CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

Analisis Keamanan Website SMK VIP Al-Huda Kebumen Menggunakan Metode Penetration Testing Execution Standard (PTES)

Abdur Rahman Fadilah[1*], Ghufron Zaida Muflih [2]
[1,2,]Program Studi Teknik Informatika, Universitas Ma'arif Nahdlatul Ulama Kebumen, Indonesia
[1*]abdurfadilah2510@gmail.com, [2]ghufron.zaida@umnu.ac.id

Abstrak: Perkembangan teknologi informasi dan penggunaan internet yang semakin meningkat menyebabkan ancaman keamanan siber terhadap aplikasi berbasis website juga mengalami peningkatan. Website SMK VIP Al Huda Kebumen sebagai media informasi dan layanan digital sekolah memiliki potensi menjadi target serangan siber apabila tidak dilakukan evaluasi keamanan secara berkala. Penelitian ini bertujuan untuk menganalisis tingkat keamanan website SMK VIP Al Huda Kebumen menggunakan metode Penetration Testing Execution Standard (PTES). Metode PTES digunakan karena memiliki tahapan pengujian yang sistematis mulai dari pre-engagement interaction, information gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, hingga reporting. Proses pengujian dilakukan menggunakan beberapa tools seperti Zenmap/Nmap, OWASP ZAP, SQLMap, DNS Scan, dan Infoga. Hasil penelitian menunjukkan bahwa website masih memiliki beberapa potensi kerentanan keamanan, seperti terbukanya beberapa port layanan penting, potensi serangan brute force pada layanan SSH, risiko pencurian kredensial pada layanan FTP, serta kemungkinan eksploitasi pada layanan cPanel. Selain itu, hasil vulnerability analysis menunjukkan adanya beberapa kerentanan dengan tingkat risiko low dan medium yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab. Meskipun sistem telah dilindungi oleh firewall dan menggunakan sistem operasi Linux dengan web server Apache, masih diperlukan peningkatan keamanan melalui pembaruan sistem secara berkala, penerapan enkripsi yang lebih baik, pembatasan akses layanan, serta implementasi kebijakan keamanan tambahan. Penelitian ini diharapkan dapat menjadi referensi dalam meningkatkan keamanan website sekolah dan mencegah ancaman siber di lingkungan pendidikan.
Kata Kunci: PTES; Website Security; Penetration Testing; OWASP ZAP; Cybersecurity

Abstract: The rapid growth of information technology and internet usage has increased cybersecurity threats to web-based applications. The website of SMK VIP Al Huda Kebumen, which functions as a digital information and service platform, has the potential to become a target of cyberattacks if security evaluations are not conducted regularly. This study aims to analyze

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

the security level of the SMK VIP Al Huda Kebumen website using the Penetration Testing Execution Standard (PTES) method. PTES was chosen because it provides systematic testing stages including pre-engagement interaction, information gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting. The testing process utilized several tools such as Zenmap/Nmap, OWASP ZAP, SQLMap, DNS Scan, and Infoga. The results indicate that the website still has several potential security vulnerabilities, including open service ports, brute force attack risks on SSH services, credential theft risks on FTP services, and possible exploitation of cPanel services. In addition, the vulnerability analysis identified several low and medium risk vulnerabilities that could potentially be exploited by attackers. Although the system is protected by a firewall and uses Linux operating system with Apache web server, further improvements are still required through regular system updates, better encryption implementation, service access restrictions, and additional security policies. This research is expected to become a reference for improving school website security and preventing cyber threats in educational environments.
Keywords: PTES; Website Security; Penetration Testing; OWASP ZAP; Cybersecurity

1. PENDAHULUAN

Perkembangan teknologi terus maju seiring dengan perkembangan zaman pada masa sekarang. Selaras juga dengan perkembangan internet pada masa sekarang yang semakin lama semakin meningkat penggunanya [1]. Tercatat pada Januari 2024 jumlah pengguna internet di dunia mencapai 5,35 miliar orang atau 66,2% dari total populasi, sedangkan di Indonesia mencapai 221,56 juta orang dengan tingkat penetrasi sebesar 79,5% [2]. Pesatnya pertumbuhan jumlah pengguna internet, baik secara global maupun di Indonesia, membawa dampak besar dalam berbagai aspek kehidupan, mulai dari ekonomi digital, pendidikan, hingga layanan publik [3].

