Journal of Applied Informatics and Computing (JAIC)
Vol.9, No.2, April 2025, pp. 404~411
e-ISSN: 2548-6861

Enhancing Website Security Using Vulnerability Assessment and Penetration Testing (VAPT) Based on OWASP Top Ten

Diana Rohmaniah [1]*, Wahid Miftahul Ashari [2], Lukman [3]***, Andriyan Dwi Putra [4]*****
* Informatika, Universitas Amikom Yogyakarta
** Teknik Komputer, Universitas Amikom Yogyakarta
*** Manajemen Informatika, Universitas Amikom Yogyakarta
**** Sistem Informasi, Universitas Amikom Yogyakarta
dianar@students.amikom.ac.id [1], wahidashari@amikom.ac.id [2], masman@amikom.ac.id [3], andriyan@amikom.ac.id [4]

Article Info

Article history:

Received 2025-01-09
Revised 2025-01-17
Accepted 2025-01-21

Keyword:

Website Security,
Vulnerability Assessment,
Penetration Testing,
OWASP Top Ten.

ABSTRACT

Website security is one of the main concerns in the digital era, given the increasing potential for cyber threats. This research aims to improve website security by using the Vulnerability Assessment and Penetration Testing (VAPT) method that refers to the OWASP Top Ten standard. The applied method includes four main stages: information gathering, vulnerability scanning, exploitation, and reporting. The results showed that there were several successfully exploited vulnerabilities, such as Clickjacking, Improper HTTP to HTTPS Redirection, Directory Listing, and Sensitive Information Disclosure, which were classified based on the OWASP Top Ten. The severity of the vulnerabilities was analyzed using Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), and Common Vulnerability Scoring System (CVSS). The analysis results show that some vulnerabilities have high severity after considering the factual conditions of the system. This research provides specific remediation recommendations to address these vulnerabilities, such as the implementation of security headers, deletion of sensitive configuration files, and dependency updates. With this approach, the research is expected to contribute to improving website security and provide effective mitigation guidelines.

I. PENDAHULUAN

Pada internet di era digital ini, keamanan dan kerahasiaan data menjadi aspek penting yang perlu diperhatikan oleh pengembang website, mengingat banyaknya layanan yang disediakan website seperti sosial media, e-commerce, dan lain-lain [1]. Website merupakan media yang tersedia di internet, yang menyediakan layanan akses data dan informasi bersifat publik termasuk organisasi nirlaba dan lembaga pemerintahan [2]. Meskipun demikian, ancaman keamanan pun semakin meningkat dan menimbulkan dampak serangan siber baik serangan yang menargetkan individu, perusahaan, dan bahkan negara [3]. Kelemahan keamanan dapat tercipta karena pengembang website menggunakan modul atau komponen pihak ketiga yang disebabkan oleh keterbatasan anggaran [4]. Terdapat banyak kasus kehilangan dan kerusakan data yang disebabkan oleh kejahatan siber yang dapat menyerang siapa pun tanpa terkecuali. Menurut data lanskap keamanan siber dari Badan Siber dan Sandi Negara tahun 2023, jumlah serangan yang terjadi selama bulan Januari – Desember 2023 adalah sebanyak 403.990.813, traffic tertinggi jumlah serangan terjadi pada bulan Agustus sebanyak 78.464.385 serangan, seperti terlihat pada Gambar 1. Hal ini menunjukkan masih lemahnya perlindungan keamanan data di Indonesia [5].

Salah satu metode yang diterapkan untuk meningkatkan keamanan website adalah dengan menggunakan metode Vulnerability Assessment and Penetration Testing (VAPT). Metode ini merupakan pendekatan yang digunakan untuk pengujian dan identifikasi kerentanan dengan dua fase utama, yaitu penilaian keamanan dan uji penetrasi. VAPT berperan penting dalam membantu organisasi meningkatkan sistem

keamanan dan mengurangi risiko serangan [6]. Penilaian kerentanan bertujuan untuk mendiagnosis dan mengakumulasikan kerentanan yang terdeteksi, sedangkan pengujian penetrasi bertugas memilih dan menerapkan teknik yang tepat untuk masuk ke dalam sistem dan mencapai jalan masuk yang tidak disetujui oleh sistem [7]. Hasil dari proses pengujian kerentanan ini akan dianalisis dan dikategorikan berdasarkan standar OWASP Top Ten, yang merupakan sepuluh daftar kerentanan paling umum terjadi dan paling serius ditemukan di aplikasi web saat ini [8]. Open Web Application Security Project (OWASP) merupakan sebuah organisasi nirlaba berbasis komunitas yang berfokus pada keamanan perangkat lunak melalui media edukasi, software open-source, dan berbagai inisiatif lain [9]. Selain mengategorikan kerentanan besrdasarkan standar OWASP Top Ten, kerentanan yang ditemukan akan diklasifikasikan berdasarkan Common Vulnerability and Exposure (CVE) dan Common Weakness Enumeration (CWE) guna memberikan informasi lebih terstruktur. Penelitian ini tidak hanya berfokus pada identifikasi kerentanan tetapi juga mengevaluasi tingkat keparahan kerentanan berdasarkan kondisi faktual menggunakan Common Vulnerability Scoring System (CVSS). Langkah ini memberikan analisis risiko yang lebih relevan dengan lingkungan operasional website. Hasil analisis ini akan dilengkapi dengan rekomendasi perbaikan spesifik yang dirancang untuk setiap kerentanan guna meningkatkan keamanan sistem secara menyeluruh.

