnya itu bagian dari FRAMESET) maka Anda akan ingin menggunakan SAMAORIGIN, sebaliknya jika Anda tidak pernah mengharapkan halaman dibingkai, Anda harus menggunakan DENY. Sebagai alternatif, pertimbangkan untuk menerapkan arahan "frame-ancestors" Kebijakan Keamanan Konten.
5.	Big Redirect Detected (Potential Sensitive Information Leak)	4	Low	Pastikan tidak ada informasi sensitif yang bocor melalui tanggapan pengalihan. Redirect tanggapan seharusnya hampir tidak memiliki konten.
6.	Cookie No HttpOnly Flag	1	Low	Pastikan bendera HttpOnly disetel untuk semua cookie.
7.	Cookie without SameSite Attribute	1	Low	Pastikan atribut SameSite disetel ke 'longgar' atau idealnya 'ketat' untuk semua cookie.
8.	Cross-Domain JavaScript Source File Inclusion	14	Low	Pastikan file sumber JavaScript dimuat hanya dari sumber tepercaya, dan sumber tidak dapat dikontrol oleh pengguna akhir aplikasi.
9.	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	1	Low	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menekan header "X-Powered-By".
10.	Strict-Transport-Security	4	Low	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security
11.	X-Content-Type-Options Header Missing	1	Low	Pastikan bahwa aplikasi/server web menyetel tajuk Content-Type dengan benar, dan menyetel tajuk X-Content-Type-Options ke 'nosniff' untuk semua halaman web. Jika memungkinkan, pastikan bahwa pengguna akhir

				menggunakan browser web yang sesuai standar dan modern yang tidak melakukan pelacakan MIME sama sekali, atau yang dapat diarahkan oleh aplikasi web/server web untuk tidak melakukan pelacakan MIME.
--	--	--	--	--

Tabel 1. Hasil Penetration Testing

Berdasarkan tabel di atas diperoleh hasil 4 dengan resiko "*Medium*" dan 7 dengan resiko "*Low*", jadi dapat disimpulkan bahwa *website* sekolah SMK Negeri 13 Medan masih perlu meningkatkan keamanan *web* mereka walau rata-rata beresiko rendah. Adapun hasil yang diperoleh dapat dilihat pada gambar berikut:



Gambar 6. Grafik Hasil Analisis Keamanan Web SMK Negeri 13 Medan

4. SIMPULAN DAN SARAN

Kesimpulan Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Informasi yang valid tentang keamanan web Sekolah SMK Negeri 13 Medan dapat diberikan dengan penerapan metode *penetration testing*. Informasi keamanan web yang diperoleh dari hasil *penetration testing* dapat dikatakan valid karena sudah memiliki standar keamanan web internasional dan diakui oleh banyak negara.
2. Penerapan metode *penetration testing* dimulai dengan menjalin kerjasama dengan pihak sekolah perihal izin untuk melakukan penyerangan terhadap web dengan bantuan *tools*. Langkah berikutnya melakukan pengumpulan data yang biasa dikategorikan sebagai *passive penetration testing*, pada

tahap ini, dilakukan pengumpulan data secara manual melalui dokumentasi dari pihak yang terkait ataupun informasi yang bersifat terbuka pada pihak terkait dengan sistem yang akan diuji. Berikutnya, pentester menjalankan pemindai kerentanan, yang menggunakan *database* kerentanan dan serangkaian pemeriksaan aktif untuk membuat perkiraan terbaik tentang kerentanan yang ada pada sistem klien. Dan yang terakhir memberikan hasil dari tahap sebelumnya kerentanan yang teridentifikasi selama pengujian, dan memberikan rekomendasi terkait langkah untuk mengurangi kerentanan yang ditemukan dan peningkatan keamanan *web*.

3. Metode *penetration testing* yang diterapkan kepada *web* SMK Negeri 13 Medan memberikan hasil ada 11 *alerts* dimana 4 beresiko *Medium* dan 7 dengan resiko *Low*.

Adapun saran yang dapat diberikan oleh penulis ialah:

1. Penulis berharap penelitian berikutnya menerapkan metode lain dalam menguji keamanan *web*, sehingga diperoleh perbandingan metode.
2. Penulis berharap pihak terkait dalam hal ini pengelola Sekolah SMK Negeri 13 Medan untuk dapat meningkatkan keamanan *web*-nya sesuai dengan rekomendasi yang diberikan.
3. Penulis berharap peneliti berikutnya menggunakan *tools* tambahan untuk dapat memberikan hasil yang lebih baik dalam mengukur keamanan sebuah *web*.

