ANALISIS KERENTANAN WEBSITE XYZ REPOSITORY MANAGEMENT PROJECT

Cipto Ardiantoro[1]
[1]Prodi Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
ciptoardiantoro@students.amikom.ac.id

Nila Feby Puspitasari[2]
[2]Prodi Teknik Informatika , Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
nilafeby @amikom.ac.id

ABSTRAK

Website XYZ *Repository Management Project* merupakan platform yang digunakan untuk mengelola, mengembangkan, dan mengkolaborasikan karya digital mahasiswa informatika. Keamanan website ini sangat penting untuk menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan untuk menganalisis kerentanan website *XYZ Repository Management Project.* Penelitian ini menggunakan metode pengujian penetrasi (*Penetration Testing)* dan Pemindaian Kerentanan (*Vulnerability Scanning)* untuk mengidentifikasi dan mengevaluasi berbagai kerentanan yang ada pada website XYZ Repository Management Project. Metodologi penelitian melibatkan beberapa tahapan, yaitu pengumpulan informasi, pengujian penetrasi testing berdasarkan standar NIST *(National Institute of Standars and Technology)* yang mencakup beberapa tahapan yaitu perencanaan *(planning)*, penemuan *(discovery*), penyerangan *(attacking)* dan pelaporan *(reporting).* Adapun alat-alat yang digunakan dalam pengujian ini meliputi perangkat lunak open-source seperti OWASP ZAP, Burp Suite, dan Nmap.

Hasil penelitian menunjukan bahwa terdapat beberapa kerentanan pada website XYZ *Repository Management Project*. Kerentanan-kerentanan tersebut meliputi keterbukaan informasi konfigurasi file *info.php, IDOR URL Manipulation* yang menampilkan informasi email pengguna dan menunjukkan bahwa ada celah signifikan dalam proteksi keamanan website tersebut. Implikasi dari temuan ini akan dianalisis lebih lanjut untuk memberikan rekomendasi mitigasi yang sesuai. Penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan website XYZ *Repository Management Project* serta memberikan wawasan bagi pengembang dan administrator sistem dalam mengelola dan memperbaiki sistem mereka. Hasil dari penelitian ini juga menekankan pentingnya pelaksanaan pengujian keamanan secara berkala untuk mengidentifikasi dan mengatasi kerentanan yang mungkin muncul seiring dengan perkembangan teknologi dan metode serangan baru.

Kata-kunci: *Keamanan, Pengujian Penetrasi, Pemindaian Kerentanan, Website XYZ Management project*

ABSTRACT

The XYZ Repository Management Project website is a platform used to manage, develop, and collaborate on the digital work of informatics students. The security of this website is very important to maintain the confidentiality and integrity of data. This study aims to analyze the vulnerability of the XYZ Repository Management Project website. This study uses the Penetration Testing and Vulnerability Scanning methods to identify and evaluate various vulnerabilities on the XYZ Repository Management Project website. The research methodology involves several stages, namely information collection, penetration testing based on NIST (National Institute of Standards and

Technology) standards which include several stages, namely planning, discovery, attack and reporting. The tools used in this test include open-source software such as OWASP ZAP, Burp Suite, and Nmap.

The results of the study indicate that there are several vulnerabilities on the XYZ Repository Management Project website. These vulnerabilities include the disclosure of info.php file configuration information, IDOR URL Manipulation that displays user email information and indicates that there is a significant gap in the security protection of the website. The implications of these findings will be further analyzed to provide appropriate mitigation recommendations. This research is expected to contribute to improving the security of the XYZ Repository Management Project website and provide insight for developers and system administrators in managing and improving their systems. The results of this study also emphasize the importance of implementing periodic security testing to identify and address vulnerabilities that may arise along with the development of new technologies and attack methods.

***Keywords**: Security, Penetration Testing, Vulnerability Scanning, XYZ Website Management Project*

1. PENDAHULUAN

1.1 Latar Belakang

Internet menjadi teknologi terbesar yang terus berkembang penggunanya di Indonesia. Jumlah pengguna internet saat ini telah mencapai 213 juta orang per Januari 2023. Jumlah ini setara 77% dari total populasi Indonesia sebanyak 276,4 juta orang (Annur, 202. Aktifitas pengguna internet yang digunakan adalah *browser* untuk menjelajahi dunia maya serta mencari informasi. Saat ini, informasi dapat ditemukan pada halaman website sebagai sarana media informasi. Website dapat mencakup berbagai jenis informasi, mulai dari artikel hingga produk atau layanan yang sangat mudah mudah diakses oleh pengguna secara luas melalui penggunaan internet (Widjaja & Widodo, 2021).

Selain mudah diakses dan digunakan, website juga menampilkan halaman yang *user-friendly* untuk pengguna menemukan informasi melalui koneksi internet. Selain itu, website harus memiliki pertahanan keamanan yang kuat agar terhindar dari tindakan kebocoran, pencurian data dan manipulasi (Madiistriyatno, 2018). Secara umum keamanan dinilai secara 3 (tiga) faktor utama yaitu disingkat dengan CIA atau *Confidentiality*, *Integrity* dan *Availability*. Ketiga faktor utama tersebut saling mengikat satu sama lain untuk melindungi informasi dari tiga sisi faktor yang berbeda sehingga disebut dengan segitiga CIA (Winarianto & Saud, 2022).

Pengelola Website XYZ atau disebut XYZ Repository Management Project adalah suatu penyimpanan projek mahasiswa/i dari XYZ.com, Yang dikembangkan serta merancang tampilan landingpage website yang bertujuan untuk mengapresiasi mahasiswa/i dalam menyelesaikan projek mata kuliah dan hasil projeknya akan diterbitkan di halaman website XYZ.com.

Berdasarkan hasil observasi dan wawancara yang telah dilakukan peneliti terkait dengan keamanan website XYZ ditemukan bahwa jenis vulnerability atau kerentanan yang memiliki jenis tipe ancaman yang berbeda dalam melakukan penyerangan pada website XYZ. Pada proses ini peneliti melakukan uji penyerangan tahapan awal untuk mengenal pola atau alur kerja sistem website dengan metode scanning dalam mengumpulkan informasi website XYZ terlebih dahulu.

