EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer **DOI:** https://doi.org/10.47065/explorer.vxix.xxxx

Analisis Komparatif Kerentanan dan Mitigasi Keamanan Website SMK At-Tamimi pada Hosting *InfinityFree* Menggunakan Metode *Penetration Testing*

Nabila[1*], Firman Jaya[2], Nur Azizah[3]
[1,2,3] STKIP PGRI Situbondo, Situbondo, Indonesia
[1*]nabilaromy219@gmail.com, [2]altamis1922@gmail.com, [3]nazizah0606@gmail.com[3]
[*)] Penulis Korespondensi

Abstrak− Penelitian ini dilatarbelakangi oleh meningkatnya kebutuhan keamanan layanan digital sekolah, sementara pengelolaan dan konfigurasi sistem pada beberapa website sekolah masih berpotensi menimbulkan celah keamanan. Tujuan dari penelitian ini adalah menganalisis sekaligus membandingkan tingkat keamanan website SMK At-Tamimi dengan hosting InfinityFree serta merekomendasikan perbaikan yang paling relevan. Metode yang digunakan adalah penetration testing nondestruktif dengan pendekatan deskriptif komparatif, melalui tahapan *footprinting, scanning-fingerprinting, vulnerability verification*, dan *reporting*. Pengujian dilakukan pada dua website sekolah, yaitu SMK At-Tamimi dan MAN 2 Situbondo, menggunakan aplikasi ZAP by Checkmarx dan pemeriksaan pendukung terhadap konfigurasi keamanan website. Hasil pengujian menunjukkan perbedaan tingkat risiko antarwebsite. Kedua website sama-sama menghasilkan 9 alert. Website SMK At-Tamimi memuat 1 temuan berisiko High (11,1%), 2 Medium (22,2%), 2 Low (22,2%), dan 4 Informational (44,4%), sedangkan MAN 2 Situbondo tidak memuat temuan High (0%), dengan 2 Medium (22,2%), 4 Low (44,4%), dan 3 Informational (33,3%). Website MAN 2 Situbondo memiliki tingkat keamanan tertinggi karena tidak ditemukan indikasi kerentanan berisiko tinggi serta konfigurasi yang lebih baik. Website SMK At-Tamimi berada pada posisi keamanan lebih rendah dibandingkan dengan website pembandingnya, karena muncul indikasi *Cloud Metadata Potentially Exposed*, namun tidak disertai bukti akses yang dapat divalidasi dalam batas pengujian. Temuan penelitian mengindikasikan perlunya penguatan konfigurasi keamanan website sekolah melalui penerapan HTTPS/SSL, penambahan header keamanan, dan pembaruan sistem secara berkala. Selain itu, penggunaan hosting berbayar dapat menjadi alternatif untuk memperoleh kontrol konfigurasi keamanan yang lebih luas dan mengurangi risiko *security misconfiguration*.

Kata kunci: Keamanan Website, *Penetration Testing*, InfinityFree, ZAP by Checkmarx, Website Sekolah

Abstract− This research is motivated by the increasing security needs of school digital services, while the management and configuration of systems on several school websites still has the potential to cause security gaps. The purpose of this study is to analyze and compare the security level of SMK At-Tamimi's website with InfinityFree hosting and recommend the most relevant improvements. The method used is non-destructive penetration testing with a comparative descriptive approach, through the stages of footprinting, scanning-fingerprinting, vulnerability verification, and reporting. The test was carried out on two school websites, namely SMK At-Tamimi and MAN 2 Situbondo, using the ZAP by Checkmarx application and supporting checks on the website security configuration. The test results show the difference in risk levels between websites. Both websites generate 9 alerts. The SMK At-Tamimi website contains 1 finding of High risk (11.1%), 2 Medium (22.2%), 2 Low (22.2%), and 4 Informational (44.4%), while MAN 2 Situbondo does not contain High (0%) findings, with 2 Medium (22.2%), 4 Low (44.4%), and 3 Informational (33.3%). The MAN 2 Situbondo website has the highest level of security because there are no indications of high-risk vulnerabilities as well as better configuration. The SMK At-Tamimi website is in a lower security position compared to its comparative website, because there is an indication of Cloud Metadata Potentially Exposed, but it is not accompanied by proof of access that can be validated within the test limit. The findings of the study indicate the need to strengthen the security configuration of school websites through the implementation of HTTPS/SSL, the addition of security headers, and regular system updates. Additionally, the use of paid hosting can be an alternative to gaining broader control over security configurations and reducing the risk of security misconfiguration.

Keywords: Website Security, Penetration Testing, InfinityFree, ZAP by Checkmarx, School Website

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

1. PENDAHULUAN

Pada era modernisasi saat ini, website sudah menjadi bagian esensial dalam berbagai aspek kehidupan, termasuk di sektor pendidikan. Website bukan sekadar berperan sebagai media informasi dan komunikasi, tetapi sekaligus berperan sebagai program layanan yang esensial bagi pranata pendidikan seperti SMK At Tamimi. Dengan semakin banyaknya informasi dan data yang tersimpan serta diproses secara daring, keamanan website menjadi prioritas utama untuk menjaga privasi, kejujuran, dan keberadaan data tersebut [1]. Setiap perangkat lunak yang beroperasi dalam sebuah sistem memiliki kemungkinan untuk dimanfaatkan oleh pihak tidak bertanggung jawab melalui kerentanan keamanan yang ada, baik melalui akses lokal maupun jarak jauh. Risiko tersebut semakin besar pada perangkat lunak berbasis web karena sifatnya yang lebih terbuka dan area serangannya yang lebih luas [2]. Risiko keamanan siber, seperti serangan hacker dan malware, terus berkembang dan menjadi tantangan serius yang harus dihadapi oleh pengelola website [3]. Data BSSN memperlihatkan bahwa serangan siber selalu mengalami peningkatan setiap tahunnya. Jika pada 2018 terdata 12,8 juta serangan, angka ini naik menjadi 74,2 juta pada 2020, dan pada 2025 bahkan sudah menembus lebih dari 3,6 miliar serangan selama satu tahun [4]. Salah satu bagian penting dalam keamanan siber adalah kemampuan untuk menemukan serta menilai kerentanan yang terdapat pada suatu situs web [5].

Salah satu cara yang diterapkan untuk mengidentifikasi dan mengatasi risiko tersebut adalah *penetration testing*. *Penetration testing* merupakan teknik pengujian penetrasi dengan mencontohkan ancaman secara teratur untuk menemukan kerentanan sebelum disalahgunakan oleh peretas [6]. Metode ini digunakan sebagai pedoman yang sistematis dan komprehensif untuk membantu para praktisi keamanan siber dalam melaksanakan proses penetration testing [7]. InfinityFree adalah salah satu provider yang menawarkan hosting, subdomain dan fitur gratis namun terbatas [8]. Penggunaan layanan hosting gratis seperti InfinityFree oleh banyak pranata pendidikan, termasuk SMK At Tamimi, menjadi fenomena yang perlu mendapatkan perhatian istimewa dalam konteks keamanan website. Hosting gratis menyediakan akses yang mudah dan harga terjangkau, akan tetapi biasanya memiliki keterbatasan dalam hal pengelolaan keamanan dan kontrol teknis. Lemahnya keamanan website berpotensi membuka celah bagi berbagai jenis serangan siber [9]. Serangan siber dapat berakibat pada kerusakan sistem, pencurian data, serta hilangnya kepercayaan dari pengguna dan pihak yang berkepentingan [10]. Berdasarkan data empiris dari berbagai insiden serangan siber pada website yang menggunakan hosting gratis, terdapat peningkatan risiko keamanan akibat kurangnya proteksi dan pengawasan yang memadai. Insiden serangan terhadap website sekolah yang menggunakan layanan hosting gratis menunjukkan adanya kebutuhan mendesak untuk melakukan evaluasi dan pengujian keamanan secara rutin.

