Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 173-183
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Analisis Keamanan Website SMP Negeri 2 Bagan Sinembah Dengan Framework ISSAF

Elpi Aprianti Saragih[1], Rezki Kurniati[2], Nurmi Hidayasari[3]
[1] Keamanan Sistem Informasi, Politeknik Negeri Bengkalis
Email: [1]elpiaprianti@gmail.com, [2]rezki@polbeng.ac.id, [3]nurmihidayasari@polbeng.ac.id
Email Penulis Korespondensi: elpiaprianti@gmail.com

Article History:
Received Jun 15th, 2025
Revised Jun 30th, 2025
Accepted Jul 24th, 2025

Abstrak

Website SMP Negeri 2 Bagan Sinembah digunakan sebagai sarana penyampaian informasi sekolah dan pendaftaran siswa baru secara daring. Namun, hingga saat ini belum pernah dilakukan pengujian keamanan terhadap situs tersebut. Oleh karena itu, penelitian ini bertujuan untuk menganalisis potensi kerentanan yang dimiliki *website* sekolah menggunakan pendekatan kerangka kerja *Information System Security Assessment Framework (ISSAF)*. Penelitian dilakukan melalui beberapa tahapan, mulai dari perencanaan, pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, pengujian penetrasi, hingga rekomendasi perbaikan. Berbagai alat bantu digunakan untuk mendeteksi celah keamanan, seperti *Whois Lookup, Nmap, Nikto, dan SlowHTTPTest*. Hasil dari pengujian menunjukkan adanya beberapa kelemahan pada sisi keamanan, antara lain tidak adanya pengaturan header keamanan, penggunaan PHP versi lama, serta potensi serangan *Denial of Service*. Temuan ini diharapkan dapat menjadi masukan bagi pihak sekolah dalam meningkatkan keamanan sistem informasi mereka secara berkelanjutan.

Kata Kunci : Keamanan *Website, ISSAF, Penetration Testing*

Abstract

The website of SMP Negeri 2 Bagan Sinembah is used as a platform for delivering school information and facilitating new student registration online. However, no security assessment has been conducted on the site to date. Therefore, this study aims to analyze potential vulnerabilities in the school's website using the Information System Security Assessment Framework (ISSAF) approach. The research follows several stages, including planning, information gathering, network mapping, vulnerability identification, penetration testing, and the formulation of improvement recommendations. Various tools were employed to detect security flaws, such as Whois Lookup, Nmap, Nikto, and SlowHTTPTest. The assessment results revealed several security weaknesses, including the absence of proper security headers, the use of an outdated PHP version, and the risk of Denial of Service (DoS) attacks. These findings are expected to provide valuable input for the school in sustainably strengthening the security of its information system.

Keyword : *Website security, ISSAF, Penetration Testing*

1. PENDAHULUAN

Keamanan *website* merupakan hal yang sangat penting diera digital seperti sekarang ini. Seiring dengan meningkatnya jumlah data yang ditukar melalui internet, setiap organisasi maupun perusahaan perlu menjaga kerahasiaan, integritas, dan otentikasi data pada *website* mereka sesuai dengan standar keamanan yang berlaku. Hal ini disebabkan oleh tingginya ketergantungan masyarakat terhadap *website*, sehingga keamanan dari sistem tersebut harus terus dievaluasi dan di tingkatkan dari waktu ke waktu [1].

Kurangnya perhatian terhadap keamanan *website* bisa memberikan dampak yang merugikan bagi pemiliknya. Tanpa sistem keamanan yang memadai, peretas dapat dengan mudah mengambil alih kendali sistem yang sudah dibangun. Kondisi ini bisa menyebabkan kebocoran data-data pribadi atau informasi penting milik lembaga atau organisasi, yang seharusnya tidak diakses oleh pihak yang tidak bertanggung jawab. Tanpa perlindungan keamanan yang kuat, data sensitif tersebut sangat rentan dibobol oleh hacker [2].

Ancaman pada sistem biasanya muncul karena kesalahan saat merancang atau mengembangkan sistem. Pihak-pihak yang tidak bertanggung jawab bisa saja memanfaatkan celah tersebut untuk melakukan serangan seperti *defacing, phishing, denial of service, brute force attack*, dan serangan lainnya [3].

Perubahan yang sangat cepat, kadang meluputkan developer dalam melakukan pengujian keamanan terhadap aplikasi yang dibangun. Pengujian merupakan proses yang sangat penting didalam pengembangan perangkat lunak yang

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 173-183
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

berkualitas tinggi, karena dari beberapa kesalahan yang dianggap tidak penting beresiko sangat berbahaya hal ini menjadi celah bagi *attacker* untuk memanfaatkan informasi yang dicuri melalui serangan kepada sistem [4].