Hasil pengujian penyerangan tahapan awal peneliti mengidentifikasi beberapa celah keamanan yang memungkinkan penyerang untuk mendapatkan informasi webserver yang digunakan dalam mengembangkan aplikasi website (Prasena,2020).

Solusi dalam permasalahan keamanan website aplikasi mengacu pada penerapan teknik dan prinsip pengembangan perangkat lunak yang aman, seperti penggunaan validasi input, menghindari SQL dan XSS serta penggunaan library dan framework yang aman. Penelitian keamanan webserver dan SSL telah dilakukan pada penelitian sebelumnya. Diantaranya penelitian yang oleh nazwita dam ramadhani. Dalam penelitian menganalisis keamanan web server dan SSL telah dilakukan penyerang mencoba untuk menyusup melalui port yang telah discanning (Utomo & Rokhmah,2022).

Penelitian dalam menerapkan keamanan terhadap kerentanan SQL Injection yang dilakukan oleh Asnawi, Dedy, Ulfi, Puji. penelitian yang diusulkan untuk berkolaborasi penanganan serangan menggunakan struktur alur NIST (*National Institute of Standards and Technology*) SP 800-53 sebagai fundamental penanganan pelaku attacker (penyerang)[8]. Melalui penelitian yang menggunakan konsep analisis kerentanan aplikasi web menggunakan kombinasi *tool* yang dilakukan oleh Moh Yunus. Masalah kerentanan dapat berupa serangan *Malware, Eksploitasi* dan *injeksi database.* Solusi pengamanan web dari gangguan atau penyerang dapat dilakukan dengan *self test* yaitu

pengujian yang dilakukan terhadap website secara legal dengan aktivitas menyerupai penyerang atau hacker (Asnawi, dkk, 2023).

Untuk menemukan dan mengidentifikasi suatu kerentanan, dengan melakukan analisis kerentanan website menjadi tujuan penelitian dalam memahami potensi ancaman celah keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab, sehingga dapat diambil langkah-langkah pencegahan yang tepat untuk meningkatkan keamanan dan integritas website XYZ (Yunus, 2019).

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas maka, rumusan masalah pada penelitian ini sebagai berikut:

1. Apa saja kerentanan keamanan yang ada pada Website XYZ Repository Management Project?
2. Bagaimana implementasi metode NIST dalam melakukan pengujian penetrasi dan hasil analisanya terhadap Website XYZ Repository Management Project?
3. Bagaimana rekomendasi perbaikan yang tepat untuk mengatasi kerentanan yang ditemukan pada Website XYZ Repository Management Project?

1.3 Batasan Maslah

Berdasarkan batasan masalah yang telah diuraikan, maka peneliti melakukan batasan masalah terhadap masalah penelitian yang sedang dilakukan sebagai berikut:

1. Melakukan *Penetration Testing* pada website XYZ Repository Management Project?
2. Penelitian ini diawali dengan menggunakan sistem operasi *Windows 10* dan *Kali Linux* versi 2023.
3. Penelitian ini menggunakan beberapa tahapan utility dan *tools* yaitu *Whois, Ping, Host, scan SSL, Dirsearch, NMAP*, dan *Burp Suite*.
4. Peneliti akan memusatkan perhatian pada analisis dan implementasi secara teknis untuk mengungkap penemuan kerentanan seperti *SQL Injection*, *Cross-site scripting* (*XSS*), dan serangan lainnya.
5. Penelitian ini melibatkan *Penetration Tester* melakukan pengujian dengan menggunakan metode *NIST,* dan tindakan *Penetration Testing*.

1.4 Tujuan Penelitian

Tujuan penelitan yang ingin dicapai dalam penelitian adalah untuk menganalisis dan memahami dampak dari kerentanan keamanan website terhadap keberlangsungan projek dan integritas data serta mengidentifikasi strategi pencegahan dan mitigasi yang efektif dalam menghadapi pencegahan keamanan digital. Dengan tujuan mengidentifikasi potensi celah keamanan yang dapat dieksploitasi oleh penyerang. Selain itu, penelitian ini bertujuan untuk mengembangkan strategi perlindungan yang efektif dan praktis untuk mengurangi resiko keamanan website XYZ serta memperkuat integritas, kerahasiaan, dan ketersediaan informasi yang disimpan dan diproses oleh Website XYZ Repository Management Project.

2. LANDASAN TEORI

2.1 Keamanan Informasi

Menurut G.J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (Cheating) atau paling mendeteksi adanya penipuan disebuah sistem berbasis informasi dimana informasinya sendiri tidak memiliki arti fisik. Keamanan informasi perlu diwaspadai dari ancaman yang bersifat internal dan eksternal baik dari dalam sistem maupun luar sistem yang akan berdampak pada ketidakstabilan sistem. Keamanan teknologi informasi mempunyai 3 (tiga) jenis prinsip yang dapat disebut CIA Kerahasian

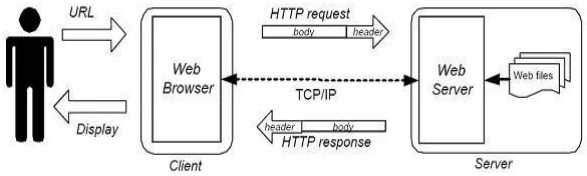
(Confidentiality), Integritas *(integrity),* dan Ketersedian (*Availability*). Gambar 2.1 CIA Triad menggambarkan tiga jenis prinsip tersebut memiliki persamaan yang sama satu dengan yang lain sehingga membentuk sebuah segitiga.