Penelitian terdahulu menunjukkan bahwa *penetration testing* pada website institusi pendidikan efektif untuk memetakan celah keamanan [11]. Selain itu, juga menyusun rekomendasi mitigasi berbasis bukti melalui tahapan pengumpulan informasi, pemindaian, validasi temuan, hingga pelaporan. Studi pada website SMA Negeri 3 Berau, misalnya, menerapkan pengujian penetrasi untuk mengidentifikasi kerentanan dan menekankan pentingnya evaluasi berkala terhadap konfigurasi serta komponen aplikasi yang digunakan [12]. Sejalan dengan itu, penelitian lain pada konteks website SMK juga melaporkan bahwa pemindaian dapat mengungkap berbagai kelemahan yang relevan untuk perbaikan keamanan layanan publik sekolah [13].

Meskipun demikian, sebagian besar penelitian sebelumnya berfokus pada identifikasi kerentanan website tanpa mempertimbangkan pengaruh jenis layanan hosting yang digunakan. Padahal, beberapa kerentanan yang termasuk dalam kategori *Security Misconfiguration* pada OWASP Top 10 berpotensi dipengaruhi oleh keterbatasan kontrol konfigurasi, pengelolaan sertifikat keamanan, dan penerapan mekanisme proteksi yang tersedia pada layanan hosting. Oleh karena itu, masih terdapat kesenjangan penelitian terkait perbandingan tingkat kerentanan antara website yang menggunakan hosting gratis dan hosting berbayar. Dengan demikian, penelitian ini berkontribusi melalui temuan komparatif yang lebih operasional mengenai perbedaan risiko keamanan yang dipengaruhi oleh keterbatasan kontrol konfigurasi hosting, sekaligus rekomendasi mitigasi yang realistis bagi pengelola website sekolah. Kebaruan (novelty) penelitian ini terletak pada penempatan jenis layanan hosting (gratis InfinityFree dibandingkan dengan berbayar) sebagai variabel pembanding utama tingkat kerentanan, aspek yang belum menjadi fokus pada studi sebelumnya yang umumnya hanya mengidentifikasi kerentanan pada satu website tanpa mengaitkannya dengan keterbatasan kontrol konfigurasi hosting. Penilaian risiko pada penelitian ini dipetakan secara eksplisit terhadap standar OWASP Top 10 [2], [14], khususnya kategori A05:2021 Security Misconfiguration, sedangkan alur pengujiannya mengadopsi prinsip pengujian terstruktur yang sejalan dengan framework PTES [15], Vulnerability Assessment [16], dan ISSAF [17], sehingga temuan dapat ditelusuri secara sistematis. Berdasarkan latar belakang tersebut, tujuan penelitian ini adalah: (1) menganalisis tingkat kerentanan keamanan website SMK At-Tamimi yang menggunakan hosting gratis InfinityFree; (2) membandingkan tingkat kerentanan tersebut dengan website MAN 2 Situbondo yang menggunakan hosting berbayar; dan (3) merumuskan rekomendasi mitigasi yang realistis bagi pengelola website sekolah.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

2. METODE PENELITIAN

Studi ini menerapkan metode komparasi deskriptif. Studi ini dilaksanakan guna mengevaluasi dan membandingkan status kerentanan keamanan website sekolah. Objek penelitian ini terdiri dari dua website sekolah pada jenjang yang setara dan dioperasikan pada lingkungan hosting berbeda, yaitu website yang menggunakan hosting gratis InfinityFree (shared hosting) sebagai objek utama dan website pembanding yang menggunakan layanan hosting berbayar dari penyedia lain. Perbandingan dilakukan berdasarkan beberapa indikator yang berkaitan dengan status kerentanan keamanan hosting dan temuan berisiko tinggi.

Berbagai pendekatan dapat digunakan untuk mengevaluasi keamanan website, seperti *security audit*, *vulnerability assessment*, dan *penetration testing*. *Security audit* berfokus pada pemeriksaan kepatuhan terhadap standar dan kebijakan keamanan [18], sedangkan *vulnerability assessment* bertujuan mengidentifikasi potensi kerentanan melalui proses pemindaian otomatis [19]. Meskipun kedua metode tersebut relatif efisien, hasil yang diperoleh umumnya hanya menunjukkan potensi kelemahan tanpa melakukan validasi lebih lanjut terhadap tingkat risikonya. Sebaliknya, *penetration testing* memungkinkan proses identifikasi dan verifikasi kerentanan berdasarkan kondisi aktual sistem sehingga memberikan gambaran keamanan yang lebih komprehensif [20]. Namun, metode ini membutuhkan waktu, keahlian, dan sumber daya yang lebih besar dibandingkan dengan metode lainnya. Oleh karena itu, penelitian ini memilih *penetration testing* karena dinilai lebih sesuai untuk menganalisis dan membandingkan tingkat kerentanan website pada lingkungan hosting yang berbeda. Pemilihan metode ini sejalan dengan sejumlah studi terdahulu yang menyatakan bahwa pengujian penetrasi memberikan gambaran kerentanan yang lebih akurat dibandingkan pendekatan otomatis semata [21], [22], [23] Serta penelitian komparatif perangkat pengujian terhadap OWASP Top 10. Dalam konteks studi kasus ini, perbedaan jenis hosting (gratis InfinityFree dibandingkan dengan berbayar) menjadi variabel utama, sehingga metode penetration testing nondestruktif diterapkan untuk mengungkap kerentanan yang berkaitan dengan keterbatasan kontrol konfigurasi pada lingkungan shared hosting.

Tahapan *Penetration Testing Execution Standard* (PTES) meliputi *Footprinting*, *Scanning-Fingerprinting*, *Vulnerability Verification*, dan *Reporting*. Namun, mengingat objek penelitian merupakan website sekolah yang aktif digunakan, tahap eksploitasi tidak dilakukan secara langsung untuk menghindari risiko gangguan layanan, perubahan data, maupun dampak operasional lainnya. Sebagai gantinya, penelitian menerapkan pendekatan verifikasi noninvasif dengan menganalisis bukti kerentanan yang diperoleh dari hasil pemindaian, respons server, konfigurasi keamanan, serta indikator risiko yang teridentifikasi. Pendekatan ini memungkinkan validasi kerentanan dilakukan secara etis tanpa mengganggu integritas dan ketersediaan sistem.

Gambar 1 menunjukkan tahapan penelitian yang mengacu pada PTES. Setiap tahapan menghasilkan keluaran yang digunakan sebagai masukan pada tahapan berikutnya. Selain menunjukkan alur penelitian, diagram juga memuat perangkat yang digunakan pada setiap tahap pengujian untuk mempermudah pemahaman proses penelitian.

