COSMIC JURNAL TEKNIK
VOL. 2, NO. 1, FEBRUARI 2024: 10-20
DOI : 10.55537/cosmic

Analisis Keamanan Pada *Website* UPM SAINTEK UIN-SU Medan Menggunakan Metode *Vulnerability Assesment*

Parlindungan Harahap[1], Ilka Zufria[2],
[1,2,3]Universitas Islam Negeri Sumatera Utara, Medan
E-mail: [1]parlinhrp289@gmail.com, [2]ilkazufria@uinsu.ac.id
Korespondensi : parlinhrp289@gmail.com

Abstrak

Saat ini, teknologi informasi memiliki peran yang sangat vital di berbagai sektor kehidupan, termasuk dunia bisnis, ekonomi, dan politik. Kehadiran teknologi sistem informasi saat ini memungkinkan pemenuhan kebutuhan masyarakat secara instan, memfasilitasi pengolahan data dengan lebih mudah, akurat, efektif, dan efisien. Meskipun demikian, perkembangan teknologi juga telah disalahgunakan oleh sejumlah pihak yang tidak bertanggung jawab, mengakibatkan kasus-kasus peretasan, penipuan, dan kejahatan siber yang menimpa individu, perusahaan, dan instansi pemerintah. Oleh karena itu, penelitian ini bertujuan untuk menganalisis dan menguji keamanan *website* Unit Penjamin Mutu Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan menggunakan metode *Vulnerability Assessment*, dengan menggunakan alat pemindaian kerentanan seperti *Owasp ZAP*. Penelitian menganalisis perlunya keamanan dalam menghadapi tantangan kejahatan siber yang semakin kompleks. Dengan memfokuskan pada metode *Vulnerability Assessment* dan menggunakan alat-alat seperti *Owasp ZAP* diharapkan dapat teridentifikasi dan diperbaiki potensi kerentanan *website* Unit Penjamin Mutu Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan. Upaya ini diharapkan dapat memberikan kontribusi positif dalam melindungi integritas dan keamanan data, mencegah potensi ancaman siber, dan meningkatkan kesadaran akan perlunya perlindungan informasi dalam lingkungan digital yang terus berkembang

Kata kunci: *website, vulnerability assessment, owaspZAP,* keamanan

Abstract

Currently, information technology has a very important role in various sectors of life, including the world of business, economics and politics. The presence of information system technology today makes it possible to meet people's needs instantly, facilitating data processing more easily, accurately, effectively and efficiently. However, technological developments have also been misused by a number of irresponsible parties, resulting in cases of hacking, fraud and cybercrime affecting individuals, companies and government agencies. Therefore, this research aims to analyze and test the security of the Quality Assurance Unit website of the Faculty of Science and Technology, North Sumatra State Islamic University, Medan using the Vulnerability Assessment method, using a vulnerability scanning tool such as Owasp ZAP. Research analyzes the need for security in facing increasingly complex cybercrime challenges. By focusing on the Vulnerability Assessment method and using tools such as Owasp ZAP, it is hoped that potential vulnerabilities can be identified and repaired on the website of the Quality Assurance Unit, Faculty of Science and Technology, North Sumatra State Islamic University, Medan. It is hoped that this effort can make a positive contribution in protecting data integrity and security, preventing potential cyber threats, and increasing awareness of the need to protect information in an ever-evolving digital environment.

Keywords: website, vulnerability assessment, owaspZAP, security

1. PENDAHULUAN

Perguruan tinggi di era digital ini tidak hanya diharapkan untuk memberikan pendidikan berkualitas, tetapi juga untuk membangun citra yang positif, meningkatkan *visibilitas*, dan berkomunikasi secara efektif dengan mahasiswa, calon mahasiswa, dosen, dan masyarakat umum.

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

Dalam konteks ini, *website* menjadi salah satu alat utama untuk mencapai tujuan tersebut. Melalui *website*, sebuah institusi pendidikan dapat menyampaikan informasi dengan cepat, menyeluruh, dan interaktif, sehingga menciptakan lingkungan komunikasi yang dinamis.[1]

Universitas Islam Negeri Sumatera Utara (UIN-SU) Medan, sebagai lembaga pendidikan tinggi yang terus berkembang, memiliki tanggung jawab untuk memastikan bahwa informasi terkini seputar kegiatan akademik dan prestasi mahasiswa dapat diakses dengan mudah oleh semua pihak yang berkepentingan. Fakultas Sains dan Teknologi, sebagai salah satu fakultas yang menawarkan program studi unggulan, memiliki kepentingan khusus dalam memperkuat citra positifnya dan menarik minat calon mahasiswa.[2]