Gambar 2.1 CIA Triad

a. *Confidentiality* (Kerahasiaan) : Merupakan prinsip yang menekankan pentingnya melindungi informasi sensitif dari akses pada pihak yang tidak berwenang. Dalam konteks keamanan website, kerahasiaan penting untuk melindungi data pengguna, informasi keuangan, atau informasi rahasia lainnya dari akses yang tidak sah. Praktek perlindungan dapat mencakup penggunaan enkripsi data, pengaturan hak akse yang tepat, dan manajemen identitas pengguna.
b. *Integrity* (Integritas) : Prinsip yang menekankan pentingnya memastikan bahwa informasi tetap benar, utuh, dan tidak dimanipulasi selama proses penyimpanan, transmisi, dan pemrosesan. Dalam keamanan website, integritas menjadi faktor utama untuk memastikan bahwa konten dan data tidak diubah atau dimanipulasi oleh penyerang.
c. *Availability* (Ketersediaan) : Berfokus untuk memastikan bahwa informasi dan layanan yang diperlukan tersedia dan dapat diakses oleh pihak yang berwenang saat diperlukan. Dalam konteks keamanan websiste, ketersediaan penting untuk memastikan bahwa situs web tetap dapat diakses oleh pengguna yang sah dan tidak terganggu oleh sserangan atau gangguan jaringan. Penerapan strategi pemantauan kinerja, pencegahan serangan DDoS, dan rencana pemulihan bencana merupakan upaya yang penting dalam menjaga ketersediaan layanan.

2.2 Definisi Website

Website dapat disimpulkan sebagai kumpulan halaman yang berisi informasi data digital baik berupa teks, gambar, animasi, suara, dan video atau gabungan dari halaman web dalam sebuah website, yang disusun dan diatur dalam tata letak yang khohesif. Website memiliki tujuan tertentu, seperti menyediakan informasi tentang topik, mengkomunikasikan gagasan atau produk, atau menyediakan platform untuk interaksi dan transaksi onine.



Gambar 2.2 Alur Kerja Website

Pada Gambar 2.2 Alur Kerja Website menunjukan cara kerja website dimana pengguna yang mengunjungi suatu website berupa URL melalui Web Browser (media untuk menuju URL yang diakses). Web Browser tersebut akan mengirimkan *request* (permintaan) berupa HTTP *request* kepada Web Server melalui *layer-layer* TCP/IP selanjutnya Web Server memberikan Web files yang direquest jika ada. Web files yang telah diberikan tidak langsung ditampilkan/di-display begitu saja namun Web Server memberikan respon kembali ke Web Browser melalui HTTP response yang juga melalui *layer-layer* TCP/IP. Kemudian hasilnya diterima oleh Web Browser yang akan dikirimkan kepada pengguna berupa Display.

2.3 Penetration Testing

Penetration testing atau sering disebut juga pen testing atau ethical hacking adalah proses uji penetrasi yang dilakukan secara sistematis untuk mengevaluasi keamanan suatu sistem, jaringan, atau aplikasi dengan cara mensimulasikan serangan yang mungkin dilakukan oleh penyerang potensial. *Penetration testing* adalah mengidentifikasi dan mengeksplorisasi kerentanan yang ada sehingga dapat diperbaiki sebelum dieksploitasi oleh penyerang.

Penetration testing memiliki 3 (tiga) metode yang banyak digunakan pada saat melakukan pengujian yaitu *Black Box testing, White Box testing,* dan *Grey Box testing. Black Box testing* merupakan pengujian sistem yang tanpa pengetahuan sebelumnya tentang infrastruktur atau kode yang diuji. *Penetration tester* akan mencoba mengeskploitasi sistem sebagaimana halnya penyerangan eksternal yang tidak memiliki akses atau indormasi internal tentang sistem yang diuji. *White Box testing* merupakan metode yang melibatkan pengujian sistem dengan pengetahuan penuh tentang infrastruktur, kode sumber, dan konfigurasi sistem yamg diuji.

Penetration Tester dapat menggunakan informasi ini untuk melakukan pengujian yang lebih mendalam dan spesifik, serta mengidentifikasi kerentanan yang mungkin tersembunyi. *Grey Box testing* merupakan gabungan dari *Black Box* dan *White Box* testing. Metode tersebut dilakukan melalui sudut pandang subjek yang berada pad sistem namun tidak mempunyai hak akses penuh terhadap pengelolah sistem secara langsung contohnya seperti pengguna website XYZ yang tidak memiliki hak akses pada bagian internal pengelolaan database website, metode ini berfokus terhadap kerentanan individual yang terdapat dalam ruang lingkup sistem.

2.4 NIST Methodology

National Institute of Standards and Technology (NIST) Penetration Testing merupakan suatu metode *Penetration Testing* yang diperkenalkan oleh badan pemerintahan Amerika Serikat yang dilakukan dalam waktu pendek secara berkala tahapan yang mempunyai jenis sederhana dan singkat. Dalam melakukan tindakan pengujian dibagi menjadi 4 (empat), yaitu perencanaan (*planning*), penemuan (*discovery*), penyerangan (*attackinig*), dan melaporkan (*reporting*).

2.4.1 Perencanaan *(Planning)*

Proses tahapan perencanaan dilakukan *information search* yang tersedia secara online atau menggunakan tools untuk mendapatkan informasi, melakukan pemindaian network, identifikasi servis dan deteksi sistem yang digunakan. Dalam tahapan biasanya akan dilakukan pengumpulan informasi dari alamat IP target seperti name server dan IP email. Alamat IP tersebut kemudian diseleksi berdasarkan ruang lingkup yang telah mendapatkan izin sebelumnya untuk dilakukan *vulnerability scan* di tahapan *discovery*. Tahapan kedua dilakukan untuk mengetahui kerentanan maupun kelemahan yang ditemukan dari struktur *source code* yang dapat terlihat dari sisi *user*.

2.4.2 Penemuan *(Discovery)*

Tahap penemuan (discovery) merupakan proses pemahaman yang diperlukan tentang target yang akan diuji yaitu memilik 2 (dua) bagian seperti pengumpulan informasi (*information gathering*) pemindaian kerentanan (*vulnerability scan*). Tujuan melakukan hal ini adalah untuk mengetahui sumber informasi mengenai targer pengujian yang berasal dari penggunaan *tools*.