Kemajuan teknologi yang sangat cepat juga membuat pengembang terkadang lupa atau melewatkan proses pengujian keamanan terhadap aplikasi yang mereka buat. Padahal pengujian merupakan bagian penting dalam pengembangan perangkat lunak yang berkualitas. Kesalahan kecil yang dianggap sepele bisa saja menjadi celah besar yang dimanfaatkan oleh *attacker* untuk melakukan pencurian atau penyalahgunaan data [5].

Penelitian ini dilakukan pada *website* SMP Negeri 2 Bagan Sinembah yang beralamat di *https://smpn2bagansinembah.sch.id/*. *Website* ini menyediakan layanan informasi sekolah dan pendaftaran siswa baru secara *online*, namun belum pernah diuji keamanannya. Oleh karena itu, penelitian ini akan menggunakan *framework ISSAF (Information System Security Assessment Framework)* yang bertujuan untuk menilai dan meningkatkan keamanan *website*. *ISSAF* memiliki lima tahapan, yaitu *planning, assessment, treatment, accreditation,* dan *maintenance*. Setelah di temukan adanya kerentanan, maka dilakukan *assessment* untuk mengetahui apakah celah tersebut bisa dieksploitasi atau tidak. Selanjutnya diberikan solusi pada tahap treatment dan di lanjutkan ke tahap *maintenance* untuk memastikan sistem tetap aman.

Alasan penelitian ini dilakukan karena *website* SMP Negeri 2 Bagan Sinembah belum pernah di analisis keamanannya, padahal digunakan untuk layanan pendaftaran siswa secara *online*. Kondisi ini bisa menjadi peluang bagi pihak yang tidak bertanggung jawab untuk menyusup dan memanfaatkan kelemahan sistem. Jika tidak segera diatasi, masalah ini bisa merusak reputasi sekolah dan mengganggu proses operasional, terutama yang berkaitan dengan akses pengguna.

Penelitian sebelumnya yang relevan pernah dilakukan dengan judul "Analisis Keamanan *Website* SMA Negeri 2 Sumbawa Besar Menggunakan Metode *Penetration Testing (Pentest)*". Dalam penelitian ini, *website* sekolah dinilai lemah keamanannya dan sangat rentan terhadap serangan. Penelitian ini menggunakan metode pentest dengan tahapan *footprinting, scanning, fingerprinting, exploit*, dan *reporting*, serta menggunakan *OWASP ZAP*. Hasilnya, ditemukan 13 kerentanan dengan tingkat risiko *low* dan medium, dan diberikan solusi untuk meningkatkan keamanannya [6].

Penelitian lainnya dilakukan dengan judul "Analisis Keamanan *Open Website* Menggunakan Metode *OWASP* dan *ISSAF*". Penelitian ini membahas masalah keamanan *website* Diskominfo Kerinci. Dalam penelitian ini digunakan metode *OWASP* dan *ISSAF* dan di temukan beberapa celah keamanan seperti *XSS* dan *SQL injection*. Solusi kemudian di berikan dan hasilnya menunjukkan risiko bisa di turunkan dari *HIGH* menjadi *LOW* [7].

Selanjutnya, penelitian berjudul "Analisis Celah Keamanan Pada *Website* Dengan Menggunakan Metode *Penetration Testing* Dan *Framework ISSAF* Pada *Website* SMK Al-Kautsar". Penelitian ini menjelaskan bahwa *website* SMK Al-Kautsar memiliki beberapa celah seperti *SQL injection, clickjacking, brute force*, dan *XSS*. Penelitian menggunakan *framework ISSAF* dengan tiga tahap: *planning and preparation, assessment,* dan *reporting*. Hasilnya menunjukkan bahwa *website* rentan terhadap serangan *DoS*, tapi aman dari *XSS* dan serangan *port* terbuka [8].

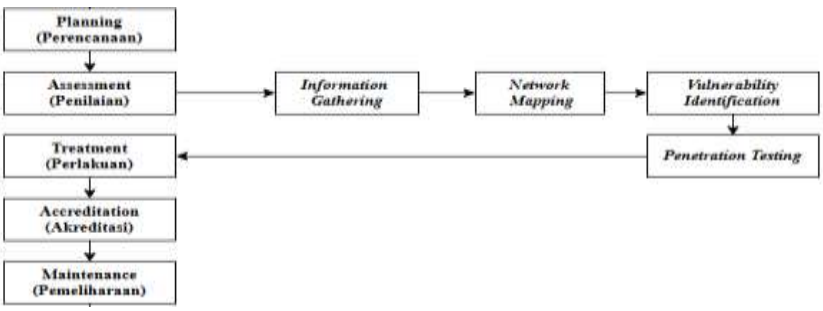
Penelitian lain berjudul "Analisis Metode OWASP (Open Web Application Security Project) Menggunakan Penetration Testing pada Keamanan Website Absensi" menyebutkan bahwa teknologi web juga memiliki potensi kerentanan yang dapat merugikan infrastruktur organisasi. Oleh karena itu, dilakukan analisis dengan metode OWASP dan penetration testing untuk mengetahui kelemahan website dan memberikan solusi [9].

