BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT

Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)

Khairrun Nisa, Muklas Adi Putra, Rizky Akbar Siregar, Muhammad Dedi Irawan
Fakultas sains dan Teknologi, Sistem Komputer, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email: [1]*khairrunnisa042@gmail.com, [2]muklasputra222@gmail.com, [3]rizkysrg62@gmail.com,
[4]muhammaddediirawan@gmail.com
Email Penulis Korespondensi: khairrunnisa042@gmail.com

Abstrak− Keamanan data pada website sangat penting untuk mencegah penyalahgunaan data atau informasi di website. Karena pesatnya kemajuan teknologi, banyak oknum yang tidak bertanggung jawab yang sering disebut dengan hacker atau peretas mencuri data. Penulis tertarik untuk mempelajari lebih lanjut tentang keamanan website Tapanuli Tengah (TAPTENG) sebagai hasil dalam penelitian ini. Pada bagian ini, penulis melakukan pengecekan keamanan website Tapanuli Tengah menggunakan metode OWASP ZAP untuk membantu dalam menentukan tindakan yang perlu diambil untuk memitigasi kerentanan. Ada beberapa tahapan OWASP yang dilakukan diantaranya Information Gathering, Session Management Testing, Data Validation Testing, dan Webservices Testing. Dari keseluruhan hasil penelitian yang terdeteksi pada website 192.187.99.170 diperoleh hasil yaitu 22079 instansi dengan nama ancaman Timestamp Disclosure – Unix dengan level ancaman berada di level Low, yang artinya berada ditingkat rendah.

Kata Kunci: Tapanuli Tengah; OWASP; Website; Keamanan

Abstract− Data security on the website is very important to prevent misuse of data or information on the website. Due to the rapid advancement of technology, many irresponsible persons who are often called hackers or hackers steal data. The author is interested in learning more about the security of the Central Tapanuli website (TAPTENG) as a result of this research. In this section, the author checks the security of the Tapanuli Tengah website using the OWASP ZAP method to assist in determining the actions that need to be taken to mitigate the vulnerability. There are several stages of OWASP that are carried out including Information Gathering, Session Management Testing, Data Validation Testing, and Webservices Testing. From the overall research results detected on the 192.187.99.170 website, the results obtained were 22079 instances with the threat name Timestamp Disclosure - Unix with the threat level at the Low level, which means it is at a low level.

Keywords: Central Tapanuli; OWASP; Website; Security.

1. PENDAHULUAN

Suatu organisasi yang bertugas mengolah informasi di lingkungan Tapanuli Tengah adalah website Pemerintah Kabupaten Tapanuli Tengah. Instansi Pemerintah Tapanuli Tengah juga perlu memiliki website yang merupakan kebutuhan yang sangat penting. Karena website bersifat online dan dapat diakses oleh semua pengguna internet, sistem keamanan melindungi situs web dari ancaman yang ditimbulkan oleh peretas[1]. Website memberikan sejumlah keunggulan, antara lain kemampuannya untuk menyampaikan informasi, memfasilitasi interaksi, menjadi tolok ukur untuk menentukan aktif atau tidaknya kegiatan pemerintah, memungkinkan individu untuk menyampaikan aspirasinya, dan memfasilitasi promosi[2]. Akibatnya, layanan situs web harus diuji keamanannya[3].

Karena pesatnya kemajuan teknologi, banyak oknum yang tidak bertanggung jawab yang sering disebut dengan hacker atau peretas mencuri data[4]. Hacker mencari lubang di server web dengan berbagai alasan dengan tujuan untuk mendapatkan informasi tentang suatu perusahaan, organisasi, atau lembaga pemerintah agar dapat merugikan pihak lain[5]. Tes keamanan dilakukan untuk menentukan tingkat kelemahan untuk menghindari serangan dari pertemuan yang tidak menyenangkan[6].