Gambar 1. Grafik serangan siber di Indonesia tahun 2023

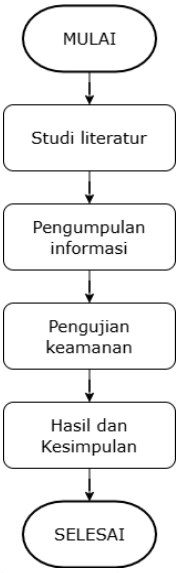
Penelitian terkait analisis keamanan website sudah dilakukan oleh beberapa peneliti, seperti pada penelitian yang berjudul Analisis Keamanan Website Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework. Penelitian ini bertujuan untuk menganalisis potensi kerentanan yang dapat dimanfaatkan oleh peretas pada web Sistem Informasi Akademik (SIA) STIKES Guna Bangsa Yogyakarta dengan framework Open Web Application Security Project (OWASP). Penelitian ini menggunakan alat-alat seperti WhoIS, SSL Scan, Nmap, dan OWASP ZAP. Hasilnya didapatkan 12 kerentanan terdeteksi dengan perincian 4 kerentanan level medium, 6 kerentanan level low dan 2 kerentanan informational [10]. Penelitian selanjutnya berjudul Analisis Keamanan Website Open Journal System (OJS) menggunakan Metode Vulnerability Assessment. Tujuan penelitian ini adalah menganalisis keamanan sistem OJS dengan metode penetration testing dengan pendekatan black box. Hasil yang didapatkan menunjukkan bahwa OJS versi 2.4.7 memiliki total 6049 kerentanan, sehingga dapat disimpulkan bahwa OJS versi 2.4.7 tidak direkomendasikan untuk digunakan karena banyaknya celah keamanan yang ditemukan [11]. Penelitian berikutnya berjudul Vulnerability Assessment and Penetration Testing Framework: Case Study of Government's Website. Penelitian ini bertujuan untuk mendeteksi potensi kerentanan, mengevaluasi dampak dan memberikan rekomendasi perbaikan dengan menerapkan framework Vulnerability Assessment and Penetration Testing (VAPT). Penelitian ini mendapatkan hasil 5 jenis ancaman pada target, yaitu Directory Listing, Full Path Disclosure, PHPInfo Disclosure, Folder Webserver Disclosure, dan Blind SQL Injection [12]. Penelitian berikutnya berjudul Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (OWASP) pada simantep.id. Penelitian ini bertujuan mengidentifikasi dan mengurangi potensi ancaman menggunakan OWASP ZAP pada situs web simantep.id yang digunakan sebagai situs penjualan online dan penyewaan gudang. Hasil yang didapatkan yaitu 3 kerentanan level medium, 3 kerentanan level low dan 4 kerentanan level informational, serta prinsip keamanan CIA (Confidentiality, Integrity, Availability) sudah diterapkan pada domain simantep.id [13]. Penelitian selanjutnya berjudul Vulnerability Assessment and Penetration Testing on Student Service Center System. Tujuan dari penelitian ini adalah mengidentifikasi kerentanan keamanan pada sistem Student Service Center yang dimiliki oleh Universitas XYZ dengan metode Grey Box yang menggabungkan teknik manual dan otomatis. Hasil dari penelitian ini adalah ditemukan kerentanan pada fungsi file upload dan path traversal pada fitur download di menu MBKM dan rincian koleksi akademik, serta kerentanan yang memiliki skor severitas sedang (4.9) berdasarkan Common Vulnerability Scoring System (CVVS) [14].

Penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, memvalidasi keakuratan kerentanan tersebut melalui eksploitasi manual, dan menghitung tingkat keparahannya berdasarkan CVSS. Hasil analisis akan dikategorikan berdasarkan standar OWASP Top Ten dan dilengkapi dengan rekomendasi perbaikan untuk mengurangi celah keamanan. Dengan pendekatan ini, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan keamanan website dan memberikan panduan mitigasi yang lebih efisien dan terfokus.

II. METODE

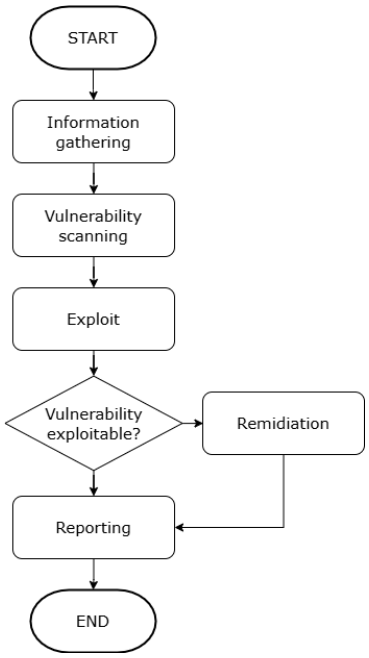
Metode yang digunakan dalam penelitian ini adalah Vulnerability Assessment and Penetration Testing (VAPT). VAPT merupakan proses evaluasi sistem aplikasi web untuk

mengidentifikasi dan mengatasi kerentanan keamanan pada website. Strategi pengujian yang digunakan adalah grey box testing. Grey box testing merupakan metode pengujian di mana penguji mengidentifikasi kerentanan dari sisi pengguna dan pengembang, penguji juga memiliki sebagian informasi tentang cara kerja internal aplikasi seperti penjelasan alur kerja, aliran data, dokumentasi API, dan teknologi yang digunakan [15]. Kerangka penelitian dapat dilihat pada Gambar 2.