Penelitian "*Company Profile Website Security Analysis Using ISSAF Method*" menyoroti masalah celah keamanan pada *website* Sanggar Tari Didik Nini Thowok. ISSAF digunakan dalam penelitian ini dengan alat bantu Kali Linux, Nmap, dan Zenmap. Selain itu, algoritma Naive Bayes digunakan untuk perhitungan akurasi. Hasilnya menunjukkan keamanan *website* masih lemah dengan akurasi hanya 54,16% [10].

Penelitian terakhir berjudul "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetrasi Test Dan *ISSAF*" bertujuan untuk menganalisis keamanan jaringan di MTsN 8 Bantul. Penelitian menggunakan *framework ISSAF* dan alat bantu seperti Kali Linux, Nmap, dan Wireshark. Hasilnya menunjukkan bahwa keamanan jaringan cukup baik dengan akurasi 72,72% [11].

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian



Gambar 1. Tahapan Penelitian

2.1.1 *Planning*

Perencanaan dalam penelitian ini mencakup penentuan target, yaitu memilih *website* yang akan diteliti dengan persetujuan dari pemiliknya. Dalam hal ini, penulis telah menetapkan target penelitian yaitu pada *website* SMP Negeri 2 Bagan Sinembah dengan alamat situs *https://smpn2bagansinembah.sch.id/* dan telah memperoleh persetujuan resmi dari pihak sekolah dalam bentuk surat. Penelitian ini bertujuan untuk membantu pihak sekolah menganalisis kerentanan pada *website* serta memberikan solusi perbaikan yang dapat diterapkan.

2.1.2 *Assessmen*

Dalam *assessment* ini penulis melakukan analisis keamanan dengan menemukan kerentanan yang ditemukan pada *website* sekolah. Proses ini mencakup beberapa langkah, yaitu: *Information Gathering, Network Mapping, Vulnerability Identification*, dan *Penetration Testing*:

a. *Information Gathering*

Dalam *information gathering* ini menggunakan *tools* seperti *Whois lookup, Securitytrails* dan *Wappalyzer:*

1. *Whois lookup*

Tahapan ini dilakukan untuk mengumpulkan informasi domain seperti pemilik domain, tanggal pendaftaran, registrar, dan status domain. *Tools* ini berguna untuk mengetahui siapa yang memiliki domain, serta kapan domain didaftarkan atau di perbarui. Untuk mengetahui informasi domain pada di *website* sekolah, gunakan *tools whois lookup* dengan mengakses *https://whois.domaintools.com/* di peramban.

2. *SecurityTrails*

Tahapan ini dilakukan untuk mengumpulkan informasi subdomain alamat IP, status DNS, dan lainnya. Untuk mengetahui informasi subdomain pada *website* sekolah, gunakan *tools securitytrails* dengan mengakses situs *https://securitytrails.com/* di peramban.

3. *Wappalyzer*

Tahapan ini dilakukan menggunakan *tools* wappalyzer untuk mendeteksi teknologi yang digunakan terlebih dahulu unduh wappalyzer ekstensi browser, lalu pasang dan buka alamat situs sekolah. Klik ikon *wappalyzer* di bilah ekstensi untuk melihat teknologi yang digunakan pada *website framework*.

4. *Network Mapping*

Tahapan ini melakukan *scanning* kerentanan dengan *tools Nmap* yang ada di Kali Linux dengan mengetikkan IP *website* sekolah dengan perintah "nmap -sV 198.252.100.221", setelah itu akan mendapatkan layanan apa yang berjalan, dan *port* mana yang terbuka

5. *Vulnerability Identification*

Tahapan ini melakukan *scanning* untuk mencari kerentanan keamanan dengan *tools* Nikto yang ada di Kali Linux dengan mengetikkan perintah "nikto -h *https://smpn2bagansinembah.sch.id/"*, setelah itu akan mendapatkan kerentanan

6. Pengujian penetrasi

Penetration *testing* merupakan pengujian kerentanan keamanan untuk mendapatkan sebuah akses dalam sistem atau *website* yang berisi simulasi metode seolah-olah penyerang akan menerobos mekanisme keamanan sistem yang dituju untuk mendapatkan akses secara ilegal [12].

2.1.3 *Treatment*

Tahap *treatment* dalam penelitian ini dilakukan dengan menganalisis hasil assessment secara menyeluruh. Setelah mengidentifikasi berbagai kerentanan, langkah selanjutnya adalah menerapkan solusi perbaikan yang sesuai. Diharapkan, dengan adanya perbaikan ini, keamanan *website* sekolah dapat lebih terjaga dan terlindungi dari potensi ancaman.

2.1.4 *Accreditation*

Akreditasi dalam penelitian ini adalah melakukan evaluasi keamanan *website* sekolah menggunakan *tools* SSL Labs untuk memastikan bahwa semua kriteria keamanan telah terpenuhi. *Tools* ini menganalisis konfigurasi SSL/TLS, sertifikat untuk memberikan penilaian menyeluruh terhadap keamanan *website* sekolah.