OWASP ZAP dapat membantu dalam menentukan tindakan yang perlu diambil untuk memitigasi kerentanan agar instansi pemerintah di Tapanuli Tengah memiliki perlengkapan yang lebih baik untuk melindungi data mereka dari serangan[7]. Salah satu aplikasi pemindai web paling populer, OWASP ZAP, adalah alat yang sangat baik untuk menyelesaikan masalah keamanan situs[8]–[10]. Sepuluh teratas diberi peringkat oleh OWASP dalam urutan eksploitasi, prevalensi umum, kemudahan deteksi, dan keparahan dampak[13]. Akibatnya, untuk mengenali bahaya dan memahami ancaman, aplikasi berbasis situs web harus diperiksa[11]. Manajer dan pengembang sistem dapat menggunakan hasil penilaian risiko situs web untuk mengamankan situs web dengan lebih baik dan mencegah serta mengurangi risiko sistem[12] . Berbagai penelitian tentang penggunaan metode OWASP untuk pengujian keamanan sistem telah menunjukkan bahwa alat dan metode memiliki dampak signifikan pada langkah dan hasil. Objek pengujian, alat, dan pendekatan semuanya bervariasi. Dimulai dengan tahapan dan diakhiri dengan analisis dan hasil rekomendasi, setiap alat dan metode unik. Penelitian ini menjelaskan berbagai jenis serangan, cara mencegah serangan pada server web, dan dampak kebocoran data pada agensi dan pengguna[14]. Kesimpulannya, melindungi terhadap serangan dari pihak yang sembrono bisa mendapatkan keuntungan dari pemantauan, pendeteksian, dan penanganan kerentanan yang dijelaskan[13].

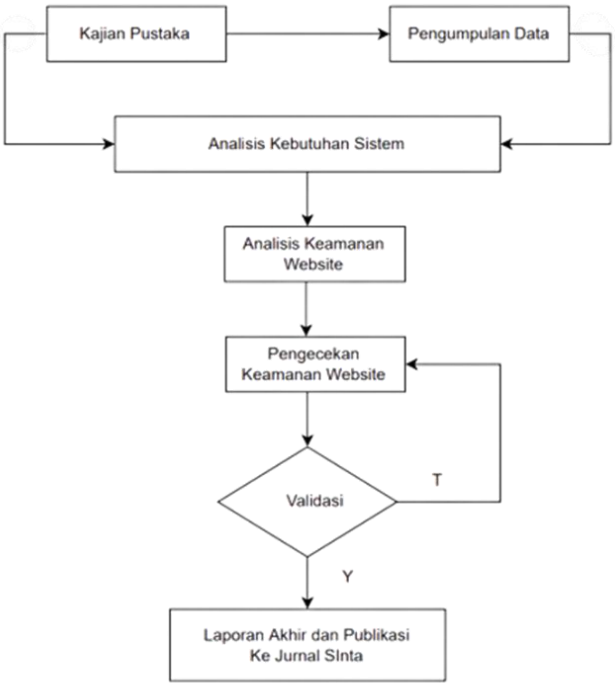
Oleh karena itu, penulis tertarik untuk menyelidiki dan menganalisis penerapan metode tersebut. Semua alat, dokumen, dan forum yang digunakan oleh Open Web Application Security Project (OWASP) gratis dan dapat diakses oleh siapa saja yang tertarik. Komunitas ini didedikasikan untuk memungkinkan bisnis mengembangkan, membeli,

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT

dan memelihara aplikasi tepercaya. untuk meningkatkan keamanan aplikasi[15]. Ini dapat memberikan gambaran tentang pengujian keamanan sistem menggunakan OWSP[16]. Saat menguji keamanan sistem, khususnya situs web menggunakan metode OWASP, seperti pada penelitian sebelumnya, literatur ini dapat dipertimbangkan. Tujuan penelitian ini adalah untuk memberikan jawaban atas pertanyaan terkait penelitian yang akan membantu dalam memahami strategi pengujian keamanan sistem

2. METODOLOGI PENELITIAN

Metode penilaian risiko OWASP digunakan dalam penelitian untuk mengidentifikasi sistem keamanan situs web di 192.187.99.170. Dengan menggunakan metode ini, dimungkinkan untuk memutuskan apa yang harus dilakukan terhadap risiko tersebut. Dengan mengetahui bahaya yang akan terjadi, banyak keuntungan yang akan didapat termasuk, menghemat waktu dan mengurangi terjadinya bahaya serius tambahan. Ada juga beberapa tahapan OWASP pada saat ini, antara lain:



Gambar 1. Tahapan Penelitian

a. Information Gathering
   Penulis mulai pada titik ini untuk mengidentifikasi versi dan jenis server web yang berjalan untuk memilih kerentanan dan eksploitasi yang sesuai untuk pengujian..
b. Session Management Testing
   Penguji harus mengetahui bahwa semua cookie telah disetel dan bahwa konfigurasi keamanan yang sesuai sedang digunakan pada saat ini.
c. Data Validation Testing
   Penulis akan melakukan validasi input pada titik ini untuk memastikan bahwa hanya data yang diformat dengan benar yang masuk ke alur kerja sistem informasi, sehingga mencegah data yang rusak tetap berada di database. Selain itu, penting untuk dicatat bahwa meskipun validasi input tidak boleh digunakan sebagai metode utama untuk mencegah XSS, SQL Injection, dan serangan lain yang tercakup dalam lembar contekan mereka sendiri, ini dapat berkontribusi secara signifikan untuk mengurangi dampaknya jika diterapkan dengan tepat.
d. Webservices Testing
   Penganalisis memulai pengujian dengan eksekusi kode sisi klien, umumnya secara lokal di browser internet atau modul program. Kode yang berjalan di sisi klien tidak sama dengan kode yang berjalan di server dan mengembalikan konten berikutnya. Selain itu dikumpulkan pula beberapa makalah, jurnal, artikel, dan makalah yang berkaitan dengan isu, tujuan, dan pembahasan dalam artikel ini untuk persiapan, khususnya yang membahas metode Zap Open Web Application Security Project (owasp zap) untuk Menganalisis Situs Tapanuli Tengah.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT

3. HASIL DAN PEMBAHASAN

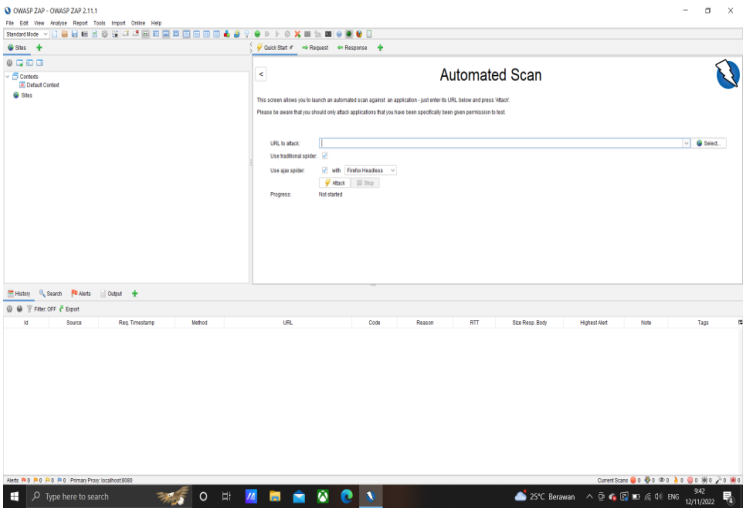
3.1 *Information Gathering*

Penulis langsung melakukan pengujian pada website Tapanuli Tengah, 192.187.99.170, karena sudah mengetahui website mana yang ingin diuji keamanannya.

3.2 *Session Management Testing*

1. Tampilan Awal

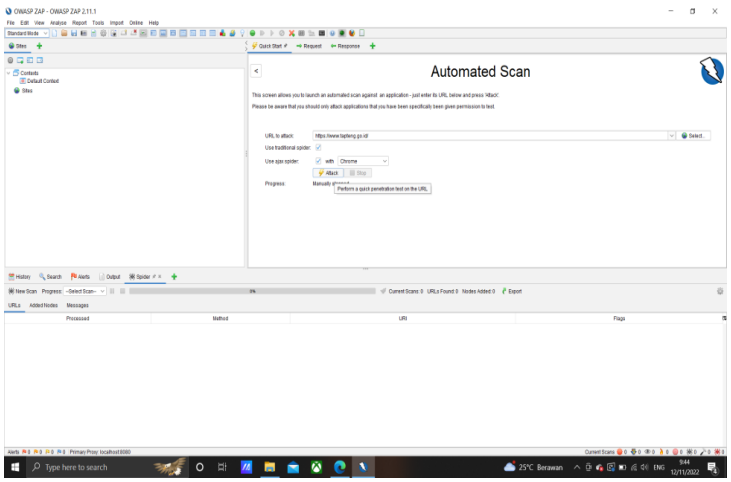
Tampilan awal akan muncul saat membuka program OWASP. Selanjutnya, klik *automatic scan* pada kolom *Welcome to OWASP ZAP*, dan akan muncul tampilan seperti pada Gambar 2



