Analisis Keamanan Website Menggunakan PTES (*Penetration Testing Execution And Standart*)

Delta Anugrah Utama[1)], Khairil,[2)] Reno Supardi,[2)]

[1]Mahasiswa, Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Jalan Meranti Raya No.32 Sawah Lebar Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: anugrahutamadelta@gmail.com
[2, 3] Dosen Tetap Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: *khairil@unived.ac.id*, *renosupardi00@gmail.com*

(Received: Nopember 2024, Revised : Februari 2024, Accepied : April 2024)

Abstract-Websites are a vital element in the evolution of the internet, with more than 1.9 billion sites worldwide today. Their use was initially limited to personal purposes, but now almost all companies have websites, such as Facebook, Apple, and BBC News. Tim Berners-Lee created the first website in the late 1980s through the World Wide Web (W3) project. Penetration Testing is an evaluation method for identifying weaknesses in a security system, network, or web application. This involves direct attacks against targets under test to detect and correct weaknesses. The aim is to identify potential weak points and ensure compliance with security policies. Test results using Accuntetix show low-level system vulnerabilities on the website of min2kotabengkulu.sch.id, which can be considered quite safe from attacks.

Keywords: Analysis of Website Security Using PTES (Penetration Testing Execution And Standard).

Intisari- Website adalah elemen vital dalam evolusi internet, dengan lebih dari 1,9 miliar situs di seluruh dunia saat ini. Penggunaannya awalnya terbatas pada tujuan pribadi, tetapi sekarang hampir semua perusahaan memiliki situs web, seperti Facebook, Apple, dan BBC News. Tim Berners-Lee menciptakan website pertama pada akhir 1980-an melalui proyek World Wide Web (W3). Penetration Testing adalah metode evaluasi untuk mengidentifikasi kelemahan dalam sistem keamanan, jaringan, atau aplikasi web. Ini melibatkan serangan langsung terhadap target yang diuji untuk mendeteksi dan memperbaiki kelemahan. Tujuannya adalah untuk mengidentifikasi potensi titik lemah dan memastikan kepatuhan terhadap kebijakan keamanan. Hasil pengujian menggunakan Accuntetix menunjukkan kerentanan sistem tingkat rendah pada website min2kotabengkulu.sch.id, yang dapat dianggap cukup aman dari serangan.

Kata Kunci : *Analisis Keamanan Website Menggunakan Ptes (Penetration Testing Execution And Standart)*

I. PENDAHULUAN

Web merupakan salah satu sumber daya dalam internet yang banyak digunakan. Web adalah sumber data dan informasi yang dapat di akses oleh semua orang melalui internet. Dengan menggunakan salah satu *software browser* seperti internet *explorer, mozilla firefox, opera browser*, maupun *google chrome.* Dengan menggunakan fasiliptas ini maka pemakai dapat menjelajahi segala informasi dan berita-berita dunia. Madrasah Ibtidaiyah Negeri 2 Kota Bengkulu adalah salah satu Madrasah yang terletak pada Kota Bengkulu dimana Madrasah Ibtidaiyah Negeri 2 Kota Bengkulu sudah menggunakan Web sebagai sarana publikasi terkait kegiatan pendidikan maupun sarana penyampaian informasi kepada walimurid. Mengingat pentingnya data yang terdapat didalamnya maka perlu diterapkan pengujian keamanan dari Website Publikasi. Pengujian yang akan dilakukan yaitu menggunakan metode *Penetration Testing* utuk mengetahui tingkat kerentanan agar terhindar dari serangan pihak yang tidak bertanggung jawab. Dari uraian diatas maka penulis tertarik mengangkat judul **"Analisis Keamanan Website Menggunakan PTES (*Penetration Testing Execution and Standart*)".**