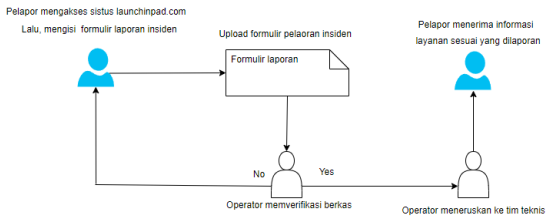
Melakukan pengumpulan informasi pada penelitian menggunakan *tools* yang pada umumnya digunakan yaitu *ping*, *whois*, dan *host*. Dimana informasi tersebut akan diperoleh melalui *IP Address, Domain Name Server* (*DNS*). Sedangkan *Vulnerability scan* adalah proses yang digunakan untuk mengumpulkan informasi mengenai kerentanan yang ditemukan pada halaman website target menggunakan *tools* yaitu *Burp suite, Nmap, Dirsearch.*

2.4.3 Penyerangan *(Attacking)*

Tahapan melakukan penyerangan merupakan hal utama untuk *Penetration Testing.* Cara tersebut untuk memberikan bukti bahwa penemuan kerentanan atau celah keamanan yang berada pada sistem adalah dengan melakukan penyerangan kerentanan seracara langsung. Dalam konteks ini keamanan informasi, penyerang pada kerentanan merujuk pada upaya untuk mengeksploitasi kelemahan atau celah dalam sistem komputer, jaringan, atau perangkat lunak. Ini dilakukan dengan tujuan untuk mendapatkan akses yang tidak sah, merusak, atau mencuri informasi sensitif.

2.4.4 Laporan *(Reporting)*

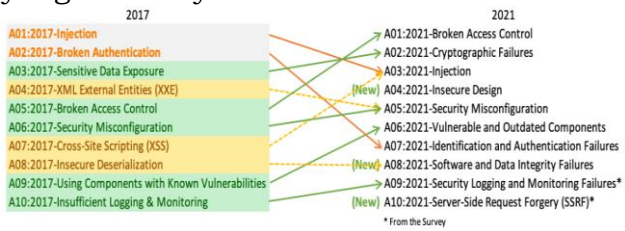
Tahapan laporan adalah tahapan akhir setelah melakukan proses pengumpulan informasi, penyerangan, dalam kegiatan penetration testing dokumen resmi yang disusun oleh seorang *Penetration Tester* keamanan untuk menyelesaikan pengujian penetrasi terhadap sistem atau aplikasi website. Laporan ini berisi hasil temuan, analisis kerentanan, rekomendasi perbaikan, dan informasi penting lainnya yang relevan untuk meningkatkan keamanan sistem. Seperti pada Gambar 2.4 Proses Berjalannya Laporan.



Gambar 2.4 Proses Berjalannya Laporan

2.5 Vulnerability OWASP Top 10

OWASP Top 10 adalah daftar 10 kerentanan keamanan yang paling umum untuk ditemukan dalam aplikasi website. menurut penelitian yang dilakukan Muhammad Rafi Ramadani, Nono Heryana, dan Agung Susilo Yuda Irawan dengan melakukan identifikasi masalah kerentanan yang terdapat dalam website dan melakukan pengujian serta analisis untuk mengetahui kondisi kerentanan website tersebut menggunakan *Open Web Aplication Security Project (OWASP).* Daftar tersebut dirangkum oleh *OWASP*, sebuah organisasi nirlaba yang fokus pada peningkatan keamanan perangkat lunak. Daftar *OWASP Top 10* diperbarui setiap tahun untuk mencerminkan tren dan perkembangan terbaru dalam keamanan aplikasi web. Berikut Gambar 2.5 Top Web Aplication Security Risk yang umumnya diakui :

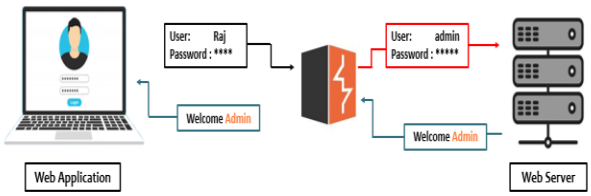


Gambar 2.5 Top 10 Web Application Security Risk

2.6 Burp Suite

Burp Suite adalah alat pengujian penetrasi (*Penetration testing tools*) yang dikembangkan oleh *PortSwigger ltd* dan dibangun berdasarkan penelitian

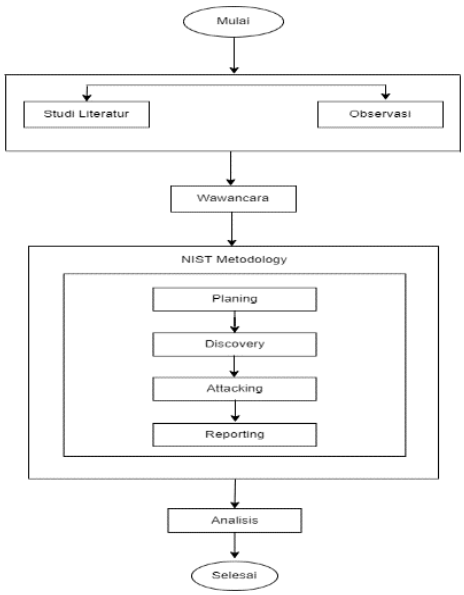
terkemuka selama bertahun-tahun. *Tools* ini pertama kali dirilis pada tahun 2004 dan telah menjadi salah satu alat yang sangat populer dan kuat untuk melakukan pengujian keamanan aplikasi website lebih dari 70.000 pengguna di lebih dari 16.000 organisasi. *PortSwigger founder and Chief Swig* menyatakan, *Burp Scanner* dibuat untuk meniru tindakan pengujian manual yang terampil. Pendekatan tersebut berlanjut hingga saat ini dan *Burp Scanner* didukung oleh tim riset keamanan web terkemuka di dunia.