Unit Penjamin Mutu (UPM) sebagai lembaga di dalam UIN-SU yang memastikan kualitas akademik dan peningkatan mutu pendidikan, diharapkan dapat menjadi ujung tombak dalam menyediakan informasi akurat dan relevan melalui media digital, yakni *website*. Evaluasi pemanfaatan *website* UPM tidak hanya relevan untuk meningkatkan kualitas komunikasi dan citra Fakultas Sains dan Teknologi, tetapi juga untuk memperkuat posisi UIN-SU Medan sebagai perguruan tinggi yang responsif terhadap perkembangan teknologi informasi.[3]

Dengan demikian, dengan latar belakang di di atas, maka di buatlah sebuah projek dengan judul : " Analisis Keamanan Pada *Website* UPM Saintek Uinsu Medan Menggunakan Metode *Vulnerability Assesment* ". Tujuan projek ini diharapkan dapat memberikan kontribusi pada pengembangan strategi komunikasi digital di lingkungan akademik, khususnya dalam konteks Fakultas Sains dan Teknologi di UIN-SU Medan. Hasil penelitian ini diharapkan dapat menjadi landasan bagi pihak terkait untuk meningkatkan kualitas dan efektivitas pemanfaatan *website* UPM sebagai alat penjamin mutu dan promosi fakultas SAINTEK UINSU medan.[4]

Dalam rangka meningkatkan tingkat keamanan *website*, Unit Penjamin Mutu Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan perlu melakukan evaluasi dan pemantauan secara berkala. Langkah-langkah proaktif, seperti penerapan metode keamanan informasi dan pemindaian kerentanan secara teratur, dapat membantu mengidentifikasi potensi risiko dan memitigasi potensi ancaman siber yang mungkin timbul. Kejahatan siber secara umum merujuk pada aktivitas kejahatan yang dilakukan dalam dunia maya dengan menggunakan jaringan komputer sebagai sarana dan internet sebagai medianya. Dalam konteks luas, kejahatan siber mencakup segala tindakan ilegal yang terjadi melalui jaringan komputer dan internet, bertujuan untuk meraih keuntungan dengan merugikan pihak lain. Dalam pengertian yang lebih spesifik, kejahatan siber merinci segala tindakan ilegal yang difokuskan pada serangan terhadap sistem keamanan komputer dan data yang diolah oleh suatu sistem komputer.[5]

Keamanan sistem informasi harus dijaga dari potensi ancaman, baik yang berasal dari internal maupun eksternal, yang dapat menyebabkan ketidakstabilan sistem. Ancaman tersebut bisa berasal dari berbagai sumber seperti mekanisme, organisasi, kelompok, atau individu, yang jika tidak diatasi dapat mengakibatkan gangguan dan kerusakan pada informasi dalam sistem. Upaya untuk menjaga keamanan sistem informasi harus dimulai dengan pemahaman dan prediksi ancaman potensial, karena serangan tidak akan terjadi tanpa adanya ancaman. Dengan melakukan prediksi ancaman sebelumnya, sistem dapat dijaga dan ketidakstabilan akibat serangan dapat diminimalisir dengan tindakan pencegahan yang telah dipertimbangkan sebelumnya.[6]

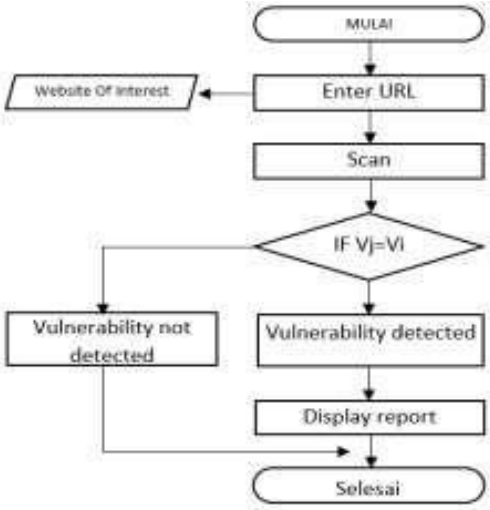
Vulnerability assessment merupakan suatu proses yang melibatkan definisi, identifikasi, dan prioritisasi kerentanan pada sistem komputer, aplikasi, dan infrastruktur jaringan. Tujuan dari proses ini adalah memberikan organisasi kemampuan untuk menilai dengan pengetahuan, kesadaran, dan pemahaman latar belakang risiko yang diperlukan, sehingga dapat memahami ancaman yang ada terhadap lingkungannya dan meresponsnya secara efektif. Secara umum, proses *vulnerability assessment* ini melibatkan penggunaan alat uji otomatis seperti pemindaian keamanan jaringan, dan hasilnya kemudian dicatat dalam laporan *vulnerability assessment*.[7]