II. TINJAUAN PUSTAKA

A. Pengertian Website

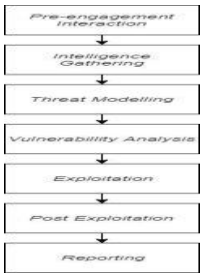
Website adalah bagian tidak terpisahkan dari perkembangan internet, dan saat ini jumlahnya mencapai 1,9 miliar di seluruh dunia. Bahkan, jumlah tersebut akan terus bertambah karena jenis website juga terus berkembang. Awalnya, tujuan penggunaan web adalah untuk pribadi saja. Namun, saat ini hampir semua perusahaan memilikinya. Sebut saja, Facebook, Apple, BBC News dan lainnya, Website pertama di dunia dibuat oleh Tim Berners-Lee pada akhir 1980-an dalam project World Wide Web (W3). Situs web tersebut resmi diluncurkan secara online pada 6 Agustus 1991

P-ISSN 1858-2680
e-ISSN 2723-4673

dengan URL http://info.cern.ch. (Wijayanti, 2022 Website merupakan sebuah teknologi sebagai media penyampaian informasi yang dapat berisi informasi seperti berita terkini tapi juga dapat berisi video maupun lagu (Fatmala dkk, 2018)

B. Penetrating Testing Execution Standard (PTES)

Penetration Testing Execution Standard (PTES) merupakan sebuah standar baru yang di desain bisnis dan penyedia servis keamanan dengan menggunakan Bahasa yang umum dengan cakupan dalam melakukan penetration testing. PTES dimulai pada awal tahun 2009 dan berawal dari pertemuan antara anggota pendiri disaat membicarakan tentang kepentingan atau kelemahan dalam penetration testing yang ada sekarang .Fase PTES didesain untuk menjelaskan sebuah Penetration Testing dan memastika client bahwa sebuah usaha level standarisasi akan diperluas pada Penetration Testing oleh semua orang yang melakukan tipe assestment ini. 7 langkah dalam melakukan Penetration Testing execution (Syarif, T. R, 2019):



Gambar 1 Tahap-Tahap PTES (*Penetration Testing Execution Standard*)

III. METODOLOGI PENELITIAN

Metode Penelitian

Dalam Penelitian skripsi ini penulis menggunakan metode penelitian eksperimen. Metode ini bersifat validation atau menguji, yaitu mengidentifikasi titik-titik lemah pada Web Madrasah Ibtidaiyah Negeri 2 Kota Bengkulu.

IV. HASIL DAN PEMBAHASAN

A. **Hasil**

Dari proses scanning yang telah dilakukan dengan menggunakan Accuntetix terdapat beberapa kemungkinan kerentanan sistem yang berada pada level Low dan beberapa informasi yang disarankan untuk meningkatkan keamanan pada website. Pada tingkat kerentanan Low website min2kotabengkulu.sch.id dapat dikatakan cukup aman dari serangan.

B. Pembahasan

Pre-engagement Interaction

Pada tahapan ini penulis melakukan konfirmasi kepada pengelola website Madrasah Ibtidaiyah Negeri 2 Kota Bengkulu sekaligus meminta izin kepala Madrasah Ibtidaiyah Negeri 2 Kota Bengkulu untuk melakukan Penetration Testing terhadap website min2kotabengkulu.sch.id. Adapun surat izin penelitian dan izin melakukan penetration testing (terlampir)

Intelegence Gathering

Pada tahapan Intelegence Gathering dilakukan pengumpulan informasi terhadap website min2kotabengkulu.sch.id Adapun pengumpulan informasi yang didapat yaitu :

1. Whois

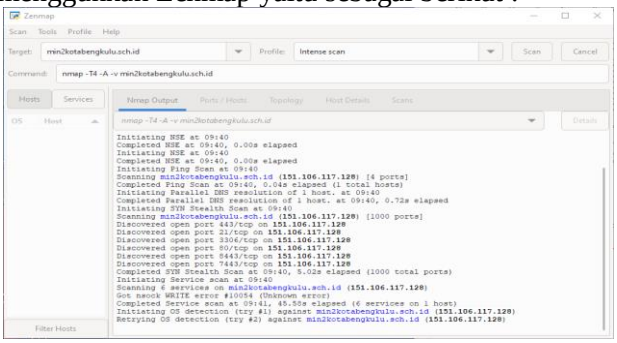
Hasil yang didapatkan dari scanning menggunakan whois yaitu sebagai berikut :

Gambar 2 Pengecekan Whois

Dari hasil scanning menggunakan Whois terlihat beberapa informasi mengenai website min2kotabengkulu.sch.id mulai dari waktu pembuatan domain, waktu habis/expired domain, dimana domain di registrasi dan status clienTransferProhibited yang mana domain tidak diizinkan ditransfer ke registrar lain atau tidak diizinkannya untuk dilakukan DNS Zone Transfer.