Gambar 2.6 Burp Suite Scanner

3. METODE PENELITIAN

3.1 Alur Penelitian



Gambar 3.1 Tahapan Alur Penelitian

Alur penelitian Gambar 3.1 Tahapan Alur Penelitian melakukan studi dimulai dengan mengidentifikasi struktur serta kompoten utama situs website tersebut. Dalam proses alur penelitian yang dilakukan akan dijelaskan mulai dari tahapan awal yang dilakukan sampai tahapan akhir berikut ini penjelasannya.

3.1.1 Tahapan Alur Penelitian

Dalam penelitian ini, menggunakan metode pengumpulan data melalui analisis kerentanan dalam melakukan serangkaian berbagai macam serangan yang dilakukan dan studi literatur untuk memahami kerentanan umum yang terhubung dengan teknologi yang digunakan. Selain itu, peneliti juga melakukan wawancara dengan pengembangan website untuk memperoleh pemahaman tentang struktur dan praktik keamanan yang diterapkan, serta melakukan pemindaian keamanan untuk mengidentifikasi kerentanan. Analisis kode sumber juga akan dilakukan untuk mengevaluasi kelemahan keamanan yang mungkin ada dalam implementasi website, dan peneliti melakukan pengujian penetrasi serta pemodelan ancaman untuk mengevaluasi resiko yang mungkin dihadapi oleh website XYZ.

3.1.2 Studi Literatur

Studi literatur menjelaskan kajian pustaka dan menyusun alur penelitian berdasarkan teori dan prakterk yang digunakan sebagai bahan penelitian. Adapun studi literatur yang digunakan pada penelitian ini diambil dari referensi jurnal, e-book, dan internet.

3.1.3 Observasi

Observasi yang dilakukan merupakan hasil pengamatan dari alur analisis kerentanan. Observasi berfokus kepada analisis terhadap kerentanan atau *vulnerability* yang ditemukan saat pengujian menggunakan domain website

target XYZ. Output dan respon yang diberikan oleh website akan dikumpulkan dan dibandingkan kembali sehingga dapat mengetahui tingkat resiko keamanan dari hasil analisis. Tabel 3.1 Hasil Observasi analisis observasi yang memicu adanya kerentanan.

Tabel 3.1 Hasil Observasi

No	Lingkup Pengujian	Deskripsi	Temuan	Rekomendasi Perbaikan
1	Infrastruktur Jaringan	Pemindaian port untuk mengidentifikasi layanan	Port 22 (SSH) terbuka	Menonaktifkan SSH jika tidak digunakan untuk mengurangi serangan brute-force
2	Aplikasi Web	Penilaian kerentanan pada aplikasi web	Kerentanan informasi webserver pada direktori info.php dan informasi data pengguna seperti email pada halaman profile	Membatasi akses ke file 'info.php' melalui konfigurasi server. Selanjutnya untuk data pengguna seperti email baiknya untuk menyembunyikan email pribadi pengguna lain untuk menghindari serangan social engineering
3	Sistem Operasi	Penetrasi pada sistem operasi	Akun pengguna dengan password lemah	Menerapkan kebijakan kata sandi yang lebih kuat dan mengatur kebijakan penutupan akun setelah berbagai upaya gagal
4	Aplikasi khusus	Evaluasi keamanan aplikasi khusus	Mengaman kan dan memperkuat proteksi terhadap serangan CSRF	Mengidentifikasi token CSRF dan menambahkan header proteksi

3.1.4 Wawancara

Wawancara pribadi yang dilakukan kepada narasumber selaku sekretaris program studi, serta tim pengembang inovasi XYZ. Dari wawancara tersebut ditemukan kerentanan mengenai tingkat keamanan website XYZ. Setiap website repository memiliki jenis layanan yang sama sebagai tempat penyimpanan untuk mengumpulkan berbagai informasi. Maka, uji kerentanan yang dilakukan terhadap website XYZ dapat dilakukan menggunakan analisis kerentanan sebagai peran yang bertugas mengidentifikasi dan mengeksploitasi kerentanan keamanan dalam sistem atau aplikasi untuk mengevaluasi keamanan. Oleh karena itu, dapat disimpulkan untuk melakukan penelitian dengan melakukan implementasi *penetration testing* pada website XYZ.

3.2 Pengujian NIST Metodology

Pada pengujian awal ini menggunakan analisis kerentanan yang terdiri dari 4 (empat) tahapan yaitu *Planning* (perencanaan), *Discovery* (penemuan), *Attacking* (penyerangan), *Reporting* (laporan). Dari hasil empat tahapan tersebut, bertujuan untuk memudahkan disaat melakukan pengujian dan menemukan hal yang berkaitan dengan kerentanan dan kembali ke tahapan awal. Meskipun dari tahapan awal dapat dilakukan penyelesaian sampai pada tahapan akhir, batasan dari informasi serta tujuan *penetration testing* telah tercapai. Tabel 3.2 Skenario Pengujian Awal sebagai contoh analisis tahapan penyerangan.

Tabel 3.2 Skenario Pengujian Awal

No	Tahapan	Deskripsi
1	*Planning* (Perencanaan)	Menetapkan tujuan analisis kerentanan dan melakukan identifikasi sumber daya yang tersedia (alat, waktu, dan tenaga kerja).
2	*Discovery* (Penemuan)	Pemahaman terhadap arsitektur situs website. Pemetaaan aplikasi infrastruktur, dan teknologi yang digunakan.
3	*Attacking* (Penyerangan)	Pemindaian (scanning) situs website untuk menemukan kerentanan yang mungkin ada. Mengeksploitasi kerentanan yang ditemukan secara etis.
4	*Reporting* (Laporan)	Mendokumentasikan penemuan kerentanan dengan jelas dan lengkap. Memberikan laporan kepada pemilik website atau tim keamanan launchinpad.com

Pada 4 (empat) tahapan sebagai langkah penelitian untuk skenario pengujian yang akan dilakukan sebanyak 9 (sembilan) pengujian sesuai dengan kerentanan umum yang terdapat pada website. Melakukan percobaan misalkan, dalam contoh skenario pengujian awal, peneliti memiliki:

1. Jumlah kasus uji untuk SQL Injection: 2.

2. Jumlah kasus sukses untuk SQL Injection : 0

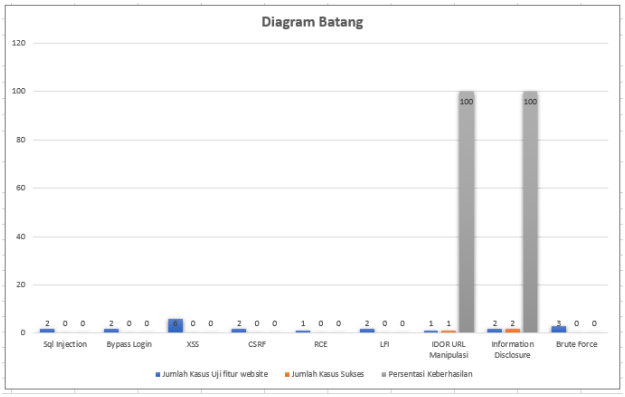
Maka, untuk menghitung persentase keberhasilan SQL Injection:

$$Persentase\ Keberhasilan\ SQL\ Injection = \frac{Jumlah\ Kasus\ Sukses}{Jumlah\ Kasus\ Uji}\ x\ 100$$

$$Persentase\ Keberhasilan\ SQL\ Injection = \frac{0}{2}\ x\ 100 = 0\%$$

Dengan demikian, persentase keberhasilan SQL Injection adalah 0%.

Proses yang sama diulang untuk setiap skenario pengujian, dimana jumlah kasus uji dan jumlah kasus sukses dihitung, dan kemudian persentase keberhasilan dihitung menggunakan rumus yang sama. Berikut Gambar 2.3 Diagram Percobaan Pengujian hasil skenario langkah awal.



Gambar 3.2 Diagram Percobaan Pengujian

4. HASIL DAN PEMBAHASAN

4.1 Implementasi

4.1.1 Discovery

Pada tahapan awal peneliti menggunakan beberapa *tools* untuk mengetahui informasi dari website target yang akan dilakukan uji pentest dengan menggunakan perintah *ping*, *whois*, *host*, *scan ssl*. Dari hasil scanning penguji melakukan pemeriksaan lebih awal sebelum masuk ke langkah-langkah proses penemuan analisis kerentanan ke tahapan umum yang ditemukan seperti *SQL Injection*, *XSS*, dan dll. Oleh karena itu, dilakukan analisis dan penerapan praktik keamanan terbaik untuk mengukur dan meningkatkan dalam mengumpulkan informasi. Berikut Tabel 4.1 Implementasi Scanning sebagai berikut:

Tabel 4.1 Implementasi Scanning

Website	Method	Keterangan	Hasil
XYZ.com	Ping	Ping digunakan untuk memastikan apakah terdapat masalah pada saat mengunjungi website. Dengan cara mengetikan $ ping launchinpad.com, hasil dari tes akan menunjukan apakah website yang ingin dikunjungi berjalan normal atau sedang masalah pada server.	Berhasil
	Whois	Pada saat perintah $ whois launchinpad.com dijalankan terdapat keselahan scanning yang mana akurasi pencarian dan hasil yang ditemukan tidak akurat.	Berhasil
	Host	perintah $ host launchinpad.com digunakan untuk mengetahui informasi tetntang nama host atau alamat IP website.	Berhasil
	Open SSL	Perintah $ echo | openssl s_client -servername domain.com -connect launchinpad.com:443 | openssl x509 -noout -dates. Untuk mengetahui cara pemeriksaan expiration date dari sertifikat SSL yang terpasang di website maupun dari file .pem	Berhasil

4.2 Pembahasan

4.2.1 Attacking

Tahapan ini merupakan bagian yang akan melakukan kegiatan *penetration testing* dari beberapa tools yang sudah dijelaskan. Pada proses ini akan dilakukan penyerangan terhadap sistem yang sudah diketahui melalui hasil analisis dan pengumpulan informasi dan menjelaskan cara gunakan vulnerability scanner BurpSuite. Tujuan hasil proses ini adalah dengan membuktikan seberapa besar ancaman dari celah kerentanan terhadap sistem dengan melakukan proses juga tahapan menyerang pada kerentanan. Pada Tabel 4.2 menunjukkan hasil penyerangan.