2.1.5 *Maintenance*

Tahap *maintenance* dalam penelitian ini bertujuan menjaga keamanan *website* sekolah melalui pemeliharaan rutin. Proses ini mencakup pemantauan sistem secara berkala untuk mendeteksi dan mencegah potensi ancaman, memastikan *website* tetap aman dan selalu diperbarui.

3. HASIL DAN PEMBAHASAN

Hasil dan pembahsan merupakan bagian yang menyajikan hasil dari pengujian yang telah di lakukan dalam penelitian. Bagian ini berisi dokumentasi temuan berdasarkan *Framework ISSAF*.

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 173-183
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3.1 Hasil *Assessment*

a. *Information gathering*

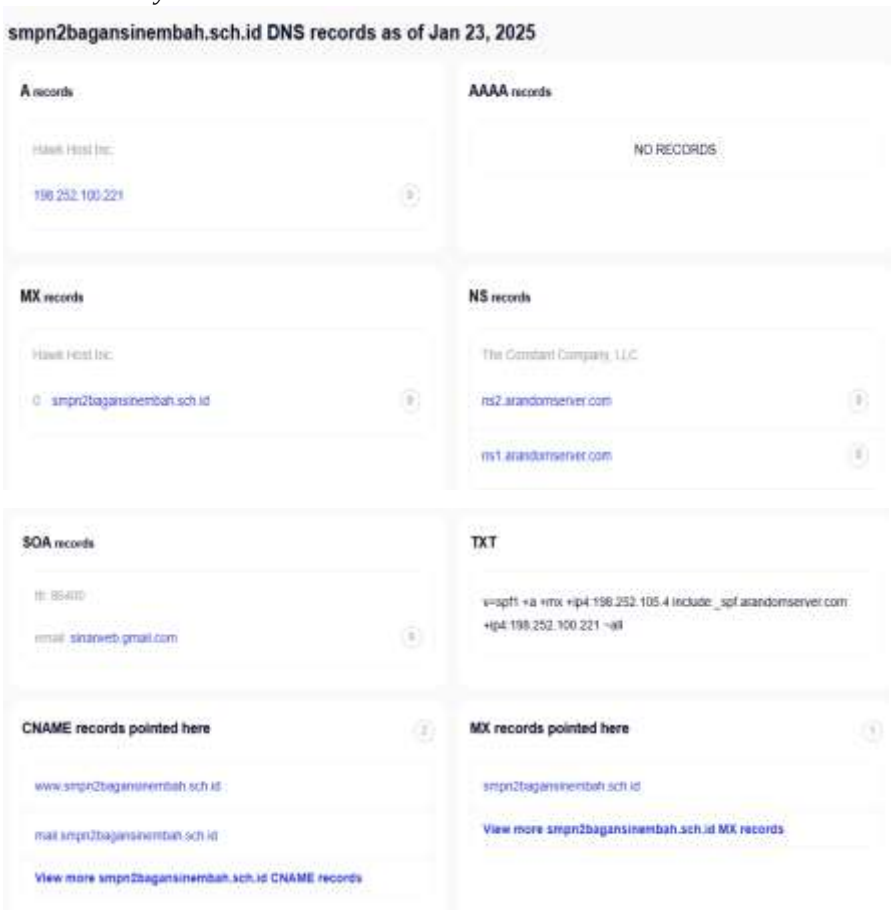
Tahapan ini memberikan hasil informasi menggunakan *tools* seperti *Whois Lookup*, *Securitytrails* dan *wappalyzer*.

1. Hasil *Tools Whois Lookup*

```
ID ccTLD whois server
Please see 'whois -h whois.id help' for usage.

Domain ID: PANDI-DO1773946
Domain Name: smpn2bagansinembah.sch.id
Created On: 2019-12-04 01:57:25
Last Updated On: 2024-12-10 01:35:04
Expiration Date: 2025-12-04 23:59:59
Status: clientTransferProhibited
Status: autoRenewPeriod

==================================================
Sponsoring Registrar Organization: PT JC Indonesia
Sponsoring Registrar URL: https://resellercamp.id
Sponsoring Registrar Street: Perintis Kemerdekaan 33
Sponsoring Registrar City: Yogyakarta
Sponsoring Registrar State/Province: DIY
Sponsoring Registrar Postal Code: 55161
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 082141570000
Sponsoring Registrar Email: sales@resellercamp.id
Name Server: ns5.sinarweb.com
Name Server: ns6.sinarweb.com
DNSSEC: Unsigned

Abuse Domain Report https://pandi.id/domain-abuse-form/?lang=en
For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes


Information Updated: 2024-12-18 18:00:06
```