2. Zenmap

Hasil yang didapatkan dari hasil scanning menggunkan Zenmap yaitu sebagai berikut :



Gambar 3 Pengecekan Zenmap GUI

Pada hasil scanning menggunakan Zenmap dengan profile instense, all TCP ports menunjukkan informasi server yang digunakan yaitu LiteSpeed hosting yang digunakan yaitu Hostiger dan beberapa port yang terdeteksi diataranya yaitu :

Tabel 11 Hasil Scanning menggunakan Zenmap

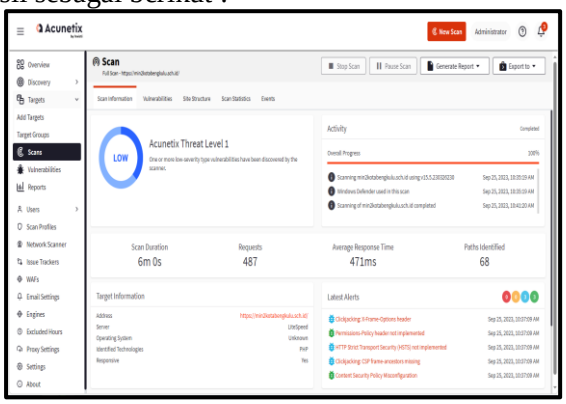
Hasil Scanning	Keterangan
Server	LiteSpeed
Platform	Hostiger

P-ISSN 1858-2680
e-ISSN 2723-4673

port 443/tcp on 151.106.117.128	Open
port 21/tcp on 151.106.117.128	Open
port 3306/tcp on 151.106.117.128	Open
Port 80/tcp on 151.106.117.128	Open
Port 8443/tcp on 151.106.117.128	Open
Port 7443/tcp on 151.106.117.128	Open

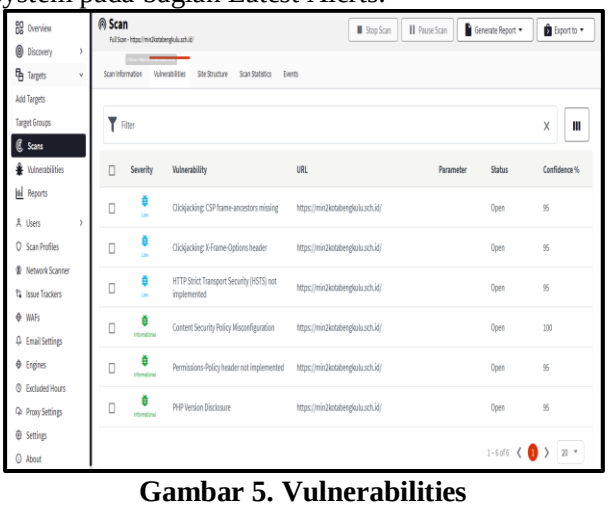
Vulnerabillity Analysis

Pada tahap ini penulis melakukan scanning terhadap website min2kotabengkulu.sch.id dengan menggunakan tools Accunetix dan mendapatkan hasil sebagai berikut :



Gambar 4. Hasil Scaning Accunetix

Pada dashboard scan information terdapat keterangan bahwa hasil scanning menunjukkan potensi kerentanan sistem yang berada pada level low dan terdapat beberapa peringatan kerentanan system pada bagian Latest Alerts.