Tabel 4.2. Hasil Penyerangan

No	Kerentanan	Deskripsi	Dampak Potensial	Tingkat Bahaya (Skala 1-5)	Status	Solusi
1	SQL Injection	Kerentanan yang memungkinkan penyerangan untuk injeksi perintah SQL yang berbahaya ke dalam formulir input.	Akses ke basis data sensitive	5	Tidak ditemukan	Memperbarui perangkat lunak database dan menerapkan input sanitization.
2	Cross-Site Scripting (XSS)	Memungkinkan penyerang untuk menyisipkan script berbahaya pada halaman web yang dilihat oleh pengguna.	Pengubahan konten, pencurian cookies.dll.	4	Tidak ditemukan	Mengimplementasikan input sanitization dan conten security police.
3	Cross-Site Request Forgery (CSRF)	Menyebabkan pengguna untuk melakukan aksi tanpa pengetahuan sistem, menggunakan kredensial otentikasi.	Manipulasi atau aksi tidak diinginkan oleh pengguna.	3	Tidak ditemukan	Mengimplementasikan permintaan dan mengonfirmasi periksa CSRF di sisi server
4	Brute Force Attack	Percobaan oromatis untuk menebak kredensial login. Dengan berbagai kombinasi kata.	Pembobolan akun, akses tidak sah.	4	Tidak ditemukan	Mengimplementasikan langkah-langkah mitigasi seperti pembatasan percobaan login dan memaksa kebijakan kata sandi yang kuat.
5	Rocme Code Execution (RCE)	Kerentanan yang memungkinkan penyerang untuk menjalankan kode jahat dari jarak jauh pada server.	Pengendalian penuh atas sistem, pencurian data sensitif, kerugian finansial.	5	Tidak ditemukan	Memperbarui perangkat lunak, membatasi akses ke fitur yang rentan, menerapkan filter input, dan memonitor aktifitas anomaly.
6	Local File Inclusion (LFI)	Kerentanan yang memungkinkan penyerang untuk memasukkan file ke dalam halaman web.	Akses ke file sensitif, pencurian data, eskalasi hak akses.	5	Tidak ditemukan	Mengimplementasikan kontrol akses yang ketat, memvalidasi dan membatasi input pengguna, dan memperbarui perangkat lunak yang rentan.
7	Informasi Disclosure	Kerentanan yang mengungkap informasi	Potensi untuk menyediakan bakan dalam serangan lebih lanjut, pencurian identitas, atau serangan social.	3	Ditemukan	Meninjau dan memperbarui pengaturan konfigurasi, mengimplementasikan kebijakan privasi yang ketat dan melatih staf tentang praktik keamanan yang tepat.
8	Insecure Direct Object Reference (IDOR)	Kerentanan yang memungkinkan penyeran untuk mengakses atau manipulasi objek secara langsung melalui referensi yang tidak aman.	Akses tidak sah ke data sensitif, pencurian informasi pengguna, eskalasi hak akses.	4	Ditemukan	Mengimplementasikan kontrol akses yang ketat, menerapkan autentikasi dan otorisasi yang kuat, melakukan validasi server-side untuk permintaan pengguna.
9	Bypass Login	Penyerang memasukkan input yang tidak valid atau manipulatif, seperti karakter khusus atau skrip injeksi, untuk mengelabui proses otentikasi	Akses tidak sah pada sistem atau aplikasi, kemungkinan penggunaan akses tersebut untuk mencuri data sensitif atau merusak sistem.	5	Tidak ditemukan	Validasi input yang kuat, termasuk pemeriksaan karakter yang tidak valid dan penyaringan skrip injeksi

Selanjutnya, proses dan cara yang dilakukan tahapan ini tidak hanya menggunakan tools dan menggunakan cara manual untuk diimplementasikan selama melakukan penetration testing tersebut. Pada Tabel 4.3 dapat dilihat dan akan dijelaskan hasil pengujian yang menunjukan adanya sejumlah kerentanan potensial yang dapat dieksploitasi oleh peneliti. Riset mendalam dilakukan untuk mengevaluasi dampak potensial dari setiap kerentanan. Berikut hasil Tabel 4.3 tentang Informasi Penyerangan.

Tabel 4.3 Informasi Penyerangan

Vulnerability	Fitur & Halaman					
	Parameter Url	Search	Login	My Project	Setting	Port SSH
SQL Injection	×	×	×			
Bypass Login			×			
XSS	×	×		×	×	
CSRF				×		
RCE					×	
LFI	×					
IDOR URL Manipulasi	✓					
Information Disclosure	✓					
Brute Force						×

4.3 Reporting

Akhir dari tahapan ini adalah laporan dan akan disampaikan secara langsung kepada tim developer dan narasumber yang telah diwawancara sebelumnya. Peneliti akan membuat laporan sesuai dengan apa yang telah ditemukan mulai dari ringkasan, kerentanan, *steps of procedure*, dan *impact*. Dari hasil laporan, peneliti akan membuat laporan yang se-efektif mungkin yang menampilkan hasil gambar dan menjelaskan secara signifikan dampak ancaman terhadap alur rancangan aplikasi website. Berikut adalah hasil laporan yang telah dikirimkan.

Tabel 4.3 Ringkasan Laporan

Kerentanan	Deskripsi	Tingkat Keparahan
Information Disclosure pada Direktori 'info.php'	Direktori 'info.php' memberikan akses terhadap informasi sensitif, seperti infomrasi konfigurasi, variabel lingkungan, atau informasi penting lainnya	Medium
IDOR URL Manipulation	Kerentanan IDOR terjadi ketika aplikasi memungkinkan penyerang untuk memanipulasi URL untuk mengakses objek atau data yang seharusnya tidak dapat diakses	LOW

4.4 Analisis

Tahapan analisis yang dilakukan merupakan proses pemeriksaan kembali untuk memastikan apakah kerentanan atau celah keamanan telah diperbaiki atau belum diperbaiki. Peneliti melakaukan analisis kembali setelah mengirimkan laporan dan akan disampaikan secara lengkap bahwa apa yang dilakukan peneliti telah tersampaikan. telah dilakukan untuk menjelaskan dan membandingkan suatu hasil dari setiap pengujian dengan menggunakan referensi dari penelitian sebelumnya**.** Dengan analisis yang telah dilakukan dapat ditarik sebuah kesimpulan dan saran bahwa dalam bagian ini dilakukan pemeriksaan kembali dari hasil tahapan dan diberikan sebuah solusi dari permasalahan.

4.4.1 Rekomendasi Perbaikan Kerentanan

Langkah atau tindakan yang direkomendasikan peneliti untuk memperbaiki atau mengurangi risiko dari kerentanan keamanan yang telah diidentifikasi dalam suatu sistem atau aplikasi. Tujuan dari rekomendasi perbaikan untuk mengurangi peluang terjadinya eksploitasi atau serangan yang memanfaatkan kerentanan tersebut.

a. Beberapa administrator server mungkin memilih untuk menonaktifkan fungsi *PHP* 'phpinfo*()*'. Karena fungsi ini menampilkan informasi yang dapat digunakan untuk menyusupi server tempat website berjalan. Meskipun menonaktifkan *phpinfo()* dapat membuat masalah debugging di *backdrop* (dan *PHP* secara umum) menjadi lebih sulit, server lebih aman.

Apabila *phpinfo()* dinonaktifkan dan ingin mengaktifkannya, berikut rekomendasi yang diberikan :

1. Apabila memiliki akses ke file php.ini server, dan baris menyertakan *disable_functions* arahan mengatakan, *disable_functions* = *phpinfo* ubah menjadi *disable_function* =
2. Dan apabila tidak memiliki akses, dapat menghubungi administrator server atau penyedia hosting.