Gambar 2. Kerangka penelitian

Gambar 2 menjelaskan tahapan penelitian yang dilakukan, yaitu dengan studi literatur, pengumpulan informasi, pengujian keamanan, serta hasil dan kesimpulan. Studi literatur dilakukan untuk memahami dasar teori dan perkembangan terbaru terkait keamanan website melalui tinjauan terhadap berbagai jurnal, artikel dan buku yang relevan. Studi ini mencakup telaah terhadap metodologi yang diterapkan dalam penelitian sebelumnya guna mendukung penelitian saat ini. Tahap selanjutnya adalah pengumpulan informasi dengan melibatkan beberapa tools guna memperoleh informasi mengenai target penelitian yang meliputi alamat IP, port yang terbuka, dan sertifikat keamanan website. Metode yang digunakan dalam tahap pengujian keamanan yaitu Vulnerability Assessment and Penetration Testing (VAPT), adapun tahapan metode VAPT dapat dilihat berdasarkan Gambar 3. Pada tahap hasil dan kesimpulan, data yang diperoleh melalui pengujian keamanan akan diolah dan dianalisis untuk mengidentifikasi pola-pola kerentanan berdasarkan CVE dan CWE. Analisis ini bertujuan untuk memahami karakteristik kerentanan yang terdeteksi serta mengklasifikasikannya berdasarkan tingkat keparahan dan potensi dampak. Hasil identifikasi ini akan menjadi dasar dalam merumuskan rekomendasi langkah mitigasi yang tepat, sehingga dapat meningkatkan ketahanan sistem terhadap potensi ancaman keamanan secara efektif.



Gambar 3. Kerangka pengujian

II. METODE

Pada bagian ini akan membahas mengenai pengujian keamanan website dengan menerapkan 4 tahapan utama, di mana setiap tahapan menggunakan tools yang sesuai dengan kebutuhan analisis keamanan. Setiap tahapan dalam proses pengujian ini dirancang untuk mengidentifikasi, mengevaluasi, dan mitigasi kerentanan keamanan yang ada pada website.

A. Information Gathering

Merupakan tahap pengumpulan informasi umum mengenai website target, termasuk mendapatkan alamat IP, pemindaian port yang terbuka, dan mengidentifikasi sertifikat keamanan Secure Socket Layer (SSL). Informasi data yang dibutuhkan pada pengujian diberikan oleh pemilik website yang mencakup mekanisme internal website dan kredensial pengguna untuk proses login. Alat yang digunakan meliputi NsLookup, Nmap, dan SSL Scan. NsLookup digunakan untuk mendapatkan alamat IP dari website test-kerdjo.frezico.com menggunakan tools NsLookup pada terminal Kali Linux dengan perintah nslookup test-kerdjo.frezico.com dan didapati hasil alamat IP yang digunakan yaitu 203.175.9.123.

```
[diana@kali]~$ nslookup test-kerdjo.frezico.com
Server: 192.168.150.2
   Address:  192.168 150.2#53
   Non-authoritative answer:
   Name: test-kerdjo.frezico.com Address:
         203.175.9.123
Name:    test-kerdjo.frezico.com Address:
2001:df1:7800:2::8:8
```

Tools berikutnya yaitu Nmap yang berfungsi sebagai alat untuk memindai port yang terbuka dan mengetahui layanan yang digunakan pada website dengan tools Nmap dengan mengetikan perintah nmap -v test- kerdjo.frezico.com. Hasil dari pemindaian ini terdapat 9 port yang terbuka, yaitu port 21, 80, 110, 143, 443, 465, 587, 993, dan 995.

```
[diana@kali]~$ nmap -v test-kerdjo.frezico.com
  Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 17:34 WIB Initiating Ping Scan at 17:34
  Scanning test-kerdjo.frezico.com (203.175.9.123) [2 ports] Completed Ping Scan at 17:34, 0.04s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 17:34
  Completed Parallel DNS resolution of 1 host. at 17:34, 0.02s elapsed Initiating Connect Scan at 17:34
  Scanning test-kerdjo.frezico.com (203.175.9.123) [1000 ports] Discovered open port 993/tcp on 203.175.9.123
  Discovered open port 80/tcp on 203.175.9.123
Discovered open port 21/tcp on 203.175.9.123
Discovered open port 143/tcp on 203.175.9.123
Discovered open port 110/tcp on 203.175.9.123
Discovered open port 995/tcp on 203.175.9.123
Discovered open port 587/tcp on 203.175.9.123
Discovered open port 465/tcp on 203.175.9.123
  Completed Connect Scan at 17:34, 4.79s elapsed (1000 total ports) Nmap scan report for test-kerdjo.frezico.com (203.175.9.123) Host is up (0.046s latency).
  Other addresses for test-kerdjo.frezico.com (not scanned): 2001:df1:7800:2::8:8
  rDNS record for 203.175.9.123: singgalang.dua.rumahweb.net Not shown: 991 filtered tcp ports (no-response)
  PORT STATE SERVICE
  21/tcp open ftp 80/tcp open http 110/tcp open pop3 143/tcp open imap 465/tcp open smtps
  587/tcp open submission 993/tcp open imaps 995/tcp open pop3s
  Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.55 seconds
```

