Analisis Keamanan Aplikasi berbasis WEB Menggunakan Tolls Arachni

PROPOSAL RISET INFORMATIKA

Muhammad Zenith Dzikrul Haqiqi NPM 21083010298

DOSEN PENGAMPU:
Dr. Basuki Rahmat, S.Si. MT.

Program Studi Informatika
Fakultas Ilmu Komputer
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Tahun 2024

Analisis Keamanan Aplikasi berbasis WEB Menggunakan Tolls ZAP

ABSTRAK

ini membahas tentang analisa keamanan aplikasi berbasis web, pada era digital saat ini, berkembangnya teknologi memudahkan menerima informasi dari berbagai sumber melalui internet. Namun, semakin meningkatnya teknologi pada informasi dan komunikasi juga muncul ancaman yang menyerang kerentanan sistem. Berdasarkan data statistik laporan anomali traffic yang terjadi di Indonesia berjumlah 21.420.466 traffic. Oleh karena itu, peningkatan keamanan sistem menjadi penting sebagai upaya untuk melindungi sistem dari anomali dan ancaman yang tidak diinginkan. maka dari itu diperlukannya evaluasi kemanan dengan menggunakan metode Vulnerability Assesment (VA), Arachni adalah tools yang cocok digunakan dalam evaluasi keamanan, penelitian ini berhasil menemukan 291 kerentanan pada beberapa web Diskominfo, kerentanan akan dianalisa menggunakan pendekatan OWASP top 10 dan akan diuji coba untuk menghasilkan profil keamanan dan bukti kerentanan yang valid. Hasil peneltian ini VA adalah salah satu metode yang cocok untuk menganalisa keamanan pada aplikasi web www.farismunir.my.id, serta profil keamanan yang harus menjadi perhatian adalah pengelolaan hak akses direktori dan file yang ada pada website.

Kata Kunci: Kerentanan, Evaluasi, ZAP, OWASP, Website, Keamanan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1 PENDAHULUAN

1.1. Latar Belakang

Perkembangan Teknologi Informasi dan Komunikasi secara pesat di Indonesia sekarang ini membuat kemudahan memperoleh serta melihat data yang ada di internet semakin mudah. Informasi secara terpusat ini ditulis dalam website yang dipublikasikan melalui internet yang dengan mudah ditemukan di mana saja. Aplikasi yang berkolaborasi dengan website diminati karena fleksbilitas akses dari aplikasi, dibanding dengan aplikasi lain, dan aplikasi berbasis web ini sangat ringan untuk digunakan tidak seperti aplikasi yang lain. Hal tersebut membuat bertambahnya jumlah penggunaan layanan aplikasi berbasis web dari tahun ke tahun, karena hanya menggunakan internet menampilkan aplikasi berbasis website yang dapat memudahkan pengguna dalam menerima informasi bahkan sampai bertukar informasi. Di era digital seperti sekarang para instansi atau organisasi organisasi semakin yakin untuk membuat aplikasi berbasis website yang mempermudah instansi atau organisasi dalam melakukan input data dan menampilkan berbagai macam infomasi untuk para penggunanya.

Kebergantungan sarana informasi menggunakan aplikasi berbasis website menjadikan isu kerentanan keamanan website saat ini sedang marak maraknya terjadi di Indonesia, banyak website yang setiap harinya tanpa sadar disusupi oleh aktivitas anomali yang diluar dari kinerja website itu sendiri. Dari data Id-SIRTII (Indonesia Security Incident Response Team On Internet Infrastructure / Coordination Center), traffic yang berpotensi memiliki anomali sejumlah 21.420.466 traffic. Data tersebut menyadarkan para pengguna internet dan perusahaan yang mengembangkan aplikasi berbasis web bahwa begitu banyak ancaman bagi sistem yang mereka gunakan dan data pribadi pengguna maupun data perusahaan. Tentu data-data pengguna dan perusahaan yang ada di website tersebut menjadi sasaran empuk apabila tidak mementingkan pada sisi keamanannya. Bocornya data membuat kerugian yang sangat besar bagi perusahaan, apabila data yang bocor dimiliki pihak yang tidak bertanggung jawab, dapat berdampak buruk dan dapat merugikan banyak pihak. Dampak kebocoran data ini akan menimbulkan

