BAB I
PENDAHULUAN

1.1 Latar Belakang

Menurut data terbaru dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), penggunaan internet di Indonesia pada tahun 2024 diperkirakan telah mencapai lebih dari 221 juta pengguna, meningkat signifikan dibandingkan dengan angka sekitar 210 juta pada tahun 2022[1]. Peningkatan ini menunjukkan bahwa semakin banyak masyarakat Indonesia yang memanfaatkan internet untuk berbagai keperluan, termasuk pendidikan, bisnis, dan interaksi sosial.

Dengan meningkatnya jumlah pengguna internet di Indonesia, ancaman keamanan siber menjadi semakin serius. Pada awal tahun 2024, tercatat hampir 6 juta ancaman siber yang terjadi selama kuartal pertama, dari Januari hingga Maret. Ketua BSSN, Luki Hermawan, mengungkapkan bahwa dalam periode Januari hingga September 2022, Indonesia mengalami lebih dari 852 juta anomali lalu lintas siber. Dari jumlah tersebut, infeksi malware menyumbang 55,6%, kebocoran data mencapai 15,20%, dan serangan trojan tercatat sebesar 10,21%[2]. Fakta ini menunjukkan pentingnya menjaga keamanan website dengan baik guna memastikan perlindungan terhadap informasi.

Sebagian besar serangan ini terjadi ketika pengguna mengunjungi situs web yang terinfeksi, sering kali tanpa disadari oleh mereka. Metode serangan yang umum termasuk malware tanpa file, yang beroperasi dengan cara menyusup ke sistem tanpa meninggalkan jejak yang jelas untuk analisis [3]. Selain itu, data menunjukkan bahwa 21,2% pengguna mengalami serangan melalui web, menempatkan Indonesia pada peringkat ke-96 secara global dalam hal risiko terkait penjelajahan web [3].

Pada tahun 2024, terjadi sebuah penyerangan pada website sebuah universitas, yang menargetkan mahasiswa yang mencari pekerjaan freelance. Hacker berpura-pura menjadi seorang klien yang membutuhkan mahasiswa untuk melakukan tugas seperti like dan subscribe video di platform YouTube. Namun,

tugas-tugas tersebut sebenarnya berisi malware yang berfungsi untuk menginstal *Remote Access Trojan* (RAT) pada perangkat mahasiswa [4]. Dengan demikian, hacker dapat melakukan *keylogging* dan memantau aktivitas mahasiswa secara diam-diam. Contoh kasus ini mirip dengan penipuan yang dialami oleh Syifa Giarsyah pada tahun 2023, di mana ia terjebak dalam skema penipuan online yang menawarkan pekerjaan *freelance* seperti like dan subscribe video di YouTube. Namun, setelah beberapa tugas, Syifa diminta untuk melakukan deposit di website kripto, yang akhirnya membuktikan bahwa ia telah menjadi korban penipuan.

Terdapat berbagai metodologi dan kerangka kerja yang direkomendasikan untuk uji penetrasi pada tahun 2025, salah satunya adalah *Information System Security Assessment Framework* (ISSAF). Penggunaan kerangka kerja ISSAF dalam penelitian saat ini semakin relevan karena ISSAF menawarkan cakupan domain yang komprehensif, memungkinkan pengujian dilakukan baik dari luar maupun dalam sistem website [5]. Dengan kemampuan cakupan domain yang baik, ISSAF dapat membantu dalam mengidentifikasi kerentanan secara menyeluruh, memperhatikan kontrol keamanan yang ada agar tidak merusak sistem website yang diuji. Di tengah meningkatnya serangan siber seperti *ransomware dan phishing*, pendekatan ini menjadi penting untuk memastikan keamanan data dan integritas sistem informasi. Penelitian terbaru menunjukkan bahwa penerapan ISSAF dapat mengungkap berbagai celah keamanan, termasuk serangan *SQL Injection dan Cross-Site Scripting (XSS)*, serta memberikan rekomendasi perbaikan untuk meningkatkan pertahanan sistem terhadap ancaman yang terus berkembang [6].

Dalam skripsi ini, akan dibahas mengenai pengujian penetrasi yang dilakukan berdasarkan kerangka kerja ISSAF, dengan menerapkan setiap tahapan untuk mengidentifikasi kerentanan yang terdapat pada *website* target. Hasil dari pengujian ini akan dianalisis secara mendalam, dan rekomendasi akan diberikan untuk mengatasi kerentanan yang ditemukan serta untuk meningkatkan keamanan *website*. Dengan meningkatnya ancaman siber di tahun 2025, penting bagi pemilik *website* untuk memahami dan mengatasi potensi risiko yang dapat membahayakan data pengguna dan integritas sistem.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah sebagai berikut :