Dan yang terakhir adalah SSL Scan yang digunakan untuk memeriksa sertifikat SSL dengan memasukkan perintah nmap --script ssl-enum-ciphers -p 443 test- kerdjo.frezico.com, seperti pada Gambar 6. Hasil pemeriksaan yang didapat, konfigurasi SSL menunjukkan Transport Layer Security (TLS) yang digunakan merupakan TLS versi terbaru yaitu TLSv1.2 dan TLSv1.3, dan website ini menggunakan cipher yang memiliki rating A atau dianggap aman karena menggunakan algoritma enkripsi yang kuat. Secara keseluruhan hasil pengujian ini menunjukkan bahwa konfigurasi TLS pada website test- kerdjo.frezico.com sudah cukup aman.

B. Vulnerability Scanning

Pemindaian kerentanan dilakukan untuk mendeteksi potensi kelemahan keamanan dalam website, seperti kesalahan konfigurasi, kerentanan dalam kode, atau titik akses yang tidak terlindungi dengan baik. Pemindaian ini menggunakan pendekatan pemindaian otomatis dengan Acunetix dan ZAP.

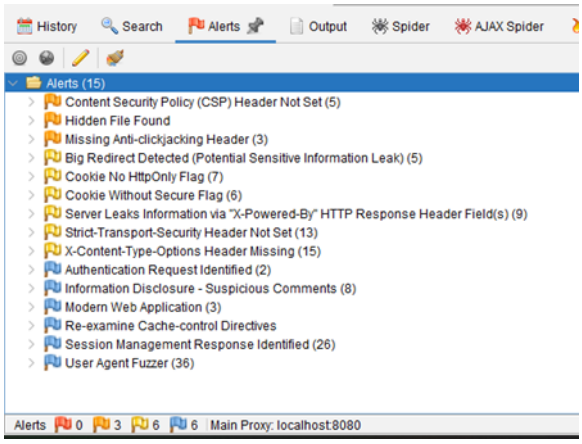
Acunetix merupakan alat pemindaian aplikasi web otomatis untuk mendeteksi kerentanan yang dapat dieksploitasi, termasuk Cross-site scripting (XSS) dan injeksi SQL. Acunetix memberikan hasil pemindaian terperinci yang tidak hanya mengidentifikasi kerentanan namun juga memberi informasi tentang cara memperbaikinya.. Acunetix memiliki kemampuan kuat untuk mendeteksi kerentanan, terutama kerentanan dengan level tinggi [16]. Acunetix menggunakan teknologi.

AcuSensor dan AcuMonitor untuk menghasilkan potensi kerentanan yang lebih akurat untuk meningkatkan keamanan situs website [17]. Pemindaian menggunakan tools Acunetix dilakukan dengan memasukkan domain dan mengisikan kredensial pengguna, pemindaian seperti pada Gambar 7 menghasilkan kerentanan dengan beberapa kategori, yaitu: kerentanan dengan level high severity vulnerabilities berjumlah 1, yaitu vulnerable package dependencies. Kerentanan dengan level medium severity vulnerabilities berjumlah 5, yaitu Development configuration files, Directory listings, Insecure HTTP usage, SSL/TLS Not implemented, dan User credential are sent in clear text. Kerentanan dengan level low severity vulnerabilities berjumlah 8, yaitu Clickjacking X-Frame- Options header, Composer installed.json publicy accessible, Cookie not marked as HttpOnly, Documentation files, Missing Content-Type Header, Possible sensitive directories, dan Version Disclosure (PHP).

Gambar 7. Pemindaian menggunakan Acunetix

ZAP merupakan tools berbasis open-source untuk menemukan kerentanan pada website yang dikembangkan oleh Open Worldwide Application Security Project (OWASP) dengan fitur pemindaian otomatis dan pemindaian manual [18]. Pemindaian menggunakan tools ZAP dilakukan dengan memasukkan domain. Hasil pemindaian dengan tools ZAP dapat dilihat pada Gambar 8, dengan perincian 3 kerentanan level medium severity yaitu Content Security Policy (CSP) Header Not Set, Hidden File Found, dan Missing Anti-clickjacking Header. 6 kerentanan dengan level low severity yaitu, Big Redirect Detected,(Potential Sensitive Information Leak), Cookie No. HttpOnly Flag, Cookie

Without Secure Flag, Server Leaks Information via "X-Powered-By" HTTP Response Header Field, Strict-Transport-Security Header Not Set, dan X-Content-Type-Option Header Missing.