Tabel 1. Tahapan Penetration Testing

Tahapan	Tools	Output
Footprinting	Whois	Informasi domain dan layanan hosting
Scanning-Fingerprinting	Nslookup, Zenmap, OWASP ZAP	Informasi DNS, alamat IP, port terbuka, dan potensi kerentanan
Vulnerability Verification	Analisis hasil pemindaian dan respons server	Kerentanan yang tervalidasi
Reporting	Analisis komparatif	Laporan hasil pengujian dan rekomendasi mitigasi

Penelitian ini tidak melakukan eksploitasi aktif terhadap kerentanan yang ditemukan. Oleh karena itu, validasi dilakukan berdasarkan bukti teknis dan indikator kerentanan yang diperoleh selama proses pengujian. Pendekatan ini dipilih untuk menjaga keamanan dan stabilitas website yang menjadi objek penelitian. Penelitian ini berfokus pada kerentanan yang berkaitan langsung dengan keamanan hosting dan risiko kerentanan tertinggi.

a. *Footprinting*

Tahap footprinting dilakukan untuk mengumpulkan informasi awal mengenai website dan layanan hosting yang digunakan. Informasi yang dikumpulkan meliputi alamat domain, jenis hosting, serta karakteristik umum server yang dapat diketahui melalui akses publik. Pada tahap ini, penulis melakukan pencarian informasi menggunakan situs web https://www.whois.com/whois/.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

b. Scanning-Fingerprinting

Pada tahap ini dilakukan pemindaian untuk mengidentifikasi alamat IP, layanan aktif, serta respons sistem terhadap pemindaian keamanan. Tahapan ini bertujuan untuk memperoleh gambaran umum mengenai lingkungan shared hosting dan keterbatasan konfigurasi keamanan yang ada. Pada tahapan ini penulis menggunakan beberapa tools antara lain sebagai berikut :

1. Nslookup
   Nslookup digunakan untuk mengetahui alamat IP dari suatu domain. Pada penelitian ini, proses pencarian DNS dilakukan melalui situs https://www.nslookup.io/ .
2. Zenmap GUI
   Zenmap adalah NMAP versi GUI [24]. Aplikasi *scanning* untuk mengetahui port yang terbuka. Setelah menjalankan pemindaian dengan memilih opsi scan, sistem akan menampilkan daftar port yang terdeteksi dalam kondisi terbuka.
3. Zap by Checkmarx
   Aplikasi ini digunakan untuk mengidentifikasi potensi celah kerentanan pada sebuah website. Caranya, salin tautan website lalu tempelkan ke dalam tool ZAP, kemudian jalankan proses pemindaian dengan memilih attack. Setelah itu, hasil pengujian akan menampilkan jenis temuan atau potensi kerentanan yang terdeteksi pada website tersebut.

c. Vulnerability Verification

Tahap ini dilakukan dalam bentuk verifikasi kerentanan, bukan eksploitasi destruktif agar celah yang diidentifikasi tidak diretas oleh hacker [25]. Peneliti memverifikasi keberadaan potensi kerentanan keamanan dengan mengamati respons sistem dan hasil pemindaian, seperti pengaturan keamanan server dan indikasi risiko pada layanan hosting yang digunakan. Tahap ini dilakukan secara etis dan tidak menyebabkan perubahan maupun gangguan pada sistem.

d. Reporting

Tahap reporting dilakukan dengan menyusun hasil pengujian yang telah diperoleh ke dalam bentuk laporan. Laporan mencakup jenis kerentanan yang ditemukan, tingkat risiko, serta saran umum untuk memproteksi website, terutama yang berhubungan dengan penggunaan layanan hosting.

3. HASIL DAN PEMBAHASAN

3.1 SMK At-Tamimi

3.1.1 Footprinting

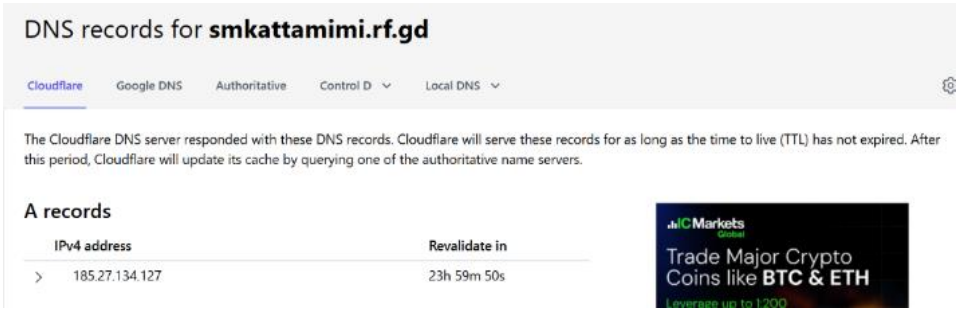
Di tahap tersebut, penulis memanfaatkan layanan Whois.com untuk mendapatkan informasi terkait domain website SMK At-Tamimi. Berdasarkan penelusuran terhadap domain https://smkattamimi.rf.gd/, diperoleh beberapa detail informasi domain sebagai berikut:

Gambar 1. Hasil Whois.com SMK At-Tamimi

3.1.2 Scanning Fingerprinting

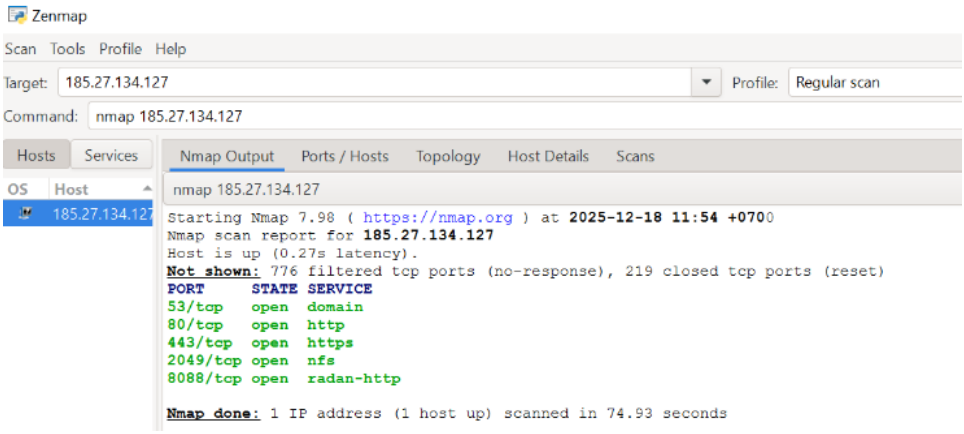
Untuk mengetahui alamat IP dari domain website SMK At-Tamimi, penulis menggunakan tool nslookup. Gambar 2 menunjukkan hasil pemindaian yang diperoleh melalui nslookup.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx



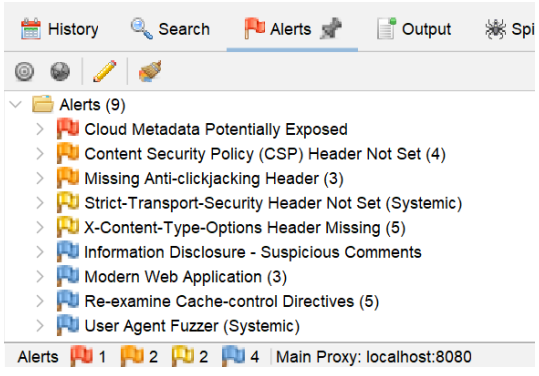
Gambar 2. Hasil Nslookup SMK At-Tamimi

Berdasarkan hasil pengujian port scanning tersebut, dapat diketahui informasi alamat situs serta alamat IP yang terkait dengan website SMK At-Tamimi. Hasil pemindaian menggunakan nslookup menampilkan data alamat IPv4 "185.27.134.127" dari website SMK At-Tamimi. Untuk mengetahui layanan server serta status port aktif pada website SMK At-Tamimi, penulis menggunakan tool Zenmap GUI. Pengujian dilakukan melalui proses port scanning, dengan hasil yang diperlihatkan pada Gambar 3.



Gambar 3. Hasil Scan Zenmap GUI SMK At-Tamimi

Berdasarkan pengujian port scanning di atas, terlihat ada beberapa port service yang statusnya terbuka seperti domain, http, https, nfs dan radan-http. Selanjutnya, penulis melakukan pengujian menggunakan Zed Attack Proxy (ZAP) by Checkmarx untuk mengidentifikasi potensi kerentanan keamanan pada website SMK At-Tamimi. Adapun hasil pengujian kerentanan yang diperoleh disajikan pada Gambar 4.