Gambar 5. Vulnerabilities

dari hasil scanning menggunakan accunetix didapatkan hasil yaitu terdapat 3 kerentanan di level low dan 3 peringatan informational sehingga dapat dikatakan website min2kotabengkulu.sch.id berada di level aman. Berikut table hasil scanning menggunakan accunetix :

Tabel 2 Hasil Scanning Accunetix

Jenis Kerentanan	Jumlah	Tingkat Kerentanan
Clickjacking: CSP frame-ancestors missing	(2)	Low
HTTP Strict Transport Security (HSTS) not implemented	(1)	Low

Selain dari hasil scanning diatas terdapat 3 peringatan dari accunetix yaitu sebagai berikut :

Tabel 3 Peringatan

Jenis Kerentanan	Jumlah	Jenis Peringatan
Content Security Policy Misconfiguration	(1)	Informasi
PHP Version Disclosure	(1)	Informasi

Berdasarkan dari hasil scanning menggunakan accunetix maka didapatkan kesimpulan bahwa tidak ada kerentanan yang berada pada level medium maupun hard hanya terdapat 3 jenis kerentanan di level low dan 3 peringatan sehingga website mi2kotabengkulu.sch.id masih termasuk aman dari serangan.

A. Penjelasan dan Penanganan Kerentanan yang ditemukan.

A. Clickjacking: X-Frame-Options Header

Clickjacking adalah teknik di mana penyerang memasukkan halaman web dalam bingkai transparan di situs web palsu. Dengan X-Frame-Options header, untuk mengatasinya yaitu dengan membatasi cara halaman web dapat dimuat dalam bingkai.

Langkah-langkah penanganan Clickjacking yaitu:

1. Memastikan mengatur header X-Frame-Options dalam pengaturan server web.
2. Atur header X-Frame-Options dengan nilai DENY atau SAMEORIGIN dalam konfigurasi server.
3. Uji situs web untuk memastikan bahwa halaman tidak dapat dimuat dalam bingkai dari situs eksternal.

Misalnya :

1. Penyerang mengirimkan email ke salah satu admin yang bertugas untuk mengelola web kemudian dengan beberapa kode halaman website dibuat transparan yang didalamnya disisikan sebuah tombol agar admin tak sengaja mengklik bagian tersebut contohnya terdapat tombol hapus pada bagian gambar banner sekolah Ketika admin telah login seperti berikut :

P-ISSN 1858-2680
e-ISSN 2723-4673

Bambar 6. Banner sekolah Ketika admin telah login

Kemudian penyerang mengirimkan sebuah email peringatan yang berpura-pura sebagai penyedia hosting "terdapat celah berbahaya pada websitemu segera perbaiki klik disini !" link yang sudah diarahkan ke halaman yang memuat bingkai transparan dan jika admin dalam status login ke dalam website maka celah click jacking akan dapat berjalan seperti berikut :

Gambar 7. Tampilan Penyerangan Email

Karena admin sudah melakukan login maka apabila admin mengklik arahan dari email tersebut maka akan otomatis menghapus banner gambar yang terdapat pada website. Celah keamanan ini juga dapat diimplementasikan kedalam hal lainnya dengan metode yang sama meload halaman website pada bingkai transparan agar admin dengan tidak sengaja mengklik atau menginputkan sesuatu keadalam bingkai transparan yang telah dibuatkan oleh si penyerang.

B. Permissions-Policy Header Not Implemented

Permissions-Policy adalah header HTTP yang memungkinkan untuk mengontrol berbagai izin di halaman web, seperti akses kamera, mikrofon, dan lainnya. Implementasi Permissions-Policy dapat membantu memitigasi risiko keamanan.

Langkah-langkah penanganan Permissions-Policy yaitu:

1. Memastikan untuk mengatur header Permissions-Policy dalam pengaturan server web.
2. Konfigurasikan Permissions-Policy sesuai dengan kebutuhan spesifik.
3. Uji situs web untuk memastikan bahwa izin diatur sesuai dengan yang telah ditentukan.

C. HTTP Strict Transport Security (HSTS) Not Implemented

HSTS adalah mekanisme keamanan yang memaksa klien (seperti browser) untuk selalu menggunakan HTTPS saat terhubung ke situs web tertentu, mengurangi risiko serangan MITM

Langkah-langkah penanganan HTTP Strict Transport Security (HSTS) Not Implemented yaitu :

1. Aktifkan HSTS di server.
2. Setel header Strict-Transport-Security dengan nilai yang sesuai.
3. Pastikan situs web hanya dapat diakses melalui HTTPS.