2. METODE PENELITIAN

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

VOL. 2, NO. 1, FEBRUARI 2024: 10-20
DOI : 10.55537/cosmic

Penelitian ini menerapkan metodologi menggunakan metode *vulnerability assessment*. Proses *Vulnerability Assessment* terdiri dari empat tahap, yaitu *footprinting*, *vulnerability Scanning*, *Vulnerability Analysis*, dan *Result.* Berikut adalah flowchart tentang metode penelitian yang dilakukan menggunakan metode.[8]



Gambar 1. Vulnerabilty Assesment

Tahap pertama adalah *Footprinting*, yaitu proses mengumpulkan informasi tentang target, seperti alamat IP, domain, dan layanan yang berjalan. Informasi ini dapat diperoleh dengan berbagai cara, seperti menggunakan alat pencari, alat *network scanner*, dan alat whois.

Tahap kedua adalah *vulnerability scanning*, yaitu proses mendeteksi kerentanan pada target. Proses ini dilakukan menggunakan alat *vulnerability scanner* yang dapat mendeteksi berbagai jenis kerentanan, seperti kerentanan *software*, kerentanan configuration, dan kerentanan architectural.[9]

Tahap ketiga adalah *vulnerability analysis*, yaitu proses menganalisis kerentanan yang telah terdeteksi. Proses ini dilakukan untuk menentukan tingkat keparahan kerentanan dan dampak potensial dari serangan yang memanfaatkan kerentanan tersebut.

Tahap keempat adalah *Result*, yaitu tahap pendokumentasian hasil *vulnerability assessment*. Hasil ini dapat digunakan untuk menyusun rencana mitigasi kerentanan.

Berikut adalah penjelasan lebih lanjut tentang masing-masing tahap:

1. *Footprinting*

Tahap ini penting untuk dilakukan karena dapat memberikan gambaran umum tentang target. Informasi yang dikumpulkan pada tahap ini dapat digunakan untuk mempermudah proses *vulnerability scanning* dan *vulnerability analysis.*

2. *Vulnerability Scanning*

Tahap ini merupakan tahap yang paling penting dalam *vulnerability assessment*. Hasil *vulnerability scanning* akan menentukan kerentanan apa saja yang dimiliki target.

3. *Vulnerability Analysis*

Tahap ini penting untuk dilakukan untuk memastikan bahwa kerentanan yang terdeteksi benar-benar merupakan kerentanan yang signifikan. Selain itu, tahap ini juga penting untuk menentukan dampak potensial dari serangan yang memanfaatkan kerentanan tersebut.

4. *Result*

Tahap ini penting untuk dilakukan untuk mendokumentasikan hasil *vulnerability assessment*. Dokumentasi ini dapat digunakan untuk menyusun rencana mitigasi kerentanan.

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

COSMIC JURNAL TEKNIK
VOL. 2, NO. 1, FEBRUARI 2024: 10-20
DOI : 10.55537/cosmic

3. HASIL DAN PEMBAHASAN

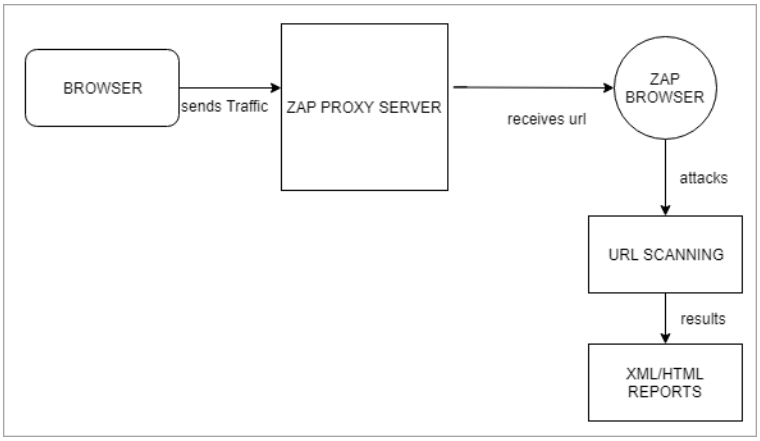
Vulnerability Scanning (OWASP ZAP)