Gambar 4. Hasil Scan ZAP SMK At-Tamimi

Berdasarkan temuan pemeriksaan yang memanfaatkan aplikasi ZAP, didapatkan beberapa kerentanan keamanan pada website SMK At-Tamimi, yaitu 9 alerts dan 4 level kerentanan, di antaranya: High, Medium, Low, dan Informational. Hasil dari pengujian kerentanan keamanan website SMK At-Tamimi menemukan 9 jenis sub file vulnerability sebagaimana ditunjukkan pada tabel dibawah ini :

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

Tabel 2. Hasil Scan Zap SMK At-Tamimi

No	Alert	Risk	Keterangan
1.	Cloud Metadata Potentially Exposed	High	Serangan Cloud Metadata dilakukan dengan memanfaatkan konfigurasi server NGINX yang kurang tepat untuk memperoleh akses ke metadata instance yang disediakan oleh layanan cloud seperti AWS, GCP, maupun Azure.
2.	Content Security Policy (CSP) Header Not Set (4)	Medium	Content Security Policy (CSP) merupakan mekanisme keamanan tambahan yang digunakan untuk membantu mendeteksi sekaligus meminimalkan berbagai ancaman siber, terutama serangan Cross-Site Scripting (XSS) dan injeksi data.
3.	Missing Anti-clickjacking Header (3)	Medium	Respons dari server belum memiliki perlindungan terhadap serangan ClickJacking. Oleh karena itu, sistem sebaiknya menerapkan header Content-Security-Policy dengan direktif frame-ancestors atau menggunakan X-Frame-Options.
4.	Strict-Transport-Security Header Not Set (Systemic)	Low	HTTP Strict Transport Security (HSTS) adalah kebijakan keamanan web yang menginstruksikan browser atau user agent lainnya agar hanya melakukan komunikasi dengan server melalui koneksi HTTPS yang aman dan dilindungi oleh TLS/SSL. Standar HSTS ditetapkan oleh IETF dan didokumentasikan dalam RFC 6797.
5.	X-Content-Type-Options Header Missing (5)	Low	Header keamanan X-Content-Type-Options belum dikonfigurasi dengan nilai nosniff. Akibatnya, beberapa versi lama Internet Explorer dan Chrome masih dapat melakukan MIME-sniffing terhadap isi respons, sehingga konten berpotensi ditafsirkan dan ditampilkan sebagai jenis konten yang berbeda dari tipe yang telah dideklarasikan sebelumnya.
6.	Information Disclosure – Suspicious Comments	Informational	Respons dari server terindikasi mengandung komentar tertentu yang dapat memberikan informasi tambahan dan berpotensi dimanfaatkan oleh penyerang.
7.	Modern Web Application (3)	Informational	Aplikasi tersebut terlihat menggunakan teknologi web modern, sehingga penggunaan Ajax Spider dinilai lebih efektif untuk proses penelusuran otomatis dibandingkan dengan metode spider biasa.
8.	Re-Examine Cache-Control Directives (5)	Informational	Header Cache-Control belum dikonfigurasi dengan baik atau bahkan tidak tersedia, sehingga browser maupun proxy masih memungkinkan untuk menyimpan salinan cache dari konten yang diakses.
9.	User Agent Fuzzer (Systemic).	Informational	Pengujian dilaksanakan untuk membandingkan perbedaan respons berdasarkan variasi User-Agent yang digunakan, seperti mode situs mobile atau akses yang menyerupai crawler mesin pencari. Proses ini mencakup perbandingan kode status respons serta nilai hash isi respons terhadap respons asli.

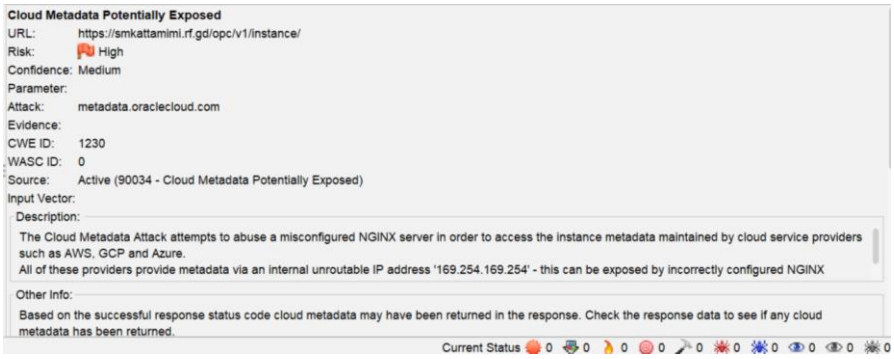
3.1.3 Vulnerability verification

Tahap eksploitasi dalam penelitian ini dilakukan dalam bentuk verifikasi kerentanan, bukan eksploitasi destruktif. Berdasarkan hasil pemindaian keamanan, ditemukan beberapa potensi kerentanan yang berkaitan dengan keamanan hosting dan risiko tinggi, antara lain:

1. Cloud Metadata Potentially Exposed

Ditemukan indikasi potensi eksposur metadata cloud yang menunjukkan adanya risiko keamanan pada layanan hosting berbasis cloud. Kerentanan ini berkaitan dengan konfigurasi server yang tidak sepenuhnya dapat dikendalikan oleh pengguna shared hosting. Kerentanan ini dibuktikan dengan hasil pemindaian yang dilakukan menggunakan ZAP by Checkmarx. Output pemindaian tersaji pada gambar dibawah ini:

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

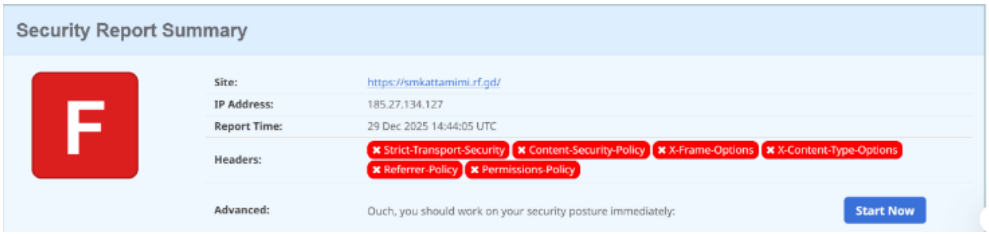


Gambar 5. Indikasi alert Cloud Metadata Potentially Exposed

Berdasarkan hasil pemindaian menggunakan ZAP by Checkmarx, teridentifikasi kerentanan *Cloud Metadata Potentially Exposed*. Temuan ini menunjukkan adanya indikasi risiko eksposur metadata cloud yang berasal dari konfigurasi lingkungan hosting. Verifikasi dilakukan melalui analisis detail alert dan deskripsi risiko yang dihasilkan oleh ZAP, tanpa melakukan akses langsung ke endpoint metadata.

2. Header Keamanan HTTP Tidak Diterapkan

Hasil pengujian menunjukkan bahwa beberapa header keamanan penting tidak diterapkan pada respons server, seperti pengaturan keamanan untuk perlindungan terhadap serangan tertentu. Kondisi ini menunjukkan keterbatasan pengguna dalam menerapkan kebijakan keamanan server pada layanan hosting gratis. Kerentanan ini juga diperiksa dengan pemeriksaan tambahan menggunakan layanan analisis header HTTP secara online menggunakan website https://securityheaders.com/ untuk memastikan konsistensi hasil pengujian terhadap konfigurasi keamanan server. Temuan dari proses pengujian disajikan pada Gambar 6.