Gambar 2. Hasil Scan Whois

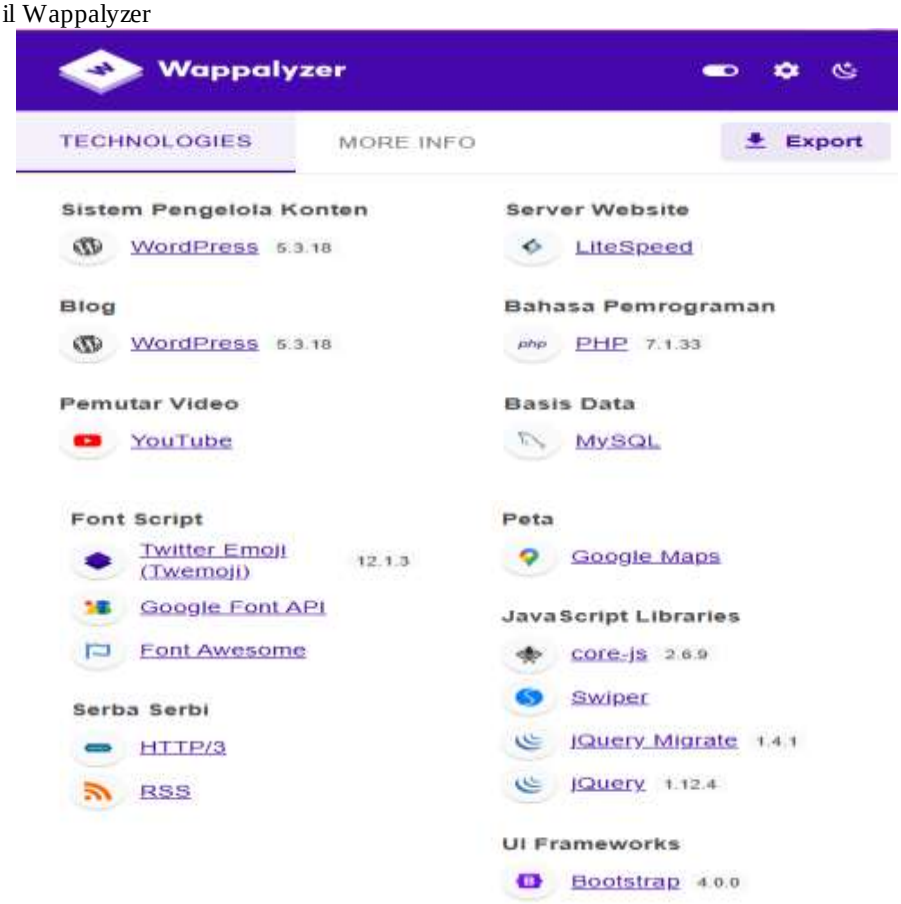
2. Hasil *Tools SecurityTrails*



Gambar 3. Hasil Scan *Securitytrails*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 173-183
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3. Hasil Wappalyzer



Gambar 4. Hasil *Wappalyzer*

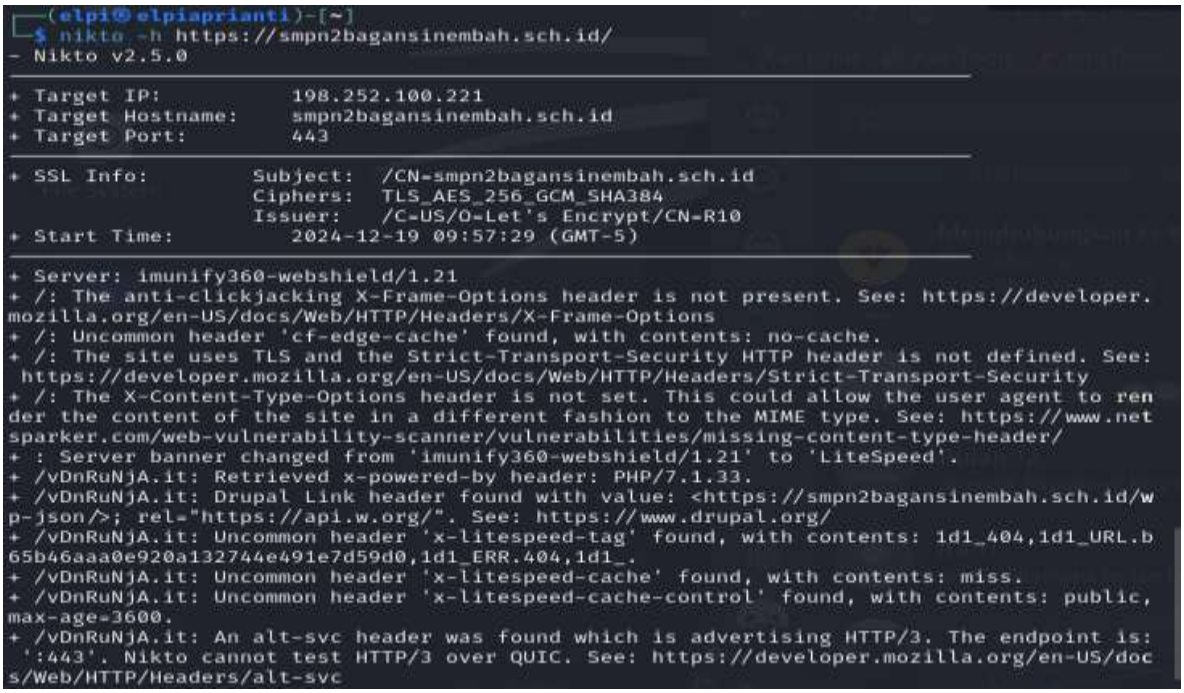
b. *Network Mapping*

```
┌──(elpi㉿elpiaprianti)-[~]
└─$ nmap -sV 198.252.100.221
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-13 13:40 EST
Nmap scan report for smpn2bagansinembah.sch.id (198.252.100.221)
Host is up (0.0069s latency).
Not shown: 969 filtered tcp ports (no-response)
PORT      STATE  SERVICE         VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp             Pure-FTPd
22/tcp    open   ssh             OpenSSH 7.4 (protocol 2.0)
25/tcp    open   smtp            Exim smtpd 4.96.2
26/tcp    open   smtp            Exim smtpd 4.96.2
53/tcp    open   domain          PowerDNS Authoritative Server 4.9.1
80/tcp    open   http            LiteSpeed
110/tcp   open   pop3            Dovecot pop3d
143/tcp   open   imap            Dovecot imapd
443/tcp   open   ssl/https       LiteSpeed
587/tcp   open   smtp            Exim smtpd 4.96.2
993/tcp   open   ssl/imap        Dovecot imapd
995/tcp   open   ssl/pop3        Dovecot pop3d
```