Gambar 8. Pemindaian menggunakan ZAP

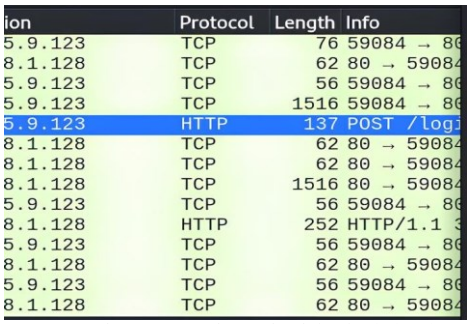
C. *Exploit*

Pada tahap eksploitasi terdapat 4 kerentanan yang berhasil di eksploitasi oleh pihak eksternal. Selain kerentanan yang dapat dieksploitasi, kerentanan lain yang terdeteksi tidak dapat dieksploitasi oleh pihak eksternal, mengingat pengujian ini memiliki akses yang terbatas. Namun, relevansi kerentanan yang terdeteksi dapat diperkuat dengan merujuk pada CVE/CWE, yang memberikan standar identifikasi dan tingkat keparahan awal. Meskipun demikian, tingkat keparahan yang ditetapkan dalam CVE/CWE perlu ditinjau ulang menggunakan Common Vulnerability Scoring System (CVSS) untuk mencerminkan risiko dalam keadaan spesifik. Penilaian CVSS mempertimbangkan faktor-faktor seperti kemampuan eksploitasi, dampak terhadap sistem, dan mekanisme mitigasi yang telah diterapkan. Dalam konteks ini, meskipun CVE menetapkan kerentanan sebagai high severity, CVSS dapat menyesuaikan tingkat keparahan berdasarkan kondisi operasional yang menunjukkan bahwa kerentanan bersifat non-exploitable oleh pihak eksternal. Peninjauan ini memastikan bahwa tingkat keparahan kerentanan mencerminkan risiko nyata dan menjadi dasar yang lebih akurat untuk pengambilan keputusan mitigasi.

Percobaan eksploitasi yang berhasil di antaranya Clickjacking, Improper HTTP to HTTPS redirection, Directory Listing dan Sensitive Information Disclosure. Percobaan eksploitasi kerentanan Clickjacking dilakukan dengan menggunakan sebuah script HTML, sehingga didapati hasil seperti Gambar 9.

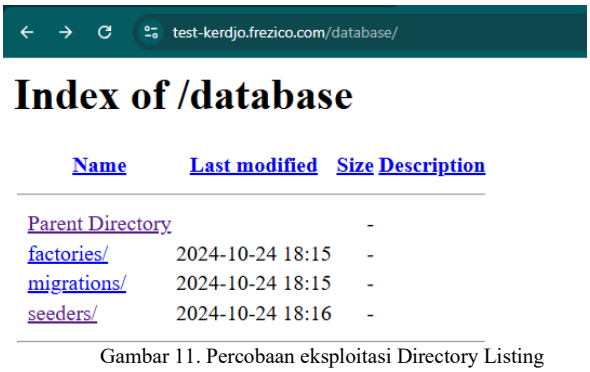
Gambar 9. Percobaan eksploitasi *Clickjacking*

Percobaan eksploitasi berikutnya adalah Improper HTTP to HTTPS redirection, yang dilakukan dengan sniffing menggunakan aplikasi Wireshark, sehingga didapati hasil seperti Gambar 10.



Gambar 10. Percobaan eksploitasi *Clickjacking*

Percobaan eksploitasi berikutnya adalah Directory Listing, yang dilakukan dengan directory scanning pada domain test-kerdjo.frezico.com, seperti pada Gambar 11.



Gambar 11. Percobaan eksploitasi Directory Listing

Percobaan eksploitasi berikutnya adalah Sensitive Information Disclosure, yang ditemukan karena adanya direcroty listing yang mengekspos direktori sensitif seperti seeder, migration, dan lain-lain. Hasilnya data sensitif berupa kredensial user dengan mudah didapatkan.

3608-4040-876F-bb04427886d1; JSS-AQ003; A** *******; AKTIF; 3; PPKSD; *********@gmail.com 7e-47a7-a20f-adc121463e74; JSS-A1814; A**** ******* ********; AKTIF;

```
    89689dac-Oc1adac8c66d; JSS-W7952; A** *********; TIDAK
AKTIF; 3; PPKSD; ************@mbiz.co.id
    7623acb-a853-859-a822-41389Fbc1346; JSS-V5266; A*****
    ******** ***** *******; AKTIF; 6; PPKSD;
    *************@gmail.com
    bce20aeb-2ce2-4e16-a1a9-221eecfb44d1; JSS-A4514; A****
    *******; AKTIF; 0; Admin
    3da1870ca-Gdab-42ad-93Fc-3e3a225dd0a3; JSS-A0017; A***
    **********, ***.; AKTIF; 2; PPKSD;
    ***************@gmail.com
...
```

D. Reporting

Tahap terakhir dalam pengujian keamanan web adalah reporting. Langkah-langkah yang dilakukan meliputi merangkum hasil analisis dan menyusun laporan berdasarkan pengujian yang telah dilakukan. Tabel 1 menyajikan laporan penilaian dan pengujian potensi kerentanan yang dipetakan berdasarkan standar OWASP Top Ten. Kerentanan yang ditemukan pada tahap pemindaian akan dipetakan dengan CVE atau CWE yang relevan sebagai identifikasi awal untuk memastikan keakuratan kerentanan. Selanjutnya, akan dilakukan identifikasi tingkat lanjut berupa percobaan eksploitasi untuk meninjau kembali level keparahan nyata dari kerentanan tersebut. Proses ini menggunakan kalkulator CVSS untuk mengevaluasi kemampuan eksploitasi dan dampak kerentanan terhadap sistem. Sebagai bagian dari laporan, dampak kerentanan dan rekomendasi perbaikan juga akan disertakan dengan tujuan mengurangi potensi celah keamanan pada sistem.