stigma bahwa tingkat keamanan sistem yang ada di Indonesia masih lemah, hal ini membuat pengguna layanan enggan menggunakan cara digital karena data yang akan diolah memiliki potensi mengalami kebocoran. Maka dari itu kini pengembang dan publisher website harus menentukan cara bagaimana mencegah kerentanan pada sistem mereka, metode apa yang akan mereka gunakan untuk mencari informasi tentang kerentanan sistem mereka. perusahaan yang mengembangkan aplikasi berbasis website memiliki peran untuk menguji coba setiap website yang dimiliki, bahkan melakukan uji coba keamanan bagi website baru atau pembaruan website menjadi sebuah kewajiban untuk memperkecil kerentanan yang ada.

.

Uji coba kerentanan memiliki beberapa tahapan Vulnerability Assesment. Vulnerability assessment dapat mendefinisikan, mengidentifikasi, mengelompokkan dan memprioritaskan kerentanan dalam sistem web[4]. Tentunya Vulnerability Assesment harus di uji coba untuk memeriksa kebenarannya, karena beberapa tools Vulnerability Assesment memiliki sifat False Positive. Dengan adanya data kerentanan pengelola dapat melakukan pengukuran resiko kerentanan menggunakan pendekatan Open Web Aplication Security Project (OWASP) untuk mengetahui penanganan dan kategori kerentanan yang ada.

Penelitian ini akan melakukan analisa kerentanan ke www.farismunir.my.id.untuk dilakukannya analisa menggunakan tools Vulnerability Assesment berupa Arachni dengan berfokus pada keamanan dari aplikasi berbasis website, dan hasil dari Vulnerability Assesment akan dilakukan uji coba dan dianalisa menggunakan pendekatan OWASP oleh peneliti setelah itu akan dikembangkan oleh pihak Faris Munir Mahdi untuk meminimalisir kerentanan yang ada pada WEB www.farismunir.my.id.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang ada peneliti akan Menentukan metode untuk Analisa keamanan aplikasi berbasis web Menentukan metode untuk Analisa

keamanan aplikasi berbasis web, dan Bagaimanakah profil keamanan dari aplikasi berbasis web di www.farismunir.my.id.

1.3. Batasan Masalah

1. Metode Analisa keamanan berbasis web ini tidak dilakukan secara manual dan hanya dilakukan secara automated (temuan Arachni).
2. Pengujian sistem keamanan aplikasi web menggunakan Teknik Blackbox.
3. Peneliti tidak menguji bagian database, OS, dan jaringan, melainkan hanya aplikasi web.
4. Peneliti hanya menggunakan pendekatan OWASP, dan tidak keseluruhannya, hanya yang memiliki kaitan dengan aplikasi web.
5. Peneliti mendapatkan website www.farismunir.my.id. yang sudah mendapat izin untuk diteliti

1.4. Tujuan Penelitian

Peneliti memiliki tujuan dari penelitian ini sebagai berikut.

1. Menentukan metode analisia keamanan aplikasi berbasis web.
2. Mengetahui profil keamanan dari aplikasi berbasis web.

1.5. Manfaat Penelitian

1) Manfaat teoritis

   Memberikan pemahaman tentang konsep keamanan aplikasi WEB serta mendukung penelitian dan pengembangan metode keamanan web menggunakan Tools ZAP.

2) Manfaat praktis

   Dapat membantu pemilik aplikasi WEB untuk membantu mempercapat deteksi keamanan dan membantu mengamankan aplikasi WEB .

BAB 2 LITERATUR REVIEW

2.1. Review Penelitian Sebelumnya

Review penelitian sebelumnya adalah langkah awal yang penting dalam menentukan bagaimana penelitian Anda akan berkontribusi pada bidang ini dan mengatasi tantangan yang mungkin muncul berdasarkan temuan-temuan sebelumnya.

