

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era globalisasi dan transformasi digital saat ini, dunia mengalami perkembangan teknologi informasi yang sangat pesat, khususnya dalam pemanfaatan internet dan sistem berbasis web. Teknologi *website* adalah salah satu alternatif yang paling banyak digunakan, untuk membantu bisnis atau mendapatkan informasi yang orang butuhkan [1]. Semakin berkembangnya aplikasi berbasis web juga diiringi dengan tingginya serangan keamanan dari berbagai teknik ancaman [2]. Keamanan informasi merupakan hal yang harus diperhatikan bagi setiap instansi agar terhindar dari gangguan atau tindakan kejahatan [3]. Meningkatnya penggunaan internet selain menghadirkan kemudahan bagi penggunanya juga bersamaan dengan dampak negatif yang dimunculkan yaitu berupa ancaman keamanan [4]. Masalah keamanan atau gangguan banyak tersebar di internet, gangguan tersebut bisa berupa serangan Malware, Eksploitasi, Injeksi database dan lain sebagainya [3]. Oleh karena itu, diperlukan suatu metode pengujian keamanan yang terstruktur seperti *Information System Security Assessment Framework* (ISSAF) untuk menguji kualitas keamanan *website* berskala global seperti Roblox.

Di tingkat nasional, pesatnya peningkatan penggunaan internet di Indonesia mendorong tingginya akses masyarakat terhadap layanan digital berbasis *website*, termasuk platform permainan daring global seperti Roblox yang banyak digunakan oleh berbagai kalangan usia, khususnya anak-anak dan remaja. Berdasarkan data *Internetworldstate*, terdapat 212,35 juta atau 76.3% dari keseluruhan populasi penduduk Indonesia yang aktif menggunakan internet [4]. Indonesia berada di peringkat ketiga, dengan sekitar 94,5% pengguna internet berusia 16-64 tahun yang bermain video game pada Januari 2022 [5]. Game Roblox menawarkan berbagai fitur interaktif yang memfasilitasi komunikasi dan kolaborasi, seperti obrolan dalam permainan, sistem pertemanan, dan kemampuan untuk membuat avatar serta dunia virtual yang dapat diakses oleh pemain lain [6]. Keberadaan fitur komunikasi terbuka dalam game ini memungkinkan anak-anak berinteraksi dengan pengguna asing tanpa pengawasan,

membuka celah bagi perlakuan tanpa sadar maupun secara sadar yang mengarah kepada eksploitasi dan manipulasi psikologis yang dilakukan kepada anak-anak yang menurut Undang - Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak bahwa anak-anak memiliki hak untuk mendapatkan perlindungan dari hal-hal tersebut [7]. Berdasarkan Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), negara memiliki kewajiban untuk melindungi anak dari praktik eksploitasi ekonomi, termasuk dalam konteks transaksi digital dan permainan daring [8]. Oleh karena itu, diperlukan pengujian kualitas keamanan *website* Roblox secara menyeluruh menggunakan metode *Information System Security Assessment Framework* (ISSAF) guna memastikan perlindungan data, keamanan interaksi, serta keselamatan pengguna, khususnya anak-anak, sesuai dengan peraturan perundang-undangan yang berlaku di Indonesia.

Meskipun Roblox telah menerapkan berbagai mekanisme keamanan, pada praktiknya masih terdapat sejumlah permasalahan yang berpotensi mengancam keamanan sistem dan pengguna. Pada tahun 2022, dunia mulai mencatat peningkatan signifikan dalam aktivitas kejahatan siber, terdapat 2.365 insiden kebocoran data yang dilaporkan secara global, yang menunjukkan bahwa ancaman digital semakin nyata dan meluas [9]. Tindak pidana siber diartikan menurut *Organization of the European Community Development* (OECD) mengartikan kejahatan siber sebagai kejahatan siber merupakan segala macam tindak pidana yang melalui komputer alat untuk merugikan pihak lain [10]. Platform yang awalnya dirancang sebagai media hiburan bagi anak-anak ini telah disalahgunakan oleh beberapa pelaku kejahatan untuk melakukan pendekatan kepada anak-anak yang dapat berujung pada eksploitasi seksual. Berdasarkan *The Legal Journal*, pada tahun 2023, Roblox melaporkan lebih dari 13.000 insiden eksploitasi anak kepada *National Center for Missing and Exploited Children*, yang menunjukkan peningkatan drastis dibandingkan tahun sebelumnya. Di tahun 2022, kasus eksploitasi anak yang dilaporkan hanya sekitar 3.000 insiden, namun laporan kasus eksploitasi anak di tahun 2023 meningkat lebih dari empat kali lipat [6]. Berdasarkan laporan dari *Kaspersky*, sekitar 34 juta kredensial akun Roblox dilaporkan terekspos di *dark web* dalam periode 2021 hingga 2023 akibat serangan