Dalam rangka mengembangkan aplikasi web yang aman, pemahaman terhadap potensi serangan terhadap aplikasi tersebut menjadi krusial. Oleh karena itu, diperlukan suatu pendekatan keamanan, seperti pengujian penetrasi atau penetration testing. Meskipun banyak perusahaan memilih alat berbayar untuk tujuan keamanan, terdapat alternatif sumber terbuka yang sangat baik, yaitu *owaspZAP*. Alat ini mempermudah proses pengujian penetrasi bagi para pengujian, menjadi pilihan yang efektif dan hemat biaya.[10]

Keunggulan *ZAP*:

1. *Zap* menyediakan lintas platform, yaitu bekerja di semua OS (Linux, Mac, Windows)
2. *Zap* dapat digunakan kembali
3. Dapat menghasilkan laporan
4. Ideal untuk pemula
5. Alat gratis

ZAP membuat *server proxy* dan membuat lalu lintas situs web melewati server. Penggunaan pemindai otomatis di *ZAP* membantu mencegat kerentanan pada situs web.



Gambar 2. Diagram Alir ZAP

Sebelum kita mengatur konfigurasi *ZAP*, mari kita kenali beberapa istilah kunci *ZAP*:

1) Sesi (Session): Sesi mengacu pada navigasi situs web untuk mengenali area yang rentan terhadap serangan. Untuk mencapai ini, dapat menggunakan browser apa pun, seperti *Mozilla Firefox*, dengan mengonfigurasi pengaturan proksi. Alternatifnya, kita dapat menyimpan sesi *ZAP* sebagai file .session untuk digunakan kembali.

2) Konteks: Konteks yang dibuat dalam *ZAP* memungkinkan serangan terhadap aplikasi web atau sekelompok URL secara simultan, sementara mengabaikan yang lainnya, untuk menghindari pembacaan data yang berlebihan.

3) Jenis serangan *ZAP*: Laporan kerentanan dapat dihasilkan melalui berbagai jenis serangan *ZAP* dengan menekan dan melakukan pemindaian URL.

Vulnerability scanning

Vulnerability scanning adalah suatu proses yang melibatkan pengumpulan informasi menggunakan alat pemindai kerentanan seperti *OwaspZAP* dan *OpenVAS* di domain

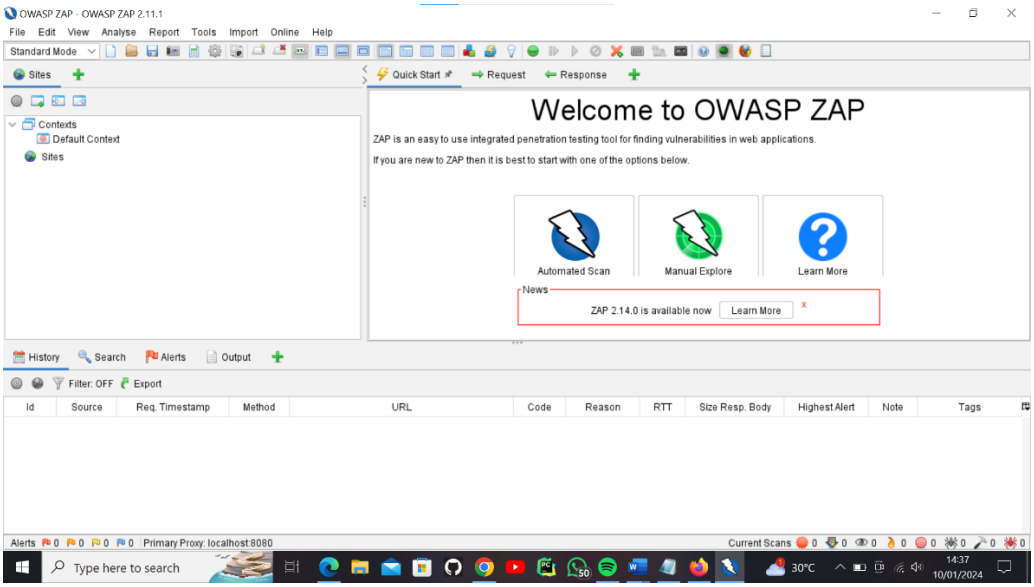
upmsaintek.uinsu.ac.id. Tujuan dari proses ini adalah untuk mengidentifikasi kelemahan yang mungkin ada dalam sistem. Proses ini menggunakan alat pemindai kerentanan yang secara otomatis melakukan pemindaian aplikasi untuk menemukan potensi celah keamanan yang dapat dimanfaatkan untuk pengembangan sistem atau kepentingan yang tidak diinginkan. Dalam