Perkembangan teknologi informasi diikuti dengan meningkatnya ancaman keamanan siber yang menjadi tantangan serius bagi berbagai sistem digital. Berdasarkan hasil riset, pada semester pertama tahun 2025 tercatat sekitar 133,4 juta serangan siber terdeteksi di Indonesia. Dari jumlah tersebut, sebagian besar serangan berasal dari jenis *Generic Protocol Command Decode* yang mencapai 68,37% dari total serangan. Berbagai bentuk ancaman siber yang sering terjadi meliputi *Denial of Service (DoS), Distributed Denial of Service (DDoS)*, serangan *defacement*, *phishing*, *malware, Trojan Horse,* hingga pembobolan kata sandi (*password cracking*). Selain itu, salah satu teknik yang banyak digunakan oleh pelaku kejahatan siber untuk menyerang basis data adalah *SQL Injection*, yaitu metode penyisipan perintah SQL berbahaya untuk memperoleh akses tidak sah ke dalam sistem database [4].

Aplikasi berbasis website menjadi salah satu target utama serangan siber, mengingat tingginya ketergantungan masyarakat terhadap layanan digital [5]. Namun, di balik kemudahan tersebut, banyak aplikasi masih menyimpan berbagai celah keamanan. Serangan seperti SQL *Injection, Cross-Site Scripting* (XSS), dan *Cross-Site Request Forgery* (CSRF) menjadi ancaman nyata yang sering mengeksploitasi kelemahan sistem [6]. Selain itu, konfigurasi keamanan yang kurang optimal, seperti penggunaan kredensial dalam bentuk teks biasa tanpa enkripsi atau absennya penerapan kebijakan keamanan seperti *Content Security Policy* (CSP) dan *Strict-Transport-Security* (HSTS), semakin memperbesar risiko. Jika celah-celah ini tidak segera diidentifikasi dan diperbaiki, sistem

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

rentan dieksploitasi oleh pihak tidak bertanggung jawab, yang dapat berujung pada pencurian data hingga pengambilalihan kendali sistem.

Masalah-masalah yang sering ditemukan dalam sistem keamanan website mencerminkan berbagai kelemahan mendasar yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Salah satu masalah utama adalah lemahnya sistem autentikasi, seperti penggunaan kata sandi yang mudah ditebak atau tidak adanya mekanisme verifikasi ganda (*two-factor authentication*)[7]. Masih banyak website yang menggunakan protokol keamanan yang sudah usang, seperti TLS 1.0, sehingga rentan terhadap serangan penyadapan data [8]. Konfigurasi server yang tidak aman, seperti pengaturan izin akses yang terlalu longgar atau kegagalan memperbarui perangkat lunak ke versi terbaru, juga menjadi celah besar dalam sistem. Tidak adanya perlindungan terhadap serangan berbasis sesi pengguna, seperti *session hijacking*, memungkinkan penyerang mengambil alih sesi aktif pengguna tanpa sepengetahuan mereka. Di sisi lain, pengelolaan kredensial yang buruk misalnya penyimpanan username dan password dalam bentuk teks biasa semakin memperburuk kondisi keamanan. Berbagai masalah ini menunjukkan pentingnya penerapan evaluasi keamanan secara sistematis dan berkala, guna memastikan bahwa sistem informasi mampu menghadapi ancaman siber yang terus berkembang.

SMK VIP Al Huda Kebumen telah memanfaatkan teknologi informasi melalui penyediaan website resmi sekolah sebagai sarana komunikasi, publikasi, dan penyebaran informasi kepada seluruh pemangku kepentingan. Website SMK VIP Al Huda Kebumen berfungsi sebagai media informasi dan layanan digital sekolah yang dirancang untuk memberikan kemudahan akses informasi kepada siswa, orang tua, guru, calon peserta didik, serta masyarakat umum. Website ini mencakup berbagai fitur penting seperti profil sekolah, informasi Penerimaan Peserta Didik Baru (PPDB), kegiatan sekolah, pengumuman, serta layanan administrasi berbasis digital.

Sebagai platform yang memegang peran vital dalam mendukung pelayanan pendidikan dan komunikasi di lingkungan SMK VIP Al Huda Kebumen, website ini memiliki potensi besar menjadi target serangan siber apabila tidak dilindungi dengan baik. Ancaman seperti peretasan, pencurian data, atau manipulasi informasi dapat mengganggu operasional serta merusak kepercayaan publik terhadap institusi sekolah [9]. Hasil observasi di SMK VIP Al Huda Kebumen, bahwa hingga saat ini belum pernah dilakukan audit terhadap keamanan website tersebut. Hal ini menunjukkan kemungkinan adanya kerentanan yang perlu segera ditangani guna menjamin keamanan data dan keberlangsungan layanan digital sekolah.