Tabel 2. 1 Tabel studi literatur yang relevan

No	Profil Pustaka	Metode dan Temuan
1	**Judul:** *Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners.* **Penulis:** Khaled Abdulghaffar, Nebrase Elmrabit, Mehdi Yousefi. **Jurnal/Prosiding:** MDPI (Multidisciplinary Digital Publishing Institute)	**Metode:** Peneliti mengembangkan kerangka kerja yang mengintegrasikan dua alat pemindai kerentanan, Arachni dan OWASP ZAP, dengan algoritma untuk mengotomatisasi proses pemindaian dan menggabungkan hasilnya. Efektivitasnya dievaluasi menggunakan metrik recall dan F-measure. **Temuan:** Berdasarkan hasil penelitian didapatkan bahwa Kombinasi alat pemindai di dalam kerangka kerja menghasilkan tingkat deteksi kerentanan yang lebih tinggi dibandingkan jika menggunakan satu alat pemindai saja, dan dari hasil pengukuran Daftar gabungan kerentanan yang dihasilkan dari kerangka kerja memiliki skor **recall** dan **F-measure** yang lebih baik. **Kelebihan :** Dengan mengintegrasikan beberapa pemindai, kerangka kerja mampu memberikan analisis keamanan yang lebih menyeluruh, sehingga mengurangi kemungkinan kerentanan yang tidak terdeteksi.. Otomasi dapat meningkatkan efisiensi pengujian, memungkinkan prosedur yang konsisten dan dapat diulang.

No	Profil Pustaka	Metode dan Temuan
		Kekurangan : Kerangka kerja masih menghasilkan sejumlah hasil positif palsu, yang merupakan kelemahan umum pada teknik pemindaian otomatis. Efektivitas kerangka kerja sangat bergantung pada kemampuan pemindai yang digunakan (Arachni dan OWASP ZAP). Keterbatasan bawaan dari alat tersebut dapat memengaruhi kinerja secara keseluruhan. Penelitian hanya menggunakan dua alat pemindai. Jika lebih banyak alat pemindai ditambahkan, hasil yang berbeda mungkin akan diperoleh .
2	**Judul:** *Vulnerability Assesment Dan Penetration Testing (VAPT) Menggunakan Metode Zero Entry Hacking (ZEH) Terhadap Website* **Penulis:** Muhammad Yaqi **Jurnal/Prosiding:** Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta	**Metode:** Penelitian ini menggunakan metode VAPT untuk mengidentifikasi kerentanan keamanan pada website Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan dengan menggunakan Metode adalah Zero Entry Hacking (ZEH), yang berfokus pada eksploitasi kerentanan tanpa memerlukan akses awal ke sistem. **Temuan:** Ditemukan beberapa kerentanan yang signifikan, termasuk SQL Injection, Cross-Site Scripting (XSS), dan kelemahan pada autentikasi pengguna. Penelitian mengungkapkan bahwa konfigurasi keamanan pada website masih lemah dan perlu ditingkatkan untuk mencegah akses tidak sah dan serangan. Kerentanan yang ditemukan telah divalidasi untuk memastikan bahwa hasil pemindaian benar dan relevan.

No	Profil Pustaka	Metode dan Temuan
		Kelebihan : Metode ZEH efektif untuk mengidentifikasi kerentanan yang spesifik dan kritis tanpa memerlukan informasi akses awal. Kerentanan yang ditemukan divalidasi dengan eksploitasi langsung untuk memastikan keakuratannya. Penelitian ini memberikan wawasan kepada pengelola website mengenai pentingnya pengujian keamanan dan konfigurasi yang tepat. **Kekurangan :** Penelitian hanya dilakukan pada satu website, sehingga hasilnya mungkin tidak dapat digeneralisasi ke sistem lain. Hasil penelitian sangat bergantung pada alat seperti OWASP ZAP, yang memiliki keterbatasan dalam mendeteksi kerentanan tertentu. Alat pemindai dapat menghasilkan hasil positif palsu yang memerlukan validasi manual untuk memastikan keakuratannya.
3	**Judul:** *Analisis Keamanan Aplikasi Web Prodi Teknik Informatika UIKA Menggunakan Acunetix Web Vulnerability* **Penulis:** Febri Al Fajar **Jurnal/Prosiding:** Jurnal Inovatif: Inovasi Teknologi Informasi dan Informatika.	**Metode:** Penelitian ini melakukan audit dan analisis aspek keamanan terhadap Aplikasi Web Prodi Teknik Informatika UIKA, penelitian ini Menggunakan Acunetix Web Vulnerability Scanner, sebuah perangkat lunak yang secara otomatis memindai aplikasi web untuk mengidentifikasi kerentanan seperti SQL Injection dan Cross-Site Scripting (XSS) **Temuan:** Hasil pengujian menemukan berbagai tingkat kerentanan, mulai dari level **Low** pada domain utama hingga level **High** pada subdomain fakultas.