Gambar 2. Tampilan Halaman Utama *OWASP ZAP*

2. Input URL Website

Setelah itu, pada kolom URL *to Attack*, kita masukkan URL *website* 192.187.99.170, pilih *Use traditional spider* dan *Use ajax spider for scanning assistance*, kemudian pilih *Start* pada tahap selanjutnya, seperti terlihat pada Gambar 3

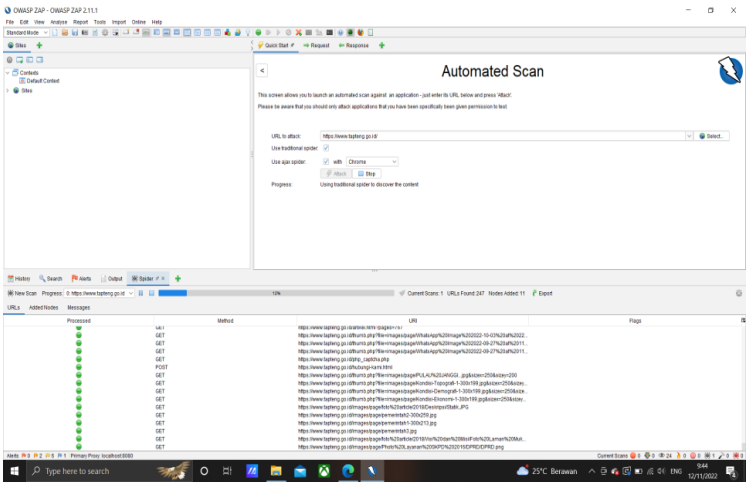


Gambar 3. Cara *Scanning OWASP ZAP*

3. Scanning Website

Proses selanjutnya adalah scanning website. Setelah URL di Input dan klik start, maka Aplikasi *OWASP-ZAP* akan mulai mencari ancaman yang ada pada *website* 192.187.99.170. Jika proses scanning selesai maka tampil hasilnya, seperti yang ditunjukkan pada Gambar 4

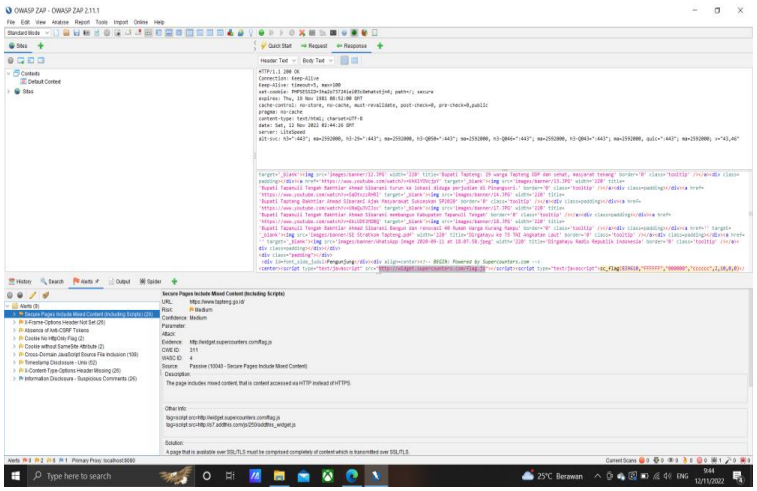
BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT



Gambar 4. *Scanning OWASP ZAP*

4. **Hasil Ancaman (*Alert*)**

Setelah pemindaian selesai, maka kita ada akan mendapatkan *alert* dari website yang di *attack* seperti yang ditampilkan pada Gambar 5



Gambar 5. Hasil *Scanning OWASP ZAP*

5. ***Finishes Scanning***

Setelah pemindaian selesai, kami menggunakan data kembali hingga semua situs web yang dipindai siap. Data yang didapatkan akan menjadi hasil akhir dari penelitian ini.