D. Clickjacking: CSP Frame-Ancestors Missing

Content Security Policy (CSP) adalah mekanisme yang memungkinkan situs web untuk membatasi sumber daya yang dapat dimuat di halaman mereka. Frame-Ancestors adalah direktif dalam CSP yang membatasi halaman mana yang boleh memuat halaman dalam bingkai.

Langkah-langkah penanganan Clickjacking: CSP Frame-Ancestors Missing yaitu :

1. Pastikan untuk menerapkan CSP di situs web.
2. Tambahkan direktif frame-ancestors ke header CSP.
3. Uji situs web untuk memastikan bahwa hanya situs yang diizinkan dapat memuat halaman dalam bingkai.

E. Content Security Policy Misconfiguration

Ini mengindikasikan bahwa konfigurasi Content Security Policy di situs web memiliki masalah. CSP seharusnya membatasi sumber daya yang dapat dimuat di halaman web untuk mengurangi risiko serangan XSS dan jenis serangan lainnya.

Langkah-langkah penanganannya yaitu :

1. Periksa konfigurasi CSP untuk menemukan dan memperbaiki kesalahan atau ketidaksesuaian.
2. Pastikan bahwa direktif CSP diatur sesuai dengan kebutuhan spesifik situs web dan tidak memungkinkan akses tidak sah atau sumber daya eksternal yang tidak aman.

F. PHP Version Disclosure

PHP Version Disclosure adalah masalah keamanan di mana informasi tentang versi PHP yang digunakan oleh server web dapat diakses oleh penyerang. Pengetahuan tentang versi PHP yang ketinggalan zaman atau memiliki kerentanannya dapat membantu penyerang mengidentifikasi celah keamanan potensial yang dapat dieksploitasi.

Langkah-langkah mengatasinya yaitu :

1. Matikan Error Reporting di Produksi

P-ISSN 1858-2680
e-ISSN 2723-4673

Pastikan bahwa pada pengaturan server produksi, opsi untuk menampilkan detail kesalahan PHP ke pengguna akhir dimatikan. Ini dapat dilakukan dengan mengonfigurasi display_errors pada php.ini untuk menjadi Off.

2. Atur expose_php ke Off:
   Dalam konfigurasi php.ini, pastikan expose_php diatur ke Off. Ini akan mencegah server dari mengirimkan header X-Powered-By yang mengungkapkan versi PHP.
3. Perbarui PHP ke Versi Terbaru
   Selalu pastikan bahwa untuk menjalankan versi PHP yang terbaru dan teraman. Versi yang lebih lama mungkin memiliki kerentanan keamanan yang diperbaiki di versi terbaru.
4. Gunakan Web Application Firewall (WAF)
   Menggunakan WAF dapat membantu melindungi aplikasi web dari berbagai jenis serangan, termasuk serangan yang memanfaatkan informasi versi PHP
5. Pemindaian Keamanan Reguler
   Lakukan pemindaian keamanan secara teratur untuk mendeteksi dan memitigasi potensi kerentanan, termasuk masalah pengungkapan versi PHP.
6. Hindari Penggunaan Ekstensi atau Fungsi Lama
   Beberapa ekstensi atau fungsi PHP lama mungkin memiliki kerentanan keamanan yang diketahui. Pastikan menggunakan versi ekstensi dan fungsi yang terbaru.
7. Blokir Informasi Versi PHP di Header Server
   mengonfigurasi server web untuk menghapus atau menyembunyikan header yang mengungkapkan informasi versi PHP. Contohnya, dalam konfigurasi Apache, yaitu dapat menambahkan atau memodifikasi baris berikut di file .htaccess:

Exploitation

SQL Injection adalah teknik serangan keamanan pada aplikasi web yang memungkinkan penyerang untuk menginjeksi kode SQL berbahaya ke dalam input yang diharapkan oleh aplikasi. Hal ini dapat menyebabkan manipulasi atau akses tidak sah ke basis data, serta eksekusi perintah SQL berbahaya.

Dari hasil pengujian scanning menggunakan Accunetix tidak didapatkan celah keamanan yang berupa SQL Injection oleh karena itu proses exploitation dengan menggunakan SQLmap tidak dilakukan.