No	Profil Pustaka	Metode dan Temuan
		Jenis Kerentanan: Kerentanan yang ditemukan meliputi SQL Injection, Cross-Site Scripting (XSS), dan beberapa peringatan web lainnya. **Kelebihan :** Penggunaan Acunetix memungkinkan identifikasi kerentanan spesifik yang mungkin tidak terdeteksi tanpa alat pemindaian otomatis. Penelitian menghasilkan laporan audit keamanan yang dapat digunakan sebagai referensi bagi pengembang aplikasi untuk meningkatkan keamanan sistem . **Kekurangan :** Meskipun Acunetix efektif, alat otomatis mungkin tidak mendeteksi semua jenis kerentanan, terutama yang memerlukan analisis manual. Seperti alat pemindaian lainnya, Acunetix mungkin menghasilkan false positives (peringatan palsu) atau false negatives (gagal mendeteksi kerentanan yang ada)

2.2 Dasar Teori

Dalam penelitian ini, dasar teori digunakan untuk memberikan landasan ilmiah terhadap analisis dan implementasi yang dilakukan. Beberapa teori yang menjadi acuan adalah sebagai berikut.

2.2.1. Aplikasi Berbasis Website

Website adalah contoh dari salah satu media yang memiliki banyak halaman dan saling berkaitan antara halaman utama dan halaman menu pada website, website juga dapat menampilkan informasi dengan berbagai macam bentuk, mulai dari tulisan berupa teks, gambar, dokumen, video, suara, dan animasi. Dalam satu website dapat di atur posisi dan media apa saja yang digunakan untuk memberikan kenyamanan penyampaian informasi kepada pengguna website. Website memiliki komponen berupa domain yang berfungsi merubah alamat website dari angka menjadi nama serta menampilkan alamat dari website (URL), Hosting berfungsi sebagai media penyimpanan bagi website. Untuk mengembangkan situs web dalam mode penerbitan Internet, diperlukan beberapa aplikasi yaitu Web Server, Database, dan Browser.

Aplikasi berbasis web adalah aplikasi yang dibuat dengan mengimplemetasikan bahasa pemrograman HTML, PHP, CSS, JS untuk membuat website dan memerlukan web server sebagai wadah dan browser untuk menjalankannya, seperti Chrome, Firefox atau Opera, Internet Explorer, Microsoft Edge dan browser lainnya. Aplikasi web merupakan salah satu website dengan ekosistem yang terstruktur dalam bentuk program dan infrastruktur komputer yang memungkinkan pengguna website bisa melakukan interaksi serta menampilkan data dari suatu database server, dengan cara menggunakan fitur yang ada didalamnya melalui koneksi internet dan mengaksesnya menggunakan alamat website yang dimasukan ke browser. Kemudian data yang sudah dimasukan akan ditampilkan kembali ke pengguna website sebagai informasi yang dihasilkan secara dinamis oleh aplikasi web melalui web browser. Berbeda dengan aplikasi APK yang mana program APK harus melakukan instalasi pada perangkat, aplikasi web ini dapat di akses dan digunakan hanya menulis alamat website menggunakan

browser dengan jaringan internet maupun jaringan lokal yang disediakan oleh perusahaan. Penggunaan aplikasi berbasis web memudahkan pemusatan informasi yang ada di perusahaan untuk disebar luaskan ke pengguna layanan aplikasi web, informasi akan ditampilkan dalam sebuah tampilan website untuk mempercepat kinerja perusahaan dan pertukaran informasi. Selain itu kegunaan dari aplikasi web ini adalah pemusatan data, data yang terpusat dan kemudahan akses data adalah fitur utama yang membuat aplikasi web lebih populer dan lebih mudah diterapkan di berbagai bidang kehidupan.

