BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi jaringan komputer dan internet telah mengubah cara bisnis beroperasi secara signifikan (Ashari, 2020). Website, sebagai salah satu teknologi digital yang umum digunakan, memberikan aksesibilitas yang luas bagi pengguna untuk mengakses informasi dan layanan tanpa terkendala oleh batasan letak dan waktu (Awad et al., 2019). Perkembangan teknologi digital telah mendorong meningkatnya penggunaan website sebagai media utama dalam penyebaran informasi, termasuk pada portal berita online (Devianto & Dwiasnati, 2021). Salah satu contoh media daring yang memanfaatkan teknologi tersebut adalah PT XYZ, yang didirikan pada tanggal 17 Agustus 2015 oleh PT XYZ. PT XYZ memiliki dua situs web utama, yaitu Situs XYZ dan XYZ Jurnalis dan XYZ Editor. Situs Situs XYZ berfungsi sebagai portal publik yang menyajikan berita kepada pembaca, sedangkan XYZ Jurnalis dan XYZ Editor digunakan sebagai sistem manajemen konten yang mendukung aktivitas internal jurnalis dan editor dalam mengelola, menulis, serta menerbitkan berita.

Saat ini, PT XYZ mencatat kunjungan bulanan yang hampir menyentuh angka 300 ribu, menunjukkan tingginya tingkat akses dan interaksi pengguna terhadap layanannya. Dengan tingginya tingkat kunjungan tersebut, aspek keamanan menjadi semakin krusial. Kebocoran data dan peretasan dapat memberikan dampak yang sangat merugikan terhadap reputasi sebuah media (Makridis, 2021). Tidak hanya itu, praktik *spoofing* atau peniruan website yang banyak digunakan untuk menyebarkan misinformasi juga dapat merusak citra media (Petratos, 2021). Ancaman siber tersebut memiliki dampak yang serius terhadap masyarakat. Rendahnya kepercayaan terhadap suatu media akibat banyaknya serangan membuat masyarakat menjadi semakin skeptis terhadap media tertentu (Fletcher & Park, 2017).

Menurut hasil wawancara PT XYZ pernah mengalami insiden peretasan yang menyebabkan seluruh database terhapus akibat serangan siber, kejadian tersebut terjadi pada tahun 2022, tepatnya pada saat hari raya idul fitri. Meskipun data dapat dipulihkan dari cadangan, kejadian ini menunjukkan adanya celah

keamanan yang dapat dieksploitasi. Kasus serupa juga terjadi di media outlet Indonesia lainnya. Pada tahun 2020, Konde.co mengalami serangan DDoS setelah merilis artikel sensitif terkait Kementerian Koperasi (*International Federation of Journalists*, 2020). Project Multatuli, media online yang fokus melaporkan isu-isu perjuangan kaum marjinal, juga menjadi korban serangan siber. Pada tahun 2023, mereka menerima serangan DDoS jenis HTTP *Flood*, botnet, *scraping data*, hingga *payload attack*, setelah menerbitkan laporan investigatif terkait isu sensitif (Cyberthreat.id, 2022). Selain itu, Tempo.co pernah mengalami serangan siber berupa DDoS pada tanggal 7 April 2025. Serangan tersebut melibatkan sekitar 120 juta payload yang menyerang antara pukul 17.50 hingga 19.20 WIB, menyebabkan gangguan akses layanan (Tempo.co, 2025).

Penelitian ini akan menganalisis keamanan sistem informasi pada website portal berita online dengan menggunakan standar OWASP Top 10 2021 serta alat OWASP ZAP untuk menguji potensi kerentanan, dan hasilnya diharapkan dapat memberikan rekomendasi strategis untuk meningkatkan keamanan website serta mengurangi risiko serangan siber yang dapat mengganggu operasional maupun kepercayaan pengguna.