B. Hasil Pengujian

Reporting

Pada tahapan repoting semua data dari hasil pengujian dikumpulkan menjadi sebuah laporan. Adapun laporan terhadap pengujian website min2kotabengkulu.sch.id adalah sebagai berikut :

1. Hasil Pengumpulan data melalui scanning Whois yaitu sebagai berikut (hasil scanning keseluruhan terlampir):

Tabel 4. Hasil Scanning Whois

Hasil Scanning	Keterangan
Domain Name	min2kotabengkulu.sch.id
Tanggal Registrasi	15 September 2020
Tanggal Berakhir	15 September 2023

2. Hasil Pengumpulan data melalui scanning menggunakan Zenmap yaitu didapatkan detail server sebagai berikut (hasil scanning keseluruhan terlampir):

Tabel 5 Hasil Scanning Zenmap

Hasil Scanning	Keterangan
Server	LiteSpeed
Platform	Hostiger
port 443/tcp on 151.106.117.128	Open
port 21/tcp on 151.106.117.128	Open
port 3306/tcp on 151.106.117.128	Open
Port 80/tcp on 151.106.117.128	Open
Port 8443/tcp on 151.106.117.128	Open
Port 7443/tcp on 151.106.117.128	Open

3. Hasil Pengujian Scanning menggunakan accunetix didapatkan beberapa kerentanan pada beberapa tingkatan yaitu sebagai berikut :

Tabel 6 Hasil Scanning Accunetix

Jenis Kerentanan	Tingkat Kerentanan
Clickjacking: CSP frame-ancestors missing	Low
Clickjacking: X-Frame-Options header	Low
HTTP Strict Transport Security (HSTS) not implemented	Low
Content Security Policy Misconfiguration	Information
Permissions-Policy header not implemented	Information
PHP Version	Information

P-ISSN 1858-2680
e-ISSN 2723-4673

Disclosure	

Terdapat 3 kerentanan yang didapatkan oleh accunetix yang berada pada level low dan 3 informasi saran perbaikan. Dapat disimpulkan berdasarkan hasil pengujian accunetix website hanya memiliki kerentanan di level low sehingga website cukup aman dan hanya dibutuhkan beberapa penyesuaian saja (hasil scanning keseluruhan terlampir).

4. Eksploitation tidak dilakukan dikarenakan tidak ditemukannya celah keamanan yang berupa SQL Injection pada saat scanning dengan Accunetix selesai dilakukan, jadi website sudah aman dari SQL Injection.

Dari semua hasil pengujian yang telah dilakukan maka dapat disimpulkan bahwa website min2kotabengkulu.sch.id sudah termasuk aman hanya saja perlu dilakukan beberapa penyesuaian yang ditemukan oleh accunetix agar keamanan website lebih meningkat lagi (data terlampir).

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil pembahasan pada BAB sebelumnya dapat ditarik kesimpulan bahwa terdapat beberapa kerentanan sistem yang terdeteksi pada saat scanning dengan menggunakan Accinetix selesai dilakukan yaitu kerentanan sistem yang berada pada level Low dan beberapa informasi yang disarankan untuk meningkatkan keamanan pada website. Pada tingkat kerentanan Low website min2kotabengkulu.sch.id dapat dikatakan cukup aman dari serangan, hanya saja disarankan agar lebih baik lagi untuk memperkuat keamanan seperti yang telah disarankan.

B. Saran

Berdasarkan pengujian pada BAB sebelumnya, Maka Penulis Menyarankan:

1. Untuk pengujian selanjutnya diharapkan menggunakan Framework yang berbeda seperti ISSAF (Information System Security Assesment Framework), atau OWASP (The Open Web Application Security Project).
2. Untuk memperbaiki kerentanan sistem yang terdapat pada level LOW maupun informasi perbaikan yang disarankan Accunetix agar keamanan website lebih meningkat.