2.2.2. Konsep Keamanan Aplikasi Berbasis WEB

Menurut Kamus Besar Bahasa Indonesia, kata dasar keamanan atau aman memiliki arti bebas dari ancaman, bahaya, dan bebas dari gangguan. Keamanan memiliki arti dalam keadaan aman atau dalam keadaan ketentraman. Keamanan aplikasi web adalah sebuah gagasan untuk menciptakan website sesuai dengan fungsinya meskipun website sedang diganggu. Konsep ini mengandalkan kontrol keamanan yang direkayasa ke dalam sistem aplikasi web untuk melindungi asset dan datanya dari orang yang tidak dikenal dan berpotensi berbuat jahat. Keamanan aplikasi web adalah pengelolaan sumber daya, termasuk alat, infrastruktur, dan data komputer, untuk melindungi sifat kerahasiaan, integritas, dan ketersediaan informasi dengan mengimplementasi aplikasi penunjang, pendidikan terkait keamanan, dan teknologi yang digunakan sesuai dengan pedoman teknis yang berlaku. Terdapat 4 klasifikasi keamanan pada sebuah sistem yaitu :

1. Keamanan Fisik

   Keamanan yang berfokus pada pihak external termasuk pihak yang berkaitan dengan alat dan media yang digunakan untuk menjalankan sistem.

2. Keamanan Sosial

   Keamanan yang berfokus kepada pereorangan dan pihak internal, kerentanan ini berkaitan dengan indentitas dan profil dari pihak yang memiliki akses, karena semua asset dan data bergantung pada pemegang akses.

3. Keamanan Data

   Keamanan yang berfous untuk mengolah data, menyimpan data dan akses data, kerentanan ini berkaitan dengan data yang dimodifikasi serta penambahan dan pengurangan data.Keamanan Sosial.

4. Keamanan Operasi

Keamanan yang berfous pada prosedur atau aturan yang berlaku untuk mengatur dan mengelola keamanan pada sistem. Namun kelemahan sistem aplikasi berbasis web masih ada dan bisa saja menjadi senjata yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab, menjadikan kelemahan pada sistem aplikasi berbasis web sebuah kerentanan yang sangat berbahaya.

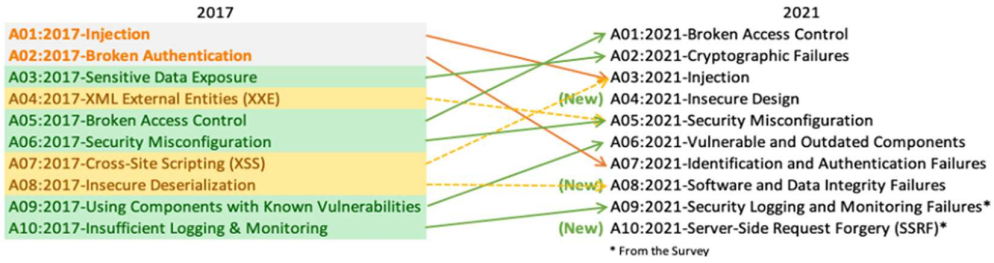
2.2.3. Kerentanan Aplikasi WEB

Menurut Kamus Besar Bahasa Indonesia, kata dasar kerentanan atau rentan memiliki arti mudah terinfeksi, dan peka atau mudah merasa. Kerentanan sendiri memiliki arti mudah terinfeksinya sesuatu yang menghasilkan akibat yang tidak diduga secara tiba - tiba. Kerentanan aplikasi web adalah kelemahan yang dapat disalahgunakan dan memiliki dampak yang mempengaruhi kinerja, data dan informasi yang ada di aplikasi berbasis web secara tiba tiba dan tidak diketahui. Rendahnya kesadaran akan kemanan siber pada pengguna dan pembuat aplikasi berbasis web membuat kerentanan dapat dengan mudah ditemukan. Apabila kerentanan tidak dapat dikendalikan maka akan dapat merugikan semua pihak yang berkaitan dengan sistem tersebut. Keberagaman serangan dan ancaman dari luar ada banyak sekali perlu di ketahui beberapa tipe dan jenis serangan yang ada, untuk mengetahui langkah pencegahan serangan dan ancaman.