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

mencari celah keamanan, aplikasi pemindai kerentanan yang digunakan adalah *Owasp Zap*. Hasil dari pencarian celah keamanan akan diuraikan dalam subbab berikut:
Hasil pemindaian dengan dirsearch

Sistem kontrol ini memungkinkan akses terhadap informasi tanpa melalui proses autorisasi, yang berpotensi menyebabkan kebocoran informasi yang bersifat sensitif. Pengujian kontrol akses yang rusak pada situs web journal.unsika.ac.id dilakukan menggunakan alat dirsearch. Perintah yang digunakan adalah dirsearch upmsaintek.uinsu.ac.id <extensions>.
Hasil pemindaian *owaspZAP*.[11]

Melakukan pencarian kelemahan keamanan dengan alat OpenVAS menghasilkan beberapa temuan celah di alamat domain unsika.ac.id, yang nantinya akan diuraikan dalam sub-bagian berikut:
Tampilan home *OwaspZAP*

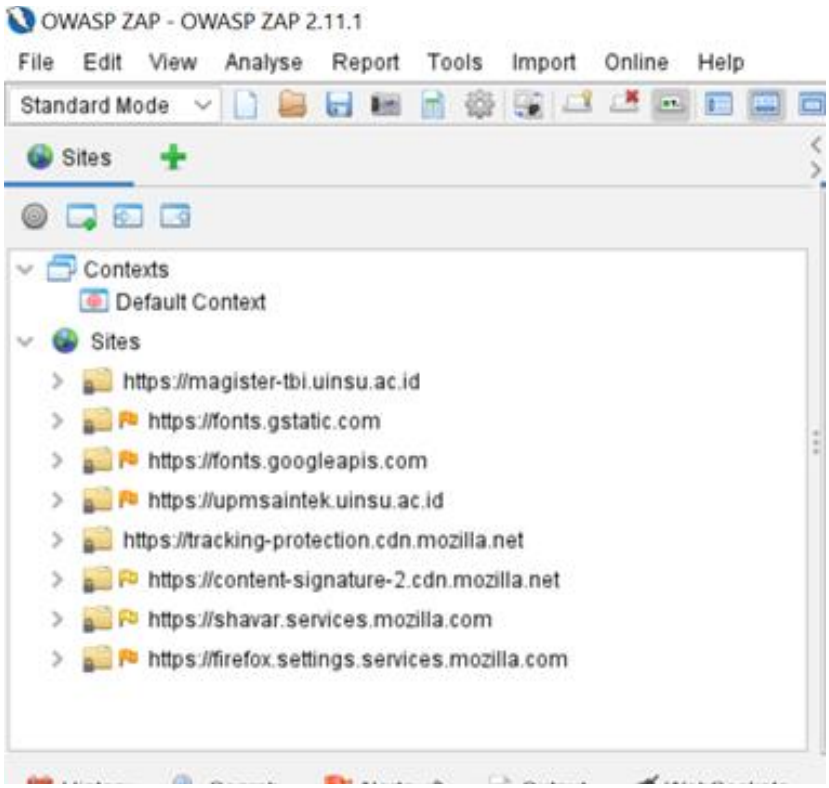


Gambar 3. Home OwaspZAP

Tampilan home *owaspZAP* adalah halaman utama yang ditampilkan saat aplikasi *ZAP* pertama kali diluncurkan. Halaman ini menyediakan akses ke berbagai fitur dan fungsi aplikasi, termasuk: Tab Status: Tab ini menampilkan informasi tentang status aplikasi *ZAP*, termasuk versi aplikasi, versi java, dan mode operasi.
Tab Scan: Tab ini memungkinkan anda untuk memulai pemindaian keamanan pada aplikasi web.
Tab Proxies: Tab ini memungkinkan anda untuk mengatur proxy *ZAP*, yang memungkinkan anda untuk memantau lalu lintas jaringan antara klien dan server.
Tab Options: Tab ini memungkinkan anda untuk mengonfigurasi opsi aplikasi *ZAP*, seperti daftar kerentanan yang ingin dicari.
Tab Tools: Tab ini menyediakan akses ke berbagai alat dan utilitas, seperti alat untuk menganalisis kode sumber dan alat untuk memanipulasi permintaan HTTP.

Hasil pemindaian *owaspZAP*
Pemindaian celah keamanan dengan alat *openVAS* mengungkapkan beberapa temuan kelemahan di domain upmsaintek.uinsu.ac.id yang akan dibahas lebih lanjut pada sub-bagian selanjutnya.