1. Bagaimana cara melakukan analisis uji penetrasi menggunakan *framework* ISSAF untuk mengidentifikasi celah keamanan pada *website* yang diuji sebagai acuan pengujian keamanan *website* lain?
2. Apa saja kerentanan yang terdeteksi pada *website* menggunakan *framework* ISSAF?
3. Bagaimana strategi yang dapat diterapkan untuk meningkatkan keamanan *website* guna memitigasi potensi serangan siber pada *website* yang diuji?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Pengujian ini difokuskan pada *website dummy*, yang merupakan *web* pengujian untuk bisa diterapkan pada *website* lain nantinya.
2. Pengujian penetrasi dilakukan dengan metode *black box testing*, sehingga informasi yang diperoleh terbatas, menggunakan *framework* ISSAF.
3. Uji coba dilakukan dengan memperhatikan keamanan sistem, tanpa menggunakan alat yang dapat membahayakan integritasi *website* lain.
4. Hasil pengujian akan didokumentasikan secara sistematis dan disusun dalam laporan yang jelas dan mudah dipahami, guna memberikan rekomendasi perbaikan untuk meningkatkan keamanan *website* tersebut.
5. Penelitian ini hanya berfokus pada analisis celah keamanan dan memberikan rekomendasi mitigasi uji penetrasi, tanpa melakukan eksploitasi lebih lanjut yang dapat merusak sistem sesuai *framework* ISSAF.
6. Jenis serangan yang diuji dalam penelitian ini dipilih pada *framework* ISSAF yaitu: *SQL Injection, Cross-Site Scripting (XSS) Attack, dan Cross-Site Request Forgery (CSRF) Injection* sebagai skenario pengujian.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah sebagai berikut:

1. Mengetahui dan memahami metode uji penetrasi yang dapat diterapkan pada *website dummy* sebagai acuan untuk pengujian keamanan pada *website*

lain serta mengidentifikasi celah keamanan sistem menggunakan *framework* ISSAF.

2. Menganalisis kerentanan yang terdeteksi pada *website dummy* untuk memahami tingkat risiko yang dihadapi.
3. Memberikan rekomendasi solusi yang efektif untuk memitigasi kerentanan yang ditemukan pada *website dummy*, guna meningkatkan keamanan dan perlindungan data pada *website* lain yang sejenis.

1.5 Manfaat Penelitian

1. Manfaat Teoritis
   - Menambah wawasan dan pemahaman mengenai metode uji penetrasi pada *website* menggunakan *framework* ISSAF.
   - Menyediakan referensi bagi peneliti lain dalam bidang keamanan siber, khususnya terkait identifikasi dan mitigasi celah keamanan pada *website*.
2. Manfaat Praktis
   - Memberikan panduan bagi pengelola *website* dalam melakukan pengujian keamanan berbasis *website dummy* sebelum diterapkan pada sistem yang sebenarnya.
   - Membantu meningkatkan kesadaran akan pentingnya keamanan siber dan penerapan langkah-langkah mitigasi untuk mengurangi risiko serangan terhadap *website*.
3. Manfaat Akademis
   - Menyediakan studi kasus yang dapat digunakan dalam pembelajaran keamanan sistem informasi dan uji penetrasi di bidang akademik.
   - Mendorong pengembangan penelitian lebih lanjut dalam meningkatkan metode uji penetrasi dan perlindungan *website* terhadap ancaman keamanan.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi pada penelitian ini dibagi ke dalam 5 bab, yaitu:

BAB I PENDAHULUAN

Dalam bab ini, dibahas mengenai latar belakang masalah, identifikasi rumusan masalah, tujuan penulisan, batasan masalah, metodologi penelitian, manfaat penelitian, serta sistematika penulisan laporan skripsi. Latar belakang ini memberikan konteks penting terkait isu yang diangkat dalam penelitian, serta alasan mengapa topik tersebut relevan untuk diteliti saat ini.

BAB II DASAR TEORI

Bab ini membahas landasan teori yang menjadi dukungan bagi penelitian, mencakup berbagai literatur dan jurnal terkini yang relevan. Teori-teori yang diuraikan meliputi metode uji penetrasi serta *tools* yang diperlukan dalam penelitian. Pembaruan informasi dari literatur terbaru sangat penting untuk memastikan bahwa teori yang digunakan adalah *state-of-the-art* dan sesuai dengan perkembangan terkini dalam bidang keamanan siber.

BAB III PERANCANGAN SISTEM

Di bab ini, dijelaskan mengenai rancangan sistem yang mencakup spesifikasi penelitian dan alur penelitian untuk melakukan uji penetrasi. Rancangan ini harus mencerminkan pendekatan yang sistematis dan terstruktur untuk memastikan efektivitas dalam pengujian yang dilakukan.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menguraikan berbagai implementasi dalam tahap pengujian penetrasi untuk menganalisis *website* target. Penggunaan beberapa *tools* terkini bertujuan untuk menemukan dan menganalisis kerentanan pada *website* tersebut. Diskusi di bagian ini juga mencakup evaluasi terhadap hasil pengujian dan rekomendasi mitigasi yang dapat diterapkan.

BAB V PENUTUP

Dalam bab ini, disajikan kesimpulan dari hasil penelitian serta cara-cara mitigasi terhadap kerentanan yang ditemukan. Selain itu, saran untuk penelitian selanjutnya juga dibahas untuk memberikan arah bagi studi-studi mendatang dalam

bidang yang sama. Penutup ini menekankan pentingnya terus menerus melakukan penelitian dan pengembangan dalam keamanan siber agar tetap relevan dengan tantangan baru yang muncul.