Gambar 6. Bukti Header HTTP SMK At-Tamimi

Pada Gambar 6 tampak bahwa tidak diterapkan headers Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, dan X-Content-Type-Options. Hal tersebut memperkuat hasil verifikasi bahwa website belum menerapkan mekanisme perlindungan keamanan pada tingkat konfigurasi server, sehingga berpotensi meningkatkan risiko terjadinya serangan berbasis injeksi konten, seperti Cross-Site Scripting (XSS). Kondisi ini menunjukkan adanya keterbatasan pengaturan keamanan yang umumnya ditemukan pada layanan hosting gratis dengan kontrol konfigurasi server yang terbatas.

3.1.4 Reporting

Setelah dilakukan pemindaian menggunakan ZAP by Checkmark, terdapat 9 risiko yang ditemukan. Dari hasil pemindaian tersebut terdapat rekomendasi yang disusun sebagai langkah mitigasi risiko yang termuat pada tabel dibawah ini:

Tabel 3. Rekomendasi Mitigasi Risk SMK At-Tamimi

No	Alert	Risk	Rekomendasi
1.	Cloud Metadata Potentially Exposed	High	Hindari mempercayai seluruh data yang berasal dari pengguna dalam konfigurasi NGINX karena dapat menimbulkan celah keamanan pada server.
2.	Content Security Policy (CSP) Header Not Set (4)	Medium	Pastikan server web, application server, load balancer, dan komponen terkait lainnya telah dikonfigurasi untuk menerapkan header Content-Security-Policy.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

3.	Missing Anti-clickjacking Header (3)	Medium	Browser modern umumnya telah mendukung header HTTP Content-Security-Policy dan X-Frame-Options. Oleh sebab itu, salah satu mekanisme tersebut perlu diterapkan pada seluruh halaman web yang disediakan oleh aplikasi atau situs.
4.	Strict-Transport-Security Header Not Set (Systemic)	Low	Pastikan server web, server aplikasi, load balancer, dan layanan pendukung lainnya dikonfigurasi untuk mengaktifkan kebijakan Strict-Transport-Security.
5.	X-Content-Type-Options Header Missing (5)	Low	Pastikan aplikasi atau server web menetapkan header Content-Type secara benar serta mengaktifkan header X-Content-Type-Options dengan nilai nosniff pada seluruh halaman web.
6.	Information Disclosure – Suspicious Comments	Informational	Hapus komentar yang berpotensi membocorkan informasi penting kepada penyerang dan lakukan perbaikan terhadap permasalahan yang berkaitan dengan komentar tersebut.
7.	Modern Web Application (3)	Informational	-
8.	Re-Examine Cache-Control Directives (5)	Informational	Untuk melindungi konten sensitif, atur header HTTP Cache-Control dengan nilai no-cache, no-store, must-revalidate. Sementara itu, untuk aset yang memang perlu disimpan dalam cache, dapat dipertimbangkan penggunaan direktif public, max-age, immutable
9.	User Agent Fuzzer (Systemic).	Informational	-

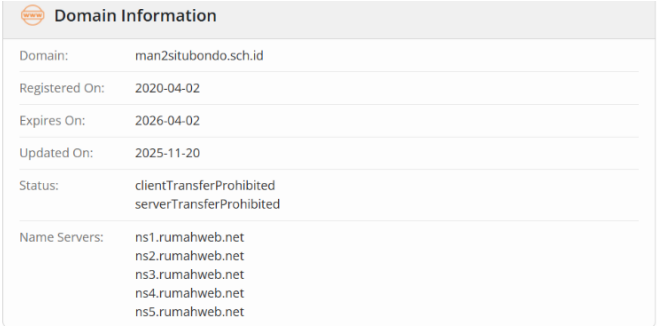
Berdasarkan hasil pemindaian keamanan, ditemukan beberapa potensi kerentanan yang berkaitan dengan konfigurasi keamanan hosting yang dipaparkan pada tahap proses vulnerability verification. Secara umum, temuan pada tahapan tersebut telah teridentifikasi bahwa website SMK At-Tamimi pada layanan InfinityFree masih memiliki beberapa potensi celah keamanan yang dominan dipicu oleh keterbatasan pengaturan serta kontrol proteksi pada lingkungan shared hosting. Celah yang teridentifikasi tidak berkaitan dengan kegagalan fungsi aplikasi website, melainkan lebih dipengaruhi oleh minimnya dukungan fitur keamanan dan ruang konfigurasi yang disediakan pada layanan hosting gratis InfinityFree.

Oleh karena itu, penulis memberikan rekomendasi kepada pengelola website SMK At-Tamimi untuk meningkatkan kontrol keamanan pada aspek yang masih dapat dikelola dari sisi pengguna, terutama dengan memastikan penggunaan HTTPS/SSL aktif dan konsisten, menerapkan penguatan konfigurasi dasar seperti pengaturan akses direktori dan pembatasan file sensitif, melakukan pembaruan rutin CMS/tema/plugin, serta mengaktifkan mekanisme pencadangan (backup) berkala. Selain itu, disarankan melakukan pemantauan keamanan secara periodik (misalnya melalui vulnerability scanning noninvasif dan audit konfigurasi), menerapkan kebijakan kata sandi yang kuat dengan autentikasi dua faktor (jika tersedia), serta mempertimbangkan migrasi ke hosting berbayar apabila dibutuhkan fitur keamanan yang lebih lengkap, dukungan teknis yang lebih responsif, dan fleksibilitas konfigurasi untuk mitigasi risiko jangka panjang.

3.2 MAN 2 Situbondo

3.2.1 Footprinting

Berdasarkan penelusuran informasi website https://man2situbondo.sch.id/ melalui Whois.com, beberapa detail informasi domain berhasil diidentifikasi seperti terlihat pada Gambar 7.



Gambar 7. Hasil whois.com MAN 2 Situbondo

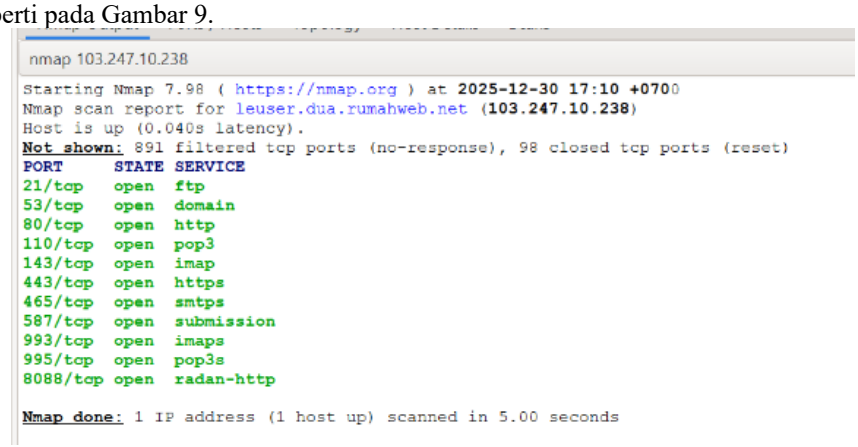
EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

3.2.2 Scanning Fingerprinting

Untuk mengecek alamat IP dari website MAN 2 Situbondo, penulis mengaplikasikan tool nslookup. Tampilan hasil analisis pemindaian dapat diperhatikan pada Gambar 8.

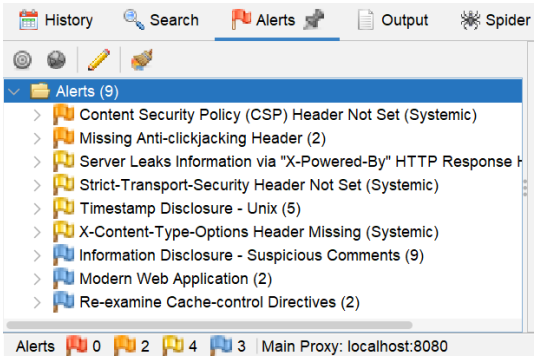
Gambar 8. Hasil Scan Nslookup MAN 2 Situbondo

Berdasarkan hasil pengujian port scanning tersebut, dapat diketahui informasi alamat situs serta alamat IP yang terkait dengan website MAN 2 Situbondo. Hasil pemindaian pada website MAN 2 Situbondo menampilkan data alamat IPv4 "103.247.10.238". Untuk mengetahui layanan server serta port yang terbuka pada website MAN 2 Situbondo, penulis menggunakan tool Zenmap GUI. Proses pengujian menghasilkan tampilan seperti pada Gambar 9.