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)



Gambar 4. Hasil Scan ZAP

Pada gambar 4 menunjukkan bahwa domain umpsaintek.uinsu.ac.id\ telah bberhasil di pindai menggunakan aplikasi *owaspZAP* yang mana tersinkronisasi dnegan aplikasi peramban *mozila firefox.*

Vulnerability Analysis
Pada fase ini, dilakukan analisis terhadap celah keamanan yang terdeteksi selama proses *vulnerability scanning*, yang disajikan dalam bentuk tabel di bawah ini:

Tabel 1. Hasil Pengujian

Vulnerability Scanning	Alert	Risk Assessment
OwaspZAP	Cross-Domain Misconfiguration	Medium
	F Vulnerable JS Library	Medium
	X-Frame-Options Header not set	Medium
	Absence of Anti-CSRF Token	Low
	Incomplete or No Cache-control Header Set	Low
	Secure Pages Include Mixed Content	Low
	Timestamp Disclosure- Unix	Low
	X-Content-Type-Options Header Missing	Low
	Content-Type Header Missing	Informational
	F Information Disclosure - Suspicilss Comments	Informational

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

Result :

Tahap terakhir dalam melakukan vulnerability assessment adalah *result*. Berdasarkan hasil pengujian pada tahap *vulnerability scanning website* upmsaintek.uinsu.ac.id memiliki 10 kerentanan yang telah diuji. Terdapat 3 resiko *Medium*, 5 *Low* dan 2 *Informational*. Berikut hasil beberapa pengujian yang akan di sajikan pada tabel berikut:

Tabel 2. Hasil Analisis

Alert	Risk Assesment	Keterangan	Solusi
Cross-Domain Misconfiguration	Medium	Pemuatan data browser web mungkin terjadi karena kesalahan konfigurasi Cross Origin Resource Sharing (CORS) di server web	Pastikan bahwa data sensitif tidak tersedia dengan cara yang tidak diautentikasi (misalnya menggunakan daftar putih alamat IP). Konfigurasikan header HTTP "Access- Control-Allow-Origin" ke kumpulan domain yang lebih ketat, atau hapus seluruh header CORS, untuk memungkinkan browser web menerapkan Kebijakan Asal yang Sama (SOP) dengan cara yang lebih ketat.
Vulnerable JS Library	Medium	Bootstrap perpustakaan yang teridentifikasi, versi 4.3.0 rentan.	Silakan upgrade bootstrap ke versi terbaru.
X-Frame-Options Header not set	Medium	Header X-Frame- Options tidak disertakan dalam respons HTTP untuk melindungi terhadap serangan 'ClickJacking'.	Sebagian besar browser Web modern mendukung header HTTP X-Frame- Options. Pastikan ini diatur pada semua halaman web yang dikembalikan oleh situs Anda (jika Anda mengharapkan halaman tersebut hanya dibingkai oleh halaman di server Anda (misalnya, itu bagian dari FRAMESET) maka Anda sebaiknya menggunakan SAMEORIGIN, sebaliknya jika Anda tidak pernah mengharapkan halaman tersebut untuk dibingkai, Anda harus menggunakan DENY. Alternatifnya, pertimbangkan untuk menerapkan arahan "frame-ancestors" dari Kebijakan Keamanan Konten.
Absence of Anti-CSRF Token	Low	Tidak ada token Anti-CSRF yang ditemukan dalam formulir pengiriman HTML. Pemalsuan permintaan lintas situs adalah	Fase: Arsitektur dan Desain Gunakan perpustakaan atau kerangka kerja yang terverifikasi yang tidak memungkinkan terjadinya kelemahan ini atau menyediakan konstruksi yang

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

serangan yang memaksa korban untuk mengirim permintaan HTTP ke tujuan target tanpa sepengetahuan atau niat mereka untuk melakukan tindakan sebagai korban.
Penyebab utamanya adalah fungsionalitas aplikasi yang menggunakan tindakan URL/formulir yang dapat diprediksi secara berulang.
Sifat serangannya adalah CSRF mengeksploitasi kepercayaan yang dimiliki situs web terhadap pengguna. Sebaliknya, skrip lintas situs (XSS) mengeksploitasi kepercayaan yang dimiliki pengguna terhadap situs web. Seperti XSS, serangan CSRF tidak harus bersifat lintas situs, namun bisa juga terjadi.
Pemalsuan permintaan lintas situs juga dikenal sebagai CSRF, XSRF, serangan satu klik, sesi berkendara, deputi bingung, dan selancar laut.