2.2.4. Open WEB Aplication Security Project (OWASP)

Open Worldwide Application Security Project (OWASP) adalah komunitas terbuka yang membahas secara detail bagaimana untuk mempermudah instansi untuk menyusun, mengembangkan, memperoleh, mengoperasikan, dan memelihara aplikasi yang aman dan optimal. Semua yang ada dalam OWASP seperti, alat, dokumen, forum, bersifat gratis dan terbuka bagi siapa saja yang tertarik untuk meningkatkan keamanan aplikasi.

OWASP sering menampilkan top 10 kerentanan aplikasi berbasis web yang sering terjadi di dunia berdasarkan survey dari komunitas OWASP yang ada. Data top 10 kerentanan yang terjadi di dunia tahun 2021 seperti gambar berikut.



Gambar 2. 1 Top 10 kerentanan OWASP

Kategori yang ada pada map top 10 dari OWASP adalah :

A01:2021-*Broken Access Control*.

A02:2021-*Cryptographic Failures*.

A03:2021-*Injection*.

A04:2021-*Insecure Design*.

A05:2021-*Security Misconfiguration*.

A06:2021-*Vulnerable and Outdated Components*.

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*.

OWASP menjadi pedoman dan perbandingan kerentanan yang ditemukan oleh Arachni dengan data top 10 OWASP untuk menentukan kerentanan mana saja yang paling sering disalahgunakan dan sedang marak terjadi, untuk meningkatkan resistensi serangan yang sedang marak.

2.2.5. Vulnerability Assasment (VA)

Vulnerability Assesment (VA) adalah analisis keamanan yang komprehensif dan mendalam seperti keamanan informasi, hasil analisis jaringan, metode manajemen, konfigurasi sistem, kesadaran keamanan aktor terkait dan keamanan fisik, untuk mengembangkan identifikasi semua potensi.

kelemahan serius yang ada. VA menjadi alat untuk pengembang website dan sistem untuk mencari kerentanan dari sistem dan web yang sedang masa testing, dengan cara kerja yang berfokus untuk mencari semua kerentanan pada subjek sistem yang menggunakan jaringan baik internet maupun lokal. VA juga merupakan bagian dari manajemen preventif dalam pengendalian keamanan TI secara keseluruhan, VA menjadi metode untuk manajemen keamanan yang reliable dan selayaknya deteksi dengan IDS (Intrusion Detection System) dan pencegahan dengan firewall dan antivirus. Waktu yang tepat untuk melakukan VA adalah pada saat masa implementasi sistem atau program baru pada sistem utama, idealnya VA sebaiknya dilakukan secara kontiniu, dan dilakukan secara berkala agar mengetahui keberadaan kerentanan yang ada pada sistem. Sangat berbahaya apabila ada pihak lain yang dapat melakukan eksploitasi untuk membongkar sistem melalui kerentanan yang tidak di sadari lebih dulu oleh pihak pengembang dan pengelola.

2.2.6. Tolls Arachni

Arachni adalah salah satu Web Aplication Vulnerability Scanner (WAVS) yang bersifat open source dan gratis. Arachni dapat menelusuri kerentanan setiap jalur yang ada pada sistem web sampai ke sistem yang menjalankan web itu sendiri.

Arachni unggul dalam mengidentifikasi kerentanan dari daftar OWASP 2021, menjadikannya aset berharga dalam meningkatkan keamanan aplikasi web. Arachni di bangun menggunakan bahasa pemrograman Ruby dan dapat berjalan di beberapa platform seperti Windows, Linux dan Mac OS, akan tetapi untuk mendapatkan potensi maksimalnya dianjurkan untuk menggunakan Linux. Arachni merubah namanya menjadi Codename SCNR dan kini berbayar, namun source code untuk menggunakan Arachni masih bisa digunakan pada laman github https://github.com/Arachni.