Gambar 9. Hasil Scan Zenmap MAN 2 Situbondo

Berdasarkan pengujian port scanning di atas, terlihat ada beberapa port service yang statusnya terbuka seperti ftp, Domain, http, pop3, imap, https, SMTP, Submission, IMAP, pop3s dan radan-http. Selanjutnya, penulis melakukan pengujian dengan memanfaatkan aplikasi ZAP untuk mengidentifikasi potensi celah kerentanan keamanan pada website MAN 2 Situbondo. Adapun hasil pengujian kerentanan yang diperoleh tampak pada Gambar 10.



Gambar 10. Hasil Scan ZAP MAN 2 Situbondo

Menurut hasil pengujian yang dijalankan menggunakan tool ZAP, didapatkan beberapa kerentanan keamanan pada website MAN 2 Situbondo, yakni 9 alerts dan 3 level kerentanan, di antaranya: Medium, Low, dan Informational. Rincian data selengkapnya tercantum pada Tabel 4.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

Tabel 4. Hasil Scan ZAP MAN 2 Situbondo

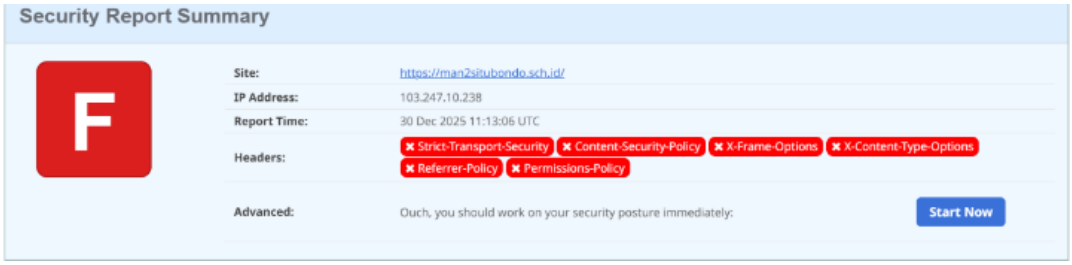
No	Alert	Risk	Keterangan
1.	Content Security Policy (CSP) Header Not Set (Systemic)	Medium	These types of attacks can lead to various security issues, including unauthorized data access, website manipulation, and malware delivery. Content Security Policy (CSP) helps reduce these risks by using standardized HTTP headers that specify which content sources are trusted and permitted to load within a webpage. The policy can regulate resources such as JavaScript, CSS, images, fonts, HTML frames, and embedded media, including audio, video, Java applets, and ActiveX components.
2.	Missing Anti-clickjacking Header (2)	Medium	The server response currently lacks protection against ClickJacking attacks. To mitigate this risk, the application should implement either the Content-Security-Policy header with the frame-ancestors directive or the X-Frame-Options header to control how the page can be embedded within frames.
3.	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (2)	Low	The web or application server exposes technology-related details through one or more X-Powered-By HTTP response headers. Disclosure of this information may assist attackers in identifying the frameworks or components used by the application, potentially making it easier to target known vulnerabilities associated with those technologies.
4.	Strict-Transport-Security Header Not Set (Systemic)	Low	HTTP Strict Transport Security (HSTS) is a web security feature that enables a server to require browsers and other user agents to communicate exclusively through secure HTTPS connections. Through this mechanism, access via unsecured HTTP is automatically blocked, ensuring that all transmitted data remains protected by TLS/SSL encryption. HSTS is officially standardized by the IETF and documented in RFC 6797.
5.	Timestamp Disclosure - Unix (5)	Low	The application or web server exposed a timestamp value in Unix format, which may reveal information related to the server's system time and internal configuration.
6.	X-Content-Type-Options Header Missing (Systemic)	Low	The X-Content-Type-Options header was not configured with the value nosniff. As a result, older releases of browsers such as Internet Explorer and Chrome may attempt to determine the file type through MIME-sniffing instead of relying on the declared content type. This behavior can cause the browser to interpret and render content differently from its intended format. Meanwhile, both older and newer versions of Firefox generally follow the specified content type without applying MIME-sniffing techniques.
7.	Information Disclosure – Suspicious Comments (9)	Informational	The server response contains comments that may reveal unnecessary information and could potentially assist attackers in understanding the application structure or behavior.
8.	Modern Web Application (2)	Informational	The target appears to use a modern web application architecture. For automated exploration and testing, the Ajax Spider is likely to provide better coverage and effectiveness compared to the conventional crawling method.
9.	Re-examine Cache-Control Directives (2)	Informational	The Cache-Control header is either missing or not configured correctly, which may permit browsers and intermediary proxies to store cached copies of the content. While this behavior can be acceptable for static resources such as CSS, JavaScript, and image files, it is important to verify that no confidential or sensitive information is unintentionally cached.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

3.2.3 Vulnerability verification

Tahap ini diterapkan sebagai proses validasi kerentanan. Mengacu pada hasil pemindaian keamanan, teridentifikasi beberapa potensi celah yang terkait dengan konfigurasi keamanan pada sisi hosting dan kerentanan risiko tinggi, di antaranya:

Hasil pengujian menunjukkan tidak ditemukannya kerentanan risiko tinggi dan tidak diimplementasikannya beberapa header keamanan penting, yaitu Content-Security-Policy (CSP), X-Frame-Options (anti-clickjacking), dan X-Content-Type-Options (nosniff). Kondisi ini mengindikasikan keterbatasan kontrol pengelola website dalam menerapkan kebijakan keamanan pada level server, sehingga meningkatkan risiko serangan berbasis injeksi konten (misalnya XSS), manipulasi tampilan (*clickjacking*), dan *MIME sniffing*. Temuan ini dibuktikan melalui alert hasil pemindaian ZAP by Checkmarx dan dapat diperkuat dengan analisis header menggunakan layanan seperti https://securityheaders.com/. Temuan dapat dilihat pada Gambar 11.



Gambar 11 Bukti header HTTP MAN 2 Situbondo

3.2.4 Reporting

Setelah dilakukan pemindaian menggunakan ZAP by Checkmark, terdapat 9 risiko yang ditemukan. Dari hasil pemindaian tersebut, terdapat rekomendasi yang disusun sebagai langkah mitigasi risiko yang tampak pada Tabel 5.

Tabel 5. Rekomendasi Risk MAN 2 Situbondo

No	Alert	Risk	Rekomendasi
1.	Content Security Policy (CSP) Header Not Set (Systemic)	Medium	Make sure that the web server, application server, load balancer, and related infrastructure are properly configured to implement the Content-Security-Policy header.
2.	Missing Anti-clickjacking Header (2)	Medium	Current web browsers support the HTTP headers Content-Security-Policy and X-Frame-Options. Therefore, at least one of these security headers should be applied to every webpage delivered by the application or website.
3.	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (2)	Low	Ensure that the web server, application server, load balancer, and similar services are configured to hide or disable the X-Powered-By header.
4.	Strict-Transport-Security Header Not Set (Systemic)	Low	Verify that the web server, application server, load balancer, and other supporting systems are configured to enforce Strict-Transport-Security.
5.	Timestamp Disclosure - Unix (5)	Low	Conduct a manual verification process to confirm that the exposed timestamp information is not sensitive and cannot be analyzed to reveal exploitable patterns.
6.	X-Content-Type-Options Header Missing (Systemic)	Low	Ensure that the application or web server defines the Content-Type header correctly and applies the X-Content-Type-Options header with the value nosniff on all webpages.
7.	Information Disclosure – Suspicious Comments (9)	Informational	Delete any comments that may disclose useful information to attackers and resolve the security issues associated with those comments.
8.	Modern Web Application (2)	Informational	-

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.vxix.xxxx

9.	Re-examine Cache-Control Directives (2)	Informational	For sensitive or protected content, configure the Cache-Control HTTP header with the directives no-cache, no-store, must-revalidate.