Gambar 5. Hasil *Scanning Tools Nmap*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 173-183
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

c. *Vulnerability Identification*



Gambar 6. Hasil *Scanning Tools Nikto*

d. Hasil *Penetration Testing*

1. Serangan *Slow HTTP DoS (Denial of Service)*

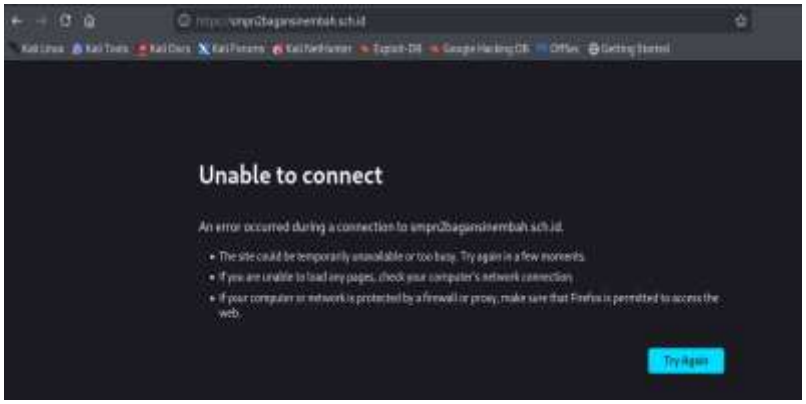
Gambar 7. Menjelaskan bawah serangan *DoS* dengan *tools SlowHTTPTest* menghasilkan bahwa web menjadi tidak responsif akibat serangan. Serangan ini menggunakan metode *Slow Headers* berhasil. Hal ini terlihat dari tingginya jumlah koneksi yang berada dalam status "pending," yang menunjukkan bahwa web tidak dapat memproses semua permintaan yang masuk. Selain itu, status layanan yang tercatat sebagai "layanan tersedia: *NO*" juga menjelaskan bahwa layanan tidak dapat diakses, yang menandakan bahwa server kesulitan dalam menangani beban yang diterimanya.

slowhttptest -c 10000 -H -g -o slowhttp -1 10 -ɛ 200 t GET -u https://198.252.100.221 -p 3

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 173-183
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Gambar 7. Pengujian serangan *Slow HTTP DoS (Denial of Service)*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 173-183
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

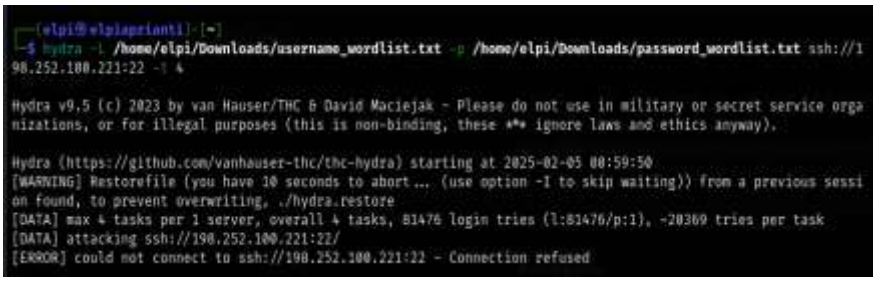


Gambar 8. Hasil web dari serangan *Slow HTTP DoS (Denial of Service)*

Gambar 8. menjelaskan setelah melakukan serangan *Slow HTTP DoS (Denial of Service) website* sekolah mengalami penurunan kinerja situs *website* , memperlambat respon terhadap pengguna. Akhirnya, *website* sekolah menjadi tidak dapat diakses dengan pesan "*Unable to connect*,".