Kurangnya audit keamanan secara berkala, tidak adanya sistem deteksi kerentanan yang aktif, serta kemungkinan penggunaan CMS atau plugin yang tidak diperbarui dapat membuka celah terhadap serangan seperti *SQL injection, cross-site scripting (XSS)*, dan serangan lainnya yang umum ditemukan dalam website institusi pendidikan. Diperlukan penerapan metode untuk mengidentifikasi, mengevaluasi, dan menguji keamanan sistem secara menyeluruh agar potensi risiko dapat diminimalkan dan integritas data serta layanan pendidikan daring tetap terjaga. Pengujian penetrasi merupakan proses penting untuk mengevaluasi keamanan sistem komputer dengan mensimulasikan serangan dari sumber jahat dan tidak sah, seperti peretasan dan *jailbreaking*. Sistem keamanan komputer melibatkan aspek teknis, manajerial, legalitas, dan politis. Aplikasi berbasis website sering menjadi target peretasan dan pembobolan sistem karena pertumbuhan penggunaan aplikasi tersebut yang pesat [10].

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 [11]. PTES mencakup aspek teknis dan bisnis dalam pengujian penetrasi. PTES pendekatan yang sistematis dan fleksibel, menjadi pilihan yang lebih menyeluruh untuk pengujian keamanan.

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

Penelitian sebelumnya menunjukkan bahwa PTES efektif digunakan untuk mengidentifikasi kerentanan keamanan pada sistem informasi berbasis web. Penelitian oleh Zen [12] bertujuan untuk memahami risiko keamanan sistem dari serangan siber dengan menerapkan penetration testing pada website teknologi informasi Pertahanan Negara, dan berhasil menemukan kerentanan seperti serangan Brute Force Password. Utoro [13] dalam penelitiannya terhadap website e-learning SMKN 1 Cibatu, mengidentifikasi celah keamanan seperti Web Server Transmits Cleartext Credential, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF), serta menemukan kerentanan Clickjacking melalui alat dari OWASP.

Sementara itu, penelitian [14] dengan judul *Analisis Metode Web Security PTES Pada Aplikasi E-Learning Universitas Negeri Padang* menemukan beberapa kerentanan seperti CSRF, file konfigurasi tidak aman, serangan Slow HTTP DoS, penggunaan TLS 1.0, dan kata sandi yang lemah. Meski teknik SQL Injection gagal karena adanya SSL, tingkat ancaman yang terdeteksi berada pada level menengah, yang menunjukkan perlunya peningkatan keamanan. Penelitian oleh [15] dengan Menggunakan *Metode PTES*, juga membuktikan bahwa metode PTES efektif dalam mengidentifikasi dan mengeksploitasi kerentanan pada website pendidikan. Keseluruhan penelitian tersebut menggarisbawahi pentingnya audit keamanan website secara berkala, khususnya dalam sektor Pendidikan.

Penelitian ini bertujuan mengevaluasi tingkat keamanan situs web SMK VIP Al-Huda Kebumen serta mengidentifikasi potensi kerentanan yang terdapat pada sistem menggunakan pendekatan *Penetration Testing Execution Standard* (PTES). Selain itu, tujuan dari hasil penelitian ini memberikan gambaran mengenai kondisi keamanan sistem informasi sekolah dan menghasilkan rekomendasi perbaikan guna meningkatkan perlindungan terhadap ancaman siber, meminimalkan risiko kebocoran data, serta mendukung operasional sistem yang lebih aman dan optimal.

2. METODE PENELITIAN

Jenis penelitian yang digunakan adalah penelitian eksperimen dengan pendekatan penetration testing terhadap website SMK VIP Al Huda Kebumen. Penelitian dilakukan menggunakan metode *Penetration Testing Execution Standard* (PTES) sebagimana dalam gambar 1.

Gambar 1. Tahapan PTES

Tahapan PTES terdiri dari beberapa tahapan berikut:

1. ***Pre-Engagement Interactions,*** tahap ini dilakukan koordinasi dengan pihak SMK VIP Al Huda Kebumen untuk menentukan ruang lingkup pengujian, target sistem yang diuji yaitu website sekolah, serta memperoleh izin pelaksanaan penetration testing. Selain itu ditetapkan batasan pengujian agar tidak mengganggu operasional website.
2. ***Information Gathering,*** pengumpulan informasi dilakukan terhadap domain website SMK VIP Al Huda Kebumen menggunakan DNS Scan, Infoga, dan Nmap.

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

Tahap ini menghasilkan informasi mengenai alamat IP, layanan yang aktif, port terbuka, serta informasi subdomain yang dapat digunakan sebagai dasar analisis keamanan.