TABEL I
KERENTANAN BERDASARKAN OWASP TOP TEN

OWASP Top TEN	**Kerentanan**
A01:2021-Broken Access Control	-
A02:2021-Cryptographic Failures	Insecure HTTP Usage, Potential Sensitive Information in Redirects, User-Agent Fuzzer or Unhandled Inputs
A03:2021-Injection	-
A04:2021-Insecure Design	-
A05:2021-Security Misconfiguration	Directory Listings, Possible Sensitive Directories, Sensitive Directories Accessible, Publicly Accessible Sensitive Files, Cookie Security Misconfigurations, Development Configuration Files, Content Security Policy (CSP) Not Implemented, Missing Headers (X-Frame-Options, Content-Type, Strict-Transport-Security),
	Clickjacking Vulnerabilities, Content Security Policy Issues, dan Session Management Issues
A06:2021-Vulnerable and Outdated Components	Vulnerable Package Dependencies
A07:2021-Identification and Authentication Failures	-
A08:2021-Software and Data Integrity Failures	-
A09:2021-Security Logging and Monitoring Failures	-
A10:2021-Server-Side Request Forgery	-

Kerentanan yang berhasil dieksploitasi pada tahap exploit di antaranya, Clickjacking, Improper HTTP to HTTPS redirection, Directory Listing dan Sensitive Information Disclosure.

Clickjacking termasuk dalam kategori A05:2021- Security Misconfiguration pada standar OWASP Top Ten, kerentanan ini disebabkan website tidak menerapkan konfigurasi X-Frame-Options dan Content Security Policy (CSP). Dampak dari serangan ini memungkinkan penyerang menipu pengguna untuk berinteraksi dengan halaman yang sudah dimodifikasi, hal ini dapat dimanfaatkan untuk mencuri data pengguna dan melakukan transaksi ilegal. Kerentanan ini relevan dengan CWE-1021 (Improper Restriction of Rendered UI Layers or Frames) sebagai identifikasi awal dan memiliki level kerentanan medium. Setelah dilakukan identifikasi tingkat lanjut dan dihitung dengan CVSS, kerentanan ini memiliki tetap pada level medium. Rekomendasi perbaikan yang dapat dilakukan adalah menerapkan header x-frame- options untuk mencegah halaman dimuat dalam iframe oleh domain lain serta menerapkan Content Security Policy (CSP) untuk mengontrol sumber daya yang dapat dimuat halaman, termasuk iframe.

Improper HTTP to HTTPS redirection termasuk dalam kategori A02:2021-Cryptographic Failures pada standar OWASP Top Ten, kerentanan ini disebabkan oleh kesalahan konfigurasi pada server website, sehingga website tidak dapat mengalihkan permintaan HTTP ke HTTPS. Dampak serangan ini memungkinkan terjadi serangan Man-In-The-Middle (MITM), penyerang dapat mencegat dan memodifikasi komunikasi antara pengguna dan server. Kerentanan ini relevan dengan CWE-319 (Cleartext Transmission of Sensitive Information) sebagai identifikasi awal dan memiliki level kerentanan medium. Setelah dilakukan identifikasi tingkat lanjut dan dihitung dengan CVSS, kerentanan ini memiliki tetap pada level medium. Rekomendasi perbaikan yaitu mengonfigurasi server untuk memastikan semua permintaan HTTP secara otomatis dialihkan ke HTTPS.

Directory Listing termasuk dalam kategori A05:2021-Security Misconfiguration pada standar OWASP Top Ten, kerentanan ini disebabkan oleh kesalahan konfigurasi pada website yang tidak memberikan batasan akses ke direktori. Dampak serangan ini memungkinkan penyerang mencuri data sensitif dan menggunakannya untuk aktivitas yang tidak diizinkan. Kerentanan ini relevan dengan CWE-548 (Exposure of Information Through Directory Listing) sebagai identifikasi awal dan memiliki level kerentanan medium.

Setelah dilakukan identifikasi tingkat lanjut dan dihitung dengan CVSS, kerentanan ini memiliki level high karena di dalam direktori terdapat informasi sensitif yang dapat diakses publik. Rekomendasi perbaikan yang dapat dilakukan adalah menutup akses direktori langsung melalui konfigurasi server.

Sensitive Information Disclosure termasuk dalam kategori A05:2021-Security Misconfiguration pada standar OWASP Top Ten, kerentanan ini disebabkan oleh kesalahan konfigurasi pada website, sehingga menampilkan data sensitif yang dapat diakses publik dan membuka peluang penyerangan. Dampak serangan ini memungkinkan penyerang menggunakan data sensitif untuk mengeksploitasi dan membahayakan data pribadi pengguna. Kerentanan ini relevan dengan CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) sebagai identifikasi awal dan memiliki level kerentanan medium. Setelah dilakukan identifikasi tingkat lanjut dan dihitung dengan CVSS, kerentanan ini memiliki level critical, karena file yang terekspos berupa data kredensial pengguna website. Rekomendasi perbaikannya yaitu menghapus file yang menyimpan kredensial, membatasi akses file yang dapat dilihat publik, dan segera menutup file sensitif yang terbuka.