3.3 Hasil Penelitian

1. Summary of Alerts

Summary of Alerts adalah Ringkasan dari ancaman yang didapatkan melalu scanning menggunakan *OWASP-ZAP*, seperti yang ditunjukkan pada Tabel 1. dibawah ini :

Tabel 1. *Summary of Alerts*

Risk Level	Number of Alerts
High	**0**
Medium	**4**
Low	**7**
Informational	**1**

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT

Hasil ringkas yang didapatkan dari pengujian *website* 192.187.99.170 seperti yang ditampilkan di Tabel 1. Ringkasan dari ancaman yang rentan untuk di bobol oleh para *Hacker.*

2. Alerts

Alerts berisi nama-nama ancaman beserta level pada ancaman tersebut dan juga berisi angka instansi dari masing-masing ancaman yang berhasil didapatkan melalui *OWASP-ZAP*, seperti yang ditunjukkan pada Tabel 2. dibawah ini :

Tabel 2. *Alerts*

Nama	Risk Level	Number of Instances
Application Error Disclosure	Medium	5
Secure Pages Include Mixed Content (Including Scripts)	Medium	239
Vulnerable JS Library	Medium	12
X-Frame-Options Header Not Set	Medium	248
Absence of Anti-CSRF Tokens	Low	39
Cookie No HttpOnly Flag	Low	13
Cookie without SameSite Attribute	Low	37
Cross-Domain JavaScript Source File Inclusion	Low	970
Incomplete or No Cache-control Header Set	Low	1
Timestamp Disclosure - Unix	Low	22079
X-Content-Type-Options Header Missing	Low	621
Information Disclosure - Suspicious Comments	Informational	384

Tabel 2. Menampilkan nama ancaman yang terdeteksi saat pengujian, dan menampilkan jumlah instansi yang rentan di bobol atau dicuri datanya. Angka instansi tertinggi dari hasil pengujian adalah 22079 instansi dengan nama ancaman *Timestamp Disclosure – Unix.* Ancaman tersebut berada di level *Low*, yang artinya berada ditingkat rendah.

3. *Alert Detail*

Alert Detail berisi solusi yang bertujuan untuk mengurangi risiko dari masing-masing ancaman yang terdeteksi oleh *OWASP-ZAP*, seperti yang ditampilkan pada Tabel 3. Dibawah ini :

Tabel 3. *Alerts Detail*

192.187.99.170		
Jenis Ancaman	**Level Ancaman**	**Solusi**
Application Error Disclosure	Medium	Tinjau kode sumber halaman ini. Terapkan halaman kesalahan khusus. Mempertimbangkan menerapkan mekanisme untuk memberikan referensi/pengidentifikasi kesalahan unik kepada klien (browser) saat mencatat detail di sisi server dan tidak memaparkannya kepada pengguna.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT

Secure Pages Include Mixed Content (Including Scripts)	Medium	Halaman yang tersedia melalui SSL/TLS harus sepenuhnya terdiri dari konten yang dikirimkan melalui SSL/TLS. Halaman tidak boleh berisi konten apa pun yang dikirimkan melalui HTTP yang tidak terenkripsi. Ini termasuk konten dari situs pihak ketiga.
Vulnerable JS Library	Medium	Harap tingkatkan ke versi terbaru jquery.
X-Frame-Options Header Not Set	Medium	Sebagian besar browser Web modern mendukung header HTTP X-Frame-Options. Pastikan itu disetel di semua halaman web yang dikembalikan oleh situs Anda (jika Anda mengharapkan halaman hanya dibingkai oleh halaman di server Anda (mis. itu bagian dari FRAMESET) maka Anda akan ingin menggunakan SAMAORIGIN, jika tidak, jika Anda tidak pernah mengharapkan halaman dibingkai, Anda harus menggunakan DENY. Sebagai alternatif, pertimbangkan untuk menerapkan arahan "frame-ancestors" Kebijakan Keamanan Konten.
Absence of Anti-CSRF Tokens	Low	**Fase: Arsitektur dan Desain** Gunakan perpustakaan atau kerangka kerja yang diperiksa yang tidak memungkinkan kelemahan ini terjadi atau disediakan konstruksi yang membuat kelemahan ini lebih mudah untuk dihindari. Misalnya, gunakan paket anti CSRF seperti OWASP CSRFGuard. **Fase: Implementasi** Pastikan aplikasi Anda bebas dari masalah skrip lintas situs, karena sebagian besar CSRF pertahanan dapat dilewati menggunakan skrip yang dikendalikan penyerang. **Fase: Arsitektur dan Desain** Hasilkan nonce unik untuk setiap formulir, tempatkan nonce ke dalam formulir, dan verifikasi noncesetelah menerima formulir. Pastikan bahwa nonce tidak dapat diprediksi (CWE-330). Perhatikan bahwa ini dapat dilewati menggunakan XSS. Identifikasi operasi yang sangat berbahaya.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT

		Saat pengguna melakukan operasi berbahaya, kirim permintaan konfirmasi terpisah untuk memastikan bahwa pengguna bermaksud melakukan itu operasi. Perhatikan bahwa ini dapat dilewati menggunakan XSS. Gunakan kontrol Manajemen Sesi ESAPI. Kontrol ini mencakup komponen untuk CSRF. Jangan gunakan metode GET untuk permintaan apa pun yang memicu perubahan status. **Fase: Implementasi** Periksa header HTTP Referer untuk melihat apakah permintaan berasal dari halaman yang diharapkan. Ini dapat merusak fungsionalitas yang sah, karena pengguna atau proxy mungkin telah dinonaktifkan mengirim Perujuk untuk alasan privasi.
Cookie No HttpOnly Flag	Low	Pastikan bahwa *flag HttpOnly* disetel untuk semua cookie.
Cookie without SameSite Attribute	Low	Pastikan atribut SameSite disetel ke 'longgar (*lax*)' atau idealnya 'ketat (*strict*)' untuk semua cookie.
Cross-Domain JavaScript Source File Inclusion	Low	Pastikan file sumber JavaScript dimuat hanya dari sumber tepercaya, dan sumbernya tidak dapat dikontrol.
Incomplete or No Cache-control Header Set	Low	Kapan pun memungkinkan, pastikan header HTTP kontrol-cache disetel dengan no-cache, no-store, harus-validasi ulang.
Timestamp Disclosure - Unix	Low	Konfirmasikan secara manual bahwa data stempel waktu tidak sensitif, dan bahwa data tidak dapat digabungkan untuk mengungkap pola yang dapat dieksploitasi.
X-Content-Type-Options Header Missing	Low	Pastikan bahwa aplikasi/server web menyetel tajuk Content-Type dengan benar, dan menyetel tajuk X-Content-Type-Options ke 'nosniff' untuk semua halaman web. Jika memungkinkan, pastikan bahwa pengguna akhir menggunakan browser web yang sesuai standar dan modern yang sama sekali tidak melakukan pelacakan MIME, atau yang dapat diarahkan oleh web aplikasi/server web untuk tidak melakukan MIME-sniffing.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT

Information Disclosure - Suspicious Comments	-	Informational	Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang dan perbaiki masalah mendasar yang mereka rujuk.

Dari pengujian yang dilakukan pada *website* 192.187.99.170, ada solusi untuk mencegah kerentanan tersebut. Seperti yang ditampilkan di Tabel 3. solusi yang mungkin untuk mencegah kerentanannya walaupun keefektifan nya belum teruji, karena untuk menguji keefektifannya hanya bisa dilakukan oleh admin *website* tersebut.