2. Serangan *SSH Brute Force* dengan *Hydra*

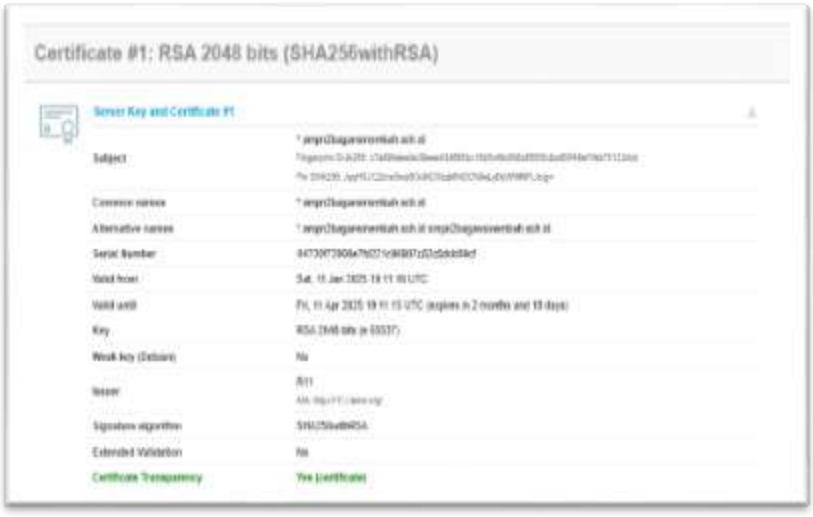
Penulis pada penelitian ini melakukan serangan *Hydra* dengan *tools brute-force* yang digunakan untuk mencoba berbagai kombinasi *username* dan *password* secara otomatis sampai menemukan yang benar. Hasilnya menunjukkan bahwa koneksi ke alamat IP yang di targetkan ditolak, yang berarti server tidak mengizinkan koneksi pada *port* yang di uji seperti pada Gambar 9.



Gambar 9. Hasil *SSH Brute Force* dengan *Hydra*

3.2 Hasil *Accreditation*

Dalam akreditasi ini, penulis melakukan pemeriksaan keamanan menggunakan SSL Labs. Dengan *tools* ini, kita dapat mengetahui validitas sertifikat SSL, tingkat keamanan sistem enkripsi yang di terapkan, serta mendeteksi potensi masalah keamanan, seperti penggunaan protokol lama atau pengaturan yang tidak optimal.



Gambar 10. *Certificate SSL Labs*

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 2 ; Juli 2025 ; Page 173-183
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Gambar 10. menampilkan hasil analisis dari pemeriksaan keamanan, seperti di tunjukkan pada, menampilkan detail sertifikat yang mengonfirmasi bahwa situs menggunakan kunci RSA dengan panjang 2048 bit dan algoritma tanda tangan SHA-256. Informasi ini mencakup subjek sertifikat, termasuk nama domain serta tanggal kedaluwarsa sertifikat. Selain itu, sertifikat tersebut memiliki validasi yang menunjukkan bahwa situs telah melalui proses verifikasi yang lebih ketat, memberikan lapisan tambahan kepercayaan bagi pengguna. Hal ini penting untuk memastikan bahwa koneksi antara pengguna dan situs tetap aman.

Gambar 11. Hasil *SSL Labs*

Gambar 11. menampilkan hasil bahwa situs memperoleh peringkat keseluruhan "A", yang mencerminkan konfigurasi SSL/TLS yang sangat baik. Peringkat ini di dukung oleh berbagai faktor, termasuk dukungan untuk protokol terbaru, keamanan dalam pertukaran kunci, dan kekuatan cipher yang di gunakan. Informasi tambahan menyatakan bahwa situs hanya berfungsi di browser yang mendukung SNI (*Server Name Indication*) serta menegaskan bahwa server mendukung TLS 3.10, yang merupakan versi protokol paling aman.

3.3 Hasil *Maintenance*

Hasil *maintenance* dalam penelitian ini untuk pemeliharaan web sekolah, penulis tidak diberikan hak untuk melakukan perbaikan secara langsung. Hal ini disebabkan karena pihak sekolah tidak memberikan akses *source code*, sehingga penulis hanya dapat menerapkan perbaikan pada *website*. Pemantauan atau pencatatan *(log)* aktivitas sistem hanya dapat dilakukan oleh pengembang *(developer)* dari pihak sekolah.

3.4 Hasil *Treatment*

Memberikan solusi perbaikan setelah dilakukan pengujian telah di lakukan pada tahap sebelumnya.