3. ***Threat Modeling,*** dilakukan identifikasi potensi ancaman yang mungkin terjadi pada website. Ancaman yang dianalisis meliputi akses tidak sah melalui port yang terbuka, eksploitasi kerentanan aplikasi web, serangan brute force, dan penyalahgunaan layanan yang tersedia pada server.
4. ***Vulnerability Analysis,*** *a*nalisis kerentanan dilakukan menggunakan OWASP ZAP dan Zenmap untuk mengidentifikasi kelemahan keamanan pada website. Pengujian difokuskan pada konfigurasi server, layanan jaringan yang aktif, serta potensi kerentanan aplikasi web berdasarkan standar keamanan OWASP.
5. ***Exploitation,*** *t*ahap eksploitasi dilakukan secara terbatas dan non-destruktif terhadap kerentanan yang ditemukan. Pengujian bertujuan untuk memverifikasi apakah kerentanan yang teridentifikasi dapat dimanfaatkan oleh pihak tidak berwenang tanpa menyebabkan gangguan pada sistem.
6. ***Post-Exploitation,*** evaluasi terhadap dampak yang mungkin ditimbulkan apabila kerentanan berhasil dimanfaatkan. Evaluasi meliputi potensi akses tidak sah, kebocoran informasi, serta risiko terhadap ketersediaan dan integritas sistem.
7. ***Reporting*****,** seluruh hasil pengujian didokumentasikan dalam bentuk laporan yang berisi temuan kerentanan, tingkat risiko, bukti hasil pengujian, serta rekomendasi mitigasi untuk meningkatkan keamanan website SMK VIP Al Huda Kebumen.

3. HASIL DAN PEMBAHASAN

Pemilihan metode PTES didasarkan pada keunggulannya yang memiliki tahapan pengujian yang terstruktur, sistematis, dan sesuai dengan standar praktik keamanan siber. Metode ini mencakup seluruh proses pengujian, mulai dari tahap pengumpulan informasi awal (intelligence gathering), analisis kerentanan (vulnerability analysis), eksploitasi, hingga penyusunan laporan akhir (reporting), sehingga mampu memberikan gambaran menyeluruh terhadap kondisi keamanan suatu sistem.

Proses pengujian memanfaatkan tools Zenmap, yang merupakan antarmuka grafis (GUI) dari Nmap, untuk melakukan pemindaian jaringan secara detail. Parameter yang diamati dalam penelitian ini meliputi beberapa aspek penting dalam keamanan jaringan, yaitu status host, alamat IP, tingkat latency atau waktu respon server, sistem operasi yang digunakan, jenis web server, serta port dan layanan yang aktif.

Hasil Pre-Engagement Interaction

Merupakan tahap awal yang dilakukan untuk menentukan ruang lingkup penelitian. Dalam penelitian ini, target yang digunakan adalah website smk.alhudajetis.com dengan jenis pengujian yang bersifat non-destruktif. Artinya, pengujian dilakukan tanpa merusak sistem dan hanya berfokus pada identifikasi kerentanan jaringan. Tahap ini memastikan bahwa penelitian dilakukan secara etis dan tidak mengganggu operasional sistem. Ruang lingkup pengujian yang ditetapkan dapat seperti pada Tabel 1.

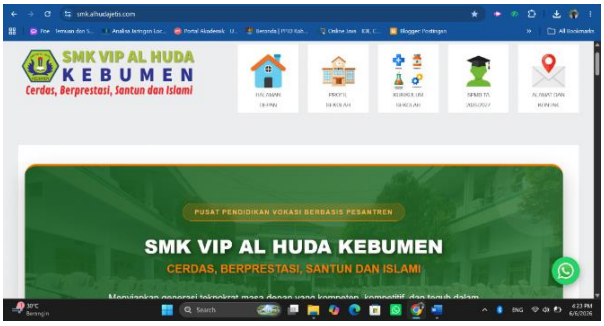
Tabel 1. Ruang Lingkup Pengujian

Aspek	Keterangan
Target Pengujian	Website SMK VIP Al Huda Kebumen (smk.alhudajetis.com)
Metode	Penetration Testing Execution Standard (PTES)
Fokus Pengujian	Identifikasi port terbuka, layanan aktif, dan kerentanan website

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

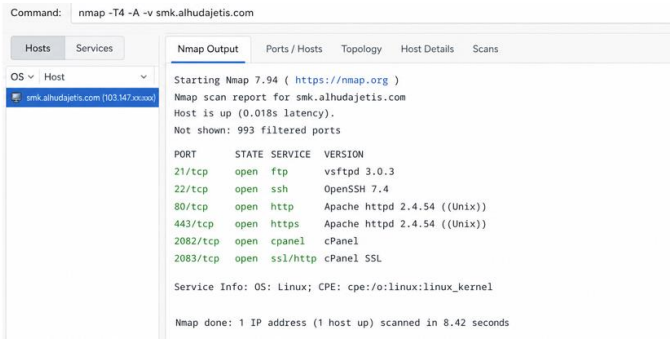
Aspek	Keterangan
Tools	Zenmap/Nmap, OWASP ZAP, DNS Scan, Infoga, SQLMap
Batasan Pengujian	Tidak melakukan perubahan data dan tidak mengganggu operasional sistem



Gambar 2. Website SMK VIP Al Huda Kebumen

Hasil Information Gathering

Hasil informasi pemindaian awal dapat dilihat pada gambar 3.