DAFTAR PUSTAKA

[1] Aufan Imron Rosad, 2018. Analisis Keamanan Sistem Informasi Akademik Dengan Web Penetration Testing Studi Kasus Universitas Xyz, Journal Esa Unggul 2018

[2] F. Ismawan, N. Isnain, and R. A. Raharjo, "Pemanfaatan Website Berbasis CMS - WordPress Sebagai Media Pembelajaran Guru Tk Binakheir Cibinong –Bogor," J. PKM Pengabdi. Kpd. Masy., vol. 03, no. 01, pp. 68–77, 2020

[3] Ghanem, M. C., & Chen, T. M. (2020). Reinforcement learning for efficient network penetration testing. Information (Switzerland), 11(1), 1–23.

[4] Jalinus, N., & Ambiyar, 2016. Media dan Sumber Belajar. *Jakarta : Kencana*, 12– 14.

[5] Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. CyberSeccurity Dan Forensik Digital, 2(2), 77–81.

[6] L. D. Samsumar, K. Gunawan, D. Program, S. Manajemen, D. Program, and S. Komputerisasi, "Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi," Ilm. Teknol. Inf. Terap., vol. IV, no. 1, pp. 73–82, 2017

[7] M. H. Adini, H. S. Purba, and R. A. Sukmawati, "The Development of Blended Learning Model Using Wordpress," 2017. doi: 10.2991/seadric-17.2017.45.

[8] M. I. Alfarisyi and K. Amila, "Rancangan Sistem Informasi Layanan Alumni ITENAS Berbasis Web," vol. 02, no. 01, pp. 132–143, 2014.

[9] M. R. Marwan, "Media Weblog dalam Jurnalistik Online," UG J., vol. 7, no. 09, pp. 27–30, 2013.

[10] Naning Nur Wijayanti (2022) Pengertian Website Lengkap Dengan Jenis dan Manfaatnya, Niaga Hoster *https://www.niagahoster.co.id/blog/pengertianwebsite/?a*. Diakses pada 01 Januari 2023

[11] Nurul Huda (2022). Apa itu WHOIS, Cara Kerja, hingga Fungsinya untuk Domain *www.dewaweb.com* *https://www.dewaweb.com/blog/apa-itu-whois/*. Diakses pada 20 Januari 2023

[12] Patrick Engebretson, 2010. The Basic of Hacking and Penetration Testing: *Ethical Hacking and Penetration Testing Made Easy, Elsevier*

[13] R. Dharmawan and G. Gata, "penerapan aplikasi penjualan online(E-Commerce) Menggunakan Content Management System Wordpress Pada Toko Jaksquare," IDEALIS Indones. J. Inf. Syst., vol. 3, no. 1, pp. 132–138, Feb. 2020, doi: 10.36080/idealis.v3i1.1863.

[14] Satoto, Kodrat Iman, Sistem Analisis Keamanan Informasi Akademik

P-ISSN 1858-2680
e-ISSN 2723-4673

Berbasis Web Di Fakultas Teknik Universitas Diponegoro 2009

[15] Syarif, T. R. (2019). Analisis Perbandingan Metode Web Security Ptes, Issaf Dan Owasp Di Dinas Komunikasi Dan Informasi Kota (Doctoral dissertation, Universitas Komputer Indonesia).

[16] Wahyu Nur Cholifah, 2018. Pengujian Black Box Testing Pada Aplikasi Action & Strategy Berbasis Android dengan Teknologi Phonegap, Jurnal String, 2018 (3), 106-110

[17] Wikipedia (2023). Apa Itu Aplikasi Web? Pengertian Dan Kegunaannya - Aplikasi. https://id.wikipedia.org/wiki/Aplikasi_web diakses pada 10 Januari 2023

[18] W. S. Fatmala, Suprapto, and A. Rachmadi, "Analisis Kualitas Layanan Website E-Commerce Berrybenka Terhadap Kepuasan Pengunjung Menggunakan Metode WebQual 4.0 dan Importance Performance Analysis (IPA)," J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 1, pp. 175–183, 2018.

[19] Yudi Mulyanto, Eka Haryanti, Jumirah, "Analisis Keamanan Website Sman 1 Sumbawa Menggunakan Metode Vulnerability Asesement "Journal Teknik Informatika, Universitas Teknologi Sumbawa 2022

P-ISSN 1858-2680
e-ISSN 2723-4673