Tabel 1. Solusi Perbaikan

No	Jenis Kerentanan	Solusi Perbaikan
1	Perpustakaan JS yang rentan	*Upgrade* ke versi terbaru dari bootstrap
2	*Header* Kebijakan Keamanan Konten *(CSP)* Tidak Di tetapkan	Pastikan semua komponen yang menangani *HTTP response* di konfigurasi dengan *header CSP* yang sesuai
3	*HTTP* ke *Transisi Insecure HTTPS* dalam *Form Posting*	Gunakan *HTTPS* untuk halaman arahan yang meng - *host* formulir yang aman.
4	*Header Anti-clickjacking* yang Hilang	Solusi untuk kerentanan ini adalah menggunakan *header HTTP* yang tepat untuk mencegah situs web di muat di dalam *frame* atau *iframe*

5	Tidak adanya Token Anti-*CSRF*	Untuk mencegah serangan *Cross-Site Request Forgery (CSRF)* dan *Cross-Site Scripting (XSS)*, perlu diterapkan token anti-*CSRF* yang unik pada setiap permintaan yang memodifikasi data, serta validasi input yang ketat, teknik input *encoding*, dan menghindari eksekusi JavaScript yang tidak aman guna mencegah pencurian token dan penyalahgunaan akses.
6	*Cookie* tanpa bendera aman *(Secure flag)*	Solusi untuk kerentanan ini adalah selalu memastikan bahwa cookie yang berisi informasi sensitif misalnya, sesi pengguna di lindungi hanya di kirimkan melalui HTTPS.
7	*Cookie* Tidak Memiliki Bendera *HttpOnly*	Pastikan bahwa *HttpOnly* di tetapkan untuk semua *cookie* yang berisi informasi sensitif. Ini memastikan bahwa *cookie* hanya dapat di akses melalui *HTTP(S) request*, bukan melalui *JavaScript* di *browser*.

4. KESIMPULAN

Berdasarkan hasil penelitian terhadap keamanan *website* SMPN 2 Bagan Sinembah, bahwa terdapat kerentanan keamanan terhadap serangan *Slow HTTP DoS (Denial of Service)* juga menjadi perhatian utama, mengingat serangan ini dapat menyebabkan layanan yang terganggu dan merugikan pengguna.

UCAPAN TERIMA KASIH

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga jurnal ini dapat disusun dan diselesaikan dengan baik. Ucapan terima kasih yang sebesar-besarnya kami sampaikan kepada dosen pembimbing, Ibu Rezki Kurniati, M.Kom., dan Ibu Nurmi Hidayasari, S.T., M.Kom., atas bimbingan, arahan, serta dukungan yang telah diberikan selama proses penelitian.

DAFTAR PUSTAKA

[1] F. Fachri, A. Fadlil, I. Riadi, A. Dahlan, Y. Jln Soepomo, and I. Artikel, "Analisis Keamanan Webserver Menggunakan Penetration Test," *JURNAL INFORMATIKA*, vol. 8, no. 2, 2021, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/ji

[2] I. Riadi, A. Yudhana, and P. Korspondensi, "ANALISIS KEAMANAN WEBSITE OPEN JOURNAL SYSTEM MENGGUNAKAN METODE VULNERABILITY ASSESSMENT," vol. 7, no. 4, 2020, doi: 10.25126/jtiik.202071928.

[3] B. Harahap, "Penerapan Keamanan Owasp Terhadap Aplikasi GTFW Pada Website Universitas Battuta," *Jurnal Informatika dan Teknologi Pendidikan*, vol. 1, no. 2, pp. 80–86, Dec. 2021, doi: 10.25008/jitp.v1i2.15.

[4] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," *Jurnal Informasi dan Teknologi*, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.

[5] 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, Dec. 2020, doi: 10.32722/multinetics.v6i2.3432.

[6] Y. Mulyanto, M. T. A. Zaen, Y. Yuliadi, and S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," *Journal of Information System Research (JOSH)*, vol. 4, no. 1, pp. 202–209, Oct. 2022, doi: 10.47065/josh.v4i1.2335.

[7] R. Ashar, "Jurnal Informasi dan Teknologi Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF," vol. 4, no. 4, 2022, doi: 10.37034/jsisfotek.v4i4.233.

[8] S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," 2023.

[9] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *Jurnal Informasi dan Teknologi*, Oct. 2022, doi: 10.37034/jidt.v4i3.236.

[10] M. Nur, K. Al Mubaroq, E. P. Silmina, and A. Firdonsyah, "Company profile website security analysis using issaf method," 2024.

[11] E. P. Silmina, A. Firdonsyah, and R. A. A. Amanda, "ANALISIS KEAMANAN JARINGAN SISTEM INFORMASI SEKOLAH MENGGUNAKAN PENETRATION TEST DAN ISSAF," *Transmisi*, vol. 24, no. 3, pp. 83–91, Aug. 2022, doi: 10.14710/transmisi.24.3.83-91.

[12] L. F. Burhani and D. Priyawati, "ANALISIS PENGUJIAN KEAMANAN WEBSITE PENGELOLAAN INTERNET DESA KRAGAN MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 1, pp. 307–319, Feb. 2024, doi: 10.29100/jipi.v9i1.4455.