Gambar 3. Hasil Pemindaian Menggunakan nmap

Berdasarkan gambar 3. Hasil identifikasi port dan layanan seperti pada tabel 2.

Tabel 2. Hasil Identifikasi Port dan Layanan

Port	Status	Service	Keterangan
21	Open	FTP	Layanan transfer file, berpotensi menimbulkan risiko pencurian kredensial
22	Open	SSH	Akses remote server, berpotensi terkena brute force attack
80	Open	HTTP	Layanan website tanpa enkripsi
443	Open	HTTPS	Layanan website dengan enkripsi SSL/TLS
2082	Open	cPanel	Panel administrasi hosting tanpa SSL
2083	Open	cPanel SSL	Panel administrasi hosting menggunakan SSL

Hasil pengumpulan informasi pemindaian awal menggunakan nmap, diperoleh informasi bahwa server website dalam kondisi aktif (host is up) dengan waktu respon

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

sebesar 0,018 detik dan menunjukkan bahwa website menggunakan sistem operasi Linux dengan web server Apache versi 2.4.54. Selain itu ditemukan beberapa layanan aktif seperti HTTP pada port 80, HTTPS pada port 443, FTP pada port 21, SSH pada port 22, dan layanan cPanel dan jenis hosting yang digunakan adalah shared hosting.

Hasil Threat Modeling
Hasil Potensi ancaman yang ditemukan dapat dilihat pada tabel 3.

Tabel 3. Potensi Ancaman

Ancaman	Target	Dampak Potensial
Brute Force Attack	SSH (Port 22)	Akses tidak sah ke server
Credential Theft	FTP (Port 21)	Pencurian username dan password
Unauthorized Access	cPanel (Port 2082/2083)	Pengambilalihan panel administrasi
SQL Injection	Database Website	Kebocoran dan manipulasi data
Cross Site Scripting (XSS)	Aplikasi Web	Pencurian sesi pengguna
Information Disclosure	Server Web	Kebocoran informasi sistem

Berdasarkan hasil analisis ancaman, terdapat beberapa potensi serangan yang mungkin terjadi pada website, antara lain: 1. Brute force attack pada layanan SSH. 2. Pencurian data login melalui layanan FTP. 3. Eksploitasi cPanel oleh pihak tidak berwenang. 4. Serangan SQL Injection dan Cross-Site Scripting (XSS). Ancaman tersebut berpotensi membahayakan data website sekolah dan sistem administrasi yang dikelola.

Hasil Vulnerability Analysis
Hasil Identifikasi Kerentanan dapat dilihat pada tabel 4.

Tabel 4. Hasil Identifikasi Kerentanan

No	Kerentanan	Tingkat Risiko	Dampak
1	FTP Service Active	Medium	Risiko pencurian kredensial
2	SSH Open Port	Medium	Potensi brute force attack
3	Missing Security Header	Low	Risiko clickjacking
4	Open cPanel Access	Medium	Potensi akses ilegal
5	Informational Disclosure	Low	Kebocoran informasi server

Hasil pemindaian menggunakan Zenmap dan OWASP ZAP menunjukkan bahwa sistem memiliki beberapa potensi kerentanan keamanan dengan kategori low dan medium risk. Ditemukan beberapa layanan aktif yang berpotensi menjadi titik masuk serangan apabila tidak dikonfigurasi dengan baik.

Hasil Tahap Exploitation
Hasil Potensi yang didapatkan dan dampaknya dapat dilihat pada tabel 5.

Tabel 5. analisis potensi eksploitasi

Layanan	Potensi Serangan	Dampak yang Mungkin Terjadi
FTP	Credential Sniffing	Kebocoran akun administrator
SSH	Brute Force Attack	Akses ilegal ke server
HTTP	Man in The Middle Attack	Kebocoran data pengguna

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

Layanan	Potensi Serangan	Dampak yang Mungkin Terjadi
cPanel	Unauthorized Access	Pengambilalihan sistem hosting
Website Application	SQL Injection dan XSS	Kebocoran data dan perubahan konten website

Hasil analisis menunjukkan bahwa layanan FTP berpotensi digunakan untuk mencuri data login karena tidak terenkripsi, layanan SSH dapat diserang menggunakan metode brute force, dan layanan cPanel berpotensi menjadi target akses ilegal oleh pihak yang tidak berwenang. Dampak tersebut meliputi pengambilalihan sistem, kebocoran data, perubahan tampilan website, serta gangguan terhadap layanan. Hal ini menunjukkan bahwa potensi kerentanan yang ditemukan dapat berdampak serius terhadap keamanan sistem.