Berdasarkan tahap vulnerability verification yang dilakukan sebagai verifikasi kerentanan yang diperoleh dari pemindaian ZAP serta pemeriksaan konsistensi melalui situs securityheaders.com, dapat disimpulkan bahwa website belum menerapkan penguatan keamanan pada tingkat konfigurasi server/hosting secara memadai. Selain itu, tidak ditemukan adanya kerentanan risiko tinggi pada website MAN 2 Situbondo.

Pembahasan ini merangkum dan membandingkan temuan dari kedua website secara kuantitatif. Pemindaian menggunakan ZAP by Checkmarx menghasilkan jumlah alert yang sama, yaitu 9 alert pada masing-masing website, namun dengan komposisi tingkat risiko yang berbeda. Pada website SMK At-Tamimi yang menggunakan hosting gratis InfinityFree, distribusi temuan terdiri atas 1 alert High (11,1%), 2 alert Medium (22,2%), 2 alert Low (22,2%), dan 4 alert Informational (44,4%). Sebaliknya, website MAN 2 Situbondo yang menggunakan hosting berbayar tidak memuat temuan berisiko High (0%), dengan 2 alert Medium (22,2%), 4 alert Low (44,4%), dan 3 alert Informational (33,3%). Perbedaan paling signifikan terletak pada keberadaan kategori High, yaitu indikasi Cloud Metadata Potentially Exposed, yang hanya muncul pada website dengan hosting gratis. Ringkasan perbandingan kedua website disajikan pada Tabel 6.

Tabel 6. Perbandingan Hasil Pengujian Kedua Website

Aspek Perbandingan	SMK At-Tamimi (InfinityFree)	MAN 2 Situbondo (Berbayar)
Jenis hosting	Gratis (shared, InfinityFree)	Berbayar (RumahWeb)
Total alert	9	9
Temuan High (%)	1 (11,1%) – Cloud Metadata Potentially Exposed	0 (0%)
Temuan Medium (%)	2 (22,2%)	2 (22,2%)
Temuan Low (%)	2 (22,2%)	4 (44,4%)
Temuan Informational (%)	4 (44,4%)	3 (33,3%)
Header keamanan HTTP	Belum diterapkan (CSP, HSTS, X-Frame-Options, X-Content-Type-Options)	Belum diterapkan (CSP, HSTS, X-Frame-Options, X-Content-Type-Options)
Kategori OWASP dominan	A05:2021 Security Misconfiguration	A05:2021 Security Misconfiguration
Tingkat keamanan relatif	Lebih rendah	Lebih tinggi

Berdasarkan Tabel 6, kedua website memiliki persamaan berupa tidak diterapkannya sejumlah header keamanan HTTP, yaitu Content-Security-Policy (CSP), Strict-Transport-Security (HSTS), X-Frame-Options, dan X-Content-Type-Options. Seluruh temuan tersebut tergolong dalam kategori A05:2021 Security Misconfiguration pada OWASP Top 10, yang berkaitan dengan konfigurasi keamanan yang belum optimal pada sisi server. Perbedaan utama terletak pada munculnya indikasi berisiko High pada website SMK At-Tamimi yang tidak ditemukan pada website pembanding. Temuan ini memperkuat dugaan bahwa keterbatasan kontrol konfigurasi pada lingkungan shared hosting gratis berkontribusi terhadap meningkatnya permukaan serangan (attack surface), khususnya pada aspek konfigurasi server yang tidak dapat diakses secara penuh oleh pengguna.

Temuan ini sejalan dengan penelitian pada website SMA Negeri 3 Berau [12] yang menyimpulkan bahwa mayoritas kerentanan website sekolah bersumber dari kesalahan konfigurasi dan ketiadaan header keamanan, bukan dari kegagalan fungsional aplikasi. Penelitian pada website SMK Muhammadiyah 2 Bontoala [13] juga melaporkan dominasi temuan kategori Security Misconfiguration. Namun, berbeda dengan kedua studi tersebut yang menguji satu website tanpa pembanding, penelitian ini menambahkan dimensi komparatif antarjenis hosting sehingga dapat menunjukkan bahwa perbedaan tingkat risiko tidak hanya ditentukan oleh kualitas pengelolaan, tetapi juga oleh keleluasaan kontrol konfigurasi yang disediakan oleh layanan hosting. Hal ini memperkuat posisi kebaruan penelitian sebagaimana dipaparkan pada bagian pendahuluan.

Secara praktis, hasil ini mengindikasikan bahwa pengelola website sekolah yang menggunakan hosting gratis perlu memberikan perhatian lebih pada penguatan konfigurasi yang masih berada dalam kendali pengguna, seperti pengaktifan HTTPS/SSL secara konsisten, penambahan header keamanan melalui berkas konfigurasi yang tersedia, serta pembaruan komponen aplikasi secara berkala. Selain itu, migrasi ke layanan

hosting berbayar dapat dipertimbangkan apabila sekolah membutuhkan keleluasaan konfigurasi keamanan yang lebih luas dan dukungan teknis yang lebih responsif.

4. KESIMPULAN

Berdasarkan hasil pengujian dan perbandingan pada Tabel 6, kedua website sama-sama menghasilkan 9 alert yang seluruhnya tergolong kategori A05:2021 Security Misconfiguration pada OWASP Top 10, dengan persamaan berupa tidak diterapkannya sejumlah header keamanan HTTP (CSP, HSTS, X-Frame-Options, dan X-Content-Type-Options). Perbedaan utama terletak pada komposisi tingkat risiko: website MAN 2 Situbondo (hosting berbayar RumahWeb) menempati tingkat keamanan tertinggi karena tidak memuat temuan berisiko High (0%), sedangkan website SMK At-Tamimi (hosting gratis InfinityFree) berada pada tingkat keamanan lebih rendah karena memuat 1 temuan High (11,1%) berupa indikasi Cloud Metadata Potentially Exposed yang muncul pada hasil pemindaian, namun tidak disertai bukti akses yang dapat divalidasi dalam batas pengujian non-destruktif sehingga diperlakukan sebagai indikasi awal. Perbedaan ini tidak semata-mata disebabkan oleh kualitas pengelolaan, tetapi juga oleh keterbatasan kontrol konfigurasi yang melekat pada lingkungan shared hosting gratis. Secara praktis, pengelola website sekolah disarankan menguatkan konfigurasi yang masih dalam kendali pengguna, seperti pengaktifan HTTPS/SSL yang konsisten, penambahan header keamanan, pembaruan komponen aplikasi secara berkala, serta evaluasi keamanan secara periodik, dan mempertimbangkan migrasi ke hosting berbayar bila membutuhkan keleluasaan konfigurasi yang lebih luas. Penelitian selanjutnya disarankan memperluas indikator evaluasi (konfigurasi TLS/HTTPS, keamanan cookie, dan isolasi shared hosting), memvalidasi temuan indikatif melalui lingkungan uji yang etis, serta menerapkan penilaian kuantitatif berbobot dengan sampel website sekolah yang lebih banyak agar kesimpulan komparatif lebih representatif.