UCAPAN TERIMA KASIH

1. Saya ingin mengucapkan terima kasih kepada keluarga saya, yang telah memberikan dukungan tak terbatas selama proses penelitian dan penulisan karya tulis ilmiah ini. Tanpa cinta, pengertian, dan semangat yang kalian berikan, saya tidak akan pernah bisa menyelesaikan penelitian ini.
2. Terima kasih yang sebesar-besarnya kepada dosen pembimbing saya, Bapak Mikha Dayan Sinaga, M.Kom. atas bimbingan, arahan, dan wawasan yang berharga dalam menjalani perjalanan penelitian ini. Beliau telah memberikan dukungan tak tergantikan.
3. Saya ingin mengungkapkan apresiasi kepada teman-teman sejawat saya yang telah memberikan inspirasi dan kerja sama yang erat. Proses diskusi dan kolaborasi dengan kalian telah memperkaya karya tulis ini.
4. Terima kasih kepada semua subjek penelitian dan partisipan yang telah berkenan menjadi bagian dari penelitian ini. Kontribusi dan wawasan kalian sangat berarti dalam menghasilkan data yang diperlukan.
5. Saya ingin mengucapkan terima kasih kepada Bapak Muhammad Abdul Rozak, S.TP selaku operator sekolah di SMK Negeri 13 Medan yang telah memberikan data penelitian untuk penelitian ini.
6. Saya berterima kasih kepada rekan-rekan peneliti dan sesama mahasiswa yang selalu memberikan masukan berharga dan berdiskusi bersama saya. Kalian telah membantu memperkaya ide-ide dalam karya tulis ini.
7. Akhirnya, terima kasih kepada semua pihak yang telah membaca dan meninjau karya tulis ilmiah ini. Kritik konstruktif dan masukan yang diberikan oleh para pembaca sangat membantu saya untuk meningkatkan kualitas penelitian ini.

REFERENSI

- [1] Hidayatulloh, S. and Saptadiaji, D., (2021). "Penetration testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)". *Jurnal Algoritma*, 18(1), pp.77-86.
- [2] Ramadhan, B., (2020). "Data Internet di Indonesia dan Perilakunya Tahun 2020". *Teknoia*.
- [3] Sanjaya, I.G.A.S., Sasmita, G.M.A. and Arsa, D.M.S., (2020). "Evaluasi Keamanan Website Lembaga X Melalui Penetration testing Menggunakan Framework ISSAF". *Jurnal Ilmiah Merpati*, 8(2), pp.113-124.

-
- [4] Azis, H. and Fattah, F., (2019). "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration testing". *ILKOM Jurnal Ilmiah*, 11(2), pp.167-174.
- [5] Ismail, R.W. and Pramudita, R., (2020). "Metode Penetration testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi". *Jurnal Mahasiswa Bina Insani*, 5(1), pp.53-62.
- [6] Wicaksono, B., Kusumaningsih, R.Y.R. and Iswahyudi, C., (2020). "Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration testing Dan Dast (Dynamic Application Security Testing)". *Jurnal Jarkom*, 8(1), pp.1-9.
- [7] Armadhani, A.P., Nofriansyah, D. and Ibnutama, K., (2022). "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration testing Standart OWASP". *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, 21(2), pp.80-88..
- [8] Sahren, S., Dalimuthe, R.A. and Amin, M., (2019). "Penetration testing Untuk Deteksi Vulnerability Sistem Informasi Kampus". In *Prosiding Seminar Nasional Riset Information Science (SENARIS) (Vol. 1, pp. 994-1001)*.
- [9] Mulyanto, Y. and Fari, A.A., (2022). "Analisis Keamanan Login Router Mikrotik Dari Serangan Bruteforce Menggunakan Metode Penetration testing (Studi Kasus: SMK NEGERI 2 SUMBAWA)". *Jurnal Informatika Teknologi dan Sains (Jinteks)*, 4(3), pp.145-155.
- [10] Zen, B.P., Gultom, R.A. and Reksoprodjo, A.H., (2020). "Analisis Security Assessment Menggunakan Metode Penetration testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara". *Teknologi Penginderaan*, 2(1)
- [11] Zaluchu, S.E., (2021). "Metode penelitian di dalam manuskrip jurnal ilmiah keagamaan". *Jurnal teologi berita hidup*, 3(2), pp.249-266.
- [12] Ridwan, M., Suhar, A.M., Ulum, B. and Muhammad, F., (2021). "Pentingnya penerapan literature review pada penelitian ilmiah". *Jurnal Masohi*, 2(1), pp.42-51.
- [13] Sinuhaji, V.V., Siregar, N.S.S. and Jamil, B., (2019). "Aktivitas Komunikasi Pemasaran Dinas Pariwisata Dan Kebudayaan Kabupaten Karo Dalam Meningkatkan Kunjungan Wisatawan (Studi Deskriptif Kualitatif Wisata Bukit Gundaling Berastagi)". *Jurnal Ilmu Pemerintahan, Administrasi Publik, dan Ilmu Komunikasi (JIPIKOM)*, 1(2), pp.105-118.
- [14] Nita Sari Br Sembiring, Mikha Dayan Sinaga, (2017). "Penerapan Metode Dempster Shafer Untuk Mendiagnosa Penyakit Dari Akibat Bakteri Treponema Pallidum". *Jurnal CSRID*, 9(3), pp. 2085-1367.
- [15] Nita Sari Br Sembiring, Mikha Dayan Sinaga, (2022). "Penerapan Metode Certainty Factor untuk Mendiagnosis Penyakit pada Anjing". *Jurnal IT*, 10(2), pp. 2252-746.