Serangan CSRF efektif dalam beberapa situasi, termasuk:
* Korban memiliki sesi aktif di situs target.
* Korban diautentikasi melalui autentikasi HTTP di situs target.
* Korban berada di jaringan lokal yang sama dengan situs target.

CSRF terutama digunakan untuk melakukan tindakan terhadap situs target dengan menggunakan hak istimewa korban, namun Teknik terbaru telah ditemukan untuk mengungkapkan informasi dengan mendapatkan akses ke respons. Risiko pengungkapan informasi membuat kelemahan ini lebih mudah dihindari.
Misalnya, gunakan paket anti-CSRF seperti OWASP CSRFGuard.

Fase: Implementasi
Pastikan aplikasi Anda bebas dari masalah skrip lintas situs, karena sebagian besar pertahanan CSRF dapat dilewati menggunakan skrip yang dikendalikan penyerang.

Fase: Arsitektur dan Desain
Hasilkan nonce unik untuk setiap formulir, tempatkan nonce ke dalam formulir, dan verifikasi nonce setelah menerima formulir. Pastikan nonce tidak dapat diprediksi (CWE-330).
Perhatikan bahwa ini dapat dilewati menggunakan XSS.
Identifikasi operasi yang sangat berbahaya. Saat pengguna melakukan operasi berbahaya, kirimkan permintaan konfirmasi terpisah untuk memastikan bahwa pengguna bermaksud melakukan operasi tersebut.
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. Hal ini dapat merusak fungsi yang sah, karena pengguna atau proxy mungkin telah menonaktifkan pengiriman Perujuk karena alasan privasi.

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

		meningkat secara dramatis ketika situs target rentan terhadap XSS, karena XSS dapat digunakan sebagai platform untuk CSRF, sehingga memungkinkan serangan beroperasi dalam batas-batas kebijakan asal yang sama.	
Incomplete or No Cache-control Header Set	Low	Header kontrol cache belum disetel dengan benar atau hilang, sehingga memungkinkan browser dan proksi menyimpan konten dalam cache.	Kapan pun memungkinkan, pastikan header HTTP kontrol cache disetel dengan no- cache, no-store, must-revalidate.
Secure Pages Include Mixed Content	Low	Halaman tersebut berisi konten campuran, yaitu konten yang diakses melalui HTTP, bukan HTTPS.	Halaman yang tersedia melalui SSL/TLS harus seluruhnya 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.
Timestamp Disclosure- Unix	Low	Stempel waktu diungkapkan oleh aplikasi/server web - Unix	Konfirmasikan secara manual bahwa data stempel waktu tidak sensitif, dan bahwa data tidak dapat dikumpulkan untuk mengungkapkan pola yang dapat dieksploitasi.
X-Content-Type- Options Header Missing	Low	Konfirmasikan secara manual bahwa data stempel waktu tidak sensitif, dan bahwa data tidak dapat dikumpulkan untuk mengungkapkan pola yang dapat dieksploitasi.	Pastikan aplikasi/server web menyetel header Tipe Konten dengan tepat, dan menyetel header 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 tidak melakukan sniffing MIME sama sekali, atau yang dapat diarahkan oleh aplikasi web/server web untuk tidak melakukan sniffing MIME.
Content-Type Header Missing	Informational	Header Tipe Konten hilang atau kosong.	Pastikan setiap halaman menyetel nilai tipe konten yang spesifik dan sesuai untuk konten yang dikirimkan.

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

4. KESIMPULAN DAN SARAN

Studi ini menguraikan analisis keamanan yang dilakukan terhadap *website* UPM SAINTEK UIN-SU Medan menggunakan metode *Vulnerability Assessment*. Melalui proses ini, berbagai kerentanan dan celah keamanan berhasil diidentifikasi dan dianalisis dengan menggunakan alat-alat seperti *OwaspZAP* dan *OpenVAS*. Temuan-temuan tersebut mengungkap potensi risiko keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab, dan memberikan pemahaman mendalam tentang kondisi keamanan website tersebut. Penerapan metode *Vulnerability Assessment* membantu dalam peningkatan keamanan secara proaktif dengan memberikan wawasan yang diperlukan untuk memperbaiki dan memitigasi potensi ancaman keamanan. Hasil analisis memberikan dasar yang kuat untuk pihak terkait, seperti pengelola *website*, untuk mengambil langkah-langkah korektif yang diperlukan guna meningkatkan keamanan sistem. Langkah-langkah ini termasuk memperbarui perangkat lunak, menutup celah keamanan yang teridentifikasi, dan mengimplementasikan kebijakan keamanan yang lebih ketat. Dengan demikian, melalui penerapan metode *Vulnerability Assessment*, studi ini memberikan kontribusi positif dalam upaya menjaga keamanan website UPM SAINTEK UIN-SU Medan, serta memberikan landasan bagi pengembangan strategi keamanan yang lebih efektif di masa depan.

