BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era digital saat ini, masyarakat cenderung mencari informasi terkini dari berbagai sumber melalui situs *web*. Hal ini menjadikan situs *web* sebagai salah satu *platform* yang paling sering digunakan untuk memenuhi kebutuhan informasi [1]. Semakin pesatnya perkembangan teknologi informasi telah membawa dampak positif di berbagai sektor, termasuk dalam perkembangan teknologi internet. Salah satu penerapannya adalah penggunaan situs *web* yang menjadi alat utama bagi banyak instansi pemerintah dan bisnis untuk melindungi data serta mendukung aktivitas mereka. Namun, masih banyak perusahaan yang membangun situs *web* sebagai media penyimpanan data tanpa memastikan bahwa situs tersebut memenuhi standar CIA *Triad*, yang digunakan untuk mengukur tingkat keamanan sebuah situs *web* [2].

Di Indonesia telah banyak mengalami pertumbuhan signifikan dalam adopsi aset digital, dengan berbagai *platform* yang memfasilitasi perdagangan aset kripto. Salah satunya *platform* terkemuka Indodax (PT Indodax Nasional Indonesia), Indodax merupakan sebuah perusahaan teknologi yang berfungsi sebagai pasar digital terbesar di Indonesia untuk transaksi aset kripto. didirikan pada tahun 2014, Indodax termasuk dalam 11 *platform* resmi yang terdaftar dan diawasi oleh Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti), menjamin kepatuhan terhadap regulasi keuangan di Indonesia. Platform ini dapat diakses melalui antarmuka web berbasis *browser* atau aplikasi mobile. Fitur-fitur utamanya meliputi pemantauan saldo aset digital, transfer antar-wallet, deposit, dan penarikan dana dalam mata uang rupiah, yang dirancang dengan antarmuka pengguna yang intuitif. Namun, meskipun memiliki reputasi yang kuat, beberapa pengguna melaporkan kendala teknis dan fungsionalitas melalui ulasan *Google Play Store* [3].

Seiring kemajuan teknologi, *website Indodax.com* juga semakin rentan terhadap ancaman peretasan dan berbagai risiko keamanan digital. Salah satu contohnya adalah serangan *Distributed Denial of Service* (DDoS), *Cross-Site*

Scripting (XSS), serangan injeksi, dan bentuk ancaman lainnya. DDoS bekerja dengan membanjiri lalu lintas server hingga layanan tertentu menjadi tidak dapat diakses. Sementara itu, XSS merupakan metode eksploitasi yang menyisipkan kode berbahaya ke dalam situs web, memungkinkan pencurian data, modifikasi tampilan, bahkan pengambilalihan sesi pengguna. Oleh karena itu, evaluasi berkala terhadap kerentanan keamanan sangat diperlukan guna memastikan perlindungan optimal bagi *website Indodax.com* dari berbagai ancaman dunia maya [4].

Pada penelitian ini difokuskan untuk pengujian keamanan situs *webite https://indodax.com/* melalui metode penetration testing dengan pendekatan kerangka ISSAF [5]. ISSAF merupakan kerangka kerja yang berfungsi untuk mengevaluasi keamanan sistem informasi secara menyeluruh melalui tahapan seperti perencanaan, pengumpulan informasi, pengujian kerentanan, dan pelaporan hasil. Dalam studi kasus, ISSAF terbukti efektif dalam menganalisis keamanan aplikasi berbasis web melalui pendekatan berlapis yang sesuai dengan praktik pengujian penetrasi [6].