Hasil Tahap Reporting

Hasil temuan teringkas dalam tabel 6.

Tabel 6. ringkasan temuan

Temuan	Tingkat Risiko	Dampak	Rekomendasi
FTP Service Active	Medium	Pencurian kredensial	Gunakan SFTP atau nonaktifkan FTP
SSH Open Port	Medium	Brute Force Attack	Terapkan MFA dan pembatasan IP
Missing Security Header	Low	Clickjacking dan XSS	Tambahkan CSP dan HSTS
Open cPanel Access	Medium	Akses ilegal ke hosting	Batasi akses administrator
Informational Disclosure	Low	Kebocoran informasi sistem	Kurangi informasi server yang ditampilkan

Tahap terakhir yang berisi kesimpulan dari seluruh proses pengujian. Berdasarkan hasil analisis, diketahui bahwa sistem memiliki beberapa potensi celah keamanan meskipun telah memiliki perlindungan dasar seperti firewall. Pengujian jaringan pada website smk.alhudajetis.com dilakukan menggunakan tools Zenmap untuk mengidentifikasi port terbuka, layanan aktif, serta konfigurasi sistem secara menyeluruh. Pengujian dilakukan menggunakan profil Intense Scan dengan perintah nmap -T4 -A -v smk.alhudajetis.com, yang memungkinkan proses scanning dilakukan secara mendalam.

Pembahasan

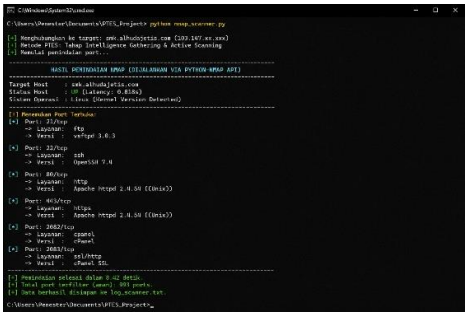
Alamat IP server terdeteksi berada pada jaringan 103.147.xxx.xxx. Sistem operasi yang digunakan adalah Linux dengan kemungkinan distribusi Ubuntu atau CentOS, sedangkan web server yang digunakan adalah Apache versi 2.4.54. Dari hasil pemindaian, ditemukan beberapa port terbuka yang menunjukkan layanan aktif, yaitu port 80 dan 443 sebagai layanan utama website, port 21 untuk FTP, port 22 untuk SSH, serta port 2082 dan 2083 untuk layanan cPanel. Sementara itu, port 3306 yang digunakan untuk database MySQL berada dalam kondisi filtered, yang menunjukkan bahwa database tidak dapat diakses langsung dari luar jaringan.

layanan HTTP dan HTTPS berfungsi sebagai akses utama website, namun apabila tidak dilakukan pengalihan otomatis ke HTTPS maka berpotensi terjadi serangan man-in-

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

the-middle yang dapat menyebabkan kebocoran data. Layanan FTP memiliki risiko karena tidak menggunakan enkripsi sehingga data dapat disadap, sedangkan layanan SSH berpotensi diserang melalui metode brute force. Hasil scanning dapat dilihat pada gambar 4.



Gambar 4. hasil scanning web

Hasil scanning juga menunjukkan adanya beberapa port yang terbuka (open ports) dan menjalankan layanan tertentu, yaitu port 21 (FTP), port 22 (SSH), port 80 (HTTP), port 443 (HTTPS), serta port 2082 dan 2083 (cPanel). Keberadaan port 80 dan 443 merupakan hal yang umum karena digunakan untuk layanan web. Akan tetapi, port lainnya seperti FTP dan SSH memiliki potensi risiko keamanan yang lebih tinggi apabila tidak dikonfigurasi dengan baik.

Keberadaan layanan FTP pada port 21 menjadi salah satu perhatian utama dalam penelitian ini. FTP secara umum tidak menggunakan enkripsi dalam proses pertukaran data, sehingga informasi seperti username dan password dapat ditransmisikan dalam bentuk teks biasa (plain text). Kondisi ini berpotensi menyebabkan kebocoran data apabila terdapat pihak yang melakukan penyadapan (sniffing) terhadap lalu lintas jaringan.