Pemilihan Arachni sebagai alat dalam menganalisa keamanan aplikasi berbasis web karena Arachni adalah salah satu tools yang powerfull¸serta mudah penggunaan dan pemasangannya. Selain itu tampilan Arachni termasuk tampilan

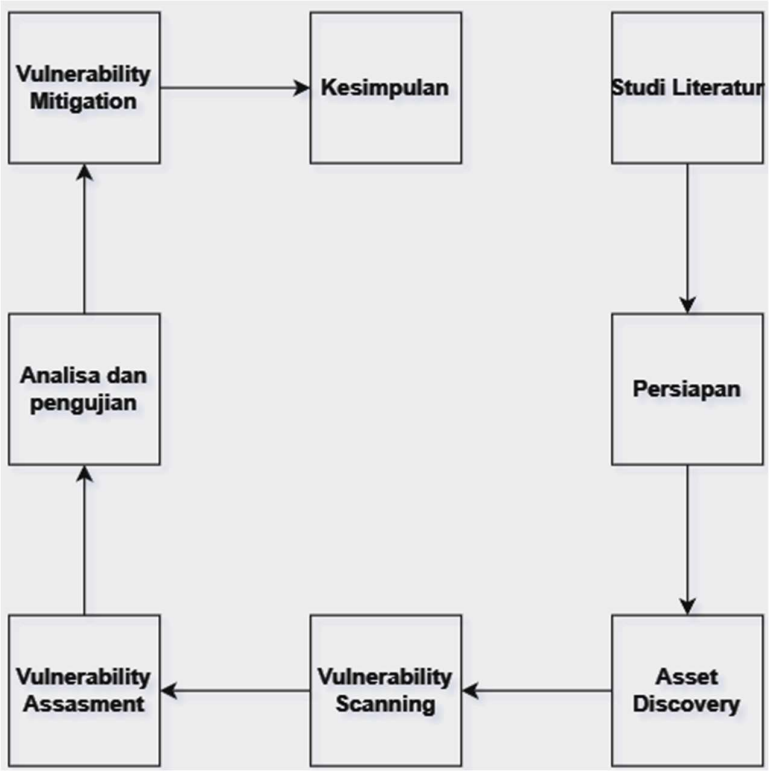
yang paling mudah dimengerti, temuan yang ditemukan juga memiliki bukti yang jelas dan dapat menjadi pertimbangan untuk melakukan tindakan perbaikan sistem.

BAB 3 METODOLOGI PENELITIAN

3.1. Metode Penelitian

Alur kerja penelitian ini ditunjukkan seperti pada **Gambar 3.1.**, tahapan-tahapan dalam penelitian ini terdiri dari :

1. Studi Literatur
2. Persiapan
3. Asset Discovery
4. Vulnerability Scanning
5. Vulnerability Assasment
6. Analisa dan pengujian
7. Vulnerability Mitigation
8. Kesimpulan



Gambar 3. 1 Diagram Alur Penelitian

1. Studi Literatur

Pada tahap ini penulis mencoba memahami bacaan yang bersumber dari teori dan jurnal untuk menambah informasi dan data yang berkaitan dengan penelitian ini, serta membaca modul pembelajaran Cyber Security.

2. Persiapan

Pada tahapan ini penulis Berkoordinasir dengan pihak Faris Munir Mahdi Untuk menjalankan Arachni, tahap ini wajib dilakukan pada penelitian ini untuk mengawasi penelitian dan memudahkan pencarian kerentanan pada aplikasi berbasis web, tahap ini bertujuan agar tidak terblokir oleh sistem pertahanan paling luar dari website seperti Firewall (WAF), IDS maupun IPS. Penulis juga mempersiapkan device yang akan digunakan sebagai media untuk melakukan VA dengan mulai menginstall virtual machine Kali Linux dan Arachni sebagai tools VA.

3. Asset Discovery

Tahap selanjutnya melihat tampilan dan fungsi website untuk melihat fitur apa saja yang dapat diakses, ditampilkan dan digunakan scara umum. Serta mengecek apakah website yang akan menjadi subjek VA masih berjalan dan tidak ditutup atau tidak diaktifkan menggunakan tools WhatsWeb pada Kali Linux.

4. Vulnerability Scanning

Pada tahap ini penulis melakuakan scan dari website www.farismunir.my.id yang disediakan oleh pihak Faris Manir Mahdi dengan menggunakan Arachni dengan profile pengujian automated dan full scan yang akan menghasilkan hasil deteksi kerentanan dan bukti celah kerentanan yang ada pada website www.farismunir.my.id yang dijadikan target pengujian arachni.