seperti *phishing* dan *malware*. Selain itu, pada tahun 2022 juga terjadi insiden keamanan di mana seorang peretas berhasil memperoleh dan merilis sekitar 4 GB dokumen internal Roblox setelah melakukan serangan *phishing* terhadap karyawan, sebagaimana dilaporkan oleh *Malwarebytes*. Hal ini menunjukkan bahwa masih terdapat potensi risiko keamanan yang signifikan baik dari sisi pengguna maupun sistem internal platform tersebut. Berdasarkan kondisi tersebut, diperlukan evaluasi dan pengujian keamanan *website* Roblox secara sistematis dan menyeluruh menggunakan metode *Information System Security Assessment Framework* (ISSAF) guna mengidentifikasi celah keamanan serta meminimalkan risiko kejahatan siber dan eksploitasi terhadap anak-anak.

Berdasarkan permasalahan tersebut, penelitian ini menggunakan *Information System Security Assessment Framework* (ISSAF) sebagai kerangka kerja dalam melakukan pengujian keamanan *website* Roblox. *Information System Security Assessment Framework* (ISSAF) adalah metode yang digunakan untuk mengevaluasi keamanan sistem, jaringan komputer ataupun kelemahan program aplikasi [11]. Penggunaan ISSAF sebagai kerangka kerja dapat membantu mengidentifikasi secara rinci potensi kerentanan yang mungkin ada pada sistem [12]. *Information System Security Assessment Framework* (ISSAF) yang dikeluarkan oleh OSSIG (*Open System Security Information Group*) merupakan kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi dalam berbagai domain dan rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domain [13]. Penggunaan ISSAF yang didukung oleh *tools Burp Suite* dan *Nessus* diharapkan mampu memberikan hasil evaluasi keamanan yang akurat, terukur, dan dapat dijadikan dasar rekomendasi peningkatan kualitas keamanan *website* Roblox. Dengan penerapan metode ISSAF yang didukung oleh *tools Burp Suite* dan *Nessus*, penelitian ini diharapkan mampu mengukur kualitas keamanan *website* Roblox secara objektif serta memberikan rekomendasi perbaikan yang efektif untuk meningkatkan perlindungan sistem dan pengguna.

Dalam konteks keamanan *website*, masih ditemukan sejumlah penelitian yang membahas identifikasi kerentanan melalui pemindaian maupun asesmen terhadap berbagai aplikasi web. Penelitian yang dilakukan oleh Prihanto et al. menunjukkan bahwa analisis kerentanan menggunakan *vulnerability assessment* pada situs web

perguruan tinggi berhasil mengidentifikasi berbagai celah keamanan yang perlu ditangani, termasuk potensi risiko serangan web seperti injeksi dan konfigurasi yang rentan [14]. Selain itu, penelitian *Vulnerability Assessment* pada aplikasi web pemerintahan menemukan berbagai celah seperti *cross-site scripting* dan *SQL injection* yang dapat membahayakan sistem jika tidak diatasi, sehingga menunjukkan kebutuhan untuk pemindaian sistematis [15]. Penelitian lain juga mengindikasikan bahwa pendekatan *vulnerability assessment* penting untuk mengidentifikasi risiko keamanan pada *website* universitas dan lembaga lain guna menjaga integritas sistem informasi [16]. Namun, sebagian besar penelitian tersebut masih terfokus pada kerentanan umum aplikasi web dan belum secara spesifik mengevaluasi *website* platform game besar seperti Roblox yang memiliki karakteristik tersendiri dalam interaksi dan pertukaran data pengguna. Selain itu, penerapan kerangka kerja terstruktur seperti ISSAF dalam konteks keamanan *website* game online masih sangat terbatas di literatur akademik Indonesia, sehingga kurang memberikan gambaran lengkap tentang kualitas keamanan yang terukur. Dengan demikian, masih terdapat kesenjangan penelitian yang membutuhkan studi lebih mendalam dan komprehensif mengenai penerapan framework terstruktur dalam menguji keamanan *website* skala global seperti Roblox. Karena itu, penelitian ini penting dilakukan untuk mengisi kesenjangan tersebut serta memberikan kontribusi ilmiah yang lebih spesifik terhadap pengujian keamanan *website* game online.