Pengujian hipotesis dilakukan berdasarkan hasil analisis dari proses scanning menggunakan metode Penetration Testing Execution Standard (PTES). Hasil pengujian menunjukkan bahwa terdapat beberapa layanan terbuka yang dapat diakses dari luar jaringan, yaitu layanan FTP pada port 21, layanan SSH pada port 22, serta layanan manajemen hosting cPanel pada port 2082 dan 2083. Keberadaan layanan-layanan tersebut menunjukkan adanya potensi titik masuk (entry point) yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, terutama apabila tidak dilengkapi dengan sistem keamanan yang memadai seperti enkripsi, pembatasan akses, dan autentikasi berlapis.

Berdasarkan hasil tersebut, diperlukan beberapa langkah mitigasi sebagaimana tabel 7.

Tabel 7. Mitigasi Keamanan Website SMK VIP Al Huda Kebumen

No	Temuan Kerentanan	Risiko	Mitigasi yang Disarankan
1	Port FTP (21) terbuka	Potensi akses tidak sah dan pencurian data	Menonaktifkan layanan FTP jika tidak digunakan atau menggantinya dengan SFTP yang lebih aman.
2	Port SSH (22) terbuka	Risiko serangan brute force dan akses ilegal	Membatasi akses SSH berdasarkan alamat IP tertentu dan menerapkan autentikasi multi faktor (MFA).
3	Port cPanel (2082 dan 2083) terbuka	Potensi penyalahgunaan panel administrasi	Membatasi akses hanya untuk administrator dan menggunakan kata sandi yang kuat serta MFA.

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

4	Konfigurasi keamanan belum optimal	Kerentanan terhadap eksploitasi sistem	Melakukan pembaruan sistem, aplikasi, dan plugin secara berkala.
5	Header keamanan belum lengkap	Rentan terhadap serangan XSS, clickjacking, dan man-in-the-middle	Menambahkan Content Security Policy (CSP), Strict-Transport-Security (HSTS), dan header keamanan lainnya.
6	Penggunaan protokol yang kurang aman	Risiko penyadapan data saat transmisi	Menggunakan protokol terenkripsi seperti HTTPS/TLS pada seluruh layanan web.

Berdasarkan tabel di atas, langkah mitigasi difokuskan pada pengurangan permukaan serangan (attack surface), penguatan mekanisme autentikasi, peningkatan keamanan konfigurasi layanan, serta penerapan kebijakan keamanan pada sisi server. Implementasi mitigasi tersebut diharapkan dapat meningkatkan tingkat keamanan website SMK VIP Al Huda Kebumen terhadap berbagai ancaman siber yang mungkin terjadi.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan menggunakan metode Penetration Testing Execution Standard (PTES), dapat disimpulkan bahwa website SMK VIP Al Huda Kebumen masih memiliki beberapa potensi kerentanan keamanan dengan tingkat risiko rendah hingga sedang yang perlu mendapatkan perhatian serius. Hasil pengujian menunjukkan adanya layanan aktif seperti FTP (port 21), SSH (port 22), HTTP/HTTPS (port 80/443), serta cPanel (port 2082/2083) yang berpotensi menjadi titik masuk serangan apabila tidak dikonfigurasi dengan baik. Layanan FTP menjadi salah satu kerentanan utama karena tidak menggunakan enkripsi secara default, sehingga berisiko terhadap pencurian data login. Layanan SSH juga berpotensi mengalami serangan brute force apabila autentikasi tidak diperkuat. akses publik terhadap cPanel meningkatkan risiko pengambilalihan sistem apabila tidak dibatasi dengan mekanisme keamanan tambahan. Penggunaan metode PTES terbukti mampu membantu proses identifikasi kerentanan secara sistematis mulai dari tahap pengumpulan informasi hingga pelaporan hasil pengujian dibuktikan bahwa hipotesis alternatif (H_1) diterima, yaitu terdapat potensi kerentanan keamanan pada website SMK VIP Al Huda Kebumen. Dengan demikian, meskipun website telah memiliki perlindungan dasar, sistem keamanan secara keseluruhan masih perlu ditingkatkan, terutama pada aspek konfigurasi layanan, kontrol akses, serta penerapan standar keamanan. Selain itu, tools seperti Zenmap, OWASP ZAP, dan SQLMap efektif digunakan dalam proses analisis keamanan website. Rekomendasi yang dapat diberikan antara lain melakukan pembaruan sistem secara berkala, menerapkan security header tambahan, membatasi akses layanan tertentu, menggunakan autentikasi yang lebih kuat, dan melakukan audit keamanan secara berkala untuk meningkatkan keamanan website.

5. REFERENCES

[1] G. Z. Muflih, I. Riadi, A. Yudhana, and H. I. Azmi, "Comparison Of Forensic Tools On Social Media Services Using," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 1, pp. 52–61, 2023, doi: 10.33387/jiko.v6i1.5872.