Kerentanan selanjutnya merupakan kerentanan yang tidak dapat dibuktikan dengan percobaan eksploitasi yang disebabkan keterbatasan akses pengujian terhadap sistem. Kerentanan tersebut adalah User Credentials Sent in Clear Text, Insecure HTTP Usage, Development Configuration Files, dan Vulnerable Package Dependencies.

Insecure HTTP Usage memiliki tingkat keparahan medium. Insecure HTTP Usage termasuk dalam kategori A02:2021-Cryptographic Failures pada standar OWASP Top Ten dan memiliki level kerentanan medium. Kerentanan ini disebabkan oleh kerentanan sebelumnya yaitu Improper HTTP to HTTPS redirection. Kerentanan ini relevan dengan CWE-319 (Cleartext Transmission of Sensitive Information). Dampaknya saluran komunikasi yang tidak teralihkan ke protokol HTTPS dapat dipantau oleh pihak tidak berwenang selama transmisi data, memungkinkan pencurian informasi sensitif. Rekomendasi perbaikan yang dapat dilakukan adalah mengonfigurasi server untuk memastikan semua permintaan HTTP secara otomatis dialihkan ke HTTPS.

Development Configuration Files termasuk dalam kategori A05:2021-Security Misconfiguration pada standar OWASP Top Ten. Kerentanan ini disebabkan oleh kesalahan konfigurasi di mana file konfigurasi pengembangan yang seharusnya tidak tersedia dilingkungan produksi dapat diakses oleh publik. File ini dapat berupa data sensitif, konfigurasi sistem, atau pengaturan debug. CWE yang relevan adalah CWE-538 (File and Directory Information Exposure) dan memiliki level kerentanan medium. Dampaknya file sensitif dapat terekspos dan menyebabkan kebocoran data. Rekomenadasi perbaikan yang dapat dilakukan adalah menghapus file konfigurasi pengembangan dan membatasi akses file sensitif.

Vulnerable Package Dependencies termasuk dalam kategori A06:2021-Vulnerable and Outdated Components pada standar OWASP Top Ten. Kerentanan ini disebabkan ketika website menggunakan versi dependensi pihak ketiga yang kadaluarsa. Secara spesifik versi package dependecies yang kadaluarsa tersebut adalah dompdf, guzzlehttp/psr7, dan rekursi tak terkendali yang mengandung kerentanan. Terdapat tiga CVE yang relevan yaitu, CVE-2023-50262, CVE-2023-29197, dan CVE-2023-50251. CWE yang relevan adalah CWE-937 (Use of Vulnerable Third-Party Components) dan memiliki level kerentanan medium. Meskipun pada tahap vulnerability scanning kerentanan ini menempati level high, kerentanan tersebut tidak dapat dieksploitasi oleh pihak eksternal. Dampaknya penyerang dapat mengeksploitasi website dengan menjalankan kode berbahaya untuk membanjiri permintaan pada server, sehingga websie akan down. Rekomenadasi perbaikan yang perlu dilakukan adalah dengan memperbaharui package dependency ke versi yang terbaru.

Selain memperbaiki celah kerentanan pada sistem untuk mengurangi celah kerentanan, organisasi perlu melatih tim untuk meningkatkan awareness terhadap keamanan website. Pemeliharaan jangka panjang juga diperlukan guna mengantisipasi adanya potensi kerentanan yang dapat dieksploitasi dan berdampak merugikan pengguna organisasi. Langkah praktis yang dapat dilakukan adalah melakukan VAPT secara berkala.

V. KESIMPULAN

Penelitian ini telah berhasil mengidentifikasi dan menganalisis kerentanan pada website menggunakan metode Vulnerability Assessment and Penetration Testing (VAPT) berdasarkan standar OWASP Top Ten. Hasil Vulnerability Assessment, pada Acunetix terdapat 1 kerentanan level high, 5 kerentanan level medium, serta 7 kerentanan level low. Pemindaian pada ZAP terdapat 3 kerentanan level medium dan 5 kerentanan di level low. Total kerentanan yang ditemukan sebanyak 14 kerentanan. Dari jumlah tersebut, tingkat keberhasilan eksploitasi sebesar 29%, dengan 4 kerentanan berhasil dieksploitasi, sementara tingkat kegagalan eksploitasi sebesar 71%, dengan 10 kerentanan yang tidak dapat dieksploitasi oleh pihak eksternal karena tidak memiliki akses. Beberapa kerentanan kritis dan berhasil dieksploitasi yang ditemukan meliputi Clickjacking, Improper HTTP to HTTPS Redirection, Directory Listing, dan Sensitive Information Disclosure. Tingkat keparahan kerentanan dianalisis lebih lanjut menggunakan CVE, CWE, dan CVSS untuk mencerminkan risiko faktual dari sistem target. Hasil penelitian menunjukkan bahwa kombinasi analisis OWASP Top Ten dengan evaluasi berbasis CVSS mampu memberikan pemahaman yang lebih mendalam terhadap risiko keamanan, sekaligus menjadi dasar untuk merumuskan langkah mitigasi yang tepat. Rekomendasi perbaikan mencakup penerapan header keamanan seperti X-Frame-Options dan Content Security Policy (CSP), penghapusan file konfigurasi yang memuat data sensitif, pembaruan paket dependensi, dan peningkatan konfigurasi server.