5. Vulnerability Assesment

Pada tahap ini penulis mendapatkan data hasil kerentanan aplikasi web dengan bukti yang ditemukan oleh tools Arachni, akan tetapi penulis memastikan kerentanan yang ada, hal ini sangat penting dilakukan karena beberapa hasil kerentanan dari Arachni bersifat False Positive yang hanya dinyatakan kerentanan, namun tetap semua kerentanan akan dilaporkan terutama kerentanan yang terbukti bisa dieksploitasi dan bisa dilakukan.

6. Analisa dan Pengujian

Pada tahapan ini penulis melakukan pendataan dari keseluruhan kerentanan yang sudah berhasil dideteksi maka akan dilakukan analisa kerentanan yang paling banyak terjadi, analisa menggunakan pendekatan OWASP top 10 untuk melihat apakah website ini termasuk dalam kategori website yang rentan pada serangan yang sering terjadi di dunia menurut OWASP, selain itu pada tahap ini peneliti melakukan pengujian berdasarkan temuan Arachni.

7. Vulnerability Mitigation

Pada tahapan ini penulis membuat laporan yang berisi data dan solusi kerentanan yang ada untuk diserahkan kepada pihak Faris Munir Mahdi.

8.Kesimpulan

Penarikan kesimpulan dilakukan dari hasil analisa dan data kerentanan yang ada pada website..

DAFTAR PUSTAKA

A. Budiman, S. Ahdan, and M. Aziz, "Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment," J. Komputasi, vol. 9, no. 2, pp. 1–10, 2021, [Online]. Available: https://jurnal.fmipa.unila.ac.id/komputasi/article/view/2800

Id-SIRTII/CC, "Laporan Bulanan Publik Hasil Monitoring Keamanan Siber Maret 2024," vol. 3, 2024, [Online]. Available: https://www.idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

A. C. Kusuma and A. D. Rahmani, "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia) Aditama Candra Kusuma , Ayu Diah Rahmani Fakultas Hukum , Universitas Pembangunan Veteran Jakarta Kemajuan teknologi sangat membantu manu," J. Huk., vol. 5, no. 01, pp. 46–63, 2022, [Online]. Available: www.bi.go.id.

Mira Orisa and M. Ardita, "Vulnerability Assesment Untuk Meningkatkan Kualitas Keamanan Web," J. Mnemon., vol. 4, no. 1, pp. 16–19, 2021, doi: 10.36040/mnemonic.v4i1.3213.

Elgamar, Konsep Dasar Pemrograman Website Dengan PHP. Ahlimedia Book, 2020.

J. Simarmata et al., Sistem Keamanan Data. KitaMenulis.id, 2022. [Online]. Available: https://kitamenulis.id/2022/10/30/sistem-keamanan data/

M. Yaqi, Vulnerability Assessment dan Penetration Testing (Vapt) Menggunakan Metode Zero Entry Hacking (Zeh) Terhadap Website Studi Kasus: Dinas Penanaman Modal …. 2023. [Online]. Available: https://repository.uinjkt.ac.id/dspace/handle/123456789/73422%0Ahttps://repository.uinjkt.ac.id/dspace/bitstream/123456789/73422/1/MUHAMMAD YAQI-FST.pdf

R. R. Yusuf and T. N. Suharsono, "Pengujian Keamanan Dengan Metode Owasp Top 10 Pada Website Eform Helpdesk," Pros. Semin. Sos. Polit. Bisnis, Akunt. dan Tek., vol. 5, p. 402, 2023, doi: 10.32897/sobat.2023.5.0.3132.

K. Abdulghaffar, N. Elmrabit, and M. Yousefi, "Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners," Computers, vol. 12, no. 11, pp. 1–17, 2023, doi: 10.3390/computers12110235.

K. Abdulghaffar, N. Elmrabit, and M. Yousefi, "Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability

Scanners," Computers, vol. 12, no. 11, pp. 1–17, 2023, doi: 10.3390/computers12110235.

Al Fajar, Febri. "Analisis Keamanan Aplikasi Web Prodi Teknik Informatika Uika Menggunakan Acunetix Web Vulnerability." *Jurnal Inovatif: Inovasi Teknologi Informasi dan Informatika* 3.2 (2020): 110-120.