[2] E. S. Mubasyier Fatah , Yohanes Ngamal, "Kemajuan Tik, Digitaslisasi Membuka Jalan Bagi Pertumbuhan Ekonomi Digital Indonesia," *Manaj. BISNIS*, vol. XVI, no. 1, 2024.

Abdur Rahman Fadilah: *Penulis Korespondensi

CHAIN: Journal of Computer Technology, Computer Engineering and Informatics
Website : https://ejournal.techcart-press.com/index.php/chain
E-ISSN 2964-2485
P-ISSN 2964-2450
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/chain.v4i3.290**
Page 218-228

[3] A. Fahrudin, G. Z. Muflih, and T. Informatika, "Analisis Forensik Digital Pada Pesan Whatsapp Yang Terenkripsi Dengan Pretty Good Privacy (Pgp) Menggunakan Framework Dfrws," vol. 9, no. 1, pp. 780–787, 2025, doi: https://doi.org/10.36040/jati.v9i1.12506.

[4] S. Lika, R. Dwi, P. Halim, and I. Verdian, "Analisa Serangan Sql Injeksi Menggunakan Sqlmap Implementation Of Online Accounting Software As Supporting Of Financial Statement," vol. 4, no. 2, pp. 88–94, 2018, doi: https://doi.org/10.31961/positif.v4i2.610.

[5] M. A. Dio Wahyu Saputra , Risqy Siwi Pradini, "Analisis dan Rekomendasi Keamanan Website Kampus X," vol. 6, no. 1, pp. 830–843, 2025, doi: https://doi.org/10.35870/jimik.v6i1.1306.

[6] N. H. Nurasmawati, Mansur, "Analisis Kerentanan Keamanan pada Website Kelurahan Rimba Sekampung dengan Menggunakan Framework OWASP ZAP," *JUTIN J. Tek. Ind. Terintegrasi*, vol. 8, no. 4, 2025, doi: 10.31004/jutin.v8i4.48523.

[7] I. Rahayu and J. M. Parenreng, "Pengujian Keamanan Website Sistem Informasi Pengajuan Judul (SIMPEL) menggunakan Metode Pengujian Penetrasi," vol. 0, pp. 1–18.

[8] R. Rahman, "Analisis Penerapan Ssl / Tls Dalam Menjaga Keamanan Transmisi Data Pada Aplikasi Web," vol. 10, no. 1, pp. 171–173, 2026.

[9] G. Z. Muflih, F. Teknik, T. Informatika, K. Jaringan, M. Routeros, and P. Pesantren, "Implementasi Web Filtering Firewall untuk Keamanan pada Jaringan Internet di Pondok Pesantren Al Hidayah Kebumen," vol. 8, pp. 46–59, 2025, doi: https://doi.org/10.36080/skanika.v8i1.3298.

[10] S. Alhidamkara and I. Lucia Kharisma, "Analisis Keamanan Website Sekolah Menengah Atas Negeri 1 Surade Dengan Pendekatan Comprehensive Website Security Assessment Website Security Analysis for State Senior High School 1 Surade with a Comprehensive Website Security Assessment Approach," pp. 57–65, 2023.

[11] D. A. Utama, K. Khairil, and R. Supardi, "Analisis Keamanan Website Menggunakan Ptes (Penetration Testing Execution And Standart)," *J. Media Infotama*, vol. 20, no. 1, pp. 106–112, 2024, [Online]. Available: https://jurnal.unived.ac.id/index.php/jmi/article/view/5367%0Ahttps://jurnal.unived.ac.id/index.php/jmi/article/download/5367/4261

[12] B. P. Zen, R. A. G. Gultom, A. H. S. Reksoprodjo, P. T. Penginderaan, F. T. Pertahanan, and U. Pertahanan, "Analisis Security Assessment Menggunakan Metode Penetration Testing Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara," pp. 105–122.

[13] S. Utoro, B. A. Nugroho, M. Meinawati, and S. R. Widianto, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," *Multinetics*, vol. 6, no. 2, pp. 169–178, 2020, doi: 10.32722/multinetics.v6i2.3432.

[14] F. Y. Fauzan and S. Syukhri, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang," *Voteteknika (Vocational Tek. Elektron. dan Inform.*, vol. 9, no. 2, p. 105, 2021, doi: 10.24036/voteteknika.v9i2.111778.

[15] M. Nur Fikri, B. Parga Zen, R. Adhitama, and E. Ahmad Firdaus, "Analisis Keamanan Sistem Informasi Website SMA Negeri 1 Sokaraja Menggunakan Metode Penetration Testing Execution Standard (PTES)," *J. Inform.*, vol. 2, no. 2, pp. 19–27, 2023, doi: 10.57094/ji.v2i2.1046.

Abdur Rahman Fadilah: *Penulis Korespondensi