Penelitian ini menegaskan pentingnya evaluasi keamanan website secara berkala dan menyeluruh. Dengan menerapkan metode VAPT yang terstandarisasi, organisasi dapat mengurangi potensi ancaman keamanan dan melindungi data pengguna secara lebih efektif.

DAFTAR PUSTAKA

[1] Nurjannah and Abdul Muni, "Analisis Keamanan Website Sekolah Sman 1 Tempuling Dengan Menggunakan Open Web Application Security Project (Owasp)," J. Perangkat Lunak, vol. 6, no. 2, pp. 351–361, 2024, doi: 10.32520/jupel.v6i2.3442.

[2] M. N. Fauzan, O. Nurdiawa, and Y. A. Wijaya, "Analisis Sistem Website Sekolah Adiwiyata Menggunakan Website Quality (WEBQUAL)," J. Janitra Inform. dan Sist. Inf., vol. 3, no. 1, pp. 40–48, 2023, doi: 10.25008/janitra.v3i1.167.

[3] Arfan Dwi Madya, Bagas Djoko Haryanto, and Devi Putri Ningsih, "Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity," Indones. J. Educ. Comput. Sci., vol. 1, no. 3, pp. 127–135, 2023, doi: 10.60076/indotech.v1i3.236.

[4] M. Aljabri et al., "Testing and Exploiting Tools to Improve OWASP Top Ten Security Vulnerabilities Detection," in Proceedings - 2022 14th IEEE International Conference on Computational Intelligence and Communication Networks, CICN 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 797–803. doi: 10.1109/CICN56167.2022.10008360.

[5] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2023," bssn.go.id. [Online]. Available: https://www.bssn.go.id/monitoring-keamanan-siber/

[6] J. Softić and Z. Vejzović, "Impact of Vulnerability Assesment and Penetration Testing (VAPT) on Operating System Security," in 2023 22nd International Symposium INFOTEH- JAHORINA, INFOTEH 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/INFOTEH57020.2023.10094095.

[7] B. A. Chandrakant and J. P. Prakash, "Vulnerability Assessment and Penetration Testing As Cyber Defence," Int. J. Eng. Appl. Sci. Technol., vol. 4, no. 2, pp. 72–76, 2019, doi: 10.33564/ijeast.2019.v04i02.012.

[8] Victor Ilyas Sugara and I Wayan Sriyasa, "Analisis Keamanan Web Menggunakan Open Web Application Security Web (OWASP)," Indones. J. Comput. Sci., vol. 13, no. 2, pp. 3315– 3327, 2024, doi: 10.33022/ijcs.v13i2.3736.

[9] S. F. Wen and B. Katt, "A quantitative security evaluation and analysis model for web applications based on OWASP application security verification standard," Comput. Secur., vol. 135, no. September, p. 103532, 2023, doi: 10.1016/j.cose.2023.103532.

[10] M. A. Mu'min, A. Fadlil, and I. Riadi, "Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework," J. Media Inform. Budidarma, vol. 6, no. 3, p. 1468, 2022, doi: 10.30865/mib.v6i3.4099.

[11] I. Riadi, A. Yudhana, and Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment," J. Teknol. Inf. dan Ilmu Komput., vol. 7, no. 4, pp. 853–860, 2020, doi: 10.25126/jtiik.2020701928.

[12] A. Almaarif and M. Lubis, "Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 10, no. 5, pp. 1874–1880, 2020, doi: 10.18517/ijaseit.10.5.8862.

[13] E. Nurelasari and D. Gumilang Al Farabi, "Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (Owasp) Pada Simantep.Id," JATI (Jurnal Mhs. Tek. Inform., vol. 8, no. 3, pp. 3049–3054, 2024, doi: 10.36040/jati.v8i3.9314.

[14] K. Nur, M. Hasyim, and S. Fathu, "Vulnerability Assessment and Penetration Testing on Student Service Center System," vol. 16, no. 2, pp. 161–171, 2024.

[15] U. Ravindran and R. V. Potukuchi, "A Review on Web Application Vulnerability Assessment and Penetration Testing," Rev. Comput. Eng. Stud., vol. 9, no. 1, pp. 1–22, 2022, doi: 10.18280/rces.090101.

[16] R. Amankwah, J. Chen, P. K. Kudjo, and D. Towey, "An empirical comparison of commercial and open-source web vulnerability scanners," Softw. - Pract. Exp., vol. 50, no. 9, pp. 1842–1857, 2020, doi: 10.1002/spe.2870.

[17] A. Kadu, B. Chalakh, K. Gorle, and S. Malpe, "' Review : Developing a website analysis tool for vulnerability scanning and re porting ,'" vol. 13, no. 2, pp. 1190–1194, 2020.

[18] A. W. Kuncoro and F. Rahma, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," Automata, vol. 3, no. 1, pp. 1–5, 2021, [Online]. Available: https://www.sciencedirect.com