Penelitian pengujian keamanan sistem informasi melalui pendekatan metodologis telah terbukti memberikan kontribusi penting baik dalam ranah akademik maupun praktik pengembangan sistem keamanan web. Beberapa studi keamanan *website* menunjukkan bahwa hasil pemindaian kerentanan tidak hanya membantu dalam mengidentifikasi kelemahan teknis sistem, tetapi juga menjadi dasar rekomendasi perbaikan yang konkret bagi pengelola aplikasi web target penelitian [15]. Penelitian lain yang mengimplementasikan *Vulnerability Assessment* pada berbagai aplikasi web menegaskan bahwa temuan kerentanan seperti *SQL Injection*, XSS, dan masalah konfigurasi dapat digunakan untuk meningkatkan mekanisme kontrol keamanan pada tingkat aplikasi maupun infrastruktur [17]. Selain itu, evaluasi keamanan web melalui metode VA juga

membantu meningkatkan kesadaran tentang pentingnya perbaikan keamanan secara berkelanjutan dalam siklus hidup pengembangan perangkat lunak [18]. Dengan demikian, penelitian ini diharapkan tidak hanya menjadi kontribusi akademik tetapi juga memberi rekomendasi praktis yang aplikatif untuk meningkatkan keamanan *website* Roblox serta menjadi dasar bagi studi lanjutan di bidang keamanan sistem informasi.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan masalah dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana penerapan ISSAF pada *website* Roblox?
2. Kerentanan apa saja yang terdeteksi oleh *Burp Suite* dan *Nessus* pada *website* Roblox?
3. Apa rekomendasi mitigasi keamanan berdasarkan temuan penelitian ini?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditetapkan, maka tujuan dari penelitian ini dapat dijabarkan sebagai berikut:

1. Menerapkan ISSAF pada proses *vulnerability assessment website Roblox*.
2. Mengidentifikasi kerentanan pada sisi aplikasi web dan server menggunakan *Burp Suite* dan *Nessus*.
3. Memberikan rekomendasi mitigasi keamanan berdasarkan hasil temuan *vulnerability assessment*.

1.4 Batasan Masalah

Penelitian ini dibatasi pada ruang lingkup tertentu agar proses analisis lebih terarah dan sesuai dengan tujuan penelitian. Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Fokus penelitian hanya pada *vulnerability assessment* terhadap aplikasi web dan server dengan metode *non-destructive testing*, sehingga tidak dilakukan aktivitas eksploitasi, perubahan data, maupun tindakan yang dapat mengganggu operasional sistem Roblox.

2. Penelitian menggunakan dua tools utama, yaitu *Burp Suite* dan *Nessus*, yang keduanya dioperasikan pada sistem operasi Windows untuk menjaga konsistensi lingkungan pengujian.
3. Target pengujian terbatas pada *website* Roblox, khususnya pada subdomain publik atau halaman web yang secara eksplisit memperbolehkan aktivitas vulnerability assessment sesuai aturan dan kebijakan Roblox.

1.5 Manfaat Penelitian

Penelitian ini diharapkan bermanfaat dan dapat menjadi referensi dalam pengujian keamanan sistem informasi. Adapun manfaat penelitian ini adalah sebagai berikut:

1. Menambah wawasan dan literatur mengenai penerapan ISSAF dalam pengujian keamanan sistem informasi, khususnya pada platform game daring berskala besar seperti Roblox.
2. Memberikan referensi tentang efektivitas dan perbandingan penggunaan dua tools keamanan, yaitu *Burp Suite* dan *Nessus*.
3. Memberikan masukan dan rekomendasi mitigasi keamanan yang dapat digunakan oleh pengembang dan tim keamanan Roblox untuk meningkatkan keamanan aplikasi dan server mereka.
4. Membantu praktisi keamanan dalam memilih tools yang tepat serta memahami kelebihan dan keterbatasan masing-masing tools dalam mendeteksi kerentanan.