Maka pada penelitian ini akan dilakukan analisis keamanan sistem informasi berupa uji penetrasi terhadap website Situs XYZ. Uji penetrasi bertujuan untuk mengidentifikasi dan memanfaatkan kelemahan yang mungkin ada dalam sistem, dengan tujuan akhir untuk meningkatkan tingkat keamanan secara keseluruhan. Uji penetrasi pada penelitian ini menggunakan kerangka kerja OWASP Top 10 2021. OWASP Top 10 2021 adalah daftar yang disusun oleh komunitas *Open Web Application Security Project* (OWASP) dunia yang mengidentifikasi sepuluh kerentanan keamanan perangkat lunak web yang paling umum. Penggunaan kerangka kerja ini dianggap penting karena telah diadopsi secara luas oleh organisasi dan ahli keamanan di seluruh dunia. Penelitian ini akan memberikan hasil berupa rekomendasi aksi sebagai langkah pencegahan. Diharapkan rekomendasi ini dapat memitigasi risiko yang teridentifikasi, memperkuat lapisan keamanan, dan secara keseluruhan melindungi website Situs XYZ dari potensi serangan siber.

1.2. Rumusan Masalah

Dari permasalahan pada latar belakang dapat diambil rumusan masalah sebagai berikut:

1. Bagaimana tingkat keamanan website PT XYZ menurut kerangka kerja OWASP?
2. Kerentanan apa saja yang menjadi prioritas perbaikan pada ruang lingkup website PT XYZ?
3. Apa tindakan yang dapat diambil untuk memperbaiki keamanan aplikasi web di PT XYZ?

1.3. Tujuan Penelitian

Adapun tujuan dan manfaat dari penelitian ini adalah sebagai berikut:

1. Mengidentifikasi kelemahan keamanan berdasarkan standar yang dijelaskan dalam kerangka kerja OWASP.
2. Menyusun strategi perbaikan dan memperkuat keamanan aplikasi berdasarkan temuan dari evaluasi menggunakan kerangka kerja OWASP.
3. Memungkinkan implementasi perubahan yang spesifik dan efektif, meningkatkan keamanan aplikasi web untuk melindungi data dan infrastruktur perusahaan.

1.4. Batasan dan Asumsi Penelitian

Adapun batasan masalah pada penelitian ini adalah, sebagai berikut:

1. Aplikasi yang dilakukan *penetration testing* pada website Situs XYZ serta XYZ Jurnalis dan XYZ Editor beserta subdomainnya.
2. Ruang lingkup pengujian adalah website Situs XYZ dan XYZ Jurnalis dan XYZ Editor beserta subdomainnya.
3. Teknik *penetration testing* yang digunakan adalah *black box testing*.

1.5. Manfaat Penelitian

1. Bagi penulis, penelitian ini memberikan wawasan tambahan mengenai metode identifikasi kerentanan keamanan pada website melalui pengujian penetrasi berdasarkan framework OWASP TOP 10 2021.
2. Bagi perusahaan, penelitian ini berguna untuk mengungkap potensi kerentanan

pada sistem website yang dimiliki, sehingga dapat mendukung peningkatan keamanan melalui langkah-langkah mitigasi yang disusun berdasarkan hasil uji penetrasi dengan acuan framework OWASP TOP 10 2021.

1.6. Sistematika Penelitian

Penelitian ini akan melalui beberapa tahapan yang telah direncanakan dengan cermat. Tahap pertama akan fokus pada pengumpulan data, yang melibatkan studi literatur untuk merujuk pada jurnal, paper, dan sumber informasi lain yang relevan untuk mendukung penelitian ini. Kemudian, dilakukan analisis website untuk mengevaluasi teknologi yang digunakan dan mendapatkan informasi terkait sistem yang diterapkan. Setelah itu, penelitian akan memasuki tahap implementasi yang mencakup vulnerability scan guna mengidentifikasi potensi kelemahan keamanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Langkah berikutnya adalah uji penetrasi sesuai dengan standar OWASP Top 10 2021 dengan pendekatan *Black Box*, untuk mengetahui tingkat keamanan website Situs XYZ. Tahap akhir dari penelitian akan melibatkan analisis hasil dari uji penetrasi yang telah dilakukan. Analisis ini akan menghasilkan rekomendasi aksi perbaikan yang diperlukan untuk meningkatkan keamanan website Situs XYZ. Dengan melalui serangkaian tahapan ini, diharapkan penelitian dapat memberikan kontribusi yang signifikan terhadap pemahaman keamanan sistem website tersebut.