REFERENSI

[1] F. Septian, M. H. Arfian, J. S. Asri, and B. Tjahjono, "Pengujian Keamanan Website dengan Metode Penetration Testing (Studi Kasus : Universitas Esa Unggul)," *J. Soc. Sci. Res. Vol.*, vol. 4, pp. 3629–3647, 2024.

[2] P. Kusuma, R. A. Pakkaja, and K. Kunci, "Analisis Vulnerability Assessment Menggunakan OWASP ZAP untuk Mengidentifikasi Celah Keamanan Website," *AICOM Artif. Intell. Comput.*, vol. 01, no. 04, pp. 115–123, 2026.

[3] S. Azizah *et al.*, "Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile : Studi literatur mengenai cybercrime dan mitigasinya kehidupan , aplikasi keuangan mobile telah menjadi salah satu inovasi terkemuka yang bisnis dalam mengakses dan mengelola keuangan s," vol. 17, no. April, pp. 221–237, 2024.

[4] A. S. R. Saepudin Hidayat, "KEMANDIRIAN SIBER INDONESIA : TANTANGAN DAN PELUANG MENUJU KEDAULATAN DIGITAL," *Int. J. Soc. Manag. Stud.*, vol. 6, no. 5, pp. 98–102, 2025.

[5] F. Widianto, E. S. Wijaya, A. P. Wicaksono, T. Informatika, F. Teknik, and U. M. Purwokerto, "Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES," *J. Pendidik. dan Teknol. Indones.*, vol. 5, no. 1, pp. 155–166, 2025.

[6] A. Fatihah and P. Dinarto, "Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ," *Innov. J. Soc. Sci. Res. Vol.*, vol. 4, no. 2, pp. 4536–4549, 2024.

[7] G. Arna and I. M. E. L. Saskara, "SECURITY TESTING WITH PENETRATION TESTING EXECUTION STANDARD (PTES) METHODS TO FIND MISCONFIGURATIONS VULNERABILITIES IN NETWORK DEVICES," *J. Elektro Luceat*, vol. 10, no. 2, 2024.

[8] A. Yahya, A. Wijaya, and W. E. Sary, "Pengembangan Strategi Digital Umkm Melalui Edukasi Pemanfaatan Website di Kedai Mbak Windah Bengkulu," vol. 5, no. 2, pp. 218–229, 2025.

[9] H. P. Fitrian, L. Abidah, K. W. Zahra, W. H. Hafidudin, T. Informatika, and U. T. Digital, "PENGARUH KESADARAN PENGGUNA TERHADAP KEBERHASILAN SERANGAN PHISHING DI JARINGAN PERBANKAN," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 2, pp. 1888–1892, 2025.

[10] M. Wahyu, A. Saputra, S. A. Ashari, and E. Larosa, "Keamanan Data Sistem Informasi Akademik ITEkes Mahardika : Penerapan Sistem Pencadangan Basis Data dengan Enkripsi AES," *Invert. J. Inf. Technol. Educ.*, vol. 4, no. 1, pp. 79–85, 2024.

[11] A. P. Armadhani, D. Nofriansyah, and K. Ibnutama, "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab Testing Menggunakan Penetration Testing Standart OWASP," vol. 21, no. 2, pp. 80–88, 2022.

[12] M. A. N. Nanda Hidayat, "ANALISIS CELAH KEAMANAN PADA WEBSITE SMA NEGERI 3

BERAU Abstraksi Keywords : Pendahuluan Tinjauan Pustaka Metode Penelitian," *J. Inf. Syst. Manag.*, vol. 6, no. 2, pp. 102–108, 2025.

[13] H. Pahlawansah, M. F. Basmar, and M. Yusuf, "Analisis Kerentanan Website SMK Muhammadiyah 2 Bontoala Makassar Menggunakan Metode OWASP (Open Web Application Security Project)," *BIOS J. Teknol. Inf. Dan Rekayasa Komput.*, vol. 6, no. 2, pp. 92–100, 2025.

[14] A. A. Zahrani, D. S. Alifah, Y. Cahyani, and I. Albana, "Analisis Vulnerability Assessment pada Sistem Informasi Website IITC Intermedia Universitas Amikom Purwokerto Menggunakan OWASP ZAP," *J. Publ. Sist. Inf. Dan Telekomun.*, vol. 3, no. 2, pp. 55–68, 2025.

[15] A. Wirasto and D. Mustofa, "ANALISIS KEAMANAN APLIKASI BERBASIS WEB DI UNIVERSITAS HARAPAN BANGSA MENGGUNAKAN PTES," *J. Inf. Interaktif*, vol. 8, no. 3, pp. 89–94, 2023.

[16] P. Satya, S. Kiran, and D. Valluri, "Web Application Security through Comprehensive Vulnerability Assessment," *Procedia Comput. Sci.*, vol. 230, no. 2023, pp. 168–182, 2024, doi: 10.1016/j.procs.2023.12.072.

[17] S. A. Nugroho and T. Rochmadi, "Analisis Keamanan Sistem Informasi Pusaka Magelang Menggunakan Open Web Application Security Project (OWASP) Dan Information Systems Security Assessment Framework (ISSAF) Security Analysis Of Magelang Pusaka Information System Using Open Web Applicati," *CyberSecurity dan Forensik Digit.*, vol. 7, no. 1, pp. 56–61, 2024.

[18] A. Y. Lestari and J. N. Utamajaya, "Audit Sistem Informasi Aplikasi Sirekap KPU : Analisis Keamanan dan Efisiensi," *J. Sains dan Teknol. Inf.*, vol. 2, no. 5, pp. 23–32, 2024.

[19] Y. Y. Pratama and I. Albana, "Analisis Risiko Keamanan Website Kompetisi Nasional Menggunakan Metode Vulnerability Assessment dan CVSS 4.0 Security Risk Analysis of National Competition Website Using Vulnerability Assessment Method and CVSS 4.0," *J. Electr. Electron. Mech. Inform. Soc. Appl. Sci.*, vol. 4, no. 2, pp. 12–28, 2025.

[20] A. D. Rahmawati, "Analisis Keamanan Jaringan Menggunakan Metode Penetration Testing Terstruktur," *J. Sist. Inf.*, vol. 1, no. 1, pp. 1–8, 2025.

[21] M. Tahir and M. Risky, "Analisis Keamanan Website Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard)," *J. Tek. Inform. Unika ST. Thomas*, vol. 09, no. 01, pp. 118–125, 2024.

[22] D. W. Febrian, R. B. Huwae, and A. Z. Mardiansyah, "Analisis Keamanan Website Perguruan Tinggi di Nusa Tenggara Barat terhadap Serangan SQL Injection , Cross-Site Scripting , dan Insecure Direct Object Reference melalui Pengujian Penetrasi Security Analysis of University Websites in West Nusa Tenggara," *J. Bumigora Inf. Technol.*, vol. 7, no. 1, pp. 25–38, 2025, doi: 10.30812/bite/v7i1.5032.

[23] F. A. Maylani, M. Tahir, N. N. Juniar, D. Sari, and W. A. Zulaica, "ANALISIS KEAMANAN WEBSITE E-LIBRARY KAMPUS DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 4, pp. 5643–5650, 2025.

[24] M. A. Mira Orisa, "VULNERABILITY ASSESSMENT UNTUK MENINGKATKAN KUALITAS KEMANAN WEB," *J. Mnemon.*, vol. 4, no. 1, pp. 16–19, 2021.

[25] I. N. B. I Kadek Ryan Jody Prayoga, Putu Wida Gunawan, "Analisis Keamanan Sistem Informasi Website Kampus Menggunakan Metode Penetration Test," *semanTIK*, vol. 11, no. 2, pp. 115–123, 2025.