4. KESIMPULAN

Tinjauan pengujian keamanan sistem informasi, khususnya yang berkaitan dengan aplikasi situs web, disediakan dalam penelitian ini. Pengujian keamanan sangat penting dalam memberikan keamanan dan kenyamanan kepada klien kerangka kerja. Ada sejumlah kelemahan dan kerentanan dalam sistem yang dapat ditemukan dengan mencari lubang keamanan dan menguji lubang keamanan. Karena pihak yang tidak memiliki akses dapat memanfaatkan kelemahan ini. Infiltrasi peretas terhadap suatu sistem mencontohkan perlunya pengujian keamanan secara teratur dan bertahap untuk menyediakan sistem yang baik kepada pengguna, terutama mengingat meningkatnya informasi tentang kebocoran data. Selain itu, diketahui dari temuan analisis bahwa metode ZAP OWASP lebih sering digunakan, dan tersedia alat sumber terbuka untuk mencari dan menguji keamanan sistem, seperti ZAP, yang sangat baik untuk menguji keamanan sistem berbasis website. Namun, sangat sedikit penelitian yang dilakukan dengan menggunakan metode OWASP versi 4 untuk pengujian keamanan. Selain itu, berbagai kelemahan keamanan dan jenis serangan semakin berkembang, membuat pendekatan yang diambil kurang ideal

UCAPAN TERIMAKASIH

Terimakasih disampaikan kepada seluruh pihak yang telah mendukung terlaksananya penelitian dan membantu dalam penyusunan penelitian ini mulai dari awal hingga selesai.

REFERENCES

[1] L. Costaner and dan Musfawati, “ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING).”
[2] T. Revolino Syarif and D. Andri Jatmiko, “ANALISIS PERBANDINGAN METODE WEB SECURITY PTES, ISSAF DAN OWASP DI DINAS KOMUNIKASI DAN INFORMASI KOTA BANDUNG.”
[3] A. Hermawan1, T. Hartati2, and Y. A. Wijaya3, “Analisa Keamanan Data melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad,” vol. 7, no. 3, 2022.
[4] A. Elanda and R. Lintang Buana, “ANALISIS KEAMANAN SISTEM INFORMASI BERBASIS WEBSITE DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) VERSI 4: SYSTEMATIC REVIEW,” 2020. [Online]. Available: www.xyz.com
[5] D. Hariyadi and F. E. Nastiti, “Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta,” Jurnal Komtika (Komputasi dan Informatika), vol. 5, no. 1, pp. 35–42, Jul. 2021, doi: 10.31603/komtika.v5i1.5134.
[6] A. W. Kuncoro, J. Informatika, F. Rahma, and M. E. Jurusan Informatika, “Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review.” [Online]. Available: https://www.sciencedirect.com
[7] 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.
[8] A. Elanda and R. Lintang Buana, “ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10,” 2021.
[9] B. Subana and A. Fadlil, “Web Server Security Analysis Using The OWASP Mantra Method,” 2020. [Online]. Available: https://iocscience.org/ejournal/index.php/mantik/index
[10] “277-Article Text-1190-1-10-20220501”.
[11] I. M. Edy Listartha, I. M. A. Premana Mitha, M. W. Aditya Arta, and I. Km. W. Yuda Arimika, “Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project),” SIMKOM, vol. 7, no. 1, pp. 23–27, Jan. 2022, doi: 10.51717/simkom.v7i1.63.
[12] A. Kerentanan Keamanan, W. Menggunakan, D. Aryanti, N. Dan, and J. N. Utamajaya, “METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA,” 2021.
[13] I. Idris, M. U. Majigi, S. Abdulhamid, M. Olalere, and S. I. Rambo, “Vulnerability Assessment of Some Key Nigeria Government Websites.”
[14] M. Bach-Nutman, “Understanding The Top 10 OWASP Vulnerabilities.”
[15] “InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan”, doi: 10.30743/infotekjar.v4i2.2332.

BULLETIN OF INFORMATION TECHNOLOGY (BIT)
Vol 3, No 4, Desember 2022, Hal 308 - 316
ISSN 2722-0524 (media online)
DOI 10.47065/ bit.v3i1. 389
https://journal.fkpt.org/index.php/BIT

[16] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," Creative Information Technology Journal, vol. 4, no. 4, p. 264, Jan. 2019, doi: 10.24076/citec.2017v4i4.119.
[17] C Rizal, "Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server," Bulletin of Information Technology (BIT), p.27-33, 2022.