Apabila *phpinfo()* diaktifkan dan ingin menonaktifkannya, maka lakukan langkah berikut:

1. Apabila memiliki akses ke file php.ini server, ubah baris yang mnyertakan arahan *disable_functions* sehingga menjadi *disable_functions* = phpinfo.
2. Dan apabila tidak memiliki akses, dapat menghubungi administrator server atau penyedia hosting.

b. Hasil penemuan kerentanan yang memperlihatkan informasi pengguna yang dapat dimanfaatkan oleh penyerang untuk memperoleh akses yang tidak sah atau melakukan tindakan yang tidak diinginkan. Dalam hal ini kerentanan yang memperlihatkan informasi pengguna seperti email merujuk pada celah keamanan yang memungkinkan penyerang untuk mengakses atau mengungkap informasi sensitif tentang pengguna seperti alamat email.

1. Sebaiknya informasi pengguna seperti email disembunyikan. Hal tersebut dapat dimanfaatkan oleh penyerang untuk mendapatkan akses penuh ke halaman pengguna lain. Salah satu contoh serangan yang dapat dimanfaatkan dari email adalah *phising* yang menyerupai tampilan halaman asli website.

5. PENUTUP

5.1 Kesimpulan

Analisis kerentanan pada website XYZ Repository Management Project telah mengungkap sejumlah kerentanan yang dapat membahayakan keamanan dan integritas sistem. Temuan ini menyoroti pentingnya peninjauan keamanan secara berkelanjutan dalam pengelolaan website dan pengembangan perangkat lunak. Kerentanan seperti keterbukaan file *info.php* dan *IDOR URL Manipulation* menunjukan bahwa ada celah signifikan dalam proteksi keamanan sistem. Tindakan perbaikan yang tepat harus segera diambil untuk mengatasi kerentanan-kerentanan ini dan mencegah penyalahgunaan atau eksploitasi lebiih lanjut. Selain itu, penelitian ini menerapkan pentingnya kesadaran akan keamanan pada semua tahap pengembangan perangkat lunak. Tim pengembang perlu dilatih secara berkala untuk mengenali dan mengatasi kerentanan keamanan serta memprioritaskan keamanan sebagai bagian integral dari siklus pengembangan perangkat lunak.

Dengan mengambil tindakan yang tepat berdasarkan temuan analisis kerentanan, yang menggunakan atau mengelola website XYZ Repository Management Project dapat meningkatkan tingkat keamanan dan mengurangi risiko serangan serta pencurian data yang mungkin terjadi. Kesimpulannya, penelitian ini menegaskan pentingnya pengawasan keamanan yang berkelanjutan dalam pengelolaan website dan pengembang perangkat lunak serta memberikan dasar untuk perbaikan keamanan yang diperlukan untuk melindung sistem dari ancaman yang mungkin timbul.

5.2 Saran

Penelitian ini dilakukan dengan melakukan *penetration testing* dan metode *NIST* sehingga masih banyak cara yang digunakan berkaitan dengan metode tersebut. Saran ini menyajikan rangkuman temuan utama dari penelitian keamanan website beserta rekomendasi untuk meningkatkan keamanan secara keseluruhan dengan keterbatasan pada penelitian. Berikut saran yang dapat dilakukan :

1. Melakukan pengujian *penetration testing*
2. Melakukan *penetration testing* metodologi OWASP TOP 10, EXPLOIT-DB
3. Melaksanakan praktik pengembangan yang aman, termasuk pengguna input validasi, enkripsi data, dan manajemen sandi yang kuat
4. Melibatkan pengujian keamanan atau ahli sebagai *penetration tester* untuk mengidentifikasi dan memperbaiki kerentanan yang baru muncul
5. Memperbarui dan mengoptimalkan konfigurasi server untuk mengurangi potensi kerentanan dan meningkatkan keamanan

DAFTAR PUSTAKA

Asnawi, C., Hariyadi, D., Aesyi, U. S., & Cahyo, P. W. (2023). Analisis dan Penanganan Insiden Siber SQL Injection Menggunakan Kerangka NIST SP 800-61R2 dan Algoritma Klusterisasi K-Means. *Jurnal Komtika (Komputasi dan Informatika)*, *7*(2), 134-144.

C. M. Annur. (2023, September 10). "Pengguna Internet di Indonesia Tebus 213 Juta Orang hingga Awal 2023," Katadata. [Online]. Tersedia: https://databoks.katadata.co.id/datapublish/2023/09/20/pengguna-internet-di-indonesia-tembus-213-juta-orang-hingga-awal-2023.

Gultom, L. M., & Harahap, M. (2018). Analisis Celah Keamanan Website Instansi Pemerintahan di Sumatera Utara. *Jurnal Teknovasi: Jurnal Teknik dan Inovasi Mesin Otomotif*,

Komputer, Industri dan Elektronika, *2*(2), 1-7.

Madiistriyatno, H. (2018). Pengamanan Pengelolaan Hak Akses Web Berbasis Yii Framework. *Syntax Jurnal Informatika*, *7*(1), 1-12

Prasena, R. R. (2020, November). Studi Komparasi Pengembangan Website Dengan Framework Codeigniter Dan Laravel. In *Conference on Business, Social Sciences and Innovation Technology* (Vol. 1, No. 1, pp. 613-621).

P. Winarianto and D. E. Saud (2022, Agustus 09). "CIA TRIAD," Binus. [Online]. Tersedia: https://student-activity.binus.ac.id/csc/2022/08/cia-triad.

Utomo, I. C., & Rokhmah, S. (2022). Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta. *Jurnal Rekayasa Teknologi Informasi (JURTI)*, *6*(2), 143-150.

Widjaja, V., & Widodo, N. M. (2021). Pengaruh Teknologi Internet Terhadap Pengetahuan Masyarakat Jakarta Seputar Informasi Vaksinasi Covid-19. *Tematik*, *8*(1), 1-13.

Yunus, M. (2019). Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4. *Jurnal Ilmiah Informatika Komputer*, *24*(1), 37-48.