DAFTAR PUSTAKA

[1] S. Devella, Y. Yohannes, and N. Rachmat, "Pelatihan Pembuatan Website Sekolah Menggunakan Wordpress Untuk Guru Tik Sma Negeri 17 Palembang," *SELAPARANG J. Pengabdi. Masy. Berkemajuan*, vol. 4, no. 2, pp. 406–411, 2021, [Online]. Available: https://journal.ummat.ac.id/index.php/jpmb/article/view/4488

[2] M. S. Hasibuan and A. Serdano, "Analisis Sentimen Kebijakan Pembelajaran Tatap Muka Menggunakan Support Vector Machine dan Naive Bayes," *JRST (Jurnal Ris. Sains dan Teknol.*, vol. 6, no. 2, pp. 199–204, 2022, [Online]. Available: https://jurnalnasional.ump.ac.id/index.php/JRST/article/view/15145

[3] I. Zufria and M. H. Azhari, "Web-Based Applications in Calculation of Family Heritage (Science of Faroidh)," *Query J. Inf. Syst.*, vol. 1, no. 01, 2017, [Online]. Available: http://jurnal.uinsu.ac.id/index.php/query/article/view/659

[4] F. Ismawan, N. Isnain, and R. A. Raharjo, "Pemanfaatan website berbasis cms-wordpress sebagai media pembelajaran guru tk binakheir cibinong–bogor," *J. PkM Pengabdi. Kpd. Masy.*, vol. 3, no. 1, pp. 68–77, 2020, [Online]. Available: https://journal.lppmunindra.ac.id/index.php/pkm/article/view/4271

[5] M. S. Hasibuan and L. M. Gultom, "Analisis Serangan Deface Menggunakan Backdoor Shell Pada Website," *Techno. Com*, vol. 17, no. 4, pp. 415–423, 2018, [Online]. Available: http://publikasi.dinus.ac.id/index.php/technoc/article/view/1887

[6] M. S. Hasibuan, "Keylogger pada Aspek Keamanan Komputer," *J. Teknovasi J. Tek. dan Inov. Mesin Otomotif, Komputer, Ind. dan Elektron.*, vol. 3, no. 1, pp. 8–15, 2018, [Online]. Available: https://www.academia.edu/download/57110625/73-144-1-SM.pdf

[7] R. Hisbullah and M. S. Hasibuan, "Pendekatan Bayes-HDSS dalam Menentukan Status Pantauan Gizi Balita," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 5, pp. 1071–1082, 2023, [Online]. Available: https://jtiik.ub.ac.id/index.php/jtiik/article/view/7437

[8] I. Zufria, H. Santoso, and D. Darsih, "Sistem Pakar Menggunakan Metode Backward Chaining Untuk Mengantisipasi Permasalahan Tanaman Kacang Kedelai Berbasis Web," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 5, no. 1, pp. 20–28, 2021, [Online]. Available: http://tunasbangsa.ac.id/ejurnal/index.php/jsakti/article/view/294

[9] I. Zufria, A. H. Hasugian, M. S. Hasibuan, and A. H. Lubis, "Literasi Digital: Pemanfaatan dan Penggunaan E-Library Menggunakan Software SLiMS" di Desa Denai Lama, Pantai

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

Labu-Deli Serdang," *J. Pengabdi. Masy.*, vol. 1, no. 1, pp. 1–10, 2022, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/japamas/article/view/7

[10] M. S. Hasibuan and I. Idris, "Intelligent LPG gas leak detection tool with SMS notification," in *Journal of Physics: Conference Series*, IOP Publishing, 2019, p. 12020. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1424/1/012020/meta

[11] A. W. Panjaitan, I. Zufria, and Y. R. Nasution, "Implementation Of Data Encryption Standard (Des) Algorithm For Data Security On Pdf Documents," *ZERO J. Sains, Mat. dan Terap.*, vol. 6, no. 2, pp. 231–236, 2023, [Online]. Available: http://jurnal.uinsu.ac.id/index.php/zero/article/view/17365/0

© 2024 The Author(s). Published by AIRA . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)