Dalam uji penetrasi penelitian ini, peneliti akan menggunakan sistem operasi kali linux. Alasan peneliti menggunakan kali linux karena dirancang khusus untuk penguji penetrasi dan keamanan informasi serta menyediakan lebih dari 600 alat yang mendukung berbagai aspek pengujian keamanan, seperti analisis kerentanan, eksploitasi, dan forensik digital. Selain itu, Kali Linux bersifat open-source, sehingga memungkinkan fleksibilitas dalam penggunaannya untuk berbagai kebutuhan pengujian keamanan[7]. Penggunaan Kali Linux didasarkan pada keunggulannya dalam mendukung metode penetration testing yang sistematis dan efisien. Dengan tools berjalan seperti whois, Nmap, Nikto, *Metasploit,* dan *Wireshark,* Kali Linux memungkinkan analisis mendalam terhadap kerentanan sistem dan aplikasi berbasis website seperti indodax. Hal ini sejalan dengan pendekatan ISSAF yang mengutamakan evaluasi keamanan secara menyeluruh melalui tahapan-tahapan yang terstruktur [8].

Berdasarkan uraian, peneliti bermaksud melakukan penelitian mengenai celah keamanan *website* untuk mengetahui sejauh mana tingkat keamanannya. Oleh karena itu, peneliti tertarik melakukan penelitian dengan judul “Pengujian

Kualitas Celah Keamanan Informasi pada *Website Indodax.com* dengan Metode *Penetration Testing* Menggunakan *Information System Security Assessment Framework* (ISSAF)". Penelitian ini menggunakan metode *penetration testing* dengan pendekatan ISSAF untuk menguji tingkat keamanan informasi pada *website* tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Apa saja kerentanan atau celah keamanan yang terdapat pada website Indodax.com berdasarkan hasil pengujian menggunakan metode *penetration testing*?
2. Bagaimana tingkat risiko yang ditimbulkan oleh celah keamanan tersebut terhadap sistem informasi pada *website* Indodax.com?

1.3 Tujuan Penelitian

Penelitian ini memiliki tujuan yang diharapkan sebagai berikut yaitu:

1. Mengidentifikasi kerentanan atau celah keamanan yang terdapat pada website Indodax.com melalui pengujian menggunakan metode penetration testing.
2. Menganalisis tingkat risiko yang ditimbulkan oleh celah keamanan tersebut terhadap sistem informasi pada website Indodax.com

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini dirancang untuk memfokuskan lingkup penelitian agar lebih terarah dan dapat diselesaikan secara efektif. Berikut adalah batasan masalah yang diterapkan:

1. Penelitian ini hanya berfokus pada *website* Indodax.com sebagai objek utama untuk mengevaluasi keamanan informasi.
2. Penelitian menggunakan metode *penetration testing* dengan kerangka kerja *Information System Security Assessment Framework* (ISSAF).
3. Alat bantu yang digunakan adalah *tools* berbasis *Kali Linux* seperti *Nmap*, *OWASP ZAP*, dan *SQLmap* dan lain-lain.

4. Penelitian hanya mengevaluasi aspek keamanan informasi berdasarkan prinsip CIA *Triad (Confidentiality, Integrity, Availability).*
   Penelitian ini dibatasi oleh waktu dan sumber daya yang tersedia, sehingga tidak semua jenis serangan atau kerentanan dapat diuji secara mendalam.

1.5 Manfaat Penelitian

Manfaat dari penelitian mengenai Pengujian Kualitas Celah Keamanan Informasi Pada Website Indodax.com Dengan Metode Penetration Testing Menggunakan Information System Security Assessment Framework (ISSAF) adalah:

1. Mengetahui tingkat kerentanan keamanan informasi yang terdapat pada website Indodax.com berdasarkan hasil pengujian.
2. Menjadi bahan evaluasi untuk meningkatkan sistem keamanan website agar lebih tahan terhadap berbagai jenis serangan siber.
3. Memberikan pemahaman mengenai penerapan metode *penetration testing* dengan pendekatan ISSAF dalam mengidentifikasi celah keamanan.
4. Menambah wawasan dan pengetahuan dalam bidang keamanan informasi, khususnya terkait penggunaan tools Kali Linux seperti Nmap, SQLmap, dan OWASP ZAP.
5. Menjadi referensi bagi penelitian selanjutnya yang berkaitan dengan keamanan sistem informasi dan pengujian penetrasi terhadap situs web.